Introduction to Mathematical Reasoning (MATH163 University of Saskatchewan)
ver. April 2021

A note on the text (April 2021)

In 2019, the Department of Mathematics and Statistics introduced a new course *MATH163 Introduction to Mathematical Reasoning* for all students in their programs. This course was designed to make explicit in the curriculum fundamental notational and cultural norms within mathematics so as to ease the path of students though upper-year courses in mathematics. Subsequently this course was adopted as a required course for students studying in the Department of Computer Science (starting 2022) and a recommended course for students completing a certification in high-school mathematics education.

In lieu of a course text, these notes are designed to be a companion for students learning the material in MATH163. They are written for students who are interested in mathematics but have little mathematics experience beyond high-school studies in pre-calculus. Notably, the implied reader of these notes has no experience with mathematical proof, writing and formalism. Great effort is made to be explicit about notation, terminology and that choices in these regards are cultural; they are not inherently right or wrong, however best practice for communicating to others dictates that we adhere to standard usage.

These notes were created during the Autumn 2021 semester at the University of Saskatchewan. They were born out of necessity; the ongoing effects of COVID-19 lead to a full cessation of on-campus activities. For students in MATH163 in that semester, the first draft of these notes comprised of their weekly reading for the course. Prior to each section of each chapter there was a 5-7 minute video introducing the broad ideas in the reading. Additionally, there were weekly drop-in office hours with the instructor to answer questions about course material.

Each section of the notes corresponds to roughly one week of material. As the following text comprises only ten chapters, in a standard in-person thirteen week semester, this leaves space for expansion. Previous in-person deliveries of this course have culminated with an introduction to number theory and significantly expanded the work in cardinality to introduce both combinatorics and the hierarchy of cardinalities of power sets.

Each section of the notes begins with a list of learning incomes and outcomes. The former list tells the reader what material they need to be familiar with in order to understand the upcoming material. Readers should return to the latter list once they have finished their work in section to be sure they have attained the learning outcomes.

Each section of the notes ends with a part titled *Test Your Understanding*. In general, these questions are not designed to challenge a reader. Instead they are meant to be a check of broad understanding of the key ideas in the section. Challenging the learner to engage more fully with the material is a task left to assessed course work.

Throughout the text the reader will find short diversions under the heading **aside**. This fragments of text often present ideas beyond the stated learning outcomes and sometimes require students to have a more mature mathematical background than the stated learning incomes. These parts of the text can be fully ignored without detriment. There are also a

small number of sections marked as **Optional**. These sections require students to have a background/sophistication beyond what is expected for students in this class.

The approach and ordering of the topics in this text is adapted from *Transition to Higher Mathematics: Structure and Proof, 2Ed.* by Dumas and McCarthy. This open-access text is an excellent supplementary resource for the material contained herein.

The many errors herein are the sole responsibility of the original author. Note, however, that in some places this text intentionally opts for small fibs in pursuing a broader learning objective.

-cd

Contents

1 Sets and Functions Part I

Learning Incomes.

- *Exposure to the idea of a mathematical function.*
- *Familiarity with standard mathematical notation used in SK secondary-school courses Foundations of Mathematics 30 or Precalculus 30*
- *Reading ability at a level at least that of an SK secondary-school graduate.*

Newly Defined Terms and Notation. *element ($\in$), natural numbers ($\mathbb{N}$), rational numbers ($\mathbb{Q}$), real numbers ($\mathbb{R}$), integers ($\mathbb{Z}$), set-builder notation, A equals B ($=$), A is a (proper) subset/superset of B ($\subset, \subseteq, \supseteq, \supset$), the union of A and B ($\cup$), the intersection of A and B ($\cap$), cartesian product of A and B ($\times$), domain of the variable.*

A good conversation to have at the start of any class (in mathematics or otherwise) is one of motivation for the course material. Sometimes mathematics courses get away with a hand wave towards *real-world* application or *improving reasoning skills*, but I think we can do a little bit better here.

We will spend most of our time in MATH 163 muddling with abstract nonsense. We'll prove discuss abstract objects and ideas often without any clear or obvious application to industry. This isn't to say that the work we do doesn't have applications in these areas – in fact the opposite is true. However, applying the material in this course to other domains requires background knowledge that we don't have. And so, at some point, you may find yourself thinking *why am I learning this?*.

Put plainly, you are learning this material now so that when you take future courses in mathematics, you are free from the burden of having to learn about the practice of mathematics while you learning new mathematical material. This course is designed to introduce you to standard norms and practices in mathematical notation and communication while also exposing to you some mathematical ideas that arise in many different mathematical domains.

The College of Arts and Sciences at the University of Saskatchewan espouses a model of *liberal arts education*. The idea is that by studying material in a variety of disciplines (including humanities classes!) we can become more culturally literate members of our society. A university education isn't the only means of attaining this literacy, and indeed one can argue that at times it isn't a particularly effective means to this goal.

For those of you who are unlikely to pursue further courses in mathematics or computer science, your learning in this course is unlikely to provide you with additional training to *do* anything in your (eventual) profession. For you, this course is part of your broader education in becoming a more culturally literate member of society. By immersing yourself

in the course material you are learning what it is like to be a mathematician – to grapple with abstract ideas that may only exist in our collective human consciousness.

Our primary goal in this course is understanding mathematical theory, not performing computations or algebraic manipulations. More often than not, we will exhibit our understanding though written explanations in complete sentences. As we progress though the course, we will talk more about what is means to *explain* as a mathematician. For now, the key thing to remember is that defined terms have meanings – they are, in a sense, shorthand for precise ideas. Thought these notes, newly defined terms are underlined. We define these terms to develop a common vocabulary so that we may communicate our mathematical ideas with ambiguity. Most of time, our difficulty in understanding (and subsequently, being able to explain) stems from an incomplete understanding of definitions.

But this is enough talking *about* mathematics for now. Let us move to actually talk some mathematics.

1.1 Preliminaries

Intuitively, a mathematical set is a collection of unique objects. Let us begin by considering a set that we may already familiar with.

Definition 1.1. *The set of natural numbers is the set* $\{0, 1, 2, 3, \dots\}$. *We denote this set by* $\mathbb{N}$

Aside. *Some people exclude* 0 *as being a natural number. This is perfectly fine and reasonable. This is a matter of preference, and there is no universal convention. In these notes, we shall use* $\mathbb{N}^+$ *to denote* $\{1, 2, 3, \dots\}$.*)*

Even without more formality, this first definition gives us a method to express the objects of a set. That is, we write down its members between braces: $\{0, 1, 2, 3, \dots\}$. Here the ellipsis denotes that we continue with the pattern.

It is not an overstatement to say that sets underpin just about every mathematical concept that you have ever encountered. This is not an obvious statement, but something we will discover throughout this semester. Thus your background mathematics knowledge already gives you some intuition about sets! And so perhaps you are already familiar with the following definition.

Definition 1.2. *When* X *is a set and* x *is a member of* X, *we say that* x *is an element of* X. *When* x *is an element of* X *we write* $x \in X$. *We write* $x \notin X$ *when* x *is not an element of* X.

Relying on our familiarity with the natural numbers we may write $4 \in \mathbb{N}$ and $\frac{1}{2} \notin \mathbb{N}$. These notations are just shorthand for the sentences "4 is in the set of natural numbers" and "$\frac{1}{2}$ is not in the set of natural numbers". The only reason to prefer the notation over the sentence is for brevity.

Our notation for set membership extends nicely to talk about multiple things being elements of the same set. For example, we can write "$2, 4 \in \mathbb{N}$" to mean "$2 \in \mathbb{N}$ and $4 \in \mathbb{N}$".

In this class we are going to define a lot of terms. We do this so that we can develop a common vocabulary to communicate precise ideas. In every definition the newly defined term will be underlined. From then on when we use that term we all have the same understanding of what the term means.

There are numerous ways to tell a reader what elements are contained in a particular set. If a set has few elements, then it may be defined by listing out the elements explicitly. For instance, $\{1, 3, 5, 7\}$ is the set of the first four odd numbers. The order in which we write the elements does not matter. The set $\{1, 3, 5, 7\}$ is the same set as

$\{1, 5, 3, 7\}$. Repeating elements also does not matter. The set $\{1, 3, 5, 7\}$ is the same set as $\{1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 3, 5, 7\}$

For sets with too many elements to list, we must provide the reader with a means to determine membership in the set. We can inform our reader that not all elements of the set have been listed, but that enough information has been provided for the reader to identify a pattern for determining membership in the set. For example, let X denote the set $\{2, 4, 6, 8, \ldots, 96, 98\}$. Here X is the set of positive even integers less than 100. However, using an ellipsis to define a set may not always work: it assumes that the reader will identify the pattern we wish to characterize.

Notice how many times the word reader is used in that last paragraph. This suggests that the purpose of using notation is to communicate unambiguously with a reader. We will return to this idea throughout the course.

Some sets are used so commonly that they have standard names and notations. Some of these you may have seen before.

Definition 1.3. *The integers are the elements of the set* $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. *This set is denoted by* $\mathbb{Z}$.

The rational numbers are the elements of the set

$$\left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}.$$

This set is denoted by $\mathbb{Q}$.

The real numbers is the set of numbers that appear on the number line. This set is denoted by $\mathbb{R}$.

Aside. *We use the symbol* $\mathbb{Z}$ *for integers because of the German word zhalen, which means numbers. We use the symbol* $\mathbb{Q}$ *for the rational numbers because of the Italian word quoziente, which means quotient. Both of these conventions go back hundreds of years.*

The symbols we use for these sets, $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *are written differently than we would write the letters* N, Z, Q, R. *These symbols are printed in blackboard script. They harken back to a time long ago (circa. 2019) when mathematics was primarily taught on a blackboard. Written this way,* $\mathbb{N}$ *will always refer to the natural numbers. Whereas we can use* N *as a label for other things if we need it.*

The definitions of $\mathbb{Q}$ and $\mathbb{R}$ express sets in a different way than just listing out the elements. In defining $\mathbb{R}$ we have just written a sentence. This is a perfectly acceptable way to define a

set. For example, it is perfectly reasonable to say *let S denote the set of students registered in MATH163.*

Let us look more closely at our definition of the rational numbers, $\mathbb{Q}$.

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid \ p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}.$$

In fact this jumble of symbols is a sentence.

"$\mathbb{Q} =$ "	translates to	"The set $\mathbb{Q}$ is defined to be"
"$\frac{p}{q}$"	translates to	" those elements with the form $\frac{p}{q}$
"$\mid$"	translates to	" where"
"$p, q \in \mathbb{Z}$ and $q \neq 0$"	translates to	" p and q are integers and q is not equal to 0"

And so when we see

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

we think (and say and read) "The set $\mathbb{Q}$ is defined to be those elements with the form $\frac{p}{q}$ where p and q are integers and q is not equal to 0". (Think for a moment– are you convinced that saying a number is rational number is equivalent to saying can be expressed in the form $\frac{p}{q}$ where p and q are integers and q is not equal to 0"?)

Our method for describing $\mathbb{Q}$ is easily adapted to define other sets. This method of describing a set is called *set-builder notation*. We will use this method quite often.

Definition 1.4. *Let X be a set, and let $P(x)$ be a statement that is either true or false for each $x \in X$. The set*

$$\{x \in X \mid P(x)\}$$

is the set of elements in X for which $P(x)$ is true. The set X is called the domain of the variable.

Often $P(x)$ is a mathematical formula. For instance, suppose $P(x)$ is the formula "$x^2 = 4$". By $P(3)$ we mean the formula with 3 substituted for x, that is $P(3)$ is the statement "$3^2 = 4$". If the substitution results in a true statement for some particular value of x, we say that $P(x)$ holds, or $P(x)$ is true. Otherwise we say that $P(x)$ does not hold, or $P(x)$ is false. In our example, $P(2)$ is true and $P(3)$ is false.

Example 1.5. *Let X denote the set*

$$\{0, 1, 4, 9, \ldots\}.$$

Using set-builder notation we can express this set as

$$X = \{x \in \mathbb{N} \mid \text{there exists } y \in \mathbb{N}, \text{so that } \ x = y^2\}.$$

*Here $P(x)$ is the formula "*there exists $y \in \mathbb{N}, \text{so that } \ x = y^2$*". The formula $P(x)$ is true whenever x is a perfect square. The formula $P(x)$ is false whenever x is not a perfect square.*

Example 1.6. *Let Y denote the set of positive even integers less than 100. The set Y can expressed as*

$$\{z \in \mathbb{N} \mid z < 100 \text{ and there exists } n \in \mathbb{N}^+ \text{ so that } z = 2n\}.$$

Take a moment to determine what $P(z)$ is. Are you convinced that $P(z)$ is true for every positive even integer less than 100 *and false otherwise?*

Aside. *There was no reason here to choose z as a variable over x in the definition of the set Y. Nothing would change if we replaced z with x in the definition of Y. Okay... I suppose the purpose of choosing z was so that I could add in this aside to make the point that variable names generally don't matter...*

For the sake of brevity, an author may not explicitly identify the domain of the variable. Be careful of this, as such an author is relying on the reader to make the necessary assumptions. For instance, consider the set

$$\{x \mid (x^2 - 2)(x - 1)(x^2 + 1) = 0\}.$$

If the domain of the variable is assumed to be $\mathbb{N}$, then

$$\{x \mid (x^2 - 2)(x - 1)(x^2 + 1) = 0\} = \{1\}.$$

If the domain of the variable is assumed to be $\mathbb{R}$, then

$$\{x \mid (x^2 - 2)(x - 1)(x^2 + 1) = 0\} = \{1, \sqrt{2}, -\sqrt{2}\}.$$

Remember, the burden of clear communication is always the author. (And so the burden is me to communicate that we will reuse names for sets very often. Two sets named X, for example, in different parts of the notes usually aren't referring to the same set.)

Another alternative is to include the domain of the variable in the condition defining membership in the set. So, if X is the intended domain of the set and $P(x)$ is the condition for membership in the set we may write $\{x \mid x \in X \text{ and } P(x)\}$ to mean $\{x \in X \mid P(x)\}$.

Example 1.7. *Consider the set $A = \{x \in \mathbb{N}^+ \mid x$ is divisible by* 2 *or x is divisible by* 3$\}$. *In this example $P(x)$ is the formula "x is divisible by* 2 *or x is divisible by* 3*". Let us consider some elements of the domain of the variable to understand which elements of $\mathbb{N}^+$ are elements of A.*

- $P(1)$ *is the statement "1 is divisible by 2 or 1 is divisible by 3." This is false, thus* $1 \notin A$.
- $P(2)$ *is the statement "2 is divisible by 2 or 2 is divisible by 3." Since* 2 *is divisible by* 2 *it follows that* $P(2)$ *is true and so* $2 \in A$.
- $P(3)$ *is the statement "3 is divisible by 2 or 3 is divisible by 3." Since* 3 *is divisible by* 3 *it follows that* $P(3)$ *is true and so* $3 \in A$.
- $P(4)$ *is true and so* $4 \in A$.
- $P(5)$ *is false and so* $5 \notin A$.
- $P(6)$ *is the statement "6 is divisible by 2 or 6 is divisible by 3". Since* 6 *is divisible by* 2 *it follows that* $P(6)$ *is true and so* $6 \in A$.
- *... this seems to be taking a while. Examining each element of* $\mathbb{N}^+$ *individually will take us more time than we have! Instead of this let us think a little about* $P(6)$.

Looking at $P(6)$ *might give us some pause. We might expect* $P(6)$ *to be false as* 6 *is divisible by* 2 *and* 6 *is divisible by* 3. *Usually in English we think of "or" as being a statement of exclusivity – either this is true or that is true. In mathematics this is not the case. By convention we assume an "or" statement to be inclusive. The statement "this is true or that is true" means that at least one of "this" or "that" is true.*

Thus A can be described as the set of all positive integers that are multiples of 2 *together with those positive integers that are multiples of* 3.

For convenience we permit the existence of a set containing no objects. We call this set the empty set and we denote it as $\{\}$. Sometimes the empty set is denoted as $\emptyset$. This choice of notation is a matter of preference.

Example 1.8. *As sets are able to contain any objects, it is reasonable to think of sets that contain other sets. For example, If* $A = 0, 1$ *and* $B = \{3\}$, *then the set* $\{A, B\}$ *is a set with two elements. The elements of the set* $\{A, B\}$ *are themselves sets, which happen to also contain elements.*

Optional things to think about–

How does this approach to mathematics compare from what you have seen in past math classes? Certainly there is no computation to be found, nor is there any half-hearted attempt to talk about real-world applications. Nor are there pictures to be seen anywhere. The only thing we really need, at this point, is our reading comprehension and a want to think carefully about what we are reading.

1.2 Relating Sets and Set Operations

Open again the notes from Section 1.1 and look at the middle of page at the discussion about the importance of specifying the domain of a variable.

.
.
.
.
.
.
.
.

Does our use of the equals sign give you pause when we write

$$\{x \mid (x^2 - 2)(x - 1)(x^2 + 1) = 0\} = \{1\}?$$

Probably not – our previous intuition about the equals sign gives us a pretty good idea of what we mean when we write this statement. But as we are taking the time to carefully define lots of other notation, it is probably good to have an agreed upon meaning for = when we talk about sets.

When are two sets equal? We might be inclined to say that two sets are equal provided they have the same elements. This then forces us to ask the question, what does it mean for two elements to be the same. This might depend on the elements. Is the function $g : \mathbb{Z} \to \mathbb{R}$ so that $g(x) = x^2$ the same function as $f : \mathbb{Z} \to \mathbb{N}$ so that $f(x) = x^2$? Even when our elements are numbers sameness might not always be clear. Is 4 the same as $\frac{16}{4}$?

Definition 1.9. *Let A and B be sets. We say A equals B when every element of A is an element of B and every element of B is an element of A. When A* equals *B we write $A = B$. When A does not equal B we write $A \neq B$.*

(If $X = Y$, then certainly $Y = X$, right? Does this follow from our definition of =?)

This definition seems a bit unwieldy. But I assure you that it will come in handy when our sets are more complicated than just sets of numbers.

There is a small bit of subtly in our use of the equal sign in mathematics. Sometimes we use the equals sign to talk about two things (sets, numbers, etc..) being equal. For example, $28 = 7 \times 4$. Other times we use the equals sign to assign a label to a particular thing (set, number, etc..) For example, let $f(x) = x^2$. In computer science the convention is to write := instead of = for this second use. Unfortunately this is not a convention adopted across other areas of mathematics.

Equality isn't the only way to relate to two sets, much in the same way the equality isn't the only way to relate two numbers. You may be familiar with the following pieces of notation denoting relations between various sets.

Definition 1.10. *Let X and Y be sets.*

When every element of X is also an element of Y we say X is a subset of Y and Y is a superset of X. When X is a subset of Y we write $X \subseteq Y$ or $Y \supseteq X$.

When X is a subset of Y and $X \neq Y$ we say X is a proper subset of Y and we write $X \subset Y$ or $Y \supset X$.

Example 1.11. *Let A denote the set $\{0, 1, 2\}$. What are all of the sets that are a subset of A? What are all of the sets that are a proper subset of A? To determine this we look back at the definition of subset and proper subset.*

The set $\{1, 2, 4\}$ is not a subset of A nor it is a proper subset of A. This set contains elements that are not elements of A. Whereas the set $\{1, 2\}$ is a subset of A and is also a proper subset of A. As is the set $\{2\}$. On the other hand, $\{0, 1, 2\}$ is a subset of A but not a proper subset of A.

What about the empty set? For now we will take it to be true, by convention, that the empty set is a subset of every set. We will justify this in a later module.

Take a moment now to list out the subsets of A. There are 8 of them. How many of these are proper subsets?

Just as we an relate sets in a similar way to how we relate numbers, we can define operations for sets just like we have operations for numbers.

Definition 1.12. *Let X and Y be sets.*

The union of X and Y, denoted as $X \cup Y$, is the set

$$X \cup Y = \{x, \mid x \in X \text{ or } x \in Y\}.$$

The intersection of X and Y, written $X \cap Y$, is the set

$$X \cap Y = \{x \mid x \in X \text{ and } x \in Y\}.$$

The cartesian product of X and Y written $X \times Y$, is the set of all ordered pairs whose first element is from X and second element is from Y. That is

$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}.$$

Aside. *The cartesian product is named for René Descartes. (17C France) Cartesian should sound familiar. The set $\mathbb{R} \times \mathbb{R}$ is the set of all ordered pairs where both elements are from $\mathbb{R}$. This seems a lot like the Cartesian plane, which we often denote as $\mathbb{R}^2$.*

Often times when we think about operations we think of it as something to "do". For example, from our experiences we would likely interpret "$7 + 3$" as "find the result when 3 things are added to 7 things". This interpretation isn't correct, but it is limiting. More broadly, "$7+3$" *is* a number. Is it is the same number as 10. This is why is would be correct to write $7 + 3 \in \mathbb{Z}$. The number represented by the symbols "$7 + 3$" is an integer. In all of mathematics we could replace the notation 10 with the notation $7 + 3$ and nothing would change.

Look again at the definition of set union. The union of X and Y *is* a set. We can talk about its elements. We can use it in other operations. More often in this course (and beyond) it will be more helpful to think of $X \cup Y$ as set rather than an instruction. The same is true for set intersection.

Aside. *Recall our discussion in Example 1.7 about the mathematical meaning of the word "or". Consider the sets $\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 2\}$ and $\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 3\}$. In Example 1.7 we seemed to get at the idea that*

$$A = \left\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 2\right\} \cup \left\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 3\right\},$$

but at the time we didn't have the terminology and subsequent notation to express this idea. (The set A is defined as in Example 1.7) But now that we have an agreed upon definition for set equality and set union we can verify that

$$A = \left\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 2\right\} \cup \left\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 3\right\}$$

But how?

We will spend a lot of time in this class talking about proofs. Without going too far into detail (right now) we can consider a proof to be a justification of a mathematical fact. In this case our mathematical fact is

$$A = \left\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 2\right\} \cup \left\{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 3\right\}$$

To justify that this is true, we can use our definition of equality for sets. (Take a moment now to go back and read it.) Let $B = \{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 2\}$ and $C = \{x \in \mathbb{N}^+ \mid x \text{ is divisible by } 3\}$. To convince our reader $A = B \cup C$ we must convince our reader that every element of A is an element of the set $B \cup C$ and every element of $B \cup C$ is an element of the set A. This is exactly what is meant by writing $A = B \cup C$.

We first convince our reader that every element of A is an element of the set $B \cup C$. Consider any element $a \in A$. Since $a \in A$, it is true that a is divisible by 2 or a is divisible by 3. If a is divisible by 2, then a is a multiple of 2 and so $a \in B$. If a is divisible by 3, then a is a multiple of 3 and so $a \in C$. In either case, we have $a \in B \cup C$. Therefore every element of a is an element of $B \cup C$.

We now convince our reader that every element of $B \cup C$ is an element of the set A. Consider any element $d \in B \cup C$. Since $d \in B \cup C$ it is true that d is an element at least one of B or C. If d is an element of B, then d is a multiple of 2, and so must be divisible by 2. Thus we conclude that $d \in A$. Similarly, if d is any element of C, then d is a multiple of 3, and so must be divisible by 3. Thus we conclude that $d \in A$. In either case we see that $d \in A$.

Since every element of A is an element of $B \cup C$ and every element of $B \cup C$ is an element of A, then by definition of set equality we can conclude $A = B \cup C$.

We'll come back to the structure of this argument at a later time. This is meant to be a first example of how a proof can look.

What about set operations involving more than two sets? Unlike arithmetic, for which there is a default order of operations, there is not a universal convention for the order in which set operations are performed. And so we must use parentheses to let our reader know the order in which the operations of union and intersection should be done. For the cartesian product we can make meaning of an expression with more than two sets as follows.

Example 1.13. *Points in three dimensions are often specified with a triple of real numbers (x, y, z), where x is the coordinate on the x-axis, y is the coordinate on the y-axis and z is the coordinate on the z-axis. We often refer to the set of all points as $\mathbb{R}^3$. Much as we can use the cartesian product of sets to think about the cartesian plane, we can use the cartesian product to think about 3D space. Consider $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$. We didn't explicitly define this, our definition of cartesian product was the product of two sets. But our choice of notation is flexible enough that we would likely understand $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ to denote the set of ordered triples where each element is an element of $\mathbb{R}$. Similarly, we can define the cartesian product of any number of sets.*

Definition 1.14. *Let k be a positive integer and let $X_1, X_2, \ldots, X_k$ be sets. Denote by $X_1 \times X_2 \cdots \times X_k$ the set*

$$X_1 \times X_2 \cdots \times X_k = \{(x_1, x_2 \ldots, x_k) \mid x_1 \in X_1, x_2 \in X_2, \ldots, x_k \in X_k\}$$

That is, $X_1 \times X_2 \cdots \times X_k$ is the set of ordered k-tuples where the ith element of the k-tuple is an element of X_i for each $1 \leq i \leq k$.

When $X = X_1 = X_2 = \cdots = X_k$ we write $X_1 \times X_2 \cdots \times X_k = X^k$.

This definition might seem a little intimidating at first, but it is very similar to the definition of cartesian product above. If we let $k = 2$ and write our this definition we get exactly our definition for cartesian product above. Once we fix some value of k, this definition gives meaning to notation $X_1, X_2, \ldots, X_k$.

- $X_1 \times X_2 \cdots \times X_k$ – is the notation we use to refer to this set.
- $(x_1, x_2 \ldots, x_k)$ – tells us that elements of this set are ordered $k-$tuples (like an ordered pair or an ordered triple, but with k parts instead of 2 or 3).
- $x_1 \in X_1, x_2 \in X_2, \ldots, x_k \in X_k$ – tells us that the first element of this $k-$tuples (namely x_1) is an element of X_1, the second element of this $k-$tuple (namely x_2) is an element of X_2, etc...

Example 1.15. *Let* $A = \{0, 1\}, B = \{7\}, C = \{cat, dog\}$. *We have*

$$A \times B \times C = \{(0, 7, cat), (1, 7, cat), (0, 7, dog), (1, 7, dog)\}$$

and

$$A^3 = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$$

With this notation it is now clear why we use $\mathbb{R}^2$ to refer to the cartesian plane – by definition we have

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

Other things to think about

- Nothing in Module 1 is required to do mathematics on one's own. These definitions and notations serve only our desire to communicate mathematical ideas with one another. Most of this notation was not standardized until the end of the 19th century. This fact is interesting for lots of reasons, chiefly among them is that the ideas of calculus were developed around two hundred years prior. It is only by way of modern mathematical conventions that today's mathematicians are able to easily communicate with one another through research publications and presentations.
- For those with a background/interest in computing – certainly every programming language you have ever used can check for set equality. Can you devise a simple algorithm to check if two sets are equal? (... you had better hope your sets are finite!)
- For those with a background/interest in teaching – what would you tell a young student who was wanted to make up and use their own symbols for numbers?
- Notice how $=, \subseteq$, and $\subset$ for sets seem reminiscent for $=, \leq$ and $<$ for numbers. We can use $<$ to define an ordering for numbers. Smaller numbers appear earlier in the

ordering as compared to larger numbers. Can we define an ordering for sets using $\subset$? What is an ordering, anyway?

- In this section we carefully defined equals ($=$) and subset ($\subseteq$) for sets. These definitions give us very specific criteria for when we may say two sets are equal or one set is a subset of another. Can you do the same for integers? That is, can you write down definitions of equals and less than that give specific criteria for when two numbers or equal or when one number is less than another?

Test Your Understanding

1. In Example 1.11 we listed out all of the subsets of a set with three elements. There were 8 of them. Can you find a formula (as a function of k) for the number of subsets of a set that has k elements? You don't need to justify why your formula is correct; just try some different values of k and see what you can notice.
2. In Example 1.15 the set $A \times B \times C$ had four elements. How many elements would be in the set $A \times B \times C \times \{x, y\}$? How many elements will there be in the set A^4? Can you find formula (as a function of k) for the number of elements in the set A^k? You don't need to justify why your formula is correct; just try some different values of k and see what you can notice.
3. Look back at Example 1.8. Does $\{A, B\} = A \cup B$? How many elements are in each?
4. Look back at the Aside that starts on page ???. In this Aside we provide an argument that convinces us that

$$\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 2 or } x \text{ is divisible by 3}\} =$$
$$\big\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 2}\big\} \cup \big\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 3}\big\}$$

   Our argument proceeded by applying the definition of $=$. We convinced our reader that every element of $\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 2 or } x \text{ is divisible by 3}\}$ is an element of

$$\big\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 2}\big\} \cup \big\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 3}\big\}$$

   and every element of

$$\big\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 2}\big\} \cup \big\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 3}\big\}$$

   is an element of $\{x \in \mathbb{N}^+ \mid x \text{ is divisible by 2 or } x \text{ is divisible by 3}\}$.

   Let us try the same approach to prove the following mathematical fact:

   Let A and B be sets. If $A \cup B = A$, then $B \subseteq A$.

   (Feel encouraged to copy directly any relevant sentences from the above)

Test Your Understanding Solution

2 Sets and Functions Part II

Learning Incomes.

- *Material presented in Module 1*
- *Exposure to the idea of a mathematical function.*
- *Familiarity with standard mathematical notation used in SK secondary-school courses Foundations of Mathematics 30 or Precalculus 30*
- *Reading ability at a level at least that of an SK secondary-school graduate.*

Newly Defined Terms and Notation. *function, domain, codomain, $f : A \to B$, image, a pre-image, $f(a)$, the pre-image, $f^{-1}(b)$, range, range(f), injection, surjection, bijection, operation, inverse, f^{-1}.*

In Module 1 we saw an introduction to various notations and definitions for sets. From our work in the last module we should recognize the following ideas–

Let A and B be sets. Each of the following are statements

- $A = B$
- $A \subseteq B$
- $B \subseteq A$
- $A \subset B$
- $B \subset A$

Depending on what the sets A and B are, each of these statements are each either true or false. Whereas each of the following are sets

- $A \cup B$
- $A \cap B$
- $A \times B$

If $A = \{1, 7, 9\}$ and $B = \{1, 7\}$, then

- $A = B$ is false;
- $A \subseteq B$ is false;
- $B \subseteq A$ is true;
- $A \subset B$ is false; and
- $B \subset A$ is true.

- $A \cup B = \{1, 7, 9\}$;
- $A \cap B = \{1, 7\}$; and
- $A \times B = \{(1, 7), (1, 9), (7, 7), (7, 9), (9, 7), (9, 9)\}$.

Let us take a moment to return to Exercise **??** from Module 1. This exercise asked you to provide a proof for the following statement:

Let A be B be sets. If $A \cup B = A$, then $B \subseteq A$.

In this context, a proof is written logical deduction that fully convinces a reader of the truth of the statement. This statement is making a claim about all possible pairs of sets, A and B. Thus is not enough to provide an example or two to fully justify that this statement is always true.

We have seen two proofs in this course already – one in Aside 1.2 and one in Exercise 4. Let us consider, informally, how we might prove the above statement.

We want to show that if some hypothesis holds, in this case $A \cup B = A$, then our conclusion, namely $B \subseteq A$, holds. But of course these jumbles of symbols just correspond to sentences. Thus we should take a moment to remind ourselves what these symbols mean.

Looking back at our definition for $\cup$ and $=$, the statement $A \cup B = A$ is exactly equivalent to the following statement: *Every element that is in at least one of A and B is an element of A and every element of A is an element of at least one of A and B.*

This statement is not true for every pair of sets A and B; but it is only those pairs of sets that satisfy the hypothesis that we are interested in. Looking back at our definition of $\subseteq$ we want to conclude that *every element of B is an element of A.*

Okay, so how can we do this?

Let us consider some element $b \in B$. We want to convince ourselves that, in fact, $b \in A$. From our hypothesis we know that every element that is in at least one of A and B is an element of A. Since b is an element of B is it is an element of at least one of A and B and thus is an element of A. Therefore $b \in A$.

Thus no matter which element of B we chose, we can be sure that it is always an element of A. This is the same as saying B is a subset of A, which is what we were trying to prove.

Now that we have convinced ourselves, the time has come to convince someone else. Unfortunately, most written proofs strip away the extraneous detail and just focus on what is necessary.

Theorem. *Let A be B be sets. If $A \cup B = A$, then $B \subseteq A$.*

Proof. Let A and B be sets so that $A \cup B = A$. Consider $b \in B$. Since $A \cup B = A$ it follows that every element of B is an element of A. Thus $b \in A$. Therefore $B \subseteq A$, as required. $\square$

(Do you see that little box over there on the right? It is a convention in mathematics to write this little box at the end of proof. This is a signal to the reader that the proof is done and the author expects them now to be convinced.)

Depending on our expected reader, this proof is less than ideal. For someone who has just learned the meaning of all the different notation, this proof would be very difficult to read. On the other hand, for someone who is very comfortable with the notation, this proof has all of the necessary detail.

We turn now to the main matter of Module 2: functions. We have spend years getting comfortable with the notation and terminology around functions like $f(x) = x^2$. It turns out that these notations and terminology are flexible enough that we can use them for functions where in the input and output may not even be numbers Our goal in this module is to develop notation and terminology for functions. Of course, we first need to agree on what we mean when we say function!

2.1 Functions

Our intuition around function is likely some sense of "assigning". That is, a function assigns a value (an output) to each input. A function, then, in some sense, can be considered to be a set of pairs: the input and the assigned output.

Consider the following set

$$A = \{(z, z^2) \mid z \in \mathbb{R}\}$$

Using our notation from the previous module we notice $A \subseteq R \times R$ – recalling our definition of the notation $\subseteq$ and the notation $\times$ we should be convinced that every element of A is an ordered pair whose first entry is from $\mathbb{R}$ and whose second entry is from $\mathbb{R}$.

(If you are not easily convinced, then you should go back to Module 1 and re-read the corresponding definitions. This should not suggest you have done something wrong in your learning. We will spend lots of time in this course referring to concepts and definitions from previous modules.)

The set A has many elements, let us examine some of them.

- $(0, 0) \in A$ as $0 \in R$ and $0 = 0^2$
- $(-3, 9) \in A$ as $-3 \in \mathbb{R}$ and $9 = (-3)^2$
- $\left(\sqrt{2.1}, 2.1\right) \in A$ as $\sqrt{2.1} \in \mathbb{R}$ and $2.1 = \left(\sqrt{2.1}\right)^2$

With not a lot of thought we should be able to convince ourselves that the elements of A are exactly the points of the parabola $f(x) = x^2$. Similarly, we can construct such a set for any function. For example consider $g(x) = \sin(x)$. The set of points of this curve are exactly the points in the set

$$\{(x, \sin(x)) \mid x \in \mathbb{R}\}$$

Let us consider another example. Let S be the set of students registered in MATH163 and consider the set

$$\{(s, g) \,|s \in S \text{ and } g \text{ is the grade that student } s \text{ gets in MATH163.}\}$$

Aside. *... this set doesn't exist yet. Your grade in the course is far from determined!*

Much like our set representation for $f(x) = x^2$ we have a set of ordered pairs in this set. In this case the ordered pair has a student as its first entry and that student's grade as the

second entry. Much like our function $f(x) = x^2$ we can consider the the second entry in the ordered pair to be "assigned" to the first entry.

With these examples in mind, we define a function as follows.

Definition 2.1. *Let A, B and f be sets. We say f is a function from A to B when f is a subset of $A \times B$ in which each element of A appears as the first entry of an ordered pair exactly once. When f is a function from A to B we write $f : A \to B$. We say that A is the domain of f and that B is the codomain of f*

Aside. *Let us parse the structure of this definition one part at a time:*

- Let A, B and f be sets.
  - *This sentence tells us the names of the objects we will need to define our new term.*
- We say f is a function from A to B
  - *The underlined part is the new term we are defining.*
- when f is a subset of $A \times B$ in which each element of A appears as the first entry of an ordered pair exactly once.
  - *This is what we mean we use our newly defined term. Our new term is shorthand to express this idea. In other words, this is the criteria that the set f must satisfy so that we may call it a function.*
- When f is a function from A to B we write $f : A \to B$.
  - *This sentence gives us a piece of notation to go along with our new definition. The piece of notation is shorthand for the underlined term in the second part.*
- We say that A is the domain of f and that B is the codomain of f
  - *Our new definition has a second definition hiding inside!*

The ordered pairs in f tell us which element of the codomain is assigned to each element of domain. To ensure that each element of A is assigned exactly one element of the codomain, we required that every element of A appears as the first entry of an ordered pair exactly once. Notice that we have no restriction on how many times an element of the codomain can appear? For $f(x) = x^2$ we are okay with having $(2, 4) \in f$ and $(-2, 4) \in f$.

Let us consider some examples.

Example 2.2. *First we consider the notion of functions with which we are likely intimately*

familiar: functions from $\mathbb{R}$ *to* $\mathbb{R}$*. Consider the line* $y = 2x$*. Every point on this line is of the form* $(x, 2x)$ *and all points of the form* $(x, 2x)$ *appear on the line.*

Consider the set $f = \{(x, 2x) \mid x \in \mathbb{R}\}$*. We notice that for any particular* $z \in \mathbb{R}$*, the number* z *only appears in a single ordered pair: the ordered pair* $(z, 2z)$*. For example, the real number* 11 *only appears as the first entry of the ordered pair* $(11, 22)$*.* 11 *appears as the first entry of no other element of* f*. Thus this set fulfills our definition of* f is a function from $\mathbb{R}$ to $\mathbb{R}$.

Example 2.3. *Let* $A = \{1, 7, 9\}$*,* $B = \{1, 7, 9, 10\}$ *and*

$$f = \{(1, 7), (7, 7), (7, 9), (9, 9)\}$$

Using our new definition of function we can ask: is f *a function from* A *to* B*?*

Let us read the definition of function one part at a time:

- Let A, B and f be sets.
  - *This is true. Certainly* A, B *and* f *are sets.*
- f is a subset of $A \times B$
  - *This is true; every element of* f *is an element of* $A \times B$ *as each element is an ordered pair which as its first entry from* A *and its second entry from* B*.*
- each element of A appears as the first entry of an ordered pair exactly once.
  - *This is false;* 7 *appears as the first entry of an ordered pair twice. Both of* $(7, 7)$ *are* $(7, 9)$ *elements of* f*.*

The set f *does not satisfy the definition of function from* A *to* B *and so we cannot say that* f *is a function from* A *to* B*.*

Exercise 2.4. *Let* $A = \{1, 7, 9\}$*,* $B = \{1, 7\}$ *and*

$$f = \{(1, 7)\,(9, 9)\}$$

Is f *a function from* A *to* B*?*

In these last two examples our sets were named A, B and f to make it easy to think about the definition of a function. Most of the time the labels of our objects (sets, functions, etc...) will not match the labels that are used in the definition.

Example 2.5. *Let*

$$h = \left\{ \left(\frac{a}{b}, b \right) | \frac{a}{b} \in \mathbb{Q} \text{ and } \tfrac{a}{b} \text{ is in lowest terms} \right\}.$$

For example, $(\frac{1}{2}, 2) \in h$*, but* $(\frac{1}{2}, 3) \notin h$ *and* $\left(\frac{2}{4}, 2\right) \notin h$*.*

Can we say h *a function from* $\mathbb{Q}$ *to* $\mathbb{Z}$*? We appeal to our definition with* $\mathbb{Q}$ *playing the role of the domain,* $\mathbb{Z}$ *playing the role of the codomain and* h *playing the role of* f*.*

Each of $\mathbb{Q}, \mathbb{Z}$ *and* h *are sets. Elements of* h *are ordered pairs, where the first element is a rational number in lowest terms and the second element is an integer. The set* h *contains every ordered pair of this form. For any* $\frac{x}{y} \in \mathbb{Q}$ *in lowest terms, we have* $\left(\frac{x}{y}, y\right) \in h$*. Thus we see* h *a function from* $\mathbb{Q}$ *to* $\mathbb{Z}$*.*

Let us return back to familiar territory with the function $f(x) = x^2$. Quite likely we understand the notation $f(7) = 49$. Put in terms of our new definition of a function, this is equivalent to saying $(7, 49) \in f$. As every function can be represented as set, we can extend our use of this piece of notation for any function.

Definition 2.6. *Let* A *and* B *be sets and let* f *be a function from* A *to* B*. For* $(a, b) \in f$ *we say* b *is the image of* a *and* a *is a pre-image of* b*. When* b *is the image of* a *we write* $f(a) = b$*.*

Example 2.7. *Let* $h : \mathbb{Q} \to \mathbb{Z}$ *be the function given in Example 2.5. Let us apply our definition of image to the element* $\left(\frac{4}{9}, 4\right) \in h$*. Since* $\left(\frac{4}{9}, 4\right) \in h$ *we can say that* 4 *is the image of* $\frac{4}{9}$ *and we can write* $h\left(\frac{4}{9}\right) = 4$*.*

Exercise 2.8. *Let* $A = \{1, 7, 9\}$*,* $B = \{1, 7, 9, 10\}$ *and*

$$f = \{(1, 7)\,(7, 7)\,, (9, 1)\}$$

Which element of B *is* $f(7)$*? Does it makes sense to talk about* $f(15)$*?*

Our definition of function requires that each element of A appear as the first entry in exactly one ordered pair of f. Thus for each $a \in A$ the notation $f(a)$ has unambiguous meaning; $f(a)$ is the element of B so that the pair $(a, f(a))$ is an element of f.

Example 2.9. S *be the set of students in MATH163. Let* $N = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$*. Let* q *be the function from* S *to* N *so that* $q(s)$ *is the first entry in the student number of student* s*.*

In this case we can see that we can use our definition and corresponding notation to fully specify a function. By writing "... so that $q(s)$ is the first entry in the student number of student s." *we are describing the set*

$$q = \{(s, n)\,|s \in S \textit{and the first entry of } s \textit{ student number is } n\}$$

Describing q as the function so that $q(s)$ is the first entry in the student number of student s is a lot easier than asking our reader to parse the jumble of notation we need to describe q using set-builder notation.

We can give all of the information about a function by stating its domain, its codomain and the image of each element of the domain. This is what we are doing when we write something like: *let $f : \mathbb{R} \to \mathbb{R}$ so that $f(x) = 2x + 3$*. By convention we understand this statement of notation to mean: *let f be the function from $\mathbb{R}$ to $\mathbb{R}$ so that the image of an element $x \in \mathbb{R}$ is $2x + 3$*. This is equivalent to writing *let f be the function from $\mathbb{R}$ to $\mathbb{R}$ so that*

$$f = \{(x, 2x + 3) \,| x \in \mathbb{R}\}$$

Let us return back to the familiar ground of $f(x) = x^2$. How do we interpret the notation $f^{-1}(7)$? Perhaps the word *inverse* or *pre-image* slipped past our mental lips as we read that last sentence? (It is okay if it didn't!)

Aside. *Are you bothered by the fact that we didn't specify a domain and codomain for $f(x) = x^2$? From our shared experiences in mathematics we likely understood the domain to be $\mathbb{R}$ and the codomain to be $\mathbb{R}$. Remember – all of these tools we are developing are to ease communication. If we are certain that our reader will understand what we mean, then we need not be so precise.*

Definition 2.10. *Let A and B be sets, let f be a function from A to B and let b be an element of B. The <u>pre-image of b</u> is the set $\{a \in A | f(a) = b\}$. We denote this set as $f^{-1}(b)$.*

Let us pick apart this definition one sentence at a time:

- *Let A and B be sets, let f be a function from A to B and let b be an element of B.*
  - This sentence sets up the rest of the definition. It tells us about the mathematical objects we will need to define our new term.
- *The <u>pre-image of b</u> is the set $\{a \in A | f(a) = b\}$.*
  - This sentence tells us the term that we are defining. For some particular $b \in B$ the pre-image of b is defined to be the set of all elements of A that have b as their image.
- *We denote this set as $f^{-1}(b)$*
  - This sentence gives us a piece of notation to use for our new definition. When we see the symbols $f^{-1}(b)$ we should say "the pre-image of b"

Aside. *Look at all of the things that we need to understand before we can understand the*

meaning of the notation $f^{-1}(b)$. We need to know what a set is. We need to know the definition of a function. We need to know about set builder notation. We need to know the meaning of the symbol $f(a)$.

We think of functions and related things to be relatively straight-forward ideas and they are. But trying to precisely define these concepts takes work! However, there is a payoff: we are developing a shared vocabulary. What is more, you are sharing this vocabulary with fellow students and mathematicians throughout the (western) world! The standardization of these notations is a relatively recent occurrence in the history of mathematics. It is only in the last hundred years or so that these notations have become standard. In fact, it isn't really true to say that all of this notation is standard. For example, just as some people exclude 0 *from* $\mathbb{N}$*, so too do some use the symbol* $\subsetneq$ *to mean proper subset. There is nothing inherently correct or incorrect about these choices. They are just standards that make it easier for us to communicate.*

When we read a definition that we don't understand, a usual reason is that we don't yet understand all of the meanings of the words in the definition. As we grapple with new definitions we will need to backtrack at times to remember the proscribed meanings of all of the words in our new definition.

Aside. *In Definition 2.6 we defined a pre-image and in Definition 2.10 we defined the pre-image. These ideas are related. A pre-image is an element of the domain. The pre-image is a set of elements of the domain. Articles matter!*

Example 2.11. *Let $f : \mathbb{R} \to \mathbb{R}$ so that $f(x) = x^2$. The notation $f^{-1}(49)$ denotes the set of all elements of $\mathbb{R}$ whose image is* 49*. We notice $7^2 = 49$ and $(-7)^2 = 49$ and so $f^{-1}(49) = \{-7, 7\}$.*

Example 2.12. *Let S be the set of students in MATH163. Let $N = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Let q be the function so that $q(s)$ is the first entry in the student number of student s. Looking at my class list, I see that no student in MATH163 has a student number that begins with* 0*. The set $\{s \in S | q(s) = 0\}$ contains no elements. This set is the empty set. We can express this idea much more compactly by writing: $q^{-1}(0) = \{\}$.*

Our definition of function requires that we specify a domain and a codomain. There is nothing in the definition of function that requires that every element of the codomain be the image of some element of the domain. We saw this in Example 2.12. Thus we can consider the set of elements of the codomain that appear as the image of some element of the domain.

