MCC: MTH 220 - DISCRETE MATH

Judy Dean
Monroe Community College

LibreTexts™

Monroe Community College

MCC: MTH 220 - Discrete Math

Judy Dean

The LibreTexts libraries are Powered by NICE CXOne and are supported by the Department of Education Open Textbook Pilot Project, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

This text was compiled on 02/04/2024

TABLE OF CONTENTS

Licensing

A detailed breakdown of this resource's licensing can be found in ***Back Matter/Detailed Licensing***.

CHAPTER OVERVIEW

1: Introduction to Discrete Mathematics

Thumbnail: Rubik's Cube. Image used with permission (CC BY-SA 3.0 Unported; Booyabazooka).

1.0 Preface

There are many discrete mathematics textbooks available, so why did I decide to invest my time and energy to work on something that perhaps only I myself would appreciate?

Mathematical writings are full of jargon and conventions that, without proper guidance, are difficult for beginners to follow. In the past, students were expected to pick them up along the way on their own. Those who failed to do so would be left behind. Looking back, I consider myself lucky. It was by God's grace that I survived all those years. Now, when I teach a mathematical concept, I discuss its motivation, explain why it is important, and provide a lot of examples. I dissect the proofs thoroughly to make sure everyone understands them. In brief, I want to show my students how to analyze mathematical problems.

Most textbooks typically hide all these details. They only show you the final polished products. By training, mathematicians love short and elegant proofs. This is reflected in their own writing. Yes, the results are beautiful, but it is a mystery how mathematicians come up with such ideas. I want a textbook that discusses mathematical concepts in greater detail. I want to teach my students how to read and write mathematical arguments. Since I could not find a textbook that suited my needs, I started writing lecture notes to supplement the main text. Marginal notes, hands-on exercises, summaries, and section exercises were subsequently added at different stages. The lecture notes have evolved into a full-length text.

Discrete mathematics is a rich subject, full of many interesting topics. Often, it is taught to both mathematics and computer science majors. Due to the limit in space, this text addresses mainly the needs of the mathematics majors. Consequently, we will concentrate on logic and proof techniques, and apply them to sets, basic number theory, and functions. In the last two chapters, we discuss relations and combinatorics, as many students will find them useful in other courses.

Since the intended audience of the text is mathematics majors, I use a number of examples from calculus. By design, I hope this can help the students review what they have learned, and see that discrete mathematics forms the foundation of many mathematical arguments.

Discrete mathematics is often a required course in computer science. I find it hard and unjust to serve two different groups of students in the same textbook. Although this text could be used in a typical first semester discrete mathematics class for the computer science majors, they need to consult another text for the second semester course. Here are two that serve this purpose well:

Alan Doerr and Kenneth Levasseur, *Applied Discrete Structures*.

Miguel A. Lerma, *Notes on Discrete Mathematics*.

Both are available on-line.

Why do I call this a workbook? There are many hands-on exercises designed to help students understand a new concept before they move on to the next. I believe the title *Workbook* reflects the nature of the book, because I expect the students to work on the hands-on exercises. But why spiral? Because the pedagogy is inspired by the spiral method. The idea is to revisit some themes and results several times throughout the course and each time further deepen your understanding. You will find some problems pop up more than once, and are solved in a different way each time. In other instances, a concept you learned earlier will be viewed from a new perspective, thus adding a new dimension to it.

I am indebted to the anonymous reviewers, whose numerous valuable comments helped to shape the workbook in its current form. I would also like to express my great appreciation to Scott Richmond of Reed Library at the State University of New York at Fredonia, who provided many helpful suggestions and editorial assistance.

The reason I developed this workbook is to help students learn discrete mathematics. If this workbook proves to be a failure, I am the one to blame. If you find this workbook serves its intended purposes, I give all the glory to God, in whom I believe and trust.

Harris Kwong
April 21, 2015

1.1: An Overview of Discrete Mathematics

What is discrete mathematics? Roughly speaking, it is the study of discrete objects. Here, discrete means "containing distinct or unconnected elements." Examples include:

- Determining whether a mathematical argument is logically correct.
- Studying the relationship between finite sets.
- Counting the number of ways to arrange objects in a certain pattern.
- Analyzing processes that involve a finite number of steps.

Here are a few reasons why we study discrete mathematics:

- To develop our ability to understand and create mathematical arguments.
- To provide the mathematical foundation for advanced mathematics and computer science courses.

In this text, we will cover these six topics:

1. ***Logic and Proof Techniques:*** Logic allows us to determine if a certain argument is valid. We will also learn several basic proof techniques.
2. ***Basic Number Theory:*** Number theory is one of the oldest branches of mathematics; it studies properties of integers. We will use the proof techniques we learned to prove some basic facts in number theory.
3. ***Sets:*** We study the fundamental properties of sets, and again we will use the proof techniques we learned to prove important results in set theory.
4. ***Relations and Functions:*** Relations and functions describe the relationship between the elements from two sets. They play a key role in mathematics.
5. ***Combinatorics:*** Combinatorics studies the arrangement of objects. For instance, one may ask, in how many ways can we form a five-letter word. It is used in many disciplines beyond mathematics.
6. ***Big O:*** A stand-alone topic on growth of functions.

All of these topics are crucial in the development of your mathematical maturity. The importance of some of these concepts may not be apparent at the beginning. As time goes on, you will slowly understand why we cover such topics. In fact, you may not fully appreciate the subjects until you start taking advanced courses in mathematics.

This is a very challenging course partly because of its intensity. We have to cover many topics that appear totally unrelated at first. This is also the first time many students have to study mathematics in depth. You will be asked to write up your mathematical argument clearly, precisely, and rigorously, which is a new experience for most of you.

Learning how to think mathematically is far more important than knowing how to do all the computations. Consequently, the principal objective of this course is to help you develop the analytic skills you need to learn mathematics. To achieve this goal, we will show you the motivation behind the ideas, explain the results, and dissect why some solution methods work while others do not.

1.2: Suggestions to Students

All mathematics courses are difficult. It takes hard work and patience to learn mathematics. Rote memorization does *not* work. Here are some suggestions that you may find helpful:

1. Do *not* skip classes.
2. Read the text, including the examples, *before* the lecture; review what you have learned after each lecture.
3. Do the exercises.
    a. First, study the examples in the book.
    b. Make an effort to understand how and why a solution works, and remember how certain types of problems should be solved.
    c. When you do a problem, ask yourself if you have seen something similar before; if you have, follow the steps in its solution.
    d. After solving a problem, look for alternate solutions, analyze and compare their differences.
4. Get help from the instructor, your friends, and whatever facility your college provides.
5. Develop good study habits.
    a. Keep working every day: study the book, your own lecture notes, and, most important of all, do the exercises at the end of each section.
    b. Form a study group of two to three students, and meet on a regular basis to study together.
    c. Check the solutions for any nonsense or discrepancies.
    d. Learn how to solve the problems systematically.
6. Perseverance. Do not give up easily.
7. Be willing to help your classmates. Trying to explain something to others is the best way to learn anything new.

Attitude is the real difference between success and failure. Nothing comes easy. To succeed, you have to work hard. But you also need to learn how to learn mathematics the right way.

- Do not rely on memorizing formulas or procedures by rote. Instead, try to understand the concepts and ideas behind them. It is important to learn when and how to use them.
- Of course, it does not mean that you need not memorize anything at all. On the contrary, many basic results and definitions need to be memorized. You may find it helpful to use a highlighter to mark the definitions and keywords that you have trouble recalling, and I urge you to review them frequently.
- Do not compartmentalize the material; all sections are connected in one way or another. Consequently, as you move along from chapter to chapter and from section to section, try to observe the connections between the concepts you have learned. Without saying, it is understood that you need to remember what you had learned earlier.
- Write down all intermediate and partial results *clearly*. For instance, if the value of x is 7, do not just jot down the number 7; instead, write $x = 7$. Otherwise, you may forget what 7 is after just a few minutes. In brief, present your results in such a way that they can be read and understood by *everyone* in the class.
- While we are on the subject, let us comment briefly how to write up a solution. *Take your homework assignments seriously*. Keep in mind: to study for a test, you may want to review your homework, so you need to be able to read your own work. Write everything clearly and neatly. The process of writing out everything correctly helps you think about what you write. Very often, incoherent and incomprehensible writing is an indication of lack of understanding of the subject matter.
- When doing your homework assignments, start with a draft, then look over it carefully, check the spelling and grammar, and revise the solution. Make sure you write in complete sentences and use correct notations. If necessary, you may have to polish it further. Before turning in the final version, be sure to check again for any mistakes that you may have overlooked.

How should a student use this workbook?

1. Read the workbook *before* class, and study the workbook *again* after each class.
2. Read and study the examples in the workbook.
3. Do the hands-on exercises.
4. Do the section exercises.

1.3: How to Read and Write Mathematics

Reading mathematics is difficult for beginners. It takes patience and practice to learn how to read mathematics. You may need to read a sentence or a paragraph several times before you understand it completely. There are writing styles and notational conventions that you acquire only by reading and paying attention to how mathematics is written. As we proceed with the course, we will discuss the details. As a starter, let us offer several suggestions.

- Make sure you know the definition of mathematical terms, the meaning and proper usage of mathematical symbols and notations. Although this may sound obvious, many beginners have difficulty understanding a mathematical argument because they fail to recall the exact meaning of certain mathematical concepts.
- Often, the reason behind a claim lies in the sentence before it. Sometimes it could be found in the preceding paragraph, and it is not unusual that you may need to check several sentences or paragraphs before it. You need to take an active role in reading mathematics, and you need to remember what you have read.
- Mathematicians prefer short and elegant proofs. To do this, they suppress the details of what they consider as "obvious" reasons. But what is obvious to one reader may not be that obvious to another. At any rate, for practical reasons, it is impossible to include every minute step in a mathematical argument. Consequently, keep your pencil and paper next to you, and be ready to check the calculation and fill in the missing details.
- It may help to try out some examples just to see how an argument works.
- After you finish reading a proof, go over it one more time, and try to summarize its key steps (in other words, try to draw an outline of the proof) in your own words.

Writing mathematics is even harder! It takes much longer to learn how to write mathematics. Of course, the most important thing about a mathematical argument is its correctness. When we say "good" mathematical writing, we are talking about precision, clarity, and sound logic.

- Be precise! For example, do not just say "it" when it is unclear which quantity you are referring to. This is particularly true in a lengthy argument. In this regard, it helps to identify and hence distinguish different quantities by their names such as x, y, z, etc.
- Use mathematical terms correctly! A common mistake is confusing an expression with an equation. An equation has an equal sign, as in

  $$x+y=5, \tag{1.3.1}$$

  but an expression does not, as in

  $$x+y. \tag{1.3.2}$$

- Likewise, the following is an inequality:

  $$x+y\geq 5. \tag{1.3.3}$$

  Do not call it an equation!
- Do not abuse the word "solve." For instance, many students would say "solve 5^2+7^3 ." A more appropriate saying should be "compute the value of 5^2+7^3, " or simply "evaluate 5^2+7^3 ."

In the beginning, it helps to follow what others do. This again means you need to read a lot of mathematical writing, and pick up styles that you are comfortable with. We often follow some conventions (unwritten rules, if you prefer) that everyone follows.

Example 1.3.1

Consider this argument for showing that $(x-y)(x+y)=x^2-y^2$:

> We want to show that
>
> $$(x-y)(x+y)=x^2-y^2. \tag{1.3.4}$$
>
> After expanding the product on the left-hand side, we find

$$= x^2 + xy - yx - y^2 = x^2 - y^2, \tag{1.3.5}$$

which is what we want to prove.

The logic and mathematics in the argument are correct, but not the notation. In formal writing, each equation should be a stand-alone equation. The last equation is incomplete, because it does not have anything on the left-hand side of the equal sign. Here is a proper way to write the argument:

Solution

We want to show that

$$(x-y)(x+y) = x^2 - y^2. \tag{1.3.6}$$

After expanding the product on the left-hand side, we find

$$(x-y)(x+y) = x^2 + xy - yx - y^2 = x^2 - y^2, \tag{1.3.7}$$

Therefore $(x-y)(x+y) = x^2 - y^2$.
which is what we want to prove.

The fix is simple: just repeat the left-hand side.

Example 1.3.2

Short and simple mathematical expressions or equations such as $a^2 + b^2 = c^2$ can be written within a paragraph. Longer ones and expressions or equations that are important should be displayed separately, and centered, on their own lines, as in

$$x^3 - y^3 = (x-y)(x^2 + xy + y^2). \tag{1.3.8}$$

If we intend to refer to the equation later, assign a number to it, and enclose the number within parentheses:

$$x^2 - y^2 = (x-y)(x+y). \tag{1.3.9}$$

Now, for example, we can say, because of 1.3.9, we find

$$135 = 144 - 9 = 12^2 - 3^2 = (12-3)(12+3) = 9 \cdot 15. \tag{1.3.10}$$

For a longer equation such as

$$(x+y)^2 = (x+y)(x+y) = x^2 + xy + xy + y^2 = x^2 + 2xy + y^2, \tag{1.3.11}$$

it may look better and easier to follow if we break it up into several lines, and line them up along the equal signs:

$$\begin{aligned} (x+y)^2 &= (x+y)(x+y) && (1.3.12) \\ &= x^2 + xy + xy + y^2 && (1.3.13) \\ &= x^2 + 2xy + y^2. && (1.3.14) \end{aligned}$$

Although we display the equation in three lines, they together form *one* equation. The equal signs at the beginning of the second and third lines indicate that they are the continuation of the previous line. Since this is actually one long equation, we only need to say $(x+y)^2$ once, namely, at the beginning.

When part of the right-hand side extends beyond the margin, you may want to balance the look of the entire equation by repositioning the left-hand side:

$$\begin{aligned} &(x^2 + 2xy + y^2)(x^2 + 2xy + y^2) \\ &\qquad = \quad x^4 + 2x^3y + x^2y^2 + 2x^3y + 4x^2y^2 + 2xy^3 + x^2y^2 + 2xy^3 + y^4 \\ &\qquad = \quad x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4. \end{aligned}$$

In the multi-line display format, always write the equal signs at the *beginning* of the lines. Do not forget to align the equal signs.

When part of the right-hand side is too long to display as a single piece, we may split it into multiple pieces:

$$\begin{aligned}(x+y)^5 &= (x+y)^2(x+y)^3 && (1.3.15)\\ &= (x^2+2xy+y^2)(x^3+3x^2y+3xy^2+y^3) && (1.3.16)\\ &= x^5+3x^4y+3x^3y^2+x^2y^3+2x^4y+6x^3y^2+6x^2y^3+2xy^4 && (1.3.17)\\ &\quad +x^3y^2+3x^2y^3+3xy^4+y^5 && (1.3.18)\\ &= x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5. && (1.3.19)\end{aligned}$$

It is a common practice to use indentation to indicate the continuation of part of a line into the next.

There will be more discussion as we continue. Let us not forget: the best way to learn is to watch and observe how others do it. Reading is a must! Reading and analyzing technical papers will surely improve your mathematical knowledge as well as your writing.

1.4: Proving Identities

There are many methods that one can use to prove an identity. The simplest is to use algebraic manipulation, as we have demonstrated in the previous examples. In an algebraic proof, there are three acceptable approaches:

- *From left to right*: expand or simplify the left-hand side until you obtain the right-hand side.
- *From right to left*: expand or simplify the right-hand side until you obtain the left-hand side.
- *Meet in the middle*: expand or simplify the left-hand side and the right-hand side *separately* until you obtain the same result from both sides.

Example 1.4.1

To prove that

$$x^3-y^3=(x-y)(x^2+xy+y^2), \tag{1.4.1}$$

we start from the right-hand side, because it is more complicated than the left-hand side. The proof proceeds as follows:

Solution

$$\begin{aligned}(x-y)(x^2+xy+y^2) &= x^3-x^2y+x^2y-xy^2+xy^2-y^3\\ &= x^3-y^3.\end{aligned}$$

Thus

$$x^3-y^3=(x-y)(x^2+xy+y^2). \tag{1.4.2}$$

Remember: start from one side and work on it until you obtain the other side.

Example 1.4.2

The following “proof” of

$$x^4+x^2y^2+y^4=(x^2+xy+y^2)(x^2-xy+y^2) \tag{1.4.3}$$

is *incorrect*:

$$\begin{aligned}x^4+x^2y^2+y^4 &= (x^2+xy+y^2)(x^2-xy+y^2)\\ &= x^4-x^3y+x^2y^2+x^3y-x^2y^2+xy^3+x^2y^2-xy^3+y^4\\ &= x^4+x^2y^2+y^4.\end{aligned}$$

Here is the reason. When we place

$$x^4+x^2y^2+y^4=(x^2+xy+y^2)(x^2-xy+y^2) \tag{1.4.4}$$

at the start of the proof, by convention, we are proclaiming that $x^4+x^2y^2+y^4$ is indeed equal to $(x^2+xy+y^2)(x^2-xy+y^2)$. However, this is what we are asked to prove. Before we have actually proved that it is true, we do not know *yet*, whether they are equal. Therefore, it is wrong to start the proof with it.

Example 1.4.3

For the same reason, the following “proof” of the identity

$$x^3-y^3=(x-y)(x^2+xy+y^2) \tag{1.4.5}$$

is *unacceptable*:

$$\begin{aligned} x^3-y^3 &= (x-y)(x^2+xy+y^2) \\ x^3-y^3 &= x^3-x^2y+x^2y-xy^2+xy^2-y^3 \\ x^3-y^3 &= x^3-y^3 \end{aligned} \tag{1.4.6}$$

By putting x^3-y^3 on the left-hand side of every line, this becomes (by convention) a collection of three equations. In a nutshell, the argument starts with an equation and we simplify until we obtain something we know is true. If this format is valid, we can "prove" that $21=6$, as follows:

$$\begin{aligned} 21 &= 6 \\ 6 &= 21 \\ 27 &= 27 \end{aligned}$$

By writing $21=6$ at the beginning of the proof, what we really say is "*Assume* $21=6$ is true." But this is what we *intend* to prove. Thus, in effect, we are putting the cart in front of the horse, which is logically incorrect. There is another explanation why this proof is incorrect. We shall discuss it in Section 2.3.

In brief: we *cannot* start with the given identity and simplify both sides until we obtain an equality (or an equation of the form $0=0$).

Example 1.4.4

Show that $\frac{1}{6}k(k+1)(2k+1)+(k+1)^2=\frac{1}{6}(k+1)(k+2)(2k+3)$.

Solution 1

We can use the "meet in the middle" approach. Recall that we cannot simplify both sides *simultaneously*. Instead, we should expand the two sides *separately*, and then compare the results. We also suggest adding more writing (in words) to help with the explanation.

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

The right-hand side expands into

$$\begin{aligned} \frac{1}{6}(k+1)(k+2)(2k+3) &= \frac{1}{6}(2k^3+9k^2+13k+6) \\ &= \frac{1}{3}k^3+\frac{3}{2}k^2+\frac{13}{6}k+1. \end{aligned}$$

Since both sides yield the same result, they must be equal.

Although the proof is correct, it requires two sets of computation. It is much easier to use either the left-to-right or the right-to-left approach.

Solution 2

A better alternative is to start from the left-hand side and simplify it until we obtain the right-hand side. Our secret weapon is factorization:

$$\begin{aligned} \frac{1}{6}k(k+1)(2k+1)+(k+1)^2 &= \frac{1}{6}(k+1)[k(2k+1)+6(k+1)] \\ &= \frac{1}{6}(k+1)(2k^2+7k+6) \\ &= \frac{1}{6}(k+1)(k+2)(2k+3). \end{aligned}$$

This approach is usually better and safer, because no messy computation is involved.

Hands-on Exercise 1.4.1

Show that

$$\frac{k(k+1)(k+2)}{3}+(k+1)(k+2)=\frac{(k+1)(k+2)(k+3)}{3}. \tag{1.4.7}$$

Be sure to use one of the three methods we discussed above.

Solution

1. Two proofs are given below, one uses direct expansion, the other uses factorization.

Solution 1: Expanding the two sides *separately*, we find

$$\begin{aligned}\frac{k(k+1)(k+2)}{3}+(k+1)(k+2) &= \frac{k^3+3k^2+2k}{3}+k^2+3k+2\\ &= \frac{k^3+3k^2+2k+3(k^2+3k+2)}{3}\\ &= \frac{k^3+6k^2+11k+6}{3},\end{aligned}$$

and
$$\frac{(k+1)(k+2)(k+3)}{3}=\frac{(k^2+3k+2)(k+2)}{3}=\frac{k^3+6k^2+11k+6}{3},$$
which establish the identity.

Solution 2: Since
$$\begin{aligned}\frac{k(k+1)(k+2)}{3}+(k+1)(k+2) &= (k+1)(k+2)\left(\frac{k}{3}+1\right)\\ &= \frac{(k+1)(k+2)(k+3)}{3},\end{aligned}$$
the identity always holds.

Summary and Review

- There are only three ways to prove an identity: left to right, right to left, or meet in the middle.
- *Never* prove an identity by simplifying both sides simultaneously.

Exercises 1.4.

Exercise 1.4.1

Let x and y be any real numbers. Prove that

$$(x+y)^3=x^3+3x^2y+3xy^2+y^3. \tag{1.4.8}$$

Exercise 1.4.2

Let x and y be any real numbers. Prove that

$$(a-b)^4=a^4-4a^4b+6a^2b^2-4ab^3+b^4. \tag{1.4.9}$$

Exercise 1.4.3

Prove that, for any distinct real numbers x and y,

$$\frac{x^3-y^3}{x-y}=x^2+xy+y^2. \tag{1.4.10}$$

Exercise 1.4.4

Prove that, for any integer k,

$$\frac{k(k+1)(k+2)(k+3)}{4}+(k+1)(k+2)(k+3)=\frac{(k+1)(k+2)(k+3)(k+4)}{4}. \tag{1.4.11}$$

Exercise 1.4.5

Prove that, for any integer k,

$$\frac{k^2(k+1)^2}{4}+(k+1)^3=\frac{(k+1)^2(k+2)^2}{4}. \tag{1.4.12}$$

1.5: Introduction to Sets and Real Numbers

Sets - An Introduction

A ***set*** is a collection of objects. The objects in a set are called its ***elements*** or ***members***. The elements in a set can be any types of objects, including sets! The members of a set do not even have to be of the same type. For example, although it may not have any meaningful application, a set can consist of numbers and names.

We usually use capital letters such as A, B, C, S, and T to represent sets, and denote their generic elements by their corresponding lowercase letters a, b, c, s, and t, respectively. To indicate that b is an element of the set B, we adopt the notation $b \in B$, which means " b belongs to B" or " b is an element of B." Consequently, saying $x \in \mathbb{R}$ is another way of saying x is a real number.

Definition: Subset

Set A is a **subset** of Set B if and only if every element in Set A is also in Set B.

In symbols:

$$A \subset B \iff x \in A \rightarrow x \in B \tag{1.5.1}$$

Real Numbers and some Subsets of Real Numbers

We designate these notations for some special sets of numbers:

$$\begin{aligned} \mathbb{N} = & \quad \text{the set of natural numbers,} \\ \mathbb{Z} = & \quad \text{the set of integers,} \\ \mathbb{Q} = & \quad \text{the set of rational numbers,} \\ \mathbb{R} = & \quad \text{the set of real numbers.} \end{aligned}$$

All these are infinite sets, because they all contain infinitely many elements. In contrast, finite sets contain finitely many elements.

We list the natural numbers and integers while defining the rational, real and irrational numbers.

$$\mathbb{N} = \{\mathbf{1, 2, 3, \ldots}\}$$

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

Definition - Rational Numbers

A **rational number** is a number that can be expressed as a ratio of two integers (with the second integer not equal to zero). Hence, a rational number can be written as $\frac{m}{n}$ for some integers m and n, where $n \neq 0$.

Definition - Real Numbers

The **real numbers** are the numbers corresponding to all the points on the number line.

Definition - Irrational Numbers

An **irrational number** is a real number that can not be expressed as a ratio of two integers; i.e., is not rational.

Closure

Definition

Given a set S with a binary operation *, S is **closed under the operation *** if and only if $x * y \in S$ for every $x \in S$ and for every $y \in S$.

Example 1.5.1

Suppose you add any two integers together. Will the sum always be an integer?

Solution

Yes; that's why the set of integers is closed under addition.

Assumption

We will use the property that the **set of integers is closed under addition, subtraction and multiplication.**

Alternate syntax is "closure of integers under multiplication".

This assumption can be used as a reason in an explanation or a proof.

Example 1.5.2

If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$ because ?

Solution

The set of integers is closed under addition.

Set Notation

Roster Notation

We can use the ***roster notation*** to describe a set if it has only a small number of elements. We list all its elements explicitly, as in

$$A = \text{the set of natural numbers not exceeding } 7 = \{1, 2, 3, 4, 5, 6, 7\}. \tag{1.5.2}$$

For sets with more elements, show the first few entries to display a pattern, and use an ellipsis to indicate “and so on.” For example,

$$\{1, 2, 3, \ldots, 20\} \tag{1.5.3}$$

represents the set of the first 20 positive integers. The repeating pattern can be extended indefinitely, as in

$$\begin{aligned} \mathbb{N} &= \{1, 2, 3, \ldots\} \\ \mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \end{aligned}$$

In regards to **parity**, an integer is either even or odd. For now, we will use our common understanding of even and odd and define these terms later in this text. The set of even integers can be described as $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$

Set-Builder Notation

We can use a ***set-builder notation*** to describe a set. For example, the set of natural numbers is defined as

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}. \tag{1.5.4}$$

Here, the vertical bar $\mid$ is read as "such that" or "for which." Hence, the right-hand side of the equation is pronounced as "the set of x belonging to the set of integers such that $x > 0$," or simply "the set of integers x such that $x > 0$." In general, this descriptive method appears in the format

$$\{\,\text{membership} \mid \text{properties}\,\}. \tag{1.5.5}$$

The notation $\mid$ means "such that" or "for which" only when it is used in the set notation. It may mean something else in a different context. Therefore, *do not* write "let x be a real number $\mid x^2 > 3$" if you want to say " let x be a real number such that $x^2 > 3$." It is considered improper to use a mathematical notation as an abbreviation.

Example 1.5.3

Write these two sets

$$\{x \in \mathbb{Z} \mid x^2 \leq 1\} \quad \text{and} \quad \{x \in \mathbb{N} \mid x^2 \leq 1\} \tag{1.5.6}$$

by listing their elements explicitly.

Solution

The first set has three elements, and equals $\{-1, 0, 1\}$. The second set is a singleton set; it is equal to $\{1\}$.

hands-on exercise 1.5.1

Use the roster method to describe the sets $\{x \in \mathbb{Z} \mid x^2 \leq 20\}$ and $\{x \in \mathbb{N} \mid x^2 \leq 20\}$.

hands-on exercise 1.5.2

Use the roster method to describe the set

$$\{x \in \mathbb{N} \mid x \leq 20 \text{ and } x = n^2 \text{ for some integer } n\}. \tag{1.5.7}$$

There is a slightly different format for the set-builder notation. Before the vertical bar, we describe the form the elements assume, and after the vertical bar, we indicate from where we are going to pick these elements:

$$\{\,\text{pattern} \mid \text{membership}\,\}. \tag{1.5.8}$$

Here the vertical bar $\mid$ means "where." For example,

$$\{x^2 \mid x \in \mathbb{Z}\} \tag{1.5.9}$$

is the set of x^2 where $x \in \mathbb{Z}$. It represents the set of squares: $\{0, 1, 4, 9, 16, 25, \ldots\}$

Example 1.5.4

The set

$$\{2n \mid n \in \mathbb{Z}\} \tag{1.5.10}$$

describes the set of even numbers. We can also write the set as $2\mathbb{Z}$.

hands-on exercise 1.5.3

Describe the set $\{2n+1 \mid n \in \mathbb{Z}\}$ with the roster method.

hands-on exercise 1.5.4

Use the roster method to describe the set $\{3n \mid n \in \mathbb{Z}\}$.

Interval Notation

An interval is a set of real numbers, all of which lie between two real numbers. Should the endpoints be included or excluded depends on whether the interval is ***open***, ***closed***, or ***half-open***. We adopt the following ***interval notation*** to describe them:

$$\begin{aligned} (a,b) &= \{x\in\mathbb{R}\mid a<x<b\}, \\ [a,b] &= \{x\in\mathbb{R}\mid a\le x\le b\}, \\ [a,b) &= \{x\in\mathbb{R}\mid a\le x<b\}, \\ (a,b] &= \{x\in\mathbb{R}\mid a<x\le b\}. \end{aligned} \tag{1.5.11}$$

It is understood that a must be less than b. Hence, the notation $(5,3)$ does not make much sense. How about $[3,3]$? This may be used in some texts to mean $\{3\}$ but we will only use $a<b$ for intervals and use roster notation for single number such as $\{3\}$.

An interval contains not just integers, but all real numbers between the two endpoints. For instance, $(1,5)\neq\{2,3,4\}$ because the interval $(1,5)$ also includes real numbers such at 1.276, $\sqrt{2}$, and π.

We can use $\pm\infty$ in the interval notation:

$$\begin{aligned} (a,\infty) = &\quad \{x\in\mathbb{R}\mid a<x\}, \\ (-\infty,a) = &\quad \{x\in\mathbb{R}\mid x<a\}. \end{aligned}$$

However, we cannot write $(a,\infty]$ or $[-\infty,a)$, because $\pm\infty$ are *not* numbers. It is nonsense to say $x\le\infty$ or $-\infty\le x$. For the same reason, we can write $[a,\infty)$ and $(-\infty,a]$, but *not* $[a,\infty]$ or $[-\infty,a]$.

Example 1.5.5

Write the intervals $(2,3)$, $[2,3]$, and $(2,3]$ in the descriptive form.

Solution

According to the definition of an interval, we find

$$\begin{aligned} (2,3) = &\quad \{x\in\mathbb{R}\mid 2<x<3\}, \\ [2,3] = &\quad \{x\in\mathbb{R}\mid 2\le x\le 3\}, \\ (2,3] = &\quad \{x\in\mathbb{R}\mid 2<x\le 3\}. \end{aligned}$$

What would you say about $[2,3)$?

Example 1.5.6

Write these sets

$$\{x\in\mathbb{R}\mid -2\le x<5\} \quad \text{and} \quad \{x\in\mathbb{R}\mid x^2\le 1\} \tag{1.5.12}$$

in the interval form.

Solution

The answers are $[-2,5)$ and $[-1,1]$, respectively. The membership of x affects the answers. If we change the second set to $\{x\in\mathbb{Z}\mid x^2\le 1\}$, the answer would have been $\{-1,0,1\}$. Can you explain why $\{-1,0,1\}\neq[-1,1]$?

Example 1.5.7

Be sure you are using the right types of numbers. Compare these two sets

$$\begin{aligned} S = &\quad \{x\in\mathbb{Z}\mid x^2\le 5\}, \\ T = &\quad \{x\in\mathbb{R}\mid x^2\le 5\}. \end{aligned}$$

One consists of integers only, while the other contains real numbers. Thus, $S=\{-2,-1,0,1,2\}$, and $T=\left[-\sqrt{5},\sqrt{5}\right]$.

Note

If the membership is not specified, such as: $\{x \mid x^2 \leq 5\}$ then it is understood that $\mathbb{R}$ is the default set that x belongs to.

hands-on exercise 1.5.5

Which of the following sets

$$\{x \in \mathbb{Z} \mid 1 < x < 7\} \quad \text{and} \quad \{x \mid 1 < x < 7\} \tag{1.5.13}$$

can be represented by the interval notation $(1, 7)$? Explain.

hands-on exercise 1.5.6

Explain why $[2, 7] \neq \{2, 3, 4, 5, 6, 7\}$

hands-on exercise 1.5.7

True or false: $(-2, 3) = \{-1, 0, 1, 2\}$? Explain.

Let S be a set of numbers; we define

$$\begin{aligned} S^+ &= \{x \in S \mid x > 0\}, \\ S^- &= \{x \in S \mid x < 0\}, \\ S^* &= \{x \in S \mid x \neq 0\}. \end{aligned}$$

In plain English, S^+ is the subset of S containing only those elements that are positive, S^- contains only the negative elements of S, and S^* contains only the nonzero elements of S.

Example 1.5.8

It should be obvious that $\mathbb{N} = \mathbb{Z}^+$.

hands-on exercise 1.5.8

What is the notation for the set of negative integers?

Some mathematicians also adopt these notations:

$$\begin{aligned} bS &= \{bx \mid x \in S\}, \\ a + bS &= \{a + bx \mid x \in S\}. \end{aligned}$$

Accordingly, we can write the set of even integers as $2\mathbb{Z}$, and the set of odd integers can be represented by $1 + 2\mathbb{Z}$.

Example 1.5.9

$$5\mathbb{Z} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} \tag{1.5.14}$$

There are three kinds of real numbers: positive, negative and zero.

Trichotomy Property

For any two real numbers, a and b one and only one of these relations is true:

- $a < b$
- $a = b$
- $a > b$.

Exercises

Exercise 1.5.1

Determine whether these statements are true or false:

a. $0 \in \mathbb{Q}$
b. $0 \in \mathbb{Z}$
c. $-4 \in \mathbb{Z}$
d. $-4 \in \mathbb{N}$
e. $2 \in 3\mathbb{Z}$
f. $-18 \in 3\mathbb{Z}$

Answer

(a) true (b) true (c) true (d) false (e) false (f) true

Exercise 1.5.2

Determine whether these statements are true or false:

a. $\sqrt{2} \in \mathbb{Z}$
b. $-1 \notin \mathbb{Z}^+$
c. $0 \in \mathbb{N}$
d. $\pi \in \mathbb{R}$
e. $\frac{4}{2} \in \mathbb{Q}$
f. $1.5 \in \mathbb{Q}$

Exercise 1.5.3

Explain why $7\mathbb{Q} = \mathbb{Q}$. Is it still true that $0\mathbb{Q} = \mathbb{Q}$?

Answer

By definition, a rational number can be written as a ratio of two integers. After multiplying the numerator by 7, we still have a ratio of two integers. Conversely, given any rational number x, we can multiply the denominator by 7, we obtain another rational number y such that $7y = x$. Hence, the two sets $7\mathbb{Q}$ and $\mathbb{Q}$ contain the same collection of rational numbers. In contrast, $0\mathbb{Q}$ contains only one number, namely, 0. Therefore, $0\mathbb{Q} \neq \mathbb{Q}$.

Exercise 1.5.4

Find the number(s) k such that $k\mathbb{Z} = \mathbb{Z}$.

Exercise 1.5.5

Determine whether these statements are true or false:

(See section on Closure.)

a. The set of natural numbers is closed under subtraction.
b. The set of integers is closed under subtraction.
c. The set of integers is closed under division.
d. The set of rational numbers is closed under subtraction.
e. The set of rational numbers is closed under division.
f. $\mathbb{Q}^*$ is closed under division.

Answer

(a) false (b) true (c) false (d) true (e) false (f) true

CHAPTER OVERVIEW

2: Logic

2.1: Propositions

The rules of logic allow us to distinguish between valid and invalid arguments. Besides mathematics, logic has numerous applications in computer science, including the design of computer circuits and the construction of computer programs. To analyze whether a certain argument is valid, we first extract its syntax.

Example 2.1.1

These two arguments:

- If $x+1=5$, then $x=4$. Therefore, if $x\neq 4$, then $x+1\neq 5$.
- If I watch Monday night football, then I will miss the following Tuesday 8 a.m. class. Therefore, if I do not miss my Tuesday 8 a.m. class, then I did not watch football the previous Monday night.

use the same format:

If p then q. Therefore if q is false then p is false.

If we can establish the validity of this type of argument, then we have proved *at once* that both arguments are legitimate. In fact, we have also proved that any argument using the same format is also credible.

Hands-on Exercise 2.1.1

Can you give another argument that uses the same format in the last example?

In mathematics, we are interested in statements that can be proved or disproved. We define a ***proposition*** (sometimes called a ***statement***, or an ***assertion***) to be a sentence that is either true or false, but not both.

Example 2.1.2

The following sentences:

- Barack Obama is the president of the United States.
- $2+3=6$.

are propositions, because each of them is either true or false (but not both).

Example 2.1.3

These two sentences:

- Ouch!
- What time is it?

are not propositions because they do not proclaim anything; they are exclamation and question, respectively.

Example 2.1.4

Explain why the following sentences are *not* propositions:

a. $x+1=2$.
b. $x-y=y-x$.
c. $A^2=0$ implies $A=0$.

Solution

a. This equation is not a statement because we cannot tell whether it is true or false unless we know the value of x. It is true when $x=1$; it is false for other x-values. Since the sentence is sometimes true and sometimes false, it cannot be a statement.
b. For the same reason, since $x-y=y-x$ is sometimes true and sometimes false, it cannot be a statement.
c. This looks like a statement because it appears to be true all the time. Yet, this is *not* a statement, because we never say what A represents. The claim is true if A is a real number, but it is not always true if A is a matrix[1]. Thus, it is not a

proposition.

Hands-on Exercise 2.1.2

Explain why these sentences are not propositions:

a. He is the quarterback of our football team.
b. $x+y=17$.
c. $AB=BA$.

Example 2.1.5

Although the sentence "$x+1=2$" is not a statement, we can change it into a statement by adding some condition on x. For instance, the following is a true statement:

For some real number x, we have $x+1=2$.

and the statement

For all real numbers x, we have $x+1=2$.

is false. The parts of these two statements that say "for some real number x" and "for all real numbers x" are called quantifiers. We shall study them in Section 6.

Example 2.1.6

Saying that

"A statement is not a proposition if we *cannot* decide whether it is true or false."

is different from saying that

"A statement is not a proposition if we do not know *how* to verify whether it is true or false."

The more important issue is whether the truth value of the statement can be determined in theory. Consider the sentence

Every even integer greater than 2 can be written as the sum of two primes.

Nobody has ever proved or disproved this claim, so we do not know whether it is true or false, even though computational data suggest it is true. Nevertheless, it *is* a proposition because it is either true or false but not both. It is impossible for this sentence to be true sometimes, and false at other times. With the advancement of mathematics, someone may be able to either prove or disprove it in the future. The example above is the famous ***Goldbach Conjecture***, which dates back to 1742.

We usually use the lowercase letters p, q and r to represent propositions. This can be compared to using variables x, y and z to denote real numbers. Since the truth values of p, q, and r vary, they are called ***propositional variables***. A proposition has only two possible values: it is either true or false. We often abbreviate these values as T and F, respectively.

Given a proposition p, we form another proposition by changing its truth value. The result is called the ***negation*** of p, and is denoted $\sim p$ or $\neg p$, both of which are pronounced as "not p." The similarity between the notations $\sim p$ and $-x$ is obvious.

We can also write the negation of p as $\overline{p}$, which is pronounced as "p bar." The truth value of $\overline{p}$ is opposite of that of p. Hence, if p is true, then $\overline{p}$ would be false; and if p is false, then $\overline{p}$ would be true. We summarize these results in a ***truth table***:

p	$\overline{p}$
T	F
F	T

Example 2.1.7

Find the negation of the following statements:

a. George W. Bush is the president of the United States.

b. It is not true that New York is the largest state in the United States.
c. x is a real number such that $x = 4$.
d. x is a real number such that $x < 4$.

If necessary, you may rephrase the negated statements, and change a mathematical notation to a more appropriate one.

Answer

a. George W. Bush is not the president of the United States.
b. It is true that New York is the largest state in the United States.
c. The phrase "x is a real number" describes what kinds of numbers we are considering. The main part of the proposition is the proclamation that $x = 4$. Hence, we only need to negate "$x = 4$". The answer is:

$$x \text{ is a real number such that } x \neq 4. \tag{2.1.1}$$

d. x is a real number such that $x \geq 4$.

Hands-on Exercise 2.1.3

a. x is an integer greater than 7. 0.4in
b. We can factor 144 into a product of prime numbers. 0.4in
c. The number 64 is a perfect square.

Summary and Review

- A proposition (statement or assertion) is a sentence which is either always true or always false.
- The negation of the statement p is denoted $\neg p$, $\sim p$, or $\overline{p}$.
- We can describe the effect of a logical operation by displaying a truth table which covers all possibilities (in terms of truth values) involved in the operation.

Exercises $\mathbf{2.1.}$

Exercise 2.1.1

Indicate which of the following are propositions (assume that x and y are real numbers).

a. The integer 36 is even.
b. Is the integer $3^{15} - 8$ even?
c. The product of 3 and 4 is 11.
d. The sum of x and y is 12.
e. If $x > 2$, then $x^2 \geq 3$.
f. $5^2 - 5 + 3$.