Definition 2.13. *Let A and B be sets and let f be a function from A to B. The range of f, denoted range(f), is the set of elements of B that are the image of some element of A. That*

is, we have

$$range(f) = \{f(a) \in B | a \in A\}$$

We should understand the range of a function to be the set of all elements of the codomain that appear as an image of an element in domain.

Example 2.14. *Let $f : \mathbb{N} \to \mathbb{R}$ so that $f(x) = \sqrt{x}$. Though the domain of f has been defined to be the set of all real numbers, not every real number is the square root of some natural number The set $range(f)$ is the set of all numbers that are a square root of some natural number.*

Exercise 2.15. *Let $A = \{1, 7, 9\}$ and let f be the function from A to A so that $f(1) = 1$ and $f(7) = 9$ and $f(9) = 9$. What elements are contained in $range(f)$?*

Exercise 2.16. *Let $f : \mathbb{Z} \to \mathbb{R}$ so that $f(x) = 2x + 1$. Notice that $range(f) = \mathbb{Z}$. If we change the domain to $\mathbb{R}$, how does this change the range?*

Example 2.17. *Continuing with Example 2.12.*

Since $q^{-1}(0) = \{\}$, there is no element $s \in S$ so that $q(s) = 0$. Thus $0 \notin range(q)$.

In fact, every student in this course has a student number that begins with 1. Therefore $range(q) = \{1\}$.

Let us use some of our new notation and terminology to prove a mathematical fact:

Theorem. *Let A and B be sets. If $f : A \to B$ and $g : A \to range(f)$ so that $g(a) = f(a)$ for each $a \in A$, then for each $b \in range(f)$ we have $g^{-1}(b) \neq \{\}$.*

Yikes! Let us parse this one part at a time. We start with our hypothesis:

If $f : A \to B$ and $g : A \to range(f)$ so that $g(a) = f(a)$ for each $a \in A$,

We are imagining the existence of these two functions, f and g, that satisfy the following:

- f has domain A and codomain B;
- g has domain A. The codomain of g is the set of elements of B that are the image of some element of a with respect to the function f.
- the image of an element of A with respect to the function g is the same as the image with respect to the function f.

And now the conclusion:

then for each $b \in range(f)$ *we have* $g^{-1}(b) \neq \{\}$.

We want to show that each element of $range(f)$ satisfies the following:

- the preimage of the element is not the empty set. That is, for each $b \in range(f)$ there is an element of a so that $g(a) = b$

(It may help you to work through this notation with a particular function f. Let $A = \{1, 7, 9\}$ and $B = \{1, 2, 3, 4, 5, 6, 7\}$. Let $f(1) = 2$, $f(7) = 2$ and $f(9) = 6$.

Use the definition of $range(f)$ to determine what elements are contained in $range(f)$? What ordered pairs are contained in the set g? Use the definition of pre-image to determine elements are in the set $g^{-1}(2)$?)

To prove our mathematical fact we assume our hypothesis is true and try to conclude that our conclusion is true. Consider some element $b' \in range(f)$. We want to conclude that $g^{-1}(b')$ is not the empty set. That is, we want to convince ourselves that there is an element of $a' \in A$ with the property that $g(a') = b'$.

Let us remember what it means for b' to be an element of $range(f)$: since $b' \in range(f)$ there exists $a' \in A$ so that $f(a') = b'$.

Since we assumed our hypothesis is true, we know that $g(a') = f(a')$. Since $f(a') = b'$ we know that $g(a') = b'$. Thus $a' \in g^{-1}(b')$. Which in turn implies that $g^{-1}(b') \neq \{\}$.

Let us compact our reasoning into a proof.

Proof. Let A and B be sets. Let $f : A \to B$ and $g : A \to range(f)$ so that $g(a) = f(a)$ for each $a \in A$.

Consider $b' \in range(f)$. Since $b' \in range(f)$ there exists some $a' \in A$ so that $f(a') = b'$. Since $f(a) = g()$ for each $a \in A$ it follows that $g(a') = b'$. Thus $a' \in g^{-1}(b')$. □

2.2 Injections, Surjections and Bijections

Consider all of the numbers on the number line. We call this set $\mathbb{R}$. Some of these numbers have interesting properties. For example, the set of integers , $\mathbb{Z}$, is the subset of the set of real numbers consisting of those real numbers that have no decimal part. The set of rational numbers, $\mathbb{Q}$, is the subset of the real numbers that can be represented as a ratio of two numbers in $\mathbb{Z}$. Much as we can consider sets of real numbers that have notable properties, so too can be think about particular functions that satisfy notable properties.

Let $A = \{1, 4, 9\}$ and $B = \{1, 7\}$. There are many different functions from A to B. (We will count them another day!) Some of these functions have their range equal to their codomain. For example, the function from A to B given by

$$\{(1, 7), (4, 1), (9, 1)\}$$

has codomain equal to $\{1, 7\}$ and range equal to $\{1, 7\}$.

Whereas the function

$$\{(1, 7), (4, 7), (9, 7)\}$$

does not have this property.

Definition 2.18. *Let A and B be sets and let f be a function from A to B. We say f is a surjection when range$(f) = B$. When f is an surjection we say that f is surjective*

Notice that if a function is an surjection, then the preimage of every element of the codomain contains at least one element.

Consider the function $f : \mathbb{R} \to \mathbb{R}$ so that $f(x) = 2x+1$. This function has the extra property that the image of each element of the domain is unique; no two elements of the domain have the same image. That is, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

On the other hand, the function $f : \mathbb{R} \to \mathbb{R}$ so that $f(x) = x^2$ does not have this property We can notice $f(-7) = f(7)$.

Definition 2.19. *Let A and B be sets and let f be a function from A to B. We say f is an injection when each element of the domain has a unique image. When f is an injection we say that f is injective*

Notice that if a function is an injection, then the preimage of every element of the codomain contains at most one element.

Exercise 2.20. *Let $A = \{1, 4, 9\}$ and $B = \{1, 7\}$ be sets. Can you find a function from A to B that is both an injection and surjection? Can you find a function from A to A that is*

both an injection and a surjection?

Definition 2.21. *Let A and B be sets and let f be a function from A to B. We say f is a bijection when f is both an injection and a surjection. When f is an bijection we say that f is bijective*

Exercise 2.22. *Let A and B be sets and let f be a bijection from A to B. Is it possible for the pre-image of some element of B to contain no elements? Is it possible for the pre-image of some element of B to contain two elements?*

Aside. *You might recognize the terms* "one-to-one" *and* "onto" *rather than the terms* "injection" *and* "surjection". *These terms are not incorrect to use, but they can cause confusion. When students learn the terms* "one-to-one" *and* "onto" *for* "injection" *and* "surjection" *they are usually taught the term* "one-to-one correspondence" *rather than the term* "bijection". *This choice of terminology can lead to confusion as it is easy to confuse the terms* "one-to-one" *and* "one-to-one correspondence".

The word "surjection" *is particularly interesting. In French the word* "sur" *means* "on top" *or* "above". *In a surjection we can imagine the elements of the domain sitting on top and covering up all of the elements of the codomain.*

2.3 Operations

Just as we have spent years of our mathematical lives talking about examples of functions without having to grapple with the definition of a function, so too have we used the word operation. In this section we grapple with a definition for this term.

Consider the function $f : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$ given by

$$f((n,m)) = \sum_1^n m$$

For example,

$$f((3,4)) = \sum_1^3 4 = 4+4+4 = 12$$

and

$$f((2,9)) = \sum_1^2 9 = 9+9 = 18$$

(Are you confused by the symbol Σ? Do an internet search for `sigma notation`.)

We observe $f((n,m)) = n \cdot m$ for every $n, m \in \mathbb{N}^+$. Multiplication of positive integers is a function!

We have spent years talking about addition and multiplication as *operations*. We now have the tools to define what we mean by the word operation in mathematics.

Definition 2.23. *Let A be a set. An operation on A is a function $f : A \times A \to A$.*

Our definition of operation is very broad, but we can see how operations that we know about nicely satisfy this definition

Example 2.24. *Let $a : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ so that $a((a_1, a_2)) = a_1 + a_2$. The function a is an operation. We usually call this function* addition

Notice that there is nothing in the definition of operation that requires us to specify a particular symbol (eg $\cdot$ for multiplication) to denote our operation. We use these symbols as convenience. It is much easier to define the symbol $\cdot$ and write $7 \cdot 9$, then it is to define the function m as above and consider $m((7,9))$. And so commonly used operations sometimes are associated with a symbol.

In your past study of lines and curves in $\mathbb{R}^2$ you may have encountered the idea of function composition.

Definition 2.25. *Let A, B and C be sets so that $f_1 : A \to B$ and $f_2 B \to C$ For $f_1, f_2 \in \mathcal{A}$, the composition of f_2 and f_1 is the function given by:*

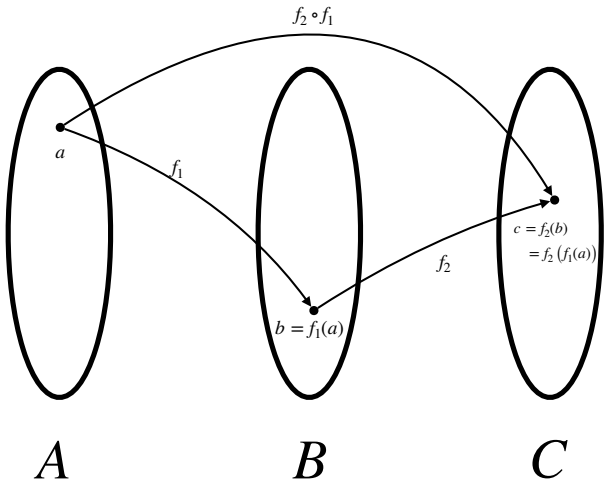
$$f_2 \circ f_1 = \{(a, f_2(f_1(a))) \,|\, a \in A\}$$

The function $f_2 \circ f_1$ has domain A and codomain C.

This definition is a great example of how strictly adhering to our agreed upon notation can make things quite confusing! In this function, ordered pairs are of the form:

$$(a, f_2(f_1(a)))$$

That is, for $a \in A$ we have $f_2 \circ f_1(a) = f_2(f_1(a))$. We find the image of a by finding its image with respect to f_1. And then taking that image and finding its image with respect to f_2. We may understand composition a little better with the following picture:



Aside. *There is nothing wrong with appealing to a picture to help make a point more clear. However you should not depend on your picture to tell the entire story. For every picture there should be sentences explaining it!*

Example 2.26. *Let $A = \{1, 4, 9\}$, $B = \{1, 7, 15\}$ and $C = \{11, 14, 21, 29, 30\}$. Consider $f : A \to B$ so that*

$$f = \{(1, 7), (4, 1), (9, 1)\}$$

and

$$g = \{(1, 11), (7, 29), (15, 21)\}$$

The function $g \circ f : A \to C$ is given by:

$$g \circ f = \{(1, 29), (4, 11), (9, 11)\}$$

Since $g \circ f$ is the name of a function we can meaningfully write $g \circ f(9)$.

This section is supposed to be about operations. And so we wonder if $\circ$ is an operation as we have defined the term above. Answering this question is... tricky and may depend on what the actual sets A, B and C are. We'll back away slowly from this wondering and leave it for another time. Instead we consider another example of function composition.

Exercise 2.27. *$A = \{1, 4, 9\}$ $B = \{1, 7, 15\}$ and consider the functions $f_1 : A \to B$ and $f_2 : B \to A$ so that*

$$f_1 = \{(1, 7), (4, 15), (9, 1)\}$$

and

$$f_2 = \{(7, 1), (15, 4), (1, 9)\}$$

Do you notice anything interesting about the functions $f_1 \circ f_2$ and $f_2 \circ f_1$?

Let A and B be sets and let f be a bijective function from A to B. Since f is bijective function, for each $b \in B$ the set $f^{-1}(b)$ contains a single element. Let g be the function from B to A so that $g(b)$ is the unique element of $a \in A$ such that $f(a) = b$.

Consider now the function $g \circ f$. By definition we see that the domain of $g \circ f$ is A and the codomain of $g \circ f$ is A.

By definition we see that for any $a \in A$ we have $g \circ f(a) = g(f(a) = a$. Thus we notice that with respect to the function $g \circ f$, the image of every element is itself!

This seems particularly interesting, we should give this phenomenon a name.

Definition 2.28. *Let A and B be sets, let f be a bijective function from A to B and let g be a function from B to A. We say g is the inverse of f when $g \circ f(a) = a$ for every $a \in A$. When g is the inverse of f we may label g as f^{-1}.*

This is an awful definition. Let us consider an example to try to get a handle on what it means.

Example 2.29. *Continuing from Exercise 2.27 we see*

$$f_1 \circ f_2 = \{(1,1),(7,7),(15,15)\}$$

and

$$f_2 \circ f_1 = \{(1,1),(4,4),(9,9)\}$$

By applying our definition we see:

$f_2^{-1} = f_1$ *and* $f_1 = f_2^{-1}$.

Look again at the elements of the functions f_1 and f_2. The ordered pairs in f_1 are reversed in f_2. This is a much better way to think about the meaning of inverse function.

Exercise 2.30. *Let $A = \{1,2,3,4,5\}$ and let $B = \{a,b,c,d,e\}$ so that $f(k)$ is the kth letter of the alphabet. What is $f^{-1}(c)$? What pairs are contained in the set f^{-1}?*

Exercise 2.31. *If you have seen the idea of function inverse before, is this very precise definition equivalent to your previous understanding of the term?*

Looking back at the notes from above, we notice that we have assigned two different meanings to the notation $f^{-1}(b)$. In Definition 2.10 we said that $f^{-1}(b)$ is a set. Whereas in Definition 2.28 we defined it to be a single element.

As much as we want to believe that mathematics may be accessing some sort of higher truth about the universe, we can't escape the foibles of our own humanity. When we use the notation $f^{-1}(b)$ we are expecting our reader to know from context which version of the notation we mean, much like when we use homonyms and homophones in written and spoken language.

Exercise 2.32. *Let A and B be a sets and let $f : A \to B$ be a bijection. Is f^{-1} is a bijection? Is it true that $(f^{-1})^{-1} = f$?*

Aside. *A common point of confusion for students of all stripes is that the following three pieces of notations denote three different functions:*

- $\sin^{-1}(x)$,
- $\sin(x)^{-1}$, *and*
- $\sin(x^{-1})$.

The first of these denotes the function that is the inverse of the function $\sin(x)$. *This function is sometimes called* $\arcsin(x)$. *The second of these denotes function* $\frac{1}{sin(x)}$. *And the third of*

these denotes the function $\sin\left(\frac{1}{x}\right)$*. This is absurd and unnecessary. This problem arises from a seeming need to denote the fraction* $\frac{1}{z}$ *as* z^{-1}*.*

But why do we use the notation z^{-1} *to denote the fraction* $\frac{1}{z}$*? Consider the integer* 1*. This integer has a wonderful property. It is unique real number so that* $1 \cdot x = x \cdot 1 = x$ *for every* $x \in \mathbb{R}$*. Multiplying by* 1 *changes nothing.*

Let A *be a set. Consider a function* $I : A \to A$ *so that* $I(a) = a$ *for every* $a \in A$*. For any bijection* $f : A \to A$ *we have* $I \circ f = f \circ I = f$*. Composing with* I *changes nothing. But what does this have to do with an inverses?*

For a bijection $f : A \to A$ *we have* $f \circ f^{-1} = f^{-1} \circ f = I$ *Similarly for any real number* x *we have* $x \cdot x^{-1} = x^{-1} \cdot x = 1$*. The function* I *with respect to composition behaves in the same manner as* 1 *with respect to multiplication.*

If you are familiar with matrix multiplication, this same phenomenon occurs with the identity matrix and matrix inverses: If A *is an* $n \times n$ *invertible matrix, we have* $AA^{-1} = A^{-1}A = I_n$ *and* $I_nA = AI_n = A$*. Suddenly the definition of multiplication for matrices seems slightly less mysterious!*

Other things to think about

- For those interested in pure mathematics: At some point you may be tempted to write down the following: Let A be the set of all sets. That is, let

$$A = \{B | B \text{ is a set}\}.$$

As A is seemingly a set, we have $A \in A$. On the face of it, this isn't terribly unreasonable, but it is a bit odd. Though a little unnatural, letting a set be a member of another set doesn't seem to cause any immediate trouble. However, consider the set

$$X = \{B | B \notin B\}$$

The set X contains all sets B that have do not have themselves as members. Our set A from above would not be an element of X. Is X an element of X? If X is an element of X, then X must satisfy the criteria $X \notin X$. Hmmm. Similarly, if $X \notin X$, then X must not satisfy the criteria $X \notin X$. Again we are troubled. We have that $X \in X$ if and only if $X \notin X$.

This phenomenon is called *Russell's Paradox*. It is named after philosopher Bertrand Russell (1872 - 1970). Attempting to resolve this paradox forces us to come up with a precise definition of what we mean by set. This topic is well-beyond the scope of this course, but is something the consider!

Test Your Understanding

1. Hiding inside of our definition of function is a way to decide what it means for two functions to be equal. Let f and g be functions with the same domain and and the same codomain. What should it mean to write $f = g$? How can we check if $f = g$?

2. One of the concepts that students coming out of secondary school seem to very adept with is the idea of the Vertical Line Test (VLT) to decide if something is a function. What part of the definition of function is speaking to the VLT for functions from $\mathbb{R}$ to $\mathbb{R}$?

3. One can imagine a Horizontal Line Test (HLT) for functions from $\mathbb{R}$ to $\mathbb{R}$. We'll say that a function passes the HLT if any horizontal line meets the function in at most one point? Which property from Section 2.2 can one detect with the HLT? What if we change the HLT so that a function passes if any horizontal line meets the function at exactly one point? at least one point?

4. Let f and g be functions such that $f \circ g$ exists. What criteria do we need on the domain, codomain and range of f and g so that $g \circ f$ also exists?

Test Your Understanding Solution

3 Relations Part I

Learning Incomes.

- *Comfort with notation for sets, particularly set builder notation and cartesian product*

Learning Outcomes.

- *Familiarity with broad idea of what a relation is*
- *Ability to decide if a set is a relation*
- *Ability decide if a relation is: reflexive, antireflexive, symmetric, antisymmetric or transitive*
- *Ability to decide if a relation is partial order*
- *Ability to decide if a relation is graph*
- *Ability to give examples of relations that satisfy one or more of the following properties: reflexive, antireflexive, symmetric, antisymmetric , transitive, partial order, graph*

Newly Defined Terms and Notation. *relation, reflexive relation, antireflexive relation, symmetric relation, antisymmetric relation, transitive relation, partial order, graph.*

Our big picture in this in this module is the following idea: given a set S, a relation on S provides structure to the set. For example, considered as just a set $\mathbb{Z}$ has no ordering. We can write down the elements of a set in any order that we want. However arranging integers in increasing order gives us a structure for the set of integers.

Consider the following subset of $\mathbb{Z} \times \mathbb{Z}$

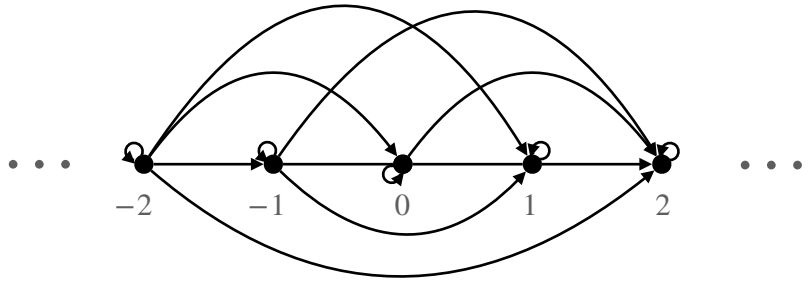
$$R_1 = \{(n_1, n_2) | n_2 - n_1 \in \mathbb{N}\}$$

Let us think for a moment about some elements of this set. For example, we have $(1, 2) \in R_1$ as $2 - 1 = 1$ and $1 \in \mathbb{N}$. We can notice that $(0, n_2) \in R_1$ whenever $n_2 \geq 0$. For which $n_1 \in \mathbb{Z}$ is $(n_1, 100) \in R_1$?
(Take a moment to think about this.)
.
.
.
.
.
.

.

We have $(n_1, 100) \in R_1$ whenever $100 - n_1 \in \mathbb{N}$. Recall $\mathbb{N} = \{0, 1, 2, \dots\}$. Thus we have $(n_1, 100) \in R_1$ whenever $100 - n_1 \geq 0$. In other words, $n_1 \leq 100$. And so R_1 contains all pairs of the form $(n_1, 100)$ where $n_1 \leq 100$ and $n_1 \in \mathbb{Z}$.

Let us draw a picture to gain some more intuition. We draw an arrow from n_1 to n_2 when $(n_1, n_2) \in R_1$.



We have only included integers from -2 to 2 in order to save space. As there are infinitely many integers, it would be impossible to draw this picture with all of the integers.

Aside. *We could have started this discussion with $\mathbb{R}$ instead of $\mathbb{Z}$, but the picture would have been much more difficult to draw!*

From our picture, we see that we have $(n_1, n_2) \in R_1$ exactly when $n_1 \leq n_2$.

With this set in hand, we never need to use the $\leq$ sign ever again! Instead of writing $9 \leq 10$ we can write $(9, 10) \in R_1$! Of course at this point you wonder, "*why would I ever want to do this?*" The answer is that you absolutely wouldn't. It is much easier for us to write and understand $9 \leq 10$, then to go through all of the struggle of understanding R_1. So why have we done this? We have done this because we already understand the relation $\leq$. In introducing the concept of relation, it is easier to us to first think about relations we are already familiar with.

Arranging integers in increasing order gives us structure for the set of integers. We are well familiar with this structure – in fact most of the time we think about $\mathbb{Z}$ as having the ordering built in. This isn't the case; $\mathbb{Z}$ is a set. Elements in a set have no order. But when we define R_1, we now know what order to put the elements in.

Depending on context we might be interested in different sorts of structure on different sorts of objects all together! And so we have a definition for relation that allows us to capture all

sorts of different structures within a single definition.

Definition 3.1. *Let S be a set. A relation on S is a subset of $S \times S$. When R is a relation on S we write $a_1 R a_2$ to denote $(a_1, a_2) \in R$. When $a_1 R a_2$ we say that a_1 is related to a_2.*

Just like with functions, for any set S there are many different relations on S. And just as we saw with injective, surjective and bijective functions, some of these relations are particularly interesting. (... I suspect we have differing definitions of interesting. I agree you may not find any of this interesting.)

Aside. *Above we examined the set*

$$R_1 = \{(n_1, n_2) | n_2 - n_1 \in \mathbb{N}\}$$

With our notation from our definition of relation, we may meaningfully write $9 R_1 10$. What would we write if we instead labelled our set as

$$\leq \; = \; \{(n_1, n_2) | n_2 - n_1 \in \mathbb{N}\}$$

The statement $9 \leq 10$ now means $(9, 10) \in \leq$, which in turn means that 9 is less than or equal to 10.

When we introduced subset in Module 1, we waved our hands towards an analogy to $\leq$. We now have the tools to be a little more precise in comparing the concepts $\leq$ and $\subseteq$. To do so, we first require some extra notation.

Definition 3.2. *Let U be a set. The set of all subsets of U is called the power set of U. We denote the power set of U as $\mathbf{2}^U$. That is*

$$\mathbf{2}^U = \{A | A \subseteq U\}$$

For example, if $U = \{x, y, z\}$, then we have

$$\mathbf{2}^U = \{\{\}, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$$

Aside. *Above we have that U has 3 elements and the set $\mathbf{2}^U$ has 2^3 elements. This is not a coincidence.*

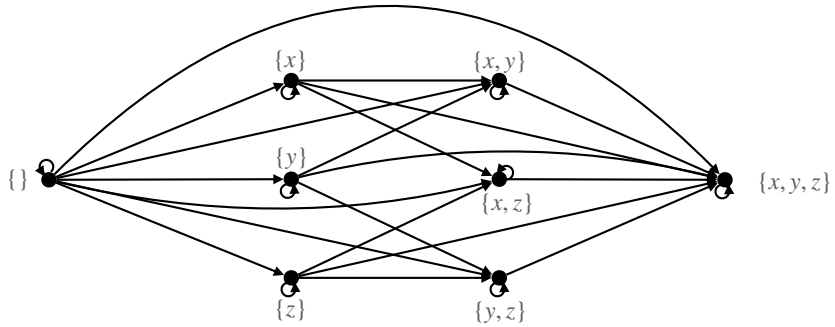
Consider the set

$$R_2 = \left\{ (A, B) \,|\, A, B \in \mathbf{2}^U \text{ and every element of } A \text{ is an element of } B. \right\}$$

For example $(\{x\}, \{x, z\}) \in R_2$.

Let us consider the elements of R_2. Each element is an ordered pair. Both entries of the ordered pair are subsets of U. And every entry of the first entry of the ordered pair is an element of the second entry of the ordered pair. This is exactly our definition of subset! We have encoded our definition of subset as a set much in the same we encoded $\leq$ as a set. (This is an ongoing theme in this course...)

Let us draw a picture to gain some further intuition. In the image below, an arrow from an element to another tells us that the first element is related to the second element.



The relation on subsets allows us to put the subsets of a set in a seeming order. (This order is from left to right in the picture). But this doesn't quite feel the same as the order we have for the integers. For any pair of integers, n_1 and n_2 at least one of the following statements is true

$$n_1 \leq n_2$$
$$n_2 \leq n_1$$

But for our relation R_2 above this is not the case. Both of the statements below are false.

$$\{x, y\} \subseteq \{y, z\}$$
$$\{y, z\} \subseteq \{x, y\}$$

We consider orderings that arise from relations further in Section 3.1.

Let us continue with another example of a relation that has nothing in common with orderings.

Let C be the set of classes offered at the University of Saskatchewan this semester that will have an exam scheduled during the final exam period. In putting together the final exam schedule, the Registrar's Office aims to ensure that no student has two final exams at the same time. How is this accomplished? Just knowing the elements of the set C does not suffice. The Registrar's Office must also know which classes have overlapping enrolment.

(Even with this knowledge, this is still a difficult task. There are far too many classes for a human to work this out by hand. Even for computer this is a difficult task!)

Let E be the relation on C so that $c_1 E c_2$ whenever there is a student registered in both c_1 and c_2. (The notation $c_1 E c_2$ is new. Take a moment to go back to the definition of relation to remind yourself what it means) In putting together the final exam schedule, the Registrar's Office must ensure that if $(c_1, c_2) \in E$, then c_1 and c_2 must be scheduled at a different time. The set C together with the set E contains all of the information necessary so that final exams can be scheduled without student conflict. The set E equips the set C with added structure.

By way of example, imagine the Registrar's Office trying to schedule exams for the following courses:

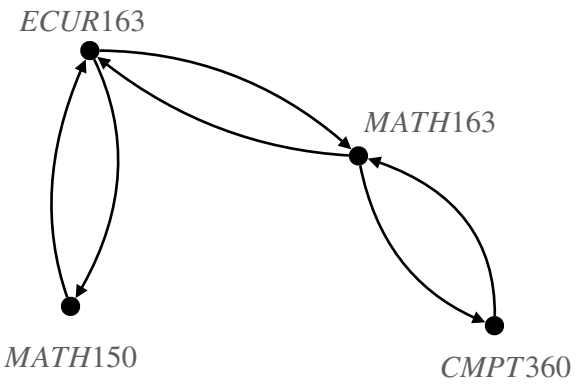
$$C = \{ECUR163, MATH150, CMPT360, MATH163\}$$

To do so, they must know which courses have overlapping enrolment. Let E be the relation on C so that $(c_1, c_2) \in E$ whenever there is a student in c_1 is also enrolled in c_2 We have

$$\begin{aligned} E = \{&(ECUR163, MATH150), (MATH150, ECUR163), (MATH163, CMPT360), \\ &(CMPT360, MATH163), (ECUR163, MATH163), (MATH163, ECUR163)\} \end{aligned}$$

(This is fake data. There is no way for you to have known what E is.)

Again we can use a picture to visualize this relation. This time, the particular layout of the picture provides us with no further information or intuition.



Using this picture we can see that we can schedule the exam for $CMPT360$ concurrently either $MATH150$ or $ECUR163$. However we cannot schedule all three of these exams at the same time, as there are students registered in both $MATH150$ and $ECUR163$.

This picture has very different structure than the previous pictures. There doesn't seem to be any sense of ordering in how it is drawn. We can see that no element is related to itself and it is possible to have arrows going both ways between a pair of elements. We return to this sort of relation in Section 3.2.

From these examples, we see that relations come in many different flavours. In this module we examine two particular types of relations – orderings and graphs.

Test Your Understanding

1. Let $S = \{s_1, s_2, s_3, s_4, s_5\}$. Which of the following are sets satisfy the definition of relation on S.

   (a) $\{(s_1, s_2), (s_1, s_3), (s_3, s_1), (s_4, s_4)\}$

   (b) $\{(s_1, s_2, s_3), (s_1, s_3), (s_3, s_1), (s_4, s_4)\}$

   (c) $\{(s_1, s_1), (s_1, s_3), (s_3, s_1), (s_4, s_4), (s_5, s_5)\}$

   (d) $\{(s_1, s_1), (s_1, s_7), (s_3, s_1), (s_4, s_4), (s_5, s_5)\}$

   (e) $\{\}$

Test Your Understanding Solution

1. (a) This is a relation. It is a subset of $S \times S$.

   (b) This is not a relation. It is not a subset of $S \times S$ as $(s_1, s_2, s_3) \notin S \times S$

   (c) This is a relation. It is a subset of $S \times S$.

   (d) This is not a relation. It is not a subset of$S \times S$ as $s_7 \notin S$.

   (e) This is a relation. It is a subset of $S \times S$. (Remember, the empty set is a subset of every set).

3.1 Orderings

Let $U = \{x, y, z\}$. Let us return to the following two relations:

$$R_1 = \{(n_1, n_2) | n_2 - n_1 \in \mathbb{N}\}$$

$$R_2 = \{(A, B) \,| A, B \in \mathbf{2}^U \text{ and every element of } A \text{ is an element of } B.\}$$

Looking at our pictures from the previous section, we notice some common features the pictures.

1. Every object has an arrow going back to itself.
2. Between any pair of distinct objects there is at most one arrow.
3. If there is an arrow from one object to a second object, and from a second object to a third object, then there is an arrow from the first object to the third object.

Translating this back to the language of relations we have

1. Every object is related to itself.
2. If x and y are distinct and x is related to y, then y is not related to x.
3. If x is related to y and y is related to z, then x is related to z.

A relation with these three properties defines a sense of ordering for the set. Following arrows in the direction of the arrow roughly corresponds to increasing. Following arrows against the direction of the arrow roughly corresponds to decreasing. To define this sense of ordering more carefully, we must define each of these three properties more precisely.

Definition 3.3. *Let S be a set and let R be a relation on S.*

- *We say R is reflexive when $(x, x) \in R$ for each $x \in S$.*
- *We say R is antisymmetric when at most one of (x, y) and (y, x) is in R for each pair $x, y \in S$ with $x \neq y$.*
- *We say R is transitive when $(x, y), (y, z) \in R$ implies $(x, z) \in R$.*

Definition 3.4. *Let S be a set and let R be a relation on S. We say R is a partial order when R is reflexive, antisymmetric and transitive.*

Exercise 3.5. *Convince yourself that each of R_1 and R_2 satisfy the definition of a partial order.*

Example 3.6. *Let* $S = \{a, b, c\}$ *and let*

$$R = \{(a, b), (b, c)(a, a), (b, b), (c, c)\}$$

Is R *a partial order? To be a partial order,* R *must be reflexive, antisymmetric and transitive.*

Reflexive
We see $(a, a) \in R$, $(b, b) \in R$ *and* $(c, c) \in R$. *Thus* $(x, x) \in R$ *for each* $x \in S$. *Therefore* R *is reflexive.*

Antisymmetric
We have three pairs of distinct elements: $a \neq b$, $b \neq c$ *and* $a \neq c$. *At most one of* (a, b) *and* (b, a) *are in* R. *At most one of* (b, c) *and* (c, b) *are in* R. *At most one of* (a, c) *and* (c, a) *are in* R. *Therefore* R *is antisymmetric.*

Transitive
We see $(a, b) \in R$ *and* $(b, c) \in R$, *but* $(a, c) \notin R$. *Therefore* R *is not transitive.*

Since R *is not transitive,* R *is not a partial order.*

To find another example of a partial order, consider the following definition.

Definition 3.7. *Let* x *and* y *be integers. We say* x *divides* y *when there exists* $k \in \mathbb{Z}$ *so that* $xk = y$. *When* x *divides* y *we say that* y *is a multiple of* x.

The terms divides and multiple are likely familiar to us. We define them here so that we have an agreed upon definition for these ideas. Having a rigourous definition is handy when we are constructing arguments. They give us a clear picture of what we need to conclude.

Consider the following relation on $\mathbb{N}^+$:

$$D = \{(x, y) | x \text{ divides } y\}$$

We claim D is a partial order. Take a moment to draw yourself a picture to gain some intuition. Draw an arrow from a to b when a divides b. Arrange your picture to have smaller integers on the left. Only include integers from 1 to 10.

The structure of the arrows seems to satisfy the three properties above. And so we will write down an justification of why D satisfies each of the required properties so as to be a partial order.

1. D is reflexive
To show that D is reflexive we must show that $(x, x) \in D$ for each $x \in \mathbb{Z}$. Having $(x, x) \in D$ is equivalent to the statement "*x divides x*". Recalling the definition of divides this statement is equivalent to saying "*there exist an integer k so that $xk = x$*. We recognize that this statement is true as, $x(1) = x$. Thus D is reflexive.

2. D is antisymmetric
To show D is antisymmetric we must show that if $(x, y) \in D$ for some pair $x, y \in \mathbb{N}^+$ with $x \neq y$, then $(y, x) \notin D$. To do this, we assume that the hypothesis of this statement holds and then explain how we know the conclusion holds as a consequence. In this case the hypothesis is: *$(x, y) \in D$ for some pair $x, y \in \mathbb{N}^+$ with $x \neq y$*. And so we consider some pair $x, y \in \mathbb{N}^+$ so that $x \neq y$ and x divides y.

Since x divides y there exists an integer k so that $xk = y$. We want to show that there is no integer k' so that $yk' = x$.

Since x and y are both positive, then k is positive. Further, since $x \neq b$, we have $k \neq 1$. Therefore $k \geq 2$ Since $xk = y$ and $k \geq 2$, necessarily $x < y$.

If there existed an integer k' so that $yk' = x$, then we could use the same argument to conclude that $y < x$. It cannot be that both $x < y$ and $y < x$. Since we know $x < y$ to be true, it must mean that $y < x$ is false. Therefore is no integer k' so that $yk' = x$.

Therefore y does not divide x. This is equivalent to saying $(y, x) \notin D$. Thus D is antisymmetric.

3. D is transitive
To show D is transitive, we must show that if $(x, y) \in D$ and $(y, z) \in D$, then $(x, z) \in D$.

As before, we assume our hypothesis is true, and then explain how we know the conclusion holds as a consequence. In this case the hypothesis is: *$(x, y) \in D$ and $(y, z) \in D$ for some $x, y, z \in \mathbb{N}^+$*. And so we consider some $x, y, z \in \mathbb{N}^+$ so that x divides y and y divides z.

Since x divides y there exists $k_x \in \mathbb{Z}$ so that $xk_x = y$. Similarly, there exists $k_y \in \mathbb{Z}$ so that $yk_y = z$. Therefore $x(k_x k_y) = z$. Since $k_x k_y \in \mathbb{Z}$, it then follows that x divides z. In other words, $(x, z) \in D$. Thus D is transitive.

Since D satisfies each of the requirements to be a partial order, necessarily D is a partial order.

Exercise 3.8. *Using the definition of partial order, show R_2 is a partial order. The structure of your argument should be similar to the structure we had when we showed D was a partial order above.*

We explore features of partial orders further on Assignment 2.

Test Your Understanding

1. Let $S = \{s_1, s_2, s_3, s_4, s_5\}$. For each set below determine if satisfies the definition of reflexive? antisymmetric? transitive? partial order? (Drawing the picture might help, but your justification should be a sentence or two.

   (a) $\{(s_1, s_1), (s_1, s_2), (s_3, s_3), (s_2, s_3), (s_1, s_3)\}$

   (b) $\{(s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_4), (s_5, s_5), (s_2, s_3), (s_3, s_4), (s_2, s_4)\}$

   (c) $\{(s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_4), (s_5, s_5)\}$

   (d) $\{(s_1, s_1), (s_2, s_2), (s_3, s_4), (s_4, s_4), (s_5, s_5), (s_2, s_3), (s_3, s_4), (s_2, s_4), (s_4, s_2)\}$

   (e) $\{(s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_3), (s_3, s_1)\}$

2. What elements must be added to (e) so that it is partial order?

Test Your Understanding Solution

1. (a)
   - Reflexive: no, (s_2, s_2) does not appear.
   - Antisymmetric: yes, if (x, y) appears with $x \neq y$, then (y, x) does not appear.
   - Transitive: yes, if (x, y) and (y, z) appear, then (x, z) appears
   - This relation is not a partial order as the relation is not reflexive.

   (b)
   - Reflexive: yes, each element of the form (x, x) appears.
   - Antisymmetric: yes, if (x, y) appears with $x \neq y$, then (y, x) does not appear.
   - Transitive: yes, if (x, y) and (y, z) appear, then (x, z) appears
   - This relation is a partial order as it is reflexive, symmetric and transitive.

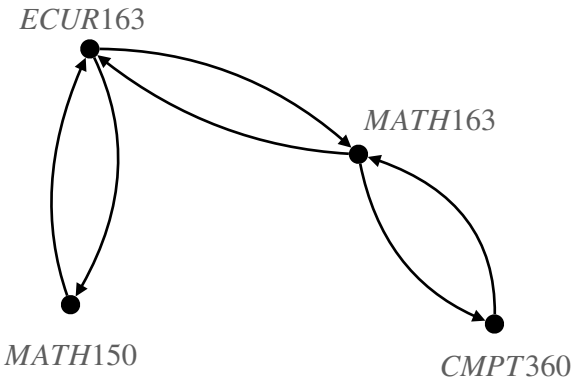
   (c)
   - Reflexive: yes, each element of the form (x, x) appears.
   - Antisymmetric: yes, if (x, y) appears with $x \neq y$, then (y, x) does not appear.
   - Transitive: yes, as no pairs elements of the form (x, y) and (y, x) appear, then definition of transitive is not violated.
   - This relation is a partial order as it is reflexive, symmetric and transitive.

   (d)
   - Reflexive: no, as (s_3, s_3) does not appear.
   - Antisymmetric: no, both (s_2, s_4) and (s_4, s_2) appear.
   - Transitive: no, (s_3, s_4) and (s_4, s_2) appear, but (s_3, s_2) does not.
   - This relation is not a partial order as the relation is not transitive.

   (e)
   - Reflexive: no, as (s_4, s_4) does not appear.
   - Antisymmetric: yes, if (x, y) appears with $x \neq y$, then (y, x) does not appear.
   - Transitive: no, (s_4, s_3) and (s_3, s_1) appear, but (s_4, s_1) does not.
   - This relation is not a partial order as the relation is not transitive.

3.2 Graphs

Let us return to our picture from our exam scheduling example.



The structure of the arrows in this case is very different from the partial orders we saw in the previous section. This particular relation is not antisymmetric. Nor is reflexive.

To try and find some common features as we did is the previous section, let us consider another practical-seeming example.

FM radio stations each operate on an frequency within the electromagnetic spectrum. For example, CBC Radio One transmits at 94.1 megahertz. To avoid interference (and confusion for listeners!) radio stations that are geographically close must operate on different frequencies. As a consequence of fundamental laws of physics (... this is me using weasel words to avoid having to explain something I don't understand), there is a limited number of frequencies on which radio stations can broadcast. And so the same frequency can be used for different radio stations in geographically far areas. (For example, 94.1 megahertz in Swift Current is home of "The Eagle 94.1", and not CBC Radio One).

The Canadian Federal Government acts as the regulatory body for radio stations in Canada. And so they have the responsibility of assigning frequencies to radio stations[1].

Let R be a set of radio stations. And let I be the relation on R so that $(r_1, r_2) \in I$ when r_1 is geographically close to r_2. For example, let

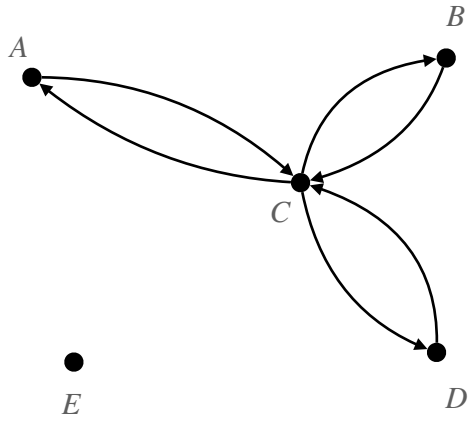
$$R = \{A, B, C, D, E\}$$

and let

$$I = \{(A, C), (C, A), (C, D), (D, C), (B, C), (C, B)\}$$

[1]See https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10759.html for further details not relevant to the course

We have the corresponding picture:



We observe that A and D may operate on the same frequency, but A and C may not.

Looking at our picture here and our picture from the exam example, we notice some common features

1. No object has an arrow going back to itself.
2. Between any pair of distinct objects there either no arrows or an arrow in both directions.

Translating this back to the language of relations we have

1. No object is related to itself.
2. If x is related to y, then y is related to x.

These are very different features we saw when we looked at structures that gave us orderings. To define these sorts of relations, we require the following definitions.

Definition 3.9. *Let S be a set and let R be a relation on S.*

- *We say R is antireflexive when $(x, x) \notin R$ for each $x \in S$.*
- *We say R is symmetric when for each $x, y \in S$, if $(x, y) \in R$, then $(y, x) \in R$.*

Definition 3.10. *Let V be a set and let E be a relation on V. We say E is a graph when E is symmetric and antireflexive.*

We will return to graphs in a later module in the course. And so for now we forgo any further analysis or examples of these objects. Instead, consider the following application of graphs.

A common research tool in the social sciences is *social network analysis*. In these contexts. the term *social networks* usually is used as a synonym for *graphs*. Consider the following example drawn from a research project done by Australian pharmacists[2]. For a hospital H, let V_H be the set of healthcare professionals (doctors, nurses, pharmacists, etc..) working in the hospital. Let E_H be the relation on V_H where $(p_1, p_2) \in E_H$ if p_1 and p_2 regularly communicate about medications. One can check that E_H satisfies the definition of a graph.

These researchers asked whether or not the structural properties of E_H could predict patient outcomes with respect to medication use. They further studied how the role (doctor, nurse, pharmacist, etc...) of each of the elements of V_H played a part in the structure of the network. One outcome of this study was that junior doctors and senior nurses play outsized roles in patient communication about medications.

---

[2]B. Chan, E. Reeve, S. Matthews, P. Carroll, J. Long, F. Held, M. Latt, V. Naganathan, G. Caplan, and S. Hilmer **(2017)** *Medicine information exchange networks among healthcare professionals and prescribing in geriatric medicine wards* British Journal of Clinical Pharmacology 83:6 1185-1196.

Test Your Understanding

1. Let $S = \{s_1, s_2, s_3, s_4, s_5\}$. For each set below determine if satisfies the definition of symmetric ? antireflexive? a graph? (Drawing a picture may help, but your justification should be a sentence or two.)

   (a) $\{(s_1, s_1), (s_1, s_2), (s_3, s_3), (s_2, s_3), (s_3, s_2), (s_2, s_1)\}$

   (b) $\{(s_2, s_3), (s_3, s_2), (s_2, s_4)\}$

   (c) $\{(s_1, s_2), (s_2, s_1), (s_3, s_4), (s_4, s_3), (s_2, s_5), (s_5, s_2)\}$

Test Your Understanding Solution

1. (a)
   - Symmetric: yes, if (x, y) appears, then (y, x) appears.
   - Anti-reflexive: no, (s_1, s_1) appears
   - Graph: This relation is not a graph; it is not anti-reflexive.

   (b)
   - Symmetric: no, (s_2, s_4) appears but (s_4, s_2) does not.
   - Anti-reflexive: yes, no element of the form (x, x) appears.
   - Graph: This relation is not a graph; it not symmetric.

   (c)
   - Symmetric: yes, if (x, y) appears, then (y, x) appears.
   - Anti-reflexive: yes, no element of the form (x, x) appears.
   - Graph: This relation is a graph.

---

4 Relations Part II

Learning Incomes.

- *Comfort with definitions for relation, reflexive, symmetric, and transitive.*

Learning Outcomes.

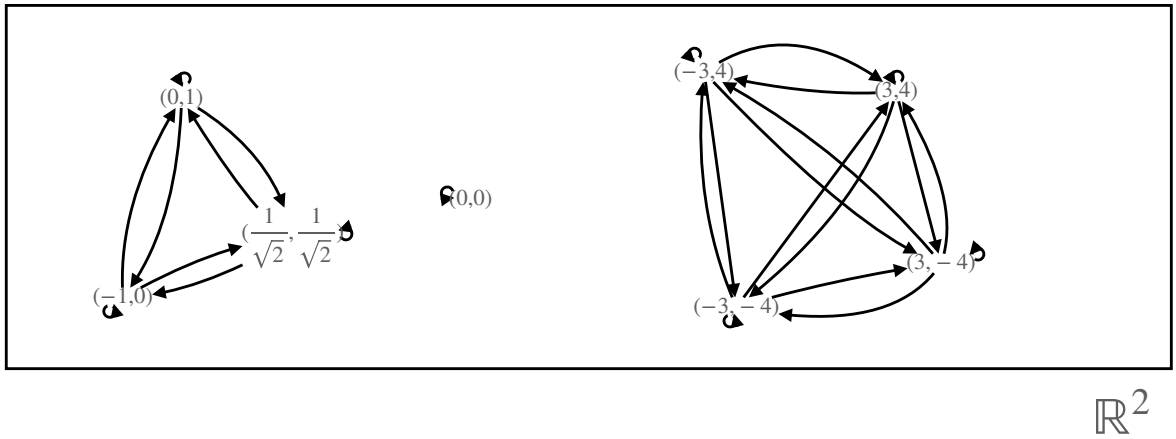
- *Show that a relation is/isn't a equivalence relation.*
- *Understand the relationship between an equivalence relation and a partition.*

Newly Defined Terms and Notation. *equivalence relation, partition, equivalence class,* $[x]$*, set of equivalence classes,* S/R*,* $\bigcup_{P\in\mathcal{P}} P$

Consider the following relation on points in $\mathbb{R} \times \mathbb{R}$

$$C = \{(x_1, y_1), (x_2, y_2) | (x_1, y_1) \text{ and } (x_2, y_2) \textit{ are the same distance from the origin.}\}$$

We wonder what properties this relation satisfies. Though $\mathbb{R}^2$ has many elements, we try to draw a picture to build some intuition.



By inspection it looks as if this relation may be reflexive, symmetric and transitive

Is C reflexive?
Recall that a relation is reflexive when every pair of the form (a, a) appears as part of the relation. Consider a point $p_1 = (x_1, y_1)$. Is $p_1 \in C$? Elements of $\mathbb{R}^2$ are in C when they are the same distance from the origin. Certainly the point p_1 is the same distance from the origin as p_1. Thus $p_1 C p_1$.

This argument is true no matter which element of $\mathbb{R}^2$ we choose. Thus C satisfies the definition of a reflexive relation.

Is C symmetric?
Recall that a relation is symmetric when if (a, b) appearing in our relation implies (b, a) appears in our relation. Consider a pair of points $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$. In asking if C is symmetric, we are asking if $p_1 C p_2$ implies $p_2 C p_1$.

If $p_1 C p_2$, then p_1 is the same distance from the origin as p_2. Therefore p_2 is the same distance from the origin as p_1. Thus $p_2 C p_1$.

Therefore C satisfies the definition of a symmetric relation.

Is C transitive?
Recall that a relation is transitive when if (a, b) and (b, c) appear in our relation, then (a, c) necessarily appears in our relation. Consider a triple of points $p_1 = (x_1, y_1), p_2 = (x_2, y_2)$ and $p_3 = (x_3, y_3)$. In asking if C is transitive, we are asking if $p_1 C p_2$ and $p_2 C p_3$ necessarily implies $p_1 C p_3$

If $p_1 C p_2$, then p_1 is the same distance from the origin as p_2. If $p_2 C p_3$, then p_2 is the same distance from the origin as p_3. We conclude that p_1 is the same distance from the origin as p_3. Thus $p_1 C p_3$.

Therefore C satisfies the definition of a transitive relation.

Our picture above has been drawn in a suggestive way – just as we saw that our relation in the intro video split $\mathbb{Z}$ into four distinct parts, here we see the same type of behaviour. The elements $\mathbb{R}^2$ are split into parts based on their distance from the origin. Though we cannot possibly draw all the elements of $\mathbb{R}^2$, our picture seems to suggest, for example, that points in $\mathbb{R}^2$ at distance 5 from the origin related only to themselves and to no other elements.

In this module we see how relations that are reflexive, symmetric and transitive give rise to such partitions.

4.1 Equivalence Relations

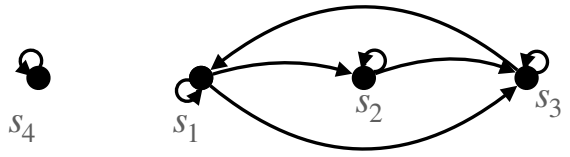
From our two examples, we have seen relations that split a set into parts based on some particular property. For remainders and $\mathbb{Z}$, the relation grouped together the integers that had the same remainder when dividing by 4. For distances and $\mathbb{R}^2$, the relation grouped together the points in $\mathbb{R}^2$ that were the same distance from the origin. That our relation grouped together the elements of the set based on some particular property seemed to be related to the relation being reflexive, symmetric and transitive.

Definition 4.1. *Let S be a set and let R be a relation on S. We say that S is an equivalence relation when it is reflexive, symmetric and transitive.*

Example 4.2. *Consider the set $S = \{s_1, s_2, s_3, s_4\}$ and the relation*

$$R = \{(s_1, s_2), (s_2, s_3), (s_1, s_3), (s_3, s_1), (s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_4)\}$$

Using the definition of equivalence relation we can check if this is an equivalence relation. Let us first draw a picture to gain some intuition.



In our picture we can see there is an arrow from s_2 to s_3 but not one from s_3 to s_2. Thus $(s_2, s_3) \in R$ but $(s_3, s_2) \notin R$. Therefore R is not symmetric. And it cannot be that R is an equivalence relation.

(This is not the only justification for why R is not an equivalence relation.)

Exercise 4.3. *What elements would we need to add to R so that it is an equivalence relation?*

Aside. *Being able to draw the picture of a relation give us great intuition for what sort of properties a relation has. However when S has lots of elements, it may not be possible to draw a picture that gives us all of the information.*

Recall the following relation introduced in the introduction to this module.

$$C = \{(x_1, y_1), (x_2, y_2) | (x_1, y_1) \text{ and } (x_2, y_2) \textit{ are the same distance from the origin.}\}$$

We showed that this relation was reflexive, symmetric and transitive. Thus it is an equivalence relation.

Let us return now to our example of *remainders when divided by* 4 from the introductory video. Consider the following relation on $\mathbb{Z}$:

$$M_4 = \{(a, b) \mid 4 \text{ divides } b - a\}$$

At a glance, this does not seem to be the exactly same relation that we introduced for remainder when dividing by 4. Let us examine some pairs of integers to see which pairs are contained in our relation.

- *Is* $(0, 4) \in M_4$*?* – Yes, as 4 divides $4 - 0$.
- *Is* $(3, 4) \in M_4$*?* – No, as 4 does not divide $4 - 3$.
- *Is* $(9, 17) \in M_4$*?* – Yes, as 4 divides $17 - 9$.
- *Is* $(42, 83) \in M_4$*?* – No, as 4 does not divide $83 - 42$.

Notice that 0 and 4 have the same remainder when divided by 4. As do 9 and 17. We see that 42 and 83 do not have the same remainder. Nor do 3 and 4.

It seems as if $(a, b) \in M_4$ if and only if a and b have the same remainder when dividing by 4. We take this as fact for now.

Theorem 4.4. *We have* aM_4b *if and only if* a *and* b *have the same remainder when divided by* 4*.*

We return to the proof of this theorem on Assignment 3.

Aside. *The statement of this theorem has a very precise structure:* aM_4b if and only if a and b have the same remainder when divided by 4 *means that the following two statements are true:*

1. *If* aM_4b*, then* a *and* b *have the same remainder when divided by* 4*; and*
2. *if* a *and* b *have the same remainder when divided by* 4*, then* aM_4b*.*

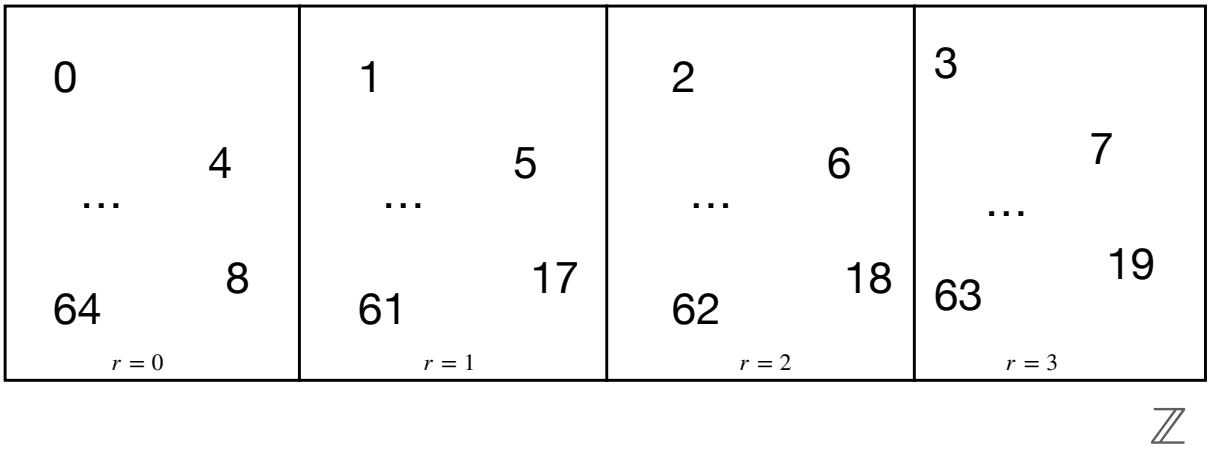
In essence this theorem means that the condition of a *and* b *having the same remainder is identical to the condition of* aM_4b*. We return to the structure of such statements in Module 5.*

We wonder if M_4 is an equivalence relation. We check if M_4 satisfies the necessary properties – reflexive, symmetric and transitive. Let a, b, c be integers.

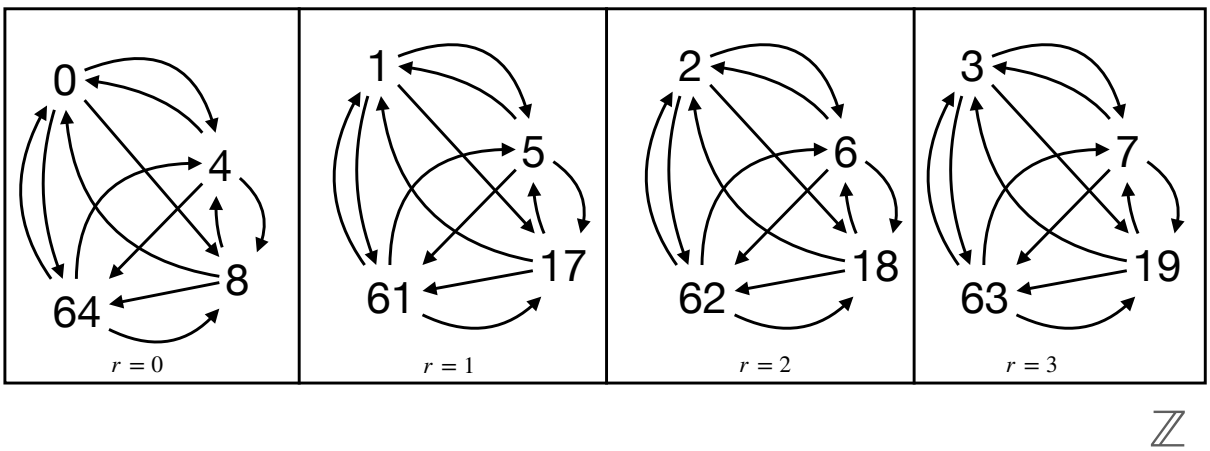
1. Since 4 divides 0, we have that 4 divides $a - a$ for any $a \in \mathbb{Z}$. Thus $(a, a) \in M_4$.
2. For any $a, b \in \mathbb{Z}$, if 4 divides $b - a$, then 4 divides $a - b$. Thus if $(a, b) \in M_4$, then $(b, a) \in M_4$.
3. For any $a, b, c \in \mathbb{Z}$, if 4 divides $b - a$ and 4 divides $c - b$, then $b - a + (c - b) = c - a$ is a multiple of 4. (Adding together two multiples of 4 gives a multiple of 4.) Thus $(a, c) \in M_4$.

Item 1. should convince us that M_4 is reflexive. Likewise, items 2. and 3. should convince is that M_4 is symmetric and transitive. Thus M_4 is an equivalence relation.

Recall the picture we looked at in the introduction video for remainders when divided by 4.



Let us combine this picture with the type of picture we draw when we picture a relation.



Notice that each arrow is contained within a particular part. Everything that has remainder 0 is related to each other and related to nothing else. Similarly, everything that has remainder 1 is related to each other and related to nothing else. Likewise, we can make similar statements for 3 and 4. It seems as if the structure that M_4 imparts on $\mathbb{Z}$ is a partition.

Let us return now to our example C from above. It is also an equivalence relation. Does it give a partition the points of $\mathbb{R}^2$ in the same way that M_4 gave a partition of $\mathbb{Z}$? To consider this, we must first agree on what we mean when we say *partition*.

Test Your Understanding

1. Let $S = \{s_1, s_2, s_3, s_4\}$ and let

   $R = \{(s_1, s_2), (s_2, s_1), (s_2, s_3), (s_3, s_2), (s_1, s_3), (s_3, s_1), (s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_4)\}$

   Determine if R is an equivalence relation.

Test Your Understanding Solution

1. We check if R is reflexive, symmetric and transitive.

   - Reflexive: For each $s \in S$ we observe $(s, s) \in R$. Therefore S is reflexive.
   - Symmetric: We examine all elements of the form (s, t) to ensure (s, t) also appears:
     - $(s_1, s_2) \in R$ and $(s_2, s_1) \in R$
     - $(s_1, s_3) \in R$ and $(s_3, s_1) \in R$
     - $(s_2, s_3) \in R$ and $(s_3, s_2) \in R$

     This exhausts all elements of the form (s, t), and so we see that R is symmetric.
   - Transitive: We examine all pairs of elements of the form (s, t) and (t, r) to ensure (s, r) appears.
     - $(s_1, s_2) \in R$ and $(s_2, s_3) \in R$ we see $(s_1, s_3) \in R$
     - $(s_2, s_1) \in R$ and $(s_1, s_3) \in R$ we see $(s_2, s_3) \in R$
     - $(s_1, s_3) \in R$ and $(s_3, s_2) \in R$ we see $(s_1, s_2) \in R$
     - $(s_3, s_1) \in R$ and $(s_1, s_2) \in R$ we see $(s_3, s_2) \in R$
     - $(s_2, s_3) \in R$ and $(s_3, s_1) \in R$ we see $(s_2, s_1) \in R$
     - $(s_3, s_2) \in R$ and $(s_2, s_1) \in R$ we see $(s_3, s_1) \in R$

     This exhausts all possibilities, and so we see that R is transitive.

   Since R is reflexive, symmetric and transitive, by definition R is an equivalence relation.

4.2 Set Partitions

Consider the following sentence: *the students in MATH163 were partitioned by their hair colour.* We understand this to mean that the students were placed into groups so that students in the same group were all of the students with the same hair colour. In such a grouping we would expect every student to be in exactly one group. (... those without hair can go in a *no hair-colour* group!) Let us describe this situation with sets.

Let S be the set of students in MATH163. Let T be the set of all possible hair colours of students in $MATH163$. For each $t \in T$, let H_t be the set of students with hair colour t. For example H_{brown} is the set of all students in MATH163 with brown hair. And H_{purple} is the set of all students in MATH163 with purple hair.

Let us notice two things:

1. Every student is in some hair-colour set. Thus, if we take the union of all of the sets of the form H_t we should get S.
2. No student can be in more than one hair-colour set. Thus, for distinct colours t_1 and t_2 we would expect $H_{t_1} \cap H_{t_2} = \{\}$.

To aid our ability to denote taking the union over many sets, we introduce a piece of notation that denotes taking the union over many sets. We do this by an analogy to how we use Σ. We recall

$$\sum_{i=1}^{7} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 7^2$$

In each subsequent term of the sum we increase our value of i.

We can also denote this sum as follows:

$$\sum_{i \in \{1,2,3,4,5,6,7\}} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + 7^2$$

Here the subscript $i \in \{1, 2, 3, 4, 5, 6, 7\}$ tells us to take the sum over all possible values that i can take in the set $\{1, 2, 3, 4, 5, 6, 7\}$.

For example

$$\sum_{i \in \{3,6,7\}} i^2 = 3^2 + 6^2 + 7^2$$

We define a similar piece of notation for set union. Let $P_1, P_2, \ldots, P_k$ be sets. And let $\mathcal{P} = \{P_1, P_2, \ldots, P_k\}$

Let

$$\bigcup_{P\in\mathcal{P}} P$$

denote the union of all sets in $\mathcal{P}$. That is,

$$\bigcup_{P\in\mathcal{P}} P = P_1 \cup P_2 \cup \cdots \cup P_k$$

Let us return to our example with hair colour. Let $\mathcal{H}$ be the set of all sets of the form H_t. That is,

$$\mathcal{H} = \{H_{brown}, H_{black}, H_{blonde}, H_{purple}, \dots\}$$

Above we said *If we take the union of all of the sets of the form H_t we should get S.* This is the same as writing

$$\bigcup_{H\in\mathcal{H}} H = S$$

Informally, we understand $\mathcal{H}$ to be a partition of S. Let us define the notion of partition formally.

Let X be a set. Following from our example with hair colour, we see that to have a partition of X we need a collection of subsets of X so that their union is X and the intersection of any two distinct subsets is empty. Formally, we have:

Definition 4.5. *Let X be a set and let $\mathcal{P}$ be a set of subsets of X. We say $\mathcal{P}$ is a partition of X when*

1. $\bigcup_{P\in\mathcal{P}} P = X$*; and*
2. $P_i \cap P_j = \{\}$ *for any pair $P_i, P_j \in \mathcal{P}$ with $P_i \neq P_j$.*

Look at the things we noticed (1. and 2.) above. Let $\mathcal{H}$ be the set of all sets of the form H_t We have

1. $\bigcup_{H\in\mathcal{H}} = S$; and
2. $H_t \cap H_s = \{\}$ whenever $H_t \neq H_s$

Thus $\mathcal{H}$ is a partition of S.

Let us return now to our relation M_4 and find our partition! For an integer a, let

$$[a] = \{b \mid aM_4b\}$$

The set $[a]$ is the set of elements of $\mathbb{Z}$ that a is related to. For example, when $a = 6$ we have:

$$[6] = \{b \mid 6M_4b\}$$

Remembering the meaning of $6M_4b$ this is the same as

$$[6] = \{b \mid 4 \text{ divides } b - 6\}$$

By Theorem 4.4, we have

$$[6] = \{b \mid b \text{ has the same remainder as 6 when divided by 4}\}$$

Noticing that 6 has remainder 2 when divided by 4 we have:

$$[6] = \{b \mid b \text{ has remainder 2 when divided by 4}\}$$

Thus [6] is the set of all integers that have remainder 2 when divided by 4. A similar argument should tell us, for example, [10] is also the set of all integers that have remainder 2 when divide by 4. And so $[6] = [10]$.

In fact, we have $[6] = [c]$ for every integer c that has remainder 2 when divided by 4. In particular, we notice $[6] = [2]$.

Consider $a' \in \mathbb{Z}$. Since each integer has remainder $0, 1, 2$ or 3 when divided by 4 exactly on of the following is true:

$$[a'] = [0]$$
$$[a'] = [1]$$
$$[a'] = [2]$$
$$[a'] = [3]$$

Therefore

$$\{[a] \mid a \in \mathbb{Z}\} = \{[0], [1], [2], [3]\}$$

Though it may be clear to us that $\{[0], [1], [2], [3]\}$ is a partition of $\mathbb{Z}$, let us wade through the morass of notations and definitions to be certain. Recalling our definition of partition, we must check two things:

1. $[0] \cup [1] \cup [2] \cup [3] = \mathbb{Z}$; and
2. $[j] \cap [k] = \{\}$ whenever $[j] \neq [k]$ $(j, k \in \{0, 1, 2, 3\})$.

1. Each element of $[0] \cup [1] \cup [2] \cup [3]$ is an element of at least one of $[0], [1], [2]$ or $[3]$. Each element of $[0], [1], [2]$ and $[3]$ is an integer. Thus each element of $[0] \cup [1] \cup [2] \cup [3]$ is an element of $\mathbb{Z}$.

Consider some $n \in Z$. Let r be the remainder when n is divided by 4. Notice $r \in \{0, 1, 2, 3\}$ Necessarily we have $n \in [r]$. Therefore $n \in [0] \cup [1] \cup [2] \cup [3]$.

Every element of $[0] \cup [1] \cup [2] \cup [3]$ is an element of $\mathbb{Z}$ and every element of $\mathbb{Z}$ is an element of $[0] \cup [1] \cup [2] \cup [3]$. And so $[0] \cup [1] \cup [2] \cup [3] = \mathbb{Z}$.

2. Consider now $j, k \in \{0, 1, 2, 3\}$ so that $j \neq k$. The set $[j]$ is the set of all integers that have remainder j when divided by 4. The set $[k]$ is the set of all integers that have remainder k when divided by 4. We want to show $[j] \cap [k] = \{\}$.

If $[j] \cap [k] \neq \{\}$, then there is an integer that has remainder j and has remainder k when divided by 4. This is absurd, as an integer can't have two different remainders when dividing by 4. Therefore it cannot be that $[j] \cap [k] \neq \{\}$. Thus $[j] \cap [k] = \{\}$.

Since 1. and 2. are satisfied, $\{[0], [1], [2], [3]\}$ is a partition of $\mathbb{Z}$.

Let us return now to thinking about equivalence relations in general. Just as we defined the set $[a]$ for the equivalence relation M_4 on $\mathbb{Z}$, we can define this set for any equivalence relation on any set.

Let S be a set and let R be an equivalence relation on S. We define the following notation:

$$[s] = \{t \mid sRt\}$$

$$S/R = \{[s] \mid s \in S\}$$

For an element $s \in S$, the set $[s]$ is the set of all elements of S that s is related to with respect to R. This set is called the equivalence class of $[s]$. The set S/R is then the set of equivalence classes of elements of S.

Example 4.6. *Let* $S = \{s_1, s_2, s_3, s_4\}$ *and*

$$R = \{(s_1, s_2), (s_2, s_1), (s_2, s_3), (s_3, s_2), (s_1, s_3), (s_3, s_1), (s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_4)\}$$

We have

$$[s_1] = \{s_1, s_2, s_3\}$$
$$[s_2] = \{s_1, s_2, s_3\}$$
$$[s_3] = \{s_1, s_2, s_3\}$$
$$[s_4] = \{s_4\}$$

and

$$S/R = \{[s_1], [s_2], [s_3], [s_4]\} = \{[s_1], [s_4]\}$$

For our relation $R = M_4$ on $S = \mathbb{Z}$ we have

$$\mathbb{Z}/M_4 = \{[a] \mid a \in \mathbb{Z}\}.$$

Each element of this set is an equivalence class. Further, each such equivalence class is equal to exactly one of $[0], [1], [2]$ or $[3]$. Thus

$$\mathbb{Z}/M_4 = \{[0], [1], [2], [3]\}$$

Above we showed $\mathbb{Z}/M_4$ is a partition of $\mathbb{Z}$. This took a lot of work and a lot of thinking!

Consider the following theorem –

Theorem. *Let S be a set and let R be an equivalence relation. The set*

$$S/R = \{[s] \mid s \in S\}$$

is a partition of S.

Above we showed that this theorem is true when $S = \mathbb{Z}$ and $R = M_4$.

If we could prove this theorem, then no matter which equivalence relation we had we would always be certain that the equivalence classes were a partition. With this theorem in hand, it would be enough to verify that M_4 was an equivalence relation to know that its equivalence classes were a partition of $\mathbb{Z}$. We will prove this theorem, but before we do we build some more comfort with this notation by returning back to $\mathbb{R}^2$ and the relation C.

(There is lots of notation in this section. Don't let it intimidate you! Read slowly and carefully. If you do not understand what a sentence means, don't just ignore it. As you read, make your own notes to make sure you understand what is being said. Refer back to the definitions of these notations in the previous section when you are confused).

Test Your Understanding

1. Let

$$P_1 = \{p_1, p_2, p_3, p_4\}$$
$$P_2 = \{p_2, p_6, p_7\}$$
$$P_3 = \{p_1, p_2, p_4\}$$

   and let $\mathcal{P} = \{P_1, P_2, P_3\}$. What elements are in the set $\bigcup_{P \in \mathcal{P}} P$

2. Let $X = \{x_1, x_2, x_3, x_4, x_5\}$, let

$$X_1 = \{x_1, x_2, x_3\}$$
$$X_2 = \{x_3, x_4\}$$
$$X_3 = \{x_5\}$$

   and let

$$\mathcal{X} = \{X_1, X_2, X_3\}$$

   Is $mathcal X$ as partition of X?

3. Let $S = \{s_1, s_2, s_3, s_4, s_5\}$ and let

   $R = \{(s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_4), (s_5, s_5), (s_1, s_2), (s_2, s_1), (s_1, s_3), (s_3, s_1), (s_2, s_3), (s_3, s_2)\}$

   (a) Which elements are contained in $[s_2]$?

   (b) How many elements are there in S/R?

Test Your Understanding Solution

1. By definition we have

$$\bigcup_{P \in \mathcal{P}} P = P_1 \cup P_2 \cup P_3 = \{p_1, p_2, p_3, p_4, p_6, p_7\}$$

2. No, $\mathcal{X}$ is not a partition of X as $X_1 \cap X_2 \neq \{\}$.
3. The set $[s_2]$ is the set of elements of S that are related to s_2. Therefore $[s_2] = \{s_1, s_2, s_3\}$
4. Since $[s_1] = [s_2] = [s_3]$ we have

$$S/R = \{[s_1].[s_4], [s_5]\}$$

Therefore S/R has three elements.

4.3 Equivalence Relations and Set Partitions

Recall the relation C on $\mathbb{R}^2$:

$$C = \{(x_1, y_1), (x_2, y_2) | (x_1, y_1) \text{ and } (x_2, y_2) \textit{ are the same distance from the origin.}\}$$

Since C is an equivalence relation, we can meaningfully talk about its set of equivalence classes: $\mathbb{R}^2/C$.

$$\mathbb{R}^2/C = \{[p] \mid p \in \mathbb{R}^2\}$$

In the last section we saw that $\mathbb{Z}/M_4$ is a partition of $\mathbb{Z}$. We wonder if $\mathbb{R}^2/C$ is a partition of $\mathbb{R}^2$.

The definition of partition has two parts. We proceed to show each of these two parts of the definition of partition is satisfied.

1. $\bigcup_{[p]\in\mathbb{R}^2/C} [p] = \mathbb{R}^2$

Let us remember what idea this was meant to convey– every element of $\mathbb{R}^2$ is contained in at least one set of the form $[p]$.

To verify 1. is true, we must show that these sets are equal to each other. That is, we show that every element in the set $\bigcup_{[p]\in\mathbb{R}^2/C}[p]$ is an element of $\mathbb{R}^2$ and every element of $\mathbb{R}^2$ is an element of $\bigcup_{[p]\in\mathbb{R}^2/C}[p]$.

Consider some $q_1 \in \bigcup_{[p]\in\mathbb{R}^2/C}[p]$. Since $q_1 \in \bigcup_{[p]\in\mathbb{R}^2/C}[p]$, there exists $p \in \mathbb{R}^2$ so that $q_1 \in [p]$. Since $[p] \subseteq \mathbb{R}^2$ and $q_1 \in [p]$ it must be that $q_1 \in \mathbb{R}^2$. Thus every element of $\bigcup_{[p]\in\mathbb{R}^2/C}[p]$ is an element of $\mathbb{R}^2$.

Consider $p_1 \in \mathbb{R}^2$. Since C is reflexive, $p_1 C p_1$. Therefore $p_1 \in [p_1]$. Thus

$$p_1 \in \bigcup_{[p]\in\mathbb{R}^2/C} [p].$$

Therefore every element of $\bigcup_{[p]\in\mathbb{R}^2/C}[p]$ is an element of $\mathbb{R}^2$. And every element of $\mathbb{R}^2$ is an element of $\bigcup_{[p]\in\mathbb{R}^2/C}[p]$. Thus $\bigcup_{[p]\in\mathbb{R}^2/C}[p] = \mathbb{R}^2$.

2. $[p] \cap [q] = \{\}$ *for any pair* $[p], [q] \in \mathbb{R}^2/C$ *with* $[p] \neq [q]$

Let us remember what idea this was meant to convey– every element of $\mathbb{R}^2$ is contained in no more than one set.

Consider $[p], [q] \in \mathbb{R}^2/C$ with $[p] \neq [q]$. To verify $[p] \cap [q] = \{\}$, we are going to take the following approach *assume* $[p] \cap [q] \neq \{\}$ *and contradict something we know to be true.* This

method is called *proof by contradiction.* The following aside gives an example of a proof by contradiction.

Aside (Proof by Contradiction)**.** *In fact we have already seen a proof by contradiction in these notes!*

In showing that $\{[0],[1].[2],[3]\}$ *was a partition of* $\mathbb{Z}$ *we wanted to show* $[j] \cap [k] = \{\}$*. We wrote the following*

If $[j] \cap [k] \neq \{\}$ then there is an integer that has remainder j and has remainder k when divided by 4. This is absurd, as an integer can't have two different remainders when dividing by 4. Therefore it cannot be that $[j] \cap [k] \neq \{\}$.

We assumed the thing we wanted to show was false, and then concluded something to be true that is actually false.

Let us return now to what we are trying to prove. We want to show $[p] \cap [q] = \{\}$. Let us assume $[p] \cap [q] \neq \{\}$ and derive a contradiction. If $[p] \cap [q] \neq \{\}$, then there is exists some element $s \in [p] \cap [q]$.

Since $s \in [p] \cap [q]$ we know pCs and qCs. Since C is symmetric, it must be that sCq. Since C is transitive it must be that pCq.

We will show $[p] = [q]$. This will contradict that we have chosen $[p]$ and $[q]$ so that $[p] \neq [q]$. To do this we apply our usual technique for showing two sets are equal.

Consider some element $p' \in [p]$. We want to show $p' \in [q]$.

Since $p' \in [p]$, it must be that pCp'. Since C is symmetric, it must be that $p'Cp$. Since pCq and C is transitive, it must be that $p'Cq$. Since C is symmetric, it must be that qCp'. Therefore $p' \in [q]$

Consider some element element $q' \in [q]$. We want to show $q' \in [p]$. Applying the same sequence of deductions as in the previous paragraph gives that $q' \in [p]$.

Since every element of $[p]$ is an element of $[q]$ and every element of $[q]$ is an element of $[p]$, necessarily we have $[p] = [q]$. However this contradicts our assumption that $[p] \neq [q]$. We showed $[p] = [q]$ by assuming $[p] \cap [q]$ was not empty. Since this assumption led to a contradiction, this assumption must be false! Thus $[p] \cap [q]$ is empty. This was what we wanted to show.

Since both parts of the definition of partition hold for $\mathbb{R}^2/C$, it then follows that $\mathbb{R}^2/C$ is a partition of $\mathbb{R}^2$.

In our example with divisibility by 4, our parts of the partition corresponded to the four possible remainders when we divide by 4. What sort of structure do our partitions correspond to here?

Consider $(0,1) \in R^2$. The set $[(0,1)]$ is the set of all elements of $(x,y) \in \mathbb{R}^2$ so that $(0,1)C(x,y)$. Recalling the criteria for a pair of elements to be in C, it must be that all elements of the set $[(0,1)]$ are at distance 1 from the origin. Similarly, the set $[(1,0)]$ is the set of all points in $\mathbb{R}^2$ that are at distance 1 from the origin. Thus

$$[(0,1)] = [(1,0)]$$

Generalizing this argument, we see

$$[(x_1,y_1)] = [(x_2,y_2)]$$

whenever (x_1,y_1) and (x_2,y_2) are the same distance from the origin.

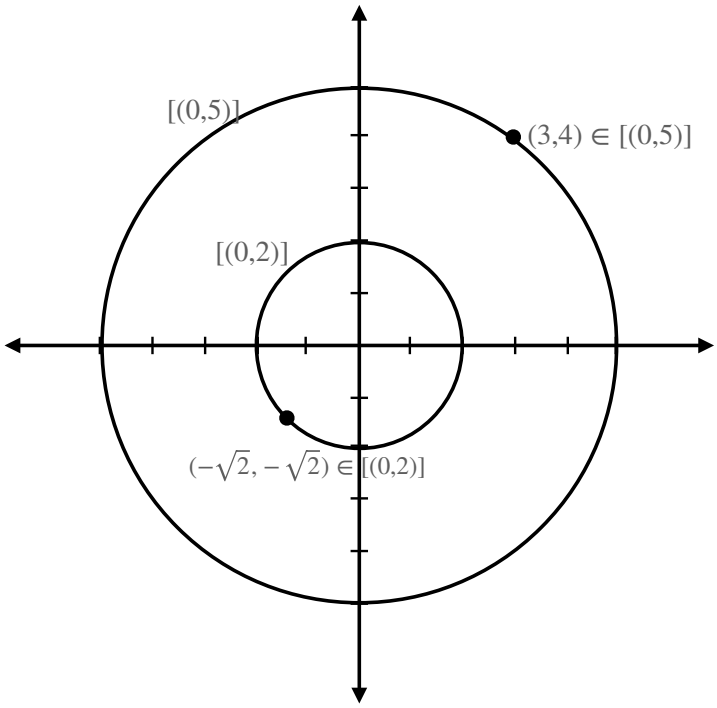
Consider $(x,y) \in R^2$ so that (x,y) is at distance r from the origin. Repeating the argument above gives

$$[(x,y)] = [(0,r)]$$

Therefore

$$\mathbb{R}^2/C = \{[(x,y)] \mid (x,y) \in \mathbb{R}^2\} = \{[(0,r)] \mid r \geq 0\}$$

An element of this set, $[(0,r)]$, is a point in $\mathbb{R}^2$ that is distance r from the origin. The set of points equidistant from the origin defines a circle centred at the origin. Thus $[(0,r)]$ is the circle centred at the origin with radius r. And so the set $\mathbb{R}^2/C$ defines a partition of $\mathbb{R}^2$ into concentric circles centred at the origin.



Let us look back at our line of reasoning in showing that $\mathbb{R}^2/C$ is a partition of $\mathbb{R}^2$. In our argument we didn't really think much about distance from the origin. We appealed only to C being reflexive, symmetric and transitive; this argument will work for any equivalence relation! If we replace $\mathbb{R}^2$ with any set S, and we replace C with any equivalence relation R, our argument is exactly the same. (Quite literally! We can copy and paste the argument that showed $\mathbb{R}^2/C$ is a partition of $\mathbb{R}^2$ and then replace $\mathbb{R}^2$ with S and C with R to get a proof of the following theorem.)

Theorem 4.7. *Let S be a set and let R be an equivalence relation. The set*

$$S/R = \{[s] \mid s \in S\}$$

is a partition of S.

Let us recall our big picture for this module. An equivalence relation lets us group together elements of a set that are the same with respect to some property. In our two examples, we grouped together integers that had the same remainder when divided by 4, and grouped together points in $\mathbb{R}^2$ that are the same distance from the origin. These groups form a partition of our original set; we have grouped things that are the same with respect to some property and every element is in exactly one group.

With our theorem above in hand, we are certain that equivalence classes of any equivalence relation are a partition!

Test Your Understanding

Let $S = \{s_1, s_2, s_3, s_4, s_5\}$ and let $R = \{(s_1, s_1), (s_2, s_2), (s_3, s_3), (s_4, s_4), (s_5, s_5), (s_1, s_2), (s_2, s_1), (s_1, s_3), (s_3,$
Using Theorem 4.7, how do you know S/R is a partition of S?

Test Your Understanding Solution

This is the same relation we saw in *4.1 Test Your Understanding.* In that exercise we determined R is an equivalence relation.

Theorem 4.7 tells us that the set of equivalence classes of an equivalence relation are a partition. Since S/R denotes the set of equivalence classes of R, necessarily S/R is a partition of S.

---

5 Introduction to Formal Logic

Learning Incomes.

- *Comfort with sets and set-builder notation*
- *Familiar with the concept of partition*

Learning Outcomes.

- *understand the meaning of the word proof when used in a mathematics context*
- *how to express a mathematical implication as a statement of formal logic*
- *how to express an if and only if statement as a statement of formal logic*
- *how to express an existentially quantified statement as a statement of formal logic*
- *how to express an universally quantified statement as a statement of formal logic*
- *be able to state the converse and contrapositive of an implication*

Newly Defined Terms and Notation.

- *mathematical statement, truth value, truth table, logically equivalent,* $T(P)$*, not* P*,* $\neg P$*,* P *and* Q*,* $P \wedge Q$*,* P *or* Q*,* $P \wedge Q$*,* P *implies* Q*,* $P \Rightarrow Q$*, hypothesis, conclusion, contrapositive, converse,* P *if and only if* Q*,* $P \Leftrightarrow Q$*, mathematical formula, existential quantifier,* $(\exists x \in X)\ P(x)$*, universal quantifier,* $(\forall x \in X)\ P(x)$*,*

Aside. *Yes, I am starting this module with an aside!. The list of new terms here seems very hefty! Don't let it intimidate you. The material that lies ahead is fairly intuitive. Any time you run in to an unfamiliar piece of notation look back to find its definition and an example of how it is used. As usual, read slowly and carefully. You have lots of time, there is no need to rush. There is no new material for the next two weeks and the question on Assignment 3 about this material is only testing if you understand the notation.*

So far in this course we have seen a small number of theorems and an even smaller number of proofs. Unlike performing calculations, there is very rarely a one-sized-fits-all approach to proving a mathematical statement. Coming up with proofs requires us to fully understand what our theorem is saying and also have a bit of an intuitive idea for why the statement we are considering is true. Only then can we begin the process of crafting our proof.

This said, there are a number of strategies we can employ when trying to come up with a proof for a mathematical statement. Understanding these strategies requires us to dive into topics in formal logic so that we may describe our mathematical statements using notation and terminology that will be the same regardless of the particular statement we are considering.

In this module we will first talk about what proofs are and discuss the difference between formal and informal proofs. We will then proceed to define some notation and terminology from the study of *formal logic* so that we may develop some strategies for informal proofs.

5.1 What are Proofs?

(The following text is adapted from Chapter 3 of *Transition to Higher Mathematics: Structure and Proof*)

For most of you, question 5 on assignment 1 went very poorly. You were asked to prove something without really knowing what it meant to prove something. This was by design. Question 5 on Assignment 1 will not count towards your Assignment 1 mark.

For many of you, it is impossible to really think about proving things until we understand what we mean when we talk about *proofs*. This section is our first introduction to this topic.

The main activity in mathematics is proving mathematical claims. This may seem surprising for you, given that most of the mathematics you have studied has been the application of techniques to deriving solutions of relatively concrete problems. In actuality, the *mathematics* is more in proving that the techniques work as opposed to applying them to specific problems. And so most students find the transition from computational mathematics to mathematical proofs very challenging.

You may wonder why we are doing this in Module 5, rather than in Module 1. To be able to think about proofs we need to have things to prove! Our work in Modules 1 - 4 was to start to get us comfortable within the culture of mathematical norms. We can only begin to be an active and interested participant in this culture until we have spend some time being befuddled by it!

What is a mathematical proof? The nature of a mathematical proof depends on the context. There is a formal notion of a mathematical proof:
A finite sequence of formal mathematical statements such that each statement either

- *is an axiom or assumption, or*
- *follows by formal rules of logical deduction from previous statements in the sequence.*

(What is a formal mathematical statement you may wonder? We see an introduction to these in Section 5.2.)

Most mathematicians do not think of mathematical proofs as formal mathematical proofs, and few mathematicians write formal mathematical proofs. This is because a formal proof is usually a tremendously cumbersome thing. Rather, mathematicians write proofs that are sequences of statements in a combination of natural language and formal mathematical symbols (interspersed with diagrams, questions, references and other devices that are intended to assist the reader in understanding the proof) that can be thought of as representing a purely formal argument. (This said, there is a push in some corners of the mathematics community to use computers to construct formal proofs. If you are interested do an internet search for `theorem prover lean`)

A good practical definition of a mathematical proof is: *an argument in favour of a mathe-*

matical statement that will convince the preponderance of knowledgeable peers of the truth of the mathematical statement

This definition is imprecise and mathematicians can disagree on whether an argument is a proof, particularly for extremely difficult or deep arguments. However, for virtually all mathematical arguments, after some time for careful consideration, the mathematical community reaches a unanimous consensus on whether it is a proof.

The notion of a mathematical proof for the student is similar to the general idea of a mathematical proof defined above. For students, their peers are their fellow students with the same knowledge and experience as them. However, as students are often asked to construct proofs for a myriad of pedagogical reasons, there are some further requirements for student proofs.

Let's define a successful proof by a student as follows:
An argument for a mathematical statement that

- *a fellow student can fully understand;*
- *the instructor cannot refute; and*
- *uses only assumptions that the instructor considers admissible.*

Note that refuting an argument is not the same as refuting the original claim. The sentence *The square of every real number is non- negative because all real numbers are non-negative.* is a false proof of a true statement.

The sentence *The square of every real number is non-negative because all triangles have three sides.* makes no sense: both statements are true, but there is no reason that the second statement follows as a consequence of the first. This is not a valid proof.

Throughout this course you are learning to use the conventions of mathematical grammar and argument. Like most conventions, these are often determined by tradition or precedent. It can be quite difficult, initially, to determine whether your mathematical exposition meets the standards for this course. This is why graders provide feedback on assignments and opportunities for revision are available.

Remember, readers of mathematics are quite impatient with trying to decipher what the author means to say– mathematics is sufficiently challenging when the author writes precisely what they intend! The burden of good communication is on the author of a mathematical proof, not the reader. A proof can be logically correct, but so difficult to follow that it is unacceptable.

Why do mathematicians care about proofs? Mathematicians depend on proofs for certainty and explanation. Once a proof is accepted by the mathematical community, it is virtually unheard of that the result is subsequently refuted. This was not always the case:

in the 19th century there were serious disputes as to whether results had really been proved or not. This led to our modern notion of a "rigorous" mathematical argument.

For very complicated results, writing a detailed proof helps us convince ourselves of the truth of the claim. After a we have hit upon the key idea behind an argument, there is a lot of hard work left developing the details of the argument. Many promising ideas fail as the author attempts to write a detailed argument based on the idea. Finally, proofs often provide a deeper insight into the result and the mathematical objects that are the subject of the proof.

Mathematical proofs are strongly related to formal proofs in a purely logical sense; the existence of an informal mathematical proof is overwhelming evidence for the existence of a formal mathematical proof. If it is not clear that the informal proof could conceivably be interpreted into a formal argument, it is doubtful that the informal argument will be accepted by the mathematical community. Consequently, mathematical arguments have a transparent underlying logical structure. For this reason we shall begin our discussion of mathematical proofs with an informal introduction to formal logic.

Aside. *There are various courses offered at the University of Saskatchewan that offer a formal introduction to formal logic. If you find this module particularly interesting, I suggest you investigate PHIL 241 and PHIL 243.*

Test Your Understanding

Compare your solution to question 5 from Assignment 1 to the posted solution.

1. Do you accept the argument in the solutions as a valid informal mathematical proof?
2. If you did not get full marks on question 1 from Assignment 1 do you understand why the grader didn't accept your argument as a valid informal mathematical proof?

   (If the answer to either of these questions is no, that is okay! Send me an email and let's figure out where you are with this course and with the material in Section 5.1)

5.2 An Informal Introduction to Formal Logic: Statements and Truth Values

As we are taking an informal approach to formal logic, we begin with a very informal definition.

Definition 5.1. *A mathematical statement is a sentence that is either true or false.*

This isn't a great definition of mathematical statement; let us not over think it. Let P be the following mathematical statement

$$\{x\} \subseteq \{y, z\}$$

This doesn't look much a like a sentence, but when we unpack our notation we have the sentence

the set containing x is a subset of the set containing y and z

This statement is false, thus P is false.

Aside. *Not every sentence can be neatly classified as being either true or false. For example, without specifying a value for x, the sentence x^2* is at least 10 *is neither true nor false. Our world of true and false gets even more complicated when we think of sentences that refer to themselves. For example, is the sentence* this sentence is false *true or false?*

By definition, each mathematical statement has a corresponding truth value: true or false. We denote these truth values as 1 and 0 respectively.

Definition 5.2. *When P is a mathematical statement that is true, then we say P has truth value 1 and we write $T(P) = 1$. When P is a mathematical statement that is false, then we say P has truth value 0 and we write $T(P) = 0$.*

Aside. *It might seem odd that we are choosing to denote true as 1 and false as 0 instead of as T and F respectively. There are some good reasons to choose 1 and 0 rather than T and F. For us, the choice of 1 and 0 over T and F is motivated by a want for clarity. We will be talking about a lot of mathematical statements over this coming modules. We will always label these statements using majuscule letters. We choose to use 1 and 0 rather than T and F so that we may avoid confusing a truth value (a 1 or a 0) with a statement (a majuscule letter.)*

In our example above we have $T(P) = 0$.

Aside. *The notation for truth value should remind us of the notation for image in the context of functions. In fact, truth values is a function! Let S be the set of all mathematical statements, we have $T : S \to \{0, 1\}$.*

Let P_1 be the statement

$$7 \textit{ is prime}$$

and let P_2 be the statement

$$15 \textit{ is an even number}$$

The sentence

$$7 \textit{ is prime and } 15 \textit{ is an even number}$$

seems like a perfectly reasonable mathematical statement. We judge this mathematical statement to be false as the statement 15 *is an even number* is false.

Just as we can use *and* and *or* to link these two sentences in natural writing/speaking, we may so the same with mathematical statements. We can also use *not* in the expected way.

Definition 5.3. *Let P and Q be mathematical statements.*

The mathematical statement P and Q is denoted as $P \wedge Q$. We have $T(P \wedge Q) = 1$ when $T(P) = 1$ and $T(Q) = 1$. We have $T(P \wedge Q) = 0$ otherwise.

The mathematical statement P or Q is denoted as $P \vee Q$. We have $T(P \vee Q) = 0$ when $T(P) = 0$ and $T(Q) = 0$. We have $T(P \vee Q) = 1$ otherwise.

The mathematical statement not P is denoted as $\neg P$. We have $T(\neg P) = 1$ when $T(P) = 0$. We have $T(\neg P) = 0$ when $T(P) = 1$

This definition seems a bit of a mess! We can organize these definitions with a truth table

P	Q	$\neg P$	$P \vee Q$	$P \wedge Q$
1	1	0	1	1
1	0	0	1	0
0	1	1	1	0
0	0	1	0	0

Looking across a row gives us the truth values for $\neg P$, $P \vee Q$ and $P \wedge Q$ based on the corresponding truth values of P and Q.