Answer

Only (a), (c), and (e) are propositions.

Exercise 2.1.2

Which of the following are propositions (assume that x is a real number)?

a. $2\pi + 5\pi = 7\pi$.
b. The product of x^2 and x^3 is x^6.
c. It is not possible for $3^{15} - 7$ to be both even and odd.
d. If the integer x is odd, is x^2 odd?
e. The integer $2^{524287} - 1$ is prime.
f. $1.7 + .2 = 4.0$.

Exercise 2.1.3

Determine the truth values of these statements:

a. The product of x^2 and x^3 is x^6 for any real number x.
b. $x^2 > 0$ for any real number x.
c. The number $3^{15} - 8$ is even.
d. The sum of two odd integers is even.

Answer

(a) false (b) false (c) false (d) true

Exercise 2.1.4

Determine the truth values of these statements:

a. $\pi \in \mathbb{Z}$.
b. $1^3 + 2^3 + 3^3 = 3^2 \cdot 4^2/4$.
c. u is a vowel.

Exercise 2.1.5

Negate these statements:

a. $\pi \in \mathbb{Z}$.
b. $1^3 + 2^3 + 3^3 = 3^2 \cdot 4^2/4$.
c. u is a vowel.

Answer

(a) $\pi \notin \mathbb{Z}$ (b) $1^3 + 2^3 + 3^3 \neq 3^2 \cdot 4^2/4$ (c) u is not a vowel

Exercise 2.1.6

Negate the following statements about the real number x:

a. $x > 0$
b. $x \leq -5$
c. $7 \leq x$

2.2: Conjunctions and Disjunctions

Given two real numbers x and y, we can form a new number by means of addition, subtraction, multiplication, or division, denoted $x+y$, $x-y$, $x\cdot y$, and x/y, respectively. The symbols $+$, $-$, $\cdot$, and $/$ are ***binary operators*** because they all work on two ***operands***. In fact, the negative sign in $-x$ can be regarded as a ***unary operator*** that changes the sign of x.

In a similar manner, from one or more logical statements, we can form a ***compound statement*** by joining them with ***logical operators***, which are also called ***logical connectives*** because they are used to connect logical statements. Obviously, negation is a unary operation.

Since a compound statement is itself a statement, it is either true or false. Therefore, we define a logical operation by describing the truth value of the resulting compound statement. The first two binary operations we shall study are conjunction and disjunction. They perform the "and" and "or" operations, respectively.

AND $\wedge$ OR $\vee$

name	meaning	notation	truth value
conjunction	p and q	$p\wedge q$	true if both p and q are true, false otherwise
disjunction	p or q	$p\vee q$	false if both p and q are false, true otherwise

Their truth values are summarized in the following truth table:

p	q	$p\wedge q$	$p\vee q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	F

Example 2.2.1

Do not use mathematical notations as abbreviation in writing. For example, do *not* write "$x\wedge y$ are real numbers" if you want to say "x and y are real numbers."

In fact, the phrase "$x\wedge y$ are real numbers" is syntactically incorrect. Since $\wedge$ is a binary *logical* operator, it is used to connect two logical statements. Here, the "x" before $\wedge$ is not a logical statement. Therefore we cannot write "$x\wedge y$ are real numbers."

Incidentally, the statement "x and y are real numbers" is actually a conjunction. It means "x is a real number and y is a real number," or symbolically,

$$(x\in\mathbb{R})\wedge(y\in\mathbb{R}). \tag{2.2.1}$$

It is wrong to write "$x\wedge y\in\mathbb{R}$." Can you explain why?

hands-on exercise 2.2.1

Write "x and y are rational" as a conjunction, first in words, then in mathematical symbols.

Example 2.2.2

The statement "New York is the largest state in the United States and New York City is the state capital of New York" is clearly a conjunction. A conjunction of two statements is true only when both statements are true. Since New York is not the largest state in the United States, the conjunction is false.

In general, in a conjunction of two statements, if the first statement is false, no further consideration of the second statement is necessary since we know the conjunction must be false. In computer science, this is referred to as the ***short circuit evaluation***.

Example 2.2.3

The statement "$\sqrt{30}$ is greater than 6 or $\sqrt{30}$ is less than 5" can be expressed symbolically as

$$\big(\sqrt{30} > 6\big) \vee \big(\sqrt{30} < 5\big). \tag{2.2.2}$$

Both statements "$\sqrt{30} > 6$" and "$\sqrt{30} < 5$" are false. Hence, their disjunction is also false.

Example 2.2.4

Determine the truth values of the following statements:

- $\big(\sqrt{30} > 5\big) \wedge \big(\sqrt{30} > 7\big)$
- Either $\big(\sqrt{30} < 5\big)$ or $\big(\sqrt{30} > 7\big)$

Solution

(a) Since $\sqrt{30} > 5$ is true, but $\sqrt{30} > 7$ is false, their conjunction is false.

(b) Since $\sqrt{30} < 5$ is false, and $\sqrt{30} > 7$ is also false, their disjunction is false.

hands-on exercise 2.2.2

Determine the truth values of the following statements:

- $\big(\sqrt{30} < 5\big)$ and $\big(\sqrt{30} > 7\big)$.
- $\big(\sqrt{30} > 5\big) \vee \big(\sqrt{30} < 7\big)$.

Be sure to show your reasons.

example 2.2.5

What does "$0 \leq x \leq 1$" really mean, logically?

Solution

It means the conjunction "$(x \geq 0) \wedge (x \leq 1)$." Hence, given a real number x, to test whether $0 \leq x \leq 1$, we have to check whether $x \geq 0$ *and* $x \leq 1$.

hands-on exercise 2.2.3

Write $5 < x < 8$ as a conjunction.

hands-on exercise 2.2.4

Many students assume that they can negate "$0 \leq x \leq 1$" by reversing the signs. However, neither "$0 \geq x \geq 1$" nor "$0 > x > 1$" is the correct negation. For example, what does "$0 \geq x \geq 1$" really mean? Actually, the statement "$0 \geq x \geq 1$" is syntactically correct, and it is always false. Can you explain why?

In the everyday usage of most languages, when we say "p or q," we normally mean ***exclusive or***, which means either p or q is true, but not both. An example is "I either pass or fail this course," which really means

Either I pass this course or I fail this course.

Sometimes, as illustrated in the statement

Either you pass this course, or I pass this course.

the connective "or" can be interpreted as an ***inclusive or***. The actual meaning of "or" in human languages depends on the context. In mathematics, however, "or" *always* means inclusive or.

Logically Equivalent

Definition

Two logical formulas p and q are said to be ***logically equivalent***, denoted

$$p \equiv q, \tag{2.2.3}$$

if p and q have have identical truth values in all cases.

Consider this truth table:

p	$\overline{p}$	$\overline{\overline{p}}$
T	F	T
F	T	F

Do you see the truth table above shows $p \equiv \overline{\overline{p}}$, ?

Summary and Review

- The conjunction "p and q" is denoted "$p \wedge q$". It is true only when both p and q are true.
- The disjunction "p or q" is denoted "$p \vee q$". It is false only when both p and q are false.
- The inequality "$a < x < b$" is actually a conjunction, it means "$(a < x) \wedge (x < b)$ ".
- Likewise, the phrase "x and y are rational" is also a conjunction, it means "x is rational and y is rational." Symbolically, we can write "$x \in \mathbb{Q} \wedge y \in \mathbb{Q}$."

Exercises **2.2.**

Exercise 2.2.1

Let p, q, and r represent the following statements:

p:	Sam had pizza last night.
q:	Chris finished her homework.
r:	Pat watched the news this morning.

Write each of these statements in symbolic form:

(a) Sam had pizza last night and Chris finished her homework.

(b) Chris did not finish her homework and Pat watched the news this morning.

(c) Sam did not have pizza last night or Chris did not finish her homework.

(d) Either Chris finished her homework or Pat watched the news this morning, but not both.

Answer

(a) $p \wedge q$
(b) $\overline{q} \wedge r$
(c) $\overline{p} \vee \overline{q}$
(d) $(q \vee r) \wedge \overline{q \wedge r}$

Exercise 2.2.2

Define the propositional variables p, q, and r as in Problem 1. Express, in words, the following symbolic statements:

(a) $p \vee q$

(b) $q \wedge r$

(c) $(p \wedge q) \vee r$

(d) $\overline{p} \vee r$

Exercise 2.2.3

Consider the following statements:

p:	Niagara Falls is in New York.
q:	New York City is the state capital of New York.
r:	New York City will have more than 40 inches of snow in 2525.

The statement p is true, but the statement q is false. Represent each of the following statements in symbolic form. What are their truth values if r is true? What if r is false?

(a) Niagara Falls is in New York and New York City is the state capital of New York.

(b) Niagara Falls is in New York or New York City is the state capital of New York.

(c) Either Niagara Falls is in New York and New York City is the state capital of New York, or New York City will have more than 40 inches of snow in 2525.

(d) New York City is not the state capital of New York and New York City will have more than 40 inches of snow in 2525.

Answer

(a) $p \wedge q$; always false regardless of the value of r.

(b) $p \vee q$; always true regardless of the value of r.

(c) $(p \wedge q) \vee r$; true if r is true, and false if r is false.

(d) $\overline{q} \wedge r$; true if r is true, and false if r is false

Exercise 2.2.4

Determine the truth values of these statements:

(a) $(0 \in \mathbb{Q}) \wedge (-4 \in \mathbb{Z})$

(b) $(-4 \in \mathbb{N}) \vee (3 \in 2\mathbb{Z})$

Exercise 2.2.5

Determine the truth values of these statements:

(a) $(-3 > -2) \wedge (\sqrt{3} > 2)$

(b) $(4^2 - 5^2 \leq 0) \vee (\sqrt{3^2 + 4^2} = 3 + 4)$

Answer

(a) false
(b) true

Exercise 2.2.6

Construct the truth tables for the following logic statements:

(a) $p \wedge \overline{q}$

(b) $\overline{p} \vee q$

(c) $\overline{p \wedge q}$

Exercise 2.2.7

Rewrite the following expressions as conjunction:

(a) $4 \leq x \leq 7$

(b) $4 < x \leq 7$

(c) $4 \leq x < 7$

Answer

(a) $(x \geq 4) \wedge (x \leq 7)$
(b) $(x > 4) \wedge (x \leq 7)$
(c) $(x \geq 4) \wedge (x < 7)$

Exercise 2.2.8

In words, the inequality $0 < x < 1$ means "x is between 0 and 1." Its negation means x is outside this range. Hence, the negation is "$x \leq 0$ or $x \geq 1$." Find the negation of the following inequalities:

(a) $0 \leq x \leq 4$

(b) $-2 < x \leq 5$

(c) $1.76 \leq x < \sqrt{5}$

Exercise 2.2.9

In volleyball it is important to know which team is serving, because a team scores a point only if that team is serving and wins a volley. If the serving team loses the volley, then the other team gets to serve. Thus, to keep score in a volleyball game between teams A and B, it may be useful to define propositional variables p and q, where p is true if team A is serving (hence false if team B is serving); and q is true if team A wins the current volley (hence false if team B wins it).

- Give a formula that is true if team A scores a point and is false otherwise.
- Give a formula that is true if team B scores a point and is false otherwise.
- Give a formula that is true if the serving team loses the current volley and is false otherwise.
- Give a formula whose truth value determines whether the serving team will serve again.

Exercise 2.2.10

Construct the truth tables for the following logic statements:

(a) $p \wedge \overline{p}$

(b) $p \vee \overline{p}$

(c) $p \wedge (q \vee r)$

(d) $(p \wedge q) \vee (q \wedge r)$

(e) $p \vee (q \wedge \overline{r})$

Exercise 2.2.11

The ***exclusive or*** operation, denoted $p \veebar q$, means "p or q, but not both."

Construct the truth table for $p \veebar q$.

Answer

p	q	$p \veebar q$
T	T	F
T	F	T
F	T	T
F	F	F

2.3: Implications

Most theorems in mathematics appear in the form of compound statements called conditional and biconditional statements. We shall study biconditional statement in the next section. Conditional statements are also called implications.

Implication $\Rightarrow$

An ***implication*** is the compound statement of the form "if p, then q." It is denoted $p \Rightarrow q$, which is read as "p implies q." It is false only when p is true and q is false, and is true in all other situations.

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

The statement p in an implication $p \Rightarrow q$ is called its ***hypothesis***, ***premise***, or ***antecedent***, and q the ***conclusion*** or ***consequence***.

Implications come in many disguised forms. There are several alternatives for saying $p \Rightarrow q$. The most common ones are

- p implies q,
- p only if q,
- q if p,
- q, provided that p.

All of them mean $p \Rightarrow q$.

Implications play a key role in logical argument. If an implication is known to be true, then whenever the hypothesis is met, the consequence must be true as well. This is why an implication is also called a ***conditional statement***.

Example 2.3.1

The quadratic formula asserts that

$$b^2 - 4ac > 0 \quad \Rightarrow \quad ax^2 + bx + c = 0 \text{ has two distinct real solutions.} \tag{2.3.1}$$

Consequently, the equation $x^2 - 3x + 1 = 0$ has two distinct real solutions because its coefficients satisfy the inequality $b^2 - 4ac > 0$.

hands-on exercise 2.3.1

More generally,

- If $b^2 - 4ac > 0$, then the equation $ax^2 + bx + c = 0$ has two distinct real solutions. In fact, $ax^2 + bx + c = a(x - r_1)(x - r_2)$, where $r_1 \neq r_2$ are the two distinct roots.
- If $b^2 - 4ac = 0$, then the equation $ax^2 + bx + c = 0$ has only one real solution r. In such an event, $ax^2 + bx + c = a(x - r)^2$. Consequently, we call r a repeated root.
- If $b^2 - 4ac = 0$, then the equation $ax^2 + bx + c = 0$ has no real solution.

Use these results to determine how many solutions these equations have:

a. $4x^2 + 12x + 9 = 0$
b. $2x^2 - 3x - 4 = 0$
c. $x^2 + x = -1$

Example 2.3.2

We have remarked earlier that many theorems in mathematics are in the form of implications. Here is an example:

- If $|r|<1$, then $1+r+r^2+r^3+\cdots=\frac{1}{1-r}$.
- It means, symbolically, $|r|<1 \Rightarrow 1+r+r^2+r^3+\cdots=\frac{1}{1-r}$.

hands-on exercise 2.3.2

Express the following statement in symbols:

If $x>y>0$, then $x^2>y^2$.

Example 2.3.3

If a father promises his kids, "If tomorrow is sunny, we will go to the beach," the kids will take it as a true statement. Consequently, if they wake up the next morning and find it sunny outside, they expect they will go to the beach. The father breaks his promise (hence making the implication false) only when it is sunny but he does not take his kids to the beach.

If it is cloudy outside the next morning, they do not know whether they will go to the beach, because no conclusion can be drawn from the implication (their father's promise) if the weather is bad. Nonetheless, they may still go to the beach, even if it rains! Since their father does not contradict his promise, the implication is still true.

Many students are bothered by the validity of an implication even when the hypothesis is false. It may help if we understand how we use an implication.

Solution

Assume we want to show that a certain statement q is true.

a. First, we find a result of the form $p \Rightarrow q$. If we cannot find one, we have to prove that $p \Rightarrow q$ is true.
b. Next, show that the hypothesis p is fulfilled.
c. These two steps together allow us to draw the conclusion that q must be true.

Consequently, if p is false, we are not expected to use the implication $p \Rightarrow q$ at all. Since we are not are going to use it, we can define its truth value to anything we like. Nonetheless, we have to maintain [pg:consistence] consistency with other logical connectives. We will give a justification of our choice at the end of the next section.

Example 2.3.4

To show that "if $x=2$, then $x^2=4$" is true, we need not worry about those x-values that are not equal to 2, because the implication is immediately true if $x \neq 2$. It suffices to assume that $x=2$, and try to prove that we *will* get $x^2=4$. Since we do have $x^2=4$ when $x=2$, the validity of the implication is established.

In contrast, to determine whether the implication "if $x^2=4$, then $x=2$" is true, we assume $x^2=4$, and try to determine whether x *must* be 2. Since $x=-2$ makes $x^2=4$ true but $x=2$ false, the implication is false.

In general, to disprove an implication, it suffices to find a counterexample that makes the hypothesis true and the conclusion false.

hands-on exercise 2.3.3

Determine whether these two statements are true or false:

a. If $(x-2)(x-3)=0$, then $x=2$.
b. If $x=2$, then $(x-2)(x-3)=0$.

Explain.

Example 2.3.5

Although we said examples can be used to disprove a claim, examples alone can *never* be used as proofs. If you are asked to show that

$$\text{if } x>2, \text{ then } x^2>4, \tag{2.3.2}$$

you cannot prove it by *checking* just a few values of x, because you may find a counterexample after trying a few more calculations. Therefore, examples are only for illustrative purposes, they are *not* acceptable as proofs.

Example 2.3.6

The statement

"If a triangle PQR is isosceles, then two of its angles have equal measure."

takes the form of an implication $p \Rightarrow q$, where

$$\begin{array}{rl} p: & \text{The triangle } PQR \text{ is isosceles} \\ q: & \text{Two of the angles of the triangle } PQR \text{ have equal measure} \end{array} \tag{2.3.3}$$

In this example, we have to rephrase the statements p and q, because each of them should be a stand-alone statement. If we leave q as "two of its angles have equal measure," it is not clear what "its" is referring to. In addition, it is a good habit to spell out the details. It helps us focus our attention on what we are investigating.

Example 2.3.7

The statement

"A square must also be a parallelogram."

can be expressed as an implication: "if the quadrilateral $PQRS$ is a square, then the quadrilateral $PQRS$ is a parallelogram."

Likewise, the statement

"All isosceles triangles have two equal angles."

can be rephrased as "if the triangle PQR is isosceles, then the triangle PQR has two equal angles." Since we have expressed the statement in the form of an implication, we no longer need to include the word "all."

hands-on exercise 2.3.1

Rewrite each of these logical statements:

a. Any square is also a parallelogram.
b. A prime number is an integer.
c. All polynomials are differentiable.

as an implication $p \Rightarrow q$. Specify what p and q are.

Example 2.3.8

What does "p unless q" translate into, logically speaking? We know that p is true, provided that q does not happen. It means, in symbol, $\overline{q} \Rightarrow p$. Therefore,

The quadrilateral $PQRS$ is not a square unless the quadrilateral $PQRS$ is a parallelogram

is the same as saying

If a quadrilateral $PQRS$ is not a parallelogram, then the quadrilateral $PQRS$ is not a square.

Equivalently, "p unless q" means $\overline{p} \Rightarrow q$, because q is a necessary condition that prevents p from happening.

Converse, Inverse, Contrapositive

Given an implication $p \Rightarrow q$, we define three related implications:

- Its ***converse*** is defined as $q \Rightarrow p$.
- Its ***inverse*** is defined as $\overline{p} \Rightarrow \overline{q}$.
- Its ***contrapositive*** is defined as $\overline{q} \Rightarrow \overline{p}$.

Among them, the contrapositive $\overline{q} \Rightarrow \overline{p}$ is the most important one. We shall study it again in the next section.

Example 2.3.9

The converse, inverse, and contrapositive of "$x > 2 \Rightarrow x^2 > 4$" are listed below.

$$ \tag{2.3.4} $$

We can change the notation when we negate a statement. If it is appropriate, we may even rephrase a sentence to make the negation more readable.

Example 2.3.5

List the converse, inverse, and contrapositive of the statement "if p is prime, then $\sqrt{p}$ is irrational."

The inverse of an implication is seldom used in mathematics, so we will only study the truth values of the converse and contrapositive.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$\overline{q}$	$\overline{p}$	$\overline{q} \Rightarrow \overline{p}$
T	T	T	T	F	F	T
T	F	F	T	T	F	F
F	T	T	F	F	T	T
F	F	T	T	T	T	T

(2.3.5)

An implication and its contrapositive always have the same truth value, but this is not true for the converse. What this means is, even though we know $p \Rightarrow q$ is true, there is no guarantee that $q \Rightarrow p$ is also true. This is an important observation, especially when we have a theorem stated in the form of an implication. So let us say it again:

$$\boxed{\text{The converse of a theorem in the form of an implication may not be true.}} \tag{2.3.6}$$

Accordingly, if you only know that $p \Rightarrow q$ is true, do not assume that its converse $q \Rightarrow p$ is also true. Likewise, if you are asked to prove that $p \Rightarrow q$ is true, do not attempt to prove $q \Rightarrow p$, because these two implications are not the same.

Example 2.3.10

We know that $p \Rightarrow q$ does not necessarily mean we also have $q \Rightarrow p$. This important observation explains the invalidity of the "proof" of $21 = 6$ in this example.

$$\begin{aligned} 21 &= 6 \\ 6 &= 21 \\ 27 &= 27 \end{aligned}$$

The argument we use here consists of three equations, but they are not individual unrelated equations. They are connected by implication.

$$\begin{aligned} & 21 = 6 \\ \Rightarrow \quad & 6 = 21 \\ \Rightarrow \quad & 27 = 27 \end{aligned}$$

Since implications are not reversible, even though we do have $27 = 27$, we cannot use this fact to prove that $21 = 6$. After all, an implication is true if its hypothesis is false. Therefore, having a true implication does not mean that its hypothesis must be true. In this example, the logic is sound, but it does not prove that $21 = 6$.

Sufficient, Necessary

There are two other ways to describe an implication $p \Rightarrow q$ in words. They are completely different from the ones we have seen thus far. They focus on whether we can tell one of the two components p and q is true or false if we know the truth value of the other.

- p is a ***sufficient condition*** for q
- q is a ***necessary condition*** for p.

They are difficult to remember, and can be easily confused. You may want to visualize it pictorially:

$$\boxed{\text{sufficient condition} \Rightarrow \text{necessary condition.}} \tag{2.3.7}$$

The idea is, assuming that $p \Rightarrow q$ is true, then

- For q to be true, it is enough to know or show that p is true. Hence, knowing p is true alone is sufficient for us to draw the conclusion the q must also be true.
- For p to be true, it is necessary to have q be true as well. Thus, knowing q is true does not necessarily mean that p must be true.

Example 2.3.11

Consider the implication

$$x = 1 \Rightarrow x^2 = 1. \tag{2.3.8}$$

If $x = 1$, we must have $x^2 = 1$. So, knowing $x = 1$ is enough for us to conclude that $x^2 = 1$. We say that $x = 1$ is a sufficient condition for $x^2 = 1$.

If $x = 1$, it is necessarily true that $x^2 = 1$, because, for example, it is impossible to have $x^2 = 2$. Nonetheless, knowing $x^2 = 1$ alone is not enough for us to decide whether $x = 1$, because x can be -1. Therefore, $x^2 = 1$ is *not* a sufficient condition for $x = 1$. Instead, $x^2 = 1$ is only a necessary condition for $x = 1$.

hands-on exercise 2.3.6

Write these statements:

a. For $x^2 > 1$, it is sufficient that $x > 1$.
b. For $x^2 > 1$, it is necessary that $x > 1$.

in the form of $p \Rightarrow q$. Be sure to specify what p and q are.

Summary and Review

- An implication $p \Rightarrow q$ is false only when p is true and q is false.
- This is how we typically use an implication. Assume we want to show that q is true. We have to find or prove a theorem that says $p \Rightarrow q$. Next, we need to show that hypothesis p is met, hence it follows that q must be true.
- An implication can be described in several other ways. Can you name a few of them?
- Converse, inverse, and contrapositive are obtained from an implication by switching the hypothesis and the consequence, sometimes together with negation.
- In an implication $p \Rightarrow q$, the component p is called the sufficient condition, and the component q is called the necessary condition.

Exercises 2.3.

Exercise 2.3.1

Let p, q, and r represent the following statements:

p:	Sam had pizza last night.
q:	Chris finished her homework.
r:	Pat watched the news this morning.

Write a symbolic statement for each of the following:

a. If Sam had pizza last night then Chris finished her homework.
b. Pat watched the news this morning only if Sam had pizza last night.
c. Chris finished her homework if Sam did not have pizza last night.
d. If it is not the case that Sam had pizza last night, then Pat watched the news this morning.
e. Sam did not have pizza last night and Chris finished her homework implies that Pat watched the news this morning.

Answer

(a) $p \Rightarrow q$
(b) $r \Rightarrow p$
(c) $\overline{p} \Rightarrow q$
(d) $\overline{p} \Rightarrow r$
(e) $(\overline{p} \wedge q) \Rightarrow r$

Exercise 2.3.2

Define the propositional variables as in Problem 1. Express in words the following logic statements:

a. $q \Rightarrow r$
b. $p \Rightarrow (q \wedge r)$
c. $\overline{p} \Rightarrow (q \vee r)$
d. $r \Rightarrow (p \vee q)$

Exercise 2.3.3

Consider the following statements:

p:	Niagara Falls is in New York.
q:	New York City is the state capital of New York.
r:	New York City will have more than 40 inches of snow in 2525.

The statement p is true, and the statement q is false. Represent each of the following statements symbolically. What is their truth value if r is true? What if r is false?

a. If Niagara Falls is in New York, then New York City is the state capital of New York.
b. Niagara Falls is in New York only if New York City will have more than 40 inches of snow in 2525.
c. Niagara Falls is in New York or New York City is the state capital of New York implies that New York City will have more than 40 inches of snow in 2525.
d. For New York City to be the state capital of New York, it is necessary that New York City will have more than 40 inches of snow in 2525.e
e. For Niagara Falls to be in New York, it is sufficient that New York City will have more than 40 inches of snow in 2525.

Answer

(a) $p \Rightarrow q$, which is false.

(b) $p \Rightarrow r$, which is true if r is true, and is false if r is false.

(c) $(p \vee q) \Rightarrow r$, which is true if r is true, and is false if r is false.
(d) $q \Rightarrow r$, which is true regardless of the whether r is true or false.
(e) $r \Rightarrow p$, which is true regardless of the whether r is true or false.

Exercise 2.3.4

Express each of the following compound statements symbolically:

a. The line L_1 is perpendicular to the line L_2 and the line L_2 is parallel to the line L_3 implies that L_1 is perpendicular to L_3.
b. If $\sqrt{47089}$ is greater than 200 and $\sqrt{47089}$ is an integer, then $\sqrt{47089}$ is prime.
c. If $\sqrt{47089}$ is greater than 200, then, if $\sqrt{47089}$ is prime, it is greater than 210.
d. If $x^3 - 3x^2 + x - 3 = 0$, then either x is positive or x is negative or $x = 0$.

Exercise 2.3.5

Express each of the following compound statements in symbols.

a. $x^3 - 3x^2 + x - 3 = 0$ only if $x = 3$.

b. A necessary condition for $x^3-3x^2+x-3=0$ is $x=3$.
c. A sufficient condition for $x^3-3x^2+x-3=0$ is $x=3$.
d. If e^π is a real number, then e^π is either rational or irrational.
e. All NFL players are huge.

Answer

(a) $x^3-3x^2+x-3=0 \Rightarrow x=3$

(b) $x^3-3x^2+x-3=0 \Rightarrow x=3$

(c) $x=3 \Rightarrow x^3-3x^2+x-3=0$

(d) $e^\pi \in \mathbb{R} \Rightarrow (e^\pi \in \mathbb{Q} \vee e^\pi \text{ is an irrational number})$

(e) A person is an NFL player $\Rightarrow$ that person is huge.

Exercise 2.3.6

Original statement: If I do not eat diner, I will wake up early.

(a) Find the converse, inverse, and contrapositive of the original statement.

(b) Which of the statements you wrote in (a) have the same meaning as the original statement?

Exercise 2.3.7

Original statement about quadrilateral $ABCD$: If $ABCD$ is a rectangle, then $ABCD$ is a parallelogram.

(a) Find the converse, inverse, and contrapositive of the original statement.

(b) Determine the truth value of the original statement, converse, inverse, and contrapositive.

Answer

(a) converse: If $ABCD$ is a parallelogram, then $ABCD$ is a rectangle.
inverse: If $ABCD$ is not a rectangle, then $ABCD$ is not a parallelogram.
contrapositive: If $ABCD$ is not a parallelogram, then $ABCD$ is not a rectangle.
(b) The original & the contrapositive are true; the converse & inverse are false.

Exercise 2.3.8

Original statement: If I do not eat dinner, I will wake up early.

(a) Rewrite the original as an equivalent statement that uses the word "necessary".

(b) Rewrite the original as an equivalent statement that uses the word "sufficient"

Exercise 2.3.9

Construct the truth tables for the following expressions:

a. $(p \wedge q) \vee r$
b. $(p \vee q) \Rightarrow (p \wedge r)$

Answer

p	q	r	$p\wedge q$	$(p\wedge q)\vee r$
T	T	T	T	T
T	T	F	T	T
T	F	T	F	T
T	F	F	F	F
F	T	T	F	T
F	T	F	F	F
F	F	T	F	T
F	F	F	F	F

p	q	r	$p\vee q$	$p\wedge r$	$(p\vee q)\Rightarrow(p\wedge r)$
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	T	T	T
T	F	F	T	F	F
F	T	T	T	F	F
F	T	F	T	F	F
F	F	T	F	F	T
F	F	F	F	F	T

Exercise 2.3.10

Construct the truth tables for the following expressions:

a. $(p\Rightarrow q)\vee(\overline{p}\Rightarrow q)$
b. $(p\Rightarrow q)\wedge(\overline{p}\Rightarrow q)$

Exercise 2.3.11

Determine (you may use a truth table) the truth value of p if

a. $(p\wedge q)\Rightarrow(q\vee r)$ is false
b. $(q\wedge r)\Rightarrow(p\wedge q)$ is false

Answer

(a) Using a truth table, we find that the implication $(p\wedge q)\Rightarrow(q\vee r)$ is always true. Hence, no truth value of p would make $(p\wedge q)\Rightarrow(q\vee r)$ false.

(b) From a truth table, we find that, $(q\wedge r)\Rightarrow(p\wedge q)$ is false only when p is false. We can draw the same conclusion without using any truth table. An implication is false only when its hypothesis (in this case, $q\wedge r$) is true *and* its conclusion (in this case, $p\wedge q$) is false. For $q\wedge r$ to be true, we need both q and r to be true. Now q is true and $p\wedge q$ is false require p to be false.

Exercise 2.3.12

Assume $p\Rightarrow q$ is true.

a. If p is true, must q be true? Explain.
b. If p is false, must q be true? Explain.
c. If q is true, must p be false? Explain.
d. If q if false, must p be false? Explain.

2.4: Biconditional Statements

Biconditional $p \Leftrightarrow q$

The ***biconditional statement*** "p if and only if q," denoted $p \Leftrightarrow q$, is true when both p and q carry the same truth value, and is false otherwise. It is sometimes abbreviated as "p iff q." Its truth table is depicted below.

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 2.4.1

The following biconditional statements

$2x-5=0 \Leftrightarrow x=5/2$,

$x>y \Leftrightarrow x-y>0$,

are true, because, in both examples, the two statements joined by $\Leftrightarrow$ are true or false simultaneously.

A biconditional statement can also be defined as the compound statement

$$(p \Rightarrow q) \wedge (q \Rightarrow p). \tag{2.4.1}$$

This explains why we call it a biconditional statement. A biconditional statement is often used to define a new concept.

Example 2.4.2

A number is even if and only if it is a multiple of 2. Mathematically, this means

$$n \text{ is even} \Leftrightarrow n=2q \text{ for some integer } q. \tag{2.4.2}$$

It follows that for any integer m,

$$mn = m \cdot 2q = 2(mq). \tag{2.4.3}$$

Since mq is an integer (because it is a product of two integers), by definition, mn is even. This shows that the product of any integer with an even integer is always even.

hands-on exercise 2.4.1

Complete the following statement:

$$n \text{ is odd} \Leftrightarrow \qquad\qquad\qquad . \tag{2.4.4}$$

Use this to prove that if n is odd, then n^2 is also odd.

Example 2.4.3

The operation "exclusive or" can be defined as

$$p \veebar q \Leftrightarrow (p \vee q) \wedge \overline{(p \wedge q)}. \tag{2.4.5}$$

See Exercise 2.2.11.

Order of Logical Operations

When we have a complex statement involving more than one logical operation, care must be taken to determine which operation should be carried out first. The ***precedence*** or ***priority*** is listed below.

Connectives	Priority
$\neg$	Highest
$\vee$, $\wedge$	$\vdots$
$\Rightarrow$	
$\Leftrightarrow$	Lowest

This is the order in which the operations should be carried out if the logical expression is read from left to right. To override the precedence, use parentheses.

Example 2.4.4

The precedence of logical operations can be compared to those of arithmetic operations.

Operations	Priority
$-$ (Negative)	Highest
Exponentiation	$\vdots$
Multiplication/Division	$\vdots$
Addition/Subtraction	Lowest

For example, $yz^{-3} \neq (yz)^{-3}$. To evaluate yz^{-3}, we have to perform exponentiation first. Hence, $yz^{-3} = y \cdot z^{-3} = \frac{y}{z^3}$.

Another example: the notation x^{2^3} means x raised to the power of 2^3, hence $x^{2^3} = x^8$; it should *not* be interpreted as $(x^2)^3$, because $(x^2)^3 = x^6$.

Example 2.4.5

It is not true that $p \Leftrightarrow q$ can be written as "$p \Rightarrow q \wedge q \Rightarrow p$," because it would mean, technically,

$$p \Rightarrow (q \wedge q) \Rightarrow p. \tag{2.4.6}$$

The correct notation is $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

hands-on exercise2.4.2

Insert parentheses in the following formula

$$p \Rightarrow q \wedge r \tag{2.4.7}$$

to identify the proper procedure for evaluating its truth value. Construct its truth table.

hand-on exercise 2.4.3

Insert parentheses in the following formula

$$p \wedge q \Leftrightarrow \overline{p} \vee \overline{q}. \tag{2.4.8}$$

to identify the proper procedure for evaluating its truth value. Construct its truth table.

More on Conditional $p \Rightarrow q$

We close this section with a justification of our choice in the truth value of $p \Rightarrow q$ when p is false. The truth value of $p \Rightarrow q$ is obvious when p is true.

p	q	$p \Rightarrow q$

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	?
F	F	?

We want to decide what are the best choices for the two missing values so that they are consistent with the other logical connectives. Observe that if $p \Rightarrow q$ is true, and q is false, then p must be false as well, because if p were true, with q being false, then the implication $p \Rightarrow q$ would have been false. For instance, if we promise

"If tomorrow is sunny, we will go to the beach"

but we do not go to the beach tomorrow, then we know tomorrow must not be sunny. This means the two statements $p \Rightarrow q$ and $\overline{q} \Rightarrow \overline{p}$ should share the same truth value.

When both p and q are false, then both $\overline{p}$ and $\overline{q}$ are true. Hence $\overline{q} \Rightarrow \overline{p}$ should be true, consequently so is $p \Rightarrow q$. Thus far, we have the following partially completed truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	?
F	F	T

If the last missing entry is F, the resulting truth table would be identical to that of $p \Leftrightarrow q$. To distinguish $p \Leftrightarrow q$ from $p \Rightarrow q$, we have to define $p \Rightarrow q$ to be true in this case.

Summary and Review

- A biconditional statement $p \Leftrightarrow q$ is the combination of the two implications $p \Rightarrow q$ and $q \Rightarrow p$.
- The biconditional statement $p \Leftrightarrow q$ is true when both p and q have the same truth value, and is false otherwise.
- A biconditional statement is often used in defining a notation or a mathematical concept.

Exercises 2.4.

Exercise 2.4.1

Let p, q, and r represent the following statements:

p:	Sam had pizza last night.
q:	Chris finished her homework.
r:	Pat watched the news this morning.

Write a symbolic statement for each of these:

(a) Sam had pizza last night if and only if Chris finished her homework.

(b) Pat watched the news this morning iff Sam did not have pizza last night.

(c) Pat watched the news this morning if and only if Chris finished her homework and Sam did not have pizza last night as well.

(d) In order for Pat to watch the news this morning, it is necessary and sufficient that both Sam had pizza last night and Chris finished her homework.

Answer

(a) $p \Leftrightarrow q$
(b) $r \Leftrightarrow \overline{p}$
(c) $r \Leftrightarrow (q \wedge \overline{p})$
(d) $r \Leftrightarrow (p \wedge q)$

Exercise 2.4.2

Define the propositional variables as in Problem 1. Express in words the statements represented by the following symbolic statements:

(a) $q \Leftrightarrow r$
(b) $p \Leftrightarrow (q \wedge r)$
(c) $\overline{p} \Leftrightarrow (q \vee r)$
(d) $r \Leftrightarrow (p \vee q)$

Exercise 2.4.3

Consider the following statements:

p:	Niagara Falls is in New York.
q:	New York City is the state capital of New York.
r:	New York City will have more than 40 inches of snow in 2525.

The statement p is true, and the statement q is false. Represent each of the following statements symbolically. What is their truth value if r is true? What if r is false?

a. Niagara Falls is in New York if and only if New York City is the state capital of New York.
b. Niagara Falls is in New York iff New York City will have more than 40 inches of snow in 2525.
c. Niagara Falls is in New York or New York City is the state capital of New York if and only if New York City will have more than 40 inches of snow in 2525.

Answer

(a) $p \Leftrightarrow q$, which is false.

(b) $p \Leftrightarrow r$, which is true if r is true, and is false if r is false.

(c) $(p \vee q) \Leftrightarrow r$, which is true if r is true, and is false if r is false.

Exercise 2.4.4

Express each of the following compound statements symbolically:

a. The product $xy = 0$ if and only if either $x = 0$ or $y = 0$.
b. The integer $n = 4$ if and only if $7n - 5 = 23$.
c. A necessary condition for $x = 2$ is $x^4 - x^2 - 12 = 0$.
d. A sufficient condition for $x = 2$ is $x^4 - x^2 - 12 = 0$.
e. For $x^4 - x^2 - 12 = 0$, it is both sufficient and necessary to have $x = 2$.
f. The sum of squares $x^2 + y^2 > 1$ iff both x and y are greater than 1.

Exercise 2.4.5

Determine the truth values of the following statements (assuming that x and y are real numbers):

a. The product $xy = 0$ if and only if either $x = 0$ or $y = 0$.
b. The sum of squares $x^2 + y^2 > 1$ iff both x and y are greater than 1.
c. $x^2 - 4x + 3 = 0 \Leftrightarrow x = 3$.
d. $x^2 > y^2 \Leftrightarrow x > y$.

Answer

(a) true (b) false (c) false (d) false

Exercise 2.4.6

Determine the truth values of the following statements (assuming that x and y are real numbers):

a. u is a vowel if and only if b is a consonant.
b. $x^2+y^2=0$ if and only if $x=0$ and $y=0$.
c. $x^2-4x+4=0$ if and only if $x=2$.
d. $xy\neq 0$ if and only if x and y are both positive.

Exercise 2.4.7

We have seen that a number n is even if and only if $n=2q$ for some integer q. Accordingly, what can you say about an odd number?

Answer

We say n is odd if and only if $n=2q+1$ for some integer q.

Exercise 2.4.8

We also say that an integer n is even if it is divisible by 2, hence it can be written as $n=2q$ for some integer q, where q represents the quotient when n is divided by 2. Thus, n is even if it is a multiple of 2. What if the integer n is a multiple of 3? What form must it take? What if n is not a multiple of 3?

2.5: Logical Equivalences

Tautology & Contradiction

Definition

A ***tautology*** is a proposition that is always true, regardless of the truth values of the propositional variables it contains.

Definition

A proposition that is always false is called a ***contradiction***.

A proposition that is neither a tautology nor a contradiction is called a ***contingency***. The term contingency is not as widely used as the terms tautology and contradiction.

Example 2.5.1

From the following truth table

p	$\overline{p}$	$p\vee\overline{p}$	$p\wedge\overline{p}$
T	F	T	F
F	T	T	F

(2.5.1)

we gather that $p\vee\overline{p}$ is a tautology, and $p\wedge\overline{p}$ is a contradiction.

In words, $p\vee\overline{p}$ says that either the statement p is true, or the statement $\overline{p}$ is true (that is, p is false). This claim is always true.

The compound statement $p\wedge\overline{p}$ claims that p is true, and at the same time, $\overline{p}$ is also true (which means p is false). This is clearly impossible. Hence, $p\wedge\overline{p}$ must be false.

Example 2.5.2

Show that $(p\Rightarrow q)\Leftrightarrow(\overline{q}\Rightarrow\overline{p})$ is a tautology.

Answer

We can use a truth table to verify the claim.

p	q	$p\Rightarrow q$	$\overline{q}$	$\overline{p}$	$\overline{q}\Rightarrow\overline{p}$	$(p\Rightarrow q)\Leftrightarrow(\overline{q}\Rightarrow\overline{p})$
T	T	T	T	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	F	T	T	T	T	T

(2.5.2)

Note how we work on each component of the compound statement separately before putting them together to obtain the final answer.