Notice $P \wedge Q$, $P \vee Q$ and $\neg P$ are mathematical statements in their own right. The truth value of these statements depends upon the truth values of P and Q.

Since $P \wedge Q$, $P \vee Q$ and $\neg P$ are mathematical statements in their own right, we can use our connectives ($\wedge$, $\vee$ and $\neg$) to consider more complicated mathematical statements. For example, given mathematical statements P and Q we can meaningfully consider the mathematical statement $(P \vee Q) \wedge \neg P$. We can use a truth table to determine the truth value of this statement as a function of the truth values of P and Q.

P	Q	$P \vee Q$	$\neg P$	$(P \vee Q) \wedge \neg P$
1	1	1	0	0
1	0	1	0	0
0	1	1	1	1
0	0	0	1	0

This table is telling us, for example, that when P and Q are both true, then $(P \vee Q) \wedge \neg P$ is false.

Example 5.4. *Construct the truth table for the statement $\neg P \wedge Q$.*

The truth value for this statement depends on the truth value of P and Q. Given the truth value of P and Q we also need to know the truth value of $\neg P$ before we can find the truth value of $\neg P \wedge Q$. We begin with a table with columns for each of P, Q, $\neg P$ and $\neg P \wedge Q$.

P	Q	$\neg P$	$\neg P \wedge Q$

We want to consider all possibilities for combinations of truth values for P and Q. And so we fill in all four possible combination. (Notice that all these possibilities are actually elements of $\{0,1\} \times \{0,1\}$).

P	Q	$\neg P$	$\neg P \wedge Q$
1	1		
1	0		
0	1		
0	0		

(There is no need to write these combinations of 0*s and* 1*s in this particular order. It feels natural to* me *to start with* $1 \mid 1$ *and end with* $0 \mid 0$*. If you want to make life easier for the grader in this course, please use this same ordering for your solutions)*

Working left to right by column, we see that we have enough information to compute the values in the third column.

P	Q	$\neg P$	$\neg P \wedge Q$
1	1	0	
1	0	0	
0	1	1	
0	0	1	

Continuing to work left to right, we now see that we have enough information to compute the values in the fourth column.

P	Q	$\neg P$	$\neg P \wedge Q$
1	1	0	0
1	0	0	0
0	1	1	1
0	0	1	0

Our fourth row is exactly the row we needed to compute to know the truth value of $\neg P \wedge Q$ *in all possible cases. And so we are done.*

Exercise 5.5. *Construct the truth table for the statement* $\neg P \vee Q$

Let us look again at the truth tables for $(P \vee Q) \wedge \neg P$ and $\neg P \wedge Q$

P	Q	$P \vee Q$	$\neg P$	$\neg P \wedge Q$	$(P \vee Q) \wedge \neg P$
1	1	1	0	0	0
1	0	1	0	0	0
0	1	1	1	1	1
0	0	0	1	0	0

Notice that the column for $\neg P \wedge Q$ is the same as the column for $(P \vee Q) \wedge \neg P$. This tells us that, in some sense, $\neg P \wedge Q$ and $(P \vee Q) \wedge \neg P$ are the same statement. We call this sense of sameness *logical equivalence.* Two statements are logically equivalent when they have the same columns in the truth table. For example, we can see P is logically equivalent to $\neg(\neg P)$

P	$\neg P$	$\neg(\neg P)$
1	0	1
0	1	0

Thinking about the concept of a *double negative* tells us that it is reasonable to have this logical equivalence

Aside. *The use of the word equivalence should remind us of equivalence relations. We can define an equivalence relation on the set of all mathematical statements, so that two statements are equivalent when they have the same column in the truth table. If we only consider statements with P and Q, how many equivalence classes does this relation have?*

Test Your Understanding

1. Which connective $(\neg, \wedge, \vee)$ should replace the question mark in the truth table below?

P	Q	$P \ ? \ Q$
1	1	1
1	0	1
0	1	1
0	0	0

2. Let P and Q be mathematical statements so that $T(P) = 1$ and $T(Q) = 0$. Determine the truth value of each of the following statements

   (a) $P \wedge Q$

   (b) $P \vee Q$

   (c) $\neg Q$

   (d) $P \wedge \neg P$

   (e) $(\neg P \wedge Q) \vee (P \vee Q)$

3. Determine if $(\neg P \wedge Q) \vee (P \vee Q)$ and $(P \wedge \neg Q) \vee (\neg P \wedge Q)$ are logically equivalent.

Test Your Understanding Solution

1. By inspection this is the truth table for "P or Q". And so the symbol $\vee$ should replace ?.

2. We appeal to the definitions of $\neg, \wedge, \vee$ given in the module.

   (a) $T(P \wedge Q) = 0$ when $T(P) = 1$ and $T(Q) = 0$

   (b) $T(P \vee Q) = 1$ when $T(P) = 1$ and $T(Q) = 0$

   (c) $T(\neg Q) = 1$ when $T(Q) = 0$

   (d) $T(P \wedge \neg P) = 0$ no matter the truth value of P.

   (e) When $T(P) = 1$ and $T(Q) = 0$ we have $T(\neg P \wedge Q) = 0$ and $T(P \vee Q) = 1$. And so $T((\neg P \wedge Q) \vee (P \vee Q)) = 1$

3. We compute the truth tables for $(\neg P \wedge Q) \vee (P \vee Q)$ and $(P \wedge \neg Q) \vee (\neg P \wedge Q)$

P	Q	$\neg P$	$\neg Q$	$\neg P \wedge Q$	$P \wedge \neg Q$	$P \vee Q$	$(\neg P \wedge Q) \vee (P \vee Q)$	$(P \wedge \neg Q) \vee (\neg P \wedge Q)$
1	1	0	0	0	0	1	1	0
1	0	0	1	0	1	1	1	1
0	1	1	0	1	0	1	1	1
0	0	1	1	0	0	0	0	0

   Since the column for $(\neg P \wedge Q) \vee (P \vee Q)$ is not the same as the column for $(P \wedge \neg Q) \vee (\neg P \wedge Q)$, the two statements are not equivalent.

5.3 Modelling Mathematical Theorems with Formal Logic

Consider the following mathematical statement

Let n be an integer. If n is divisible by 4, then n is even.

Is this mathematical statement true? Well, if n is divisible by 4, then n is a multiple of 4. And so there exists an integer k so that $n = 4k$. Notice now that $n = 4k = 2(2k)$. Therefore n is a multiple of 2. This is the same as saying that n is even. Therefore n is even.

Aside. *Does this argument fit the definition of informal mathematical proof we outlined in the previous section?*

With our natural English vocabulary, we might want to reach for the word *implies* to describe the relationship between n being divisible by 4 and n being even.

Let n be an integer. The integer n is divisible by 4 implies n is even.

Let P be the statement

n is divisible by 4.

and let Q be the statement

n is even.

We may rewrite our statement above as:

P implies Q.

The statement *P implies Q* satisfies our definition of mathematical statement – it is either true or false. (In this case it is true) Thus to fully encode similar statements in formal logic must find a way to encode *if, then* conditions as mathematical statements. We do this by defining *implication*.

Aside. *In natural English writing and speaking we sometimes use often the word implies to* suggest *a more casual relationship between two things. For example, one might say:*

My low mark on Assignment 1 implies that I am bad at mathematics.

But of course there are many other reasons Assignment 1 may have gone poorly for you. Given the context of this semester, it is not at all reasonable to equate your marks with any sort of skill or aptitude for mathematics! (In fact, this is largely true even outside the context of teaching and learning in a pandemic.)

In mathematics, our meaning when we use the word implies *is much stronger If we say P* implies *Q, then knowing P is true makes it definite that Q is true.*

Definition 5.6. *Let P and Q be mathematical statements. The mathematical statement P* implies *Q is denoted as $P \Rightarrow Q$. We call P the hypothesis of the implication and we call Q the conclusion of the implication. The truth values for the mathematical statement $P \Rightarrow Q$ are given by the following table.*

P	Q	$P \Rightarrow Q$
1	1	1
1	0	0
0	1	1
0	0	1

Exercise 5.7. *Using a truth table, show*

$$P \Rightarrow Q$$

is logically equivalent to

$$\neg P \vee Q$$

At this point, this definition (that is, the values in the truth table) for implies is unmotivated. Let us examine some examples to convince ourselves that it is a reasonable definition for P implies Q.

Consider the sentence

If I close my eyes, then I cannot read these notes.

Let P be the hypothesis

I close my eyes

and Q be the conclusion

I cannot read these notes.

Then our sentence above corresponds to $P \Rightarrow Q$. Since the sentence above is true, we have $T(P \Rightarrow Q) = 1$. Thus, our definition for $T(P \Rightarrow Q)$ seems reasonable when $T(P) = 1$ and $T(Q) = 1$ as in this case we have $T(1 \Rightarrow 1) = 1$.

If I can read these notes, then my eyes are are open.

This is sentence gives the same information as the previous one. Defining P and Q as above, this is sentence the statement $\neg Q \Rightarrow \neg P$. Above we agreed that this sentence is true. Thus

$$T(\neg Q \Rightarrow \neg P) = 1$$

when $T(P) = 1$ and $T(Q) = 1$

And so we have

$$T(0 \Rightarrow 0) = 1.$$

This agrees with our definition for the fourth row in the truth table for $\Rightarrow$ above. This example convinces us that the first and last rows in our definition of $\Rightarrow$ are reasonable.

We consider some other examples to justify the other two rows in our truth table for $\Rightarrow$. Consider the statement

If my shoes are wet, then it is raining.

This sentence is false. It is entirely possible for my shoes to be wet without it raining. (Perhaps I have fallen into a lake.)

Let P be the statement

My shoes are wet.

And let Q be the statement

It is raining.

Thus when $T(P) = 1$ and $T(Q) = 0$ we have

$$T(1 \Rightarrow 0) = 0.$$

This justifies the third row in the truth table for implies. Our only remaining row left to justify is

$$T(0 \Rightarrow 1) = 1.$$

Consider the following sentence.

$$\textit{If } n \geq 3 \textit{ and } n \textit{ is prime, then } n \textit{ is odd.}$$

This sentence is true no matter which value of n we consider. Let P be the hypothesis.

$$n \geq 3 \textit{ and } n \textit{ is prime}$$

and let Q be the conclusion

$$n \textit{ is odd}$$

Since the sentence above is true, we should have

$$T(P \Rightarrow Q) = 1$$

no matter the truth values of P and Q.

For example, when $n = 7$ we have $T(P) = 1$ and $T(Q) = 1$ and indeed we have

$$T(1 \Rightarrow 1) = 1$$

Consider then the case $n = 9$. In this case we have $T(P) = 0$ and $T(Q) = 1$. Since

$$T(P \Rightarrow Q) = 1$$

it must be that

$$T(0 \Rightarrow 1) = 1$$

This justifies the third row in our definition of implies.

Aside. *That we have* $T(0 \Rightarrow 1) = 1$ *feels weird.*

Continuing with this example, we relied on our intuition to tell us that the implication

$$\textit{If } n \geq 3 \textit{ and } n \textit{ is prime, then } n \textit{ is odd.}$$

is true. But what is our strategy for actually writing down a proof?

Our tools in our study of formal logic give us a strategy to show that this theorem is true. To prove that our theorem is correct, we must verify

$$T(P \Rightarrow Q) = 1$$

Looking at our truth table for implies, we can see that when $T(P) = 0$, have $T(P \Rightarrow Q) = 1$ regardless of the truth value for Q.

Thus to verify

$$T(P \Rightarrow Q) = 1$$

we need to show that if $T(P) = 1$, then necessarily $T(Q) = 1$.

Proof. Let us assume we have $T(P) = 1$. If our integer $n \geq 3$ is prime, then it has no divisors other than one and itself. In particular, 2 does not divide n. Therefore n is odd. Thus $T(Q) = 1$. □

Aside. *Does this fit the definition of informal mathematical proof we outlined in Section 5.1 of this module?*

Before we move onto further types of statements, let us return to one of our examples above:

If I close my eyes, then I cannot read these notes.

In our discussion above we stated that this statement had the same meaning as the statement

If I can read these notes, then my eyes are are open.

This latter sentence is called the contrapositive. More formally –

Definition 5.8. *Let P and Q be statements. The statements $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ are logically equivalent. The statement $\neg Q \Rightarrow \neg P$ is called the contrapositive of $P \Rightarrow Q$.*

Let P be the statement

I close my eyes

and Q be the statement

I cannot read these notes.

The contrapositive of the statement $P \Rightarrow Q$ is the statement

If I can read these notes, then my eyes are open.

The logical equivalence of an implication and its contrapositive gives us a technique to prove an implication is true. From our example above, we considered the statement

Let n be an integer. If n is divisible by 4, then n is even.

The contrapositive of this implication is the statement

Let n be an integer. If n is odd, then n is not divisible by 4.

Since these two statements are logically equivalent, proving this second statement is true tells that the first statement is true. Proving the statement of the contrapositive is something we will make much use of in the upcoming modules.

5.3.1 Converse Statements

Our experience with division more or less tells us directly that the statement

Let n be an integer. If n is divisible by 4, then n is even.

is true.

What about the statement

Let n be an integer. If n is even, then n is divisible by 4

This statement definitely isn't true. The integer 6 is even, but 6 is not divisible by 4. In general, knowing that a statement $P \Rightarrow Q$ is true or false tells us nothing about the truth value of the statement $Q \Rightarrow P$.

Definition 5.9. *Let P and Q be statements. The statement $Q \Rightarrow P$ is called the converse of the implication $P \Rightarrow Q$. In general, the truth value of an implication and its converse are unrelated.*

The relationship between an implication and its converse can change depending on the particular statements P and Q. In our example above

Let n be an integer. If n is divisible by 4, then n is even.

the implication is true and the converse is not. However, there are times when both the implication and the converse are true.

5.3.2 If and Only If Statements

Recall Theorem 4.4 from Module 4.

Theorem. *We have aM_4b if and only if a and b have the same remainder when divided by 4.*

Rather than being of the form *if P, then Q*, the statement of this theorem is of the form *P if and only if Q*. In the aside following the statement of the theorem in Module 4 it noted that the use of the phrase *if and only if* was meant to mean that the following two statements are true.

1. if aM_4b, then a and b have the same remainder when divided by 4; and
2. if a and b have the same remainder when divided by 4, then aM_4b.

Notice the relationship between these two implications. The second is the converse of the first (and the first is the converse of the second!). In this case both implication and the converse are true.

Let a and b be integers. Let P be the statement

$$aM_4b$$

and let Q be the statement

$$a \text{ and } b \text{ having the same remainder when divided by } 4$$

Interpreted as outlined above, the statement

$$P \textit{ if and only if } Q$$

seems like a perfectly reasonable mathematical statement – it is either true or false. We define this connective, if and only if, as follows:

Definition 5.10. *Let P and Q be mathematical statements. The mathematical statement P if and only if Q is denoted as $P \Leftrightarrow Q$. The truth value of the mathematical statement*

$P \Leftrightarrow Q$ is given by the following table.

P	Q	$P \Leftrightarrow Q$
1	1	1
1	0	0
0	1	0
0	0	1

Notice that $P \Leftrightarrow Q$ is true exactly when P and Q have the same truth values. When $P \Leftrightarrow Q$ is true we can understand P and Q to be *mathematical synonyms*. The two statements give identical information.

Exercise 5.11. *Using a truth table, show*

$$P \Leftrightarrow Q$$

is logically equivalent to

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

Test Your Understanding

1. For each implication below, write out as sentences the converse and the contrapositive.
   (a) If $n = 54$, then n is prime.
   (b) If $A = \{\}$, then $A \cup B = B$
   (c) If R is an equivalence relation on S, then S/R is a partition of S.
2. Determine which of the following if and only if statements are true:
   (a) Let S be a shape. S is a square if and only if S is a rectangle.
   (b) Let a and b be integers. a is greater or equal to b if and only if $b - a < 0$.
   (c) $A \cup B = B$ if and only if $A = \{\}$.

Test Your Understanding Solution

1. (a)
   - Converse: If n is prime, then $n = 54$
   - Contrapositive: If n is not prime, then $n \neq 54$.

   (b)
   - Converse: If $A \cup B = B$, then $A = \{\}$
   - Contrapositive: If $A \cup B \neq B$, then $A \neq \{\}$

   (c)
   - Converse: If S/R is a partition of S, then R is an equivalence relation on S.
   - Contrapositive: If S/R is not a partition of S, then R is not an equivalence relation on S.

2. (a) The statement: "If S is a square then $S$is a rectangle" is true. The statement "If S is a rectangle, then S is a square" is false. Therefore the statement S is a square if and only if S is a rectangle is false.

   (b) The statement "If a is greater than b, then $b - a < 0$ " is true. The statement "if $b - a < 0$, then a is greater than b" is true. Therefore the statement "a is greater or equal to b if and only if $b - a < 0$" is true.

   (c) The statement: "if $A \cup B = B$, then $A = \{\}$." is false. The statement "if $A = \{\}$., then $A \cup B = B$ " is true. Therefore the statement " $A \cup B = B$ if and only if $A = \{\}$." is false.

5.4 Formulas and Quantifiers in Formal Logic

At the start of this module our definition of mathematical statement told us that every mathematical statement was either true or false. But as we got to the end of the previous section we started to think about mathematical statements that were true or false depending on the value of some variable.

Consider the sentence

$$x^2 \text{ is less than } 10$$

This sentence is neither true nor false unless we specify a value of x. This is the exact situation we saw when we introduced set-builder notation. Recall our definition from Module 1.

Definition. *Let X be a set, and let $P(x)$ be a statement that is either true or false for each $x \in X$. The set*

$$\{x \in X \mid P(x)\}$$

is the set of elements in X for which $P(x)$ is true. The set X is called the domain of the variable.

From this, we arrive at a definition of mathematical formula.

Definition 5.12. *Let X be a set. A mathematical formula over X is a statement that is true for false depending on the choice of $x \in X$. We denote a mathematical formula with the notation $P(x)$.*

For example, for $x \in \mathbb{Z}$ let $P(x)$ be the mathematical formula

$$x \text{ is even}$$

For some values of x we have that $P(x)$ is true, whereas for others $P(x)$ is false.

5.4.1 Quantifiers

Recall again Theorem 4.10 from Module 4.

Theorem. *Let S be a set and let R be an equivalence relation. The set*

$$S/R = \{[s] \mid s \in S\}$$

is a partition of S.

This theorem is telling us that for each equivalence relation R on S, the set S/R is a partition of S. Let us try to express this theorem using our language of formal logic by using a formula.

Let S be a set and let $ERel$ be the set of all possible equivalence relations on S. For $R \in ERel$, let $P(R)$ be the formula

$$S/R \text{ is a partition of } S$$

The theorem above is saying

$$\text{For each } R \in ERel \text{ we have } T(P(R)) = T$$

This is a mathematical statement – it is either true or false..

Our tools from the previous parts don't quite seem enough to express this statement in formal logic. Written this way, it is not an *implication*, nor an *if and only if* statement. Let us now develop the tools to model such statements in formal logic.

Let X be a set and let $P(x)$ be a formula over X. For each $z \in X$, the statement $P(z)$ is either true or false. Let T_X be the set of elements of X for which $P(x)$ is true. Similarly, let F_X be the set of elements of X for which $P(x)$ is false.

Example 5.13. *If $P(x)$ is the formula x* is even*, then*

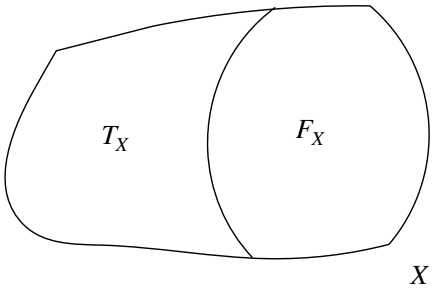
$$T_{\mathbb{Z}} = \{\ldots, -2, 0, 2, \ldots\}$$
$$F_{\mathbb{Z}} = \{\ldots, -3, -1, 1, 3, \ldots\}$$

Whereas when $P(x)$ is the formula S/R is a partition*, we have $F_{ERel} = \{\}$ and $T_{ERel} = ERel$*

Formally we define T_X and F_X as follows:

$$T_X = \{z \mid T(P(z)) = 1\}$$
$$F_X = \{z \mid T(P(z)) = 0\}$$

Notice that the set $\{T_X, F_X\}$ is a partition of X.



Of course, drawing the picture this way seems to suggest that each of T_X and F_X are necessarily non-empty. In our example above with $X = ERel$ we had that $F_{ERel} = \{\}$. Let us consider what it would mean for one of T_X or F_X to be the empty set.

If $F_X = \{\}$, then for each $z \in X$ we have $T(P(z)) = 1$. Whereas if $F_X \neq \{\}$, then there is at least one $z \in X$ so that $T(P(z)) = 0$.

If $T_X = \{\}$, then for each $z \in X$ we have $T(P(z)) = 0$. Whereas if $T_X \neq \{\}$, then there is at least one $z \in X$ so that $T(P(z)) = 1$.

And so for a formula $P(x)$ the following are mathematical statements – they are each either true or false.

$$\textit{For each } z \in X \textit{ we have } T(P(z)) = 1$$

$$\textit{There exists at least one } z \in X \textit{ so that } T(P(z)) = 0$$

The first of these statements is true when $F_X = \{\}$. The second of these statements is true when $T_X \neq \{\}$

We define the following notation.

Definition 5.14. *Let X be a set and let $P(x)$ be a formula over X. We write*

$$(\forall x \in X)\, P(x)$$

to mean the statement

$$\text{For each } z \in X \text{ we have } T(P(z)) = T.$$

We call the symbol $\forall$ the universal quantifier

Definition 5.15. *Let X be a set and let $P(x)$ be a formula over X. We write*

$$(\exists x \in X)\, P(x)$$

to mean the statement

$$\text{There exists at least one } z \in X \text{ so that } T(P(z)) = T.$$

We call the symbol $\exists$ the existential quantifier

Aside. *In other places you may see $\forall$ defined to mean* "for all" *and $\exists$ defined to mean* "there exists"*. These phrases are much more standard in mathematics, but I think they aren't quite as clear when students are learning for the first time. We should understand the phrase* "for all $x \in X$" *to mean the same as* "for each $x \in X$" *and we should understand the phrase* "there exists $x \in X$" *to mean the same as* "there exists at least one $x \in X$"*.*

Aside. *Which of the following is easier to understand?*

- $X \cup Y \neq Y \implies \exists x \in X$ *so that* $x \notin Y \Rightarrow X \not\subseteq Y$
- *If $X \cup Y \neq Y$, then there exists $x \in X$ so that $x \notin Y$. This then implies that X is not a subset of Y.*

It is the second one, right?

The goal of mathematical communication is to communicate mathematical ideas. When we doctor up our writing with more mathematical symbols than necessary we are not being more mathematical. Instead we are doing a bad job at communicating.

At no time have these notes for this section used any of our new notation: $\vee, \wedge, \neg, \Rightarrow, \Leftrightarrow, \forall$ and $\exists$ as part of English sentences to replace the words or, and, not, implies, if and only if, for each *and* there exists*. These are symbols in formal logic and should not be used when we are trying to communicate mathematics to another person (such as in our assignment solutions). Using these symbols instead of communicating in plain language the words we want to express puts a significant barrier between us and our readers.*

5.4.2 Proving statements with existential quantifiers

For $n \in \mathbb{N}$, let $P(n)$ be the formula *n is prime.* From our work in the previous section, we can meaningfully consider the mathematical statement

$$(\exists x \in \mathbb{N})\, P(x)$$

This statement is true. There is at least one $n \in \mathbb{N}$ so that n is prime. If asked for further evidence, how would you convince someone that the statement is true? From our discussion above about the sets $F_{\mathbb{N}}$ and $T_{\mathbb{N}}$ it is enough to demonstrate that $T_{\mathbb{N}}$ contains at least one element. We can do this by giving an example of an element that is in $T_{\mathbb{N}}$. For example, since 5 is prime, we have $T(P(5)) = 1$ and so $5 \in T_{\mathbb{N}}$. Therefore the statement

$$(\exists x \in \mathbb{N})\, P(x)$$

is true.

This is an excellent strategy for proving existentially quantified statements. It is enough to give just a single example that makes the statement true.

On the other hand, this strategy does not work for universally quantified statements. Even though we can find many examples of $z \in \mathbb{N}$ so that $T(P(z)) = T$, the statement

$$(\forall x \in \mathbb{N})\, P(x)$$

is false. We return to strategies to prove universally quantified statements in Module 6.

5.4.3 Multiple Quantifiers

Just as we could chain together our connectives to create more complicated statements, there is nothing stopping us from doing the same with quantifiers in formulas that have multiple variables.

Let $P(x, y)$ be the following formula over $\mathbb{R}^2$

$$x > y$$

For example, $P(3, 4)$ is false, and $P(11, 3)$ is true.

Consider the following two statements

For every value of $x \in \mathbb{R}$ there exists at least one value of $y \in \mathbb{R}$ so that $x > y$.

There exists at least one value $x \in \mathbb{R}$ so that for every value of $y \in \mathbb{R}$ we have $x > y$.

The first of these statements is true. For any value of x one chooses, say x', we can certainly find a value for y so that $x' > y$ (For example, once we have chosen $x = x'$, we can choose y to be $x' - 1$.)

One the other hand, this second statement is false. Given a value for x, say x', , we can always find at least one value of y so that $y \leq x'$.

Encoding these two statements in our language of formal logic gives:

$$(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})P(x, y)$$

and

$$(\exists x \in \mathbb{R})\,(\forall y \in \mathbb{R})P(x, y)$$

Test Your Understanding

1. Let $P(n)$ be the following formula over $\mathbb{Z}$:

$$\textit{exactly one of } n-1,\ n \textit{ and } n+1 \textit{ is even}$$

   (a) Give an example of an element in $T_{\mathbb{Z}}$ or state there are none.

   (b) Give an example of an element in $F_{\mathbb{Z}}$ or state there are none.

   (c) Using your answer from (a), determine if the following statement is true: $(\exists n \in \mathbb{Z})\ P(n)$.

   (d) Using your answer from (b) determine if the following statement is true: $(\forall n \in \mathbb{Z})\ P(n)$.

2. Let $P(x, y)$ be the following formula over $\mathbb{R}^2$:

$$x \leq y$$

   For each statement below first write it out as a sentence and then determine if it is true.

   (a) $(\exists (x, y) \in \mathbb{R}^2) \quad P(x, y)$

   (b) $(\forall (x, y) \in \mathbb{R}^2) \quad P(x, y)$

   (c) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R}) \quad P(x, y)$

   (d) $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R}) \quad P(x, y)$

Test Your Understanding Solution

1. (a) Exactly one of 1,2 and 3 is even. Thus $P(2)$ is true. Therefore $2 \in T_{\mathbb{Z}}$.

   (b) Two of 0,1, and 2 are even. Thus $P(2)$ is false. Therefore $1 \in F_{\mathbb{Z}}$.

   (c) Since $T_{\mathbb{Z}}$ is not empty, there is at least one $n \in \mathbb{N}$ so that $P(n)$ is true. Therefore $(\exists n \in \mathbb{Z})\ P(n)$ is true.

   (d) Since $F_{\mathbb{Z}}$ is not empty, there is at least one $n \in \mathbb{Z}$ so that $P(n)$ is false. Therefore $(\forall n \in \mathbb{Z})\ P(n)$ is false.

2. (a) "There exists at least one pair $(x, y) \in \mathbb{R}^2$ so that the statement $x \leq y$ is true". This statement is true as $P(0, 1)$ is true.

   (b) "For each pair $(x, y) \in \mathbb{R}^2$ the statement $x \leq y$ is true". This statement is false as $P(1, 0)$ is false.

   (c) "For each $x \in \mathbb{R}$ we can find at least one $y \in \mathbb{R}$ so that $P(x, y)$ is true". This statement is true, as given x we can take $y = x + 1$ to make $P(x, y)$ true.

   (d) "There exists at least one $y \in \mathbb{R}$ so that for each $x \in \mathbb{R}$ the statement $P(x, y)$ is true". This statement is false. For every $y \in \mathbb{R}$ there is at least one $x \in \mathbb{R}$ so that $P(x, y)$ is false.

5.5 Optional Section: Limits to Infinity

You will not be assessed on any of the content for this section. Feel free to ignore it.

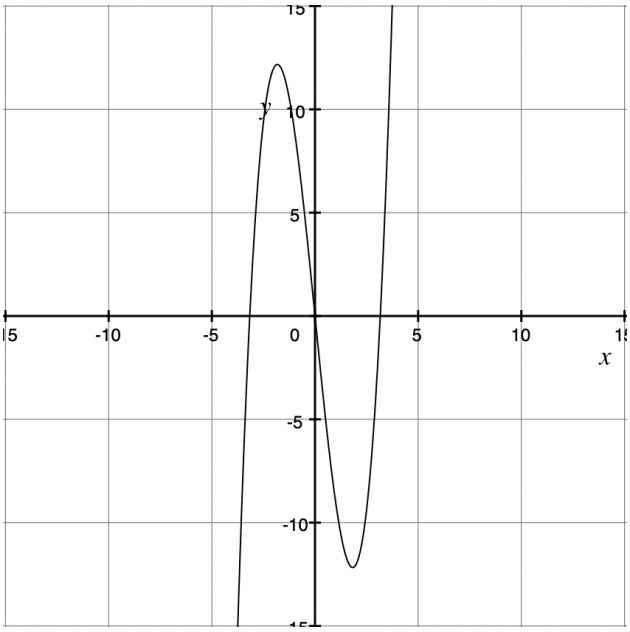
Quite likely you have encountered the following notation in a calculus class:

$$\lim_{x\to\infty} f(x) = \infty$$

As we have seen through our work so far in this class, mathematical notation short-hand for mathematical ideas. Asked what this notation means I expect most of you would respond, quite fairly, something like

It means that as the input to the function gets bigger, then the output of the function gets bigger and bigger

Let us see if we can massage this intuition into something a little bit more precise. To do so let us consider the function $f(x) = x^3 - 10x$.



I suspect we agree that the following statement is true:

$$\lim_{x\to\infty} x^3 - 10x = \infty$$

Looking at our picture of the function $x^3 - 10x$ it is not quite true that the value of the function gets bigger as we input bigger values. For example, when $x = -2$ we see that

$x^3 - 10x > 5$. Whereas for $x = 2$ we see that $x^3 - 10x < 5$.

However it is true that eventually the function $x^3 - 10$ is bigger than 5 and stays bigger than 5.

Let us then, informally, consider

$$\lim_{x \to \infty} f(x) = \infty$$

to mean:

for every k, the function $f(x)$ is eventually always bigger than k

Okay, now we will turn to our formal notation. We change our example to think about a linear function to make things easier to think about.

For $x, k \in \mathbb{R}$, let $P(x, k)$ denote the formula

$$2x + 1 > k$$

For some values of x and k this statement is true. Whereas for other values of x and k this statement is false. To simplify our consideration further let us restrict our attention by setting $k = 3$.

Using our notation from above we can see

$$T\left((\forall x \in \mathbb{R})\, P(x, 3)\right) = 0$$
$$T\left((\exists x \in \mathbb{R})\, P(x, 3)\right) = 1$$

Thinking about the second of these statements, for which values of $x \in \mathbb{R}$ do we have $T(P(x, 3)) = 1$? This is equivalent to asking, for which values of $x \in R$ is $2x + 1 > 3$? This is a question which we know to answer: We have $2x + 1 > 3$ exactly when $x > 1$.

And so we can say something stronger than

$$T\left((\exists x \in \mathbb{R})\, P(x, 3)\right) = 1$$

In fact there exists a value $x' \in \mathbb{R}$ so that $T(P(x, 3)) = 1$ whenever $x > x'$. (In particular, this is true when we choose $x' = 1$) Translating this back to our notation in formal logic:

$$T\left((\exists x' \in \mathbb{R})\, (\forall x > x')\; P(x, 3)\right) = 1$$

Back to our English writing, this is the same as :

There exists a real number x' so that for every x that is greater than x' it is true that $2x' + 1 > 3$.

What does this mean in the concept of limits? When we talk about a limit going off towards infinity we are saying that our function is eventually always bigger than any real number. Above we have shown not only that the function $2x + 1$ bigger than 3 at $x = 1 + \epsilon$, but in fact $2x + 1$ is bigger than 3 for every value $x > 1$. We could substitute 3 for any other value, say k, and still be able to find a value x' so that $2x + 1$ is bigger than k whenever x is greater than x'. (The value of x' would depend on which specific k we were thinking about. When $k = 3$ we found $x' = 1$. For $k = 10$ we would find $x' = 9/2$)

So, then, what should we make of the statement

$$((\forall k \in \mathbb{R})\,(\exists x' \in \mathbb{R})\,(\forall x > x')\;\; P(x, k)) = 1$$

We have swapped out our 3 for the variable k. This statement says:

For every integer $k \in \mathbb{R}$ we can find a value $x' \in \mathbb{R}$ so that $2x + 1$ is bigger than k whenever x is greater than x'. This is the definition of a limit going to infinity.

Definition 5.16. *Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous function. We say the limit of $f(x)$ as x goes to infinity is infinity when for every $k \in \mathbb{R}$ there exists $x' \in \mathbb{R}$ so that $f(x) > k$ whenever $x > x'$.*

When the limit of $f(x)$ as x goes to infinity is infinity we write

$$\lim_{x \to \infty} f(x) = \infty$$

What do you think the notation

$$\lim_{x \to \infty} f(x) = -\infty$$

means?

What about the notation

$$\lim_{x \to -\infty} f(x) = \infty$$

Aside. *Are you taking MATH110 this term and not finding it particularly interesting or challenging? Instead of taking MATH116 next semester you can instead take MATH177.*

MATH177 is a version of Calculus II that approaches the topics using careful definitions rather than vague intuition.

---

6 Mathematical Induction Part I

Learning Incomes.

- *Comfort with notation formulas and quantifiers.*
- *Understand the reason behind writing down proofs.*

Learning Outcomes.

- *Understand the broad roadmap of a proof by induction*
- *Be convinced that proof by induction is a valid proof technique.*

Proof by Mathematical Induction is a topic that some of you may already be familiar with. Depending on how and where you may have first learned about it, justifying the technique (as opposed to using the technique) was probably not the main learning outcome. Regardless of your past experience with this technique, in this course understanding the technique is as important as being able to apply it.

Let $P(n)$ be a formula over $\mathbb{N}$. Recall the meaning of the notation

$$(\forall n \in \mathbb{N})\, P(n)$$

.
.
.
.
.
.
.
(It is in Module 5.4. If you are not clear on what this notation means, what follows in this module isn't going to make much sense.)

As opposed to statements of the form $(\exists n \in \mathbb{N})\, P(n)$, justifying the truth of a universally quantified statement seems like a lot more work – we cannot just provide examples of particular values of n for which $P(n)$ is true. Instead we must argue that $P(n)$ is true for each and every possible value of n. Proof by induction is a technique that lets us justify the truth of a universally quantified statement.

Remembering our reason for writing proofs, a proof by induction is a roadmap for your reader. It tells your reader how to prove $P(n)$ is true for any particular value of n they may care about. If, from what you have written, your reader can verify $P(n)$ is true for any particular value of n that they may care about, then necessarily $P(n)$ is true for every possible value of n.

Imagine your reader wanted to verify $P(7)$ was true for some formula $P(n)$ over $\mathbb{N}$. Instead of telling them directly how to prove $P(7)$ is true, you told them the following two facts:

(1) $P(0)$ is true; and

(2) for every $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

When $k = 6$, (2) says:

if $P(6)$ *is true, then* $P(7)$ *is true.*

Thus, for your reader to verify $P(7)$ is true is suffices for them to verify $P(6)$ is true and then apply (2) with $k = 6$.

Similarly, when $k = 5$, (2) says:

if $P(5)$ *is true, then* $P(6)$ *is true.*

Thus, for your reader to verify $P(6)$ is true it suffices for them to verify $P(5)$ is true and then apply (2) with $k = 5$. And so, for your reader to verify $P(7)$ is true, it suffices for them to verify $P(5)$ is true.

Continuing in this fashion, we can conclude for your reader to verify $P(7)$ is true, it suffices for them to verify $P(0)$ is true. Looking at statement (1), we have told our reader that $P(0)$ is true. And so by knowing (1) and (2) are true, the reader is certain $P(7)$ is true.

Statement (1) tells us that $P(0)$ is true. Statement (2) with $k = 0$ then tells us that $P(1)$ is true. Statement (2) with $k = 1$ then tells us that $P(2)$ is true. Continuing in this fashion, we should be convinced that when (1) and (2) hold, then $P(n)$ is true for any $n \in \mathbb{N}$.

Just as we have seen in various other topics in this course, learning about induction in this course requires us both to understand the abstract workings, as well as be practised with concrete examples. Most of our upcoming work on Assignment 4 will be devoted to these two aims.

At some point in this course, you may feel as if mathematical induction is *magic*. It will seem as if we are assuming our conclusion! When you have this feeling return to this introduction and read it again. We are not assuming our conclusion, instead we are assuming the hypothesis of (2). (This may not make sense now. But it will when you return to this introduction after you have worked with this technique for a little bit.)

Aside. *If you have studied programming techniques, mathematical induction may feel very similar to recursive algorithms. Proving correctness for a recursive algorithm usually requires a proof by induction. Further, inductive proofs often point the way towards recursive algorithms.*

In both of these techniques (induction and recursion) the actual proof or code can be quite short and succinct. For these tasks hard part usually isn't writing the proof or writing the code, it is figuring out what to do.

Fluent speakers of western English may recognize the adage:

If you give a someone a fish they will be hungry again tomorrow. If you teach them to catch a fish you feed them for a lifetime

Proof by induction is a *teach someone to fish* proof technique. Instead of telling your reader (or yourself!) how to verify $P(n)$ is true for a particular $n \in \mathbb{N}$. You are telling them how to verify $P(n)$ is true for any $n \in \mathbb{N}$ they may care about.

(Does anyone know if this adage exists in other languages? I would love to supplement these notes with a similar statement from other cultures.)

6.1 The Principle of Mathematical Induction

We begin with an example. Let n be a non-negative integer. Consider the following sum:

$$s(n) = \sum_{i=0}^{n} 2^i = 2^0 + 2^1 + 2^2 + \cdots + 2^n$$

When n is small it is easy to compute values of $s(n)$:

$$\begin{aligned} s(0) &= 2^0 = 1 \\ s(1) &= 2^0 + 2^1 = 3 \\ s(2) &= 2^0 + 2^1 + 2^2 = 7 \\ s(3) &= 2^0 + 2^1 + 2^2 + 2^3 = 15 \\ s(4) &= 2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 31 \end{aligned}$$

You may notice each of these values is one fewer than a power of 2.

$$\begin{aligned} s(0) &= 2^1 - 1 \\ s(1) &= 2^2 - 1 \\ s(2) &= 2^3 - 1 \\ s(3) &= 2^4 - 1 \\ s(4) &= 2^5 - 1 \end{aligned}$$

We wonder does this pattern hold in general. That is, does $s(n) = 2^{n+1} - 1$ for each non-negative integer n? Let us consider the case $n = 5$, but rather than compute directly, let us try a different approach:

$$s(5) = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5$$

Notice $2^0 + 2^1 + 2^2 + 2^3 + 2^4 = s(4)$. We have already confirmed $s(4) = 2^5 - 1$. Thus

$$s(5) = \left(2^0 + 2^1 + 2^2 + 2^3 + 2^4\right) + 2^5 = s(4) + 2^5 = \left(2^5 - 1\right) + 2^5$$

Simplifying, we notice $2^5 + 2^5 = 2(2^5) = 2^6$. Therefore $s(5) = 2^6 - 1$

Using this same technique, we can verify $s(6) = 2^7 - 1$ as

$$s(6) = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = s(5) + 2^6$$

Using $s(6) = 2^7 - 1$ we can use the same technique to verify $s(7) = 2^8 - 1$. We could continue on indefinitely. For any particular value of k, once we have verified that our formula holds for $s(k)$, we can then verify that our formula holds for $s(k + 1)$.

Let us think now about how we can express these ideas using our language of formal logic. Let $P(n)$ be the following formula over $\mathbb{N}$

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

For any particular value of $n \in \mathbb{N}$, this is a mathematical statement – it is either true for false. We have confirmed that each of $P(0), P(1), P(2), P(3), P(4)$ and $P(5)$ is true. In asking if the statement

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

holds for each integer $n \geq 0$, we are asking if $P(n)$ is true for each $n \geq 0$.

Think back a moment to the argument we made to verify that $P(5)$ is true. Consider the sum

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5$$

Since $P(4)$ is true, we have $2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 2^5 - 1$. Therefore

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 = \left(2^0 + 2^1 + 2^2 + 2^3 + 2^4\right) + 2^5 = (2^5 - 1) + 2^5 = 2^6 - 1.$$

In this argument there is nothing particular special about $n = 4$ and $n = 5$. Using this same argument, we can verify that if $P(k)$ is true for some $k \in \mathbb{N}$, then necessarily $P(k + 1)$ is true:

For some $k \in \mathbb{N}$, if we knew for certain that

$$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$$

then we could conclude:

$$\sum_{i=0}^{k+1} 2^i = \left(\sum_{i=0}^{k} 2^i\right) + 2^{k+1} = \left(2^{k+1} - 1\right) + 2^{k+1} = 2^{k+2} - 1$$

Thus if $P(k)$ is true for some $k \in \mathbb{N}$, then necessarily $P(k + 1)$ is true. Since $P(0)$ is true, this then should convince us that $P(n)$ is true for every $n \in \mathbb{N}$. That is, the statement $(\forall n \in \mathbb{N})\, P(n)$ is true

Let us consider another example and employ a similar technique. Recall that for a set X the set of all subsets of X is denoted as $\mathbf{2}^X$. We call $\mathbf{2}^X$ the power set of X. For example, when $X = \{x_1, x_2, x_3\}$ we have

$$\mathbf{2}^X = \{\{\}, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, \{x_1, x_2, x_3\}\}$$

Notice here that X has 3 elements and $\mathbf{2}^X$ has $2^3 = 8$ elements.

Consider now the empty set. We have $\mathbf{2}^{\{\}} = \{\{\}\}$. This set has a single element: the empty set. And so we notice the empty set has 0 elements and $\mathbf{2}^{\{\}}$ has $2^0 = 1$ elements.

Let $P(n)$ be the formula

There are 2^n subsets of a set n elements.

Above we have verified that $P(0)$ and $P(3)$ are true. Take a moment to convince yourself that $P(1)$ and $P(2)$ are both true.

Consider now the case $n = 4$. The two columns below list out all of the subsets of the set $X = \{x_1, x_2, x_3, x_4\}$.

$\{\}$	$\{x_4\}$
$\{x_1\}$	$\{x_1, x_4\}$
$\{x_2\}$	$\{x_2, x_4\}$
$\{x_3\}$	$\{x_3, x_4\}$
$\{x_1, x_2\}$	$\{x_1, x_2, x_4\}$
$\{x_1, x_3\}$	$\{x_1, x_3, x_4\}$
$\{x_2, x_3\}$	$\{x_2, x_3, x_4\}$
$\{x_1, x_2, x_3\}$	$\{x_1, x_2, x_3, x_4\}$

Notice that the eight sets on the left are exactly the subsets of the set $\{x_1, x_2, x_3\}$. The sets on the right are those same subsets but with the addition of the element x_4.

We see that the subsets of X can be partitioned into those that do not contain x_4 and those that do contain x_4. The subsets that do not contain x_4 are the subsets of $\{x_1, x_2, x_3\}$. For every subset of X that does not contain x_4, there is a corresponding subset of X that does contain x_4. Therefore the number of subsets of $\{x_1, x_2, x_3, x_4\}$ is exactly two times the number of subsets of $\{x_1, x_2, x_3\}$. Since there are 2^3 subsets of a set with three elements (we know this because $P(3)$ is true), there must be $2 \times 2^3 = 2^4$ subsets of a set with four elements. Therefore $P(4)$ is true.

This same argument can be used to show that there are 2^5 subsets of a set with five elements. We can write down all of the subsets of the set $\{x_1, x_2, x_3, x_4, x_5\}$ in two columns. The first of these columns are all of the subsets that do not contain x_5. The second of these columns are the subsets we get by adding x_5 to each subset in the first column. The first column is the set of subsets of the set $\{x_1, x_2, x_3, x_4\}$. Since $P(4)$ is true, this column has 2^4 subsets. Therefore there are $2 \times 2^4 = 2^5$ subsets of $\{x_1, x_2, x_3, x_4, x_5\}$. And so we see that $P(5)$ is true.

Using this same argument, we can verify that if a set with k elements has 2^k subsets, then necessarily a set with $k + 1$ elements has 2^{k+1} subsets.

We can write down all of the subsets of the set $\{x_1, x_2, \ldots, x_{k+1}\}$ in two columns. The first of these columns are all of the subsets that do not contain x_{k+1}. The second of these columns are the subsets we get by adding x_{k+1} to the subset to each subset in the first column. The first column is the set of subsets of the set $\{x_1, x_2, \ldots, x_k\}$. If $P(k)$ is true, this column has 2^k subsets. Therefore there are $2 \times 2^k = 2^{k+1}$ subsets of $\{x_1, x_2, \ldots, x_{k+1}\}$. And so we see that if $P(k)$ is true, then $P(k+1)$ is true.

That is to say, if $P(k)$ is true for some $k \in \mathbb{N}$, then necessarily $P(k+1)$ is true. Since $P(0)$ is true, this then should convince us that $P(n)$ is true for every $n \in \mathbb{N}$. That is, the statement $(\forall n \in \mathbb{N})\, P(n)$ is true

In both of our example above we justified the truth the universally quantified statement: $(\forall n \in \mathbb{N})\, P(n)$ by showing to be true the following two statements:

1. $P(0)$
2. for every $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$

This technique is so ubiquitous that this proof technique is its own theorem:

Theorem (The Principle of Mathematical Induction)**.** *Let $P(n)$ be a formula over $\mathbb{N}$. If the following two statements are true, then $P(n)$ is true for each integer $n \geq 0$.*

(1) $P(0)$; and

(2) for each $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true.

Though stated as a theorem, the Principle of Mathematical Induction is a proof technique. If we can show that the hypotheses of this theorem hold for some particular formula $P(n)$ over $\mathbb{N}$, then applying the theorem above tells us the statement $(\forall n \in \mathbb{N})\, P(n)$ is true.

Let us return to our first-example and use the Principle of Mathematical Induction to prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for each $n \in \mathbb{N}$.

Theorem 6.1. *For every $n \in \mathbb{N}$ we have $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$*

Proof. We proceed by induction on n. Let $P(n)$ the following formula over $\mathbb{N}$:

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

We show that both (1) and (2) hold in the hypothesis of the Principle of Mathematical Induction for $P(n)$.

(1) $P(0)$ is true:
$P(0)$ is the statement

$$2^0 = 2^1 - 1$$

Since $2^0 = 1$ and $2^1 - 1 = 1$, then $P(0)$ is true.

(2) for each $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true

Consider some integer $k \geq 0$ so that $P(k)$ is true. Since $P(k)$ is true, we know

$$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1.$$

Consider the statement $P(k+1)$:

$$\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$$

Notice

$$\sum_{i=0}^{k+1} 2^i = \left(\sum_{i=0}^{k} 2^i \right) + 2^{k+1}$$

Since $P(k)$ is true, we have

$$\sum_{i=0}^{k+1} 2^i = \left(2^{k+1} - 1\right) + 2^{k+1}$$

Therefore

$$\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$$

And so it follows that $P(k+1)$ is true.

Since both of the hypotheses in the the Principle of Mathematical Induction hold, necessarily the conclusion holds. That is, $P(n)$ is true for each integer $n \geq 0$. Therefore for every $n \in \mathbb{N}$ we have

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

□

We leave the proof of our second example to Assignment 4.

The statement of (2) is essential a mini-theorem in and of itself. In showing that (2) holds, we assume the hypothesis is true (i.e., we assume P(k) is true for some $k \in \mathbb{N}$) and we then show that the conclusion is true (i.e., $P(k+1)$ is true).

Aside. *If you have seen* `proof by induction` *before you may wonder why the phrases* `base case, induction hypothesis and induction step` *have not yet appeared. In standard use, the term* `base case` *refers to (1) in the statement of the Principle of Mathematical*

Induction. The term `induction hypothesis` *refers to the hypothesis of (2) in the statement of the Principle of Mathematical Induction. The term* `induction step` *refers to proving the conclusion of (2) in the statement of the Principle of Mathematical Induction.*

Using these terms is not wrong, not at all! If you are comfortable with these terms, then please continue to use them. I have avoided these terms because for students seeing these ideas for the first time, hiding (1) and (2) behind these terms sometimes makes proof by induction feel like magic. As we get more comfortable with induction we will come to realize that we need not even invoke the ideas of induction directly in our proofs. Just mentioning to our reader that we are proceeding by induction will be enough to communicate our general proof strategy.

In our use of the Principle of Mathematical Induction we are proving that some formula over $\mathbb{N}$ holds for every value of n. To verify $P(k+1)$ is true for some particular value of k, we use the hypothesis that $P(k)$ is true.

When $P(n)$ was the formula

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1,$$

we used the truth of $P(4)$ to verify that $P(5)$ was true. Even though $P(3), P(2), P(1)$ and $P(0)$ were also true, we did not directly invoke these facts in verifying that $P(5)$ was true. However the technique of proof by induction is flexible enough for formulas where we need to invoke the truth of many previous cases in order to determine the truth of the case we are considering. We consider this in the following section.

Test Your Understanding

1. Let $P(n)$ be the following formula over $\mathbb{N}$:

$$5 \text{ divides } 6^n - 1$$

We apply the Principle of Mathematical Induction to show $P(n)$ is true for all $n \in \mathbb{N}$

(a) Explain why $P(0)$ is true. (Be sure to refer to the definition of the word divides)

(b) For this formula, the hypothesis of (2) in the Principle of Mathematical Induction is

$$\text{for } k \in \mathbb{Z},\ 5 \text{ divides } 6^k - 1$$

State the conclusion of (2) for this formula.

(c) To show that the conclusion of (2) is true whenever the hypothesis of (2) is true, we must show that if 5 divides $6^k - 1$, then 5 divides $6^{k+1} - 1$. By manipulating equations, show $6^{k+1} - 1 = 5(6t + 1)$

(d) Using a template similar to the proof of Theorem 6.1, write a full proof of the following theorem:

Theorem. *For every* $n \in \mathbb{N}$ 5 *divides* $6^n - 1$

Test Your Understanding Solution

1. (a) When $n = 0$ we have $6^n - 1 = 0$. There exists an integer $t \in \mathbb{Z}$ so that $0t = 0$, therefore 0 divides $6^0 - 1$. Therefore $P(0)$ is true.

   (b) 5 divides $6^{k+1} - 1$

   (c)

$$\begin{aligned} 5(6t+1) &= 5\left(6\frac{6^k-1}{5}+1\right) \\ &= 5\left(6\frac{6^k-1}{5}+\frac{5}{5}\right) \\ &= 6\left(6^k-1\right)+5 \\ &= 6^{k+1}-6+5 \\ &= 6^{k+1}-1 \end{aligned}$$

   (d) There exists an integer so that 5 multiplied by that integer gives $6^{k+1} - 1$. Therefore 5 divides $6^{k+1} - 1$.

   (e) We proceed by induction on n.

   (1) P(0) is true
   Notice $6^0 - 1 = 0$. As 5 times 0 is 0 it follows that 5 divides $6^0 - 1$. Therefore $P(0)$ is true.

   (2) If $P(k)$ is true, then $P(k+1)$ is true
   If $P(k)$ is true for some $k \in \mathbb{N}$, then there exists an integer t so that $5t = 6^k - 1$.

   Notice

$$\begin{aligned} 5(6t+1) &= 5\left(6\frac{6^k-1}{5}+1\right) \\ &= 5\left(6\frac{6^k-1}{5}+\frac{5}{5}\right) \\ &= 6\left(6^k-1\right)+5 \\ &= 6^{k+1}-6+5 \\ &= 6^{k+1}-1 \end{aligned}$$

   Therefore 5 divides $6^{k+1} - 1$.

   Since both hypotheses in the statement of the Principle of Mathematical Induction hold for the formula $P(n)$, necessarily $P(n)$ is true for each $n \in \mathbb{N}$. In other words, $n \in \mathbb{N}$ 5 divides $6^n - 1$ for every $n \in \mathbb{N}$.

6.2 The Principle of Strong Mathematical Induction

Our modern base-ten place-value system of notation is incredibly useful. It is so engrained in us, that most of the time we don't even notice. Recall that the notation

$$1342$$

Refers to the number equal to

$$1 \times 10^4 + 3 \times 10^2 + 4 \times 10^1 + 2 \times 10^0$$

This system is based upon powers of 10 and uses the digits $0 - 9$. Such a system is likely based upon us humans having ten fingers.

Imagine what our number system would be like if we only had thumbs. We may have developed a place-value system based upon powers of 2 using digits 0 and 1. For example we would write:

$$1101$$

to refer to the number equal to

$$1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0.$$

We would express this number as 13 in our base-ten notation.

Is it clear that every number is either power of 2 or can be expressed as a sum of powers of 2?

Numbers on the left are in base ten. The equivalent representation in base two is on the right. The equals sign means that the two pieces of notation represent the same integer.

$$\begin{aligned} 0 &= 0 \\ 1 &= 1 \\ 2 &= 10 \\ 3 &= 11 \\ 4 &= 100 \\ 5 &= 101 \\ 6 &= 110 \end{aligned}$$

So far so good, now what about 7? Rather than continue with the pattern, let us try and be slightly clever. We notice that $7 = 4 + 3$. The integer 4 can be expressed as 100 in base two. The integer 3 can be expressed as 011 in base two. Thus

$$4 = 1 \times 2^2 + 0 \times 2^1 + 0 \times 2^0$$
$$3 = 1 \times 2^1 + 1 \times 2^0$$

Adding these together yields

$$7 = 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$$

Thus 7 can be expressed as 111 in base-two.

Marching on, let us think about 8. Since $8 = 2^3$, this isn't terribly interesting– 8 is a power of two.

$$7 = 111$$
$$8 = 1000$$

For 9 we can use the same strategy as for 7. We notice $9 = 8 + 1 = 2^3 + 2^0$ and so 9 can be expressed as 1001 in base-two.

We could continue on with this, but this may take a while. Let us assume we have been successful in expressing each integer up to, say, 24 as a power of 2 or as a sum of powers of 2. To express 25 as a sum of distinct powers of 2, we notice $25 = 16 + 9$. As we have assumed we have been successful in expressing each integer up to 24 as a power or 2 or sum of powers of 2, then we know that each of 16 and 9 can be expressed in this way: $16 = 2^4$ and $9 = 2^3 + 2^0$. Therefore 25 can be expressed as a sum of powers of 2.

Let us assume we have been successful in expressing each integer up to, say, k, as a power of 2 or as a sum of powers of 2. If the integer $k+1$ is a power of 2, then it can be expressed as a power of 2. Otherwise there is some largest integer ℓ so that ℓ is a power of 2 and $\ell < k+1$. Since each of ℓ and $k+1-\ell$ are less than $k+1$, as we worked our way up to $k+1$ we must have been able to express each of ℓ and $k+1-\ell$ as a power of 2 or as a sum of powers of 2. Adding together these sums gives us $k+1$ as a sum of powers of 2.

Let $P(n)$ be the following formula over $\mathbb{N}$

$$n \text{ is a power of 2 or can be expressed as a sum of powers of 2.}$$

In our work above we have verified the following information

1. $P(0)$ is true
2. For any $k \in \mathbb{N}$, if each of $P(0), P(1), \ldots, P(k)$ is true, then $P(k+1)$ is true.

When $k = 0$, (2) tells us that $P(1)$ is true. Now when $k = 1$, (2) tells us that $P(2)$ is true. Continuing in this manner, we should be convinced that $P(n)$ is true for each $n \in \mathbb{N}$.

To hone our intuition further, let us consider another example.

Recall that a prime number is an integer $n \geq 2$ so that the only positive divisors of n are 1 and itself. The study of prime numbers has some surprisingly important applications in the cryptography – the art of communicating in secret code. For example, most security systems for online commerce depend on some fundamental facts about prime numbers.

Any integer $n \geq 2$ that is not prime is called composite. Necessarily, for any composite integer n there exists a pair of integers a and b in the range $[2, n-1]$ so that $n = ab$. If each of a and b are composite, then again they can be expressed as the product of two integers. This process will stop when all of the factors we have found are prime.

For example, consider the integer 30. Since 30 even we have

$$30 = 2 \times 15$$

Since $15 = 3 \times 5$ we have

$$30 = 2 \times 3 \times 5$$

As each of 2, 3 and 5 is prime, we can continue this process no further. Notice that we have expressed the integer 30 a product of prime numbers.

For another example consider the integer 6136. This integer is divisible by 4 (this is not obvious) and so we find

$$6136 = 4 \times 1534$$

The integer 4 is composite. As is 1534. And so

$$6136 = 2 \times 2 \times 2 \times 767$$

Continuing this process we can find $767 = 13 \times 59$. And so

$$6136 = 2 \times 2 \times 2 \times 13 \times 59$$

Each of these integers $2, 13$ and 59 is prime. And so we have written 6136 as a product of prime numbers.

It seems reasonable that we could repeat this sort of process with any composite integer $n \geq 2$. In doing so we may be able to save ourselves some time by using factorizations we have already found.

Consider the integer $n = 184080$. With some calculator work we can find

$$184080 = 30 \times 6136$$

We have already expressed each of 30 and 6136 as a product of prime numbers. And so it follows that 184080 can be expressed as a product of prime numbers. Therefore

$$\begin{aligned} 184080 &= (2 \times 3 \times 5) \times (2 \times 2 \times 2 \times 13 \times 59) \\ &= 2^4 \times 3 \times 5 \times 13 \times 59 \end{aligned}$$

Let $P(n)$ be the following formula over $\mathbb{N}$

$$n + 2 \textit{ is prime or can be expressed as a product of prime numbers}$$

From our work above it seems reasonable that the statement $(\forall n \in \mathbb{N})\, P(n)$ is true. Certainly $P(0)$ is true. Let k be an integer. Imagine we have verified that each of $P(0), P(1), \ldots, P(k)$ is true. If the integer $k + 3$ is prime, then $P(k + 1)$ is true. Otherwise, $k + 3$ is composite and so there exists integers a and b in the range $[2, k + 2]$ so that $k + 3 = ab$. Since we have verified that each of $P(0), P(1), \ldots, P(k)$ is true, necessarily $P(a - 2)$ and $P(b - 2)$ are both true. Therefore each of a and b are either prime or can be expressed as a product of prime numbers. Therefore $k + 3$ can be expressed as a product of prime numbers. And so we see $P(k + 1)$ is true.

Since $P(0)$ is true, and whenever each of $P(1), P(2), \ldots P(k)$ is true it follows that $P(k+1)$ is true, then we should be convinced that $P(n)$ is true for each $n \in \mathbb{N}$.

Just as we did for the Principle of Mathematical Induction, we state this proof technique as a theorem.

Theorem (The Principle of Strong Mathematical Induction)**.** *Let $P(n)$ be a formula over $\mathbb{N}$. If the following two statements are true, then $P(n)$ is true for each integer $n \geq 0$.*

1. *$P(0)$; and*
2. *for each $k \geq 0$, if each of $P(0), P(1), \ldots, P(k)$ is true, then $P(k + 1)$ is true.*

The Principle of Strong Mathematical Induction is a proof technique. If we can show that the hypotheses hold for some particular formula $P(n)$ over $\mathbb{N}$, then applying the theorem above tells us the statement $(\forall n \in \mathbb{N})\, P(n)$ is true.

Let us return to our first example and use the Principle of Mathematical Induction to prove that every positive integer can be expressed as a sum of powers of 2.

Theorem 6.2. *Every natural number can be expressed as a sum of powers of 2.*

Proof. We proceed by induction on n. Let $P(n)$ the following formula over $\mathbb{N}$:

$$n \textit{ is a power of } 2 \textit{ or can be expressed as a sum of powers of } 2.$$

We show that both (1) and (2) hold in the hypothesis of the Principle of Strong Mathematical Induction.

(1) $P(0)$ is true:
$P(0)$ is the statement

$$0 \textit{ can be expressed as a sum of powers of } 2.$$

This statement is true as $2^0 = 1$. Therefore $P(0)$ is true.

(2) for each $k \geq 0$, if each of $P(0), P(1), \ldots, P(k)$ is true, then $P(k+1)$ is true.
Consider some integer $k \geq 0$ so that each of $P(0), P(1), \ldots P(k)$ is true. Therefore each integer in the range $[0, k]$ can be expressed as a sum of powers of 2.

We want to show that $P(k+1)$ is true. That is, we want to show that the integer $k+1$ can be expressed as a sum of powers of 2.

If $k+1$ is a power of two, then $k+1 = 2^t$ for some integer t. In this case, $P(k+1)$ is true.

Otherwise, assume $k+1$ is not a power of 2. Let $\ell = 2^t$ be the largest power of 2 that is smaller than $k+1$. Thus

$$k + 1 = \ell + r$$

where r is a positive integer less than 2^t. By hypothesis, $P(\ell)$ and $P(r)$ are both true. Therefore each of ℓ and r can be expressed as a sum of powers of 2. Adding these sums together gives a $k+1$ as a sum of powers of 2. Therefore, $P(k+1)$ is true.

Since both statements of the Theorem of Strong Mathematical Induction hold, necessarily the conclusion holds. Therefore $P(n)$ is true for each $n \geq 0$. In other words, the integer n can be represented in base two for every integer $n \geq 0$. □

Test Your Understanding

1. In talking about expressing each integer $n \geq 2$ as a product of prime numbers, why did we define $P(n)$ to be the formula

   $$n + 2 \textit{ is prime or can be expressed as a product of prime numbers}$$

   instead of

   $$n \textit{ is prime or can be expressed as a product of prime numbers}$$

2. What integer is represented as 10001 in base-2?

3. In second last paragraph of the proof of Theorem 6.4, how do we know $P(\ell)$ and $P(r)$ are both true?

Test Your Understanding Solution

1. In our work here we are talking about universally quantified formulas over $\mathbb{N}$. Since 0 and 1 are neither prime nor composite, the formula

   $$n \text{ is prime or can be expressed as a product of prime numbers}$$

   is not true for $n = 0$ and $n = 1$.

2. 10001 corresponds to the integer equal to

   $$1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 17$$

3. Each of ℓ and r are in the range $[1, k]$ as they are positive and less than $k + 1$. By hypothesis $P(k')$ is true for each $1 \leq k' \leq k$. Therefore $P(\ell)$ and $P(r)$ are both true.

6.3 Proving the Principle of Mathematical Induction

Recall the statement of the Principle of Mathematical Induction

Theorem (The Principle of Mathematical Induction)**.** *Let $P(n)$ be a formula over $\mathbb{N}$. If the following two statements are true, then $P(n)$ is true for each integer $n \geq 0$.*

(1) $P(0)$; and

(2) for each $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true

As this is a theorem there ought to be a proof that convinces us that it is true! As we have done for other proofs in this course, we will proceed by contradiction. That is, we will assume that the hypothesis of the theorem is true and the conclusion of the theorem is false. From this we will derive an absurdity. The absurdity we will find is a natural number ℓ so that $P(\ell)$ is both true and false. This then convinces us that if the hypothesis is true, then the conclusion must also be true.

In this theorem the hypothesis is:

The following two statements hold

(1) $P(0)$ is true; and

(2) for each $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true

and the conclusion is:

$$P(n) \text{ is true for each integer } n \geq 0.$$

If the conclusion is false, then there must be at least one value of n for which $P(n)$ is false. Let F be the set of such values. That is,

$$F = \{t \mid P(t) \text{ is false } \}$$

Since the conclusion is false, necessarily $F \neq \{\}$. Of all of the elements of F, let us use the label ℓ to refer to the smallest. Is it possible that $\ell = 0$? (Take a moment to think about this before you go on).

.
.
.
.
.

As we assumed our hypothesis to be true, it must be that $P(0)$ is true. Therefore $0 \notin F$ and so $\ell \neq 0$.

To find our contradiction let us consider the number $\ell - 1$. Since $\ell \geq 1$, necessarily $\ell - 1 \geq 0$. What can we say about the truth value of $P(\ell - 1)$? (Take a moment to think about this before you go on. How did we choose ℓ?).

.
.
.
.
.
.

Recall that ℓ is the smallest element of F. That is, it is the smallest natural number so that $P(\ell)$ is false. Since $\ell - 1 < \ell$, necessarily $P(\ell - 1)$ is true.

Let us return now to thinking about the hypothesis. We have assumed true the statement

$$\textit{for each } k \geq 0\textit{, if } P(k) \textit{ is true, then } P(k+1) \textit{ is true.}$$

When $k = \ell - 1$ this statement is:

$$\textit{if } P(\ell - 1) \textit{ is true, then } P(\ell) \textit{ is true.}$$

We have just shown that $P(\ell - 1)$ is true. Therefore $P(\ell)$ is true. This statement contradicts the fact that $P(\ell)$ is false. Since $P(\ell)$ cannot be both true and false, then ℓ does not exist! That is to say, there is no smallest natural number in the set F. Therefore $F = \{\}$. Since F is empty, it must be that $P(n)$ is true for every $n \in \mathbb{N}$. This last statement

$$P(n) \textit{ is true for every } n \in \mathbb{N}$$

is exactly the conclusion of our theorem!

Let us write this all down succinctly as a proof of the Principle of Mathematical Induction.

Proof. We proceed by contradiction. Let $P(n)$ be a formula over $\mathbb{N}$ so that the statement $(\forall n \in \mathbb{N})\, P(n)$ is false, but the following two statements are true:

(1) $P(0)$

(2) for each $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true

Let $F = \{t \mid P(t) \text{ is false }\}$. By (1), we have $0 \notin F$. Let ℓ be the smallest element of F. By our choice of ℓ we have $\ell - 1 \notin F$. Therefore $P(\ell - 1)$ is true. By (2) it follows that $P(\ell)$

is true. This is a contradiction as ℓ was chosen so that $P(\ell)$ is false. Therefore $F = \{\}$ and so the statement $(\forall n \in \mathbb{N})\, P(n)$ is true. □

Aside. *Our proof of the Principle of Mathematical Induction turns on the following sentence:*

Let ℓ be the smallest element of F

In our proof, F is a non-empty subset of $\mathbb{N}$. With this sentence we are asserting the existence of some smallest element. If we think of the elements of $\mathbb{N}$ as being ordered according to the total order R_1 in Module 3, are we always certain that such a smallest element exists?

At the lowest level, abstract mathematics depends on a list of axioms, statements that we assume to be true. Most of the time we don't ever think about the axioms that underpin our work as they are so common-sense that they seem to not require proof. (In fact, this it likely the first time you have learned about the existence of mathematical axioms!)

The `well-ordering principle` *is the axiom that let's us assert the existence of the smallest element of F. Assuming that the well-ordering principle holds allows us to prove the statement of the Principle of Mathematical Induction.*

The respective wikipedia pages on the `Peano Axioms`*, the* `well-ordering principle`*, and* `Euclidean geometry` *provide more information on these sorts of things should be you interested.*

Test Your Understanding

1. The second last sentence of this proof is

   This is a contradiction as ℓ was chosen so that $P(\ell)$ is false

   How does our choice of ℓ tell us ℓ is false?

2. Why does knowing $F = \{\}$ tell us that the statement $(\forall n \in \mathbb{N})\, P(n)$ is true?

3. Near the start of the proof we state

   By our choice of ℓ , we have $\ell - 1 \notin F$

   How does our choice of ℓ tell us $\ell - 1 \notin F$?

Test Your Understanding Solution

1. We chose ℓ so that ℓ was the smallest integer so that $P(\ell)$ is false.
2. The set F is the set of all natural numbers t so that $P(t)$ is false. If $F = \{\}$, then $P(n)$ must be true for each $n \in \mathbb{N}$. Therefore the statement $(\forall n \in \mathbb{N})\, P(n)$ is true.
3. We chose ℓ so that ℓ was the smallest integer so that $P(\ell)$ is false. Since (1) is true, $\ell \neq 0$. Therefore $\ell - 1 \in \mathbb{N}$. Since $\ell - 1 < \ell$ and ℓ is the smallest integer so that $P(\ell)$ is false, we know $P(\ell - 1)$ is true. The set F is the set of all natural numbers t so that $P(t)$ is false. Since $P(\ell - 1)$ is false we know $\ell - 1 \notin F$

---

7 Mathematical Induction Part II

Learning Incomes.

- *Understand the broad roadmap of a proof by induction*
- *Be convinced that proof by induction is a valid proof technique.*

Learning Outcomes.

- *Be able to recognize when an attempted proof by induction provides a full roadmap to showing $P(n)$ is true for all $n \in \mathbb{N}$.*
- *Be able to adapt the method of proof by induction for formulas that are true over some domain $\{a, a+1, \dots\}$ with $a \in \mathbb{Z}$.*

Learning Outcomes.

In Module 7 we continue our work with the technique of mathematical induction for proving universally quantified statements over $\mathbb{N}$.

We begin with an example to further solidify our intuition for mathematical induction, we then look at examples that seem like mathematical induction should yield a valid proof, but we are unable to directly apply our theorems from Module 6.

Consider a natural number n and the remainder when 2^n is divided by 3. The only possible remainders when a number is divided by 3 are $0, 1$ or 2. For a natural number n, the integer 2^n may be very large even when n is relatively small. For example even though 1000 is a fairly pedestrian number, the number 2^{1000} is an absurdly big number – it is more than the number of atoms in the universe. Despite the fact that 2^{1000} is absurdly big, we will find it possible to compute its remainder when divided by 3.

Let us start with some small values of n to see if we can divine some sort of pattern:

n	2^n	Remainder after dividing by 3
0	1	1
1	2	2
2	4	1
3	8	2
4	16	1
5	32	2

The rightmost column here is very suggestive! It seems as if 2^n has remainder 1 when n is even and has remainder 2 when n is odd. If this pattern holds, then 2^{1000} would have

remainder 1 when divided by 3.

Let us see if we can use a proof by induction to prove our conjecture.

Aside. *A conjecture is a guess at something that might be true. Once we have a proof for our conjecture it becomes a theorem. Here our conjecture is*

$$2^n \textit{ has remainder } 1 \textit{ when } n \textit{ is even and has remainder } 2 \textit{ when } n \textit{ is odd.}$$

As we have done in previous work on induction, let us build some intuition by trying to find the remainder when 2^6 is divided by 3 without actually computing 2^6 and performing division. Our key observation will be

$$2^6 = 2 \times 2^5 = 2^5 + 2^5$$

We have

$$\begin{aligned} 2^6 &= 2^5 + 2^5 \\ &= (3(10) + 2) + (3(10) + 2) \\ &= 3(10 + 10 + 1) + 1 \\ &= 3(21) + 1 \end{aligned}$$

And so we see that 2^6 has remainder 1 when dividing by 3. (The quotient is 21.) As we only needed to know the remainder for 2^5 it seems as if we will be proceeding using the Principle of Mathematical Induction.

Let us think now about the work we will do in (2) for the Principle of Mathematical Induction. As with 2^6 our key observation is $2^{k+1} = 2^k + 2^k$.

When $k+1$ is even, necessarily k is odd. And so 2^k will have remainder 1 when dividing by 3. That is, there exists an integer q so that $2^k = 3q + 1$. Therefore

$$2^{k+1} = (3q + 1) + (3q + 1) = 3(2q) + 2$$

And so we see 2^{k+1} has remainder 2 when divided by 3.

When $k+1$ is odd, necessarily, k is even. And so 2^k will have remainder 2 when dividing by 3. That is, there exists an integer q so that $2^k = 3q + 2$. Therefore

$$2^{k+1} = (3q + 2) + (3q + 2) = 3(2q + 1) + 1$$

And so we see 2^{k+1} has remainder 1 when divided by 3.

Thus for any $k \geq 0$, if our conjecture is true when $n = k$, then our conjecture is true when $n = k + 1$. Since our conjecture

(1) is true when $n = 0$; and

(2) if our conjecture is true for $n = k$, then it is true for $n = k + 1$,

then the Principle of Mathematical Induction tells is that our conjecture is true for every $n \in \mathbb{N}$.

We write down a full proof of the theorem:

Theorem 7.1. *Let n be a natural number. When n is even, the remainder when 2^n is divided by 3 is 1. When n is odd, the remainder when 2^n is divided by 3 is 2*

Proof. We proceed by induction on n. We notice that 0 is even, we have $2^0 = 1$ and 1 has remainder 1 when divided by 3. And so the claim holds when $n = 0$.

Consider now $n = k + 1$. When $k + 1$ is even, necessarily k is odd. By induction, 2^k will have remainder 1 when dividing by 3. That is, there exists an integer q so that $2^k = 3q + 1$. Therefore

$$2^{k+1} = (3q + 1) + (3q + 1) = 3(2q) + 2$$

And so we see 2^{k+1} has remainder 2 when divided by 3.

When $k + 1$ is odd, necessarily k is even. By induction, 2^k will have remainder 2 when dividing by 3. That is, there exists an integer q so that $2^k = 3q + 2$. Therefore

$$2^{k+1} = (3q + 2) + (3q + 2) = 3(2q + 1) + 1$$

And so we see 2^{k+1} has remainder 1 when divided by 3.

Therefore the claim holds when $n = k + 1$ provided that it holds for $n = k$. The result now follows by induction. □

Aside. *Notice how much shorter the proof is than all of the work that went in to figuring out how the proof should go! This is very common in all proofs in mathematics. In textbooks and in mathematics research, it is common for authors to hide all the scaffolding and only show the reader the finished product (i.e., the proof.).*

From a teaching and learning point of view, this is less than ideal. You are able to read this proof more easily because of the work that is presented above. If you had just been handed the proof it would be much more difficult to figure out what was going on.

7.1 Fibonacci Numbers

The Fibonacci Numbers is the sequence of natural numbers that starts with 0 and 1 and proceeds so that each subsequent number is the sum of the previous two:

$$0, 1, 1, 2, 3, 5, 8, 13, 21 \ldots$$

Aside. *This sequence of numbers is named after an 12th Century Italian mathematician. Fibonacci studied these numbers as a pretence to solving a rather unrealistic applied problem of counting the number of rabbits after a fixed number of generations of breeding. Beyond the Fibonacci numbers, Fibonacci is best known for creating a mathematics textbook named* Liber Abaci.

Though this sequence of numbers is named for Fibonacci, he is far from the first to have studied them. References to this sequence appear as far back as India in 200 BCE. At this time, these numbers were being examined by an Indian author named Pingala. He used these numbers to count the number of fixed-length music patterns that could be made using short and long syllables. Pingala's work on short and long syllable sequences can be seen as an early form of binary notation.

Despite the fact that Pingala was studying these numbers more than 1000 years before Fibonacci was born, in the "grand" tradition of western mathematics, we have canonized Fibonacci in the literature and left the contributions of non-European mathematicians in the margins.

Though we generally view the Fibonacci numbers as a sequence, in fact they are a function in disguise!

Let $F : \mathbb{N} \to \mathbb{N}$ so that $F(0) = 0, F(1) = 1$ and $F(n) = F(n-1) + F(n-2)$ for all $n \geq 2$.

For example,

- $F(2) = F(1) + F(0) = 1 + 0 = 1$
- $F(3) = F(2) + F(1) = 1 + 1 = 2$
- $F(4) = F(3) + F(2) = 2 + 1 = 3$
- $F(5) = F(4) + F(3) = 3 + 2 = 5$

The Fibonacci numbers are *recursive*, the value of the next number in the sequence depends on the previous values in the sequence. For example, to compute $F(100)$ we would need to compute $F(99)$ and $F(98)$. Doing so would require us first compute $F(97)$ and $F(96)$. Continuing on we notice that to compute $F(100)$ we would need to first compute $F(t)$ for every $t \in \{0, 1, 2 \ldots, 99\}$. This seems dreadfully inefficient.

Aside. *If you are approaching this course with an eye towards computer science, you might had an assignment question writing recursive code for computing Fibonacci numbers. Given*

how difficult that task may have been, you may be dismayed at what follows; we examine a formula that computes these values directly! From a memory management point-of-view a direct computation is far better than a recursive procedure as we don't need to worry about the size of the stack in our recursion.

However, all is not lost! Though we don't have the tools to derive an explicit formula for $F(100)$ we do have the tools to prove that one is correct. If you look at the wikipedia page for the Fibonacci Numbers you will see the formula

$$F(n) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

For example, using this formula and a calculator we find

$$F(8) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^8 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^8 = 21$$

Aside. *If you have taken a course in Linear Algebra, you have probably encountered eigenvalues. In fact, one can use eigenvalues to derive this formula. If you are taking MATH266 next term, we'll spend some of our time talking about Linear Algebra for sequences of integers. Fibonacci-like sequences will figure heavily.*

There are lots of mathematical facts that I found astounding. This one is in the top ten. That the above formula returns an integer for when the input n is a positive integer seems very unexpected. Look at all of those irrational square roots!

In thinking about how we can show that this formula is correct for every $n \in \mathbb{N}$ we recall that $F(n)$ depends on the values of $F(n-1)$ and $F(n-2)$. If the formula is correct for $F(n-1)$ and $F(n-2)$, then perhaps we can use algebraic manipulations to show that the formula is correct for $F(n)$. This line of thinking should point us towards induction – we want to prove a universally quantified statement by providing a roadmap for the statement to be verified for any particular value of n that we care about.

Theorem 7.2. *For $n \in \mathbb{N}$, let $F(n)$ denote the nth Fibonacci number. We have*

$$F(n) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Since the value of $F(n)$ may depend on more than one previous case, we proceed using the Principle of Strong Mathematical Induction.

Let $P(n)$ be the formula

$$F(n) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

(1) We find

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^0 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^0 &= \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}} \\ &= 0 \\ &= F(0)\end{aligned}$$

And so we see $P(0)$ is true.

(2) Let $k \geq 0$ be an integer so that each of $P(0), P(1), \ldots, P(k)$ is true. To show $P(k+1)$ is true we must show

$$F(k+1) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

By definition $F(k+1) = F(k) + F(k-1)$ for all $k+1 \geq 2$. Since each of $P(k)$ and $P(k-1)$ are true we have

$$\begin{aligned}F(k+1) &= F(k) + F(k-1) \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\end{aligned}$$

Aside. *The algebraic manipulations below aren't the point of this discussion. At this point, don't spend much time trying to figure out how one line follows from the next. The important part is the equality following the word therefore. The algebraic manipulations are only included to forestall the expected question of* how did you get that?

Grouping and factoring, we find

$$\begin{aligned}F(k+1) &= F(k) + F(k-1) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\right) - \frac{1}{\sqrt{5}}\left(\left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right)\end{aligned}$$

Notice

$$\begin{aligned}
\left(\frac{1+\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} &= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{-1} + \left(\frac{1+\sqrt{5}}{2}\right)^{-2}\right) \\
&= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\frac{2}{1+\sqrt{5}} + \frac{4}{\left(1+\sqrt{5}\right)^2}\right) \\
&= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\frac{2+2\sqrt{5}}{\left(1+\sqrt{5}\right)^2} + \frac{4}{\left(1+\sqrt{5}\right)^2}\right) \\
&= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\frac{6+2\sqrt{5}}{6+2\sqrt{5}}\right) \\
&= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}
\end{aligned}$$

Similarly

$$\left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1} = \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

Therefore

$$F(k+1) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

And so if each of $P(0), P(1), \ldots, P(k)$ is true, then $P(k+1)$ is true.

From this work, are we convinced that our theorem is true? Remembering our explanation for *why* induction works, our two steps in a proof by induction provide for us a roadmap to verify that $P(n)$ is true for any particular value of n that we care about. From this work, are you convinced, say, $P(5)$ is true?

.
.
.
.
.
.
.
.
.
.
.
.

.

By (2), we see that we can confirm that $P(5)$ is true provided we can confirm $P(4)$ and $P(3)$ are true. Similarly, to confirm that $P(4)$ and $P(3)$ are true, (2) tells us that we need only confirm that $P(1)$ and $P(2)$ are true. To confirm $P(2)$ is true we need only confirm that $P(0)$ and $P(1)$ are true. We confirmed $P(0)$ is true in (1). But where did we confirm $P(1)$ is true?

Recall our definition of the Fibonacci numbers:

Let $F : \mathbb{N} \to \mathbb{N}$ so that $F(0) = 0, F(1) = 1$ and $F(n) = F(n-1) + F(n-2)$ for all $n \geq 2$.

Our work in using $F(k+1) = F(k) + F(k-1)$ is only valid when $k + 1 \geq 2$. In particular, this work is meaningless when $k + 1 = 1$. That is, it is not helpful for verifying $P(1)$ is true.

(1) confirms that $P(0)$ is true. And (2) confirms that $P(k+1)$ is true for $k \geq 1$ whenever each of $P(0), P(1), P(2), \ldots, P(k)$ is true. Since we have not shown anywhere that $P(1)$ is true, we have not provided to our reader (and ourselves!) a complete roadmap that lets us verify $P(n)$ is true for every $n \in \mathbb{N}$. Our work is insufficient to even verify $P(2)$ is true! This problem is remedied by separately verifying $P(1)$ is true.

Notice

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^1 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^1 &= \frac{1+\sqrt{5}}{2\sqrt{5}} - \frac{1-\sqrt{5}}{2\sqrt{5}} \\ &= 1 \\ &= F(1)\end{aligned}$$

Let us collect this all into a proof of our theorem:

Condensed proof of Theorem 7.2. We proceed by strong induction on n. We notice

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^0 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^0 &= \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}} \\ &= 0 \\ &= F(0)\end{aligned}$$

and

$$\begin{aligned}\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^1 - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^1 &= \frac{1+\sqrt{5}}{2\sqrt{5}} - \frac{1-\sqrt{5}}{2\sqrt{5}} \\ &= 1 \\ &= F(1)\end{aligned}$$

Consider now the case $n = k+1$ with $k+1 \geq 2$. By induction we have

$$\begin{aligned}F(k+1) &= F(k) + F(k-1) \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\end{aligned}$$

Rearranging and factoring yields

$$\begin{aligned}F(k+1) &= F(k) + F(k-1) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\right) - \frac{1}{\sqrt{5}}\left(\left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right)\end{aligned}$$

Aside. *Again, the algebraic manipulations here are not particularly the point of this exercise.*

Notice

$$\begin{aligned}\left(\frac{1+\sqrt{5}}{2}\right)^k + \left(\frac{1+\sqrt{5}}{2}\right)^{k-1} &= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{-1} + \left(\frac{1+\sqrt{5}}{2}\right)^{-2}\right)\\ &= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\frac{2}{1+\sqrt{5}} + \frac{4}{\left(1+\sqrt{5}\right)^2}\right)\\ &= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\frac{2+2\sqrt{5}}{\left(1+\sqrt{5}\right)^2} + \frac{4}{\left(1+\sqrt{5}\right)^2}\right)\\ &= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\left(\frac{6+2\sqrt{5}}{6+2\sqrt{5}}\right)\\ &= \left(\frac{1+\sqrt{5}}{2}\right)^{k+1}\end{aligned}$$

Similarly

$$\left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1} = \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

Therefore

$$F(k+1) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

The result now follows from the Principle of Strong Mathematical Induction. □

This sort of situation arises often when we proceed using strong induction. When our rote steps for a proof by strong induction don't provide us with a roadmap to verify $P(n)$ is true for every $n \in \mathbb{N}$ we may need to verify some specific cases separately.

Aside. *If you have seen proof by induction before or have been looking at other resources, you may recognize that in this section we have been thinking about* multiple base cases. *Thinking about this work in this way isn't wrong at all, but it does separate us from the statement of the statement of the principle of (strong) mathematical induction. In fact, when we deal with* multiple base cases *we are dealing with separate cases in (2). For some small values of $k+1$ it may not matter that each of $P(0), P(1), \ldots, P(k)$ are true when we show $P(k+1)$ is true. Nevertheless we are still showing the statement $\bigwedge_{t=0}^{k} P(t) \Rightarrow P(k+1)$ is true.*

(We haven't formally (or formerly!) defined the notation $\bigwedge_{t=0}^{k} P(t)$. Can you figure out what it ought to mean in the context of formal logic based on how we defined the notation $\bigcup$ when we talked about partitions?)

Test Your Understanding

1. The condensed proof of Theorem 7.2 proceeds by strong induction without being explicit about the two steps in constructing a proof by induction. Which of the statements directly uses the assumption that each of $P(0), P(1), ...P(k)$ are true:

   (a)

   $$\begin{aligned} F(k+1) &= F(k) + F(k-1) \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1} \end{aligned}$$

   (b)

   $$\left(\frac{1-\sqrt{5}}{2}\right)^k + \left(\frac{1-\sqrt{5}}{2}\right)^{k-1} = \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

   (c)

   $$F(k+1) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}$$

2. Show $F(n) \leq 2^n$ for all $n \in \mathbb{N}$

Test Your Understanding Solution

1. The answer is a. Recall $P(n)$ is the formula

$$F(n) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

Therefore $P(k-1)$ and $P(k)$ are respectively the statements

$$F(k-1) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}$$

$$F(k) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k}$$

And so in writing

$$\begin{aligned} F(k+1) &= F(k) + F(k-1) \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1} \end{aligned}$$

we are directly invoking the fact that each of $P(k)$ and $P(k-1)$ is true.

2. We show $F(n) \leq 2^n$ for all $n \in \mathbb{N}$.

We proceed by strong induction on n. We begin by noting $F(0) = 0$, $F(1) = 1$, $2^0 = 1$ and $2^1 = 2$. Thus the claim holds when $n = 0$ and $n = 1$.

Consider now the case $n = k+1$ for $k+1 \geq 2$. By definition we have $F(k+1) = F(k) + F(k-1)$. By hypothesis we have $F(k) \leq 2^k$ and $F(k-1) \leq 2^{k-1}$. Therefore

$$F(k+1) \leq 2^k + 2^{k-1} \leq 2^k + 2^k = 2^{k+1}$$

The result now follows by strong induction.

7.2 What if the formula isn't true for some small values of n, but is true for all larger values of n? – The Offset Problem

We continue with another example. Consider the inequality

$$2^n > 2n + 1$$

In the past you likely learned how to *solve* such inequalities. In that context, *solve* usually means *find all values of n so that this inequality holds*. Let us restrict our attention to natural numbers and make a table of observations for when this inequality holds.

n	2^n	$2n+1$	$2^n > 2n+1$?
0	$2^0 = 1$	$2(0)+1 = 1$	$False$
1	2	3	$False$
2	4	5	$False$
3	8	7	$True$
4	16	9	$True$
5	32	11	$True$
6	64	13	$True$
7	128	15	$True$

From our observations it seems as if $2^n > 2n + 1$ for all $n \geq 3$. In thinking about a proof by induction of this statement, we wonder if we can prove $2^8 > 2(8) + 1$ without having to actually do any computations.

Notice $2(8) + 1 = 2(7) + 1 + 2$. Since $2^7 > 2(7) + 1$ we have

$$2(8) + 1 = (2(7) + 1) + 8 < 2^7 + 2$$

And since $2^8 = 2^7 + 2^7$, necessarily $2^8 > 2^7 + 2$. Therefore

$$2(8) + 1 < 2^7 + 2 < 2^7 + 2^7 = 2^8$$

And so $2^8 > 2(8) + 1$.

Thinking about k and $k+1$ rather than 7 and 8 may suggest to us that we can proceed using induction. Let us take a quick moment to recall the Principle of Mathematical Induction.

Theorem (The Principle of Mathematical Induction)**.** *Let $P(n)$ be a formula over $\mathbb{N}$. If the following two statements are true, then $P(n)$ is true for each integer $n \geq 0$.*

(1) $P(0)$; and

(2) for each $k \geq 0$, if $P(k)$ is true, then $P(k+1)$ is true.

If $P(n)$ is the formula

$$2^n > 2n + 1$$

then we cannot directly use the Principle of Mathematical Induction to prove $P(n)$ is true for all $n \geq 3$. The Principle of Mathematical Induction only lets us prove that a formula is true for all $n \in \mathbb{N}$. Instead then, let us consider the formula $Q(n)$

$$2^{n+3} > 2(n + 3) + 1$$

Now we see that $Q(0)$ is true, and from our work above we expect $Q(n)$ to be true for all $n \in \mathbb{N}$. We can now directly apply the Principle of Mathematical Induction to show $2^n > 2n + 1$ for all $n \geq 3$.

In this example we had to be a little sneaky in defining our formula so our was true for every $n \in \mathbb{N}$. We dealt in this same manner of sneakiness when we looked at writing integers $n \geq 2$ as a product of prime numbers. Instead of worrying about such sneakiness each time we encounter this offset problem, instead we can modify our statement of the The Principle of Mathematical Induction.

Theorem 7.3. *Let $Q(n)$ be a formula and let a be an integer. If the following two statements are true, then $Q(n)$ is true for each integer $n \geq a$.*

(1) $Q(a)$; and

(2) for each $k \geq a$, if $Q(k)$ is true, then $Q(k + 1)$ is true.

As this is a theorem, we ought to be able to prove that this theorem is true. We can do this using the Principle of Mathematical Induction. We return to this later in the course.

Instead we return to our example above and provide a proof using Theorem 7.3

Theorem 7.4. *For all integers $n \geq 3$ we have $2^n > 2n + 1$*

Proof. We proceed by induction on n, beginning with $n = 3$. When $n = 3$ we have $2^3 = 8$ and $2(3) + 1 = 7$ and so we confirm $2^n > 2n + 1$ when $n = 3$.

Consider now $n = k + 1$ with $k + 1 \geq 4$. Notice $2(k + 1) + 1 = (2k + 1) + 2$. Since $k \geq 3$ we have $2^{k+1} > 2^k + 2$. By induction we have $2^k > 2k + 1$. And so

$$2(k + 1) + 1 = (2k + 1) + 2 < 2^k + 2 < 2^{k+1}$$

Therefore the claim holds when $n = k + 1$ provided that it holds for $n = k$. The result now follows by induction. □

This proof doesn't directly invoke $Q(n)$, nor does it directly invoke the statement of the theorem above. This is okay! Remember, a proof by induction is a roadmap. The work presented in this proof is enough to be able to verify $2^n > 2n + 1$ for every $n \geq 3$.

Aside. *We worked awfully hard for such a short proof! Hard work in mathematics is often measured by number of words we end up writing down in our proofs. The* thinking *is the hard work. The proof is the outcome of the hard work, not the work itself.*

Test Your Understanding

The proof of Theorem 7.4 proceeds by implicitly applying Theorem 7.3.

1. What is $Q(n)$ in the proof of. Theorem 7.3 when we use this theorem in our proof of Theorem 7.4
2. In applying the statement of Theorem 7.3 to prove Theorem 7.4, what value does a take?

Test Your Understanding Solution

1. $Q(n)$ is the formula $2^n > 2n + 1$.
2. Since we want to show $Q(n)$ is true for all $n \geq 4$, we need $a = 4$ in the statement of Theorem 7.3.

7.3 Common Questions About Induction

- How do I know when to use induction for a proof?

  Induction is a proof technique for universally quantified statements. In these statements the thing we want to prove is parametrized by integers. Induction is a useful technique when we can notice that the truth for one value follows from the truth of previous values. Unfortunately there is no way to know a priori that this is the case. Knowing when *to use induction comes with experience. For the remainder of this course you will be told when to approach a proof via induction.*

- How do I show that the conclusion of (2) in the Principle of Mathematical Induction is true?

  As you have seen from the examples in Module 6 and 7, proof by induction is a template for a proof rather than being a proof itself. The work we do in showing that (1) and (2) hold depend on what $P(n)$ actually is. You can be assured, however, that when you are asked to use induction in this class you will be not be left adrift. Such questions will either be similar to something in the notes, or they will come with hints.

- When do I use strong induction versus regular induction?