Example 2.5.3

Show that the argument

"If p and q, then r. Therefore, if not r, then not p or not q."

is valid. In other words, show that the logic used in the argument is correct.

Answer

Symbolically, the argument says

$$[(p\wedge q)\Rightarrow r]\Rightarrow[\overline{r}\Rightarrow(\overline{p}\vee\overline{q})]. \tag{2.5.3}$$

We want to show that it is a tautology. It is easy to verify with a truth table. We can also argue that this compound statement is always true by showing that it can never be false.

Suppose, on the contrary, that ([eqn:tautology]) is false for some choices of p, q, and r. Then

$$(p \wedge q) \Rightarrow r \quad \text{must be true,} \qquad \text{and} \qquad \overline{r} \Rightarrow (\overline{p} \vee \overline{q}) \quad \text{must be false.} \tag{2.5.4}$$

For the second implication to be false, we need

$$\overline{r} \quad \text{to be true,} \qquad \text{and} \qquad \overline{p} \vee \overline{q} \quad \text{to be false.} \tag{2.5.5}$$

They in turn imply that r is false, and both $\overline{p}$ and $\overline{q}$ are false; hence both p and q are true. This would make $(p \wedge q) \Rightarrow r$ false, contradicting the assumption that it is true. Thus, ([eqn:tautology]) cannot be false, it must be a tautology.

hands-on exercise 2.5.1

Use a truth table to show that

$$[(p \wedge q) \Rightarrow r] \Rightarrow [\overline{r} \Rightarrow (\overline{p} \vee \overline{q})] \tag{2.5.6}$$

is a tautology.

Answer

We need eight combinations of truth values in p, q, and r. We list the truth values according to the following convention. In the first column for the truth values of p, fill the upper half with T and the lower half with F. In the next column for the truth values of q, repeat the same pattern, separately, with the upper half and the lower half. So we split the upper half of the second column into two halves, fill the top half with T and the lower half with F. Likewise, split the lower half of the second column into two halves, fill the top half with T and the lower half with F. Repeat the same pattern with the third column for the truth values of r, and so on if we have more propositional variables.

Complete the following table:

p	q	r	$p \wedge q$	$(p \wedge q) \Rightarrow r$	$\overline{r}$	$\overline{p}$	$\overline{q}$	$\overline{p} \vee \overline{q}$	$\overline{r} \Rightarrow (\overline{p} \vee \overline{q})$	$[(p \wedge q) \Rightarrow r] \Rightarrow [\overline{r} \Rightarrow (\overline{p} \vee \overline{q})]$
T	T	T								
T	T	F								
T	F	T								
T	F	F								
F	T	T								
F	T	F								
F	F	T								
F	F	F								

(2.5.7)

Question: If there are four propositional variables in a proposition, how many rows are there in the truth table?

Biconditional and Equivalence

Note

Two logical formulas p and q are ***logically equivalent***, denoted $\boldsymbol{p \equiv q}$**,** (defined in section 2.2) if and only if $\boldsymbol{p \Leftrightarrow q}$ **is a tautology.**

We are *not* saying that p is equal to q. Since p and q represent two different statements, they cannot be the same. What we are saying is, they always produce the same truth value, regardless of the truth values of the underlying propositional variables. That is why we write $p \equiv q$ instead of $p = q$.

Example 2.5.4

We have learned that

$$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p), \tag{2.5.8}$$

which is the reason why we call $p \Leftrightarrow q$ a biconditional statement.

Example 2.5.5

Use truth tables to verify the following equivalent statements.

- $p \Rightarrow q \equiv \overline{p} \vee q$. [equiv1]
- $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$. [equiv2]

Answer

The truth tables for (a) and (b) are depicted below.

p	q	$p \Rightarrow q$	$\overline{p}$	$\overline{p} \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

(2.5.9)

(2.5.10)

Example ([equiv1]) is an important result. It says that $p \Rightarrow q$ is true when one of these two things happen: (i) when p is false, (ii) otherwise (when p is true) q must be true.

hands-on exercise 2.5.2

Use truth tables to establish these logical equivalences.

a. $p \Rightarrow q \equiv \overline{q} \Rightarrow \overline{p}$
b. $p \vee p \equiv p$
c. $p \wedge q \equiv \overline{\overline{p} \vee \overline{q}}$
d. $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$

Answer

We have set up the table for (a), and leave the rest to you.

p	q	$p \Rightarrow q$	$\overline{q}$	$\overline{p}$	$\overline{q} \Rightarrow \overline{p}$
T	T				
T	F				
F	T				
F	F				

(2.5.11)

hands-on exercise 2.5.3

The logical connective exclusive or, denoted $p \veebar q$, means either p or q but not both. Consequently,

$$p \veebar q \equiv (p \vee q) \wedge \overline{(p \wedge q)} \equiv (p \wedge \overline{q}) \vee (\overline{p} \wedge q). \tag{2.5.12}$$

Construct a truth table to verify this claim

Properties

Properties of Logical Equivalence. Denote by T and F a tautology and a contradiction, respectively. We have the following properties for any propositional variables p, q, and r.

1. ***Commutative properties***: $p \vee q \equiv q \vee p$,
   $p \wedge q \equiv q \wedge p$.
2. ***Associative properties***: $(p \vee q) \vee r \equiv p \vee (q \vee r)$,
   $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.
3. ***Distributive laws***: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$,
   $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$.
4. ***Idempotent laws***: $p \vee p \equiv p$,
   $p \wedge p \equiv p$.
5. ***De Morgan's laws***: $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$,
   $\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$.
6. ***Laws of the excluded middle***, or ***inverse laws***: $p \vee \overline{p} \equiv T$,
   $p \wedge \overline{p} \equiv F$.
7. ***Identity laws***: $p \vee F \equiv p$,
   $p \wedge T \equiv p$.
8. ***Domination laws***: $p \vee T \equiv T$,
   $p \wedge F \equiv F$.
9. Equivalence of an implication and its contrapositive: $p \Rightarrow q \equiv \overline{q} \Rightarrow \overline{p}$.
10. Writing an implication as a disjunction: $p \Rightarrow q \equiv \overline{p} \vee q$.
11. The negation of an implication: $\overline{p \Rightarrow q} \equiv p \wedge \overline{q}$

Be sure you understand and memorize the last three equivalences, because we will use them frequently in the rest of the course.

It may not be easy to memorize the names of all these properties; however, they should all make sense to you. The important name is De Morgan's laws. Let us explain them in words, and compare them to similar operations on the real numbers,

1. ***Commutative properties***: In short, they say that "the order of operation does not matter." It does not matter which of the two logical statements comes first, the result from conjunction and disjunction always produces the same truth value. Compare this to addition of real numbers: $x + y = y + x$. Subtraction is not commutative, because it is not always true that $x - y = y - x$. This explains why we have to make sure that an operation is commutative.
2. ***Associative properties***: Roughly speaking, these properties also say that "the order of operation does not matter." However, there is a key difference between them and the commutative properties.
   - Commutative properties apply to operations on *two* logical statements, but associative properties involves *three* logical statements. Since $\wedge$ and $\vee$ are *binary* operations, we can only work on a pair of statements at a time. Given the three statements p, q, and r, appearing in that order, which pair of statements should we operate on first? The answer is: it does not matter. It is the order of *grouping* (hence the term associative) that does not matter in associative properties.
   - The important consequence of the associative property is: since it does not matter on which pair of statements we should carry out the operation first, we can eliminate the parentheses and write, for example,
     $$p \vee q \vee r \tag{2.5.13}$$
     without worrying about any confusion.
   - Not all operations are associative. Subtraction is not associative. Given three numbers 5, 7, and 4, in that order, how should we carry out two subtractions? Which interpretation should we use:
     $$(5-7)-4, \qquad \text{or} \qquad 5-(7-4)? \tag{2.5.14}$$

Since they lead to different results, we have to be careful where to place the parentheses.

3. ***Distributive laws***: When we mix two *different* operations on three logical statements, one of them has to work on a pair of statements first, forming an "inner" operation. This is followed by the "outer" operation to complete the compound statement. Distributive laws say that we can distribute the "outer" operation over the inner one.
4. ***Idempotent laws***: When an operation is applied to a pair of identical logical statements, the result is the same logical statement. Compare this to the equation $x^2 = x$, where x is a real number. It is true only when $x = 0$ or $x = 1$. But the logical equivalences $p \vee p \equiv p$ and $p \wedge p \equiv p$ are true for all p.
5. ***De Morgan's laws***: When we negate a disjunction (respectively, a conjunction), we have to negate the two logical statements, and change the operation from disjunction to conjunction (respectively, from conjunction to a disjunction).
6. ***Laws of the excluded middle***, or ***inverse laws***: Any statement is either true or false, hence $p \vee \overline{p}$ is always true. Likewise, a statement cannot be both true and false at the same time, hence $p \wedge \overline{p}$ is always false.
7. ***Identity laws***: Compare them to the equation $x \cdot 1 = x$: the value of x is unchanged after multiplying by 1. We call the number 1 the multiplicative identity. For logical operations, the identity for disjunction is F, and the identity for conjunction is T.
8. ***Domination laws***: Compare them to the equation $x \cdot 0 = 0$ for real numbers: the result is always 0, regardless of the value x. The "zero" for disjunction is T, and the "zero" for conjunction is F.

Example 2.5.6

What is the negation of $2 \leq x \leq 3$? Give a logical explanation as well as a graphical explanation.

Answer

The inequality $2 \leq x \leq 3$ means

$$(x \geq 2) \wedge (x \leq 3). \tag{2.5.15}$$

Its negation, according to De Morgan's laws, is

$$(x < 2) \vee (x > 3). \tag{2.5.16}$$

The inequality $2 \leq x \leq 3$ yields a closed interval. Its negation yields two open intervals. Their graphical representations on the real number line are depicted below.

(130,60)(-20,-45) (-20,0)(1,0)130 (30, 0)(30,0)2 (20,-25)(20,20)2 (50,-25)(20,20)3 (0,-50)(90,20)$(x \geq 2) \wedge (x \leq 3)$ (30, 0)(1,0)30

(130,60)(-20,-45) (-20,0)(1,0)130 (30, 0)(30,0)2 (20,-25)(20,20)2 (50,-25)(20,20)3 (0,-50)(90,20)$(x < 2) \vee (x > 3)$ (-20, 0)(1,0)48 (62, 0)(1,0)48

Take note of the two endpoints 2 and 3. They change from inclusion to exclusion when we take negation.

hands-on exercise 2.5.4

Since $0 \leq x \leq 1$ means "$x \geq 0$ and $x \leq 1$," its negation should be "$x < 0$ or $x > 1$". Explain why it is inappropriate, and indeed incorrect, to write "$0 > x > 1$."

hands-on exercise 2.5.5

Expand $(p \vee q) \wedge (r \vee s)$.

Example 2.5.7

We have used a truth table to verify that

$$[(p \wedge q) \Rightarrow r] \Rightarrow [\overline{r} \Rightarrow (\overline{p} \vee \overline{q})] \tag{2.5.17}$$

is a tautology. We can use the properties of logical equivalence to show that this compound statement is logically equivalent to T. This kind of proof is usually more difficult to follow, so it is a good idea to supply the explanation in each step. Here is a complete proof:

$$\tag{2.5.18}$$

This is precisely what we called the left-to-right method for proving an identity (in this case, a logical equivalence).

Example 2.5.8

Write $\overline{p \Rightarrow q}$ as a conjunction.

Answer

It is important to remember that

$$\overline{p \Rightarrow q} \not\equiv q \Rightarrow p, \tag{2.5.19}$$

and

$$\overline{p \Rightarrow q} \not\equiv \overline{p} \Rightarrow \overline{q} \tag{2.5.20}$$

either. Instead, since $p \Rightarrow q \equiv \overline{p} \vee q$, it follows from De Morgan's law that

$$\overline{p \Rightarrow q} \equiv \overline{\overline{p} \vee q} \equiv p \wedge \overline{q}. \tag{2.5.21}$$

Alternatively, we can argue as follows. Interpret $\overline{p \Rightarrow q}$ as saying $p \Rightarrow q$ is false. This requires p to be true and q to be false, which translates into $p \wedge \overline{q}$. Thus, $\overline{p \Rightarrow q} \equiv p \wedge \overline{q}$.

Summary and Review

- Two logical statements are logically equivalent if they always produce the same truth value.
- Consequently, $p \equiv q$ is same as saying $p \Leftrightarrow q$ is a tautology.
- Beside distributive and De Morgan's laws, remember these two equivalences as well; they are very helpful when dealing with implications.

$$p \Rightarrow q \equiv \overline{q} \Rightarrow \overline{p} \qquad \text{and} \qquad p \Rightarrow q \equiv \overline{p} \vee q. \tag{2.5.22}$$

Exercises 2.5.

Exercise 2.5.1

Use a truth table to verify the De Morgan's law $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$.

Answer

p	q	$p \vee q$	$\overline{p \vee q}$	$\overline{p}$	$\overline{q}$	$\overline{p} \wedge \overline{q}$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Exercise 2.5.2

Use truth tables to verify the two associative properties.

Exercise 2.5.3

Construct a truth table for each formula below. Which ones are tautologies?

a. $(\overline{p} \vee q) \Rightarrow p$
b. $(p \Rightarrow q) \vee (p \Rightarrow \overline{q})$
c. $(p \Rightarrow q) \Rightarrow r$

Answer

Only (b) is a tautology, as indicated in the truth tables below.

(a)

p	q	$\overline{p}$	$\overline{p} \vee q$	$(\overline{p} \vee q) \Rightarrow p$
T	T	F	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	T	F

(b)

p	q	$p \Rightarrow q$	$\overline{q}$	$p \Rightarrow \overline{q}$	$(p \Rightarrow q) \vee (p \Rightarrow \overline{q})$
T	T	T	F	F	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	T	T

(c)

p	q	r	$p \Rightarrow q$	$(p \Rightarrow q) \Rightarrow r$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	T
T	F	F	F	T
F	T	T	T	T
F	T	F	T	F
F	F	T	T	T
F	F	F	T	F

Exercise 2.5.4

Use truth tables to verify these logical equivalences.

a. $(p \wedge q) \Leftrightarrow p \equiv p \Rightarrow q$
b. $(p \wedge q) \Rightarrow r \equiv p \Rightarrow (\overline{q} \vee r)$
c. $(p \Rightarrow \overline{q}) \wedge (p \Rightarrow \overline{r}) \equiv \overline{p \wedge (q \vee r)}$

Exercise 2.5.5

Use only the properties of logical equivalences to verify (b) and (c) in Problem 4.

Answer

The proofs are displayed below without explanations. Be sure to fill them in.

$$\text{(b)}\quad \begin{aligned} (p \wedge q) \Rightarrow r &\equiv \overline{p \wedge q} \vee r \\ &\equiv (\overline{p} \vee \overline{q}) \vee r \\ &\equiv \overline{p} \vee (\overline{q} \vee r) \\ &\equiv p \Rightarrow (\overline{q} \vee r) \end{aligned}$$

(c) $(p \Rightarrow \overline{q}) \wedge (p \Rightarrow \overline{r}) \equiv (\overline{p} \vee \overline{q}) \wedge (\overline{p} \vee \overline{r})$
$\equiv \overline{p} \vee (\overline{q} \wedge \overline{r})$
$\equiv \overline{p} \vee \overline{q \vee r}$
$\equiv \overline{p \wedge (q \vee r)}$

Exercise 2.5.6

Determine whether formulas u and v are logically equivalent (you may use truth tables or properties of logical equivalences).

$u:\ (p \Rightarrow q) \wedge (p \Rightarrow \overline{q})$	$v:\ \overline{p}$
$u:\ p \Rightarrow q$	$v:\ q \Rightarrow p$
$u:\ p \Leftrightarrow q$	$v:\ q \Leftrightarrow p$
$u:\ (p \Rightarrow q) \Rightarrow r$	$v:\ p \Rightarrow (q \Rightarrow r)$

Exercise 2.5.7

Find the converse, inverse, and contrapositive of these implications.

a. If triangle ABC is isosceles and contains an angle of 45 degrees, then ABC is a right triangle.
b. If quadrilateral $ABCD$ is a square, then it is both a rectangle and a rhombus.
c. If quadrilateral $ABCD$ has two sides of equal length, then it is either a rectangle or a rhombus.

Answer

(a)

Converse:	If triangle ABC is a right triangle, then ABC is isosceles and contains an angle of 45 degrees.
Inverse:	If triangle ABC is not isosceles or does not contain an angle of 45 degrees, then ABC is not a right triangle.
Contrapositive:	If triangle ABC is not a right triangle, then ABC is not isosceles or does not contain an angle of 45 degrees.

(b)

Converse:	If quadrilateral $ABCD$ is both a rectangle and a rhombus, then $ABCD$ is a square.
Inverse:	If quadrilateral $ABCD$ is not a square, then it is not a rectangle or not a rhombus.
Contrapositive:	If quadrilateral $ABCD$ is not a rectangle or not a rhombus, then $ABCD$ is not a square.

(c)

Converse:	If quadrilateral $ABCD$ is either a rectangle or a rhombus,

	then $ABCD$ has two sides of equal length.
Inverse:	If quadrilateral $ABCD$ is does not have two sides of equal length,
	then it is not a rectangle and it is not a rhombus.
Contrapositive:	If quadrilateral $ABCD$ is not a rectangle and it is not a rhombus,
	then $ABCD$ is does not have two sides of equal length.

Exercise 2.5.8

Negate the following implications:

a. $x^2 > 0 \Rightarrow x > 0$.
b. If $PQRS$ is a square, then $PQRS$ is a parallelogram.
c. If $n > 1$ is prime, then $n + 1$ is composite.
d. If x and y are integers such that $xy \geq 1$, then either $x \geq 1$ or $y \geq 1$.

Exercise 2.5.9

Determine whether the following formulas are true or false:

a. $\overline{p \Leftrightarrow q} \equiv \overline{p} \Leftrightarrow \overline{q}$
b. $(p \Rightarrow q) \wedge (p \Rightarrow \overline{q}) \equiv \overline{p}$
c. $p \Rightarrow q \equiv q \Rightarrow p$

Answer

(a) false (b) true (c) false

Exercise 2.5.10

Determine whether the following formulas are true or false:

a. $(p \Rightarrow q) \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$
b. $p \Rightarrow (q \vee r) \equiv (p \Rightarrow q) \vee (p \Rightarrow r)$
c. $p \Rightarrow (q \wedge r) \equiv (p \Rightarrow q) \wedge (p \Rightarrow r)$

Exercise 2.5.11

Which of the following statements are equivalent to the statement "if $x^2 > 0$, then $x > 0$"?

a. If $x > 0$, then $x^2 > 0$.
b. If $x \leq 0$, then $x^2 \leq 0$.
c. If $x^2 \leq 0$, then $x \leq 0$.
d. If $x^2 \not> 0$, then $x \not> 0$.

Answer

Only (b).

Exercise 2.5.12

Determine whether the following formulas are tautologies, contradictions, or neither:

a. $(p \Rightarrow q) \wedge \overline{p}$
b. $(p \Rightarrow \overline{q}) \wedge (p \wedge q)$
c. $(p \Rightarrow \overline{q}) \wedge q$

Exercise 2.5.13

Simplify the following formulas:

a. $p \wedge (p \wedge q)$
b. $\overline{\overline{p} \vee q}$
c. $\overline{p \Rightarrow \overline{q}}$

Answer

(a) $p \wedge q$
(b) $p \wedge \overline{q}$
(c) $p \wedge q$

Exercise 2.5.14

Simplify the following formulas:

a. $(p \Rightarrow \overline{q}) \wedge (\overline{q} \Rightarrow p)$
b. $\overline{p \wedge \overline{q}}$
c. $p \wedge (\overline{p} \vee q)$

Exercise 2.5.15

T stands for a tautology & F stands for a contradiction.

True or False?

a. $F \to \overline{q}$

b. $p \vee T$

c. $F \wedge p$

d. $\overline{T} \vee F$

Answer

(a) true (b) true (c) false (d) false

Exercise 2.5.16

T stands for a tautology & F stands for a contradiction.

Simplify to an equivalent expression that is a single letter (T, F, p or ~p)

a. $\overline{T} \vee F \equiv$

b. $T \wedge p \equiv$

c. $F \wedge \overline{p} \equiv$

d. $F \vee \overline{p} \equiv$

e. $(F \vee T) \vee F \equiv$

f. $(F \vee T) \wedge T \equiv$

2.6 Arguments and Rules of Inference

In this section we will look at how to test if an argument is valid. This is a test for the *structure* of the argument. A valid argument does not always mean you have a true conclusion; rather, the conclusion of a valid argument must be true if all the premises are true. We will also look at common valid arguments, known as Rules of Inference as well as common invalid arguments, known as Fallacies.

Arguments

Definition

An **argument** is a set of initial statements, called **premises**, followed by a **conclusion.**

Definition

An argument is **valid** if and only if in every case where all the premises are true, the conclusion is true. Otherwise, the argument is **invalid**.

Here is an example:

If I read my text, I will understand how to do my homework.

I understand how to do my homework.

Therefore, I read my text.

Our first premise: is *If I read my text, then I understand how to do my homework.*

Our second premise is:*I understand how to do my homework.*

Our conclusion is *I read my text.*

Let's use t means *I read my text* and u means *I understand how to do my homework.*

Symbolically, our argument is:

$t \rightarrow u$

u

$\therefore t$

Testing the validity of an argument by truth table.

We represent this argument by working out its premises and conclusion on a truth table:

t	u	$t \rightarrow u$	u	t
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F

t	u	$t \to u$	u	t
F	F	T	F	F

Notice we repeat the column for u and the column for t because one is a premise and one is a conclusion.

Since a valid argument must have a true conclusion in all cases where the premises are true, we need to examine the rows where all premises are true.

Definition

Given a truth table representing an argument, the rows where all the premises are true are called the **critical rows.**

We test an argument by considering all the critical rows. If the conclusion is true in all critical rows, then the argument is valid. This is another way of saying the conclusion of a valid argument must be true in every case where all the premises are true.

Look for rows where all premises are true.

premise 1 premise 2

conclusion

t	u	$t \to u$	u	t
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	F

We see that the 1st and 3rd rows are critical rows. In the 1st row, the conclusion is true. However, in the 3rd row, a critical row, the conclusion is false.

Thus this argument is ________________.

Answer

INVALID

Example 1

Consider this argument.

If Pat goes to the store, Pat will buy $1,000,000 worth of food.

Pat goes to the store.

Therefore, Pat buys $1,000,000 worth of food.

This is a valid argument (you can test it on a truth table).

However, even though Pat goes to the store, Pat does not buy $1,000,000 worth of food. The conclusion is false.

How can the conclusion of a valid argument be false?

Solution

The validity of an argument refers to its structure. Given a valid argument, the conclusion must be true if the premises are true. In this case the first premise is NOT true, and thus the conclusion does not need to be true.

The conclusion of a valid argument can be false if one or more of the premises is false.

Rules of Inference

A number of valid arguments are very common and are given names. Know these four:

Modus Ponens

$p \rightarrow q$

p

$\therefore q$

Modus Tollens

$p \rightarrow q$

$\sim q$

$\therefore \sim p$

Elimination

$p \vee q$

$\sim p$

$\therefore q$

Transitivity

$p \rightarrow q$

$q \rightarrow r$

$\therefore p \rightarrow r$

As you think about the rules of inference above, they should make sense to you. Furthermore, each one can be proved by a truth table.

If you see an argument in the form of a rule of inference, you know it's valid.

Example 2

Explain why this argument is valid:

If I go to the movies, I will not do my homework.

I do my homework.

Therefore, I did not go to the movies.

Solution

This is valid by Modus Tollens.

Fallacies

Fallacies are invalid arguments. Know the names of these two common fallacies.

Converse Error

$p \to q$

q

$\therefore p$

Inverse Error

$p \to q$

~p

$\therefore$ ~q

If you think about the converse and inverse (and that they do not have the same meaning as the original implication) you can see why these fallacies have these names. You can use a truth table to show these fallacies are arguments that are__________________.

Answer

INVALID

Example 3

Explain why this argument is valid or invalid:

If I go to the movies, I will not do my homework.

I did not go to the movies.

Therefore, I did do my homework.

Solution

This is invalid; it is an inverse error.

Exercises

Exercise 1

True or False?

(a) Given a valid argument with true premises, the conclusion must be true.

(b) Given a valid argument with false premises, the conclusion must be false.

(c) Given an invalid argument, the conclusion must be false.

Answer

(a) true (b) false (c) false

Exercise 3

Decide if the following arguments are valid or invalid. State the Rule of Inference of fallacy used.

(a)

If it snows, then school is closed.

School is open.

Therefore it is not snowing.

(b)

My pet is a cat or my pet is a dog.

My pet is not a dog.

Therefore my pet is a cat.

(c)

If the movie is long, I will fall asleep.

I do fall asleep.

Therefore the movie was long.

Answer

(a) VALID, Modus Tollens
(b) VALID, Elimination
(c) INVALID, Converse Error

Exercise 5

Use a truth table to determine if this argument is valid or invalid. Include a clear explanation.

$\overline{p} \vee (q \rightarrow r)$

$\overline{r}$

$\therefore \overline{p \wedge q}$

Answer

As seen below, there are three critical rows, namely the 4th, 6th and 8th rows. We can see that in every case where all the premises are true, the conclusion is also true. Thus, this is a valid argument.

premise 1 premise 2

conclusion

p	q	r	$\overline{p}$	$q \rightarrow r$	$\overline{p} \vee (q \rightarrow r)$	$\overline{r}$	$p \wedge q$	$\overline{p \wedge q}$
T	T	T	F	T	T	F	T	F

p	q	r	$\overline{p}$	$q \to r$	$\overline{p} \vee (q \to r)$	$\overline{r}$	$p \wedge q$	$\overline{p \wedge q}$
T	T	F	F	F	F	T	T	F
F	T	T	T	T	T	F	F	T
F	T	F	T	F	T	T	F	T
T	F	T	F	T	T	F	F	T
T	F	F	F	T	T	T	F	T
F	F	T	T	T	T	F	F	T
F	F	F	T	T	T	T	F	T

Exercise 7

Use a truth table and an explanation to prove Modus Ponens is a valid form of an argument.

Answer

As seen below, the only critical row is the first row. We can see that in the one case that all the premises are true, the conclusion is also true. Thus, Modus Ponens has the form of a valid argument.

premise 1 premise 2

conclusion

p	q	$p \to q$	p	q
T	T	T	T	T
T	F	F	T	T
F	T	T	F	F
F	F	T	F	F

2.7: Quantifiers

Propositional Function

The expression

$$x > 5 \tag{2.7.1}$$

is neither true nor false. In fact, we cannot even determine its truth value unless we know the value of x. This is an example of a ***propositional function***, because it behaves like a function of x, it becomes a proposition when a specific value is assigned to x. Propositional functions are also called ***predicates***.

Example 2.7.1

Denote the propositional function "$x > 5$" by $p(x)$. We often write

$$p(x): \quad x > 5. \tag{2.7.2}$$

It is not a proposition because its truth value is undecidable, but $p(6)$, $p(3)$ and $p(-1)$ are propositions.

Example 2.7.2

Define

$$q(x, y): \quad x + y = 1. \tag{2.7.3}$$

Which of the following are propositions; which are not?

a. $q(x, y)$
b. $q(x, 3)$
c. $q(1, 1)$
d. $q(5, -4)$

For those that are, determine their truth values.

Answer

Both (a) and (b) are not propositions, because they contain at least one variable. Both (c) and (d) are propositions; $q(1, 1)$ is false, and $q(5, -4)$ is true.

hands-on Exercise 2.7.1

Determine the truth values of these statements, where $q(x, y)$ is defined in Example $2.7.2$.

a. $q(5, -7)$
b. $q(-6, 7)$
c. $q(x + 1, -x)$

Although a propositional function is not a proposition, we can form a proposition by means of ***quantification***. The idea is to specify whether the propositional function is true for all or for some values that the underlying variables can take on.

Universal Quantifier

Definition

The ***universal quantification*** of $p(x)$ is the proposition in any of the following forms:

- $p(x)$ is true for all values of x.
- For all x, $p(x)$.
- For each x, $p(x)$.
- For every x, $p(x)$.
- Given any x, $p(x)$.

All of them are symbolically denoted by

$$\forall x\, p(x), \tag{2.7.4}$$

which is pronounced as

"for all x, $p(x)$".

The symbol $\forall$ is called the ***universal quantifier***, and can be extended to several variables.

Example 2.7.3

The statement

"For any real number x, we always have $x^2 \geq 0$"

is true. Symbolically, we can write

$$\forall x \in \mathbb{R}\, (x^2 \geq 0), \qquad \text{or} \qquad \forall x\, (x \in \mathbb{R} \Rightarrow x^2 \geq 0). \tag{2.7.5}$$

The second form is a bit wordy, but could be useful in some situations.

Example 2.7.4

The statement

$$\forall x \in \mathbb{R}\, (x > 5) \tag{2.7.6}$$

is false because x is not always greater than 5. To disprove a claim, it suffices to provide only one counterexample. We can use $x = 4$ as a counterexample.

However, examples cannot be used to prove a universally quantified statement. Consider the statement

$$\forall x \in \mathbb{R}\, (x^2 \geq 0). \tag{2.7.7}$$

By direct calculations, one may demonstrate that $x^2 \geq 0$ is true for many x-values. But it does not *prove* that it is true for *every* x, because there may be a counterexample that we have not found yet. We have to use mathematical and logical argument to prove a statement of the form "$\forall x\, p(x)$."

Example 2.7.5

The statement

"Every Discrete Mathematics student has taken Calculus I and Calculus II"

is clearly a universally quantified proposition. To express it in a logical formula, we can use an implication:

$$\forall x\, (x \text{ is a Discrete Mathematics student} \Rightarrow x \text{ has taken Calculus I and Calculus II}) \tag{2.7.8}$$

An alternative is to say

$$\forall x \in S\, (x \text{ has taken Calculus I and Calculus II}) \tag{2.7.9}$$

where S represents the set of all Discrete Mathematics students. Although the second form looks simpler, we must define what S stands for.

Existential Quantifier

Definition

The ***existential quantification*** of $p(x)$ takes one of these forms:

- There exists an x such that $p(x)$.
- For some x, $p(x)$.
- There is some x such that $p(x)$.

We write, in symbol,

$$\exists x\, p(x), \tag{2.7.10}$$

which is pronounced as

"There exists x such that $p(x)$."

The symbol $\exists$ is called the ***existential quantifier***. It can be extended to several variables.

Notice the pronouciation includes the phrase "such that". Don't forget to say that phrase as part of the verbalization of a symbolic existential statement.

Example 2.7.6

To prove that a statement of the form "$\exists x\, p(x)$" is true, it suffices to find an example of x such that $p(x)$ is true. Using this guideline, can you determine whether these two propositions

a. $\exists x \in \mathbb{R}\, (x > 5)$
b. $\exists x \in \mathbb{R}\, (\sqrt{x} = 0)$

are true?

Answer

a. True. For example: $x = 6$.
b. True. For example: $x = 0$.

Example 2.7.7

The proposition

"There exists a prime number x such that $x + 2$ is also prime"

is true. We call such a pair of primes ***twin primes***.

hands-on Exercise 2.7.2

Name a few more examples of twin primes.

Example 2.7.8

The proposition

"There exists a real number x such that $x > 5$"

can be expressed, symbolically, as

$$\exists x \in \mathbb{R}\, (x > 5), \qquad \text{or} \qquad \exists x\, (x \in \mathbb{R} \wedge x > 5). \tag{2.7.11}$$

Notice that in an existential quantification, we use $\wedge$ instead of $\Rightarrow$ to specify that x is a real number.

hands-on Exercise 2.7.3

Determine the truth value of each of the following propositions:

a. For any prime number x, the number $x + 1$ is composite.
b. For any prime number $x > 2$, the number $x + 1$ is composite.
c. There exists an integer k such that $2k + 1$ is even.
d. For all integers k, the integer $2k$ is even.
e. For any real number x, if x^2 is an integer, then x is also an integer.

hands-on Exercise 2.7.4

The proposition

"The square of any real number is positive"

is a universal quantification

"For any real number x, $x^2 > 0$."

Is it true or false?

Negation with Quantifiers

To negate that a proposition always happens, is to say there exists an instance where it does not happen.

To negate that a proposition exists, is to say the proposition always does not happen.

Symbolically:

$\overline{\forall x P(x)} \equiv \exists x \overline{P(x)}$

and

$\overline{\exists x P(x)} \equiv \forall x \overline{P(x)}$

hands-on Exercise 2.7.5

Negate the propositions in Hands-On Exercise 2.7.3

Example 2.7.9

The statement

"All real numbers x satisfy $x^2 \geq 0$"

can be written as, symbolically, $\forall x \in \mathbb{R}\,(x^2 \geq 0)$. Its negation is $\exists x \in \mathbb{R}\,(x^2 < 0)$. In words, it says "There exists a real number x that satisfies $x^2 < 0$."

hands-on Exercise 2.7.6

Negate the statement

"Every Discrete Mathematics student has taken Calculus I and Calculus II."

Summary and Review

- There are two ways to quantify a propositional function: universal quantification and existential quantification.
- They are written in the form of "$\forall x\, p(x)$" and "$\exists x\, p(x)$" respectively.
- To negate a quantified statement, change $\forall$ to $\exists$, and $\exists$ to $\forall$, and then negate the statement.

Exercises 2.7.

Exercise 2.7.1

Consider these propositional functions:

$p(n)$:	n is prime
$q(n)$:	n is even
$r(n)$:	$n > 2$

Express these formulas in words:

a. $\exists n \in \mathbb{Z}\,(p(n) \wedge q(n))$
b. $\forall n \in \mathbb{Z}\,[r(n) \Rightarrow p(n) \vee q(n)]$

c. $\exists n \in \mathbb{Z}\,[p(n) \wedge (q(n) \vee r(n))]$
d. $\forall n \in \mathbb{Z}\,[(p(n) \wedge q(n)) \Rightarrow \overline{r(n)}]$

Answer

(a) There exists an integer n such that n is prime and n is even.

(b) For all integers n, if $n > 2$, then n is prime or n is even.

(c) There exists an integer n such that n is prime, and either n is even or $n > 2$.

(d) For all integers n, if n is prime and n is even, then $n \leq 2$.

Exercise 2.7.2

Write each of the following statements in symbolic form:

a. For every even integer n there exists an integer k such that $n = 2k$.
b. There exists a right triangle T that is an isosceles triangle.
c. Given any quadrilateral Q, if Q is a parallelogram and Q has two adjacent sides that are perpendicular, then Q is a rectangle.

Exercise 2.7.3

Determine whether these statements are true or false:

a. There exists an even prime integer.
b. There exist integers s and t such that $1 < s < t < 187$ and $st = 187$.
c. Given any real numbers x and y, $x^2 - 2xy + y^2 > 0$.

Answer

(a) true (b) true (c) false

Exercise 2.7.4

Determine whether these statements are true or false:

a. There is a rational number x such that $x^2 \leq 0$.
b. For all $x \in \mathbb{Z}$, either x is even, or x is odd.
c. There exists a unique number x such that $x^2 = 1$.

Exercise 2.7.5

Negate this universal conditional statement (think about how a conditional statement is negated).

For all cats, if a cat eats 3 meals a day, then that cat weighs at least 10 lbs.

Answer

There exists a cat that eats 3 meals a day and weighs less than 10 lbs.

Exercise 2.7.6

Negate this universal conditional statement.

$\forall x \in \mathbb{R}(x < 0 \rightarrow x + 1 < 0)$.

Answer

$\exists x \in \mathbb{R}(x < 0 \wedge x + 1 \geq 0)$.

Exercise 2.7.7

original: *No student wants a final exam on Saturday.*

a. Write the original statement symbolically.

b. Negate the original statement symbolically.

C. Negate the original statement informally (in English).

Answer

a. $\forall\ students\ x\ (x \text{ does not want a final exam on Saturday})$.
b. $\exists\ a\ student\ x\ (x \text{ does want a final exam on Saturday})$.
c. Some student does want a final exam on Saturday.

Exercise 2.7.8

For this statement, (i) represent it in symbolic form, (ii) find the symbolic negation (in simplest form), and (iii) express the negation in words.

There exist rational numbers x_1 and x_2 such that $x_1 < x_2$ and $x_1^3 - x_1 > x_2^3 - x_2$.

Exercise 2.7.9

The easiest way to negate the proposition

"A square must be a parallelogram"

is to say

"It is not true that a square must be a parallelogram."

Yet, it is not the same as saying

"A square must not be a parallelogram."

Can you explain why? What are other ways to express its negation in words?

Answer

The statement "a square must be a parallelogram" means, symbolically,

$$\forall PQRS\,(PQRS \text{ is a square} \Rightarrow PQRS \text{ is a parallelogram}), \tag{2.7.12}$$

but the statement "a square must not be a parallelogram" means

$$\forall PQRS\,(PQRS \text{ is a square} \Rightarrow PQRS \text{ is not a parallelogram}). \tag{2.7.13}$$

The second statement is not the negation of the first. The correct negation, in symbol, is

$$\exists PQRS\,(PQRS \text{ is a square} \wedge PQRS \text{ is a parallelogram}). \tag{2.7.14}$$

In words, it means "there exists a square that is not a parallelogram."

Exercise 2.7.10

Negate these statements:

a. All squared numbers are positive.
b. All basketball players are over 6 feet tall.
c. No quarterback is under 6 feet tall.

2.8: Multiple Quantifiers

Multiple Quantifiers

Multiple quantifiers can be used. With more than one quantifier, the order makes a difference.

Example 2.8.1

When multiple quantifiers are present, the order in which they appear is important. Determine whether these two statements are true or false.

$\forall x \in \mathbb{Z}\ \exists y \in \mathbb{R}^*\ (xy < 1)$

$\exists y \in \mathbb{R}^*\ \forall x \in \mathbb{Z}\ (xy < 1)$

Here, $\mathbb{R}^*$ denotes the set of all nonzero real numbers.

Answer

a. To prove that the statement is true, we need to show that no matter what integer x we start with, we can always find a nonzero real number y such that $xy < 1$. For $x \leq 0$, we can pick $y = 1$, which makes $xy = x \leq 0 < 1$. For $x > 0$, let $y = \frac{1}{x+1}$, then $xy = \frac{x}{x+1} < 1$. This concludes the proof that the first statement is true.
b. Let $y = 1$. Can we find an integer x such that $xy \geq 1$? Definitely! For example, we can set $x = 2$. This counterexample shows that the second statement is false. *NOTE: the statement is false, but this is not a valid explanation. Do you see why? What do you need to show an existence statement is false?*

hands-on Exercise 2.8.1

True or false: $\exists y \in \mathbb{R}\ \forall x \in \mathbb{Z}\ (xy < 1)$?

Example 2.8.2

Many theorems in mathematics can be expressed as quantified statements. Consider

“If x is rational and y is irrational, then $x + y$ is irrational.”

This is same as saying

“Whenever x is rational and y is irrational, then $x + y$ is irrational.”

The keyword “whenever” suggests that we should use a universal quantifier.

$$\forall x, y\ (x \text{ is rational} \wedge y \text{ is irrational} \Rightarrow x + y \text{ is irrational}). \tag{2.8.1}$$

It can also be written as

$$\forall x \in \mathbb{Q}\ \forall y \notin \mathbb{Q}\ (x + y \text{ is irrational}). \tag{2.8.2}$$

Although this form looks complicated and seems difficult to understand (primarily because it is quite symbolic, hence appears to be abstract and incomprehensible to many students), it provides an easy form for negation. See the discussion below.

The fact that an implication can be expressed as a universally quantified statement sounds familiar.

Negation with Multiple Quantifiers

We shall learn several basic proof techniques in Chapter 3. Some of them require negating a logical statement. Since many mathematical results are stated as quantified statements, it is necessary for us to learn how to negate a quantification. The rule is rather simple. Interchange $\forall$ and $\exists$, and negate the statement that is being quantified. In other words,

$$\overline{\forall x\, p(x)} \equiv \exists x\, \overline{p(x)}, \qquad \text{and} \qquad \overline{\exists x\, p(x)} \equiv \forall x\, \overline{p(x)}. \tag{2.8.3}$$

If we have $\forall x \in \mathbb{Z}$, we only change it to $\exists x \in \mathbb{Z}$ when we take negation. It should *not* be negated as $\exists x \notin \mathbb{Z}$. The reason is: we are only negating the quantification, not the membership of x. In symbols, we write

$$\overline{\forall x \in \mathbb{Z}\, p(x)} \equiv \exists x \in \mathbb{Z}\, \overline{p(x)}. \tag{2.8.4}$$

The negation of "$\exists x \in \mathbb{Z}\, p(x)$" is obtained in a similar manner.