  If showing $P(k+1)$ is true only requires you to know $P(k)$ is true, then you are using induction. Otherwise you are using strong induction. By and large, you can always imagine proceeding using strong induction. If it turns out that you don't need to know that any cases other than the previous case are true, your proof will (probably) still be valid.

- Induction feels like magic, when we assume $P(k)$ is true it seems as if we are assuming our conclusion is true. Why is this okay?

  Go back and read Section 6.0. There is a particular paragraph there that speaks to this confusion.

- I have learned about induction before/ I watched some youtube videos about induction. What do `base case`, `induction hypotheis` and `induction step` mean?

  When induction is introduced without first looking at formal logic, one cannot easily state the Principle of Mathematical Induction. In these pedagogical paradigms, the term `base case` *refers to showing that (1) holds in the Principle of Mathematical Induction. The term* `induction hypothesis` *refers to the hypothesis of (2) in the Principle of Mathematical Induction. The term* `induction step` *refers the showing that the conclusion of (2) in the Principle of Mathematical Induction is true.*

  Most of the places where these terms are introduced have as the primary learning outcome that students be able to construct induction proofs that depend on their ability to manipulate algebraic equations. Our goal in this course is broader. Rather than just reaching for a mechanical understanding of induction as a proof technique, we are

also aiming for deeper understanding of why induction is a valid proof technique. This will allow us to not be distracted by the validity of induction when it is used in more abstract settings.

Feel free to use these terms in your proofs.

- I have learned about induction before/ I watched some youtube videos about induction. Why are we thinking about the case $n = 0$ in (1)? Other resources start with $n = 1$.

  We introduced proof by induction as a technique for verifying the truth of universally quantified statements over $\mathbb{N}$. *In Module 1 we made a few short comments about having* $0 \in \mathbb{N}$. *We could not include* 0 *from* $\mathbb{N}$ *and continue our work exactly as before, except in (1) we would consider* $P(1)$ *as the first case.*

  Look back at the example of counting the number of subsets of a set with n *elements.* $P(n)$ *was the statement*

  $$A \text{ set with } n \text{ elements has } 2^n \text{ subsets.}$$

  This statement is certainly true when $n = 0$. *If we wanted to start our induction at* $n = 1$, *to capture the case when our set is empty, we would need our formula to be*

  $$A \text{ set with } n - 1 \text{ elements has } 2^{n-1} \text{ subsets.}$$

  This would be perfectly fine.

- When will I ever use this/ why do I need to know this?

  If you are planning on or required to take mathematics courses beyond the 100 and 200 level, significant time will be spent on justifying why certain mathematical facts are true. Learning about induction in examples that are not conceptually deep will make it so when induction is used for abstract mathematics, you will not be focussed on understanding why induction works.

  If you are looking for justification on why you must learn about abstract mathematics if you are not planning on being a mathematician, then I can offer little more than a shrug of my shoulders and a comment that rarely does one question the value of studying literature or history at the university level. We don't study these things so that we may directly apply them in the workplace (universities are not merely vocational colleges, even for students in vocational programs like engineering or education), we study them so that we may become more culturally literate humans.

- Okay, now you are just opining from your pulpit about the cultural value of learning mathematics.

  That's... not a question.

---

8 An Introduction to Graph Theory

Learning Incomes.

- *Recall the meaning of a graph from Module 3*
- *Be fluent with set notation*
- *Understand the technique of proof by induction.*

Learning Outcomes.

- *Understand two different representations of a graph (sets and picture) and be able to convert between them.*
- *Be fluent in graph theoretic terminology*
- *Be able to explain why a tree has at least two vertices of degree* 1.
- *Be able to explain why a tree with n vertices has $n-1$ edges*
- *Be able to find a k-colouring of a graph for some fixed integer k.*
- *Understand the relationship between $\chi(G)$ and Δ_G*
- *Be able to compute the number of graphs with a particular vertex set.*
- *Understand the relationship between the number of vertices in a vertex set and the number of possible graphs that have that vertex set.*
- *Understand the statement of the Handshaking Lemma and be able to explain why it is true.*

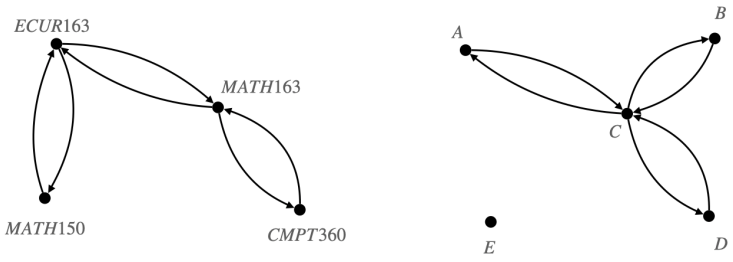
Newly Defined Terms and Notation.

- *graph, edge, vertex, adjacent, incident, path, cycle, degree, connected tree, k-colouring, chromatic number, χ, Δ_G*

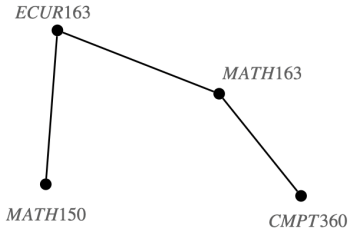
In Module 5 we started thinking carefully about proofs in mathematics and in Modules 6 and 7 we saw a proof technique, mathematical induction, that provides us a framework for proving universally quantified statements.

In Module 3 we briefly introduced graphs. In this module we examine graphs a little more closely so that we may begin to get our hands dirty with writing our own proofs.

Recall from Module 3 that a graph is an anti-reflexive and symmetric relation.



When draw pictures of graphs, since we know that the relation in symmetric, we may instead use lines to connected related points instead of arrows.



We can extend this convention in describing a graph. Instead of thinking of a graph as a relation, we can think of a graph as a pair of sets – vertices and edges.

Definition 8.1. *A graph G is a pair $G = (V_G, E_G)$ where V_G is a set called vertices and E_G is a set called edges. The elements of E_G are subsets of V_G that contain two elements.*

(note: the singular of the word "vertices" is "vertex")

For the graph in our previous picture we have:

$$V_G = \{MATH150, ECUR163, MATH163, CMPT360\}$$
$$E_G = \{\{MATH150, ECUR163\}, \{MATH163, ECUR163\}, \{MATH163, CMPT360\}\}$$

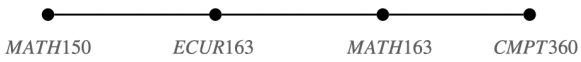
This graph has 4 vertices and 3 edges.

As we can express a graph as an ordered pair, we have a built in definition for what it means for two graphs to be equal. For ordered pairs (p_1, p_2) and (q_1, q_2) we have $(p_1, p_2) = (q_1, q_2)$ exactly when $p_1 = q_1$ and $p_2 = q_2$. And so we may write $G = H$ for graphs G and H when $V_G = V_H$ and $E_G = E_G$

Expressing a graph as an ordered pair of sets transmits the exact same information as the picture. A picture of a graph can be quite helpful in understanding which vertices are adjacent. But for large graphs, such a representation is infeasible.

Consider the graph $S = (V_S, E_S)$ where V_S is the set of courses offered in Fall 2020 at the University of Saskatchewan and where a pair of courses are adjacent when there is at least one student registered in both. The set V_S contains over 1000 elements. Drawing a picture is impossible!

Graphs capture *relational* data. That is, they tell us which elements are related to each other. When we draw a picture of a graph, we can draw the vertices in any place we want. How a picture of graph is laid out does not affect which elements are related to each other. For example, we may draw our graph above as



To be able to talk about particular vertices being related, we introduce the following terminology. Let G be a graph let $e \in E$. Since e is an edge, it is equal to pair $\{u, v\}$ so that $u, v \in V$ and $u \neq v$. In this context we say u and v are adjacent and u is incident with e,

Definition 8.2. *Let G be a graph, let v be a vertex of G and let k be a natural number. We say v has degree k when v is incident with exactly k edges.*

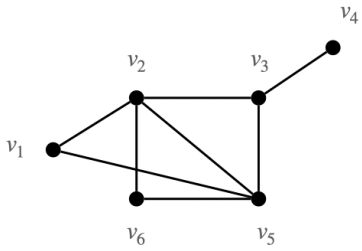
In our graph, the vertex $MATH163$ is adjacent to both $CMPT360$ and $ECUR163$. Since the vertex $MATH163$ is incident with exactly $k = 2$ edges, we say that this vertex has degree 2.

Aside. *Our definition of graph is that it is a pair of a sets. A picture of a graph is one way (of many) to represent a graph. A graph can also be represented using a matrix whose entries are each either 0 or 1. The entry $a_{i,j} = 1$ means that the edge ij exists in the graph.*

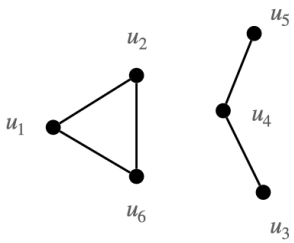
As graphs can be represented as matrices, tools from the study of Linear Algebra can be used to study properties of graphs. Surprisingly, looking at the eigenvalues of a graph can tell you something about how well connected the graph is. (This fact is entirely non-obvious!)

8.1 Preliminaries

Consider the two graphs shown below.



G_1



G_2

Which one of these graphs would you say is *connected*?

Though we haven't defined what the word *connected* means in the context of graphs, our intuition likely tells us that is it the graph on the left it the one that we should called *connected*.

If we try to write down a definition of connected we may arrive at something like:

A first attempt of a definition. *A graph G is connected when we can get from every vertex to every other vertex.*

But of course we are now faced hoping our reader understands the meaning of the phrase *get from every vertex to every other vertex.* This seems okay if we can easily draw a picture of our graph, but how can we know if a graph with 1000 vertices is connected? Let us try then to come up with a more workable definition of *connected*.

When we say *get from every vertex to every other vertex.* we probably mean that for every pair of vertices there is a way to traverse the vertices and edges of the graph to get from one vertex to the other. We encapsulate this idea with the word *path*

Definition 8.3. *Let $G = (V_G, E_G)$ be a graph and let x and y be vertices of G. We say there is a path from x to y when there is a sequence of distinct vertices*

$$z_0, z_1, z_2, \ldots, z_k$$

so that $z_0 = x$, $z_k =$ and for every $i \in \{0, 1, 2, \ldots, k-1\}$ we have $\{z_i, z_{i+1}\} \in E_G$

It has been a while since we have looked carefully at a definition. Let us take a moment to parse this definition:

- *Let $G = (V_G, E_G)$ be a graph and let x and y be vertices of G.*
  To define our new term we need to invoke a graph and pair of vertices in the graph.

- *We say there is a path from x to y when*
  We are defining a new term: path from x to y. The sentence that follows this one will tell us exactly what we mean when we use this new term.
- *there is a sequence of distinct vertices $z_0, z_1, z_2, \ldots, z_k$ so that*
  This sentence is telling us that a path from x to y is a sequence of distinct vertices that satisfies some properties.
- *so that $z_0 = x$, $z_k = y$ and for every $i \in \{0, 1, 2, \ldots, k-1\}$ we have $\{z_i, z_{i+1}\} \in E_G$*
  The properties are:
  1. $z_0 = x$: The first vertex of the sequence is x.
  2. $z_k = y$: The last vertex of the sequence is y.
  3. for every $i \in \{0, 1, 2, \ldots, k-1\}$ we have $\{z_i, z_{i+1}\} \in E_G$: if we look at any pair of subsequent vertices z_i, z_{i+1} in our sequence, there is an edge from the first vertex to the second vertex. I.e., $\{z_i, z_{i+1}\} \in E_G$.

Looking at the graph G_1 above, consider the sequence of vertices:

$$v_1, v_5, v_3, v_4$$

This is a sequence of distinct vertices. The first vertex is v_1. The last vertex is v_4. And we have the following edges in our graph: $\{v_1, v_5\}, \{v_5, v_3\}, \{v_3, v_4\}$. Therefore is sequence is a path from v_1 to v_4

This brings us now to a workable definition of connected.

Definition 8.4. *Let G be a graph. We say G is connected when for every pair of distinct vertices $u, v \in V_G$ there is a path from u to v.*

Comparing this definition to our first attempt above, they are essentially saying the same thing. The latter definition, however, has the added benefit of being unambiguous. As long as our reader knows what a graph is and understands our set notation, then they will know what we mean when we use the word *connected*.

Looking at our definition for path we required each of the vertices to be distinct. Let us consider the effect of changing our definition so that the first and last vertices are the same. What should we call a sequence of distinct adjacent vertices so that the first vertex and last vertex are the same? For example, consider the sequence

$$v_1, v_2, v_3, v_5, v_1$$

This isn't a path; the first and last vertices are the same. But it does satisfy all of the other properties necessary to call a sequence of vertices a path.

Definition 8.5. *Let $G = (V_G, E_G)$ be a graph. A cycle is a sequence of vertices*

$$z_0, z_1, z_2, \ldots, z_k$$

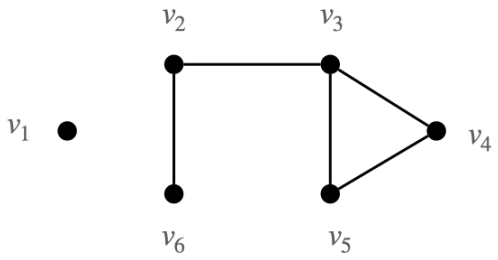
so that $x_0 = x_k$, all other vertices are distinct, and for each $i \in \{0, 1, 2, \ldots, k-1\}$ we have $\{x_i, x_{i+1}\} \in E$

For our examples above we have seen that just as some graphs are connected and others are not, some graphs contain cycles and others do not. In the following section we study those connected graphs that contain no cycles.

Test Your Understanding

1. Which of these graphs is connected:

   (a)



   (b) $G = (V_G, E_G)$ with $V_G = \{z_1, z_2, z_3, z_4, z_5, z_6\}$ and $E_G = \{\{z_1, z_2\}, \{z_1, z_3\}, \{z_1, z_4\}, \{z_1, z_5\}\}$.

   (c) $H = (V_H, E_H)$ with $V_H = \{y_i \mid 1 \leq i \leq 500\}$ and $E_H = \{\{y_i, y_{i+1}\} \mid 1 \leq i \leq 499\}$.

Test Your Understanding Solution

1. (a) This graph is not connected. There is no path from v_1 to v_2.

   (b) This graph is not connected. Vertex z_6 is not part of any edge and so there is no path from z_6 to any other vertex.

   (c) This graph is connected. For any pair of vertices y_j and y_k with $j < k$ we have the path

   $$y_j, y_{j+1}, y_{j+2}, \ldots, y_{k-1}, y_k$$

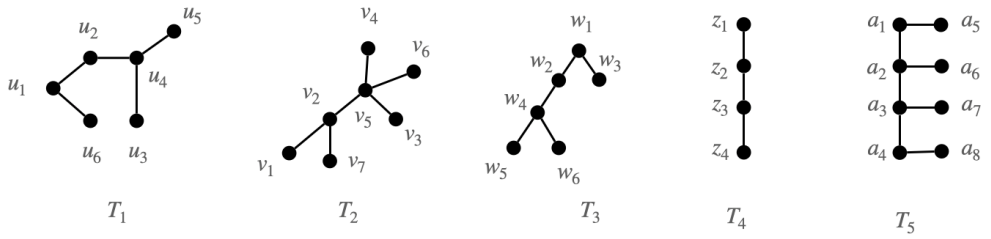
8.2 Trees

We begin with a definition.

Definition 8.6. *Let G be a connected graph. We say that G is a tree when G has no cycles.*

Trees have a wide variety of practical applications, particularly in computer science. As opposed to practical interest, our interest in trees is more so in that they are a new mathematical object that is easily understood. And so we can practice our mathematical reasoning and communication skills by way of their study.

Let us look at some examples of trees.



For each of the trees shown above, take a moment to count the following things:

- the number of vertices
- the number of edges
- the number of vertices of each degree.

For example, T_1 has

- 6 vertices
- 5 edges
- 3 vertices of degree 1
- 3 vertices of degree 2.

.
.
.
.
.
.
.
.

.
There are lots of patterns to notice here. In particular, we are interested in the following two mathematical facts:

Lemma 8.7. *If T is a tree with at least two vertices, then T has at least one vertex of degree 1.*

Theorem 8.8. *If G is a tree with $n \geq 1$ vertices, then G has $n - 1$ edges.*

It turns out that these two mathematical facts are related! We devote the remainder of this section to proving that these two results are true. We begin with Lemma 8.7.

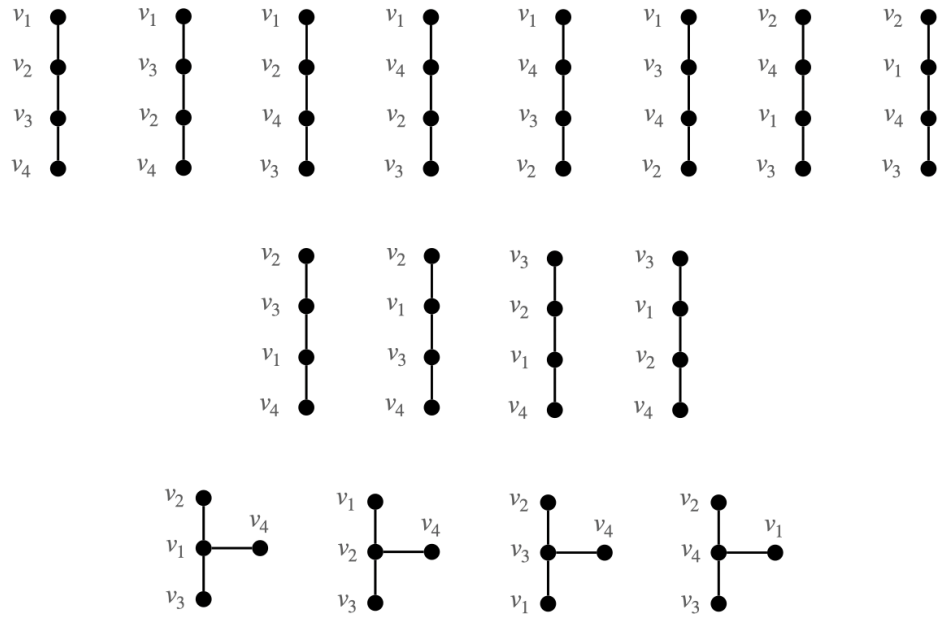
Let T be a tree and consider a vertex $v \in V$. There may be many paths in T that start at v. Let P be a path in T that starts at v and contains the most number of vertices possible. Since P is a path it is a sequence of distinct vertices of T: $v_1, v_2, \ldots, v_k$.

Since this path is as long as possible, we cannot add any vertices to the end to make a longer path. Since all of the vertices of the path must be distinct, this must mean that all of the vertices adjacent to v_k are already contained in the path (otherwise we could make the path one vertex longer). We know that v_k is adjacent to v_{k-1}. It is possible that v_k is adjacent to any other vertex on the path? (Remember that T is a tree.)
.
.
.
.
.
.
.
.

No! As if so, T would have a cycle! If v_k was adjacent to some other vertex on the path, say, v_i, then $v_i, v_{i+1}, \ldots, v_{k-1}, v_k, v_i$ is a cycle. As T is a tree is has no cycles. Therefore v_{k-1} is the only vertex adjacent to v_k and so v_k has degree 1.

We turn now to Theorem 8.8. Imagine we had a tree T with $n_T = 5$ vertices and m_T edges. We want to conclude T has 4 edges. Let $V_T = \{v_1, v_2, v_3, v_4, v_5\}$. Since T is a tree, then by Lemma 8.7 we are guaranteed that T has at least one vertex of degree 1. Let v_5 be such a vertex. (If $deg(v_5) \neq 1$, then we can relabel the vertices so that v_5 is the one with degree one.) Consider the effect of removing v_5 and its incident edge from T. What remains is certainly still a tree; as T has no cycles, removing a vertex from T cannot create a cycle. Let T' be the tree formed from T by removing a v_5 from T. The tree T' has four vertices

and has vertex set $\{v_1, v_2, v_3, v_4\}$ so is one of the following trees:



(These are all of the trees that have vertex set $\{v_1, v_2, v_3, v_4\}$. Other than trial and error, there is no good way for you to know that these indeed are all such trees.)

Aside. *That the vertices of a tree must have labels is a pain. If we don't care about the labels, then there are only two* different *trees here. We discuss what it means for graphs to be the same and different in this sense in Section 8.5. (This section is optional.)*

Each of these trees has 4 vertices and 3 edges. Since we formed T' from T by removing a single edge and a single vertex, it must be that T has $4+1=5$ vertices and $3+1=4$ edges.

When we remove a vertex of degree 1 from a tree, the number of vertices and edges each go down by 1. It is this idea that forms the basis of our proof by induction for Theorem 8.8

Proof of Theorem 8.8. Let $P(n)$ be the formula over $\{1, 2, 3, \ldots, \}$

A tree with n vertices has $n-1$ edges.

To prove our theorem we show that both hypotheses in the Principle of Mathematical Induction hold.

(1) $P(1)$ is true
Let T be a tree with a single vertex. Since T has only one vertex it has no edges. Therefore T has $0 = 1 - 1$ edges. Therefore a tree with 1 vertex has $1 - 1$ edges. And so $P(1)$ is true.

(2) if $P(k)$ is true, then $P(k+1)$ is true

Let T be a tree with $n = k+1$ vertices. By Lemma 8.7, T has a vertex of degree one. Let v be a vertex of degree one in T. Let T_v be the tree formed from T by removing v and its incident edge. The tree T_v has k vertices. Since $P(k)$ is true, T_v has $k-1$ edges. Therefore T has $k+1$ vertices and k edges. And so it follows that $P(k+1)$ is true.

Since both (1) and (2) hold in the statement of the Principle of Mathematical Induction, so must the conclusion. Therefore for every $n \geq 1$, a tree with n vertices has $n-1$ edges. □

We now present the same proof, but without invoking all of the formal machinery of the Principle of Mathematical Induction.

Proof of Theorem 8.8. We proceed by induction on n. Let T be a tree with $n = 1$ vertices. Since T has just one vertex it has no edges and so T has $0 = 1 - 1 = n - 1$ edges.

Consider now a tree T with $n = k+1$ vertices. By Lemma 8.7, T has a vertex of degree 1. Let v be a vertex of degree 1 in T. Let T_v be the tree produced from T by removing v and its incident edge. The tree T_v has k vertices and so by induction it has $k-1$ edges. Therefore T has $k+1$ vertices and k edges. The result now follows by induction. □

Aside. *You may wonder why we have described the mathematical fact about vertices of degree* 1 *as a* Lemma *and the mathematical fact about number of edges in a tree as a* Theorem

We can give labels to our mathematical results to indicate to our reader their function. A Theorem *is main result. A* Lemma *is a small result that aids us in the proof of a* Theorem*. Some authors and writers use the word* Proposition *to refer to a mathematical results that seem less important than a Theorem.*

The choice use of this different words is entirely a cultural. Some people (such as the writer of these notes) never speak of Propositions*, only* Theorems*. Whereas others preserve the word* Theorem *for* important *results. (Of course, the decision about what counts as* important *is also cultural! Are the important things only those that have direct application?)*

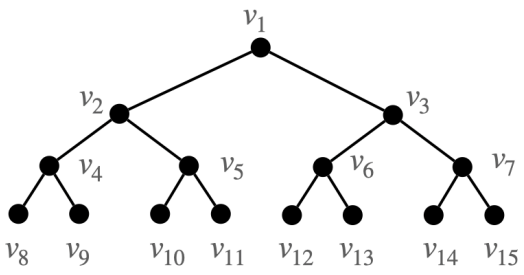
Another word that appears in these context is Corollary*. A corollary is a result that follows almost directly from the statement of a Theorem. For example...*

Corollary 8.9. *Let G be a connected graph with $n \geq 3$ vertices. If G has at least n edges then G has a cycle.*

Proof. Let G be a connected graph with n vertices and at least n edges. By Theorem 8.7, since G does not have $n-1$ edges, G cannot be a tree. Since G is connected and is not a tree, G must have a cycle. □

Test Your Understanding

1. For the tree below, count the following things:



   (a) number of vertices of degree 1

   (b) number of vertices of degree 2

   (c) number of vertices of degree 3

   (d) number of vertices.

2. Explain why the sum of your answers for (a), (b) and (c) gives your answer for (d)

3. Let T be a tree with n vertices. From our work in 8.2 we showed that T has at least one vertex of degree 1. Of coursen$T$ may have many more than one vertices of degree 1. Find a formula for the maximum number of vertices of degree 1 that T can have.

Test Your Understanding Solution

1. (a) 8

   (b) 1

   (c) 6

   (d) 15

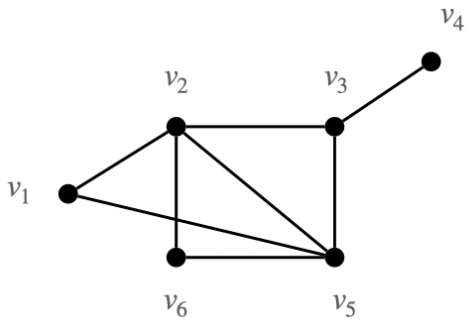
2. Every vertex of the tree has degree 1, 2 or 3. Therefore when we sum up the vertices of each degree we count each vertex exactly once.

3. A tree with $n \geq 3$ vertices can have at most $n-1$ vertices of degree 1. Such a tree has a vertex of degree $n-1$ adjacent to $n-1$ vertices of degree 1.

8.3 Graphs and Counting

In the previous section we proved that every tree has a vertex of degree 1. However when we look back at our pictures we see that every tree with at least one edge has at least two vertices of degree 1. Let us shelf this observation for now and first think about how the mere act of *counting* can help us prove things about graphs.

Consider the graph shown below.



This graph has 6 vertices and 8 edges. Consider going around to each vertex and summing up its degree.

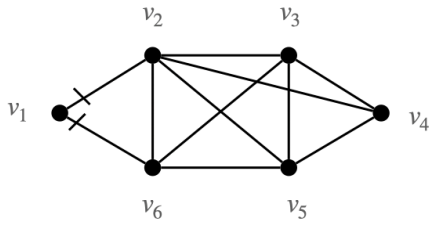
$$\sum_{v \in V} deg(v) = deg(v_1)+deg(v_2)+deg(v_3)+deg(v_4)+deg(v_5)+deg(v_6) = 2+4+3+1+4+2 = 16$$

16 is exactly twice the number of edges. Take a moment to look at other examples of graphs in these modules. Compare the sum of the vertex degrees with the number of edges.
.
.
.
.
.
.
.
.
.
. These observations give us the following result.

Lemma 8.10 (The Handshake Lemma)**.** *If G is a graph with n vertices and m edges, then*

$$2m = \sum_{v \in V_G} deg(v)$$

Before we can even think about writing down a proof this fact we need to understand why such a fact is true. Take the sum of the degrees of the vertices in the graph below. As you go around each vertex and sum its degree, mark each edge that you count. For example, when we count up the of degree of v_1 we mark all of the edges incident with v_1:



.
.
.
.
.
.
.
.
.
.
.
.
.
.
.

Aside. *The dotted vertical lines that appear in various places in the notes are places for you to stop and do a little bit of guided independent thinking. I suspect you that you will get more out of these notes if you spend the minute or so doing this thinking rather than just skipping down the to next part. If you are lost, attending the live tutorials is a good place to get help.*

How many times did you make a mark at each vertex?
How many times did you mark each edge?

And so we observe *An edge* $\{v_i, v_j\} \in E_G$ *contributes +1 to* $deg(v_i)$ *and +1 to* $deg(v_j)$*. And so every edge contributes* $+2$ *to the sum* $\sum_{v \in V_G} deg(v)$.

We are now ready to write our proof!

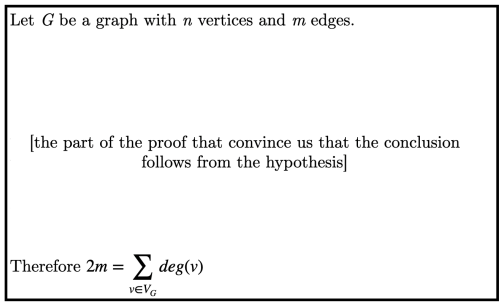
Our hypothesis in Handshaking Lemma is: *G is a graph with n vertices and m edges.* This tells us what the first sentence of our proof should be:

Let G be a graph with n vertices and m edges.

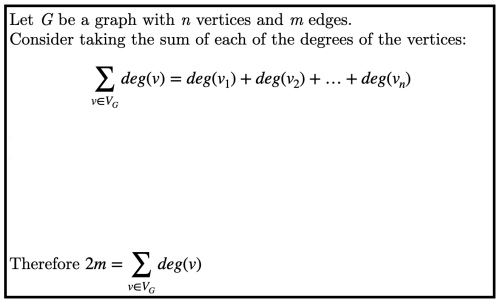
Our conclusion is $2m = \sum_{v \in V_G} deg(v)$. As we are trying to convince our reader the conclusion is true whenever the hypothesis is true, our last sentence in our proof should be

Therefore $2m = \sum_{v \in V_G} deg(v)$.

And so right now our proof looks like this:



In looking at the equality we want to verify, and comparing it to our thoughts above, we want to be able to talk about the terms in the sum on the right. And so it makes sense next to introduce the sum.



Looking at our key observation, we want to write a sentence that conveys our key observation

to our reader. So let us use exactly this sentence!

Let G be a graph with n vertices and m edges.
Consider taking the sum of each of the degrees of the vertices:

$$\sum_{v \in V_G} deg(v) = deg(v_1) + deg(v_2) + \ldots + deg(v_n)$$

An edge $\{v_i, v_j\} \in E_G$ contributes $+1$ to $deg(v_i)$ and $+1$ to $deg(v_j)$.
And so every edge contributes exactly $+2$ to the sum $\sum_{v \in V_G} deg(v)$.

Therefore $2m = \sum_{v \in V_G} deg(v)$

And now our conclusion is inescapable!

Let G be a graph with n vertices and m edges.
Consider taking the sum of each of the degrees of the vertices:

$$\sum_{v \in V_G} deg(v) = deg(v_1) + deg(v_2) + \ldots + deg(v_n)$$

An edge $\{v_i, v_j\} \in E_G$ contributes $+1$ to $deg(v_i)$ and $+1$ to $deg(v_j)$.
And so every edge contributes exactly $+2$ to the sum $\sum_{v \in V_G} deg(v)$.

Therefore $\sum_{v \in V_G} deg(v)$ is equal to twice the number of edges.

Therefore $2m = \sum_{v \in V_G} deg(v)$

Aside. *Proof writing is like putting together a jigsaw puzzle. For the reader, the final product should be one cohesive piece of writing. However just like a jigsaw puzzle, our proof doesn't need to be put together in any particular order.*

In doing mathematics we generally undertake two types of writing: writing to understand *and* writing to explain. *Our* writing to understand *is deeply personal. It never needs to be shown to anyone. It consists of our scratch notes, our idle thoughts and is often filled with errors and confusion. The result of our* writing to understand *is our ability to* write to explain. *Writing a proof is an act of* writing to explain. *But look at all of the work we had to do to* understand *before we could* write to explain*!*

Unlike most of the mathematics you have seen before, there are very few one-sized fits all approaches to writing a proof. Our own personal writing to understand *should point us towards the sequence of sentences we need to write down in order to* write to explain.

Just like numerical calculation, proof writing in mathematics is a skill to be developed. One cannot learn to write (and read) proofs without lots of practice!

Imagine there are n people meeting for the first time. As is custom in the West when people meet, everyone shakes hands with one another. Every person shakes hands with $n-1$ other people.

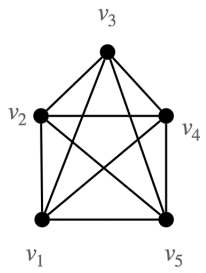
Consider a graph G where the n vertices are the n people and and edge between a pair of vertices denotes that the pair of people shook hands. Each edge corresponds to a handshake. And so the total number of handshakes is exactly the number of edges. Using the Handshaking Lemma we have

$$m = \frac{1}{2}\sum_{v \in V} deg(v) = \frac{1}{2}\sum_{v \in V} deg(v) = \frac{n(n-1)}{2}$$

In this graph denoting handshakes, every pair of vertices is adjacent. A graph in which every vertex is adjacent seems particularly interesting, so we define the following terminology.

Definition 8.11. *Let G be a graph. If every pair of vertices in G is adjacent, then we say G is complete*

For example, this a complete graph with 5 vertices:



Without counting up its edges one by one, we can use the Handshake Lemma to tell us that this graph has $\frac{5(4)}{2} = 10$ edges.

And so from our argument above we have the following statement.

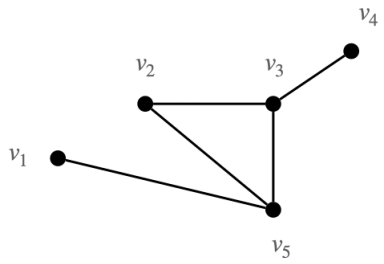
Theorem 8.12. *A complete graph with $n \geq 1$ vertices has $\frac{n(n-1)}{2}$ edges.*

In the last section we saw all of the trees with vertex set $\{v_1, v_2, v_3, v_4\}$. There we significantly more than we expected! By counting the number of edges in a complete graph with n vertices, we can in fact count the number of graphs there are with vertex set $\{v_1, v_2, \ldots, v_n\}$. We begin with a small example.

Let $V = \{v_1, v_2, v_3, v_4, v_5\}$. Let E_k be the edge set of the complete graph with vertex set V. That is,

$$E_k = \{\{v_i, v_j\} \mid 1 \leq i < j \leq 5\}$$

Consider the graph H shown below.



This graph has vertex set $V = \{v_1, v_2, v_3, v_4, v_5\}$ and edge set

$$E_H = \{\{v_1, v_5\}, \{v_2, v_5\}, \{v_2, v_3\}, \{v_3, v_5\}, \{v_3, v_4\}\}$$

Notice $E_H \subseteq E_k$ – indeed, each edge is of the form $\{v_i, v_j\}$ with $1 \leq i < j \leq 5$

And so we see that every subset of E_k corresponds to a graph with vertex set V and vice versa. Therefore the number of graphs with vertex set V is equal to the number of subsets of E_k.

Theorem 8.13. *Let $n \geq 1$ be an integer and let V be a set with n elements. There are ???? different graphs with vertex set V.*

(Take a moment to look back at Module 6 to remember the number of subsets of a set and then fill in the ???? in the statement of the theorem above. Be careful – don't confuse the two different uses of the parameter n. The set E_k does not have n elements.)

Aside. *Take a moment to appreciate of things we need to understand in order to state and understand Theorem 8.13!*

The Handshake Lemma is not yet done bearing its fruits! Returning back to trees, we can use the Handshaking Lemma to show that every tree with at least one edge has at least two vertices of degree 1. From Theorem 8.8, we know that a tree with n vertices has $n-1$ edges. And so for a tree T we have

$$2(n-1) = \sum_{v \in V} deg(v)$$

By Lemma 8.7, T has at least one vertex of degree 1. Let x be such a vertex. Denote the remaining vertices as $v_2, v_3, \ldots, v_n$. Let us examine more closely the equality $2(n-1) = \sum_{v \in V} deg(v)$.

$$\begin{aligned} 2(n-1) &= deg(x) + deg(v_2) + \cdots + \deg(v_n) \\ 2n-2 &= 1 + deg(v_2) + \cdots + \deg(v_n) \\ 2n-3 &= deg(v_2) + \cdots + \deg(v_n) \end{aligned}$$

There are $n-1$ terms in the sum

$$deg(v_2) + \cdots + \deg(v_n)$$

And so the average value of a term in the sum is

$$\frac{deg(v_2) + \cdots + \deg(v_n)}{n-1} = \frac{2n-3}{n-1} = 2 - \frac{1}{n-1}$$

Since the average value of a term in the sum is less than 2, at least one term in this sum has to be less than 2. These terms all correspond to vertex degrees in T, and so each term is an element of the set $\{1, 2, 3, \ldots, n-1\}$. And so a term that is less than 2 corresponds to a vertex (other than x) that has degree 1. Therefore T has at least two vertices of degree 1.

Theorem 8.14. *If T is a tree, then T has at least two vertices of degree 2.*

Test Your Understanding

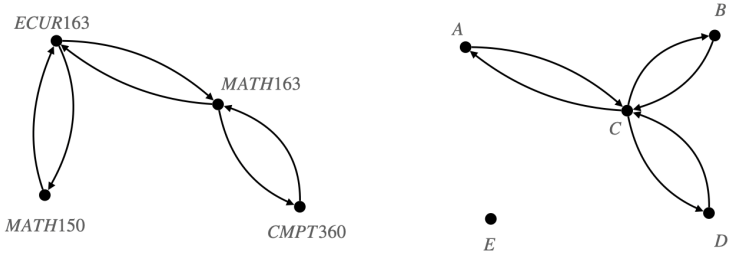
1. What replaces ??? in the statement of Theorem 8.13?
2. How many graphs are there with vertex set $V = \{a, b, c, d, e, f\}$.
3. Let G be a graph in which every vertex has degree 3. Is it possible that G has an odd number of vertices?

Test Your Understanding Solution

1. $2^{\frac{n(n-1)}{2}}$
2. This set has $n = 6$ elements and so there are $2^{\frac{6(5)}{2}} = 2^{15}$ graphs with vertex set $V = \{a, b, c, d, e, f\}$.
3. By the Handshake Lemma it must be that $\sum_{v \in V} deg(v)$ is even. If each vertex of G has degree 3 then we may write this sum as $\sum_{v \in V} deg(v) = \sum_{v \in V} 3 = 3n$, where n denotes the number of vertices in G. By the Handshake Lemma this number must be even. If n is odd then $3n$ is odd. Therefore n must be even.

8.4 Graph Colouring

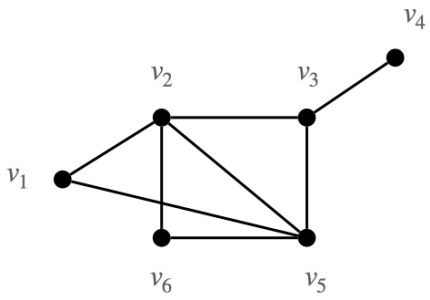
We close our work on graphs by returning to our two examples from when we introduced graphs in Module 3:



In both of these examples we want to assign a label to each of the vertices so that adjacent vertices get different labels. In doing so we wanted to use the fewest number of labels possible. Of course, the names of vertices and the names of labels don't make any difference and so let us capture this process with the following two definitions.

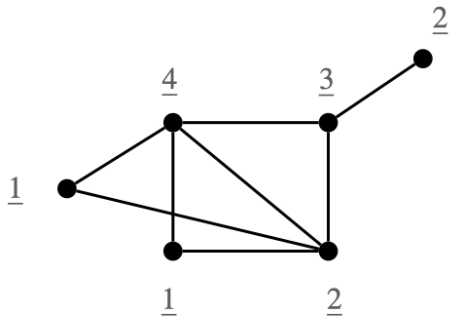
Definition 8.15. *Let G be a graph and let $k \geq 1$ be an integer. A k-colouring of G is a function $c : V \to \{1, 2, 3, \ldots, k\}$ so that for all edges $\{u, v\} \in E$ we have $c(u) \neq c(v)$. We refer to the elements of the set $\{1, 2, 3, \ldots, k\}$ as colours.*

Let G be the graph shown below:



Let $c : V(G) \to \{1, 2, 3, 4\}$ so that

- $c(v_1) = c(v_6) = 1$
- $c(v_2) = 4$
- $c(v_3) = 3$
- $c(v_4) = c(v_5) = 2$



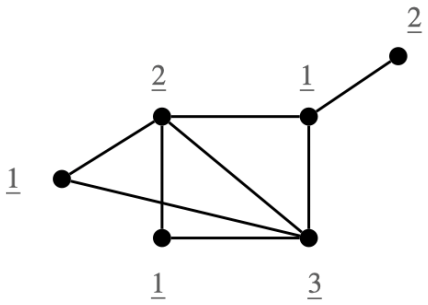
(The underlined numbers indicate the colour assigned to each vertex. We underline these colours so that we don't confuse the colour of each vertex with the name of the vertex)

As adjacent vertices have different colours, this is a 4-colouring.

Aside. *Why do we call this a k-colouring if the labels are $\{1, 2, 3, \ldots, k\}$ and not actual colours? Convention. We use numbers rather than colours in our figures so that those who colour blind can still follow these notes.*

Definition 8.16. *Let G be a graph. The chromatic number of G is the smallest k so that G has as k-colouring. We denote the chromatic number of G with the notation $\chi(G)$.*

In our example above, we saw a 4-colouring of our graph. In fact this graph admits a 3-colouring:



The chromatic number of G, $\chi(G)$, is the smallest k so that G has a k-colouring. And so the existence of this 3-colouring tells us $\chi(G) \leq 3$.

To conclude $\chi(G) = 3$ we must convince ourselves that G has no 1-colouring and has no 2-colouring. Take a moment to convince yourself of these facts.

.
.
.
.

.
.
.
.
.
.

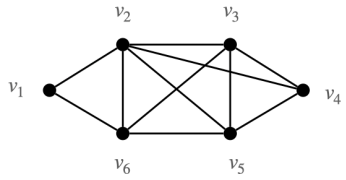
Aside. *Here the symbol χ is the lower-case Greek letter named "chi". It is usually pronounced as* `k-eye`*. This is unrelated to this symbol's use in statistics (χ^2 distributions) Why do we use a greek letter to denote this parameter? Convention.*

Our examples so far have been quite small. However in most practical contexts, the number of vertices is very large. Recall the graph S defined in Section 8.0: $S = (V_S, E_S)$ where V_S is the set of courses offered in Fall 2020 at the University of Saskatchewan and where a pair of courses are adjacent when there is at least one student that is registered in both. The set V_S contains over 1000 elements.

A final exam schedule corresponds to a colouring of S. Each colour corresponds to a time slot for an exam. Vertices that are adjacent must get different colours as they have overlapping enrolment. In an ideal world (ha!) the Registrar's Office would be able to design a final exam schedule so that no student was scheduled for simultaneous exams and the exam period used as few exam writing slots as possible. Computing the minimum number of needed exam writing slots corresponds to finding the chromatic number of S. Such a task is a computationally infeasible.[3] That is to say, computing the chromatic number of a very large graph may take a computer hundreds of years!

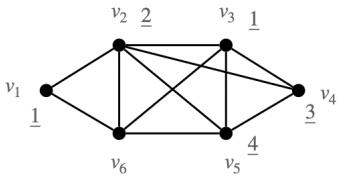
The exam schedule for Fall 2020 runs from December 8th - 23rd (16 total days). There are three exam slots per day. And so there are a total of $16 \times 3 = 48$ exam slots. To find an exam schedule in which no student has a conflict, the Registrar's office needs only to find a 48-colouring of S, rather than the chromatic number of the S.

As computing the exact chromatic number of a graph is computationally difficult, we consider a method to find an upper bound on this parameter. Consider colouring the vertices of this graph below in order always using the lowest colour possible.



[3] viz. the problem is NP-hard. (If that doesn't mean anything to you, that is okay! Just ignore this footnote.)

We begin by colouring v_1 with 1. Since v_2 is adjacent to v_1 we must colour v_2 with 2. Since v_3 is adjacent to v_2 but not to v_1 we may colour it with 1. We continue in this fashion and colour vertices v_4 and v_5



At this point, we are at v_6. The set of colours appearing on vertices adjacent to v_6 are $\{1, 2, 4\}$ and so we colour v_6 with colour 3.

Using this process, when we come to colour a vertex v, there are at most $deg(v)$ colours already appearing amongst the vertices adjacent to v. And so as long as we have more than $deg(v)$ colours available, we can find a colour for v.

Let G be a graph with n vertices and let $\Delta_G = \max\{deg(v)|v \in V(G)\}$. That is, Δ_G is the maximum degree of a vertex in G. Consider colouring (using the colours $\{1, 2, 3, \ldots, \Delta_G+1\}$) the vertices of a graph in order:

$$v_1, v_2, \ldots, v_n$$

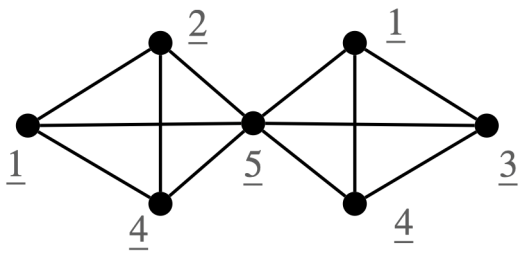
As we colour the vertices one at a time, when we arrive at a vertex v it is adjacent to no more than $deg(v)$ vertices that are already coloured. Since $deg(v) \leq \Delta_G$ there must be some colour amongst $\{1, 2, 3, \ldots, \Delta_G + 1\}$ available. Therefore G has a $\Delta_G + 1$-colouring. And so

Theorem 8.17. *For every graph G we have $\chi(G) \leq \Delta_G + 1$*

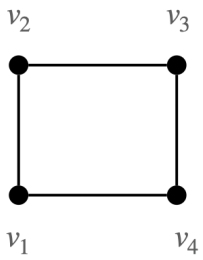
Aside. *The symbol Δ is the capital Greek letter "delta". Its use here is unrelated to its use in calculus. And again, its use here is dictated only by convention.*

Test Your Understanding

1. Let K_n denote the complete graph with n vertices. Find $\chi(K_n)$.
2. For which value of k is the colouring shown below a k-colouring of the graph?



3. Find the chromatic number of the graph shown above.
4. Let C_n denote the graph on n vertices that is a cycle. The graph C_4 is shown below.



C_4

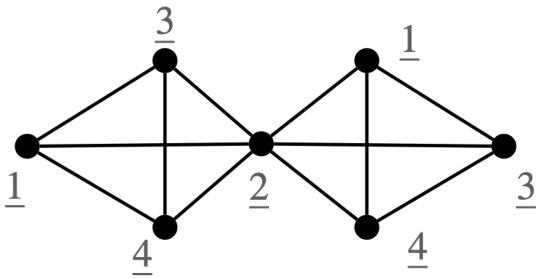
Determine $\chi(C_n)$ for each $n \geq 3$

Test Your Understanding Solution

1. In a complete graph every pair of vertices is adjacent. Therefore every vertex must be assigned a unique colour. And so $\chi(K_n) = n$.

2. Each of the colours 1,2,3,4 and 5 appear. Therefore this is a 5-colouring.

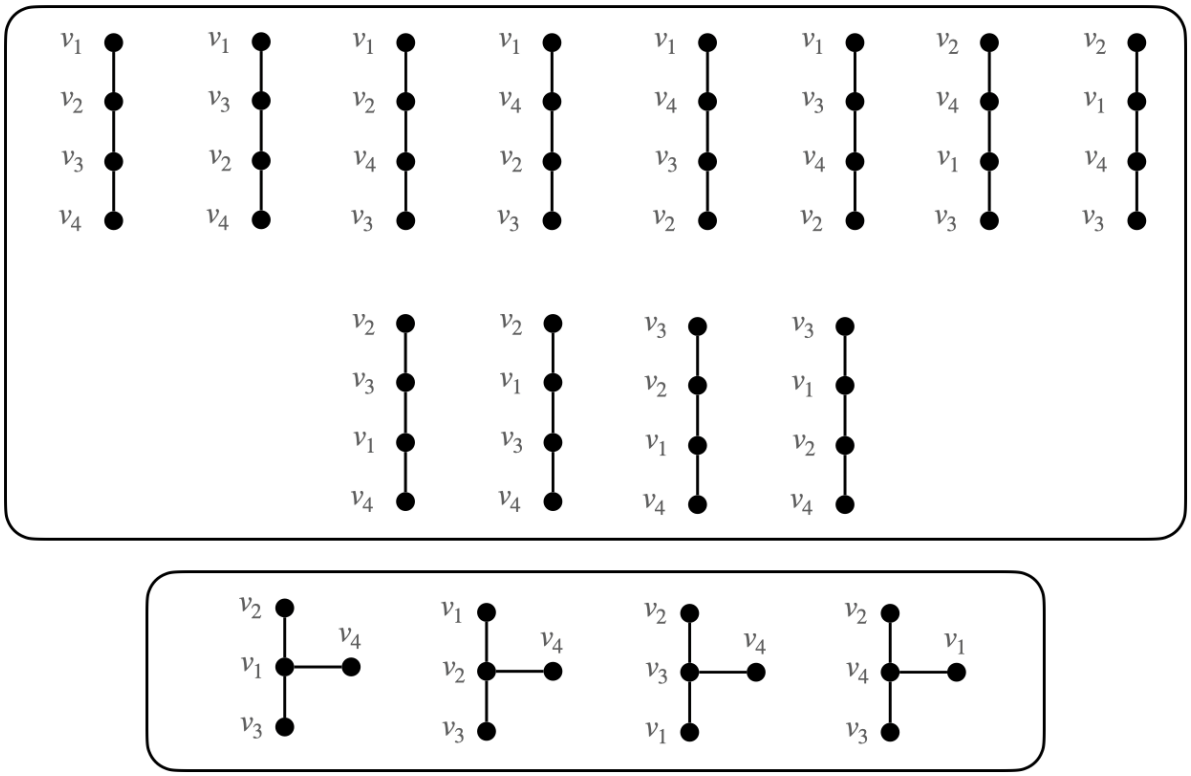
3. Let H be the graph shown. Since H contains a complete graph with four vertices, we have $\chi(H) \geq 4$. The image below gives a 4-colouring of H and so we have $\chi(H) = 4$.



4. Since C_n has at least one edge we have $\chi(C_n) \geq 2$. When n is even we may alternate between using colours 1 and 2 on the vertices and so we have $\chi(C_n) = 2$. If we try this same procedure when n is odd we colour the last vertex with the same colour as the first vertex. Since these vertices are adjacent, this is not a colouring. This is resolved by colouring the last vertex instead with colour 3. And so when n is odd we have $\chi(C_n) = 3$.

8.5 Graph Isomorphism and Unlabelled Graphs (Optional)

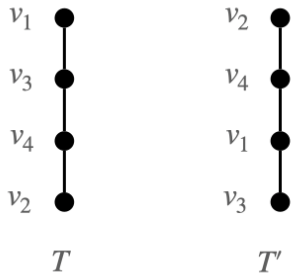
Looking back at our trees on four vertices with vertex set $\{v_1, v_2, v_3, v_4\}$ from Section 8.2, we can separate them into two groups.



In the section we think about in what sense the trees in the same group are the same.

(Here we are grouping things based on being the same with respect to a particular property. This sure looks like an equivalence relation and its corresponding partition. More on this in a moment.)

Let us look at the two graphs in the first group.



These two graphs have different edges sets, and so they are not equal. But *clearly* (?) they are the *same*. So, what should *same* mean here?

There is a natural correspondence between the vertices in the first tree and the vertices in the second tree:

T	T'
v_1	v_2
v_3	v_4
v_4	v_1
v_2	v_3

This correspondence is in fact a bijection! Let $\phi : V(T) \to V(T')$ so that

- $\phi(v_1) = v_2$
- $\phi(v_2) = v_3$
- $\phi(v_3) = v_4$
- $\phi(v_4) = v_1$

Aside. *The symbol ϕ is the lower-case Greek letter "phi". It is sometimes pronounced as* `fee`*, but it is often pronounced as* `f-eye`*.*

Notice that the image of an edge with respect to this bijection is an edge. For example, the edge $\{v_1, v_2\} \in E_T$ maps to the edge $\{\phi(v_1), \phi(v_2)\} = \{v_2, v_4\} \in E_{T'}$. Similarly the image of a non-edge is also a non-edge. For example, $\{v_1, v_4\} \notin E_T$ and $\{\phi(v_1), \phi(v_4)\} = \{v_2, v_1\} \notin E_{T'}$.

That is, we have the following property:

$$\{\phi(u), \phi(v)\} \in E_{T'} \text{ if and only if } \{u, v\} \in E_T.$$

When we are permitted to change the labels on the vertices, these two graphs have the same edge set. We capture these ideas in general with the following definition.

Definition 8.18. *Let $G = (V_G, E_G)$ and $H = (V_H, E_H)$. We say G is isomorphic to H when there exists a bijection $\phi : V_G \to V_H$ so that $\{\phi(u), \phi(v)\} \in E_H$ if and only if $\{u, v\} \in E_G$. We say ϕ is an graph isomorphism. When G is isomorphic to H we write $G \cong H$.*

An graph isomorphism is a bijection from one graph to another that preserves exactly the structure of the first graph. And so saying two graphs are isomorphic is akin to saying that they have the *same* structure but possibly a different labelling. We can understand an isomorphism as the act of erasing the labels from G and replacing them with the corresponding labels in H.

The idea of isomorphism is an important one in mathematics. Two mathematical objects being isomorphic usually means that they are the same when we ignore the specific labels we are using.

In you have studied Linear Algebra, you have seen isomorphism before, even if you didn't know it. With respect to structure of adding vectors, a plane that contains the origin is isomorphic to $\mathbb{R}^2$. Similarly a line through the origin is isomorphic to $\mathbb{R}$. If you are taking MATH 266 in term 2, you will see more about isomorphisms in Linear Algebra.

Back to equivalence classes! Let $\mathcal{G}$ be the set of all graphs with all possible labellings. Consider the relation on $\mathcal{G}$

$$R = \{(G, H) | G \cong H\}$$

This is an equivalence relation. The equivalence classes are sets of graphs that are isomorphic to each other. For each equivalence class we can draw an *unlabelled graph*. From our tree example above we could draw the graph

to represent all of the trees on four vertices that have this same structure.

In the context of proving facts about graphs, the labels in the vertex set are rarely relevant. And so in the study of *Graph Theory* one proceeds to prove facts about unlabelled graphs. Using this equivalence relation, proving a fact about an unlabelled graph proves that same fact for every graph contained in the equivalence class that the unlabelled graph represents.

9 Complex Numbers

Learning Incomes.

- *Definitions of sine, cosine and radian angle measure.*
- *Be fluent with set notation*

Learning Outcomes.

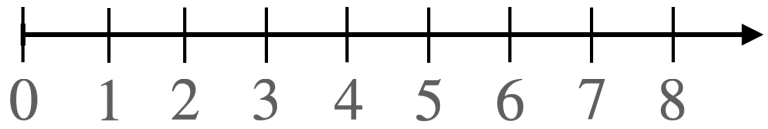
- *Perform operations (addition and multiplication) with complex numbers*
- *Be able to find the magnitude and complex conjugate of a complex number*
- *Understand the relationship between a complex number, its conjugate and its magnitude*
- *Be able to express a complex number using trigonometric ratios*
- *Find the location of a complex number in the Complex Plane.*

Newly Defined Terms and Notation.

- *complex number,* $\mathbb{C}$*,* $Re(z), Im(z)$*, complex conjugate,* $\overline{z}$*, magnitude,* $|z|$*, Complex Plane.*

Imagine for a moment you had never heard of negative numbers. This, perhaps, isn't too difficult to imagine; if you never learned about them in primary or secondary school it is no guarantee that you would come across them as part of your day-to-day existence. No one goes to the shops to buy -3 mangoes.

In your mind's eye, the number line looks like this:



In your world of only positive thoughts, what would you say if you encountered the equation

$$x + 1 = 0$$

Not knowing of negative numbers, you were proclaim quite confidently that there was no solution for this equation. "*There is nothing you can add to 1 to get 0!*", you would cry.

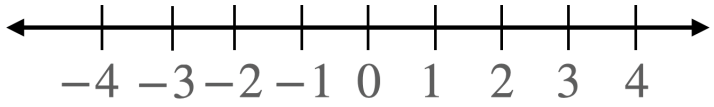
But, in your quest for answers and for exploration, perhaps you invent a new number.

Definition 9.1. *Let* -1 *denote the unique number* x *so that* $x + 1 = 0$*.*

With your newly defined number, -1, you feel confident in knowing that, at least in your own personal world of mathematics, the equation $x + 1 = 0$ has a solution. When faced with the equation $x + 2 = 0$ you realize that you can extend your definition of -1 to find a solution for $x + a = 0$ for any $a \in \mathbb{N}$

Definition 9.2. *For $a \in \mathbb{N}$, let $-a$ denote the unique number x so that $x + a = 0$*

With this new found knowledge you have, in effect, extended your number line of $\mathbb{N}$ to be the number line for $\mathbb{Z}$



Aside. *Congratulations, you have just defined the negative integers! This previous definition is in fact a very reasonable mathematical definition of the notation $-a$.*

Notation for numbers is strange when we think more carefully about it. In the same way that the word cat *and an actual cat are not the same thing, the numeral* 1 *the quantity we are referring to when we use this symbol are not the same thing. The same is true for the symbol -1. A negative quantity is different than the symbol we use to represent it. Okay, that's enough applied linguistics for now – this isn't meant to be a course in semiotics of mathematics. I don't know that de Saussure had much to say about signs in mathematics communication.*

Brimming with confidence you wonder for which other equations heretofore unsolvable could you define an answer. Happening upon the equation

$$x^2 + 1 = 0$$

you decide to define the following piece of notation:

Definition 9.3. *Let i denote the unique number x so that $x^2 + 1 = 0$.*

Since $i^2 + 1 = 0$, rearranging we have $i^2 = -1$ and so $i = \sqrt{-1}$. With this new number, you quickly realize that there is an entire new class of equations you can solve. For example, consider the equation

$$x^2 + x + 1 = 0$$

Using the quadratic formula, we have

$$x = \frac{-1 \pm \sqrt{1 - 4(1)(1)}}{2} = -\frac{1}{2} \pm \frac{\sqrt{-3}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}\sqrt{-1}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$$

Just as before we knew about negative numbers we were stymied by equations like $x+5=0$, now that we have a solution to $x^2+1=0$ we can always find solutions to equations of the form $ax^2+bx+c=0$. No longer does a negative discriminant prevent us from finding solutions to our quadratic equations.

Informally, complex numbers are numbers of the form $a+bi$, with $a, b \in \mathbb{R}$. We denote the set of complex numbers as $\mathbb{C}$. We can proceed to add and multiply complex numbers by treating i a variable, collecting like terms, using the distributive law and remembering that we have defined i^2 be equal to -1. For example

$$\begin{aligned}(1+2i)+(3+4i) &= 1+3+2i+4i \\ &= 4+6i\end{aligned}$$

and

$$\begin{aligned}(1+2i)\cdot(3+4i) &= 1(3+4i)+2i(3+4i) \\ &= 3+4i+6i+8i^2 \\ &= 3+4i+6i-8 \\ &= -5+10i\end{aligned}$$

Throughout this course we have taken the view that mathematics notation and convention is the layer on top of mathematics that permits us to more easily communicate mathematical ideas with one another. Our goal in this module is to develop some of the underlying mathematics that gives meaning to our manipulation of complex numbers. In doing so we find that these numbers permit a geometric interpretation.

We begin our work by recalling some fundamental ideas surrounding trigonometric ratios and radians. Depending on our prerequisite for this course (Foundations 30 or Precalc 30), some or all of this material may be new. (This is okay!) Even if this material is not new for you, it is worth your time to review it. In further sections of this module we were refer specifically to some things appearing below.

Following this, we approach the topic of complex numbers with a bit of a sneak attack by first developing some intuition for a pair of operations defined on elements of $\mathbb{R}^2$. We then formally define complex numbers and see how our work with our operations in $\mathbb{R}^2$ emulate exactly the expected operations we have for addition and multiplication of complex numbers.

We culminate our work with an optional discussion on what is perhaps the most famous mathematical identity of all, Euler's Identity.

$$e^{i\pi}+1=0$$

Aside. *Recall that MATH163 is a foundational course within the Department of Mathematics and Statistics. The topics that appear in this course are meant to be students' first exposure*

to topics that will appear and reappear throughout upper-year courses. You might feel as if we aren't really doing *anything with complex numbers in this module. You are mostly right. The point of this topic being introduced in this course is so that when you see them in future courses, you will be able to focus on their application rather than having to first spent time getting some intuition for them.*

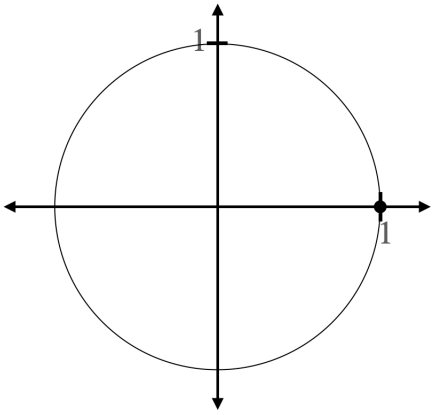
The theory of complex numbers was first developed in the late 16th Century. When first introduced they were cast off by some as being mostly meaningless. (I assume this is why they where given the pejorative name of imaginary*). However, their use became notably interesting once researchers realized that they provided a path to the* Fundamental Theorem of Algebra *– Every polynomial of degree n has, counted with multiplicity, exactly n roots in* $\mathbb{C}$.

9.1 The Unit Circle: Defining Radians and Trigonometric Ratios (Refresher)

This section is designed to remind you of some definitions you may have learned at some point, but may be lost in your memory. In particular we recall the definitions of *radian*, *cosine* and *sine*.

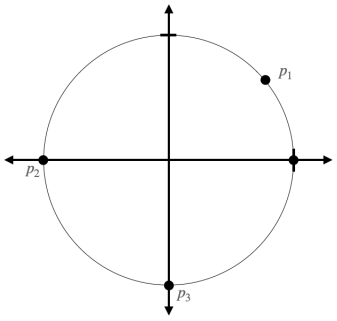
Even if this material is not new for you, it is worth your time to review it. In further sections of this module we were refer specifically to some things appearing below.

Consider a circle of radius 1 centred at the origin of the xy plane:



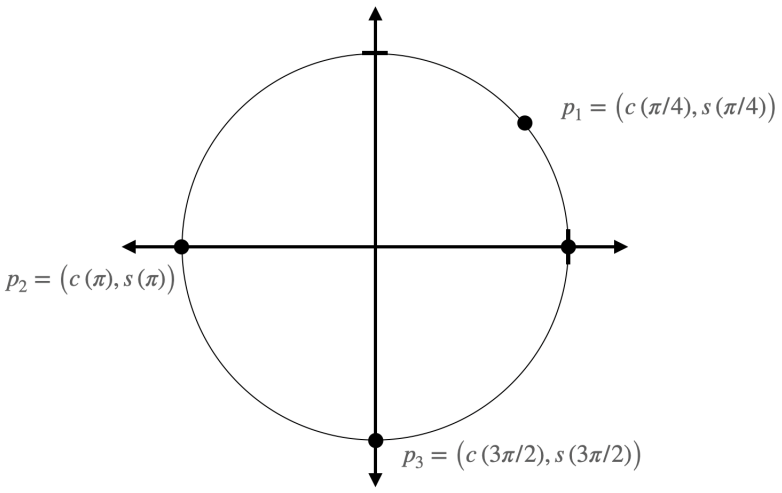
Imagine travelling around the circle anti-clockwise starting from the the indicated point, $(1, 0)$. As you travel around the circle you stop periodically and record how far you have travelled. Since the circle has radius 1, you calculate its circumference to be 2π. And so, for example, when you have travelled one-eighth of the way around the circle you have travelled a total distance of $\frac{1}{8}(2\pi) = \frac{\pi}{4}$. The table below gives the distances d you have travelled to reach the marked points

p	d
p_1	$\frac{\pi}{4}$
p_2	π
p_3	$\frac{3\pi}{2}$



As you travel around the circle you realize that you can associate the coordinates of points on the circle with distance you must travel to get there. Let $c(d)$ denote the the x-coordinate

of the point we reach after travelling distance d. And let $s(d)$ denote the y-coordinate of the point we reach after travelling distance d. For example

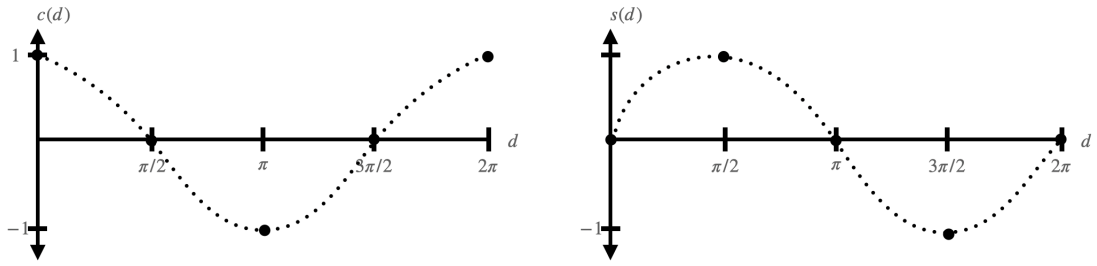


Let us take a moment to investigate these two functions c and s. Computing some values we find

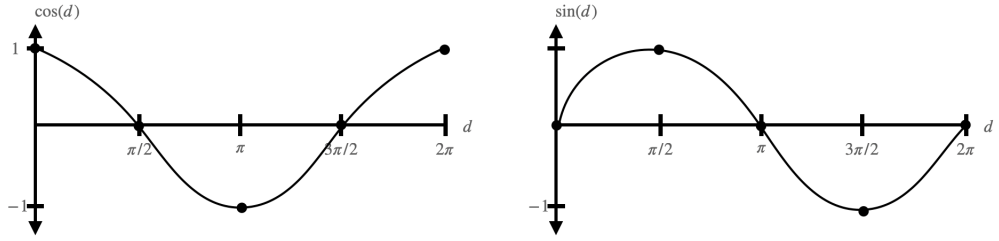
d	$c(d)$	$s(d)$
0	1	0
$\pi/2$	0	1
π	-1	0
$3\pi/2$	0	-1
2π	1	0

(For example, when we have travelled a distance of π anti-clockwise around the circle starting at $(1, 0)$ we have reached $(-1, 0)$)

Eye-balling some curves based on our calculations we have



These functions look awfully familiar. In fact, they are exactly the functions cosine and sine.



Definition 9.4. *For $d \in [0, 2\pi)$, let $\underline{\cos(d)}$ denote the x-coordinate of the point on unit circle reached by travelling distance d anti-clockwise around the circle starting at $(0, 1)$. For $d \in [0, 2\pi)$, let $\underline{\sin(d)}$ denote the y-coordinate of the point on unit circle reached by travelling distance d anti-clockwise around the circle starting at $(0, 1)$.*

Aside. *Yep, sine and cosine have a definition. This is one of a few different equivalent definitions for these functions.*

The word sine *is derived from a Sanskrit word. Its path to the English language comes by way of transliteration of a word into Arabic followed by a subsequent translation of a similar sounding Arabic word to English. The word sine appears in English texts from over 400 years ago.*

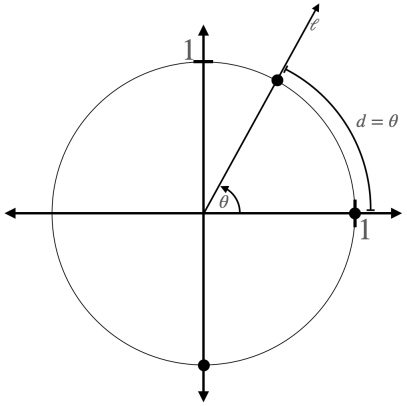
The study of trigonometric functions is ancient and universal. For example, their study appears in work in Greece in the 1st century, in India in the 4th century and in work during the early Golden Age of Islam in the 9th century.

"*But wait!*", we cry. "*Aren't cosine and sine related somehow to angles? How can we define them in terms of the distance around the circle from the point $(1, 0)$?*

For any point (x, y) on the unit circle, consider the line ℓ from the origin through (x, y). Let θ denote the angle that this line makes with the positive x-axis.

Just as we can associate each point on the circle with a distance in the range $[0, 2\pi)$, we can associate this angle θ with this same distance. In fact, we can use this distance as the label for our angle.

Definition 9.5. *Let ℓ be a line with one end at the origin. We denote the angle formed between ℓ and the positive x-axis as θ where $d = \theta$ is the distance around the unit circle from $(1, 0)$ to the point of intersection between ℓ and the unit circle. We call θ the $\underline{\text{radian angle}}$.*



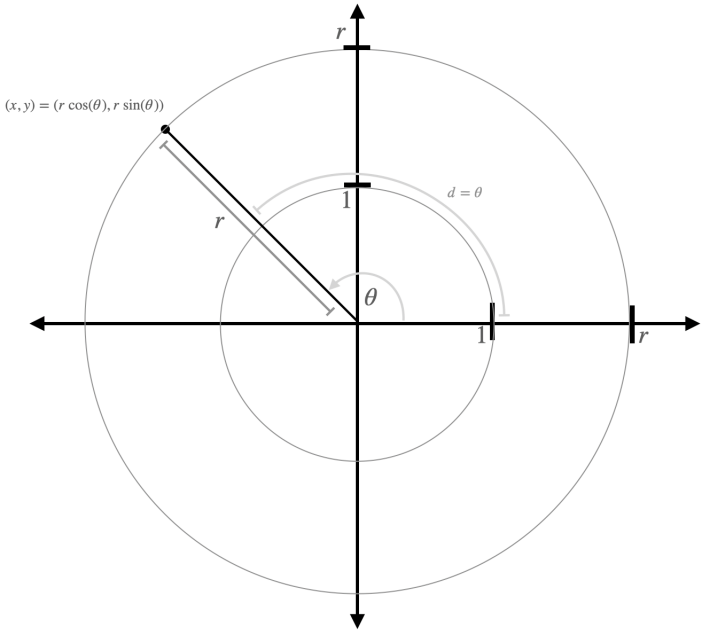
Aside. *Think of a radian angle as multiplying a fraction by 2π. This fraction tells us the distance we must travel around the unit circle to reach the corresponding point. This is a great example of how the mindless "rule" of always reducing fractions their lowest terms can lead to confusion. We write $\pi/4$ to talk about the angle formed walking $1/8$ of the way around the circle. Surely it is more clear to express this angle as $\frac{1}{8}(2\pi)$?*

Just as we denote any point on the unit circle using cosine, sine and radian angle, we may in fact denote any point in $\mathbb{R}^2$ this way.

Theorem 9.6. *For $r > 0$, let C_r be the circle of radius r centred at the origin. And let ℓ be a line through the origin so that the radian angle between the positive x-axis and ℓ is θ. The point of intersection of ℓ and C_r is given by $(r\cos(\theta), r\sin(\theta))$.*

We omit the proof of this fact as there is no assumption in this course that you are familiar with concepts in geometry, such as similar triangles. One may obtain a proof of this theorem by reasoning about similar triangles in the image below and in various related images where

the point of intersection lies in different quadrants.

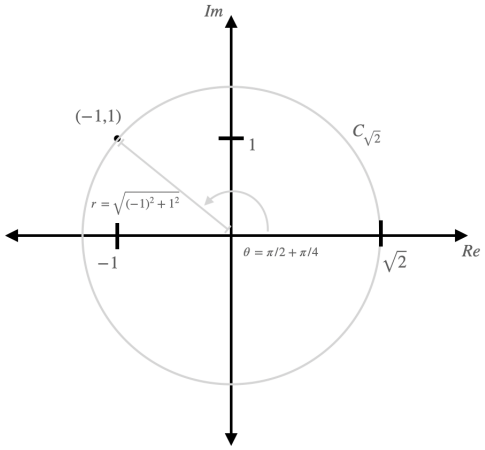


For any point $(x, y) \in \mathbb{R}^2$ there exists a circle centred at the origin that passes through (x, y). And so we have:

Corollary 9.7. *For every $(x, y) \in \mathbb{R}^2$, there exists $r \geq 0$ and $\theta \in [0, 2\pi)$ so that*

$$(x, y) = (r\cos(\theta), r\sin(\theta)).$$

For example, we can express the point $(-1, 1)$ as $(\sqrt{2}\cos(3\pi/4), \sqrt{2}\sin(3\pi/4))$.



Aside. *We have managed to define radian angles without having to invoke degrees. Using* $90°$ *to denote a quarter rotation relies on us having to* remember*, without any intuition, that a full rotation corresponds to* $360°$*. We have chosen as a society to define the full rotation as* $360°$*. That there are* $360°$ *in a full rotation is only* correct *insofar that we have all decided to agree on this convention. (The choice of* 360 *is in fact a good one – there are lots of divisors of* 360*, which makes it easy to express exactly lots of different angles. This is the same reason that* 60 *is a good choice for number of minutes in an hour. Choosing to define there to be* 24 *hours in a day is, however, patently absurd. We can blame ancient Egypt for that.)*

On the other hand we can reason *that* $\pi/8$ *denotes a quarter rotation by remembering only that the ratio between the diameter of a circle and its circumference is denoted as* π*. The only convention that we are required to agree upon to reach a* correct *answer is that we use the symbol* π *to denote this ratio. (We don't even need to know the value of* π*!)*

9.2 Sneaking Up on Complex Numbers

A Note on Section 9.2 *The material in this section is only here to set up material in Section 9.3. The definition of* multiplication *presented herein for elements of $\mathbb{R}^2$ does not match the definitions for product of two elements $\mathbb{R}^2$ we may have learned about in Linear Algebra. This okay as we are not talking about vectors in this section.*

Let us forget for the moment about our quest to understand complex numbers by taking a diversion back into *operations*. Recall the following definition from Module 2:

Definition 9.8. *Let A be a set. An operation on A is a function $f : A \times A \to A$.*

In almost all practical matters we associate a symbol with our operation. For example, we write multiplication of positive integers as $3 \cdot 4$ rather than defining the function $m : \mathbb{N} \to \mathbb{N}$ so that $m(n_1, n_2) = \sum_{i=i}^{n_1} n_2$ and then considering $m(3, 4)$.

Aside. *Collectively we shudder as we remember that difficult question from an early assignment in this class.*

Let us define the following two operations, addition and multiplication, for elements of $\mathbb{R}^2$:

$$(a, b) + (c, d) = (a + c, b + d) \tag{1}$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc) \tag{2}$$

In (1) we are defining a new meaning for addition for two elements $\mathbb{R}^2$. The first appearance of "+" in this line is piece of notation we will us to denote this operation. The second appearance of "+" in this line is referring to our familiar notation for addition of real numbers. The same is true in (2). The first appearance of "$\cdot$" is defining the meaning of this symbol when applied to elements of $\mathbb{R}^2$ in this particular context.

Aside. *Don't think about vectors. This second operation is not the dot product. Unfortunately we re-use symbols depending on context and expect our reader to follow. You won't encounter the use of $\cdot$ for this operation on $\mathbb{R}^2$ anywhere beyond the context of this course, and indeed this module. The choice to use the symbol $\cdot$ here is setting up work in the following section.*

For example

$$(1, 2) + (3, 4) + (1 + 3, 2 + 4) = (4, 6)$$
$$(1, 2) \cdot (3, 4) = (1(3) - 2(4), 1(4) + 2(3)) = (-5, 10)$$

and

$$(0, 1) \cdot (0, 1) = (0 - (1), 0 + 0) = (-1, 0)$$

Though the first operation here seems like a natural definition for addition of elements of $\mathbb{R}^2$, this second operation doesn't seem to be well motivated at all! To try to gain some intuition about this operation, let us explore a little more.

For $(a, b) \in \mathbb{R}$ consider the product $(a, b) \cdot (1, 0)$.

$$(a, b) \cdot (1, 0) = (a - 0, 0 + b) = (a, b)$$

Multiplication by $(1, 0)$ doesn't change anything! Let $e = (1, 0)$. For any $p \in \mathbb{R}^2$ we have

$$p \cdot e = p$$

(Since elements of $\mathbb{R}^2$ are ordered pairs, when we declare $p \in \mathbb{R}^2$ we have that $p = (x, y)$ for some particular $(x, y) \in \mathbb{R}^2$)

This property seems quite familiar to us when we think about the outcome of multiplying elements of $\mathbb{R}$ by 1. Let $e = 1$. For any $p \in \mathbb{R}$ we have

$$p \cdot e = p$$

Looking at our definition for addition we see the same sort of behaviour when we consider the element $(0, 0)$

$$(a, b) + (0, 0) = (a + 0, b + 0) = (a, b)$$

Addition by $(0, 0)$ doesn't change anything! Let $f = (0, 0)$. For any $p \in \mathbb{R}^2$ we have

$$p + f = p$$

Aside. *Prepositions in English are weird. We say* multiplication by*, but saying* addition by *sounds unnatural to the ear of a speaker of English as a first language.*

This property seems quite familiar to us when we think about the outcome of adding 0 to elements of $\mathbb{R}$. Let $f = 0$. For any $p \in \mathbb{R}$ we have

$$p + f = p$$

Our new definition of multiplication and addition for elements of $\mathbb{R}^2$ has some more things in common with our intuition for addition and multiplication of elements in $\mathbb{R}$.

Consider elements of the form $(x, 0)$. For example we have

$$(6, 0) + (4, 0) = (6 + 4, 0 + 0) = (10, 0)$$

and

$$(6, 0) \cdot (4, 0) = (6(4) - 0, 0 + 0) = (24, 0)$$

In general we have

$$(a, 0) + (b, 0) = (a + b, 0)$$

and

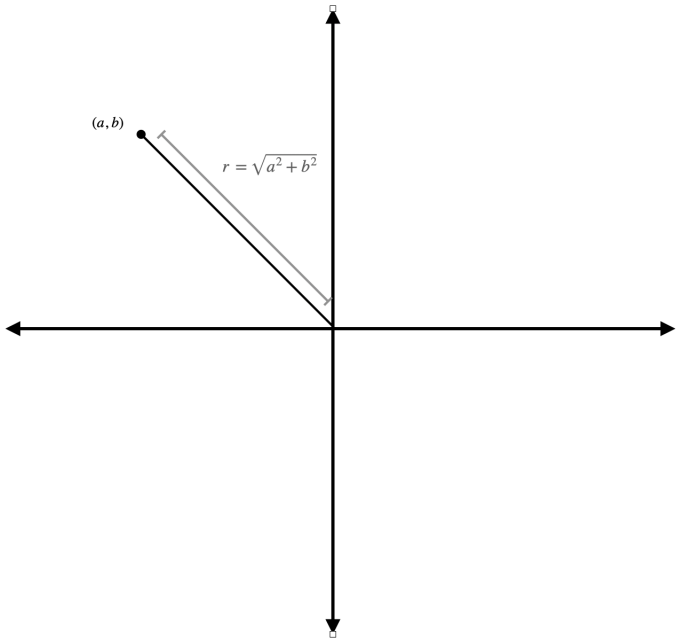
$$(a, 0) \cdot (b, 0) = (ab - 0, 0a + 0b) = (ab, 0)$$

Addition and multiplication on elements $(a, 0)$ and $(b, 0)$ performs exactly the same function as addition and multiplication of a and b. And so we see that when we restrict our second coordinate to be 0, our versions of addition and multiplication for elements of $\mathbb{R}^2$ has the same effect as addition and multiplication in $\mathbb{R}$.

Our new version of multiplication has one last secret in store for us. For $(a, b) \in \mathbb{R}^2$ consider the product $(a, b) \cdot (a, -b)$.

$$(a, b) \cdot (a, -b) = (a^2 + b^2, (-ab) + (ba)) = (a^2 + b^2, 0)$$

Remembering that we are thinking about points in the plane, the expression $a^2 + b^2$ is very familiar!



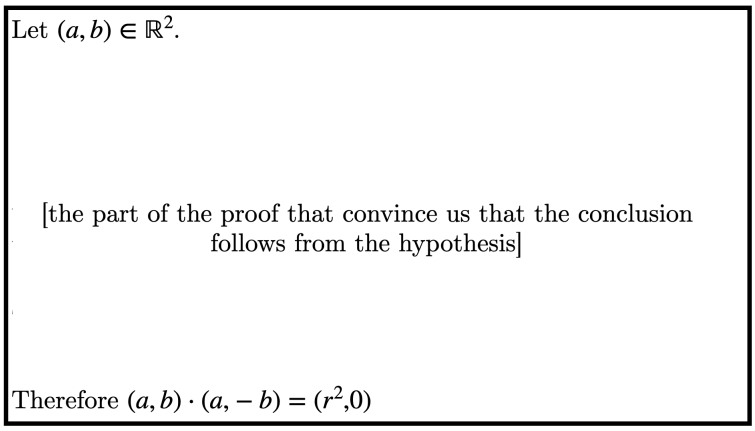
That is

Theorem 9.9. *If* $(a, b) \in \mathbb{R}^2$*, then*

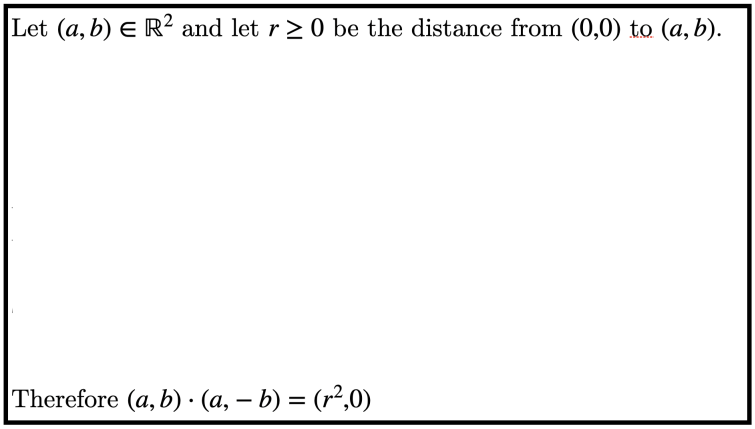
$$(a, b) \cdot (a, -b) = (r^2, 0)$$

where r is the distance from the origin to the point (a, b) in $\mathbb{R}^2$.

Let us take a moment to write out a short proof of this theorem. Since we want to prove something about a product of the form $(a, b) \cdot (a, -b)$ we should begin by introducing these mathematical objects. We want to show $(a, b) \cdot (a, -b) = (r^2, 0)$ and so we know what the last sentence of our proof should be.



We also want to say something about the parameter r, and so we should introduce this to our reader as well.



We want to say something about the product $(a, b) \cdot (a, -b)$ and so we compute it:

Let $(a, b) \in \mathbb{R}^2$ and let $r \geq 0$ be the distance from (0,0) to (a, b).
We compute

$$(a, b) \cdot (a, -b) = (a^2 + b^2, (-ab) + ba) = (a^2 + b^2, 0)$$

Therefore $(a, b) \cdot (a, -b) = (r^2, 0)$

Now to finish our argument, we want to remind our reader of the formula for finding r

Let $(a, b) \in \mathbb{R}^2$ and let $r \geq 0$ be the distance from (0,0) to (a, b).
We compute

$$(a, b) \cdot (a, -b) = (a^2 + b^2, (-ab) + ba) = (a^2 + b^2, 0)$$

Recall

$$r = \sqrt{a^2 + b^2}$$

Therefore $(a, b) \cdot (a, -b) = (r^2, 0)$

Module 9 was supposed to be about complex numbers, but it seems as if we are a long way from our goal of learning about these objects. Before we define complex numbers let us take a quick moment to notice a few things above.

With our definition of multiplication in $\mathbb{R}^2$ the element $(1, 0)$ played the role of 1. This is further emphasized when we noted that elements of the form $(x, 0) \in \mathbb{R}$ behave the same as $x \in \mathbb{R}$ when we think about multiplication. Thinking of elements of $\mathbb{R}$, there is no element x such that $x^2 = -1$. However, when we define multiplication for elements of $\mathbb{R}^2$ we find

$$(0, 1) \cdot (0, 1) = (-1, 0)$$

That is, the equation $x^2 = (-1, 0)$ has a solution: $x = (0, 1)$. When we think about multiplication, the element $(-1, 0)$ in $\mathbb{R}^2$ corresponds to $-1 \in \mathbb{R}$. It sure looks then as if we have found *something* that when squared gives -1. If we label $(0, 1)$ with the label i, then can we write $i^2 = -1$?

9.3 Defining Complex Numbers

If we label $(0, 1)$ with the label i, then can we write $i^2 = -1$? Yes... sort of.

Recall our definition of the rational numbers from Module 1.

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

When we write a rational number, say $\frac{1}{2}$, we are expressing a single quantity. Though the horizontal line in $\frac{1}{2}$ reminds us of division, writing $\frac{1}{2}$ is denoting a single quantity – the value on the number line that is halfway between 0 and 1.

With this thought in our minds, we define the set of complex numbers

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

For example, $3 + 7i$ is a complex number. So is $\frac{1}{2} + (-6)i$. As is $\pi + \pi i$.

Definition 9.10. *For a complex number $z = a + bi$ we say a is the real part of z and b is the imaginary part of z. We denote these parts respectively as $Re(z)$ and $Im(z)$.*

For $z = 3 + 7i$ we have $Re(z) = 3$ and $Im(z) = 7$.

When we write a complex number, say $1 + 2i$, we are expressing a single quantity. Though the plus sign in $1 + 2i$ reminds us of addition, writing $1 + 2i$ is denoting a single quantity – but what quantity is it denoting? To discover this, we first define a pair of operations, addition and multiplication for elements of $\mathbb{C}$.

$$(a + bi) + (c + di) = (a + c) + (b + d)i \tag{3}$$
$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \tag{4}$$

For example

$$(1 + 2i) + (3 + 4i) = (1 + 3) + (2 + 4)i = 4 + 6i$$
$$(1 + 2i) \cdot (3 + 4i) + (1(3) - 2(4)) + (1(4) + 2(3))i = -5 + 10i$$

and

$$(0 + 1i) \cdot (0 + 1i) = (0 - (1)) + (0 + 0)i = 1 + 0i$$

There are lots of + signs hanging out in (3). Let us label them and talk about them one at a time:

$$(1 +_1 2i) +_2 (3 +_3 4i) = (1 +_4 3) +_5 (2 +_6 4)i$$

- $+_1$ is the $+$ we use when we are denoting an element of $\mathbb{C}$.
- $+_2$ is the $+$ we are defining so that we have an agreed upon definition of what it means to add elements of $\mathbb{C}$.
- $+_3$ is the $+$ we use when we are denoting an element of $\mathbb{C}$.
- $+_4$ is the $+$ we use to denote addition of elements of $\mathbb{R}$
- $+_5$ is the $+$ we use when we are denoting an element of $\mathbb{C}$.
- $+_6$ is the $+$ we use to denote addition of elements of $\mathbb{R}$.

Aside. *Noting the different use of the $+$ sign seems very familiar to what we did in the previous section with equation (1). Looking back, we also see that equation (2) and equation (4) are strikingly similar*

This is awful! Why would we use the symbol $+$ to refer to three different things?

Imagine you were teaching someone to add complex numbers without needing for them to really understand what they were doing. (... I suspect such a thing is easy for us to imagine.)

If you showed them

$$(1 + 2i) + (3 + 4i)$$

and then said

Collect like terms.

they would dutifully do so

$$\begin{aligned}(1 + 2i) + (3 + 4i) &= 1 + 3 + 2i + 4i \\ &= 4 + 6i\end{aligned}$$

and arrive at the right answer. Though adding complex numbers looks like we are *collecting like terms*, we aren't in fact doing so. We use the phrase *collecting like terms* to talk about the process of simplifying an expression that contains variables. There are no variables in sight here!

Similarly if you gave them the product

$$(1 + 2i) \cdot (3 + 4i)$$

and told them to use the distributive law, collect like terms and set $i^2 = -1$, they would

find:

$$\begin{aligned}(1+2i)\cdot(3+4i) &= 1(3+4i)+2i(3+4i)\\ &= 3+4i+6i+8i^2\\ &= 3+4i+6i-8\\ &= -5+10i\end{aligned}$$

and arrive at the right answer. Though multiplying complex numbers looks like we are using the distributive law, we aren't in fact doing so. Even though we see a $+$, as discussed above this does not denote addition, but is part of the way we express a complex number.

It is exactly for this convenience that that the mathematics community collectively uses the notation $a+bi$ to denote a complex number. We could just as easily denote a complex number as (a,b), but choosing to denote a complex number as $a+bi$ allows us to ignore the fact that $a+bi$ is an exotic number thing and just pretend that it is a number and that i^2 denotes -1.

Aside. *One of the myths of science education is that the things in the curriculum are objectively true. If you took chemistry in secondary school you probably learned about the Bohr-Rutherford model of an atom. A key feature of this model is that electrons are these tiny little particles that orbit around a nucleus. Once we get to upper-year chemistry in university we learn, in fact, that electrons aren't really particles that can be said to be in any particular place. Instead they exist as a probability cloud.*

The Bohr-Rutherford model of the atom is just that – a model. It gives us the information we need to so that we can more easily learn about other concepts in chemistry without being bogged down by the details. Teaching a student about reduction and oxidation would be very difficult without the Bohr-Rutherford Model!

I suspect the same phenomenon occurs when we teach secondary school students about complex numbers. When we teach students about complex numbers for the first time, they are a tool to solve quadratic equations. And so students are taught that they are collecting like terms and using the distributive law when they manipulate complex numbers. Though this isn't completely true, it still leads to the correct outcome.

When we defined sets we took some time to define carefully what it means for a pair of sets to be equal. As we are using the equals sign in our work with complex numbers we should probably take a moment to think about what equality means for elements of $\mathbb{C}$.

Definition 9.11. *Let $z, z' \in \mathbb{C}$ so that $z = a+bi$ and $z' = c+di$. We write $z = z'$ when $a = c$ and $b = d$.*

Aside. *How does this differ to the meaning of equality for elements of $\mathbb{Q}$. It is certainly*

possible to have $\frac{a}{b} = \frac{c}{d}$*, but have* $a \neq b$ *and* $c \neq d$*.*

Let us take some time to get more familiar with our definitions for multiplication and addition for elements of $\mathbb{C}$.

For $a + bi \in \mathbb{C}$ consider the product $(a + bi) \cdot (1 + 0i)$.

$$(a + bi) \cdot (1 + 0i) = (a - 0) + (0 - (-b)i = a + bi$$

Multiplication by $1 + 0i$ doesn't change anything! Let $e = 1 + 0i$. For any $z \in \mathbb{C}$ we have

$$z \cdot e = p$$

Looking at our definition for addition we see the same sort of behaviour when we consider the element $0 + 0i$

$$(a + bi) + (0 + 0i) = (a + 0) + (b + 0)i = a + bi$$

Addition by $0 + 0i$ doesn't change anything! Let $f = 0 + 0i$. For any $z \in \mathbb{C}$ we have

$$z + f = p$$

Aside. *Prepositions in English are weird. We say* multiplication by*, but saying* addition by *sounds unnatural to the ear of a speaker of English as a first language.*

Our new definition of multiplication and addition for elements of $\mathbb{C}$ has some more things in common with our intuition for addition and multiplication of elements in $\mathbb{R}$.

Consider elements of the form $(a + 0i)$. For example we have

$$(6 + 0i) + (4 + 0i) = (6 + 4) + (0 + 0)i = 10 + 0i$$

and

$$(6 + 0i) + (4 + 0i) = (6(4) - 0) + (0 + 0)i = 24 + 0i$$

In general we have

$$(a + 0i) + (b + 0i) = (a + b) + 0i$$

and

$$(a + 0i) \cdot (b + 0i) = ab + 0i$$

Addition and multiplication on elements $a+0i$ and $b+0i$ performs exactly the same function as addition and multiplication of a and b. And so we see that when we restrict to complex numbers z with $Im(z) = 0$, our version of addition and multiplication for elements of $\mathbb{C}$ has the same effect as addition and multiplication in $\mathbb{R}$. We take advantage of this similarity by

not writing a real or imaginary part when it is equal to 0. For example, rather than writing $6 + 0i$ we can just write 6. In this same vein, rather than writing $0 + 7i$ we can just write $7i$

Looking back to one of our examples from above we had:

$$(0 + 1i) \cdot (0 + 1i) = (0 - 1) + (0 + 0)i = -1 + 0i$$

Using our convention of dropping the zero parts of the imaginary number we write:

$$(1i) \cdot (1i) = -1$$

For variables with coefficient 1 we write x in place of $1x$. Adopting the same convention here yields

$$i \cdot i = -1$$

When we multiply a real number by itself we write n^2 rather than $n \cdot n$. Applying this same convention yields

$$i^2 = -1$$

Having $i^2 = -1$ was not part of our definition of complex numbers. It arose as a consequence of our definition of multiplication for elements of $\mathbb{C}$ and adopting conventions for expressing elements of $\mathbb{C}$ that we use in other domains of mathematics.