Example 2.8.11

We find

$$\overline{\forall x \in \mathbb{Z}\ \exists y \in \mathbb{R}^*\ (xy < 1)} \equiv \exists x \in \mathbb{Z}\ \forall y \in \mathbb{R}^*\ (xy \geq 1), \tag{2.8.5}$$

and

$$\overline{\exists y \in \mathbb{R}^*\ \forall x \in \mathbb{Z}\, (xy < 1)} \equiv \forall y \in \mathbb{R}^*\ \exists x \in \mathbb{Z}\, (xy \geq 1). \tag{2.8.6}$$

Remember that we do not change the membership of x and y.

Example 2.8.12

The statement

"All real numbers x satisfy $x^2 \geq 0$"

can be written as, symbolically, $\forall x \in \mathbb{R}\ (x^2 \geq 0)$. Its negation is $\exists x \in \mathbb{R}\ (x^2 < 0)$. In words, it says "There exists a real number x that satisfies $x^2 < 0$."

Summary and Review

- Symbolically, here's how to negate statements with quantifiers: $\overline{\forall x\, p(x)} \equiv \exists x\, \overline{p(x)}$, and $\overline{\exists x\, p(x)} \equiv \forall x\, \overline{p(x)}$.
- In general, "$\forall x\, \exists y\, p(x,y)$" is NOT the same as "$\exists y\, \forall x\, p(x,y)$", so order makes a difference.

Exercises 2.8.

Exercise 2.8.1

Determine whether these statements are true or false:

a. There is an integer m such that both $m/2$ is an integer and, for every integer k, $m/(2k)$ is not an integer.
b. For every integer n, there exists an integer m such that $m > n^2$.
c. There exists a real number x such that for every real number y, $xy = 0$.

Answer

(a) false (b) true (c) true

Exercise 2.8.2

Negate the following statements:

a. For all real numbers x, there exists an integer y such that $p(x,y)$ implies $q(x,y)$.
b. There exists a rational number x such that for all integers y, either $p(x,y)$ or $r(x,y)$ is true.
c. For all integers x, there exists an integer y such that if $p(x,y)$ is true, then there exists an integer z so that $q(x,y,z)$ is true.

Exercise 2.8.3

Find the negation (in simplest form) of each symbolic statement.

a. $\forall x < 0 \wedge x \in \mathbb{R}\ \forall y, z \in \mathbb{R}\ (y < z \Rightarrow xy > xz)$
b. $\forall x \in \mathbb{Z}\ [p(x) \vee q(x)]$

c. $\forall x, y \in \mathbb{R}\,[p(x,y) \Rightarrow q(x,y)]$

Answer

(a) $\exists x < 0 \wedge x \in \mathbb{R}\; \exists y, z \in \mathbb{R}\;(y < z \wedge xy \leq xz)$

(b) $\exists x \in \mathbb{Z}\;[\overline{p(x)} \wedge \overline{q(x)}]$

(c) $\exists x, y \in \mathbb{R}\;[p(x,y) \wedge \overline{q(x,y)}]$

Exercise 2.8.4

For this statement, (i) represent it in symbolic form, (ii) find the symbolic negation (in simplest form), and (iii) express the negation in words.

For all real numbers x and y there exists an integer z such that $2z = x + y$.

Exercise 2.8.5

For each statement, (i) represent it in symbolic form, (ii) find the symbolic negation (in simplest form), and (iii) express the negation in words.

a. For all real numbers x and y, $x + y = y + x$.
b. For every positive real number x there exists a real number y such that $y^2 = x$.
c. There exists a real number y such that, for every integer x, $2x^2 + 1 > x^2 y$.

Answer

(a)

$\forall x, y \in \mathbb{R}\,(x + y = y + x)$
$\exists x, y \in \mathbb{R}\,(x + y \neq y + x)$
There exist real numbers x and y such that $x + y \neq y + x$.

(b)

$\forall x \in \mathbb{R}^+\; \exists y \in \mathbb{R}\,(y^2 = x)$
$\exists x \in \mathbb{R}^+\; \forall y \in \mathbb{R}\,(y^2 \neq x)$
There exists a positive real number x such that for all real numbers y, $y^2 \neq x$.

(c)

$\exists y \in \mathbb{R}\, \forall x \in \mathbb{Z}\,(2x^2 + 1 > x^2 y)$
$\forall y \in \mathbb{R}\, \exists x \in \mathbb{Z}\,(2x^2 + 1 \leq x^2 y)$
For every real number y, there exists an integer x such that $2x^2 + 1 \leq x^2 y$.

1. Some students may not be familiar with matrices. A matrix is rectangular array of numbers. Matrices are important tools in mathematics. The product of two matrices of appropriate sizes is defined in a rather unusual way. It is the peculiar way that two matrices are multiplied that makes matrices so useful in mathematics. The square of a matrix is of course the product of the matrix with itself. It is well-defined only when the matrix is a square matrix. As it turns out, the order of multiplication of two matrices is important. In other words, given any two matrices A and B, it is not always true that $AB = BA$.↩

CHAPTER OVERVIEW

3: Proof Techniques

3.1: An Introduction to Proof Techniques

Initial Suggestions

A proof is a logical argument that verifies the validity of a statement. A good proof must be correct, but it also needs to be clear enough for others to understand. In the following sections, we want to show you how to write mathematical arguments. It takes practice to learn how to write mathematical proofs; you have to keep trying! We would like to start with some suggestions.

1. **Write at the level of your peers**. A common question asked by many students is: how much detail should I include in a proof? One simple guideline is to write at the level that your peers can understand. Although you can skip the detailed computation, be sure to include the major steps in an argument.
2. **Use symbols and notations appropriately**. Do not use mathematical symbols as abbreviations. For example, do not write "x is a number >4." Use "x is a number greater than 4" instead. Do not use symbols excessively either. It is often clearer if we express our idea in words. Finally, do not start a sentence with a symbol, as in "Suppose $xy>0$. x and y have the same signs." It would look better if we combine the two sentences, and write "Suppose $xy>0$, then x and y have the same signs."
3. **Display long and important equations separately**. Make the key mathematical results stand out by displaying them separately on their own. Be sure to center these expressions. Number them if you need to refer to them later. See Examples 3.3.1 and 3.1.2.
4. **Write in complete sentences, with proper usage of grammar and punctuation**. A proof is, after all, a piece of writing. It should conform to the usual writing rules. Use complete sentences, and do not forget to check the grammar and punctuation.
5. **Anticipate any questions your reader might have** and answer them as part of your proof.
6. **Start with a draft**. Prepare a draft. When you feel it is correct, start revising it: check the accuracy, remove redundancy, and simplify the sentence structure. Organize the argument into short paragraphs to enhance the readability of a proof. Go over the proof and refine it further.

Definitions and Properties

Here is information, some of which was introduced in section 1.5, that will be important for proof writing.

Closure

We will assume the set of integers is **closed under addition, subtraction and multiplication.**

(Closure of a set under an operation was defined in section 1.5.)

Note: closure of other sets under any operations cannot be assumed. So, for example the statement *"the set of rational numbers is closed under multiplication"* cannot be used as a reason, unless you prove this within your proof.

Definition: Rational numbers

Here is the definition of **rational numbers.**

A **rational number** is a real number which can be written as a fraction, $\frac{a}{b}$ where a, b are integers and $b \neq 0$.

In symbols:

$n \in \mathbb{Q} \Leftrightarrow \exists a, b \in \mathbb{Z}(n=\frac{a}{b} \wedge b \neq 0)$

Definition: Even & Odd

Here is the definition of **even and odd numbers.**

Given n is an integer,

n is **even** $\leftrightarrow \exists k \in \mathbb{Z}(n=2k)$

n is **odd** $\leftrightarrow \exists m \in \mathbb{Z}(n = 2m+1)$

Terminology: The condition of being even or odd is the **parity** of an integer.

Here's a property about the parity of integers which we will prove later in this chapter.

Parity Property

Every integer is either even or odd and not both.

Zero Product Property

$\forall a, b \in \mathbb{R}, \qquad ab = 0 \rightarrow a = 0 \vee b = 0$

You have used the Zero Product Property for solving quadratic equations by factoring.

$$(x-6)(x+4) = 0 \tag{3.1.1}$$

Since these two binomials mulitply to zero, one must be zero.

$$x-6 = 0 \vee x+4 = 0 \tag{3.1.2}$$

In proofs, you may need the contrapositive of the Zero Product Property:

$a \neq 0 \wedge b \neq 0 \rightarrow ab \neq 0$.

You may refer to this as the Zero Product Property as well.

Examples

Example 3.1.1

Show that the product of two odd integers is odd.

Proof

Let x and y be any two odd integers. We want to prove that xy is odd. We can say $x = 2s+1$ and $y = 2t+1$ for some integers s and t by definition of odd. By substitution,

$$xy = (2s+1)(2t+1). \tag{3.1.3}$$

By algebra,

$$xy = 4st + 2s + 2t + 1 = 2(2st + s + t) + 1, \tag{3.1.4}$$

where $2st + s + t$ is an integer since the integers are closed under addition and multiplication. Therefore, xy is odd by definition of odd. Thus the product of two odd integers is odd. QED.

Question 1

Why didn't we use $2s+1$ for both x and y ??

Question 2

Why did we need to show $2st + s + t$ is an integer ??

In this proof, we need to use two different quantities s and t to describe x and y because they need not be the same. If we write $x = 2s+1$ and $y = 2s+1$, we are in effect saying that $x = y$. We have to stress that s and t are integers, because just saying $x = 2s+1$ and $y = 2t+1$ does not guarantee x and y are odd. For instance, the even number 4 can be written as $2 \cdot \frac{3}{2} + 1$, which is of the form $2s+1$. It is obvious that 4 is not odd. Even though we can write a number in the form $2s+1$, it does not necessarily mean the number must be odd, *unless* we know with certainty that s is an integer. This example illustrates the importance of paying attention to the details in our writing.

.

hands-on exercise 3.1.1

Let n be an integer. Show that if n is odd, then n^3 is odd.

Some proofs basically require direct computation.

Example 3.1.2

Let a and b be two rational numbers such that $a < b$. Show that the weighted average $\frac{1}{3}a + \frac{2}{3}b$ is a rational number between a and b.

Proof

Since a and b are rational numbers, we can write $a = \frac{m}{n}$ and $b = \frac{p}{q}$ for some integers m, n, p, and q, where $n, q \neq 0$ by definition of rational numbers. Then using algebra

$$\frac{1}{3}a + \frac{2}{3}b = \frac{1}{3} \cdot \frac{m}{n} + \frac{2}{3} \cdot \frac{p}{q} = \frac{mq+2np}{3nq}. \tag{3.1.5}$$

$\frac{mq+2np}{3nq}$ is a rational number since $mq+2np$ and $3np$ are integers because the integers are closed under addition and multiplication, and $3nq \neq 0$ by the Zero Product Property since $3 \neq 0 \wedge n \neq 0 \wedge q \neq 0$. Since $a < b$, we know $b > a$. Using algebra, it follows that

$$b - a > 0 \tag{3.1.6}$$

$$\frac{2}{3}(b-a) > 0, \tag{3.1.7}$$

$$\frac{2}{3}b - \frac{2}{3}a > 0, \tag{3.1.8}$$

$$\frac{2}{3}b + \frac{1}{3}a - a > 0, \tag{3.1.9}$$

$$\left(\frac{1}{3}a + \frac{2}{3}b\right) - a > 0 \tag{3.1.10}$$

$$\frac{1}{3}a + \frac{2}{3}b > a \tag{3.1.11}$$

. In a similar fashion, we also find $\frac{1}{3}a + \frac{2}{3}b < b$. Thus, $\frac{1}{3}a + \frac{2}{3}b$ is a rational number between a and b.

hands-on Exercise 3.1.2

Show that $\frac{1}{3}a+\frac{2}{3}b$ is closer to b than to a.

Hint

Compute the distance between a and $\frac{1}{3}a+\frac{2}{3}b$, and compare it to the distance between $\frac{1}{3}a+\frac{2}{3}b$ and b.

Example 3.1.3

Let m and n be positive integers. Show that, if mn is even, then an $m\times n$ chessboard can be fully covered by non-overlapping dominoes.

Remark

This time, the names m and n have already been assigned to the two positive integers. Thus, we can refer to them in the proof without an introduction.

Solution

Since mn is even, one of the two integers m and n must be even (this actually needs a proof, but we will assume it to be true for now). Without loss of generality (since the other case is similar), we may assume m, the number of rows, is even. Then $m=2t$ for some integer t by definition of even. Each column can be filled with $m/2=t$ non-overlapping dominoes placed vertically. As a result, the entire chessboard can be covered with nt non-overlapping vertical dominoes.

Exercises

Exercise 3.1.1

Show that, between any two rational numbers a and b, where $a<b$, there exists another rational number.

Hint

Try the midpoint of the interval $[a,b]$.

Proof

Since a and b are rational numbers, we can write $a=\frac{p}{q}$ and $b=\frac{j}{k}$ for some integers p, q, j, and k, where $q\neq 0$ and $k\neq 0$ by definition of rational numbers; also $\frac{p}{q}<\frac{j}{k}$. Then choose $m=\frac{1}{2}(a+b)=\frac{1}{2}\left(\frac{p}{q}+\frac{j}{k}\right)=\frac{kp+jq}{2kq}$.
First we show m is a rational number: $kp+jq$ and $2kq$ are integers because the integers are closed under addition and multiplication, and $2kq\neq 0$ by the Zero Product Property since $2\neq 0\wedge k\neq 0\wedge q\neq 0$.

Next, we must show $a<m$ and $m<b$.
Since $\frac{p}{q}<\frac{j}{k}$,

$$\frac{1}{2}\left(\frac{p}{q}+\frac{j}{k}\right)<\frac{1}{2}\left(\frac{j}{k}+\frac{j}{k}\right)=\frac{j}{k}=b. \tag{3.1.12}$$

In other words,

$$m<b. \tag{3.1.13}$$

Since $\frac{p}{q}<\frac{j}{k}$,

$$a=\frac{1}{2}\left(\frac{p}{q}+\frac{p}{q}\right)<\frac{1}{2}\left(\frac{p}{q}+\frac{j}{k}\right)=m. \tag{3.1.14}$$

In other words,

$$a<m. \tag{3.1.15}$$

Thus, $\frac{1}{2}(a+b)$ is a rational number between a and b.

Question

Why did we NOT just say "$\frac{1}{2}(a+b)$ is a rational number since the rational numbers are closed under addition and multiplication"??

Exercise 3.1.2

Prove the rational numbers are closed under addition.

Exercise 3.1.3

Show that, between any two rational numbers a and b, where $a < b$, there exists another rational number closer to b than to a.

Hint

Use a weighted average of a and b.

Answer

Answer is not here yet.

Exercise 3.1.4

Prove: *the sum of two odd integers is a even*.

Exercise 3.1.5

Show that there is a rational number between 1 and 5 whose distance from 5 is seven times as long as its distance from 1.

Exercise 3.1.6

Prove *the square of an even integer is even*.

Exercise 3.1.7

State the parity of each of these numbers & explain:

(a) -11 (b) 0.8 (c) 502

Solution

(a) -11 is odd because -11 = 2(-6)+1 and -6 is an integer
(b) 0.8 has no parity since it is not an integer
(c) 502 is even because 502 = 2(251) and 251 is an integer

Exercise 3.1.8

Show that given any rational number x, there exists an integer y such that x^2y is an integer.

Hint

Since x is rational, we can write $x = \frac{m}{n}$ for some integers m and n, where $n \neq 0$. All you need to do is to describe y in terms of m and n.

Exercise 3.1.9

The natural numbers are closed under subtraction. True or False? Prove your answer.

Answer

False, the natural numbers are not closed under subtraction. Here is a counterexample. Consider 5 and 8. 5 and 8 are natural numbers. However, 5 - 8 is not a natural number, hence the natural numbers are not closed under subtraction.

Exercise 3.1.10

Show that given any rational number x, and any positive integer k, there exists an integer y such that $x^k y$ is an integer.

3.2: Direct Proofs

Preview Activity 1 (Definition of Divides, Divisor, Multiple, is Divisible by)
In Section 3.1, we studied the concepts of even integers and odd integers. The definition of an even integer was a formalization of our concept of an even integer as being one this is "divisible by 2," or a "multiple of 2." We could also say that if "2 divides an integer," then that integer is an even integer. We will now extend this idea to integers other than 2. Following is a formal definition of what it means to say that a nonzero integer m divides an integer n.

Definition of Divides

A nonzero integer m **divides** an integer n provided that there is an integer q such that $n = m \cdot q$. We also say that m is a **divisor** of n, m is a **factor** of n, n **is divisible by** m, and n is a **multiple** of m. The integer 0 is not a divisor of any integer. If a and b are integers and $a \neq 0$, we frequently use the notation $a|b$ as a shorthand for "a divides b."

A Note about Notation: Be careful with the notation $a|b$. This does not represent the rational number $\dfrac{a}{b}$. The notation $a|b$ represents a relationship between the integers a and b and is simply a shorthand for "a divides b." "Divides" as in $a|b$ is a relation (true or false), while "divided by" as in $\dfrac{a}{b}$ or a/b is an operation (results in a number) .

The definition for "divides" can be written in symbolic form using appropriate quantifiers as follows: A nonzero integer m **divides** an integer n provided that $(\exists q \in \mathbb{Z})(n = m \cdot q)$.

Restated, let a and b be two integers such that $a \neq 0$, then the following statements are equivalent:

- a ***divides*** b,
- a is a ***divisor*** of b,
- a is a ***factor*** of b,
- b is a ***multiple*** of a, and
- b is ***divisible by*** a.

They all mean

Given the initial conditions, there exists an integer q such that $b = aq$.

In terms of division, we say that a divides b if and only if the remainder is zero when b is divided by a. We adopt the notation

$$a \mid b \qquad [\text{spoken as ''} a \text{ divides } b\text{''}] \tag{3.2.1}$$

Do not use a forward slash $/$ or a backward slash $\backslash$ in the notation. To say that a does not divide b, we add a slash across the vertical bar, as in

$$a \nmid b \qquad [\text{spoken as ''} a \text{ does not divide } b\text{''}] \tag{3.2.2}$$

The definition of divisibility is very important. Many students fail to finish very simple proofs because they cannot recall the definition. So here we go again:

$$a \mid b \;\Leftrightarrow\; b = aq \;\text{ for some integer } q.$$

Both integers a and b can be positive or negative, and b could even be 0. The only restriction is $a \neq 0$. In addition, q must be an integer. For instance, $3 = 2 \cdot \frac{3}{2}$, but it is certainly absurd to say that 2 divides 3.

Example 3.2.1

Since $14 = (-2) \cdot (-7)$, it is clear that $-2 \mid 14$.

hands-on exercise 3.2.1

1. Use the definition of divides to explain why 4 divides 32 and to explain why 8 divides -96.
2. Give several examples of two integers where the first integer does not divide the second integer.
3. According to the definition of “divides,” does the integer 10 divide the integer 0? That is, is 10 a divisor of 0? Explain.
4. Use the definition of “divides” to complete the following sentence in symbolic form: “The nonzero integer m does not divide the integer n means that ....”
5. Use the definition of “divides” to complete the following sentence without using the symbols for quantifiers: “The nonzero integer m does not divide the integer n. ....”
6. Give three different examples of three integers where the first integer divides the second integer and the second integer divides the third integer.

hands-on exercise 3.2.2

Verify that

$$5 \mid 35, \quad 8 \nmid 35, \quad 25 \nmid 35, \quad 7 \mid 14, \quad 2 \mid -14, \quad \text{and} \quad 14 \mid 14, \tag{3.2.3}$$

by finding the quotient q and the remainder r such that $b = aq + r$, and $r = 0$ if $a \mid b$.

Definition of Prime & Composite

An integer $p > 1$ is a ***prime*** if $\forall a, b \in \mathbb{Z}$, if $ab = p$ then either $a = p \wedge b = 1$ or $a = 1 \wedge b = p$

An integer $n > 1$ is a ***composite*** if $\exists a, b \in \mathbb{Z}\,(ab = n)$ with $1 < a < n \wedge 1 < b < n$.

Notes:

- The integer 1 is neither prime nor composite.
- A positive integer n is composite if it has a divisor d that satisfies $1 < d < n$.

With our definition of "divisor" we can use a simpler definition for *prime,* as follows.

Definition

An integer $p > 1$ is a ***prime*** if its positive divisors are 1 and p itself. Any integer greater than 1 that is not a prime is called ***composite***.

Example 3.2.2

The integers $2, 3, 5, 7, 11, 13, 17, 19, 23, ..$ are primes.

hands-on exercise 3.2.3

What are the next five primes after 23?

Sometimes, we can use a constructive proof when a proposition claims that certain values or quantities exist.

Example 3.2.3

Given any positive integer n, show that there exist n consecutive composite positive integers.

Solution

For each positive integer n, we claim that the n integers

$$(n+1)!+2, \quad (n+1)!+3, \quad \ldots \quad (n+1)!+n, \quad (n+1)!+(n+1) \tag{3.2.4}$$

are composite. Here is the reason. For each i, where $2 \le i \le n+1$, the integer

$$\begin{aligned}(n+1)!+i &= 1\cdot 2\cdot 3\cdots(i-1)i(i+1)\cdots(n+1)+i \\ &= i\,[\,1\cdot 2\cdot 3\cdots(i-1)(i+1)\cdots(n+1)+1\,]\end{aligned}$$

is divisible by i and greater than i, and hence is composite.

hands-on Exercise 3.2.4

Construct five consecutive positive integers that are composite. Verify their compositeness by means of factorization.

Theorem 3.2.1 Consecutive Integers have opposite parity

This is a theorem you can refer to in later work. The proof of this theorem illustrates a technique called "Proof by Cases".

Proof

Let n be any integer. $n+1$ is the next consecutive integer, by the meaning of consecutive.

We will consider two cases.

Case 1: n is even.

Since n is even, there exists an integer k such that $n=2k$ by the definition of even.

$n+1=2k+1$ by substitution. Thus $n+1$ is odd by definition of odd. We have n is even and $n+1$ is odd, so in this case, these consecutive integers have opposite parity.

Case 2: n is odd.

Since n is odd, there exists an integer j such that $n=2j+1$ by the definition of odd.

$n+1=2j+1+1$ by substitution. By algebra, $n+1=2j+2=2(j+1)$. Since $\mathbb{Z}$ is closed under addition, $j+1$ is an integer. Thus $n+1$ is even by definition of even. We have n is odd and $n+1$ is even, so in this case, these consecutive integers have opposite parity.

We know by the Parity Property that n is either even or odd, so we have covered all cases.

$\therefore$ Consecutive integers have opposite parity.

Proof by Cases

When writing a proof by cases be careful to

- clearly define what each case is
- prove each case thoroughly
- include a justification that all cases have been covered (this might be at the start or the end of the set of cases)
- see more examples of proof by cases in the next section

hands-on exercise 3.2.5

Show that n^3+n is even for all $n \in \mathbb{N}$.

Theorem 3.2.2 The Fundamental Theorem of Arithmetic or Prime Factorization Theorem

1. Each natural number greater than 1 is either a prime number or is a product of prime numbers.
2. let $n \in \mathbb{N}$ with $n > 1$. Assume that

$$n = p_1p_2\cdots p_r \text{ and that } n = q_1q_2\cdots q_s, \tag{3.2.5}$$

where $p_1p_2\cdots p_r$ and $q_1q_2\cdots q_s$ are prime with $p_1 \le p_2 \le \cdots \le p_r$ and $q_1 \le q_2 \le \cdots \le q_s$. Then $r = s$, and for each j from 1 to r, $p_j = qj$.

Proof

The proof uses mathematical induction. This is a proof technique we will be covering soon.

Definition

Let a and b be integers, not both 0. A **common divisor** of a and b is any nonzero integer that divides both a and b. The largest natural number that divides both a and b is called the **greatest common divisor** of a and b. The greatest common divisor of a and b is denoted by gcd(a, b).

Some Mathematical Terminology

In Section 1.2, we introduced the idea of a direct proof. Since then, we have used some common terminology in mathematics without much explanation. Before we proceed further, we will discuss some frequently used mathematical terms.

A **proof** in mathematics is a convincing argument that some mathematical statement is true. A proof should contain enough mathematical detail to be convincing to the person(s) to whom the proof is addressed. In essence, a proof is an argument that communicates a mathematical truth to another person (who has the appropriate mathematical background). A proof must use correct, logical reasoning and be based on previously established results. These previous results can be axioms, definitions, or previously proven theorems. These terms are discussed below.

Surprising to some is the fact that in mathematics, there are always **undefined terms**. This is because if we tried to define everything, we would end up going in circles. Simply put, we must start somewhere. For example, in Euclidean geometry, the terms “point,” “line,” and “contains” are undefined terms. In this text, we are using our number systems such as the natural numbers and integers as undefined terms. We often assume that these undefined objects satisfy certain properties. These assumed relationships are accepted as true without proof and are called axioms (or postulates). An **axiom** is a mathematical statement that is accepted without proof. Euclidean geometry starts with undefined terms and a set of postulates and axioms. For example, the following statement is an axiom of Euclidean geometry:

Given any two distinct points, there is exactly one line that contains these two points.

The closure properties of the set of integers discussed in Section 3.1 are being used as axioms in this text.

A **definition** is simply an agreement as to the meaning of a particular term. For example, in this text, we have defined the terms “even integer” and “odd integer.” Definitions are not made at random, but rather, a definition is usually made because a certain property is observed to occur frequently. As a result, it becomes convenient to give this property its own special name. Definitions that have been made can be used in developing mathematical proofs. In fact, most proofs require the use of some definitions.

In dealing with mathematical statements, we frequently use the terms “conjecture,” “theorem,” “proposition,” “lemma,” and “corollary.” A **conjecture** is a statement that we believe is plausible. That is, we think it is true, but we have not yet developed a proof that it is true. A **theorem** is a mathematical statement for which we have a proof. A term that is often considered to be synonymous with “theorem” is proposition.

Often the proof of a theorem can be quite long. In this case, it is often easier to communicate the proof in smaller “pieces.” These supporting pieces are often called lemmas. A **lemma** is a true mathematical statement that was proven mainly to help in the proof of some theorem. Once a given theorem has been proven, it is often the case that other propositions follow immediately from the fact that the theorem is true. These are called corollaries of the theorem. The term **corollary** is used to refer to a theorem that is easily proven once some other theorem has been proven.

Example 3.2.4

Suppose we have proved the "Even Product Theorem": *The product of any two even integers is an even integer.*

Do you see how the related statement could be called a Corollary to the Even Product Theorem: *The square of any even integer is even.*

Why is this a corollary to the Even Product Theorem and what is the proof of this corollary?

Solution

The square of any even integer is even is a corollary to the Even Product Theorem because it follows that theorem almost immediately.
The square of any even integer is even.
Proof:
Let x be any even integer. Since x^2 means $(x)(x)$ we know x^2 is the product of two even integers, thus by the Even Product Theorem, x^2 is even. Therefore, the square of any even integer is even. W^5

Summary and Review

- To prove an implication $p \Rightarrow q$, start by assuming that p is true. Use the information from this assumption, together with any other known results, to show that q must also be true.
- If necessary, you may break p into several cases $p_1, p_2, \ldots$, and prove each implication $p_i \Rightarrow q$ (separately, one at a time) as indicated above.
- Be sure to write the mathematical expressions clearly. Use different variables if the quantities involved may not be the same.
- To get started, write down the given information, the assumption, and what you want to prove.
- In the next step, use the definition if necessary, and rewrite the information in mathematical notations. The point is, try to obtain some mathematical equations or logical statements that we can manipulate.
- If you are stuck, think about the how the proof will end & write that down. Sometimes it helps to work backwards.

Exercises

Exercise 3.2.1

Prove or disprove: $2^n + 1$ is prime for all nonnegative integer n.

Solution

Consider $n = 3$; n is a nonnegative integer.

$$2^n + 1 = 2^3 + 1 = 9. \tag{3.2.6}$$

9 is not prime, since $(3)(3) = 9$, thus the statement: $2^n + 1$ is prime for all nonnegative integer n is false.

Exercise 3.2.2

Prove if n is an integer, then n^2 has the same parity as n.

Hint

Use proof by cases.

Exercise 3.2.3

Let n be an integer.

a. Show that if n is odd, then n^2 is also odd.
b. Show that if n is odd, then n^4 is also odd.
c. A ***corollary*** is a result that can be derived easily from another result. Derive (b) as a corollary of (a).
d. Show that if m and n are odd, then so is mn.
e. Show that if m is even, and n is odd, then mn is even.

Solution to (a)

If n is odd, then n^2 is also odd.
Proof: Let n be any odd integer. By definition of odd, $\exists k \in \mathbb{Z}(n = 2k+1)$.
$n^2 = (2k+1)^2$, by substitution. Then by algebra, $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$.
Since the set of integers is closed under multiplication and addition, $(2k^2+2k) \in \mathbb{Z}$.
So, by the definition of odd, n^2 is odd.
Therefore, if n is odd, then n^2 is also odd.

W^5

Exercise 3.2.4

Prove that, for any odd integer n, the number $2n^2+5n+4$ must be odd.

Exercise 3.2.5

Let n be an integer.

a. Prove that if n is a multiple of 3, then n^2 is also a multiple of 3.
b. Prove that if n is a multiple of 7, then n^3 is also a multiple of 7.

Solution to (a)

If n is a multiple of 3, then n^2 is also a multiple of 3.
Proof: Let n be any multiple of 3. By definition of multiple, there exists an integer k such that $n = 3k$.
$n^2 = (3k)^2$, by substitution. Then by algebra, $n^2 = (3k)^2 = 9k^2 = 3(3k^2)$.
Since the set of integers is closed under multiplication, $(3k^2) \in \mathbb{Z}$.
So, by the definition of multiple, n^2 is a multiple of 3.
Therefore, if n is a multiple of 3, then n^2 is also a multiple of 3.

W^5

Exercise 3.2.6

Prove that if $a \mid b$ and $c \mid (-a)$ then $(-c) \mid b$

Exercise 3.2.7

Prove that if $ac \mid bc$ then $a \mid b$

Exercise 3.2.8

Recall that we can use a counterexample to disprove an implication. Show that the following claims are false:

a. If x and y are integers such that $x^2 > y^2$, then $x > y$.
b. If n is a positive integer, then n^2+n+41 is prime.

Exercise 3.2.9

Explain why the following arguments are invalid:

a. Let n be an integer. If n^2 is odd, then n is odd. Therefore, n must be odd.
b. Let n be an integer. If n is even, then n^2 is also even. As an integer, n^2 could be odd. Hence, n cannot be even. Therefore, n must be odd.

Solution

(a) There is no information about n^2, so the statement "if n^2 is odd, then n is odd" is irrelevant to the parity of n.
(b) n^2 could be odd, but we also have n^2 could be even. So, we do not have enough information to determine the parity of n.

Exercise 3.2.10

Analyze the following reasoning:

a. Let S be a set of real numbers. If x is in S, then x^2 is in S. But x is not in S, hence x^2 is not in S.
b. Let S be a set of real numbers. If x is in S, then x^2 is in S. Therefore, if x^2 is in S, then x is in S.

Exercise 3.2.11

Show that there exists an integer n such that n, $n+2$ and $n+4$ are all primes.

Solution

Consider $n=3$. The numbers are $3, 5, 7$.

Exercise 3.2.12

Prove: If n is odd, then n^2-1 is divisible by 4.

3.3: Q-R Theorem and Mod

When we divide a positive integer (the dividend) by another positive integer (the divisor), we obtain a quotient. We multiply the quotient to the divisor, and subtract the product from the dividend to obtain the remainder. Such a division produces two results: a quotient and a remainder.

This is how we normally divide 23 by 4:

$$\begin{array}{r} 5 \\ 4\,\overline{)23} \\ \underline{20} \\ 3 \end{array} \tag{3.3.1}$$

In general, the division $b \div a$ takes the form

$$\begin{array}{r} q \\ a\,\overline{)\;b} \\ \underline{aq} \\ r \end{array} \tag{3.3.2}$$

so that $r = b - aq$, or equivalently, $b = aq + r$. Of course, both q and r are integers. Yet, the following "divisions"

$$\begin{array}{r} 4 \\ 4\,\overline{)23} \\ \underline{16} \\ 7 \end{array} \qquad \begin{array}{r} 2 \\ 4\,\overline{)23} \\ \underline{8} \\ 15 \end{array} \qquad \begin{array}{r} 6 \\ 4\,\overline{)23} \\ \underline{24} \\ -1 \end{array} \qquad \begin{array}{r} 7 \\ 4\,\overline{)23} \\ \underline{28} \\ -5 \end{array} \tag{3.3.3}$$

also satisfy the requirement $b = aq + r$, but that is not what we normally do. This means having $b = aq + r$ alone is not enough to define what quotient and remainder are. We need a more rigid definition.

Theorem 3.3.1 Quotient-Remainder Theorem

Given any integers a and d, where $d > 0$, there exist integers q and r such that

$$a = dq + r, \tag{3.3.4}$$

where $0 \leq r < d$. Furthermore, q and r are uniquely determined by a and d.

The integers a, d, q, and r are called the ***dividend***, ***divisor***, ***quotient***, and ***remainder***, respectively. Notice that a is a multiple of d if and only if $r = 0$.

Remark

This is the outline of the proof:

- Describe how to find the integers q and r such that $a = dq + r$.
- Show that our choice of r satisfies $0 \leq r < d$.
- Establish the uniqueness of q and r.

Regarding the last part of the proof: to show that a certain number x is uniquely determined, a typical approach is to assume that x' is another choice that satisfies the given condition, and show that we must have $x = x'$.

Proof

This proof is not here because this proof needs the principle of Well-ordering Principle which we will cover soon.

However, the outline above describes the general format of the proof.

Notes:

- You can refer to the Quotient-Remainder Theorem in later work
- We use Q-R Theorem or Q-R Thm as a nick name.

You should not have any problem dividing a positive integer by another positive integer. This is the kind of long division that we normally perform. It is more challenging to divide a negative integer by a positive integer. When b is negative, the quotient q will be negative as well, but the remainder r must be *nonnegative*. In a way, r is the deciding factor: we choose q such that the remainder r satisfies the condition $0 \leq r < a$.

In general, for any integer b, dividing b by a produces a decimal number. If the result is not an integer, round it *down* to the next smaller integer (see Example 3.3.1). It is the quotient q that we want, and the remainder r is obtained from the subtraction $r = b - aq$. For example,

$$\frac{-22}{7} = -3.1428\ldots. \tag{3.3.5}$$

Rounding it down produces the quotient $q = -4$, and the remainder is $r = -22 - 7(-4) = 6$; and we do have $-22 = 7 \cdot (-4) + 6$.

Example 3.3.1

According to the Quotient-Remainder Theorem, compute the quotients q and the remainders r when m is divided by d:

(a) $m = 47, d = 5$ & (b) $m = -47, d = 5$ & (c) $m = -41, d = 12$

Solution

(a) 47 = 9(5)+2, so $q = 5$, $r = 2$
(b) -47 = -10(5)+3, so $q = -10$, $r = 3$
(c) -41 = -4(12)+7, so $q = -4$, $r = 7$

hands-on Exercise 3.3.1

According to the Quotient-Remainder Theorem, compute the quotients q and the remainders r when b is divided by a:

(a) $b = 128, a = 7$ & (b) $b = -128, a = 7$ & (c) $b = -389, a = 16$

Be sure to verify that $b = aq + r$.

Definition MOD (and div)

Given integers a and b, with $a > 0$,

$$b \bmod a = r \leftrightarrow b = aq + r \tag{3.3.6}$$

where $q \in \mathbb{Z}$, $r \in \mathbb{Z}$ and $0 \leq r < a$.

Furthermore,

$$b \operatorname{div} a = q \leftrightarrow b = aq + r. \tag{3.3.7}$$

where $q \in \mathbb{Z}$, $r \in \mathbb{Z}$ and $0 \leq r < a$.

div and mod are binary operators where $b \operatorname{div} a$ gives the quotient, and $b \bmod a$ yields the remainder of the integer division $b \div a$. Notice $b \operatorname{div} a$ can be positive, negative, or even zero. But $b \bmod a$ is always a nonnegative integer less than a. In fact, $b \bmod a$ will take on one of the values from 0, 1, 2, ..., $a - 1$.

example 3.3.2

Let n be an integer such that $n \bmod 6 = 4$. Determine the value of $(2n + 5) \bmod 6$.

Solution

The given information implies that $n=6q+4$ for some integer q. Then

$$2n+5=2(6q+4)+5=12q+8+5=12q+13=12q+12+1=6(2q+2)+1. \tag{3.3.8}$$

Therefore, $(2n+5) \bmod 6=1$.

hands-on Exercise 3.3.2

Let n be an integer such that $n \bmod 11=5$. Compute the value of d $(6n-4) \bmod 11$.

example 3.3.3

Suppose today is Wednesday. Which day of the week is it a year from now?

Solution

Denote Sunday, Monday, …, Saturday as Day 0, 1, … 6, respectively. Today is Day 3. A year (assuming 365 days in a year) from today will be Day 368. Since

$$368=7\cdot 52+4, \tag{3.3.9}$$

it will be Day 4 of the week. Therefore, a year from today will be Thursday.

hands-on Exercise 3.3.3

Suppose today is Friday. Which day of the week is it 1000 days from today?

Representations of Integers using Modulo

From the Quotient-Remainder Theorem, we know that any integer divided by a positive integer will have a set number of remainders, and thus a set number of representations.

For example, any integer divided by 7 will produce a remainder between 0 and 6, inclusive. So every integer, n can be represented by one of the following:

$n=7q \quad n=7q+1 \quad n=7q+2 \quad n=7q+3 \quad n=7q+4 \quad n=7q+5 \quad n=7q+6,$ where $q\in\mathbb{Z}$.

These representations can be used to prove the statement: *The square of any odd integer has the form $8m+1$ for some integer m.*

Start by choosing an arbitrary odd integer n. State that by the Quotient-Remainder Theorem any integer is able to be represented in one of these ways:

$n=4q \quad n=4q+1 \quad n=4q+2 \quad n=4q+3,$ for some integer q.

Using the fact that n is odd, you will be able to eliminate two of these representations, leaving just two possibilities.

The rest of the proof proceeds using proof by cases (the 2 remaining cases). (See exercises.)

Example 3.3.5

Show that if an integer n is not divisible by 3, then n^2-1 must be a multiple of 3.

Remark

The letter n has been used to identify the integer of interest to us, and it appears in the hypothesis of the implication that we want to prove. Nonetheless, many authors would start their proofs with the familiar phrase “Let n be … .”

Answer

Let n be an integer that is not divisible by 3. When it is divided by 3, the remainder is 1 or 2. Hence, $n=3q+1$ or $n=3q+2$ for some integer q.

Case 1: If $n=3q+1$ for some integer q, then by algebra

$$n^2-1=9q^2+6q=3(3q^2+2q), \tag{3.3.10}$$

where $3q^2+2q$ is an integer because the $\mathbb{Z}$ is closed under multiplication and addition. Thus in this case, n^2-1 is a multiple of 3, by definition of multiple.

Case 2: If $n=3q+2$ for some integer q, then by algebra

$$n^2-1=9q^2+12q+3=3(3q^2+4q+1), \tag{3.3.11}$$

where $3q^2+4q+1$ is an integer because the $\mathbb{Z}$ is closed under multiplication and addition. Thus in this case, n^2-1 is a multiple of 3, by definition of multiple..

In both cases, we have shown that n^2-1 is a multiple 3. Therefore, if an integer n is not divisible by 3, then n^2-1 must be a multiple of 3.

W^5

hands-on exercise 3.3.6

Show that $n(n+1)(2n+1)$ is divisible by 6 for all $n \in \mathbb{N}$.

Hint

One of the two integers n and $n+1$ must be even (you MAY refer to the theorem: *Consecutive integers have opposite parity*.), so we can easily show that the product $n(n+1)(2n+1)$ is a multiple of 2. Hence, it remains to show that it is also a multiple of 3. Consider three cases: $n=3q$, $n=3q+1$, or $n=3q+2$, where q is an integer.

Absolute Value and Triangle Inequality Theorem

Definition

For all real numbers x,

$$|x|=\begin{cases}-x & \text{if } x<0\\ x & \text{if } x\geq 0\end{cases}$$

Theorem 3.3.1 Triangle Inequality Theorem

For all real numbers x and y, the following inequality holds: $|x+y| \leq |x|+|y|$.

Proof

proof is still to come

Summary and Review

- Given any integer b, and any positive integer a, there exist uniquely determined integers q and r such that $b=aq+r$, where $0 \leq r < a$.
- We call q the quotient, and r the remainder.
- The reason we have unique choices for q and r is the criterion we place on r. It has to satisfy the requirement $0 \leq r < a$.
- In fact, the criterion $0 \leq r < a$ is the single most important deciding factor in our choice of q and r.
- We define two binary operations on integers. The div operation yields the quotient, and the $\bmod$ operation produces the remainder, of the integer division $b \div a$. In other words, $b \operatorname{div} a = q$, and $b \bmod a = r$.

Exercises

exercise 3.3.1

Find

(a) $300 \bmod 13 =$

(b) $-115 \bmod 11 =$

(c) $145 \bmod -22 =$

Solution

(a) 1 because 23(13)= 299 and 300 = 23(13) +1
(b) 6 because -11(11)= -121 and -115 = -11(11) + 6
(c) impossible since -22 is not greater than 0.

exercise 3.3.2

Find $b \bmod a$, where

(a) $79 \bmod 19 =$

(b) $59 \bmod 18 =$

(c) $-823 \bmod 16 =$

(d) $172 \bmod -8 =$

(e) $-134 \bmod 20 =$

exercise 3.3.3

Let m and n be integers such that

$$m \bmod 5 = 1, n \bmod 5 = 3. \tag{3.3.12}$$

Determine

(a) $(m+n) \bmod 5$

(b) $(mn) \bmod 5$

exercise 3.3.4

Prove that among any three consecutive integers, one of them is a multiple of 3.

Hint

Let the three consecutive integers be n, $n+1$, and $n+2$. What are the possible values of $n \bmod 3$? What does this translate into, according to the division algorithm? In each case, what would n, $n+1$, and $n+2$ look like?

exercise 3.3.5

Prove that $n^3 - n$ is always a multiple of 3 for any integer n by

a. A case-by-case analysis.
b. Factoring $n^3 - n$.

exercise 3.3.6

Prove *The square of any odd integer has the form* $8m+1$ *for some integer* m.

(See comments in the text, *Representations of Integers using Modulo*, about this proof.)

exercise 3.3.7

Let m and n be integers such that

$$a \bmod 5 = 4, b \bmod 5 = 2. \tag{3.3.13}$$

Prove

$$(ab) \bmod 5 = 3. \tag{3.3.14}$$

3.4: Indirect Proofs

Instead of proving $p \Rightarrow q$ directly, it is sometimes easier to prove it indirectly. There are two kinds of ***indirect proofs***: proof by contrapositive, and proof by contradiction.

Proof by Contrapositive

Proof by contrapositive is based on the fact that an implication is equivalent to its contrapositive. Therefore, instead of proving $p \Rightarrow q$, we may prove its contrapositive $\overline{q} \Rightarrow \overline{p}$. Since it is an implication, we could use a direct proof:

Assume $\overline{q}$ is true (hence, assume q is false).

Show that $\overline{p}$ is true (that is, show that p is false).

The proof may proceed as follow:

Prove: $p \Rightarrow q$

Proof: We will prove the contrapositive of the stated result.

That is, we will prove $\overline{q} \Rightarrow \overline{p}$.

Assume q is false, . . .

.

.

.

. . . Therefore p is false.

Thus $\overline{q} \Rightarrow \overline{p}$.

Therefore, by contraposition, $p \Rightarrow q$.

Lemma 3.4.1

Let n be an integer. Show that if n^2 is even, then n is also even.

Proof:

Proof by contrapositive: We want to prove that if n is odd, then n^2 is odd. Let n be an odd integer, then $n = 2t+1$ for some integer t by definition of odd. By algebra

$$n^2 = 4t^2 + 4t + 1 = 2(2t^2 + 2t) + 1. \tag{3.4.1}$$

Since $\mathbb{Z}$ is closed under addition & multiplication, $2t^2 + 2t$ is an integer. Hence n^2 is odd by definition of odd.

Thus if n is odd, then n^2 is odd.

Therefore, by contraposition, for all integers n if n^2 is even, then n is even.

Note: Lemma $3.4.1$ will be used in the proof that $\sqrt{2}$ is irrational, later in this section.

Example 3.4.1

Show that if n is a positive integer such that the sum of its positive divisors is $n+1$, then n is prime.

Solution

We shall prove the contrapositive of the given statement. We want to prove that if n is composite, then the sum of its positive divisors is not $n+1$. Let n be a composite number. Then its divisors include 1, n, and at least one other positive divisor x different from 1 and n. So the sum of its positive divisors is at least $1+n+x$. Since x is positive, we gather that

$$1 + n + x > 1 + n. \tag{3.4.2}$$

We deduce that the sum of the divisors cannot be $n+1$. Therefore, if the sum of the divisors of n is precisely $n+1$, then n must be prime.

Proof by Contradiction

Another indirect proof is ***proof by contradiction***. To prove that $p \Rightarrow q$, we proceed as follows:

Suppose $p \Rightarrow q$ is false; that is, assume that p is true and q is false.

Argue until we obtain a contradiction, which could be any result that we know is false.

How does this prove that $p \Rightarrow q$? Assuming that the logic used in every step in the argument is correct, yet we still end up with a contradiction, then the only possible flaw must come from the supposition that $p \Rightarrow q$ is false. Consequently, $p \Rightarrow q$ must be true.

This is what a typical proof by contradiction may look like:

Proof: Suppose not. That is, suppose p is true and q is false. Then

. . .

.

.

a contradiction!!

Thus our assumption that p is true and q is false cannot be true.

Therefore, $p \Rightarrow q$ must be true.

There is a more general form for proving a statement r, which needs not be an implication. To prove the proposition r by contradiction, we follow these steps:

Suppose r is false.

Argue until we obtain a contradiction.

Proof: Suppose not. That is, suppose r is false. Then . . .

.

.

a contradiction!!

Thus our assumption that r is false cannot be true.

Therefore, r must be true.

Example 3.4.2

Show that if P is a point not on a line L, then there exists exactly one perpendicular line from P onto L.

Solution

Suppose we can find more than one perpendicular line from P onto L. Pick any two of them, and denote their intersections with L as Q and R. Then we have a triangle PQR, where the angles PQR and PRQ are both 90°. This implies that the sum of the interior angles of the triangle PQR exceeds 180°, which is impossible. Hence, there is only one perpendicular line from P onto L.

Example 3.4.3

Show that if $x^2 < 5$, then $|x| < \sqrt{5}$.

note: *if no set of numbers is specified, the default is the set of real numbers.*

Solution

Assume $x^2 < 5$. We want to show that $|x| < \sqrt{5}$. Suppose, on the contrary, we have $|x| \geq \sqrt{5}$.

By definition, $|x| = x$ or $|x| = -x$.

So either $x \geq \sqrt{5}$, or $-x \geq \sqrt{5}$.

The second case, $-x \geq \sqrt{5}$ is the same as $x \leq -\sqrt{5}$ (by multiplying both sides by negative 1).

If $x \geq \sqrt{5}$, then $x^2 \geq 5$, by algebra; note: since x is a positive number the inequality sign does not change.

If $x \leq -\sqrt{5}$, we again have $x^2 \geq 5$, by algebra; note: since x is a negative number the inequality sign reverses.

In either case, we have both $x^2 \geq 5$ and $x^2 < 5$ which is a contradiction.

Hence $|x| < \sqrt{5}$.

$\therefore$ if $x^2 < 5$, then $|x| < \sqrt{5}$.

hands-on exercise 3.4.1

Prove that if $x^2 \geq 49$, then $|x| \geq 7$.

Example 3.4.4

Prove

$$[(p \Rightarrow q) \wedge p] \Rightarrow q \tag{3.4.3}$$

is a tautology.

Solution

Suppose $[(p \Rightarrow q) \wedge p] \Rightarrow q$ is false for some statements p and q. Then we find

- $(p \Rightarrow q) \wedge p$ is true, and
- q is false.

For the conjunction $(p \Rightarrow q) \wedge p$ to be true, we need

- $p \Rightarrow q$ to be true, and
- p to be true.

Having p true and $p \Rightarrow q$ true, we must have q true. That gives us q is true and q is false, a contradiction! Thus it cannot be that $[(p \Rightarrow q) \wedge p] \Rightarrow q$ is false. Therefore, $[(p \Rightarrow q) \wedge p] \Rightarrow q$ is always true, hence it is a tautology.

Example 3.4.5

Prove, by contradiction, that if x is rational and y is irrational, then $x + y$ is irrational.

Solution

Let x be a rational number and y an irrational number. We want to show that $x + y$ is irrational. Suppose, on the contrary, that $x + y$ is rational. Then

$$x + y = \frac{m}{n} \tag{3.4.4}$$

for some integers m and n, where $n \neq 0$ by definition of rational. Since x is rational, we also have

$$x = \frac{p}{q} \tag{3.4.5}$$

for some integers p and q, where $q \neq 0$ by defintion of rational. It follows by substitution that

$$\frac{m}{n} = x + y = \frac{p}{q} + y. \tag{3.4.6}$$

Hence by algebra,

$$y = \frac{m}{n} - \frac{p}{q} = \frac{mq - np}{nq}, \tag{3.4.7}$$

where $mq - np$ and nq are both integers because $\mathbb{Z}$ is closed under addition and multiplication. Also $nq \neq 0$ by the Zero Product Property. This makes y rational by definition of rational. Now we have y is rational and y is irrational (by assumption). This is a contradiction! Thus, $x + y$ cannot be rational, it must be irrational.

$\therefore$ if x is rational and y is irrational, then $x + y$ is irrational.

hands-on exercise 3.4.2

Prove that

$$\sqrt{x+y} \neq \sqrt{x} + \sqrt{y} \tag{3.4.8}$$

for any positive real numbers x and y.

Hint

The words "for any" suggest this is a universal quantification. Be sure you negate the problem statement properly.

Lemma 3.4.2

We will use this lemma (along with Lemma 3.4.1) for the proof that $\sqrt{2}$ is irrational.

Lemma 3.4.2 Given a rational number, x, x can be written as a fraction $\frac{m}{n}$ where $m, n \in \mathbb{Z}$, $n \neq 0$ and $\frac{m}{n}$ is in lowest terms.

Proof:

Given a rational number, x, x can be written as a fraction $\frac{a}{b}$ where $a, b \in \mathbb{Z}$,$b \neq 0$ by definition of rational number.

If $\frac{a}{b}$ is not in lowest terms, then a and b have a common factor. Divide out that common factor to get an equivalent fraction, $\frac{c}{d}$.

If $\frac{c}{d}$ is not in lowest terms, then c and d have a common factor. Divide out that common factor to get an equivalent fraction, $\frac{f}{g}$.

If $\frac{f}{g}$ is not in lowest terms, then f and g have a common factor. Divide out that common factor to get an equivalent fraction, $\frac{j}{k}$.

Continue this process until the numerator and denominator do not have any common factors. Rename the numerator as m and the denominator as n.

Now $x = \frac{m}{n}$ and $\frac{m}{n}$ is in lowest terms.
$\therefore$ a rational number can be written as a fraction in lowest terms.

The $\sqrt{2}$ is irrational.

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

Proof:

Suppose, on the contrary, $\sqrt{2}$ is rational. Then we can write

$$\sqrt{2} = \frac{m}{n} \tag{3.4.9}$$

for some positive integers m and n such that m and n do not share any common divisor except 1 (hence $\frac{m}{n}$ is in lowest terms) by Lemma 3.4.2. Squaring both sides and cross-multiplying yields

$$2n^2 = m^2. \tag{3.4.10}$$

Since $\mathbb{Z}$ are closed under multiplication, n^2 is an integer and thus m^2 is even by the definition of even. Consequently, by Lemma 3.4.1, m is also even. Then we can write $m = 2s$ for some integer s by the definition of even. By substitution and algebra, the equation above becomes

$$2n^2 = m^2 = (2s)^2 = 4s^2. \tag{3.4.11}$$

Hence,

$$n^2 = 2s^2. \tag{3.4.12}$$

Since $\mathbb{Z}$ are closed under multiplication, s^2 is an integer and thus n^2 is even by the definition of even. Consequently, by Lemma 3.4.1, n is also even. Even numbers are divisible by 2, by the definition of divides. We have shown that both m and n are divisible by 2. This contradicts the assumption that m and n do not share any common divisor. Thus is is not possible for $\sqrt{2}$ to be rational.

Therefore, $\sqrt{2}$ must be irrational.

hands-on exercise 3.4.3

Prove that $\sqrt{3}$ is irrational.

Very often, a proof by contradiction can be rephrased into a proof by contrapositive or even a direct proof, both of which are easier to follow. If this is the case, rewrite the proof.

Example 3.4.6

Show that $x^2 + 4x + 6 = 0$ has no real solution. In symbols, show that $\nexists x \in \mathbb{R}, (x^2 + 4x + 6 = 0)$.

Solution

Consider the following proof by contradiction:

> Suppose there exists a real number x such that $x^2 + 4x + 6 = 0$.
> Using calculus, it can be shown that the function $f(x) = x^2 + 4x + 6$
> has an absolute minimum at $x = -2$. **Need to show those calculus steps.**
>
> Thus, $f(x) \geq f(-2) = 2$ for
> any x. This contradicts the assumption that there exists an x
> such that $x^2 + 4x + 6 = 0$. Thus, $x^2 + 4x + 6 = 0$ has no real solution.

A close inspection reveals that we do not really need a proof by contradiction. The crux of the proof is the fact that $x^2 + 4x + 6 \geq 2$ for all x. This already shows that $x^2 + 4x + 6$ could never be zero. It is easier to use a direct proof, as follows.

> Using calculus, we see $f'(x) = 2x + 4$. Setting $f'(x) = 0$ we get $x = -2$. Since $f''(x) = 2$, thus $f''(-2) = 2$,we find that the function $f(x) = x^2 + 4x + 6$ has an
> absolute minimum at $x = -2$. Therefore, for any x, we always have
> $f(x) \geq f(-2) = 2$. Hence, there does not exist any x such that
> $x^2 + 4x + 6 = 0$.

Do you agree that the second proof (the direct proof) is more elegant?

Proving a Biconditional Statement

Recall that a biconditional statement $p \Leftrightarrow q$ consists of two implications $p \Rightarrow q$ and $q \Rightarrow p$. Hence, to prove $p \Leftrightarrow q$, we need to establish these two "directions" separately.

Example 3.4.7

Let n be an integer. Prove that n^2 is even if and only if n is even.

Solution

($\Rightarrow$) We first prove that if n^2 is even, then n must be even.

We shall prove its contrapositive: if n is odd, then n^2 is odd. If n is odd, then we can write $n = 2t+1$ for some integer t by definition of odd. Then by algebra

$$n^2 = (2t+1)^2 = 4t^2 + 4t + 1 = 2(2t^2 + 2t) + 1, \tag{3.4.13}$$

where $2t^2 + 2t$ is an integer since $\mathbb{Z}$ is closed under addition and multiplication. Thus, n^2 is odd. So, if n is odd, then n^2 is odd. By contraposition, if n^2 is even, then n is even.

($\Leftarrow$) Next, we prove that if n is even, then n^2 is even.

If n is even, we can write $n = 2t$ for some integer t by definition of even. Then

$$n^2 = (2t)^2 = 4t^2 = 2 \cdot 2t^2, \tag{3.4.14}$$

where $2t^2$ is an integer since $\mathbb{Z}$ is closed under multiplication. Hence, n^2 is even. if n is even, then n^2 is even.

$\therefore$ n^2 is even if and only if n is even.

hands-on exercise 3.4.4

Let n be an integer. Prove that n is odd if and only if n^2 is odd.

Summary and Review

- We can use indirect proofs to prove an implication.
- There are two kinds of indirect proofs: proof by contrapositive and proof by contradiction.
- In a proof by contrapositive, we actually use a direct proof to prove the contrapositive of the original implication.
- In a proof by contradiction, we start with the supposition that the implication is false, and use this assumption to derive a contradiction. This would prove that the implication must be true.
- A proof by contradiction can also be used to prove a statement that is not of the form of an implication. We start with the supposition that the statement is false, and use this assumption to derive a contradiction. This would prove that the statement must be true.
- Sometimes a proof by contradiction can be rewritten as a direct proof. If so, the direct proof is the more direct way to write the proof.

Exercises

exercise 3.4.1

Let n be an integer. Prove that if n^2 is even, then n must be even. Use

(a) A proof by contrapositive (this one is done - see proof of Lemma 3.4.1)

(b) A proof by contradiction.

Remark

The two proofs are very similar, but the wording is slightly different, so be sure you present your proof clearly.

exercise 3.4.2

Let n be an integer. Prove that if n^2 is a multiple of 3, then n must also be a multiple of 3. Use

(a) A proof by contrapositive.

(b) A proof by contradiction.

exercise 3.4.3

Let n be an integer. Prove that if n is even, then $n^2 = 4s$ for some integer s.

exercise 3.4.4

Let m and n be integers. Show that $mn = 1$ implies that $m = 1$ or $m = -1$.

exercise 3.4.5

Let x be a real number. Prove by contrapositive: if x is irrational, then $\sqrt{x}$ is irrational. Apply this result to show that $\sqrt[4]{2}$ is irrational, using the assumption that $\sqrt{2}$ is irrational.

exercise 3.4.6

Let x and y be real numbers such that $x \neq 0$. Prove that if x is rational, and y is irrational, then xy is irrational.

exercise 3.4.7

Prove that $\sqrt{5}$ is irrational.

exercise 3.4.8

Prove that $\sqrt[3]{2}$ is irrational.

exercise 3.4.9

Let a and b be real numbers. Prove that if $a \neq b$, then $a^2 + b^2 \neq 2ab$.

exercise 3.4.10

Use contradiction to prove that, for all integers $k \geq 1$,

$$2\sqrt{k+1} + \frac{1}{\sqrt{k+1}} \geq 2\sqrt{k+2}. \tag{3.4.15}$$

exercise 3.4.11

Let m and n be integers. Prove that mn is even if and only if m is even or n is even.

exercise 3.4.12

Let x and y be real numbers. Prove that $x^2 + y^2 = 0$ if and only if $x = 0$ and $y = 0$.

exercise 3.4.13

Prove that, if x is a real number such that $0 < x < 1$, then $x(1-x) \leq \frac{1}{4}$.

exercise 3.4.14

Let m and n be positive integers such that 3 divides mn. Prove that 3 divides m, or 3 divides n.

exercise 3.4.15

Prove that the logical formula

$$(p \Rightarrow q) \vee (p \Rightarrow \overline{q}) \tag{3.4.16}$$

is a tautology.

(See example 3.4.4.)

exercise 3.4.16

Prove that the logical formula

$$[(p \Rightarrow q) \wedge (p \Rightarrow \overline{q})] \Rightarrow \overline{p} \tag{3.4.17}$$

is a tautology.

(See example 3.4.4.)

3.5: The Euclidean Algorithm

Definitions: common divisor

Let a and b be integers, not both 0. A **common divisor** of a and b is any nonzero integer that divides both a and b. The largest natural number that divides both a and b is called the **greatest common divisor** of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$

Preview Activity 3.5.1: The GCD and the Division Algorithm

When we speak of the quotient and the remainder when we "divide an integer a by the positive integer b," we will always mean the quotient q and the remainder r guaranteed by the Quotient Remainder Theorem.

1. Each row in the following table contains values for the integers a and b. In this table, the value of r is the remainder (from the Division Algorithm) when a is divided by b. Complete each row in this table by determining $\gcd(a, b)$, r, and $\gcd(b, r)$.

a	b	$\gcd(a, b)$	Remainder r	$\gcd(b, r)$
44	12			
75	21			
50	33			

2. Formulate a conjecture based on the results of the table in Part (1).

We have already studied a good deal of number theory in this text in our discussion of proof methods. In particular, we have studied even and odd integers, divisibility of integers, and the Quotient-Remainder Theorem.

Before we develop an efficient method for determining the greatest common divisor of two integers, we need to establish some properties of greatest common divisors.

Lemma 3.5.1

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then $\gcd(0, b) = b$.

Lemma 3.5.2

Let c and d be integers, not both equal to zero. If q and r are integers such that $c = d \cdot q + r$, then $\gcd(c, d) = \gcd(d, r)$.

Proof

Let c and d be integers, not both equal to zero. Assume that q and r are integers such that $c = d \cdot q + r$. For ease of notation, we will let

$$m = \gcd(c, d) \text{ and } n = \gcd(d, r).$$

Now, m divides c and m divides d. Consequently, there exist integers x and y such that $c = mx$ and $d = my$. Hence,

$$\begin{aligned} r &= c - d \cdot q \\ r &= mx - (my)q \\ r &= m(x - yq). \end{aligned} \tag{3.5.1}$$

But this means that m divides r. Since m divides d and m divides r, m is less than or equal to $\gcd(d, r)$. Thus, $m \le n$.

Using a similar argument, we see that n divides d and n divides r. Since $c = d \cdot q + r$, we can prove that n divides c. Hence, n divides c and n divides d. Thus, $n \le \gcd(c, d)$ or $n \le m$. We now have $m \le n$ and $n \le m$. Hence, $m = n$ and $\gcd(c, d) = \gcd(d, r)$.

Progress Check 3.5.1: Illustrations of Lemma 3.5.2

We completed several examples illustrating Lemma 8.1 in Preview Activity $3.5.1$. For another example, let $c = 56$ and $d = 12$. The greatest common divisor of 56 and 12 is 4.

1. According to the Division Algorithm, what is the remainder r when 56 is divided by 12?
2. What is the greatest common divisor of 12 and the remainder r?

   The key to finding the greatest common divisor (in more complicated cases) is to use the Division Algorithm again, this time with 12 and r. We now find integers q_2 and r_2 such that

   $$12 = r \cdot q_2 + r_2. \tag{3.5.2}$$
3. What is the greatest common divisor of r and r_2?

Answer

(1) 8
(2) 4; 12 = 8(1) +4
(3) 4

The Euclidean Algorithm

The example in Progress Check 8.2 illustrates the main idea of the **Euclidean Algorithm** for finding gcd(a, b), which is explained in the proof of the following theorem.

Theorem 3.5.1: Euclidean Algorithm

Let a and b be integers with $a > b \geq 0$. Then gcd(a, b) is the only natural number d such that

(a) d divides a and d divides b, and
(b) if k is an integer that divides both a and b, then k divides d.

Note: if $b = 0$ then the gcd(a, b)=a, by Lemma 3.5.1.

Proof

Let a and b be integers with $a > b \geq 0$, and let $d =$ gcd(a, b). By the Quotient Remainder Theorem, there exist integers q_1 and r_1 such that

$$a = b \cdot q_1 + r_1, \text{ and } 0 \leq r_1 < b. \tag{3.5.3}$$

If $r_1 = 0$, then equation (8.1.3) implies that b divides a. Hence, $b = d =$ gcd(a, b) and this number satisfies Conditions (a) and (b).

If $r_1 > 0$, then by Lemma 8.1, gcd(a, b) = gcd(b, r_1). We use the Division Algorithm again to obtain integers q_2 and r_2 such that

$$b = r_1 \cdot q_2 + r_2, \text{ and } 0 \leq r_2 < r_1. \tag{3.5.4}$$

If $r_2 = 0$, then equation (8.1.4) implies that r_1 divides b. This means that $r_1 =$ gcd(b, r_1). But we have already seen that gcd(a, b) = gcd(b, r_1). Hence, $r_1 =$ gcd(a, b). In addition, if k is an integer that divides both a and b, then, using equation (8.1.3), we see that $r_1 = a - b \cdot q_1$ and, hence k divides r_1. This shows that $r_1 =$ gcd(a, b) satisfies Conditions (a) and (b).

If $r_2 > 0$, then by Lemma 8.1, gcd(b, r_1) = gcd(r_1, r_2). But we have already seen that gcd(a, b) = gcd(b, r_1). Hence, gcd(a, b) = gcd(r_1, r_2). We now continue to apply the Division Algorithm to produce a sequence of pairs of integers (all of which have the same greatest common divisor). This is summarized in the following table:

Original Pair	Equation from Division	Inequality from Division Algorithm	New Pair
(a,b)	$a = b \cdot q_1 + r_1$	$0 \leq r_1 < b$	(b,r_1)

Original Pair	Equation from Division	Inequality from Division Algorithm	New Pair
(b, r_1)	$b = r_1 \cdot q_2 + r_2$	$0 \le r_2 < r_1$	(r_1, r_2)
(r_1, r_2)	$r_1 = r_2 \cdot q_1 + r_3$	$0 \le r_3 < r_2$	(r_2, r_3)
(r_2, r_3)	$r_2 = r_3 \cdot q_1 + r_4$	$0 \le r_4 < r_3$	(r_3, r_4)
(r_3, r_4)	$r_3 = r_4 \cdot q_1 + r_5$	$0 \le r_5 < r_4$	(r_4, r_5)
...	...	...	...

From the inequalities in the third column of this table, we have a strictly decreasing sequence of nonnegative integers ($b > r_1 > r_2 > r_3 > r_4 \cdots$). Consequently, a term in this sequence must eventually be equal to zero. Let p be the smallest natural number such that $r_{p+1} = 0$. This means that the last two rows in the preceding table will be

Original Pair	**Equation from Division Algorithm**	**Inequality from Division Algorithm**	**New Pair**
(r_{p-2}, r_{p-1})	$r_{p-2} = r_{p-1} \cdot q_p + r_p$	$0 \le r_p < r_{p-1}$	(r_{p-1}, r_p)
(r_{p-1}, r_p)	$r_{p-1} = r_p \cdot q_{p+1} + 0$		

Remember that this table was constructed by repeated use of Lemma 8.1 and that the greatest common divisor of each pair of integers produced equals gcd(a, b). Also, the last row in the table indicates that r_p divides r_{p-1}. This means that gcd(r_{p-1}, r_p) $= r_p$ and hence $r_p =$ gcd(a, b).

This proves that $r_p =$ gcd(a, b) satisfies Condition (a) of this theorem. Now assume that k is an integer such that k divides a and k divides b. We proceed through the table row by row. First, since $r_1 = a - b \cdot q$, we see that

$$k \text{ must divide } r_1.$$

The second row tells us that $r_2 = b - r_1 \cdot q_2$. Since k divides b and k divides r_1, we conclude that

$$k \text{ divides } r_2.$$

Continuing with each row, we see that k divides each of the remainders $r_1, r_2, r_3, \ldots, r_p$. This means that $r_p =$ gcd(a, b) satisfies Condition (b) of the theorem.

Example 3.5.1: (Using the Euclidean Algorithm)

Let $a = 234$ and $b = -42$. We will use the Euclidean Algorithm to determine gcd(234, 42).

Step	**Original Pair**	**Equation from Division Algorithm**	**New Pair**
1	(234, 42)	$234 = 42 \cdot 5 + 24$	(42, 24)
2	(42, 24)	$42 = 24 \cdot 1 + 18$	(24, 18)
3	(24, 18)	$24 = 18 \cdot 1 + 6$	(18, 6)
4	(18, 6)	$18 = 6 \cdot 3$	

So gcd(234, 42) = 6 and hence gcd(234, -42) = 6.

Exercises

Exercise 3.5.1:

1. Find each of the following greatest common divisors by using the Euclidean Algorithm.

(a) gcd(21, 2511) (b) gcd(110, 2511) (c) gcd(509,1177)

2. Find each of the following greatest common divisors by using the Euclidean Algorithm.
(a) gcd(10933, 832) (b) gcd(1265,18400)

3. Let $a, b \in \mathbb{Z}^+$ find
(a) gcd(a,1) (b) gcd(a,a) (c) gcd(a,0) if $a > 0$ (d) gcd(a,35) if $a = 35b + 14$

Answer:

(a) 1 (b) a (c) a (d) 7

4. Disprove *mod is distributive over multiplication for the set* $\mathbb{Z}^+$, i.e. using $a, b, c \in \mathbb{Z}^+$.

3.6: Mathematical Induction - An Introduction

Mathematical induction can be used to prove that an identity is valid for all integers $n \geq 1$. Here is a typical example of such an identity:

$$1+2+3+\cdots+n = \frac{n(n+1)}{2}. \tag{3.6.1}$$

More generally, we can use mathematical induction to prove that a propositional function $P(n)$ is true for all integers $n \geq a$.

Principal of Mathematical Induction (PMI)

Given a propositional function $P(n)$ defined for integers n, and a fixed integer a.

Then, if these two conditions are true

1. $P(a)$ is true.
2. if $P(k)$ is true for some integer $k \geq a$, then $P(k+1)$ is also true.

then the $P(n)$ is true for all integers $n \geq a$.

Outline for Mathematical Induction

To show that a propositional function $P(n)$ is true for all integers $n \geq a$, follow these steps:

- ***Base Step***: Verify that $P(a)$ is true.
- ***Inductive Step***: Show that if $P(k)$ is true for some integer $k \geq a$, then $P(k+1)$ is also true.
  - Assume $P(n)$ is true for an arbitrary integer, k with $k \geq a$. This is the inductive hypothesis.
  - With this assumption (the inductive hypothesis), show $P(k+1)$ is true.
- Conclude, by the Principle of Mathematical Induction (PMI) that $P(n)$ is true for all integers $n \geq a$.

The base step is also called the ***basis step*** or the ***anchor step*** or the ***initial step***.

The base step and the inductive step, together, prove that

$$P(a) \Rightarrow P(a+1) \Rightarrow P(a+2) \Rightarrow \cdots. \tag{3.6.2}$$

Therefore, $P(n)$ is true for all integers $n \geq a$. Compare induction to falling dominoes. When the first domino falls, it knocks down the next domino. The second domino in turn knocks down the third domino. Eventually, all the dominoes will be knocked down. But it will not happen unless these conditions are met:

- The first domino must fall to start the motion. If it does not fall, no chain reaction will occur. This is the base step.
- The distance between adjacent dominoes must be set up correctly. Otherwise, a certain domino may fall down without knocking over the next. Then the chain reaction will stop, and will never be completed. Maintaining the right inter-domino distance ensures that $P(k) \Rightarrow P(k+1)$ for each integer $k \geq a$.

To prove the implication

$$P(k) \Rightarrow P(k+1) \tag{3.6.3}$$

in the inductive step, we need to carry out two steps: assuming that $P(k)$ is true, then using it to prove $P(k+1)$ is also true. So we can refine an induction proof into a 3-step procedure:

- Verify that $P(a)$ is true.
- Assume that $P(k)$ is true for some integer $k \geq a$.
- Show that $P(k+1)$ is also true.

The second step, the assumption that $P(k)$ is true, is referred to as the ***inductive hypothesis.*** This is how a mathematical induction proof may look:

The idea behind mathematical induction is rather simple. However, it must be delivered with precision.

- Be sure to say "Assume $P(n)$ holds for *some* integer $k \geq a$." Do not say "Assume it holds for *all* integers $k \geq a$." If we already know the result holds for all $k \geq a$, then there is no need to prove anything at all.
- Be sure to specify the requirement $k \geq a$. This ensures that the chain reaction of the falling dominoes starts with the first one.
- Do not say "let $n = k$" or "let $n = k+1$." The point is, you are not assigning the value of k and $k+1$ to n. Rather, you are *assuming* that the statement is true *when* n equals k, and using it to show that the statement also holds *when* n equals $k+1$.

Some proofs by induction

$1+2+3+\cdots+n$

Example 3.6.1

Use mathematical induction to show proposition $P(n)$:

$$1+2+3+\cdots+n = \frac{n(n+1)}{2} \tag{3.6.4}$$

for all integers $n \geq 1$.

Proof

Base Step: consider n = 1

On the Left-Hand Side (LHS) we get 1. On the Right-Hand Side (RHS) we get $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Thus $P(n)$ is true for $n=1$.

Inductive step: Assume $P(n)$ is true for $n = k, k \geq 1$. In other words, $P(k)$ is true so our inductive hypothesis is

$$1+2+3+\cdots+k = \frac{k(k+1)}{2}. \tag{3.6.5}$$

Consider the left-hand side of $P(k+1)$.

$$1+2+3+\cdots+(k+1) = 1+2+\cdots+k+(k+1), \tag{3.6.6}$$

we can regroup this as

$$1+2+3+\cdots+(k+1) = [1+2+\cdots+k]+(k+1), \tag{3.6.7}$$

so that $1+2+\cdots+k$ can be replaced by $\frac{k(k+1)}{2}$, by the inductive hypothesis.

Using the inductive hypothesis, we find

$$\begin{aligned} 1+2+3+\cdots+(k+1) &= 1+2+3+\cdots+k+(k+1) \\ &= \frac{k(k+1)}{2}+(k+1) \\ &= (k+1)\left(\frac{k}{2}+1\right) \\ &= (k+1)\cdot\frac{k+2}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

Therefore, the identity also holds when $n = k+1$.

Thus, by the Principle of Mathematical Induction (PMI),

$$1+2+3+\cdots+n = \frac{n(n+1)}{2} \tag{3.6.8}$$

for all integers $n \geq 1$.

We can use the ***summation notation*** (also called the ***sigma notation***) to abbreviate a sum. For example, the sum in the last example can be written as

$$\sum_{i=1}^{n} i. \tag{3.6.9}$$

The letter i is the ***index of summation***. By putting $i=1$ under $\sum$ and n above, we declare that the sum starts with $i=1$, and ranges through $i=2$, $i=3$, and so on, until $i=n$. The quantity that follows $\sum$ describes the pattern of the terms that we are adding in the summation. Accordingly,

$$\sum_{i=1}^{10} i^2 = 1^2+2^2+3^2+\cdots+10^2. \tag{3.6.10}$$

In general, the sum of the first n terms in a sequence $\{a_1, a_2, a_3, \ldots\}$ is denoted $\sum_{i=1}^{n} a_i$. Observe that

$$\sum_{i=1}^{k+1} a_i = \left(\sum_{i=1}^{k} a_i\right) + a_{k+1}, \tag{3.6.11}$$

which provides the link between $P(k+1)$ and $P(k)$ in an induction proof.

$\sum_{i=1}^{n} i^2$

Example $3.6.2$

Use mathematical induction to show that, for all integers $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = 1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{3.6.12}$$

Proof

Base Step: When $n=1$, the left-hand side reduces to $1^2=1$, and the right-hand side becomes $\frac{1\cdot 2\cdot 3}{6}=1$; hence, the identity holds when $n=1$.

Inductive Step: Assume it holds when $n=k$ for some integer $k \geq 1$; that is, assume for some integer $k \geq 1$ that

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6} \tag{3.6.13}$$

.

Consider $n=k+1$.

$$\sum_{i=1}^{k+1} i^2 = 1^2+2^2+3^2+\cdots+k^2+(k+1)^2. \tag{3.6.14}$$

From the inductive hypothesis, we find

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 \tag{3.6.15}$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \tag{3.6.16}$$

$$= \frac{k(k+1)(2k+1)+6(k+1)^2}{6} \tag{3.6.17}$$

$$\frac{(k+1)[k(2k+1)+6(k+1)]}{6} \tag{3.6.18}$$

$$\frac{(k+1)(2k^2+7k+6)}{6} \tag{3.6.19}$$

$$\frac{(k+1)(k+2)(2k+3)}{6} \tag{3.6.20}$$

$$\frac{(k+1)(k+2)(2(k+1)+1)}{6}. \tag{3.6.21}$$

Therefore, the identity also holds when $n=k+1$.
Thus, by PMI for all integers $n \geq 1$,

$$\sum_{i=1}^{n} i^2 = 1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{3.6.22}$$

hands-on exercise 3.6.1

It is time for you to write your own induction proof. Prove that

$$1\cdot 2+2\cdot 3+3\cdot 4+\cdots+n(n+1) = \frac{n(n+1)(n+2)}{3} \tag{3.6.23}$$

for all integers $n \geq 1$.

hands-on exercise 3.6.2

Use induction to prove that, for all positive integers n,

$$1\cdot 2\cdot 3+2\cdot 3\cdot 4+\cdots+n(n+1)(n+2) = \frac{n(n+1)(n+2)(n+3)}{4}. \tag{3.6.24}$$

hands-on exercise 3.6.3

Use induction to prove that, for all positive integers n,

$$1+4^1+4^2+\cdots+4^n = \frac{4^{n+1}-1}{3}. \tag{3.6.25}$$

All three steps in an induction proof must be completed; otherwise, the proof may not be correct.

Example 3.6.3

Can we just use examples?

Never attempt to prove $P(k) \Rightarrow P(k+1)$ *by examples alone*. Consider

$$P(n): \qquad n^2+n+11 \text{ is prime.} \tag{3.6.26}$$

In the inductive step, we want to prove that

$$P(k) \Rightarrow P(k+1) \qquad \text{for ANY } k \geq 1. \tag{3.6.27}$$

The following table verifies that it is true for $1 \leq k \leq 9$:

n	1	2	3	4	5	6	7	8	9
n^2+n+11	13	17	23	31	41	53	67	83	101

(3.6.28)

Nonetheless, when $n=10$, $n^2+n+11=121$ is composite. So $P(9)\Rightarrow P(10)$ is false. The inductive step breaks down when $k=9$.

Example 3.6.4

The base step is equally important. Consider proving

$$P(n): \qquad 3n+2=3q \text{ for some integer } q \tag{3.6.29}$$

for all $n\in\mathbb{N}$. Assume $P(k)$ is true for some integer $k\geq 1$; that is, assume $3k+2=3q$ for some integer q. Then

$$3(k+1)+2=3k+3+2=3+3q=3(1+q). \tag{3.6.30}$$

Therefore, $3(k+1)+2$ can be written in the same form. This proves that $P(k+1)$ is also true. Does it follow that $P(n)$ is true for all integers $n\geq 1$? We know that $3n+2$ cannot be written as a multiple of 3. What is the problem?

Solution

The problem is: we need $P(k)$ to be true for at least one value of k so as to start the sequence of implications

$$P(1)\Rightarrow P(2), \qquad P(2)\Rightarrow P(3), \qquad P(3)\Rightarrow P(4), \qquad \ldots \tag{3.6.31}$$

The induction fails because we have not established the basis step. In fact, $P(1)$ is false. Since the first domino does not fall, we cannot even start the chain reaction.

Remark

Thus far, we have learned how to use mathematical induction to prove identities. In general, we can use mathematical induction to prove a statement about n. This statement can take the form of an identity, an inequality, or simply a verbal statement about n. We shall learn more about mathematical induction in the next few sections.

Summary and Review

- Mathematical induction can be used to prove that a statement about n is true for all integers $n\geq a$.
- We have to complete three steps.
- In the base step, verify the statement for $n=a$.
- In the inductive hypothesis, assume that the statement holds when $n=k$ for some integer $k\geq a$.
- In the inductive step, use the information gathered from the inductive hypothesis to prove that the statement also holds when $n=k+1$.
- Be sure to complete all three steps.
- Pay attention to the wording. At the beginning, follow the template closely. When you feel comfortable with the whole process, you can start venturing out on your own.

Exercises

Exercise 3.6.1

Use induction to prove that

$$1^3+2^3+3^3+\cdots+n^3=\frac{n^2(n+1)^2}{4} \tag{3.6.32}$$

for all integers $n\geq 1$.

Exercise 3.6.2

Use induction to prove that the following identity holds for all integers $n\geq 1$:

$$1+3+5+\cdots+(2n-1)=n^2. \tag{3.6.33}$$

Proof

Base Case: consider $n=1$. $2(1)-1=1$ and $1^2=1$ so the LHS & RHS are both 1. This works for $n=1$.

Inductive Step: Assume this works for some integer, $k \geq 1$. In other words, $1+3+5+\cdots+(2k-1)=k^2$. (Inductive Hypothesis)

Consider the case of $n=k+1$. $1+3+5+\cdots+(2k-1)+(2(k+1)-1)$

$$=k^2+(2(k+1)-1) \text{ by inductive hypothesis} \tag{3.6.34}$$

$$=k^2+2k+2-1=k^2+2k+1=(k+1)^2 \text{ by algebra} \tag{3.6.35}$$

$1+3+5+\cdots+(2(k+1)-1)=(k+1)^2$; assuming our proposition works for k it will also work for $k+1$.

By PMI, $1+3+5+\cdots+(2n-1)=n^2$ for all integers, $n \geq 1$.

W^5

Exercise 3.6.3

Use induction to show that

$$1+\frac{1}{3}+\frac{1}{3^2}+\cdots+\frac{1}{3^n}=\frac{3}{2}\left(1-\frac{1}{3^{n+1}}\right) \tag{3.6.36}$$

for all positive integers n.