With our convention that we write elements of the form $a + 0i$ just as a, we then realize we may in fact interpret every real number as a complex number whose imaginary part is 0. And so we have $\mathbb{R} \subset \mathbb{C}$.

Looking back at the work we did in Section 9.2, this all seems quite repetitive! Our definition for addition and multiplication of elements of $\mathbb{R}^2$ seems very similar how we defined these concepts for elements of $\mathbb{C}$. The only real difference here seems to be a matter of notation. An element $(a, b) \in \mathbb{R}^2$ and the element $a + bi \in \mathbb{C}$ seem to act the same when we perform multiplication and addition. In fact, we can consider these as two different notations to refer to the same thing.

It was here in our work in Section 9.2 we looked at the product $(a, b) \cdot (a, -b)$ and proved it was equal to $(r^2, 0)$ where r was the distance from the origin to (a, b) in $\mathbb{R}^2$. At this point we wonder if we can do the same thing for elements of $\mathbb{C}$ and products of the form $(a+bi)\cdot(a+(-b)i)$. A problem arises when we realize we have no meaning for the word *origin* or *distance* when we talk about elements of $\mathbb{C}$. These concepts arise from our knowledge of the Cartesian Plane. And so to arrive at a meaningful interpretation of the product $(a + bi) \cdot a + (-b)i$, we first define the *Complex Plane*.

The Complex Plane consists of two axes, the real axis, which is horizontal, and the imaginary axis, which is vertical. Each axis is indexed by $\mathbb{R}$ according to the usual total order on this set. The point of intersection of the vertical line through a on the real axis and the horizontal line though b on the imaginary axis is denoted as $a + bi$. (See the picture on the following page.)

We can now define an analogy for distance in the complex plane.

Definition 9.12. *Let $z = a + bi$ be a complex number. The magnitude of z is the length of the line from $0 + 0i$ to $a + bi$ in the complex plane. We denote this quantity as $|z|$. This quantity is given by the formula*

$$|z| = \sqrt{a^2 + b^2}$$

For example, when $z = 3 + 4i$ we have.

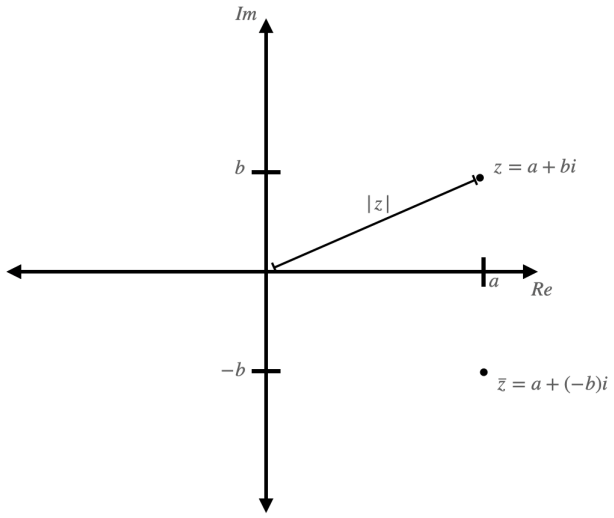
$$|z| = \sqrt{3^2 + 4^2} = 5$$

Aside. *When we defined multiplication in $\mathbb{R}^2$ a short aside told you not to think of these points as vectors as the product we were defining was not the same as the dot product. Thinking of elements of $\mathbb{C}$ as vectors in the Complex Plane is a good mental model. It makes it much easier to understand the meaning of magnitude as the length of a vector.*

When we looked at our multiplication operation for $\mathbb{R}^2$ we related the product $(a, b) \cdot (a, -b)$ to the distance from the origin to (a, b). With this same goal in mind for elements of $\mathbb{C}$, we have the following definition.

Definition 9.13. *Let $z = a + bi$ be a complex number. The complex conjugate of z is the complex number $a + (-b)i$. We denote this quantity as $\overline{z}$. That is, we define*

$$\overline{z} = a + (-b)i$$



Putting these pieces together, we arrive at our analogue for Theorem 9.9 for complex numbers.

Theorem 9.14. *For every $z \in \mathbb{C}$ we have*

$$|z|^2 = z \cdot \overline{z}$$

Proof. Let $z = a + bi$ be a complex number. By definition, $\overline{z} = a + (-b)i$. We compute

$$z \cdot \overline{z} = (a + bi) \cdot (a + (-b)i) = a^2 + b^2 + 0i = a^2 + b^2$$

Recall $|z| = \sqrt{a^2 + b^2}$. Therefore $z \cdot \overline{z} = |z|^2$. □

In Section 9.1 we spent some time reviewing some trigonometric concepts. Given that the Complex Plane seems to only differ from the Cartesian Plane in the names of the axes and how we label the points, our work in defining sine, cosine and radians extends to the complex plane.

Since every $(a, b) \in \mathbb{R}^2$ can be expressed as

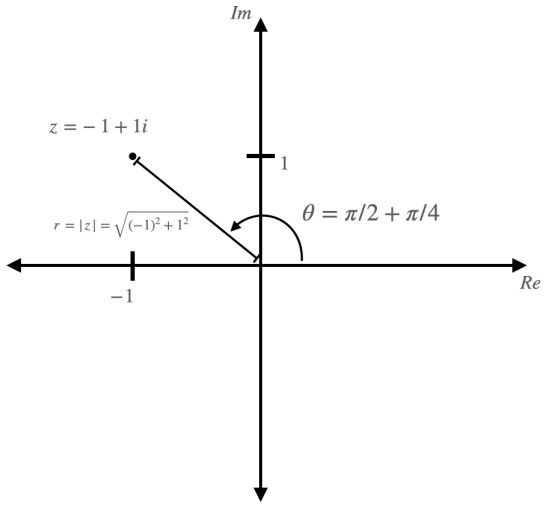
$$(r\cos(\theta), r\sin(\theta))$$

so too can we express a complex number in this way.

Theorem 9.15. *For every $z \in \mathbb{C}$, there exists $r \geq 0$ and $\theta \in [0, 2\pi]$ so that*

$$z = r\cos(\theta) + i\,(r\sin(\theta))$$

Example 9.16. *Let $z = -1 + 1i$. Find r and θ so that $z = r\cos(\theta) + i\,(r\sin(\theta))$.*
With a quick sketch we see $r = |z| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}$ and $\theta = \pi/2 + \pi/4 = 3\pi/4$.



And so

$$z = \sqrt{2}\cos(3\pi/4) + i\left(\sqrt{2}\sin(3\pi/4)\right)$$

Aside. *Notice that we have written* $i\,(r\sin(\theta))$ *rather than writing* $(r\sin(\theta))\,i$ *for the imaginary part of* z *in the statement of this theorem. The only reason to do this is convention. Writing* $(r\sin(\theta))\,i$ *in the statement of this theorem would carry the same meaning.*

Theorem 9.16 tells us that for each complex number $z = a + bi$ there is a pair (r, θ) so that $z = r\cos(\theta) + i\,(r\sin(\theta))$. And so instead of denoting a complex number by reference to its position in the complex plane, which is what we do when we write $z = a + bi$, we could instead denote a complex number with the pair (r, θ). Such a coordinate system is called *Polar Coordinates.* For example, we could refer to $z = -1 + 1i$ with the pair $(\sqrt{2}, 3\pi/4)$. If you take further courses in calculus beyond the 100-level, such coordinates will make an appearance.

At the start of this section we looked at the notation for $\mathbb{Q}$ and noted that even though $\frac{1}{2}$ looks like division, in fact it represents a singular quantity – the point on the real number line that is halfway between 0 and 1. We then wondered, what quantity does $a + bi$ represent? We now have the tools to answer this question. The quantity $a + bi$ is the point in the complex plane where the lines $Re(z) = a$ and $Im(z) = b$ intersect. In this same vein, we can interpret a quantity $s \in \mathbb{R}$ as the point in the complex plane where the lines $Re(z) = s$ and $Im(z) = 0$ intersect.

Aside. *If you read the material on graph isomorphism in the Module 8, recognize that when we thinking about addition and multiplication we defined respectively for* $\mathbb{R}^2$ *and* $\mathbb{C}$*, the only difference is the labels we use for the elements of the set. As the only difference between these two structures is the labelling, there is an isomorphism between* $\mathbb{R}^2$ *and* $\mathbb{C}$ *that preserves the structure of these operations.*

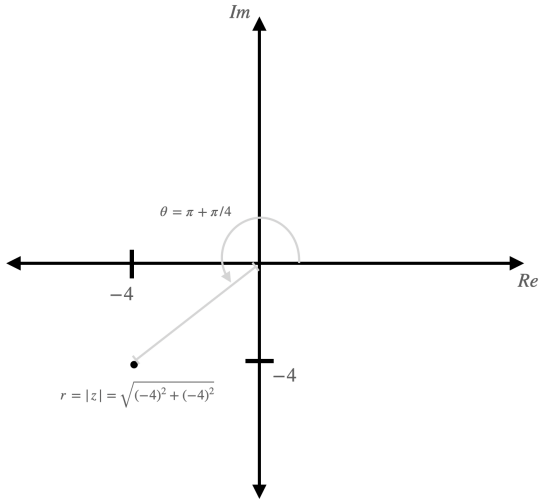
If you are taking MATH 362 next term, you will come to recognize this as a ring isomorphism*.*

Test Your Understanding

1. Let $z = 6 + 8i$ and $z' = 4 + 2i$.
   (a) Compute $z + z'$.
   (b) Compute $z \cdot z'$.
   (c) Compute $|z|$.
2. Let $z = -4 + (-4)i$. Find r and θ so that $z = r\cos(\theta) + ir\sin(\theta)$.

Test Your Understanding Solution

1. Let $z = 6 + 8i$ and $z' = 4 + 2i$.
   (a) We have $z + z' = z + z' = (6 + 8i) + (4 + 2i) = 10 + 10i$
   (b) We have $z \cdot z' = z \cdot z' = (6 + 8i) \cdot (4 + 2i) = 8 + 44i$
   (c) Compute $|z| = |z| = \sqrt{6^2 + 8^2} = \sqrt{36 + 64} = 10$
2. Let $z = -4 + (-4)i$. We sketch



And so we see $r = |z| = \sqrt{32} = 4\sqrt{2}$ and $\theta = \pi + \pi/4 = 5\pi/4$. Therefore

$$z = 4\sqrt{2}\cos(5\pi/4) + i4\sqrt{2}\sin(5\pi/4)$$

9.4 Euler's Identity (Optional)

A Note About Section 9.4 *Various parts of our work in this section invoke concepts that are beyond what is explicitly appears in the stated pre-requisites for this course. In particular, we lean on some knowledge of derivatives and the exponential function e^x. This material is included here because most students in this class have taken or are currently taking a first-year course in calculus. There is no expectation that every student has a sufficient background to follow all of the work below. The statement of Theorem 9.19 is particularly important if you are planning on taking second year calculus courses (MATH226/226 or MATH276/277)*

You will not be assessed on any of the material that appears in this section

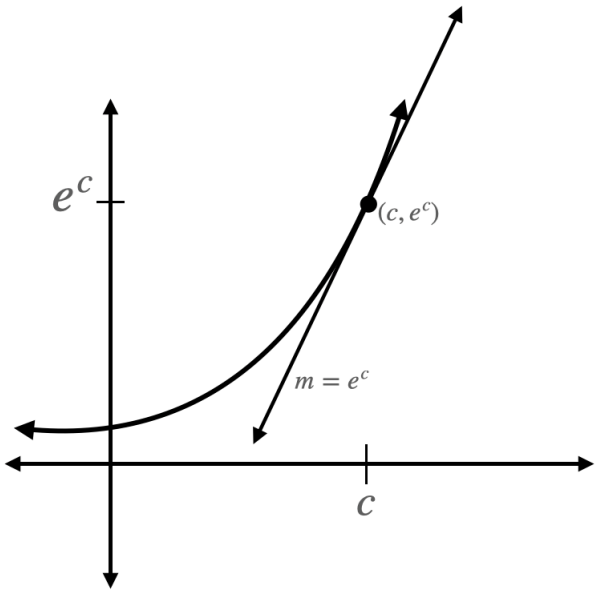
With our work on preliminary notions for complex numbers behind us, we now return to Euler's Identity:

$$e^{i\pi} + 1 = 0$$

Subtracting 1 from both sides of the equality yields

$$e^{i\pi} = -1$$

Recall e^x is defined to be the unique exponential function for which $\frac{d}{dx}e^x = e^x$. That is, for any $c \in \mathbb{R}$ to tangent line to the curve e^x and $x = c$ has slope e^c.



Following our work above, recall that angles can measured with values in the range $[0, 2\pi)$. In our approach to understanding Euler's Identity, we will think of the π that appears as an angle.

Instead of studying Euler's Identity directly, we consider a function $f : [0, 2\pi) \to \mathbb{C}$ where

$$f(\theta) = e^{i\theta}$$

To show Euler's Identity is true, it suffices to show $f(\pi) = -1 + 0i$.

Before we get down to some abstract nonsense, let us stop for a moment and consider a practical and seemingly unrelated matter: how does a calculator work?

If you pick up a calculator and punch in $e^{1.7}$ you get

$$e^{1.7} \approx 5.4739473917$$

As we can punch in just about any exponent that we want and get an immediate answer suggests to us that our calculator has not stored all possible values of the function e^x in its memory. There are infinitely many choices for x and the calculator has only finite memory.

Calculators in fact provide estimates of these values by computing a function $g : \mathbb{R} \to \mathbb{R}$ so that the difference between $g(c)$ and e^c is imperceptibly small for every $c \in \mathbb{R}$. One way to estimate e^x is by using a polynomial.

From our work above, we know two important features about e^x:

1. $e^0 = 1$; and
2. $\frac{d}{dx}e^x = e^x$

To try to express e^x as a polynomial of degree n let us try to find a polynomial that also has these two features. Let $h(x) : \mathbb{R} \to \mathbb{R}$ so that

$$h(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

with coefficients $a_i \in \mathbb{R}$ for all $1 \leq i \leq n$. If this function is to be equal to e^x, then it must satisfy the two properties above

1. If $h(0) = 1$, then $a_0 + a_1(0) + a_2(0)^2 + \cdots + a_n(0)^n = 1$ and so $a_0 = 1$.
2. $h'(x) = h(x)$, then

$$a_1 + 2a_2x + 3a_3x^3 + \cdots + na_nx^{n-1} = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

Here we see a problem: $h(x)$ has degree n and $h'(x)$ has degree $n - 1$. And so it cannot be that $h(x) = h'(x)$. It doesn't seem possible to express e^x as a polynomial.

However, if we allow ourselves to think of a polynomial with infinitely many terms, new hope emerges of expressing e^x has a polynomial. Consider

$$h(x) = \sum_{i=0}^{\infty} a_ix^i = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots$$

Following our reasoning above, we have $a_0 = 1$. If $h(x) = e^x$, then $h'(x) = h(x)$. Consider

$$h(x) = a_0 + a_1x + a_2x^2 + \ldots$$
$$h'(x) = a_1 + 2a_2x + 3a_3x^2 + \ldots$$

If these two polynomials are equal, then corresponding terms must have equal coefficients. For every $i \geq 0$ the coefficient of x^i in $h(x)$ must be the same as the coefficient in $h'(x)$. And so we arrive at the following system of equations.

$$\begin{aligned} a_0 &= a_1 \\ a_1 &= 2a_2 \\ a_2 &= 3a_3 \\ a_3 &= 4a_4 \\ a_4 &= 5a_5 \\ &\vdots \end{aligned}$$

On the left are the coefficients of terms in $h(x)$. On the right are the corresponding coefficients in $h'(x)$.

For the first equality, we notice that since $a_0 = 1$, we have $a_1 = 1$. And now for the second equality, since $a_1 = 1$, we have $a_2 = \frac{1}{2}$. Continuing on in this matter, since $a_2 = \frac{1}{2}$ we have $a_3 = \frac{1}{2\times 3}$. Since $a_3 = \frac{1}{2\times 3}$ we have $a_4 = \frac{1}{2\times 3\times 4}$. In general we find

$$a_k = \frac{1}{k!}$$

for all $k \geq 1$. (We could prove this using induction if we were so inclined.)

And so we have

$$h(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} \ldots$$

Throwing around infinite sums without taking too much care to think about what they mean probably isn't the most logically sound thing for us to have done. Let us test our outcome by comparing the value of $h(1)$ with e^1 to see if our symbol manipulation has any real meaning.

Of course we cannot compute $h(1)$ exactly as it has infinitely many terms. And so let us truncate this sum after six terms. We find

$$\begin{aligned} 1 + 1 + \frac{1^2}{2!} + \frac{1^3}{3!} + \frac{1^4}{4!} + \frac{1^5}{5!} &= 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} \\ &= 2 + \frac{60}{120} + \frac{20}{120} + \frac{5}{120} + \frac{1}{120} \\ &= 2 + \frac{86}{120} \\ &= 2.71\overline{6} \end{aligned}$$

When we compare $2.71\overline{6}$ with $e^1 \approx 2.718$ we find this is a very close approximation! If we were to take more than the first six terms of this sum, our approximation would improve.

And so, we are moderately convinced that we can write

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

where we choose to define $0! = 1$ so that we may express this as a single sum.

Aside. *If you have studied Taylor Series before – yes, this is the Taylor Series for e^x at $a = 0$.*

Returning from our diversion on calculators back to our study of complex numbers, we can now make a little bit more sense of $e^{i\theta}$.

$$\begin{aligned} e^{i\theta} &= \sum_{k=0}^{\infty} \frac{(i\theta)^k}{k!} \\ &= 1 + (i\theta) + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \dots \\ &= 1 + i\theta + \frac{i^2\theta^2}{2!} + \frac{i^3\theta^3}{3!} + \dots \end{aligned}$$

Aside. *This is a bit sketchy, no? What does it mean to evaluate e^x a complex point $x \in \mathbb{C}$?*

Computing powers of complex numbers using the identity $i^2 = -1$, we find:

t	i^t
1	i
2	-1
3	$-i$
4	1
5	i
6	-1
7	$-i$
8	1
$\vdots$	$\vdots$

The value of i^t seems to depend on the remainder when t is divided by 4

t	i^t
$4\ell + 1$	i
$4\ell + 2$	-1
$4\ell + 3$	$-i$
4ℓ	1

And so returning to our expression for $e^{i\theta}$ as an infinite sum we find.

$$e^{i\theta} = 1 + i\theta + \frac{-1\theta^2}{2!} + \frac{-i\theta^3}{3!} + \frac{1\theta^4}{4!} + \frac{i\theta^5}{5!} + \frac{-1\theta^6}{6!} + \frac{-i\theta^7}{7!} + \frac{1\theta^8}{8!} \dots$$

Each of the terms has one of $i, -1, -i$ or 1 in the numerator.

- Terms with i in the numerator correspond to indices that have remainder 1 when dividing by 4. The index of such terms are of the form $4\ell + 1$.
- Terms with -1 in the numerator correspond to indices that have remainder 2 when dividing by 4. The index of such terms are of the form $4\ell + 2$.
- Terms with $-i$ in the numerator correspond to indices that have remainder 3 when dividing by 4. The index of such terms are of the form $4\ell + 3$.
- Terms with 1 in the numerator correspond to indices that have remainder 0 when dividing by 4. The index of such terms are of the form 4ℓ.

And so we may group the terms based on their index as follows

$$e^{i\theta} = \sum_{\ell=0} \frac{\theta^{4\ell}}{(4\ell)!} + i\sum_{\ell=0} \frac{\theta^{4\ell+1}}{(4\ell+1)!} + \sum_{\ell=0} -\frac{\theta^{4\ell+2}}{(4\ell+2)!} + i\sum_{\ell=0} -\frac{\theta^{4\ell+3}}{(4\ell+3)!}$$

Aside. *Don't be put off by this part! It is not as confusing at it looks. Write out the first few terms* $\sum_{\ell=0} \frac{\theta^{4\ell+1}}{(4\ell+1)!}$.

If you have studied infinite series before, this reordering of the terms may make you uneasy. What does absolute convergence even mean here? How can we take a limit of complex numbers?

Let

$$c(\theta) = \sum_{\ell=0} \frac{\theta^{4\ell}}{(4\ell)!} - \sum_{\ell=0} \frac{\theta^{4\ell+2}}{(4\ell+2)!}$$

and

$$s(\theta) = \sum_{\ell=0} \frac{\theta^{4\ell+1}}{(4\ell+1)!} - \sum_{\ell=0} \frac{\theta^{4\ell+3}}{(4\ell+3)!}$$

And so we have $e^{i\theta} = c(\theta) + i\ s(\theta)$

Aside. *If* $c(\theta), s(\theta) \in \mathbb{R}$*, then* $e^{i\theta}$ *looks a lot like a complex number expressed so that the real part is a function of an angle and the imaginary part is also a function of an angle. This looks a lot like how we can express a complex number using Theorem 9.15*

Just as we have $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$, it turns out that $c(\theta)$ and $s(\theta)$ are functions that are very well known to us. That they are functions of an angle should lead to us to suspect they may be related to trigonometric functions. By evaluating these functions at 0 and computing their derivatives, their identities are revealed!

$$\begin{aligned} c(0) &= 1 + \sum_{\ell=1} \frac{0^{4\ell}}{(4\ell)!} - \sum_{\ell=0} \frac{0^{4\ell+2}}{(4\ell+2)!} = 1 \\ s(0) &= \sum_{\ell=0} \frac{0^{4\ell+1}}{(4\ell+1)!} - \sum_{\ell=0} \frac{0^{4\ell+3}}{(4\ell+3)!} = 0 \end{aligned}$$

$$\begin{aligned} c'(\theta) &= 0 + \sum_{\ell=1} \frac{(4\ell)\theta^{4\ell-1}}{(4\ell)!} - \sum_{\ell=0} \frac{(4\ell+2)\theta^{4\ell+1}}{(4\ell+2)!} \\ &= \sum_{\ell=1} \frac{\theta^{4\ell-1}}{(4\ell-1)!} - \sum_{\ell=0} \frac{\theta^{4\ell+1}}{(4\ell+1)!} \\ &= \sum_{\ell=0} \frac{\theta^{4\ell+3}}{(4\ell+3)!} - \sum_{\ell=0} \frac{\theta^{4\ell+1}}{(4\ell+1)!} \\ &= -s(\theta) \end{aligned}$$

Aside. *Again, don't be put off by the manipulation of these sums. To see how one line follows from the previous write out a few terms of the sums. Pay attention to how the starting value for ℓ changes between the second and third lines.*

Similarly we can show $s'(\theta) = c(\theta)$.

From previous work on trigonometric ratios we may recall:

$$\begin{aligned} \cos(0) &= 1 \\ \sin(0) &= 0 \\ \frac{d}{d\theta}\cos(\theta) &= -\sin(\theta) \\ \frac{d}{d\theta}\sin(\theta) &= \cos(\theta) \end{aligned}$$

The relationship between $c(\theta)$ and $s(\theta)$ is exactly the relationship between $\cos(\theta)$ and $\sin(\theta)$. And in fact we have

$$\begin{aligned} \cos(\theta) &= \sum_{\ell=0} \frac{\theta^{4\ell}}{(4\ell)!} - \sum_{\ell=0} \frac{\theta^{4\ell+2}}{(4\ell+2)!} \\ \sin(\theta) &= \sum_{\ell=0} \frac{\theta^{4\ell+1}}{(4\ell+1)!} - \sum_{\ell=0} \frac{\theta^{4\ell+3}}{(4\ell+3)!} \end{aligned}$$

Aside. *We don't have the tools in this course to prove this directly. This hand-waving argument comparing the function values at* 0 *and comparing the derivatives will have to suffice.*

Recalling $e^{i\theta} = c(\theta) + i\ s(\theta)$, we conclude

Theorem 9.17 (Euler's Formula)**.**

$$e^{i\theta} = cos(\theta) + i\sin(\theta)$$

Recalling that $\theta \in [0, 2\pi)$ is a variable in the statement of Euler's Formula, we consider $\theta = \pi$

$$\begin{aligned} e^{i\pi} &= cos(\pi) + i\sin(\pi) \\ &= -1 + 0i \\ &= -1 \end{aligned}$$

And so

Corollary 9.18 (Euler's Identity)**.**

$$e^{i\pi} + 1 = 0$$

Though we have no way to justify it, multiplication by a constant works as we expect in this context, and so we have

Theorem 9.19. *For every* $r \geq 0$ *and every* $\theta \in [0, 2\pi)$ *we have*

$$re^{i\theta} = rcos(\theta) + i\ r\sin(\theta)$$

Corollary 9.20. *For every* $z \in \mathbb{C}$ *there exists* $r \geq 0$ *and* $\theta \in [0, 2\pi)$ *so that* $z = re^{i\theta}$

Returning to Example 9.16 we have

$$z = -1 + 1i = \sqrt{2}\cos(3\pi/4) + i\left(\sqrt{2}\sin\left(3\pi/4\right)\right) = \sqrt{2}e^{i\frac{3\pi}{2}}$$

Aside. *Euler (pronounced* oiler*) was a Swiss Mathematician. He derived this formula in the mid 18th Century using exactly this method – by manipulation known representations of* $\cos(x)$, $\sin(x)$ *and* e^x *as infinite sums.*

It wasn't for another fifty years that the connection was made between Euler's Formula and an interpretation of complex numbers as points in the complex plane. This connection was made by Scandinavian mathematician, Caspar Wessel.

Aside. *This section is full of sketchy looking mathematics! How do we make meaning of a polynomial with an infinite number of terms? How do we know that our ability to differentiate functions extends to polynomials with infinitely many terms? When we first learned about the function e^x it had domain $\mathbb{R}$, how can we evaluate it for $x \in \mathbb{C}$?*

These sorts of topics are covered in upper-year mathematics courses. Infinite sequences and estimating functions using polynomials appear in second-year calculus courses. Work on functions of complex variables appear in MATH 379.

---

10 Set Cardinality Part I

Learning Incomes.

- *Recall the definitions of injection, surjection and bijection*
- *Be fluent with set notation*

Learning Outcomes.

- *Understand the steps needed to show* $|A| = |B|$.
- *Understand the meaning of the notation* $|A| = k$.

Newly Defined Terms and Notation.

- *cardinality,* $|A| = k$, $|A| = |B|$, $\lceil k \rceil$, *binary string of length* n.

All the way back on Assignment 1 we grappled with the following question.

> (b) Using your observations from part (a), can you make any statements that relate the existence of injections, surjections and bijections and the number of elements in a domain and codomain? You do not need to show that your statements are correct. (*3 marks*)

In our work we deduced, informally, that a bijection can only exist between sets that have the same number of elements. Perhaps this is an idea that was intuitive to us, or perhaps it was a hard won battle with notation and definition. In either case, we return to this topic in Module 10. We define some notation that allows us to incorporate these ideas our language of mathematics. In doing so, we run up against some unexpected consequences of some seemingly straightforward definitions.

We begin by developing two definitions that allow us to speak more carefully of the number of elements in a set.

The act of counting is probably the first *mathematical task* that any of us encounter. Think about the act of counting how many there are of some object. As you enumerate each of the objects you are counting, you say aloud $1, 2, 3, \ldots$ *etc.*. Though you have never realized it before, you are constructing a function. The image of each object you count is the number you are assigning it it.

For this end we define the following notation.

Definition 10.1. *Let* $\lceil 0 \rceil = \{\}$. *For every* $n \geq 1$ $[n]$, *let* $\lceil n \rceil = \{1, 2, 3, 4, \ldots, n\}$.

For example

$$\lceil 7 \rceil = \{1, 2, 3, 4, 5, 6, 7\}$$

We use the term *cardinality* to describe the number of elements in a set.

Definition 10.2. *Let A be a set and let $k \geq 1$ be an integer. We say A has cardinality k when A there is a bijection $f : A \to \lceil k \rceil$. When A has cardinality k we write $|A| = k$. When $A = \{\}$ we write $|A| = 0$.*

As an example, consider the set

$$B = \{00, 11, 10, 01\}$$

Consider the function: $f : B \to \{1, 2, 3, 4\}$ given by $f(00) = 1, f(11) = 2, f(10) = 3, f(01) = 4$. This is a bijection and so $|B| = 4$. The set B has cardinality 4.

Aside. *Yes, it is obvious that B has four elements. As we have seen throughout this course, it is good to start with obvious examples so that we may be able to build some intuition before we encounter more treacherous mathematical terrain.*

Back on Assignment 1 we talked about the existence and non-existence bijections based on the number of elements in the respective sets. With this in mind, we have the following definition.

Definition 10.3. *Let A and B be sets. We say A and B have the same cardinality when there exists a bijection $f : A \to B$. When A and B have the same cardinality we write $|A| = |B|$.*

Aside. *This may seem like an odd definition to choose to have. Why do we not prove that $|A| = |B|$ when there is a bijection $f : A \to B$? To begin to answer this question consider the following question – does there exist an integer $k \geq 0$ so that $|\mathbb{N}| = k$? By defining $|A| = |B|$ as above we have the flexibility in our notation to talk about two infinite sets to have the same cardinality. We consider this further below in these notes.*

Using Definition 10.3 we can count the number of objects in a set by showing it has the same cardinality as a set whose cardinality we know.

As a first example of an interesting mathematical object we can count with this technique, we consider binary strings – that is, sequences of 0 and 1s. Binary strings are ubiquitous in the computing sciences. At a fundamental level, computers store and transmit data as binary strings.

Definition 10.4. *Let $n \geq 1$ be an integer. A binary string of length n is a sequence of length n where each entry is either 0 or 1.*

For example, 010011 is a binary string of length six. We can index the entries in a binary string starting from the left:

$$b_1 b_2 \cdots b_{n-1} b_n$$

For example, for $b = 1110$ we have: $b_1 = 1, b_2 = 1, b_3 = 1$ and $b_4 = 0$. Let B_n be the set of all binary strings of length n. We have

$B_1 = \{0, 1\}$
$B_2 = \{00, 01, 10, 11\}$
$B_3 = \{000, 001, 010, 100, 011, 101, 110, 111\}$
$B_4 = \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111, 1000, 1001, 1010, 1100, 1011, 1101, 1110, 1111\}$

As we are thinking about cardinality let us take a moment to write down the cardinality of each of these sets.

$$|B_1| = 2$$
$$|B_2| = 4$$
$$|B_3| = 8$$
$$|B_4| = 16$$

Noticing here that the numbers on the right are all powers of two, it seems we have $|B_n| = 2^n$. We confirm this for $n = 5$ by finding a bijection from B_5 to a set that we already know has 2^5 elements, the power set of a set with 5 elements!

Let $f_5 : \mathbf{2}^{\lceil 5 \rceil} \to B_5$ be a function so that the image of a subset $A \subseteq \lceil 5 \rceil$ is a binary string of length 5 so that for all $1 \leq i \leq 5$ we have

$$b_i = \begin{cases} 1 & i \in A \\ 0 & i \notin A \end{cases}$$

For example $f_5(\{2, 3, 5\}) = 01101$ and $f_5(\{\}) = 00000$.

To show $|B_5| = |\mathbf{2}^{\lceil 5 \rceil}| = 2^5$ we show f_5 is a bijection. To show f_5 is a bijection we show that f_5 is both an injection and a surjection.

To show f_5 is an injection we must show that for all subsets $A, B \subseteq \lceil 5 \rceil$ with $A \neq C$ we have $f(A) \neq f(C)$. If $A \neq C$ then there exists an element of A that is not an element of C. Let $k \in \lceil 5 \rceil$ so that $k \in A$ but $k \notin C$. Let $f(A) = a_1 a_2 a_3 a_4 a_5$ and $f(C) = c_1 c_2 c_3 c_4 c_5$. Since $k \in A$ we have $a_k = 1$. Since $k \notin C$ we have $c_k = 0$. Therefore $f(A) \neq f(C)$.

To show f_5 is a surjection we must show that for all $b \in B_5$ there exists $B \subseteq \lceil 5 \rceil$ so that $f(B) = b$. For $b \in B_5$ consider the set

$$B = \{k \mid b_k = 1, k \in \lceil 5 \rceil\}$$

For example, if $b = 01001$ *we have* $b_1 = 0, b_2 = 1, b_3 = 0, b_4 = 0, b_5 = 1$ *and so*

$$B = \{k \mid b_k = 1, k \in \lceil 5 \rceil\} = \{2, 5\}$$

Notice now $f(B) = f(\{2, 5\}) = 01001$

By construction we have $f(B) = b$. Therefore f_5 is a surjection.

Since f_5 is both an injection and a surjection it follows that f_5 is a bijection. Since f_5 is a bijection, by definition we have $|B_5| = |\mathbf{2}^{\lceil 5 \rceil}|$. Since $|\mathbf{2}^{\lceil 5 \rceil}| = 2^5$, it then follows that $|B_5| = 2^5$. Therefore there are 2^5 binary strings of length 5.

Recognizing that there is nothing too special about $n = 5$ in this argument, we realize we can probably use this same strategy to construct a bijection $f_n : \mathbf{2}^{\lceil n \rceil} \to B_n$ for every $n \geq 1$. Such a bijection would then tell us $|B_n| = 2^n$.

Theorem 10.5. *For every* $n \geq 1$ *there are* 2^n *binary strings of length* n*.*

Aside. *There are many other ways to prove that there are* 2^n *binary strings of lengths* n*. If you are wondering* "why did we do it like this instead of just..."*, it is because this example is here to highlight the power of definition 10.3. If you are interested in techniques for counting mathematical objects, consider taking* MATH327 Combinatorics and Enumeration.

STOP HERE AND GO BACK TO CANVAS TO WATCH THE PART II VIDEO ON SET CARDINALITY

Our definitions for cardinality above seem a little more complicated than they need to be. If you have seen set cardinality it was likely introduced only as a piece of notation:

Let $|A|$ denote the number of elements in A.

With this definition, writing $|A| = |B|$ requires the assumption that the number of elements of A is some integer k. In particular we can't write down this equality when A and B have infinitely many elements. What does it mean for two infinities to be equal?

However, with our definition above for $|A| = |B|$ we can talk about two infinite sets having the same cardinality without having to grapple with the meaning of the statement

$$\infty = \infty$$

(This equality is mostly nonsense. It hurt me deeply to write it. The symbol ∞ does not represent a number. Without first defining what it means for two infinities to be equal, the equality is meaningless. Every time you write this down a mathematician sadly cries to themselves.)

With our goal of understanding what cardinality means for sets with infinitely many elements we define what we mean when we use the word infinite in this context.

Definition 10.6. *Let A be a set. We say A is finite when there exists $k \in \mathbb{N}$ so that $|A| = k$. When A is not finite we say A is infinite.*

Remembering the meaning of the notation $|A| = k$, saying that a set is finite is the same as saying that there is a bijection from the set to a set of the form $\lceil k \rceil$.

Without too much trouble, we can perhaps convince ourselves that both $\mathbb{N}$ and $\mathbb{R}$ are infinite. What can we say then about the cardinality of $\mathbb{N}$ and $\mathbb{R}$? As these sets are both infinite, perhaps we expect we can write $|\mathbb{N}| = |\mathbb{R}|$? To begin to build some intuition for the weirdness of cardinality in infinite sets, we compare the cardinality of the set of even natural numbers and the set of natural numbers.

Let $\mathbb{E} = \{2n \mid n \in \mathbb{N}\}$. Consider the function $f : \mathbb{N} \to \mathbb{E}$ so that $f(n) = 2n$ for all $n \in \mathbb{N}$. For example, $f(3) = 6$. We show f is bijection by showing f is both an injection and a surjection.

To show f is an injection we must show that if $n_1 \neq n_2$, then $f(n_1) \neq f(n_2)$. Consider $n_1, n_2 \in \mathbb{N}$ so that $n_1 \neq n_2$. If $n_1 < n_2$, then $2n_1 < 2n_2$ and so $f(n_1) \neq f(n_2)$. Similarly, if $n_2 < n_1$, then $f(n_2) \neq f(n_1)$. Therefore if $n_1 \neq n_2$, then $f(n_1) \neq f(n_2)$. By definition of injective, it then follows that f is injective.

To show f is surjective we must show that for every $m \in \mathbb{E}$ there exists $n_1 \in \mathbb{N}$ so that $f(n_1) = m$. Since $m \in \mathbb{E}$ there exists $n \in \mathbb{N}$ so that $m = 2n$. Thus $f(n_1) = m$ for $n_1 = n$. Therefore f is surjective.

Since f is both injective and surjective, necessarily f is a bijection. Since f is a bijection, we have

$$|\mathbb{E}| = |\mathbb{N}|.$$

Wait... what?

We have $\mathbb{E} \subset \mathbb{N}$. How is it possible that these two sets have the same cardinality? Our intuition tells us that $\mathbb{E}$ has *half as many* elements as $\mathbb{N}$?

Aside. *We ask ourselves, what does* half as many *mean in the context of a quantity of things that isn't finite? Our fraction vocabulary depends on us being able to split a whole into an equal number of smaller pieces of the same size. This doesn't really work when our whole is an infinite number of things.*

These sets have the same cardinality because they satisfied our agreed upon definition of what it means for two sets to have the same cardinality. Our definitions for cardinality came from our intuition and experiences with finite sets. But nothing in our definition stopped us from applying them to infinite sets. Let us try to do the same with $\mathbb{R}$ and $\mathbb{N}$.

If $|\mathbb{N}| = |\mathbb{R}|$, then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$. Just as we did with the Fibonacci numbers we can consider a function $f : \mathbb{N} \to \mathbb{R}$ as sequence

$$f(0), f(1), f(2), \ldots$$

Let $a_i = f(i)$ for each $i \geq 0$. And so we may re-write this sequence as

$$a_0, a_1, a_2, \ldots$$

Since f is a surjection, every element of $\mathbb{R}$ appears somewhere in this sequence. We will derive a contradiction by finding an element of $r \in \mathbb{R}$ so that r does not appear in the sequence. This will then tell is there can be no bijection from $\mathbb{N}$ to $\mathbb{R}$.

Each element of this sequence is a real number. Let a_i^0 denote the one's digit of a_i. Let a_i^j denote the jth decimal digit of a_i. For example, if

$$a_3 = 34515.21049$$

then

$$\begin{aligned} a_3^0 &= 5 \\ a_3^1 &= 2 \\ a_3^2 &= 1 \\ a_3^3 &= 0 \\ a_3^5 &= 4 \\ a_3^6 &= 9 \\ a_3^7 &= 0 \\ a_3^8 &= 0 \\ a_3^9 &= 0 \\ a_3^{10} &= 0 \\ &\vdots \end{aligned}$$

Consider the number $r = r^0.r^1r^2r^3, \ldots$ so that for all $i \geq 0$ we have

$$r_i = \begin{cases} 0 & a_i^i \in \{1\} \\ 1 & a_i^i \in \{0, 2, 3, 4, 5, 6, 7, 8, 9\} \end{cases}$$

For example, imagine our sequence $a_0, a_1, a_2, a_3, a_4, \ldots$ proceeded as

$$41, 18.5, -11.\overline{3}, 5.21149, 2.71835356, \ldots$$

In this case we would have $r^0 = 0$ as $a_0^0 = 1$ (a_0^0 is the one's digit of $a_0 = 41$) We would have $r^1 = 1$ as $a_1^1 \in \{0, 2, 3, 4, 5, 6, 7, 8, 9\}$ (a_1^1 is the first decimal digit of digit of $a_1 = 18.5$) Continuing in this fashion we have

$$r = 0.1101\ldots$$

Certainly we have $r \in \mathbb{R}$. It may have infinitely many digits, but there are lots of real numbers with infinitely many digits; π for example.

We claim r does not appear anywhere in the sequence

$$a_0, a_1, a_2 \ldots$$

We do this by comparing r with each entry of this sequence starting with a_0

Recall the definition of the number $r = r^0.r^1r^2r^3, \ldots$ so that for all $i \geq 0$ we have

$$r_i = \begin{cases} 0 & a_i^i \in \{1\} \\ 1 & a_i^i \in \{0, 2, 3, 4, 5, 6, 7, 8, 9\} \end{cases}$$

Let us compare r with a_0 by looking at their one's digit:

- If $a_0^0 = 1$, then $r_0 \neq a_0^0$ as $r^0 = 0$.
- If $a_0^0 \in \{0, 2, 3, 4, 5, 6, 7, 8, 9\}$, then $r^0 \neq a_0^0$ as $r^0 = 1$

Since r and a_0 disagree in their one's digit, necessarily $r \neq a_0$.

Let us compare r with a_1 by looking at their first decimal digit:

- If $a_1^1 = 1$, then $r_1 \neq a_1^1$ as $r^1 = 0$.
- If $a_1^1 \in \{0, 2, 3, 4, 5, 6, 7, 8, 9\}$, then $r^1 \neq a_1^1$ as $r^1 = 1$

Since r and a_0 disagree in their first decimal digit:, necessarily $r \neq a_1$.

Let us compare r with a_2 by looking at their second decimal digit:

- If $a_2^2 = 1$, then $r_2 \neq a_2^2$ as $r^2 = 0$.
- If $a_2^2 \in \{0, 2, 3, 4, 5, 6, 7, 8, 9\}$, then $r^2 \neq a_0^0$ as $r^2 = 1$

Since r and a_2 disagree in their second decimal digit:, necessarily $r \neq a_2$.

This argument is getting a bit repetitive. We generalize.

For every $k \geq 1$ let us compare r with a_k by looking at their kth decimal digit:

- If $a_k^k = 1$, then $r_k \neq a_k^k$ as $r^k = 0$.
- If $a_k^k \in \{0, 2, 3, 4, 5, 6, 7, 8, 9\}$, then $r^k \neq a_k^k$ as $r^k = 1$

Since r and a_k disagree in their kth decimal digit:, necessarily $r \neq a_k$.

From this last argument we see that $r \neq a_k$ for any $k \in \mathbb{N}$. Therefore r appears nowhere in the sequence

$$a_0, a_1, a_2, \ldots$$

Recall $r_i = f(i)$ for each $i \geq 0$. Therefore r does not appear anywhere in the sequence

$$f(0), f(1), f(2), \ldots$$

Therefore r is not the image of any element of $\mathbb{N}$ with respect to f. Therefore f is not a surjection. Therefore it cannot be that f is a bijection. Therefore there is no bijection from $\mathbb{N}$ to $\mathbb{R}$. And so $\mathbb{N}$ and $\mathbb{R}$ do not have the same cardinality. That is, $|\mathbb{N}| \neq |\mathbb{R}|$. And so

The infinity that is the quantity of natural numbers is not the same infinity that is the quantity of real numbers.

On this incredibly bizarre (but true!) statement, we end our work in set cardinality and close the book (.pdf?) on MATH 163 for the semester. Take a moment to appreciate the work you have done this semester. I suspect this is the first time you have read nearly 200 pages of mathematics on a single subject. In itself, this is an impressive feat!

Good luck with your final exams!

Aside. *The conclusion that* $|\mathbb{N}| \neq |\mathbb{R}|$ *is the first in a sequence of completely unintuitive results about the cardinalities of infinite sets. Just as we proved* $|\mathbb{E}| = |\mathbb{N}|$ *by constructing an explicit bijection, so too can we prove* $|\mathbb{N}| = |\mathbb{Q}|$*. Sets that have the same cardinality as* $\mathbb{N}$ *are called* countable*.*

That $|\mathbb{N}| \neq |\mathbb{R}|$ *suggests that an equivalence relation on the collection of all infinite sets so that sets in the same part of the partition have the same cardinality is worth a closer look. By showing* $|\mathbf{2}^X| \neq |X|$ *for every set* X*, it then follows*

$$|\mathbb{N}| \neq |\mathbf{2}^{\mathbb{N}}| \neq |\mathbf{2}^{\mathbf{2}^{\mathbb{N}}}| \neq |\mathbf{2}^{\mathbf{2}^{\mathbf{2}^{\mathbb{N}}}}| \neq \cdots$$

This then implies that this partition has infinitely many parts; each of the sets

$$\mathbb{N}, \mathbf{2}^{\mathbb{N}}, \mathbf{2}^{\mathbf{2}^{\mathbb{N}}}, \mathbf{2}^{\mathbf{2}^{\mathbf{2}^{\mathbb{N}}}}, \cdots$$

are in their own part of the partition.

Just as the cardinality of $\mathbb{N}$ *and* $\mathbb{R}$ *represent two different "sizes" of infinity. This sequence of infinite sets with differing infinite cardinalities, suggest to us that there are infinitely many different "sizes" of infinity. We can arrange these different "sizes" of infinity as a partial order based on the existence of injections. The study of this partial order leads to some deep foundational questions about mathematics and the existence of mathematical statements that can neither be proven true nor false. For more information, do an internet search for* `the continuum hypothesis`*.*

---

11 Set Cardinality Part II

After taking some time to learn about infinite cardinality, we now return back to sets with finite cardinality. We introduce fundamental counting principles. Rather than contrived "real world" examples, it may be better to lean on previous course material, relations and graph theory, to discuss counting techniques. Define $\binom{n}{k}$ to be the number of k-subsets of an n element set. Introduce factorial notation of the purpose of counting the number of arrangements (words). Then derive the formula for $\binom{n}{k}$.

---

12 An Introduction to Number Theory

Back in the discussion of equivalence relations we introduced congruence modulo 4 without actually using the standard notation or terminology. In this section we do these things.

When $n = 2$ our congruence classes are odd and even integers. For other values of n, our congruence classes correspond to possible remainders when dividing by n. We motivate the meaning of operations ($+$ and $\times$) of these equivalence classes by remembering/generalizing facts about sums and products of even and odd numbers (e.g. odd + even = odd).

Once we have multiplication in place we can talk about exponentiation. Notice Fermat's Little Theorem and advertise for MATH364.

Look at the exponentiation table for the complex unit i Notice a similar result to Fermat's Little Theorem. Talk briefly about "isomorphism" with the complex unit and $\mathbb{Z}_4$

Another good exercise is briefly introducing ideas leading to isomorphism.

Index

Table of Notation