Exercise 3.6.4

Use induction to establish the following identity for any integer $n \geq 1$:

$$1-3+9-\cdots+(-3)^n=\frac{1-(-3)^{n+1}}{4}. \tag{3.6.37}$$

Exercise 3.6.5

Use induction to show that, for any integer $n \geq 1$:

$$\sum_{i=1}^{n} i \cdot i! = (n+1)!-1. \tag{3.6.38}$$

Exercise 3.6.6

Use induction to prove the following identity for integers $n \geq 1$:

$$\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)}=\frac{n}{2n+1}. \tag{3.6.39}$$

Exercise 3.6.7

Prove $2^{2n}-1$ is divisible by 3, for all integers $n \geq 0$.

Proof

Base Case: consider $n=0$. $2^{2(0)}-1=1-1=0$. 0 is divisible by 3 because 0 = 0(3).

Inductive Step: Assume this works for some integer, $k \geq 0$. In other words, $2^{2k}-1$ is divisible by 3. (Inductive Hypothesis)

Since $2^{2k}-1$ is divisible by 3, there exists some integer, m such that $2^{2k}-1=3m$, by definition of divides.

Consider the case of $n=k+1$. By algebra:

$$2^{2(k+1)}-1=2^{2k+2}-1=2^{2k}\cdot 2^2-1=2^{2k}\cdot 4-1=2^{2k}\cdot(3+1)-1=3\cdot 2^{2k}+2^{2k}-1 \tag{3.6.40}$$

$$=3\cdot 2^{2k}+3m \text{ by inductive hypothesis} \tag{3.6.41}$$

$$=3(2^{2k}+m) \text{ by algebra} \tag{3.6.42}$$

$2^{2(k+1)}-1=3(2^{2k}+m)$ and $(2^{2k}+m)\in\mathbb{Z}$ since the integers are closed under addition and multiplication.

So, $2^{2(k+1)}-1$ is divisible by 3 by the definition of divisible.

Thus assuming our proposition works for k it will also work for $k+1$.

By PMI, $2^{2n}-1$ is divisible by 3, for all integers $n\geq 0$.

W^5

Exercise 3.6.8

Evaluate $\sum_{i=1}^{n}\frac{1}{i(i+1)}$ for a few values of n. What do you think the result should be? Use induction to prove your conjecture.

Exercise 3.6.9

Use induction to prove that

$$\sum_{i=1}^{n}(2i-1)^3=n^2(2n^2-1) \tag{3.6.43}$$

whenever n is a positive integer.

Exercise 3.6.10

Use induction to show that, for any integer $n\geq 1$:

$$1^2-2^2+3^2-\cdots+(-1)^{n-1}n^2=(-1)^{n-1}\frac{n(n+1)}{2}. \tag{3.6.44}$$

Exercise 3.6.11

Use mathematical induction to show that

$$\sum_{i=1}^{n}\frac{i+4}{i(i+1)(i+2)}=\frac{n(3n+7)}{2(n+1)(n+2)} \tag{3.6.45}$$

for all integers $n\geq 1$.

Exercise 3.6.12

Use mathematical induction to show that

$$3+\sum_{i=1}^{n}(3+5i)=\frac{(n+1)(5n+6)}{2} \tag{3.6.46}$$

for all integers $n\geq 1$.

Answer

No answer here at this time.

3.7: The Well-Ordering Principle

Number theory studies the properties of integers. Some basic results in number theory rely on the existence of a certain number. The next theorem can be used to show that such a number exists.

The Well-Ordering Principle

Every nonempty subset of $\mathbb{N}$ has a smallest element.

Proof

In fact, we cannot prove the principle of well-ordering with just the familiar properties that the natural numbers satisfy under addition and multiplication. Hence, we shall regard the principle of well-ordering as an axiom. Interestingly though, it turns out that the principle of mathematical induction and the principle of well-ordering are logically equivalent. This means if you accept one as an axiom, you can use that to prove the other.

Theorem 3.7.2

The Principle of Mathematical Induction holds if and only if the Well-Ordering Principle holds.

Proof

($\Rightarrow$) Suppose S is a nonempty set of natural numbers that has no smallest element. Let

$$R = \{x \in \mathbb{N} \mid x \leq s \text{ for every } s \in S\}. \tag{3.7.1}$$

Since S does not have a smallest element, it is clear that $R \cap S = \emptyset$. It is also obvious that $1 \in R$. Assume $k \in R$. Then any natural number less than or equal to k must also be less than or equal to s for every $s \in S$. Hence $1, 2, \ldots, k \in R$. Because $R \cap S = \emptyset$, we find $1, 2, \ldots, k \notin S$. If $k+1 \in S$, then $k+1$ would have been the smallest element of S. This contradiction shows that $k+1 \in R$. Therefore, the principle of mathematical induction would have implied that $R = \mathbb{N}$. That would make S an empty set, which contradicts the assumption that S is nonempty. Therefore, any nonempty set of natural numbers must have a smallest element.

($\Leftarrow$) Let S be a set of natural numbers such that

$1 \in S$,

For any $k \geq 1$, if $k \in S$, then $k+1 \in S$.

Suppose $S \neq \mathbb{N}$. Then $\overline{S} = \mathbb{N} - S \neq \emptyset$. The principle of well-ordering states that $\overline{S}$ has a smallest element z. Since $1 \in S$, we deduce that $z \geq 2$, which makes $z-1 \geq 1$. The minimality of z implies that $z-1 \notin \overline{S}$. Hence, $z-1 \in S$. Condition (ii) implies that $z \in S$, which is a contradiction. Therefore, $S = \mathbb{N}$.

The principle of well-ordering is an existence theorem. It does not tell us which element is the smallest integer, nor does it tell us how to find the smallest element.

Example 3.7.1

Consider the sets

$$\begin{aligned} A &= \{n \in \mathbb{N} \mid n \text{ is a multiple of } 3\}, \\ B &= \{n \in \mathbb{N} \mid n = -11 + 7m \text{ for some } m \in \mathbb{Z}\}, \\ C &= \{n \in \mathbb{N} \mid n = x^2 - 8x + 12 \text{ for some } x \in \mathbb{Z}\}. \end{aligned}$$

It is easy to check that all three sets are nonempty, and since they contain only positive integers, the principle of well-ordering guarantees that each of them has a smallest element.

These smallest elements may not be easy to find. It is obvious that the smallest element in A is 3. To find the smallest element in B, we need $-11 + 7m > 0$, which means $m > 11/7 \approx 1.57$. Since m has to be an integer, we need $m \geq 2$. Since

$-11+7m$ is an increasing function in m, its smallest value occurs when $m=2$. The smallest element in B is $-11+7\cdot 2=3$.

To determine the smallest element in C, we need to solve the inequality $x^2-8x+12>0$. Factorization leads to $x^2-8x+12=(x-2)(x-6)>0$, so we need $x<2$ or $x>6$. Because $x\in\mathbb{Z}$, we determine that the minimum value of $x^2-8x+12$ occurs at $x=1$ or $x=7$. Since

$$1^2-8\cdot 1+12=7^2-8\cdot 7+12=5, \tag{3.7.2}$$

The smallest element in C is 5.

Example 3.7.2

The principle of well-ordering may not be true over real numbers or negative integers. In general, not every set of integers or real numbers must have a smallest element. Here are two examples:

The set $\mathbb{Z}$.

The open interval $(0,1)$.

The set $\mathbb{Z}$ has no smallest element because given any integer x, it is clear that $x-1<x$, and this argument can be repeated indefinitely. Hence, $\mathbb{Z}$ does not have a smallest element.

A similar problem occurs in the open interval $(0,1)$. If x lies between 0 and 1, then so is $\frac{x}{2}$, and $\frac{x}{2}$ lies between 0 and x, such that

$$0<x<1 \quad\Rightarrow\quad 0<\frac{x}{2}<x<1. \tag{3.7.3}$$

This process can be repeated indefinitely, yielding

$$0<\cdots<\frac{x}{2^n}<\cdots<\frac{x}{2^3}<\frac{x}{2^2}<\frac{x}{2}<x<1. \tag{3.7.4}$$

We keep getting smaller and smaller numbers. All of them are positive and less than 1. There is no end in sight, hence the interval $(0,1)$ does not have a smallest element.

The idea behind the principle of well-ordering can be extended to cover numbers other than positive integers.

Definition

A set T of real numbers is said to be ***well-ordered*** if every nonempty subset of T has a smallest element.

Therefore, according to the principle of well-ordering, $\mathbb{N}$ is well-ordered.

Example 3.7.3

Show that $\mathbb{Q}$ is not well-ordered.

Solution

Suppose x is the smallest element in $\mathbb{Q}$. Then $x-1$ is a rational number that is smaller than x, which contradicts the minimality of x. This shows that $\mathbb{Q}$ does not have a smallest element. Therefore $\mathbb{Q}$ is not well-ordered.

[eg:PWO-03]

hands-on exercise 3.7.1

Show that the interval $[0,1]$ is not well-ordered by finding a subset that does not have a smallest element

Summary and Review

- A set of real numbers is said to be well-ordered if every nonempty subset in it has a smallest element.
- A well-ordered set must be nonempty and have a smallest element.
- Having a smallest element does not guarantee that a set of real numbers is well-ordered.

- A well-ordered set can be finite or infinite, but a finite set is always well-ordered.

Exercises

Exercise 3.7.1

Find the smallest element in each of these subsets of $\mathbb{N}$.

a) $\{n \in \mathbb{N} \mid n = m^2 - 10m + 28 \text{ for some integer } m\}$.

b) $\{n \in \mathbb{N} \mid n = 5q + 3 \text{ for some integer } q\}$.

c) $\{n \in \mathbb{N} \mid n = -150 - 17d \text{ for some integer } d\}$.

d) $\{n \in \mathbb{N} \mid n = 4s + 9t \text{ for some integers } s \text{ and } t\}$.

Exercise 3.7.2

Determine which of the following subsets of $\mathbb{R}$ are well-ordered:

1. $\{\ \}$
2. $\{-9, -7, -3, 5, 11\}$
3. $\{0\} \cup \mathbb{Q}^+$
4. $2\mathbb{Z}$
5. $5\mathbb{N}$
6. $\{-6, -5, -4, \ldots\}$

Exercise 3.7.3

Show that the interval $[3, 5]$ is not well-ordered.

Hint

Find a subset of $[3, 5]$ that does not have a smallest element.

Exercise 3.7.4

Assume $\emptyset \neq T_1 \subseteq T_2 \subseteq \mathbb{R}$. Show that if T_2 is well-ordered, then T_1 is also well-ordered.

Hint

Let S be a nonempty subset of T_1. We want to show that S has a smallest element. To achieve this goal, note that $T_1 \subseteq T_2$.

Exercise 3.7.5

Prove that $2\mathbb{N}$ is well-ordered

Exercise 3.7.6

Assume $\emptyset \neq T_1 \subseteq T_2 \subseteq \mathbb{R}$. Prove that if T_1 does not have a smallest element, then T_2 is not well-ordered.

3.8: More on Mathematical Induction

Here are some more examples of mathematical induction.

Example 3.8.1

Prove that $n(n+1)(2n+1)$ is a multiple of 6 for all integers $n \geq 1$.

Remark

We have already seen how to prove this claim using a proof by cases, which is actually an easier way to prove that $n(n+1)(2n+1)$ is divisible by 6. Nonetheless, we shall demonstrate below how to use induction to prove the claim.

Discussion

In the inductive hypothesis, it is clear that we are assuming $k(k+1)(2k+1)$ is a multiple of 6. In the inductive step, we want to prove that

$$(k+1)(k+2)[2(k+1)+1] = (k+1)(k+2)(2k+3) \tag{3.8.1}$$

is also a multiple of 6. A multiple of 6 can be written as $6q$ for some integer q. Since we have two multiples of 6, we need to write

$$k(k+1)(2k+1) = 6q \tag{3.8.2}$$

and

$$(k+1)(k+2)(2k+3) = 6Q \tag{3.8.3}$$

to distinguish them. By using the lowercase and uppercase of the same letter, we indicate that they are different values. Yet, because they come from the same letter, they both share some common attribute, in this case, being the quotients when the respective values are divided by 6.

Now, in the inductive step, we need to make use of the equation $k(k+1)(2k+1) = 6q$ from the inductive hypothesis. This calls for connecting the product $(k+1)(k+2)(2k+3)$ to the expression $k(k+1)(2k+1)$. Since they share the common factor $k+1$, what remains to do is write $(k+2)(2k+3)$ in terms of $k(2k+1)$.

We are asked to prove that $n(n+1)(2n+1)$ is a multiple of 6. This is not an identity. Therefore, do not say "assume/show that the *identity* holds when … ." Instead, say "assume/show that the *claim* is true when … ."

Solution

Proceed by induction on n. When $n=1$, we have $n(n+1)(2n+1) = 1\cdot 2\cdot 3 = 6$, which is clearly a multiple of 6. Hence, the claim is true when $n=1$. Assume the claim is true when $n=k$ for some integer $k \geq 1$; that is, assume that we can write

$$k(k+1)(2k+1) = 6q \tag{3.8.4}$$

for some integer q. We want to show that the claim is still true when $n=k+1$; that is, we want to show that

$$(k+1)(k+2)[2(k+1)+1] = (k+1)(k+2)(2k+3) = 6Q \tag{3.8.5}$$

for some integer Q. Using the inductive hypothesis, we find

$$\begin{aligned}
(k+1)(k+2)(2k+3) &= (k+1)(2k^2+7k+6) \\
&= (k+1)[(2k^2+k)+(6k+6)] \\
&= (k+1)[k(2k+1)+6(k+1)] \\
&= k(k+1)(2k+1)+6(k+1)^2 \\
&= 6q+6(k+1)^2 \\
&= 6\,[q+(k+1)^2],
\end{aligned}$$

where $q+(k+1)^2$ is clearly an integer. This completes the induction.

hands-on exercise 3.8.1

Prove that n^2+3n+2 is even for all integers $n \geq 1$.

Induction can also be used to prove inequalities, which often require more work to finish.

Example 3.8.2

Prove that

$$1+\frac{1}{4}+\cdots+\frac{1}{n^2} \leq 2-\frac{1}{n} \tag{3.8.6}$$

for all positive integers n.

Draft. In the inductive hypothesis, we assume that the inequality holds when $n=k$ for some integer $k \geq 1$. This means we assume

$$\sum_{i=1}^{k} \frac{1}{i^2} \leq 2-\frac{1}{k}. \tag{3.8.7}$$

In the inductive step, we want to show that it also holds when $n=k+1$. In other words, we want to prove that

$$\sum_{i=1}^{k+1} \frac{1}{i^2} \leq 2-\frac{1}{k+1}. \tag{3.8.8}$$

In order to use the inductive hypothesis, we have to find a connection between these two inequalities. Obviously, we have

$$\sum_{i=1}^{k+1} \frac{1}{i^2} = \left(\sum_{i=1}^{k} \frac{1}{i^2}\right)+\frac{1}{(k+1)^2}. \tag{3.8.9}$$

Hence, it follows from the inductive hypothesis that

$$\sum_{i=1}^{k+1} \frac{1}{i^2} = \left(\sum_{i=1}^{k} \frac{1}{i^2}\right)+\frac{1}{(k+1)^2} \leq 2-\frac{1}{k}+\frac{1}{(k+1)^2}. \tag{3.8.10}$$

The proof would be complete if we could show that

$$2-\frac{1}{k}+\frac{1}{(k+1)^2} \leq 2-\frac{1}{k+1}. \tag{3.8.11}$$

There is no guarantee that this idea will work, but this should be the first thing we try.

After rearrangement, the inequality becomes

$$\frac{1}{k+1}+\frac{1}{(k+1)^2} \leq \frac{1}{k}, \tag{3.8.12}$$

which is equivalent to $\frac{k+2}{(k+1)^2} \leq \frac{1}{k}$. Cross-multiplication yields

$$k(k+2) \leq (k+1)^2. \tag{3.8.13}$$

Since

$$k(k+2)=k^2+2k, \qquad \text{and} \qquad (k+1)^2=k^2+2k+1, \tag{3.8.14}$$

it is clear that what we want to prove is indeed true.

Polish It Up! Next, we rearrange the argument to make it read more smoothly. Essentially all we need is to run the argument *backward*. To improve the flow of the argument, we can prove a separate result on the side before we return to the main argument.

Proof 1

Proceed by induction on n. When $n=1$, the left-hand side becomes 1, and so does the right-hand side; thus, the inequality holds. Assume it holds when $n=k$ for some integer $k \geq 1$:

$$\sum_{i=1}^{k} \frac{1}{i^2} \leq 2-\frac{1}{k}. \tag{3.8.15}$$

We want to show that it also holds when $n=k+1$:

$$\sum_{i=1}^{k+1} \frac{1}{i^2} \leq 2-\frac{1}{k+1}. \tag{3.8.16}$$

To finish the proof, we need to derive an inequality. Notice that

$$k(k+2)=k^2+2k<k^2+2k+1=(k+1)^2. \tag{3.8.17}$$

Hence, after dividing both sides by $k(k+1)^2$, we obtain

$$\frac{k+2}{(k+1)^2}<\frac{1}{k}. \tag{3.8.18}$$

This leads to

$$\frac{1}{k+1}+\frac{1}{(k+1)^2}=\frac{(k+1)+1}{(k+1)^2}=\frac{k+2}{(k+1)^2}<\frac{1}{k}, \tag{3.8.19}$$

which is equivalent to

$$-\frac{1}{k}+\frac{1}{(k+1)^2}<-\frac{1}{k+1}. \tag{3.8.20}$$

We now return to our original problem. It follows from the inductive hypothesis and ([eq:induct2-ineq]) that

$$\begin{aligned}\sum_{i=1}^{k+1} \frac{1}{i^2} &= \left(\sum_{i=1}^{k} \frac{1}{i^2}\right)+\frac{1}{(k+1)^2} \\ &\leq 2-\frac{1}{k}+\frac{1}{(k+1)^2} \\ &< 2-\frac{1}{k+1}.\end{aligned}$$

Therefore, the inequality still holds when $n=k+1$, which completes the induction.

Remark

The key step in the proof is to establish ([eq:induct2-ineq]), which can be done by means of contradiction.

Proof 2

Proceed by induction on n. When $n=1$, the left-hand side becomes 1, and so does the right-hand side; thus, the inequality holds. Assume it holds when $n=k$ for some integer $k \geq 1$:

$$\sum_{i=1}^{k} \frac{1}{i^2} \leq 2-\frac{1}{k}. \tag{3.8.21}$$

We want to show that it also holds when $n=k+1$:

$$\sum_{i=1}^{k+1} \frac{1}{i^2} \leq 2-\frac{1}{k+1}. \tag{3.8.22}$$

To finish the proof, we need the following inequality. We claim that

$$-\frac{1}{k}+\frac{1}{(k+1)^2}<-\frac{1}{k+1}. \tag{3.8.23}$$

Suppose, on the contrary, that

$$-\frac{1}{k}+\frac{1}{(k+1)^2}\geq -\frac{1}{k+1}. \tag{3.8.24}$$

Clear the denominators by multiplying $k(k+1)^2$ to both sides of the inequality. We find

$$-(k+1)^2+k\geq -k(k+1), \tag{3.8.25}$$

or equivalently,

$$-k^2-k-1\geq -k^2-k, \tag{3.8.26}$$

which is the same as saying $-1\geq 0$. This contradiction proves that ([eq:induct2-ineqalt]) must be true.

We now return to our original problem. It follows from the inductive hypothesis and ([eq:induct2-ineqalt]) that

$$\begin{aligned}\sum_{i=1}^{k+1}\frac{1}{i^2} &= \left(\sum_{i=1}^{k}\frac{1}{i^2}\right)+\frac{1}{(k+1)^2} \\ &\leq 2-\frac{1}{k}+\frac{1}{(k+1)^2} \\ &< 2-\frac{1}{k+1}.\end{aligned}$$

Therefore, the inequality still holds when $n=k+1$, which completes the induction.

hands-on exercise 3.8.2

Show that $n<2^n$ for all integers $n\geq 1$.

We do not have to start with $n=1$ in the basis step. We can start with any integer n_0.

Generalization. To show that $P(n)$ is true for all integers $n\geq n_0$, follow these steps:

a. Verify that $P(n_0)$ is true.
b. Assume that $P(k)$ is true for some integer $k\geq n_0$.
c. Show that $P(k+1)$ is also true.

The major difference is in the basis step: we need to verify that $P(n_0)$ is true. In addition, in the inductive hypothesis, we need to stress that $k\geq n_0$.

Example 3.8.3

Use mathematical induction to show that

$$\sum_{i=0}^{n}4^i=\frac{1}{3}(4^{n+1}-1) \tag{3.8.27}$$

for all integers $n\geq 0$.

Solution

Proceed by induction on n. When $n=0$, the left-hand side reduces to $\sum_{i=0}^{0}4^i=4^0=1$, and the right-hand side becomes $\frac{1}{3}(4^1-1)=\frac{1}{3}\cdot 3=1$. Hence, the formula holds when $n=0$. Assume it holds when $n=k$ for some integer $k\geq 0$; that is, assume

$$\sum_{i=0}^{k}4^i=\frac{1}{3}(4^{k+1}-1). \tag{3.8.28}$$

We want to show that it also holds when $n=k+1$; that is,

$$\sum_{i=0}^{k+1} 4^i = \frac{1}{3}(4^{k+2}-1). \tag{3.8.29}$$

Using the inductive hypothesis, we find

$$\begin{aligned} \sum_{i=0}^{k+1} 4^i &= \left(\sum_{i=0}^{k} 4^i\right) + 4^{k+1} \\ &= \tfrac{1}{3}\left(4^{k+1}-1\right) + 4^{k+1} \\ [3pt] &= \tfrac{1}{3}\left(4^{k+1}-1+3\cdot 4^{k+1}\right) \\ [3pt] &= \tfrac{1}{3}\left(4\cdot 4^{k+1}-1\right) \\ [3pt] &= \tfrac{1}{3}\left(4^{k+2}-1\right), \end{aligned}$$

which is what we want to prove, thereby completing the induction.

hands-on exercise 3.8.3

Prove that, for any integer $n \geq 0$,

$$1+\frac{2}{3}+\frac{4}{9}+\cdots+\left(\frac{2}{3}\right)^n = 3\left[1-\left(\frac{2}{3}\right)^{n+1}\right]. \tag{3.8.30}$$

Example 3.8.4

Use mathematical induction to show that

$$n^n \geq 2^n \tag{3.8.31}$$

for all integers $n \geq 2$.

Solution

Proceed by induction on n. When $n=2$, the inequality becomes $2^2 \geq 2^2$, which is obviously true. Assume it holds when $n=k$ for some integer $k \geq 2$:

$$k^k \geq 2^k. \tag{3.8.32}$$

We want to show that it still holds when $n=k+1$:

$$(k+1)^{k+1} \geq 2^{k+1}. \tag{3.8.33}$$

Since $k \geq 2$, it follows from the inductive hypothesis that

$$(k+1)^{k+1} \geq k^{k+1} = k \cdot k^k \geq 2 \cdot 2^k = 2^{k+1}. \tag{3.8.34}$$

Therefore, the inequality still holds when $n=k+1$. This completes the induction.

Summary and Review

- We can use induction to prove a general statement involving an integer n.
- The statement can be an identity, an inequality, or a claim about the property of an expression involving n.
- An induction proof need not start with $n=1$.
- If we want to prove that a statement is true for all integers $n \geq n_0$, we have to verify the statement for $n=n_0$ in the basis step.
- In addition, we need to assume that $k \geq n_0$ in the inductive hypothesis.

Exercises

Exercise 3.8.1

Use induction to prove that $n(n+1)(n+2)$ is a multiple of 3 for all integers $n \geq 1$.

Exercise 3.8.2

Use induction to show that n^3+5n is a multiple of 6 for any nonnegative integer n.

Exercise 3.8.3

Use induction to prove that

$$2+\left(1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}}\right)>2\sqrt{n+1} \tag{3.8.35}$$

for all integers $n\geq 1$.

Exercise 3.8.4

Use induction to prove that

$$2\left(1+\frac{1}{8}+\frac{1}{27}+\cdots+\frac{1}{n^3}\right)\leq 3-\frac{1}{n^2} \tag{3.8.36}$$

for all integers $n\geq 1$.

Exercise 3.8.5

Use induction to prove that

$$a+ar+ar^2+\cdots+ar^n=\frac{a(r^{n+1}-1)}{r-1} \tag{3.8.37}$$

for all nonnegative integers n, where a and r are real numbers with $r\neq 1$.

Exercise 3.8.6

Use induction to prove that, for any integer $n\geq 2$,

$$6\sum_{i=2}^{n} i(i+2)=2n^3+9n^2+7n-18. \tag{3.8.38}$$

Exercise 3.8.7

Use induction to prove that, for any integer $n\geq 0$,

$$1-\frac{2}{5}+\frac{4}{25}+\cdots+\left(-\frac{2}{5}\right)^n=\frac{5}{7}\left[1-\left(-\frac{2}{5}\right)^{n+1}\right]. \tag{3.8.39}$$

Exercise 3.8.8

Use induction to show that $n!>2^n$ for all integers $n\geq 4$.

Exercise 3.8.9

Use induction to prove that $n^2>4n+1$ for all integers $n\geq 5$.

Exercise 3.8.10

Prove that $2n+1<2^n$ for all integers $n\geq 3$.

Exercise 3.8.11

Define

$$S_n=\frac{1}{2!}+\frac{2}{3!}+\frac{3}{4!}+\cdots+\frac{n}{(n+1)!}. \tag{3.8.40}$$

a. Evaluate S_n for $n = 1, 2, 3, 4, 5$.
b. Propose a simple formula for S_n.
c. Use induction to prove your conjecture for all integers $n \geq 1$.

Exercise 3.8.12

Define $T_n = \sum_{i=0}^{n} \frac{1}{(2i+1)(2i+3)}$.

a. Evaluate T_n for $n = 0, 1, 2, 3, 4$.
b. Propose a simple formula for T_n.
c. Use induction to prove your conjecture for all integers $n \geq 0$.

CHAPTER OVERVIEW

4: Sets

Thumbnail: Overlapping sets. (CC BY-SA 3.0 Unported; Chris-martin via Wikipedia).

4.1: An Introduction to Sets

Introduction & Real Number Subsets

Note: Some information from section 1.5 is repeated here for a refresher; however, there is new material in this section as well and the exercises are different. (See the Table of Contents.)

A ***set*** is a collection of objects. The objects in a set are called its ***elements*** or ***members***. The elements in a set can be any types of objects, including sets! The members of a set do not even have to be of the same type. For example, although it may not have any meaningful application, a set can consist of numbers and names.

We usually use capital letters such as A, B, C, S, and T to represent sets, and denote their generic elements by their corresponding lowercase letters a, b, c, s, and t, respectively. To indicate that b is an element of the set B, we adopt the notation $b \in B$, which means " b belongs to B" or " b is an element of B.

We designate these notations for some special sets of numbers:

$$\begin{aligned} \mathbb{R} = & \text{the set of real numbers,} \\ \mathbb{Q} = & \text{the set of rational numbers,} \\ \mathbb{Z} = & \text{the set of integers,} \\ \mathbb{N} = & \text{the set of natural numbers (positive integers).} \end{aligned}$$

All these are infinite sets, because they all contain infinitely many elements. In contrast, finite sets contain finitely many elements.

Roster Notation

We can use the ***roster notation*** to describe a set if we can list all its elements explicitly, as in

$$A = \text{the set of natural numbers not exceeding } 7 = \{1,2,3,4,5,6,7\}. \tag{4.1.1}$$

For sets with more elements, show the first few entries to display a pattern, and use an ellipsis to indicate "and so on." For example,

$$\{1,2,3,\ldots,20\} \tag{4.1.2}$$

represents the set of the first 20 positive integers. The repeating pattern can be extended indefinitely, as in

$$\begin{aligned} \mathbb{N} = & \{1,2,3,\ldots\} \\ \mathbb{Z} = & \{\ldots,-2,-1,0,1,2,\ldots\} \end{aligned}.$$

The set of even integers can be described as $\{\ldots,-4,-2,0,2,4,\ldots\}$

Set-Builder Notation

We can use a ***set-builder notation*** to describe a set. For example, the set of natural numbers is defined as

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}. \tag{4.1.3}$$

Here, the vertical bar | is read as "such that" or "for which." Hence, the right-hand side of the equation is pronounced as "the set of x belonging to the set of integers such that $x > 0$," or simply "the set of integers x such that $x > 0$." In general, this descriptive method appears in the format

$$\{\,\text{membership} \mid \text{properties}\,\}. \tag{4.1.4}$$

The notation | means "such that" or "for which" only when it is used in the set notation. It may mean something else in a different context. Therefore, *do not* write "let x be a real number | $x^2 > 3$" if you want to say " let x be a real number such that $x^2 > 3$." It is considered improper to use a mathematical notation as an abbreviation.

Example 4.1.1

Write these two sets

$$\{x \in \mathbb{Z} \mid x^2 \leq 1\} \quad \text{and} \quad \{x \in \mathbb{N} \mid x^2 \leq 1\} \tag{4.1.5}$$

by listing their elements explicitly.

Answer

The first set has three elements, and equals $\{-1, 0, 1\}$. The second set is a singleton set; it is equal to $\{1\}$.

There is a slightly different format for the set-builder notation. Before the vertical bar, we describe the form the elements assume, and after the vertical bar, we indicate from where we are going to pick these elements:

$$\{\,\text{pattern} \mid \text{membership}\,\}. \tag{4.1.6}$$

Here the vertical bar $\mid$ means "where." For example,

$$\{x^2 \mid x \in \mathbb{Z}\} \tag{4.1.7}$$

is the set of x^2 where $x \in \mathbb{Z}$. It represents the set of squares: $\{0, 1, 4, 9, 16, 25, \ldots\}$

Example 4.1.2

The set

$$\{2n \mid n \in \mathbb{Z}\} \tag{4.1.8}$$

describes the set of even numbers. We can also write the set as $2\mathbb{Z}$.

Note

If the membership is not specified, such as: $\{x \mid x^2 \leq 5\}$ then it is understood that $\mathbb{R}$ is the default set that x belongs to.

Interval Notation

An interval is a set of real numbers, all of which lie between two real numbers. Should the endpoints be included or excluded depends on whether the interval is ***open***, ***closed***, or ***half-open***. We adopt the following ***interval notation*** to describe them:

$$\begin{aligned} (a,b) &= \{x \in \mathbb{R} \mid a < x < b\}, \\ [a,b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\}, \\ [a,b) &= \{x \in \mathbb{R} \mid a \leq x < b\}, \\ (a,b] &= \{x \in \mathbb{R} \mid a < x \leq b\}. \end{aligned} \tag{4.1.9}$$

It is understood that a must be less than b. Hence, the notation $(5, 3)$ does not make much sense. How about $[3, 3]$? This may be used in some texts to mean 3 but we will only use $a < b$ for intervals and use roster notation for a single number such as 3.

An interval contains not just integers, but all real numbers between the two endpoints. For instance, $(1, 5) \neq \{2, 3, 4\}$ because the interval $(1, 5)$ also includes real numbers such at 1.276, $\sqrt{2}$, and π.

We can use $\pm\infty$ in the interval notation:

$$\begin{aligned} (a, \infty) &= \quad \{x \in \mathbb{R} \mid a < x\}, \\ (-\infty, a) &= \quad \{x \in \mathbb{R} \mid x < a\}. \end{aligned}$$

However, we cannot write $(a, \infty]$ or $[-\infty, a)$, because $\pm\infty$ are *not* numbers. It is nonsense to say $x \leq \infty$ or $-\infty \leq x$. For the same reason, we can write $[a, \infty)$ and $(-\infty, a]$, but *not* $[a, \infty]$ or $[-\infty, a]$.

Example 4.1.3

Write the intervals $(2, 3)$, $[2, 3]$, and $(2, 3]$ in the descriptive form.

Solution

According to the definition of an interval, we find

$$\begin{aligned} (2,3) &= \quad \{x \in \mathbb{R} \mid 2 < x < 3\}, \\ [2,3] &= \quad \{x \in \mathbb{R} \mid 2 \leq x \leq 3\}, \\ (2,3] &= \quad \{x \in \mathbb{R} \mid 2 < x \leq 3\}. \end{aligned}$$

What would you say about $[2, 3)$?

Example 4.1.5

Be sure you are using the right types of numbers. Compare these two sets

$$\begin{aligned} S= &\quad \{x\in\mathbb{Z}\mid x^2\leq 5\}, \\ T= &\quad \{x\in\mathbb{R}\mid x^2\leq 5\}. \end{aligned}$$

One consists of integers only, while the other contains real numbers. Thus, $S=\{-2,-1,0,1,2\}$, and $T=\left[-\sqrt{5},\sqrt{5}\,\right]$.

Let S be a set of numbers; we define

$$\begin{aligned} S^+= &\quad \{x\in S\mid x>0\}, \\ S^-= &\quad \{x\in S\mid x<0\}, \\ S^*= &\quad \{x\in S\mid x\mathbb{N}eq 0\}. \end{aligned}$$

In plain English, S^+ is the subset of S containing only those elements that are positive, S^- contains only the negative elements of S, and S^* contains only the nonzero elements of S.

Example 4.1.6

It should be obvious that $\mathbb{N}=\mathbb{Z}^+$.

Some mathematicians also adopt these notations:

$$\begin{aligned} bS= &\quad \{bx\mid x\in S\}, \\ a+bS= &\quad \{a+bx\mid x\in S\}. \end{aligned}$$

Accordingly, we can write the set of even integers as $2\mathbb{Z}$, and the set of odd integers can be represented by $1+2\mathbb{Z}$.

Empty Set

An ***empty set*** is a set that does not contain any elements.

$$\{x\in\mathbb{R}\mid x>0 \text{ and } x<0\} \tag{4.1.10}$$

is an example of an empty set. We use an empty set as a convenient way of declaring that a problem has no solution: we say that the solution set is an empty set. We denote an empty set with the notation $\emptyset$ or $\{\,\}$. Notice we say "an" empty set. We will need to prove uniqueness in order to call it "the" empty set.

Example 4.1.7

Determine which of these statements are true.

$$\begin{aligned} \{x\in\mathbb{R}\mid (x^2+2)(x^2+3)=0\} &= \emptyset, \\ \{x\in\mathbb{Z}\mid (x^2-2)(x^2+3)=0\} &= \emptyset, \\ \{x\in\mathbb{R}\mid (x^2-2)(x^2+3)=0\} &= \emptyset, \\ \{x\in\mathbb{R}\mid (x^2-2)(x^2+3)\geq 0\} &= \emptyset. \end{aligned}$$

Solution

The answers are: true, true, false, and false, respectively.

Equality of Sets

Two sets A and B are said to be ***equal*** if they contain the same collection of elements. More rigorously, we define

$$A=B\Leftrightarrow\forall x\,(x\in A\Leftrightarrow x\in B). \tag{4.1.11}$$

Since the elements of a set can themselves be sets, exercise caution and use proper notation when you compare the contents of two sets.

Note: We will also use subsets for another definition for equality ofsets in the next section.

Example 4.1.9

Explain why $\{0,\{1\}\} \neq \{0,1\}$.

Solution

The set $\{0,\{1\}\}$ consists of two elements: the integer 0 and the set $\{1\}$. The set $\{0,1\}$ also consists of two elements, both of them integers; namely, 0 and 1.

You may find the following analogy helpful. Imagine a set being a box. You open a box to look at its contents. The box itself can be compared to the curly braces $\{$ and $\}$. What it holds is exactly what we call the elements of the set it represents. The contents of the two sets $\{0,\{1\}\}$ and $\{0,1\}$ are depicted in the boxes shown in the Figure below (well, not yet - the correct figure will be inserted at a later time - see if you can use your imagination for now).

(200,80) (0,0)(130,0)2 (0, 0)(0,50)2(1,0)50 (0, 0)(50, 0)2(0,1)50 (0,50)(50, 0)2(1,1)20 (20,70)(1,0)50 (50, 0)(1,1)20 (70,20)(0,1)50 (20,50)(0,1)20 (0, 0, 20,20) (20,20, 70,20) (20,20, 20,50) (15,30)(25, 0)2 (10,30)(10,15)0 (35,30)(10,15)1 (25,25) (0, 0)(0,20)2(1,0)20 (0, 0)(20, 0)2(0,1)20 (0,20)(20, 0)2(0,0, 8,8) (8,28)(1,0)20 (20, 0)(0,0, 8,8) (28, 8)(0,1)20 (8,20)(0,1) 8 (0, 0, 8, 8) (8, 8, 28, 8) (8, 8, 8,20)

When you open the first box, you find two items. One of them is the number 0; the other is another box that contains the number 1. The second box also contains two items that are both numbers. What you find in these two boxes is not the same. Hence, the sets they represent are different.

hands-on exercise 4.1.10

Name some differences between the sets $\{0,\{1\}\}$ and $\{\{0\},\{1\}\}$.

Example 4.1.10

True or false: $\mathbb{Z} = \{\{\ldots,-3,-2,-1\},0,\{1,2,3,\ldots\}\}$?

Solution

The set on the left is $\mathbb{Z}$, and

$$\mathbb{Z} = \{\ldots,-3,-2,-1,0,1,2,3,\ldots\}. \tag{4.1.12}$$

It is an infinite set. The set on the right consists of only three elements:

a. the set $\{\ldots,-3,-2,-1\}$, which is the set of negative integers,
b. the integer 0, and
c. the set $\{1,2,3,\ldots\}$ which is the set of positive integers.

Hence, they are not equal. Notice that

$$\mathbb{Z} \neq \{\{\ldots,-3,-2,-1\},\{0\},\{1,2,3,\ldots\}\} \tag{4.1.13}$$

either, because the set on the right is a set of three sets, while the set on the left is a set of integers. One has three elements; the other has infinitely many elements.

To reduce confusion, instead of saying a set of sets, we could say a ***collection of sets*** or a ***family of sets***. For example,

$$\{\{1,3,5,\ldots,\},\{2,4,6,\ldots\}\} \tag{4.1.14}$$

is a family of two sets, one of which is the set of positive odd integers; the other is the set of positive even integers.

Cardinality of Finite Sets

A set is said to be ***finite*** if it has a finite number of elements. The number of elements in a finite set A is called its ***cardinality***, and is denoted by $|A|$. Hence, $|A|$ is always nonnegative. If A is an infinite set, some authors would write $|A| = \infty$; however, we will use more specific designations for the cardinality of infinite sets. More will be revealed in the next chapter about the cardinality of infinite sets.

Example 4.1.11

While it is trivial that $|\{1,4,7,8\}| = 4$ and $|\{0,1\}| = 2$, it may not be obvious that

$$\big|\{0,\{1\}\}\big| = 2, \tag{4.1.15}$$

and

$$\big|\{\{\ldots,-3,-2,-1\},0,\{1,2,3,\ldots\}\}\big| = 3. \tag{4.1.16}$$

What matters is the number of entries in a set, which can be compared to how many items you can find when you open a box. Here is another example:

$$|\{x\in\mathbb{R} \mid x^2 = 9\}| = 2 \tag{4.1.17}$$

because the equation $x^2 = 9$ has two real solutions. What is $|\{x\in\mathbb{N} \mid x^2 = 9\}|$?

hands-on exercise 4.1.11

Determine these cardinalities:

a. $|\{x\in\mathbb{Z} \mid x^2 - 7x - 6 = 0\}|$
b. $|\{x\in\mathbb{R} \mid x^2 - x - 12 < 0\}|$
c. $|\{x\in\mathbb{Z} \mid x \text{ is prime and } x \text{ is even}\}|$

Recall that your answers should be nonnegative.

hands-on exercise 4.1.12

Explain why it is incorrect to say $|\emptyset| = \emptyset$. In fact, it is nonsense to say $|\emptyset| = \emptyset$. Explain. What should be the value of $|\emptyset|$?

We close this section with an important remark about sets. It follows from the definition of equality of sets that we do not count repeated elements as separate elements. For example, suppose a small student club has three officers:

chair:	Mary,
vice chair:	John,
secretary:	John;

and let A represent the set of its officers, and B the set of positions in its executive board, then $|A| = 2$ and $|B| = 3$, because

$$A = \{\text{Mary}, \text{John}\}, \tag{4.1.18}$$

and

$$B = \{\text{chair}, \text{vice chair}, \text{secretary}\}. \tag{4.1.19}$$

Example 4.1.12

Find the errors in the following statement:

$$|\{-2,2\}| = \{\,|-2|,|2|\} = \{2\} = 2, \tag{4.1.20}$$

and correct them.

Solution

This statement contains several errors. The first mistake is assuming that we can distribute the "absolute value" symbols $|\quad|$ over the contents of a set:

$$|\{-2,2\}| \mathbb{N}eq \{\,|-2|,|2|\}. \tag{4.1.21}$$

After all, the two vertical bars do not mean absolute value in this case. Instead, it means the cardinality of the set $\{-2,2\}$. Hence, $|\{-2,2\}|=2$.

The second equality $\{|-2|,|2|\}=\{2\}$ is correct. After taking absolute values, both entries become 2. However, we do not write $\{|-2|,|2|\}=\{2,2\}$ because a set should not contain repetition. Therefore, it is correct to say $\{|-2|,|2|\}=\{2\}$.

The last equality $\{2\}=2$ is wrong. We cannot compare a set to a number. Imagine the set $\{2\}$ as a box containing only one object, and that object is the number 2. In contrast, 2 on the right-hand side is left in the open air without any containment. It is clear that $\{2\}\neq 2$.

The entire statement contains multiple mistakes; some of them are syntactical errors while some are conceptual. Nevertheless, we do have $|\{-2,2\}|=2$. Although the final answer is correct, the argument used to obtain it is not.

In some situations, we do want to count repeated elements as separate elements, as in $S=\{1,2,2,2,3,3,4,4\}$. We call such a collection a ***multiset*** instead of an ordinary set. In this case, $|S|=8$.

Summary and Review

- A set is a collection of objects (without repetitions).
- To describe a set, either list all its elements explicitly, or use a descriptive method.
- Intervals are sets of real numbers.
- The elements in a set can be any type of object, including sets.
- We can even have a set containing dissimilar elements. In particular, we can mix elements and sets inside a set.
- An empty set is a set with no elements.
- If a set A is finite, its cardinality $|A|$ is the number of elements it contains. Consequently, $|A|$ is always nonnegative.

Exercises

Exercise 4.1.1

Write each of these sets by listing its elements explicitly (that is, using the roster method).

(a) $\{n\in\mathbb{Z}\mid -6<n<4\}$
(b) $\{n\in\mathbb{N}\mid -6<n<4\}$
(c) $\{x\in\mathbb{Q}\mid x^3-x^2-6x=0\}$
(d) $\{x\in\mathbb{Q}\mid x^4-11x^2+18=0\}$.

Solution

(a) $\{-5,-4,-3,-2,-1,0,1,2,3\}$(b) $\{1,2,3\}$(c) $\{0,-2,3\}$(d) $\{-3,3\}$

Exercise 4.1.3

Write each of the following sets in the form $\{n\in\mathbb{Z}\mid p(n)\}$ with a logical statement $p(n)$ describing the property of n.

(a) $\{\ldots,-3,-2,-1\}$
(b) $\{\ldots,-27,-8,-1,0,1,8,27,\ldots\}$
(c) $\{0,1,4,9,16,\ldots\}$

Solution

(a) $\{n\in\mathbb{Z}\mid n<0\}$

(b) $\{n\in\mathbb{Z}\mid n \text{ is a perfect cube}\}$

(c) $\{n\in\mathbb{Z}\mid n \text{ is a perfect square}\}$

Exercise 4.1.5

Whenever possible, express these sets in the form S^+, S^-, bS, or $a+bS$ for some appropriate set S.
(a) $\{\ldots,-3,-2,-1\}$
(b) $\{\ldots,-27,-8,-1,0,1,8,27,\ldots\}$

(c) $\{0,1,4,9,16,\ldots\}$
(d) $\{\ldots,-15,-10,-5,0,5,10,15,\ldots\}$
(e) $\{0,4,8,12,\ldots\}$
(f) $\{\ldots,-14,-8,-2,4,10,16,\ldots\}$

Solution

(a) $\mathbb{Z}^{-}$ (d) $5\mathbb{Z}$ (f) $4+6\mathbb{Z}$

Remark. We cannot write (b) as $\mathbb{Z}^3$ and (c) as $\mathbb{Z}^2$, because $\mathbb{Z}^3$ and $\mathbb{Z}^2$ mean something else. If we drop 0 from (e), then $\{4,8,12,\ldots\}=4\mathbb{N}$ However, the inclusion of 0 makes it harder to describe (d) in the form of $4S$.

Exercise 4.1.6

Determine whether the following sets are empty, finite sets, or infinite sets:

a. $\{2n+1 \mid n \in \mathbb{N}\}$
b. $\{x \in \mathbb{R} \mid x^2<0\}$
c. $\{x \in \mathbb{Q} \mid x \geq 0 \text{ and } x \leq 0\}$
d. $\{x \in \mathbb{N} \mid x<0 \text{ or } x>0\}$

Exercise 4.1.7

Write each of these sets in the interval notation.

(a) $\{x \in \mathbb{R} \mid -4<x<7\}$
(b) $\{x \in \mathbb{R} \mid -4<x \leq 7\}$
(c) $\{x \in \mathbb{R}^{+} \mid -4<x \leq 7\}$

Solution

(a) $(-4,7)$ (b) $(-4,7]$ (c) $(0,7]$

Exercise 4.1.8

Is $[-\infty, \infty]$ a legitimate or correct notation? Explain.

Exercise 4.1.9

Determine which of the following statements are true, and which are false.

(a) $a \in \{a\}$
(b) $\{3,5\}=\{5,3\}$
(c) $\emptyset \in \emptyset$
(d) $\emptyset=\{\emptyset\}$
(e)$\{\ \}=\emptyset$
(f) $\emptyset \in \{\emptyset\}$

Solution

(a) true (b) true (c) false (d) false (e) true (f) true

Exercise 4.1.10

Evaluate the following expressions.

(a) $|\{x \in \mathbb{Z} \mid -4<x<7\}|$
(b) $|\{x \in \mathbb{Z} \mid -4<x \leq 7\}|$
(c)$|\{x \in \mathbb{N} \mid -4<x \leq 7\}|$

(d) $|\{x \in \mathbb{R} \mid x^4 - 2x^3 - 35x^2 = 0\}|$
(e)$|\{-3, -2, 2, 3\}|$
(f) $|\{x \in \mathbb{Q} \mid x^2 = 3\}|$

Exercise 4.1.11

Determine which of the following statements are true, and which are false.

(a) $2 \in (2, 7)$
(b) $\sqrt{2} \in (1, 3)$
(c) $\left(\sqrt{5}\right)^2 \in \mathbb{Q}$
(d) $-5 \in \mathbb{N}$

Solution

(a) false (b) true (c) true (d) false

Exercise 4.1.12

Give examples of sets A, B and C such that:

a. $A \in B$ and $B \in C$, and $A \notin C$
b. $A \in B$ and $B \in C$, and $A \in C$

Exercise 4.1.13

Determine whether the following statements are correct or incorrect *syntactically*. For those that are syntactically correct, determine their truth values; for those that are syntactically incorrect, suggest ways to fix them.

(a) $(3, 7\,] = 3 < x \leq 7$.
(b) $\{x \in \mathbb{R} \mid x^2 < 0\} \equiv \emptyset$.

Solution

(a) It is incorrect to write (3,7]=3<x≤7 because (3,7] is a set, but 3<x≤7 is a logical statement.
(b) No, because both {x∈R∣x2<0} and ∅ are sets, so we should use an equal sign to compare them. The notation ≡ only applies to logical statements. The correct way to say it is "{x∈R∣x2<0}=∅."

Exercise 4.1.14

Determine whether the following statements are correct or incorrect *syntactically*. For those that are syntactically correct, determine their truth values; for those that are syntactically incorrect, suggest ways to fix them.

a. $\frac{7}{4} \in [2, \sqrt{7})$.
b. There does not exist x such that $x \in \mathbb{R}^+$ and $\mathbb{R}^-$.
c. If $(0, \infty)$, then x is positive.

4.2: Subsets and Power Sets

We usually consider sets containing elements of similar types. The collection of all the objects under consideration is called the ***universal set***, and is denoted $\mathcal{U}$. For example, for numbers, the default universal set is $\mathbb{R}$.

Venn Diagrams

Example 4.2.1

Venn diagrams are useful in demonstrating set relationship. Let

$$\begin{aligned} \mathcal{U} &= && \text{set of geometric figures,} \\ S &= && \text{set of squares,} \\ P &= && \text{set of parallelogram,} \\ R &= && \text{set of rhombuses,} \\ L &= && \text{set of rectangles,} \\ C &= && \text{set of circles.} \end{aligned}$$

Their relationship is displayed in the figure below.

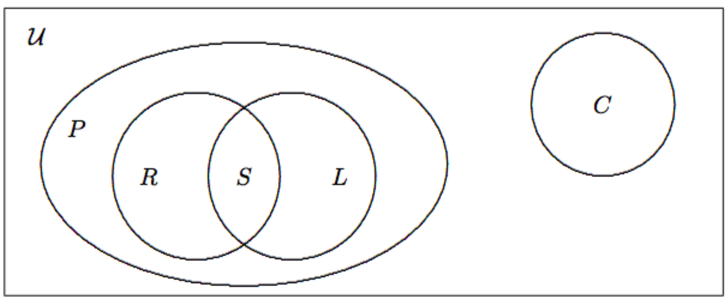


Figure 4.2.1: The relationship among various sets of geometric figures.

The pictorial representation in the figure above is called a ***Venn diagram***. We use a rectangle to represent the universal set, and circles or ovals to represent the sets inside the universal set. The relative positions of these circles and ovals indicate the relationship of the respective sets. For example, having R, S, and L inside P means that rhombuses, squares, and rectangles are parallelograms. In contrast, circles are incomparable to parallelograms.

Definition: Subset

Set A is a subset of set B, denoted by $A \subseteq B$, if every element of A is also an element of B. See Figure (figure not here yet).

Symbolicly:

$A \subseteq B$ if and only if $x \in A \to x \in B$.

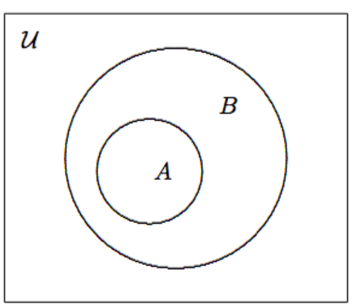


Figure 4.2.2: The Venn diagram for $A \subseteq B$.

In some texts, you may see this notation: B is a ***superset*** of A, and write $B \supseteq A$, which is similar to $y \geq x$.

Example 4.2.2

It is clear that $\mathbb{N} \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq \mathbb{R}$. We can nest these two relationships into one, and write $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R}$. More generally, we have

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}. \tag{4.2.1}$$

Compare this to $x \leq y \leq z \leq w$. We shall discover many similarities between $\subseteq$ and $\leq$.

Example 4.2.3

It is obvious that

$$\{1,2,7\} \subseteq \{1,2,3,6,7,9\} \tag{4.2.2}$$

because all three elements 1, 2, and 7 from the set on the left also appear as elements in the set on the right. Meanwhile,

$$\{1,2,7\} \not\subseteq \{1,2,3,6,8,9\} \tag{4.2.3}$$

because 7 belongs to the first set but not the second.

Example 4.2.4

The following statements are true:

- $\{1,2,3\} \subseteq \mathbb{N}$.
- $\{x \in \mathbb{R} \mid x^2 = 1\} \subseteq \mathbb{Z}$.

Be sure you can explain clearly why these subset relationships hold.

hands-on exercise 4.2.1

Are these statements true or false?

- $\{-1,2\} \not\subseteq \mathbb{N}$, and $\{-1,2\} \subseteq \mathbb{Z}$.
- $\{x \in \mathbb{Z} \mid x^2 \leq 1\} \subseteq \mathbb{R}$.

Example 4.2.5

Do not assume that if $A \not\subseteq B$ then we must have $B \subseteq A$. For instance, if $A = \{1,5,7\}$ and $B = \{3,8\}$, then $A \not\subseteq B$; but we also have $B \not\subseteq A$.

The last example demonstrates that $A \not\subseteq B$ is more complicated than just changing the subset notation as we do with inequalities. We need a more precise definition of the subset relationship:

$$A \subseteq B \Leftrightarrow \forall x \in \mathcal{U}\,(x \in A \Rightarrow x \in B) \tag{4.2.4}$$

It follows that

$$A \not\subseteq B \Leftrightarrow \exists x \in \mathcal{U}\,(x \in A \wedge x \notin B).$$

Hence, to show that A is not a subset of B, we need to find an element x that belongs to A but not B. There are three possibilities; their Venn diagrams are depicted in Figure $4.2.3$.

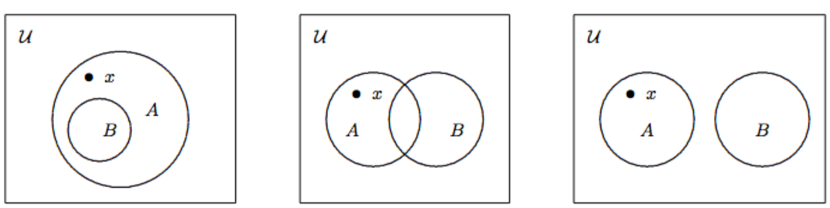


Figure $4.2.3$: Three cases of $A \not\subseteq B$.

Example 4.2.6

We have $[3,6] \subseteq [2,7)$, and $[3,6] \not\subseteq [4,7)$. We also have $(3,4) \subseteq [3,4]$.

hands-on exercise 4.2.2

True or false: $[3,4) \subseteq (3,4)$? Explain.

To prove $S \subseteq T$

To prove a set is a subset of another set, follow these steps.

(1) Let x be an arbitrary element of set S.

(2) Show x is an element of set T.

This proves every element of set S is an element of T.

Example:

Prove $\mathbb{Z} \subseteq \mathbb{Q}$.

Let $x \in \mathbb{Z}$.

$x = \frac{x}{1}$.

See if you can continue this proof.

Continuation of Proof

Since $x \in \mathbb{Z}$ and $1 \in \mathbb{Z}$ and $1 \neq 0$,
$\frac{x}{1} \in \mathbb{Q}$, by definition of rational numbers.

Thus $x \in \mathbb{Q}$, by substitution.

$\therefore \mathbb{Z} \subseteq \mathbb{Q}$.

With the notion of universal set, we can now refine the definition for set equality; here's our original definition:

$$A = B \Leftrightarrow \forall x \in \mathcal{U}\,(x \in A \Leftrightarrow x \in B) \tag{4.2.5}$$

Logically, $x \in A \Leftrightarrow x \in B$ is equivalent to

$$(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A). \tag{4.2.6}$$

Therefore, we can also define the equality of sets via subset relationship:

Equality of Sets: Subset Definition

$$A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A) \tag{4.2.7}$$

which can be compared to

$$x = y \Leftrightarrow (x \leq y) \wedge (y \leq x) \tag{4.2.8}$$

for real numbers x and y.

This new definition of set equality suggests that in order to prove that $A = B$, we could use this two-step argument.

To Prove Sets Equal

(1) Show that $A \subseteq B$.

(2) Show that $B \subseteq A$.

.

This technique is useful when it is impossible or impractical to list the elements of A and B for comparison. This is particularly true when A and B are defined abstractly. We will apply this technique in the coming sections.

The two relationship $\subseteq$ and $\leq$ share many common properties. The ***transitive property*** is another example.

Theorem $4.2.1$ Transitivity of Subsets

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

Discussion

The theorem statement is in the form of an implication. To prove $p \Rightarrow q$, we start with the assumption p, and use it to show that q must also be true. In this case, these two steps become

- Assume that $A \subseteq B$ and $B \subseteq C$.
- Show that $A \subseteq C$.

How can we prove that $A \subseteq C$? We know that $A \subseteq C$ means

$$\forall x \in \mathcal{U}\,(x \in A \Rightarrow x \in C). \tag{4.2.9}$$

So we have to start with $x \in A$, and attempt to show that $x \in C$ as well. How can we show that $x \in C$? We need to use the assumption $A \subseteq B$ and $B \subseteq C$.

Proof

Assume $A \subseteq B$ and $B \subseteq C$.
Let $x \in A$. Since $A \subseteq B$, $x \in B$ by definition of subset.
Likewise, since $B \subseteq C$, $x \in C$, by definition of subset.
Thus $\forall x \in \mathcal{U}\,(x \in A \Rightarrow x \in C)$.
So we conclude that $A \subseteq C$ by definition of subset.

$\therefore$ if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

The proof relies on the definition of the subset relationship. Many proofs in mathematics are rather simple if you know the underlying definitions.

Example $4.2.7$ A Biconditional Proof

Prove that $x \in A \Leftrightarrow \{x\} \subseteq A$, for any element $x \in \mathcal{U}$

Discussion

We call $p \Leftrightarrow q$ a biconditional statement because it consists of two implications $p \Rightarrow q$ and $p \Leftarrow q$. Hence, we need to prove it in two steps:

- Show that $p \Rightarrow q$.
- Show that $q \Rightarrow p$.

We call these two implications the ***necessity*** and ***sufficiency*** of the biconditional statement, and denote them $(\Rightarrow)$ and $(\Leftarrow)$, respectively. In this problem,

- $(\Rightarrow)$ means "$x \in A \Rightarrow \{x\} \subseteq A$".
- $(\Leftarrow)$ means "$\{x\} \subseteq A \Rightarrow x \in A$".

This is a sketch of how the proof may look:

$(\Rightarrow)$ Assume $x \in A$. ... Therefore $\{x\} \subseteq A$.

$(\Leftarrow)$ Assume $\{x\} \subseteq A$. ... Therefore $x \in A$.

We now proceed to finish the proof.

Answer

(⇒) Assume $x \in A$. The set $\{x\}$ contains only one element x, which is also an element of A. Thus, every element of $\{x\}$ is also an element of A. By definition of subset, $\{x\} \subseteq A$.

(⇐) Assume $\{x\} \subseteq A$. The definition of the subset asserts that every element of $\{x\}$ is also an element of A. In particular, x is an element of $\{x\}$, so by definition of subset, it is also an element of A. Thus, $x \in A$.

Definition - Proper subset

The set A is a ***proper subset*** of B, denoted $A \subset B$, if A is a subset of B, and $A \neq B$. Symbolically, $A \subset B \Leftrightarrow (A \subseteq B) \wedge (A \neq B)$. Equivalently,

$$A \subset B \Leftrightarrow (A \subseteq B) \wedge \exists x \in \mathcal{U}\,(x \in B \wedge x \notin A). \tag{4.2.10}$$

See the Venn diagram in Figure $4.2.4$.

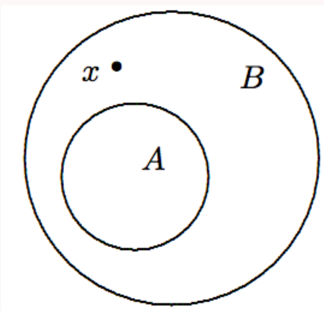


Figure $4.2.4$: The definition of a proper subset.

Example $4.2.8$

It is clear that $[0,5] \subset \mathbb{R}$. We also have

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}. \tag{4.2.11}$$

Note the similarities between $\subset$ and $<$. Compare the last expression to

$$x < y < z < w. \tag{4.2.12}$$

Here is another similarity between $\subset$ and $<$. For numbers, $x<y$ and $y<z$ together imply that $x<z$. This is the transitive property. In a similar fashion, for sets, if $A \subset B$ and $B \subset C$, then $A \subset C$; the transitive property holds for proper subsets.

hands-on exercise $4.2.3$

True or false: $(3,4) \subset [3,4]$? How about $(3,4) \subset (3,4]$?

Empty Set Theorems

Theorem $4.2.2$ $\emptyset$ is a Subset of Every Set

For any set A, we have $\emptyset \subseteq A$ and $A \subseteq A$. In particular, $\emptyset \subseteq \emptyset$.

Proof

Since every element of A also appears in A, it follows immediately that $A \subseteq A$. To show that $\emptyset \subseteq A$, we need to verify the implication

$$x \in \emptyset \Rightarrow x \in A \tag{4.2.13}$$

for any arbitrary $x \in \mathcal{U}$. Since $\emptyset$ is empty, $x \in \emptyset$ is always false; hence, the implication is always true. Consequently, $\emptyset \subseteq A$ for any set A. In particular, when $A = \emptyset$, we obtain $\emptyset \subseteq \emptyset$.

Theorem $\mathbf{4.2.3}$ The $\emptyset$ is Unique

An empty set is defined as a set with no elements. We want to show there is just one empty set; only one set that has no elements. Then we can refer to it as "the" empty set.

Proof

Suppose E_1 and E_2 are empty sets, that is, they each have no elements. From Theorem 4.2.2, since E_1 has no elements, $E_1 \subseteq E_2$. By the same reasoning, $E_2 \subseteq E_1$. Now from the definition of equality, $E_2 = E_1$. Thus there is just one empty set.

Example 4.2.9

Determine the truth values of these expressions.

(a) $\emptyset \in \emptyset$ & (b) $1 \subseteq \{1\}$ & (c) $\emptyset \in \{\emptyset\}$

Answer

(a) By definition, an empty set contains no element. Consequently, the statement $\emptyset \in \emptyset$ is false.

(b) A subset relation only exists between two sets. To the left of the symbol $\subseteq$, we have only a number, which is not a set. Hence, the statement is false. In fact, this expression is syntactically incorrect.

(c) The set $\{\emptyset\}$ contains one element, which happens to be an empty set. Compare this to an empty box inside another box. The outer box is described by the pair of set brackets $\{\ldots\}$, and the (empty) box inside is $\emptyset$. It follows that $\emptyset \in \{\emptyset\}$ is a true statement.

hands-on exercise 4.2.4

Determine the truth values of these expressions.

(a) $\emptyset \subseteq \{\emptyset\}$ & (b) $\{1\} \subseteq \{1, \{1,2\}\}$ & (c) $\{1\} \subseteq \{\{1\}, \{1,2\}\}$

Definition-Power Set

The set of all subsets of A is called the ***power set*** of A, denoted $\mathscr{P}(A)$.

Since a power set itself is a set, we need to use a pair of left and right curly braces (set brackets) to enclose all its elements. Its elements are themselves sets, each of which requires its own pair of left and right curly braces. Consequently, we need at least two levels of set brackets to describe a power set.

Example $\mathbf{4.2.10}$ Examples of Power Sets

Let $A = \{1,2\}$ and $B = \{1\}$. The subsets of A are $\emptyset$, $\{1\}$, $\{2\}$ and $\{1,2\}$. Therefore,

$$\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}. \tag{4.2.14}$$

In a similar manner, we find

$$\mathscr{P}(B) = \{\emptyset, \{1\}\}. \tag{4.2.15}$$

We can write directly

$$\mathscr{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}, \qquad \text{and} \qquad \mathscr{P}(\{1\}) = \{\emptyset, \{1\}\} \tag{4.2.16}$$

without introducing letters to represent the sets involved.

hands-on exercise 4.2.5

Let us evaluate $\mathscr{P}(\{1,2,3,4\})$. To ensure that no subset is missed, we list these subsets according to their sizes. Since $\emptyset$ is the subset of any set, $\emptyset$ is always an element in the power set. This is the subset of size 0. Next, list the singleton subsets (subsets with only one element). Then the doubleton subsets, and so forth. Complete the following table.

size	subsets
0	$\emptyset$
1	$\{1\},\{2\},\ldots$
2	$\{1,2\},\{1,3\},\ldots$
3	$\{1,2,3\},\ldots$
4	$\ldots$

(4.2.17)

Since $A \subseteq A$ for any set A, the power set $\mathscr{P}(A)$ always contains A itself. As a result, the last subset in the list should be A itself.

We are now ready to put them together to form the power set. All you need is to put all the subsets inside a pair of bigger curly braces (a power set is itself a set; hence, it needs a pair of curly braces in its description). Put your final answer in the space below.

Check to make sure that the left and right braces match perfectly.

Example 4.2.11

Since A is a subset of A, it belongs to $\mathscr{P}(A)$. Nonetheless, it is improper to say $A \subseteq \mathscr{P}(A)$. Can you explain why? What should be the correct notation?

Answer

The power set $\mathscr{P}(A)$ is the collection of all the subsets of A. Thus, the elements in $\mathscr{P}(A)$ are subsets of A. One of these subsets is the set A itself. Hence, A itself appears as an *element* in $\wp(A)$, and we write $A \in \wp(A)$ to describe this *membership*.

This is different from saying that $A \subseteq \mathscr{P}(A)$. In order to have the *subset* relationship $A \subseteq \mathscr{P}(A)$, every element in A must also appear as an element in $\mathscr{P}(A)$. The elements of $\mathscr{P}(A)$ are sets (they are subsets of A, and subsets are sets). An element of A is not the same as a subset of A. Therefore, although $A \subseteq \mathscr{P}(A)$ is syntactically correct, its truth value is false.

hands-on exercise 4.2.6

Explain the difference between $\emptyset$ and $\{\emptyset\}$. How many elements are there in $\emptyset$ and $\{\emptyset\}$? Is it true that $\mathscr{P}(\emptyset)=\{\emptyset\}$?

Theorem 4.2.3 2^n subsets for a set with n elements.

If A is an n-element set, then $\mathscr{P}(A)$ has 2^n elements. In other words, an n-element set has 2^n distinct subsets.

Proof

How many subsets of A can we construct? To form a subset, we go through each of the n elements and ask ourselves if we want to include this particular element or not. Since there are two choices (yes or no) for each of the n elements in A, we have found $\underbrace{2\cdot 2\cdots 2}_{\text{n times}}=2^n$ subsets.

hands-on exercise 4.2.7

How many elements are there in $\mathscr{P}(\{\alpha,\beta,\gamma\})$? What are they?

hands-on exercise 4.2.8

What is the cardinality of $\emptyset$? How about $\mathscr{P}(\emptyset)$? Describe $\mathscr{P}(\emptyset)$.

hands-on exercise 4.2.9

Is it correct to write $|\mathscr{P}(A)| = 2^{|A|}$? How about $|\mathscr{P}(A)| = 2^A$? Explain.

Example $\mathbf{4.2.12}$ Complicated Power Sets

When a set contains sets as elements, its power set could become rather complicated. Here are two examples.

$$\begin{aligned} \mathscr{P}(\{\{a\},\{1\}\}) &= \Big\{\emptyset,\{\{a\}\},\{\{1\}\},\{\{a\},\{1\}\}\Big\}, \\ \mathscr{P}(\{\emptyset,\{1\}\}) &= \Big\{\emptyset,\{\emptyset\},\{\{1\}\},\{\emptyset,\{1\}\}\Big\}. \end{aligned}$$

Be sure you understand the notations used in these examples. In particular, examine the number of levels of set brackets used in each example.

Summary and Review

- A set S is a subset of another set T if and only if every element in S can be found in T.
- In symbols, $S \subseteq T \Leftrightarrow \forall x \in \mathcal{U}\,(x \in S \Rightarrow x \in T)$.
- Consequently, to show that $S \subseteq T$, we have to start with an arbitrary element x in S, and show that x also belongs to T.
- For sets S and T, $S = T \Leftrightarrow (S \subseteq T) \wedge (T \subseteq S)$.
- The definition of subset relationship implies that for any set S, we always have $\emptyset \subseteq S$ and $S \subseteq S$.
- The empty set is unique.
- The power set of a set S, denoted $\wp(S)$, contains all the subsets of S.
- If $|S| = n$, then $|\mathscr{P}(S)| = 2^n$. Hence, an n-element set has 2^n subsets.
- To construct $\mathscr{P}(S)$, list the subsets of S according to their sizes. Be sure to use a pair of curly braces for each subset, and enclose all of them within a pair of outer curly braces.

Exercises

Exercise 4.2.1

Determine which of the following statements are true and which are false.

- (a) $\{1,2,3\} \subseteq \{0,1,2,3,4\}$
- (b) $\{1,2,3\} \subseteq \mathbb{N}$
- (c) $\{1,2\} \subset [1,2]$
- (d) $[2,4] \subseteq (0,6)$
- (e) $[2,4) \subset [2,4]$
- (f) $[2,4) \subseteq (2,4]$

Answer

All are true except (f) is false.

Exercise 4.2.2

Determine which of the following statements are true and which are false.

- (a) $a \subseteq \{a\}$
- (b) $\{a\} \subseteq \{a,b\}$
- (c) $\emptyset \subseteq \emptyset$
- (d) $\emptyset \subseteq \{\emptyset\}$
- (e) $\emptyset \subset \{\emptyset\}$
- (f) $\{a\} \subseteq \mathscr{P}(\{\{a\},\{b\}\})$

Exercise 4.2.3

True or false: $5\mathbb{N} \subseteq \mathbb{N}$? Explain.

Answer

True. $5\mathbb{N}$ contains all the integers that are multiples of 5, and each of these is an integer.

Exercise 4.2.4

True or false: $\mathbb{N} \subseteq 6\mathbb{N}$? Explain.

Exercise 4.2.5

Determine which of the following statements are true, and which are false. Explain!

- (a) $\{a\} \in \{a, b, c\}$
- (b) $\{a\} \subseteq \{\{a\}, b, c\}$
- (c) $\{a\} \in \mathscr{P}(\{\{a\}, b, c\})$

Answer

(a) False, because the set $\{a\}$ cannot be found in $\{a, b, c\}$as an element.

(b) False, because a, the sole element in $\{a\}$, cannot be found in $\{\{a\}, b, c\}$as an element.

(c) False. For $\{a\} \in \mathscr{P}(\{\{a\}, b, c\})$ the set $\{a\}$ must be a subset of $\{\{a\}, b, c\}$ This means a must belong to $\{\{a\}, b, c\}$ which is not true.

Exercise 4.2.6

Determine whether the following statements are true or false:

- (a) The empty set $\emptyset$ is a subset of $\{1, 2, 3\}$.
- (b) If $A = \{1, 2, 3\}$, then $\{1\}$ is a subset of $\mathscr{P}(A)$.
- (c) $\emptyset \in \{1, 2, 3\}$.

Exercise 4.2.7

Find the power set of the following sets.

- (a) $\{a, b\}$
- (b) $\{4, 7\}$
- (c) $\{x, y, z, w\}$
- (d) $\{\{a\}\}$
- (e) $\{a, \{b\}\}$
- (f) $\{\{x\}, \{y\}\}$

Answer

(e) $\{\emptyset, \{a\}, \{\{b\}\}, \{a, \{b\}\}\}$

Exercise 4.2.8

Evaluate the following sets.

- (a) $\mathscr{P}(\{\emptyset\})$
- (b) $\mathscr{P}(\mathscr{P}(\{a, b\}))$
- (c) $\mathscr{P}(\mathscr{P}(\mathscr{P}(\emptyset)))$

Exercise 4.2.9

Determine which of the following statements are true, and which are false.

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

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

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

(d) $\{a\} \in \mathscr{P}(\{a,b,c\})$

(e) $\emptyset \in \{a,b,c\}$

Answer

(a) True (b) False (c) False (d) True (e) False

Exercise 4.2.10

Let $P = \{n \in \mathbb{Z} \mid n = 3k \text{ for some integer } k\}$ and $Q = \{m \in \mathbb{Z} \mid m = 6j - 15 \text{ for some integer } j\}$.

(a) Prove $Q \subseteq P$.

(b) Explain with a counter example why $P \nsubseteq Q$.

Exercise 4.2.11

Determine which of the following statements are true, and which are false.

(a) $\mathbb{Z}^+ \in \mathbb{Q}$

(b) $\mathbb{Q}^+ \subseteq \mathbb{R}$

(c) $\mathbb{Q} \subseteq \mathbb{Z}$

(d) $\mathbb{Z}^+ = \mathbb{N}$

Answer

(a) False (b) True (c) False (d) True

Exercise 4.2.12

Let $A = \{n \in \mathbb{Z} \mid n = 8k - 3 \text{ for some integer } k\}$ and $B = \{m \in \mathbb{Z} \mid m = 8j + 5 \text{ for some integer } j\}$.

Prove $A = B$.

Exercise 4.2.13

We have learned that $A \subseteq A$ for any set A.

Which of these is correct: (a) $A \in \mathscr{P}(A)$ or (b) $A \subseteq \mathscr{P}(A)$?

Answer

(a) is correct (b) is incorrect

4.3: Unions and Intersections

We can form a new set from existing sets by carrying out a set operation.

Definition: $A \cap B$

Given two sets A and B, define their ***intersection*** to be the set

$$A \cap B = \{x \in \mathcal{U} \mid x \in A \wedge x \in B\} \tag{4.3.1}$$

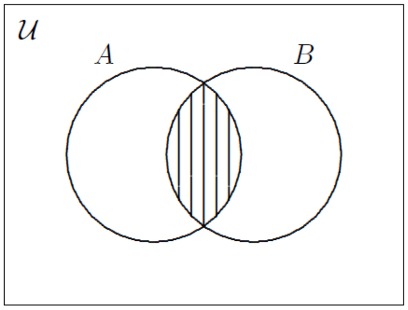
Loosely speaking, $A \cap B$ contains elements common to both A and B.

Definition: $A \cup B$

The ***union*** of A and B is defined as

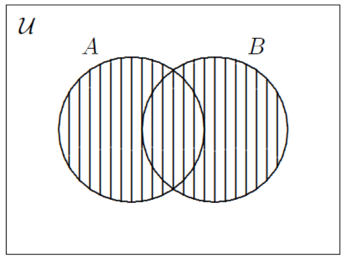
$$A \cup B = \{x \in \mathcal{U} \mid x \in A \vee x \in B\} \tag{4.3.2}$$

Thus $A \cup B$ is, as the name suggests, the set combining all the elements from A and B.



$A \cap B$

INTERSECTION



$A \cup B$

UNION

Definition: $A - B$

The ***set difference*** $A - B$, sometimes written as $A \setminus B$, is defined as

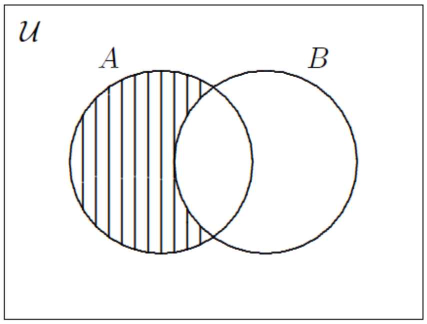
$$A - B = \{x \in \mathcal{U} \mid x \in A \wedge x \notin B\} \tag{4.3.3}$$

In words, $A - B$ contains elements that can only be found in A but not in B. Operationally speaking, $A - B$ is the set obtained from A by removing the elements that also belong to B.

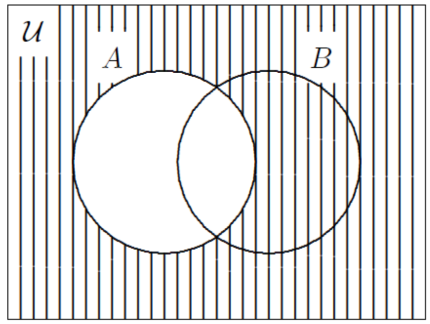
Definition: $\overline{A}$

The ***complement*** of A, denoted by $\overline{A}$, A' or A^c, is defined as

$$\overline{A} = \{x \in \mathcal{U} \mid x \notin A\} \tag{4.3.4}$$



$A-B$

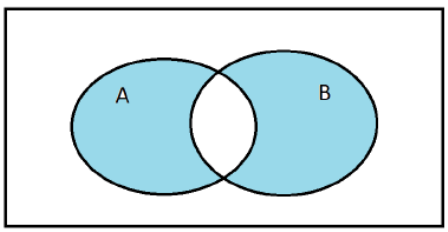


$\overline{A}$

Definition: $A \bigtriangleup B$

The ***symmetric difference*** $A \bigtriangleup B$, is defined as

$$A \bigtriangleup B = (A-B) \cup (B-A) \tag{4.3.5}$$



A △ B

Definition: Disjoint

Two sets are **disjoint** if their intersection is empty.

For example, consider $S=\{1,3,5\}$ and $T=\{2,8,10,14\}$.

$S \cap T = \emptyset$ so S and T are disjoint.

Remark

We would like to remind the readers that it is not uncommon among authors to adopt different notations for the same mathematical concept. Likewise, the same notation could mean something different in another textbook or even another branch of mathematics. It is important to develop the habit of examining the context and making sure that you understand the meaning of the notations when you start reading a mathematical exposition.

Example 4.3.1

Let $\mathcal{U}=\{1,2,3,4,5\}$, $A=\{1,2,3\}$, and $B=\{3,4\}$. Find $A\cap B$, $A\cup B$, $A-B$, $B-A$, $A \bigtriangleup B$, $\overline{A}$, and $\overline{B}$.

Solution

We have

$$\begin{aligned} A\cap B = & \{3\}, \\ A\cup B = & \{1,2,3,4\}, \\ A-B = & \{1,2\}, \\ B\bigtriangleup A = & \{1,2,4\}. \end{aligned}$$

We also find $\overline{A}=\{4,5\}$, and $\overline{B}=\{1,2,5\}$.

hands-on exercise 4.3.1

Let $\mathcal{U}=\{\text{John, Mary, Dave, Lucy, Peter, Larry}\}$,

$$A=\{\text{John, Mary, Dave}\}, \qquad \text{and} \qquad B=\{\text{John, Larry, Lucy}\}. \tag{4.3.6}$$

Find $A\cap B$, $A\cup B$, $A-B$, $B-A$, $\overline{A}$, and $\overline{B}$.

hands-on exercise 4.3.2

If $A\subseteq B$, what would be $A-B$?

Example 4.3.2

The set of integers can be written as the

$$\mathbb{Z}=\{-1,-2,-3,\ldots\}\cup\{0\}\cup\{1,2,3,\ldots\}. \tag{4.3.7}$$

Can we replace $\{0\}$ with 0? Explain.

hands-on exercise 4.3.3

Explain why the following expressions are syntactically incorrect.

- $\mathbb{Z}=\{-1,-2,-3,\ldots\}\cup\ 0\ \cup\{1,2,3,\ldots\}$.
- $\mathbb{Z}=\ldots,-3,-2,-1\ \cup\ 0\ \cup\ 1,2,3,\ldots$
- $\mathbb{Z}=\ldots,-3,-2,-1\ +\ 0\ +\ 1,2,3,\ldots$
- $\mathbb{Z}=\mathbb{Z}^-\ \cup\ 0\ \cup\ \mathbb{Z}^+$

How would you fix the errors in these expressions?

Example 4.3.3

For any set A, what are $A\cap\emptyset$, $A\cup\emptyset$, $A-\emptyset$, $\emptyset-A$ and $\overline{\overline{A}}$?

Answer

It is clear that

$$A\cap\emptyset=\emptyset, \qquad A\cup\emptyset=A, \qquad \text{and} \qquad A-\emptyset=A. \tag{4.3.8}$$

From the definition of set difference, we find $\emptyset-A=\emptyset$. Finally, $\overline{\overline{A}}=A$.

Example 4.3.4

Write, in interval notation, $[5,8)\cup(6,9]$ and $[5,8)\cap(6,9]$.

Answer

The answers are

$$[5,8)\cup(6,9]=[5,9], \qquad \text{and} \qquad [5,8)\cap(6,9]=(6,8). \tag{4.3.9}$$

They are obtained by comparing the location of the two intervals on the real number line.

hands-on exercise 4.3.4

Write, in interval notation, $(0,3)\cup[-1,2)$ and $(0,3)\cap[-1,2)$.

Example 4.3.5

We are now able to describe the following set

$$\{x\in\mathbb{R}\mid(x<5)\vee(x>7)\} \tag{4.3.10}$$

in the interval notation. It can be written as either $(-\infty,5)\cup(7,\infty)$ or, using complement, $\mathbb{R}-[5,7]$. Consequently, saying $x\notin[5,7]$ is the same as saying $x\in(-\infty,5)\cup(7,\infty)$, or equivalently, $x\in\mathbb{R}-[5,7]$.

To Prove a Set is Empty

To **prove a set is empty**, use a proof by contradiction with these steps:

(1) Assume not. That, is assume . . . is not empty.

(2) This means there is an element is . . . by definition of the empty set.

(3) Let $x\in\ldots$.

(4) Come to a contradition and wrap up the proof.

Example 4.3.6

Prove: $\forall A\in\mathcal{U}, A\cap\emptyset=\emptyset$.

Proof: Assume not. That is, assume for some set A, $A\cap\emptyset\neq\emptyset$.
By definition of the empty set, this means there is an element in $A\cap\emptyset$.

Let $x\in A\cap\emptyset$.

$x\in A\wedge x\in\emptyset$ by definition of intersection.

This says $x\in\emptyset$, but the empty set has no elements! This is a contradiction!

Thus, our assumption is false, and the original statement is true.
$\forall A\in\mathcal{U}, A\cap\emptyset=\emptyset$.

Set Properties

Notes:

(a) These properties should make sense to you and you should be able to prove them. However, you are not to use them as reasons in a proof. Rather your justifications for steps in a proof need to come directly from definitions. The exception to this is DeMorgan's Laws which you may reference as a reason in a proof.

(b) You do not need to memorize these properties or their names. However, you should know the meanings of: commutative, associative and distributive. Also, you should know DeMorgan's Laws by name and substance.

The following properties hold for any sets A, B, and C in a universal set $\mathcal{U}$.

1. ***Commutative properties***: $A\cup B=B\cup A$,
$A\cap B=B\cap A$.
2. ***Associative properties***: $(A\cup B)\cup C=A\cup(B\cup C)$,
$(A\cap B)\cap C=A\cap(B\cap C)$.
3. ***Distributive laws***: $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$,
$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

4. ***Idempotent laws***: $A \cup A = A$,
$A \cap A = A$.
5. ***De Morgan's laws***: (a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$,
(b) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
6. ***Laws of the excluded middle***, or ***inverse laws***: $A \cup \overline{A} = \mathcal{U}$,
$A \cap \overline{A} = \emptyset$.

As an illustration, we shall prove the distributive law

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{4.3.11}$$

We need to show that

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C), \qquad \text{and} \qquad (A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C). \tag{4.3.12}$$

Here is a proof of the distributive law $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof

First we will show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.
Let $x \in A \cup (B \cap C)$.
$x \in A \vee x \in B \cap C$ by definition of union.

Case 1: $x \in A$.
Since $x \in A$, $x \in A \cup B$, by definition of union and $x \in A \cup C$, by definition of union.
$\therefore x \in (A \cup B) \cap (A \cup C)$, by definition of intersection.

Case 2: $x \in B \cap C$.
$x \in B \wedge x \in C$, by definition of intersection.
$x \in A \cup B$, by definition of union and $x \in A \cup C$, by definition of union.
$\therefore x \in (A \cup B) \cap (A \cup C)$, by definition of intersection.

We have shown if $x \in A \cup (B \cap C)$ then $x \in (A \cup B) \cap (A \cup C)$.
So, by definition of subset, $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Next, we will show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.
Let $x \in (A \cup B) \cap (A \cup C)$.
$x \in (A \cup B) \wedge x \in (A \cup C)$ by definition of intersection.
Case 1: $x \in A$.
Since $x \in A$, we have $x \in A \cup (B \cap C)$ by definition of union.

Case 2: $x \notin A$.
Since $x \in (A \cup B)$, $x \in A \vee x \in B$ by definition of union, so x must be an element of B.
Furthermore, since $x \in (A \cup C)$, $x \in A \vee x \in C$ by definition of union, so x must be an element of C.
We have $x \in B \wedge x \in C$, thus $x \in B \cap C$. by definition of intersection.
And so, $x \in A \cup (B \cap C)$. by definition of union.

In both cases, if $x \in (A \cup B) \cap (A \cup C)$, then $x \in A \cup (B \cap C.)$
So, by definition of subset, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C.)$

It follows that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, by definition of equality of sets.

hands-on exercise 4.3.5

Prove that $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$.

hands-on exercise 4.3.6

Prove that if $A\subseteq B$ and $A\subseteq C$, then $A\subseteq B\cap C$.

Discussion

Let us start with a draft. The statement we want to prove takes the form of

$$(A\subseteq B)\wedge(A\subseteq C)\Rightarrow A\subseteq B\cap C. \tag{4.3.13}$$

Hence, what do we assume and what do we want to prove?

Assume:
Want to Prove:

Did you put down we assume $A\subseteq B$ and $A\subseteq C$, and we want to prove $A\subseteq B\cap C$? Great! Now, what does it mean by $A\subseteq B$? How about $A\subseteq C$? What is the meaning of $A\subseteq B\cap C$?

$A\subseteq B$ means: For any $x\in\mathcal{U}$, if $x\in A$, then $x\in B$ as well.
$A\subseteq C$ means:
$A\subseteq B\cap C$ means:

How can you use the first two pieces of information to obtain what we need to establish?

Now it is time to put everything together, and polish it into a final version. Remember three things:

- the outline of the proof,
- the reason in each step of the main argument, and
- the introduction and the conclusion.

Put the complete proof in the space below.

Here are two results involving complements.

Theorem 4.3.1

For any two sets A and B, we have $A\subseteq B\Leftrightarrow \overline{B}\subseteq\overline{A}$.

Theorem 4.3.2

For any sets A, B and C,

(a) $A-(B\cup C) = (A-B)\cap(A-C)$

(b) $A-(B\cap C) = (A-B)\cup(A-C)$

Summary and Review

- Memorize the definitions of intersection, union, and set difference. We rely on them to prove or derive new results.
- The intersection of two sets A and B, denoted $A\cap B$, is the set of elements common to both A and B. In symbols, $\forall x\in\mathcal{U}\left[x\in A\cap B\Leftrightarrow(x\in A\wedge x\in B)\right]$.
- The union of two sets A and B, denoted $A\cup B$, is the set that combines all the elements in A and B. In symbols, $\forall x\in\mathcal{U}\left[x\in A\cup B\Leftrightarrow(x\in A\vee x\in B)\right]$.
- The set difference between two sets A and B, denoted by $A-B$, is the set of elements that can only be found in A but not in B. In symbols, it means $\forall x\in\mathcal{U}\left[x\in A-B\Leftrightarrow(x\in A\wedge x\notin B)\right]$.
- The symmetric difference between two sets A and B, denoted by $A\bigtriangleup B$, is the set of elements that can be found in A and in B, but not in both A and B. In symbols, it means $\forall x\in\mathcal{U}\left[x\in A\bigtriangleup B\Leftrightarrow x\in A-B\vee x\in B-A)\right]$.

Exercises

Exercise 4.3.1

Write each of the following sets by listing its elements explicitly.

(a) $[-4, 4] \cap \mathbb{Z}$

(b) $(-4, 4] \cap \mathbb{Z}$

(c) $(-4, \infty) \cap \mathbb{Z}$

(d) $(-\infty, 4] \cap \mathbb{N}$

(e) $(-4, \infty) \cap \mathbb{Z}^-$

(f) $(4, 5) \cap \mathbb{Z}$

Answer

(a) $\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

(b) $\{-3, -2, -1, 0, 1, 2, 3, 4\}$

(c) $\{-3, -2, -1, 0, 1, 2, 3, \ldots\}$

Exercise 4.3.2

Assume $\mathcal{U} = \mathbb{Z}$, and let

$A = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} = 2\mathbb{Z}$,

$B = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = 3\mathbb{Z}$,

$C = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\} = 4\mathbb{Z}$.

Describe the following sets by listing their elements explicitly.

(a) $A \cap B$

(b) $C - A$

(c) $A - B$

(d) $A \cap \overline{B}$

(e) $B - A$

(f) $B \cup C$

(g) $(A \cup B) \cap C$

(h) $(A \cup B) - C$

Exercise 4.3.3

Are these statements true or false?

(a) $[1, 2] \cap [2, 3] = \emptyset$

(b) $[1, 2) \cup (2, 3] = [2, 3]$

Answer

(a) false (b) false

Exercise 4.3.4

Let the universal set $\mathcal{U}$ be the set of people who voted in the 2012 U.S. presidential election. Define the subsets D, B, and W of $\mathcal{U}$ as follows:

$$\begin{aligned} D = & \quad \{x \in \mathcal{U} \mid x \text{ registered as a Democrat}\}, \\ B = & \quad \{x \in \mathcal{U} \mid x \text{ voted for Barack Obama}\}, \\ W = & \quad \{x \in \mathcal{U} \mid x \text{ belonged to a union}\}. \end{aligned}$$

Express the following subsets of $\mathcal{U}$ in terms of D, B, and W.

(a) People who did not vote for Barack Obama.

(b) Union members who voted for Barack Obama.

(c) Registered Democrats who voted for Barack Obama but did not belong to a union.

(d) Union members who either were not registered as Democrats or voted for Barack Obama.

(e) People who voted for Barack Obama but were not registered as Democrats and were not union members.

(f) People who were either registered as Democrats and were union members, or did not vote for Barack Obama.

Exercise 4.3.5

An insurance company classifies its set $\mathcal{U}$ of policy holders by the following sets:

$$\begin{aligned} A = & \quad \{x \mid x \text{ drives a subcompact car}\}, \\ B = & \quad \{x \mid x \text{ drives a car older than 5 years}\}, \\ C = & \quad \{x \mid x \text{ is married}\}, \\ D = & \quad \{x \mid x \text{ is over 21 years old}\}, \\ E = & \quad \{x \mid x \text{ is a male}\}. \end{aligned}$$

Describe each of the following subsets of $\mathcal{U}$ in terms of A, B, C, D, and E.

(a) Male policy holders over 21 years old.

(b) Policy holders who are either female or drive cars more than 5 years old.

(c) Female policy holders over 21 years old who drive subcompact cars.

(d) Male policy holders who are either married or over 21 years old and do not drive subcompact cars.

Answer

(a) $E \cap D$ (b) $\overline{E} \cup B$

Exercise 4.3.6

Let A and B be arbitrary sets. Complete the following statements.

(a) $A \subseteq B \Leftrightarrow A \cap B =$ ____________________

(b) $A \subseteq B \Leftrightarrow A \cup B =$ ____________________

(c) $A \subseteq B \Leftrightarrow A - B =$ ____________________

(d) $A \subset B \Leftrightarrow (A - B =$ ____________________ $\wedge B - A \neq$ ____________________)

(e) $A \subset B \Leftrightarrow (A \cap B =$ ____________________ $\wedge A \cap B \neq$ ____________________)

(f) $A - B = B - A \Leftrightarrow$ ____________________

Exercise 4.3.7

Give examples of sets A and B such that $A \in B$ and $A \subset B$.

Answer

For example, take $A=\{x\}$, and $B=\{\{x\},x\}$.

Exercise 4.3.8

(a) Prove De Morgan's law, (a) .

(b) Prove De Morgan's law, (b) .

Exercise 4.3.9

Let A, B, and C be any three sets. Prove that if $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.

Answer

Assume $A \subseteq C$ and $B \subseteq C$, we want to show that $A \cup B \subseteq C$.

Let $x \in A \cup B$. we want to show that $x \in C$ as well.

Since $x \in A \cup B$, then either $x \in A$ or $x \in B$ by definition of union.

Case 1: If $x \in A$, then $A \subseteq C$ implies that $x \in C$ by definition of subset.

Case 2: If $x \in B$, then $B \subseteq C$ implies that $x \in C$ by definition of subset.

In both cases, we find $x \in C$. So, if $x \in A \cup B$ then $x \in C$.

This proves that $A \cup B \subseteq C$ by definition of subset.

$\therefore$ For any sets A, B, and C if $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.

Exercise 4.3.10

Prove Theorem 4.3.1

Exercise 4.3.11

(a) Prove Theorem 4.3.2 part (a)

(b) Prove Theorem 4.3.2 part (b)

Exercise 4.3.12

Let A, B, and C be any three sets. Prove that

(a) $A-B=A \cap \overline{B}$

(b) $A=(A-B) \cup (A \cap B)$

(c) $A-(B-C)=A \cap (\overline{B} \cup C)$

(d) $(A-B)-C=A-(B \cup C)$

Exercise 4.3.13

Comment on the following statements. Are they syntactically correct?

(a) $x \in A \cap x \in B \equiv x \in A \cap B$

(b) $x \in A \wedge B \Rightarrow x \in A \cap B$

Answer

(a) The notation $\cap$ is used to connect two sets, but "$x \in A$" and "$x \in B$" are both logical statements. We should also use $\Leftrightarrow$ instead of $\equiv$. The statement should have been written as "$x \in A \wedge x \in B \Leftrightarrow x \in A \cap B$."

(b) If we read it aloud, it sounds perfect:

$$\text{If } x \text{ belongs to } A \text{ and } B, \text{ then } x \text{ belongs to } A \cap B. \tag{4.3.14}$$

The trouble is, every notation has its own meaning and specific usage. In this case, $\wedge$ is not exactly a replacement for the English word "and." Instead, it is the notation for joining two logical statements to form a conjunction. Before $\wedge$, we have "$x \in A$," which is a logical statement. But, after $\wedge$, we have "B," which is a set, and not a logical statement. It should be written as "$x \in A \wedge x \in B \Rightarrow x \in A \cap B$."

Exercise 4.3.14

Prove or disprove each of the following statements about arbitrary sets A and B. If you think a statement is true, prove it; if you think it is false, provide a counterexample.

(a) $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$

(b) $\mathscr{P}(A \cup B) = \mathscr{P}(A) \cup \mathscr{P}(B)$

(c) $\mathscr{P}(A - B) = \mathscr{P}(A) - \mathscr{P}(B)$

Remark

To show that two sets U and V are equal, we usually want to prove that $U \subseteq V$ and $V \subseteq U$. For the subset relationship, we start with let $x \in U$. In this problem, the element x is actually a set. Since we usually use uppercase letters to denote sets, for (a) we should start the proof of the subset relationship "Let $S \in \mathscr{P}(A \cap B)$," using an uppercase letter to emphasize the elements of $\mathscr{P}(A \cap B)$ are sets. These remarks also apply to (b) and (c).

Exercise 4.3.15

Let $\mathcal{U} = \{1,2,3,4,5,6,7,8\}$, $A = \{2,4,6,8\}$, $B = \{3,5\}$, $C = \{1,2,3,4\}$ and $D = \{6,8\}$. Find

(a) $A \cap C$ (b) $A \cap B$ (c) $\emptyset \cup B$

(d) $\emptyset \cap B$ (e) $A - (B \cup C)$ (f) $C - B$

(g) $A \,\triangle\, C$ (h) $A \cup \mathcal{U}$ (i) $A \cap D$

(j) $A \cup D$ (k) $B \cap D$ (l) $B \,\triangle\, C$

(m) $A \cap \mathcal{U}$ (n) $\overline{A}$ (o) $\overline{B}$.

(p) $D \cup (B \cap C)$ (q) $\overline{A \cup C}$ (r) $\overline{A} \cup \overline{C}$

(s) Which pairs of sets are disjoint?

Answer

(a) $\{2,4\}$ (b) $\emptyset$ (c) B (d) $\emptyset$

Exercise 4.3.16

Prove:

If $A \subseteq B$ then $A - B = \emptyset$.

4.4: Cartesian Products

Another way to obtain a new set from two given sets A and B is to form ordered pairs.

Definition: Ordered Pair

An ***ordered pair*** (x,y) consists of two values x and y. Their order of appearance is important, so we call them first and second elements respectively. Consequently, $(a,b) \neq (b,a)$ unless $a=b$. In general, $(a,b)=(c,d)$ if and only if $a=c$ and $b=d$.

Definition: Cartesian Product

The ***Cartesian product*** of A and B is the set

$$A \times B = \{(a,b) \mid a \in A \wedge b \in B\} \tag{4.4.1}$$

Thus, $A \times B$ (read as "A cross B") contains all the ordered pairs in which the first elements are selected from A, and the second elements are selected from B.

Example 4.4.1

Let $A=\{\text{John}, \text{Jim}, \text{Dave}\}$ and $B=\{\text{Mary}, \text{Lucy}\}$. Determine $A \times B$ and $B \times A$.

Solution

We find

$$\begin{aligned} A \times B &= \{(\text{John}, \text{Mary}), (\text{John}, \text{Lucy}), (\text{Jim}, \text{Mary}), (\text{Jim}, \text{Lucy}), (\text{Dave}, \text{Mary}), (\text{Dave}, \text{Lucy})\}, \\ B \times A &= \{(\text{Mary}, \text{John}), (\text{Mary}, \text{Jim}), (\text{Mary}, \text{Dave}), (\text{Lucy}, \text{John}), (\text{Lucy}, \text{Jim}), (\text{Lucy}, \text{Dave})\}. \end{aligned} \tag{4.4.2}$$

In general, $A \times B \neq B \times A$.

Example 4.4.2

Determine $A \times B$ and $A \times A$:

$A=\{1,2\}$ and $B=\{2,5,6\}$.

$A=\{5\}$ and $B=\{0,7\}$.

Solution

(a) We find

$$\begin{aligned} A \times B &= \{(1,2),(1,5),(1,6),(2,2),(2,5),(2,6)\}, \\ A \times A &= \{(1,1),(1,2),(2,1),(2,2)\}. \end{aligned}$$

(b) The answers are $A \times B = \{(5,0),(5,7)\}$, and $A \times A = \{(5,5)\}$.

hands-on exercise 4.4.1

Let $A=\{a,b,c,d\}$ and $B=\{r,s,t\}$. Find $A \times B$, $B \times A$, and $B \times B$.

Example 4.4.3

Determine $\wp(\{1,2\}) \times \{3,7\}$. Be sure to use correct notation.

Solution

For a complicated problem, divide it into smaller tasks and solve each one separately. Then assemble them to form the final answer. In this problem, we first evaluate

$$\wp(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}. \tag{4.4.3}$$

This leads to

$$\begin{aligned} \wp(\{1,2\}) \times \{3,7\} &= \{\emptyset, \{1\}, \{2\}, \{1,2\}\} \times \{3,7\} \\ &= \{(\emptyset,3), (\emptyset,7), (\{1\},3), (\{1\},7), (\{2\},3), (\{2\},7), (\{1,2\},3), (\{1,2\},7)\}. \end{aligned}$$

Check to make sure that we have matching left and right parentheses, and matching left and right curly braces.

hands-on exercise 4.4.2

Find $\{a,b,c\} \times \wp(\{d\})$.

Example 4.4.4

How could we describe the contents of the Cartesian product $[1,3] \times \{2,4\}$? Since $[1,3]$ is an infinite set, it is impossible to list all the ordered pairs. We need to use the set-builder notation:

$$[1,3] \times \{2,4\} = \{(x,y) \mid 1 \leq x \leq 3, y = 2,4\}. \tag{4.4.4}$$

We can also write $[1,3] \times \{2,4\} = \{(x,2),(x,4) \mid 1 \leq x \leq 3\}$.

hands-on exercise 4.4.3

Describe, using the set-builder notation, the Cartesian product $[1,3] \times [2,4]$.

Cartesian products can be extended to more than two sets. Instead of ordered pairs, we need ***ordered n-tuples***. The ***n-fold Cartesian product*** of n sets $A_1, A_2, \ldots, A_n$ is the set

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for each } i, 1 \leq i \leq n\} \tag{4.4.5}$$

In particular, when $A_i = A$ for all i, we abbreviate the Cartesian product as A^n.

Example 4.4.5

The n-dimensional space is denoted $\mathbb{R}^n$. It is the n-fold Cartesian product of $\mathbb{R}$. In special cases, $\mathbb{R}^2$ is the xy-plane, and $\mathbb{R}^3$ is the xyz-space.

Example 4.4.6

If $D = \{1,2\}$ then $D^3 = D \times D \times D =$

Solution

$$\{(1,1,1),(1,1,2),(1,2,2),(1,2,1),(2,1,1),(2,1,2),(2,2,2),(2,2,1)\}$$

hands-on exercise 4.4.5

Let $A = \{1,2\}$, $B = \{a,b\}$, and $C = \{r,s,t\}$. Find $A \times B \times C$.

Example 4.4.7

From a technical standpoint, $(A \times B) \times C$ is different from $A \times B \times C$. Can you explain why? Can you discuss the difference, if any, between $(A \times B) \times C$ and $A \times (B \times C)$? For instance, give some specific examples of the elements in $(A \times B) \times C$ and $A \times (B \times C)$ to illustrate their differences.

Solution

The elements of $(A\times B)\times C$ are ordered pairs in which the first coordinates are themselves ordered pairs. A typical element in $(A\times B)\times C$ takes the form of

$$\big((a,b),c\big). \tag{4.4.6}$$

The elements in $A\times B\times C$ are ordered triples of the form

$$(a,b,c). \tag{4.4.7}$$

Since their elements look different, it is clear that $(A\times B)\times C\neq A\times B\times C$. Likewise, a typical element in $A\times(B\times C)$ looks like

$$\big(a,(b,c)\big). \tag{4.4.8}$$

Therefore, $(A\times B)\times C\neq A\times(B\times C)$, and $A\times(B\times C)\neq A\times B\times C$.

Theorem 4.4.1

For any sets A, B, and C, we have

$$\begin{aligned} A\times(B\cup C) &= (A\times B)\cup(A\times C), \\ A\times(B\cap C) &= (A\times B)\cap(A\times C), \\ A\times(B-C) &= (A\times B)-(A\times C). \end{aligned}$$

Remark

How would we show that the two sets S and T are equal? We need to show that

$$x\in S\Leftrightarrow x\in T. \tag{4.4.9}$$

The complication in this problem is that both S and T are Cartesian products, so x takes on a special form, namely, that of an ordered pair. Consider the first identity as an example

$A\times(B\cup C)=(A\times B)\cup(A\times C)$.

We need to show that

$$(u,v)\in A\times(B\cup C)\Leftrightarrow(u,v)\in(A\times B)\cup(A\times C). \tag{4.4.10}$$

We prove this in two steps: first showing $\Rightarrow$, then $\Leftarrow$, which is equivalent to first showing $\subseteq$, then $\supseteq$.

Proof

Let $(u,v)\in A\times(B\cup C)$. Then by definition of Cartesian Product, $u\in A$, and $v\in B\cup C$.

The definition of union implies that $v\in B$ or $v\in C$. Thus far, we have found

- $u\in A$ and $v\in B$, or
- $u\in A$ and $v\in C$.

By definition of Cartesian Product, this is equivalent to

- $(u,v)\in A\times B$, or
- $(u,v)\in A\times C$.

Thus, $(u,v)\in(A\times B)\cup(A\times C)$. This proves that $A\times(B\cup C)\subseteq(A\times B)\cup(A\times C)$, by definition of subset.

Next, let $(u,v)\in(A\times B)\cup(A\times C)$. Then $(u,v)\in A\times B$, or $(u,v)\in A\times C$ by definition of union.

This means, by definition of Cartesian Product,

- $u\in A$ and $v\in B$, or
- $u\in A$ and $v\in C$.

Both conditions require $u\in A$, so we can rewrite them as

- $u\in A$, and

- $v \in B$ or $v \in C$;

which is equivalent to

- $u \in A$, and
- $v \in B \cup C$ by definition of union.

Thus, $(u, v) \in A \times (B \cup C)$. We have proved that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. Together with $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ that we have proved earlier, we conclude that $A \times (B \cup C) = (A \times B) \cup (A \times C)$, by definition of Set Equality.

Theorem 4.4.2

If A and B are finite sets, with $|A| = m$ and $|B| = n$, then $|A \times B| = mn$.

Proof

The elements of $A \times B$ are ordered pairs of the form (a, b), where $a \in A$, and $b \in B$. There are m choices of a. For each fixed a, we can form the ordered pair (a, b) in n ways, because there are n choices for b. Together, the ordered pairs (a, b) can be formed in mn ways.

The argument we used in the proof is called ***multiplication principle***. We shall study it again in Chapter 7. In brief, it says that if a job can be completed in several steps, then the number of ways to finish the job is the product of the number of ways to finish each step.

Corallary 4.4.3

If $A_1, A_2, \ldots, A_n$ are finite sets, then $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.

Corollary 4.4.4

If A is a finite set with $|A| = n$, then $|\mathscr{P}(A)| = 2^n$.

Proof

Let the elements of A be $a_1, a_2, \ldots, a_n$. The elements of $\mathscr{P}(A)$ are subsets of A. Each subset of A contains some elements from A. Let $B = \{0, 1\}$, so B^n is $B \times B \times B \times B \times \ldots$ n times. B^n is the set of all possible n-tupples (or strings) with 1s and 0s. Associate to each subset S of A an ordered n-tuple $(b_1, b_2, \ldots, b_n)$ from B^n such that

$$b_i = \begin{cases} 0 & \text{if } a_i \notin S, \\ 1 & \text{if } a_i \in S. \end{cases} \tag{4.4.11}$$

The value of the ith element in this ordered n-tuple indicates whether the subset S contains the element a_i. It is clear that the subsets of A are in one-to-one correspondence with the n-tuples. This means the power set $\mathscr{P}(A)$ and the Cartesian product B^n have the same cardinality. Since there are 2^n ordered n-tuples, we conclude that there are 2^n subsets as well.

This idea of one-to-one correspondence is a very important concept in mathematics. We shall study it again in Chapter 5.

Summary and Review

- The Cartesian product of two sets A and B, denoted $A \times B$, consists of ordered pairs of the form (a, b), where a comes from A, and b comes from B.
- Since ordered pairs are involved, $A \times B$ usually is not equal to $B \times A$.
- The notion of ordered pairs can be extended analogously to ordered n-tuples, thereby yielding an n-fold Cartesian product.
- If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.

Exercises

Exercise 4.4.1

Let $X = \{-2, 2\}$, $Y = \{0, 4\}$ and $Z = \{-3, 0, 3\}$. Evaluate the following Cartesian products.

a. $X \times Y$
b. $X \times Z$
c. $Z \times Y \times Y$

Solution

(a) $\{(-2,0),(-2,4),(2,0),(2,4)\}$

(b) $\{(-2,-3),(-2,0),(-2,3),(2,-3),(2,0),(2,3)\}$

Exercise 4.4.2

Consider the sets X, Y and Z defined in Problem 1. Evaluate the following Cartesian products.

a. $X \times Y \times Z$
b. $(X \times Y) \times Z$
c. $X \times (Y \times Z)$

Exercise 4.4.3

Without listing all the elements of $X \times Y \times X \times Z$, where X, Y, and Z are defined in Problem 1, determine $|X \times Y \times X \times Z|$.

Solution

$2 \cdot 2 \cdot 2 \cdot 3 = 24$.

Exercise 4.4.4

Let $A = \{1,2,3\}$ and $B = \{5,6\}$.

(a) $|A \times B| =$

(b) True or False?

(b1) $(1,6) \in A \times B$

(b2) $(5,2) \in A \times B$

(b3) $A \subseteq A \times B$

(b4) $\{(1,5),(2,6)\} \subseteq A \times B$

(b5) $(3,3) \in A \times B$

(b6) $(2,5) \in A \times B$

(b7) $(1,5) \subseteq A \times B$

(b8) $\{(5,2),(6,1),(6,3)\} \subseteq B \times A$

Exercise 4.4.5

Which of the following are elements of the Cartesian product $[1,3] \times \{2,4\}$? (see Example 4.4)

Note: assume (,) indicates ordered pairs, not intervals; [,] does indicate a closed interval.

(a) (1,2) (b) (4,4) (c) (4,3) (d) (2,4) (e) (1.7, 4) (f) [2,3]

(g) (0.7, 4) (h) (2.7, 4) (i) (3, 4) (j) (1.5, 2) (k) (3,3) (l) (2.981, 2)

Answer

(a) YES $(1,2) \in [1,3] \times \{2,4\}$ (b) No (c) No (d) YES (e) YES (f) No
(g) No (h) YES (i) YES (j) YES (k) No (l) YES

Exercise 4.4.6

Determine $|\mathscr{P}(\mathscr{P}(\mathscr{P}(\{1,2\})))|$.

Exercise 4.4.7

Consider the set $X = \{-2, 2\}$. Evaluate the following Cartesian products.

a. $X \times \mathscr{P}(X)$
b. $\mathscr{P}(X) \times \mathscr{P}(X)$
c. $\mathscr{P}(X \times X)$

Solution

(a) $\{(-2, \emptyset), (-2, \{-2\}), (-2, \{2\}), (-2, \{-2, 2\}), (2, \emptyset), (2, \{-2\}), (2, \{2\}), (2, \{-2, 2\})\}$

Exercise 4.4.8

Let A and B be arbitrary nonempty sets.

a. Under what condition does $A \times B = B \times A$?
b. Under what condition is $(A \times B) \cap (B \times A)$ empty?

Exercise 4.4.9

Let A, B, and C be any three sets. Prove that

a. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
b. $A \times (B - C) = (A \times B) - (A \times C)$

Exercise 4.4.10

Let A, B, and C be any three sets. Prove that if $A \subseteq B$, then $A \times C \subseteq B \times C$.

4.5: Index Sets and Partitions

$$\bigcup_{i=1}^{n} A_i \text{ and } \bigcap_{i=1}^{n} A_i \tag{4.5.3}$$

The notion of union can be extended to three sets:

$$A \cup B \cup C = \{x \in \mathcal{U} \mid (x \in A) \vee (x \in B) \vee (x \in C)\}. \tag{4.5.4}$$

It is obvious how to generalize it to the union of any number of sets. We use a notation that resembles the summation notation to describe such a union:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n. \tag{4.5.5}$$

We define

$$\bigcup_{i=1}^{n} A_i = \{x \in \mathcal{U} \mid (x \in A_1) \vee (x \in A_2) \vee \cdots \vee (x \in A_n)\}. \tag{4.5.6}$$

It looks messy! Here is a better alternative:

$$\bigcup_{i=1}^{n} A_i = \{x \in \mathcal{U} \mid x \in A_i \text{ for } \textit{some } i \in \mathbb{N}, \text{ where } 1 \leq i \leq n\}. \tag{4.5.7}$$

In a similar manner, $\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$, and we define

$$\bigcap_{i=1}^{n} A_i = \{x \in \mathcal{U} \mid x \in A_i \text{ for } \textit{all } i \in \mathbb{N}, \text{ where } 1 \leq i \leq n\} \tag{4.5.8}$$

In plain English, $\bigcup_{i=1}^{n} A_i$ is the collection of all elements in the A_i's, and $\bigcap_{i=1}^{n} A_n$ is the collection of all elements *common* to all A_i's.

Example 4.5.1

For $i = 1, 2, 3, \ldots$, let $A_i = [-i, i]$. First, construct several A_i for comparison, because it may help us detect any specific pattern. See Figure below. It is clear that $A_1 \subset A_2 \subset \cdots$. Thus, $\bigcup_{i=1}^{n} A_i = [-n, n] = A_n$, and $\bigcap_{i=1}^{n} A_i = [-1, 1] = A_1$.

hands-on Exercise 4.5.1

Evaluate $\bigcup_{i=1}^{n} B_i$ and $\bigcap_{i=1}^{n} B_i$, where $B_i = [0, 2i)$ for $i \in \mathbb{N}$.

$$\bigcup_{i=1}^{\infty} A_i \text{ and } \bigcap_{i=1}^{\infty} A_i \tag{4.5.9}$$

It is obvious that we can also extend the upper bound to infinity.

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots = \{x \in \mathcal{U} \mid x \in A_i \text{ for } \textit{some } i \in \mathbb{N}\},$$
$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \cdots = \{x \in \mathcal{U} \mid x \in A_i \text{ for } \textit{all } i \in \mathbb{N}\}.$$

In some situations, we may borrow the idea of partial sums from calculus. We first find the union or intersection of the first n sets, then take the limit as n approaches infinity. Thus, if the limit is well-defined, the

$$\bigcup_{i=1}^{\infty} A_i = \lim_{n\to\infty} \bigcup_{i=1}^{n} A_i, \qquad \text{and} \qquad \bigcap_{i=1}^{\infty} A_i = \lim_{n\to\infty} \bigcap_{i=1}^{n} A_i. \tag{4.5.10}$$

Example 4.5.2

Let $A_i = [-i, i]$. We have learned from the last example that $\bigcup_{i=1}^{n} A_i = [-n, n]$ and $\bigcap_{i=1}^{n} A_i = [-1, 1]$. Hence,

$$\bigcup_{i=1}^{\infty} A_i = \lim_{n\to\infty} [-n, n] = (-\infty, \infty), \qquad \text{and} \qquad \bigcap_{i=1}^{\infty} A_i = [-1, 1]. \tag{4.5.11}$$

Recall that we write $(-\infty, \infty)$ instead of $[-\infty, \infty]$ because $\pm\infty$ are *not* numbers, they are merely symbols representing infinitely large values.

hands-on Exercise 4.5.2

Evaluate $\bigcup_{i=1}^{\infty} B_i$ and $\bigcap_{i=1}^{\infty} B_i$, where $B_i = [0, 2i)$.

Example 4.5.3

Let $B_i = \left(0, 1 - \frac{1}{2i}\right]$. Determine $\bigcup_{i=1}^{\infty} B_i$ and $\bigcap_{i=1}^{\infty} B_i$.

Solution

Once again, we have $B_1 \subset B_2 \subset \cdots$. It is easy to check that

$$\bigcup_{i=1}^{n} B_i = B_n = \left(0, 1 - \frac{1}{2n}\right], \qquad \text{and} \qquad \bigcap_{i=1}^{n} B_i = B_1 = \left(0, \frac{1}{2}\right]. \tag{4.5.12}$$

It follows that

$$\bigcup_{i=1}^{\infty} B_i = \lim_{n\to\infty} \left(0, 1 - \frac{1}{2n}\right] = (0, 1), \qquad \text{and} \qquad \bigcap_{i=1}^{\infty} B_i = \left(0, \frac{1}{2}\right]. \tag{4.5.13}$$

Note that $\lim_{n\to\infty} \left(0, 1 - \frac{1}{2n}\right] \neq (0, 1]$ because the endpoint 1 does not belong to any B_i.

hands-on Exercise 4.5.3

Let $C_i = \left[0, 1 - \frac{1}{i}\right]$. Determine $\bigcup_{i=1}^{\infty} C_i$ and $\bigcap_{i=1}^{\infty} C_i$.

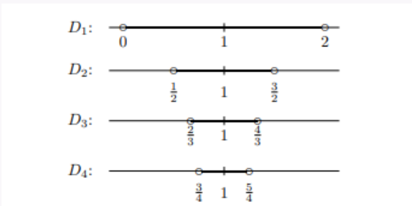
Example 4.5.4

Let $D_i = \left(1 - \frac{1}{i}, 1 + \frac{1}{i}\right)$. Determine $\bigcup_{i=1}^{\infty} D_i$ and $\bigcap_{i=1}^{\infty} D_i$.

Solution

As the value of i increases, the value of $\frac{1}{i}$ decreases. Hence, the left endpoint $1-\frac{1}{i}$ increases, and the right endpoint $1+\frac{1}{i}$ decreases.

i	$D_i = \left(1-\frac{1}{i}, 1+\frac{1}{i}\right)$
1	$(0,2)$
$[6pt]2$	$\left(\frac{1}{2}, \frac{3}{2}\right)$
$[6pt]3$	$\left(\frac{2}{3}, \frac{4}{3}\right)$
$[6pt]4$	$\left(\frac{3}{4}, \frac{5}{4}\right)$



It is clear that $D_1 \supseteq D_2 \supseteq D_3 \supseteq \cdots$. Thus, $\bigcup_{i=1}^{\infty} D_i = D_1 = (0,2)$, and $\bigcap_{i=1}^{\infty} D_i = \{1\}$.

hands-on exercise 4.5.4

Let $E_i = \left[-i, 1+\frac{1}{i}\right)$. Determine $\bigcup_{i=1}^{\infty} E_i$ and $\bigcap_{i=1}^{\infty} E_i$.

hands-on Exercise 4.5.5

For each positive integer i, define $F_i = \{i, i+1, i+2, \ldots, 3i\}$. Determine $\bigcup_{i=1}^{\infty} F_i$ and $\bigcap_{i=1}^{\infty} F_i$.

The next two results are obvious.

Theorem 4.5.1

If $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$, then $\bigcap_{i=1}^{\infty} A_i = A_1$.

Theorem 4.5.2

If $A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$, then $\bigcup_{i=1}^{\infty} A_i = A_1$.

Indexed Family of Sets

How could we describe the union $A_2 \cup A_4 \cup A_6 \cup \cdots$? Well, we can write

$$\bigcup_{i \text{ even}} A_i, \tag{4.5.14}$$

which means that union of A_i, where i is even. Since the set of even positive integers is denoted by $2\mathbb{N}$, another way to describe the same union is

$$\bigcup_{i \in 2\mathbb{N}} A_i. \tag{4.5.15}$$

It means the union all A_i, where i is taken out from the set $2\mathbb{N}$. Accordingly,

$$\bigcup_{i=0}^{\infty} A_i = \bigcup_{i\in\mathbb{N}} A_i, \qquad \text{and} \qquad \bigcap_{i=0}^{\infty} A_i = \bigcap_{i\in\mathbb{N}} A_i. \tag{4.5.16}$$

We can even go one step further, by allowing i to be taken from any set of integers, or any set of real numbers, or even any set of objects. The only restriction is that A_i must exist, and its content must somehow depend on i.

In general, given a nonempty set I, if we could associate with each $i \in I$ a set A_i, we define the ***indexed family of sets*** $\mathcal{A}$ as

$$\mathcal{A} = \{A_i \mid i \in I\}. \tag{4.5.17}$$

We call I the ***index set***, and define

$$\begin{aligned} \bigcup_{i\in I} A_i &= \{x \mid x \in A_i \text{ for } \textit{some } i \in I\}, \\ \bigcap_{i\in I} A_i &= \{x \mid x \in A_i \text{ for } \textit{all } i \in I\}. \end{aligned}$$

Let us look at a few examples.

Example 4.5.5

To describe the union

$$A_1 \cup A_3 \cup A_7 \cup A_{11} \cup A_{23}, \tag{4.5.18}$$

we first define the index set to be $I = \{1, 3, 7, 11, 23\}$, which is the set of all the subscripts used in the union. Now the union can be conveniently described as $\bigcup_{i\in I} A_i$.

Example 4.5.6

Consider five sets

$$\begin{aligned} A_1 &= \{1, 4, 23\}, \\ A_2 &= \{7, 11, 23\}, \\ A_3 &= \{3, 6, 9\}, \\ A_4 &= \{5, 17, 22\}, \\ A_5 &= \{3, 6, 23\}. \end{aligned}$$

Let $I = \{2, 5\}$, then

$$\bigcup_{i\in I} A_i = A_2 \cup A_5 = \{7, 11, 23\} \cup \{3, 6, 23\} = \{3, 6, 7, 11, 23\}. \tag{4.5.19}$$

Likewise, $\bigcap_{i\in I} A_i = A_2 \cap A_5 = \{7, 11, 23\} \cap \{3, 6, 23\} = \{23\}$.

hands-on Exercise 4.5.6

Let $J = \{1, 4, 5\}$. Evaluate $\bigcup_{i\in J} A_i$ and $\bigcap_{i\in J} A_i$, where A_is are defined in the last example.

hands-on Exercise 4.5.7

An index set could be a set of any objects. For instance, the sets of numbers in the last example could be the favorite Lotto numbers of five different students. We could index these sets according to the names of the students:

$$\begin{aligned} A_{John} &= \{1, 4, 23\}, \\ A_{Mary} &= \{7, 11, 23\}, \\ A_{Joe} &= \{3, 6, 9\}, \\ A_{Pete} &= \{5, 17, 22\}, \\ A_{Lucy} &= \{3, 6, 23\}. \end{aligned}$$

If $I = \{\text{Mary}, \text{Joe}, \text{Lucy}\}$, what is $\bigcup_{i\in I}$? How would you interpret its physical meaning?

example 4.5.7

Let $I = \{x \mid x \text{ is a living human being }\}$, and define

$$\begin{aligned} B_i &= \{x \in I \mid x \text{ is a child of } i\}, \\ A_i &= \{i\} \cup B_i \end{aligned}$$

for each $i \in I$. Then

$$\bigcap_{i\in I} A_i = \emptyset, \qquad \bigcup_{i\in I} A_i = I, \qquad \bigcap_{i\in I} B_i = \emptyset, \tag{4.5.20}$$

and

$$\bigcup_{i\in I} B_i = I - \{x \mid x\text{'s parents are both deceased}\}. \tag{4.5.21}$$

We leave it as an exercise to verify these unions and intersections.

hands-on Exercise 4.5.8

Verify the intersection and union in the last example.

hands-onExercise 4.5.9

If I represents a set of students, and A_i represents the set of friends of student i, interpret the meaning of $\bigcup\limits_{i\in I} A_i$ and $\bigcap_{i\in I} A_i$.

We close this section with yet another generalization of De Morgan's laws.

Theorem 4.5.3 Extended De Morgan's laws

For any nonempty index set I, we have

$$\overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \overline{A_i}, \qquad \text{and} \qquad \overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i}. \tag{4.5.22}$$

Proof 1

Let $x \in \overline{\bigcup\limits_{i\in I} A_i}$, then

$$x \notin \bigcup_{i\in I} A_i = \{x \mid x \in A_i \text{ for } \textit{some } i \in I\}. \tag{4.5.23}$$

This means $x \notin A_i$ for every $i \in I$. Hence, $x \in \overline{A_i}$ for each $i \in I$. Consequently,

$$x \in \bigcap_{i\in I} \overline{A_i}. \tag{4.5.24}$$

This proves that $\overline{\bigcup\limits_{i\in I} A_i} \subseteq \bigcap_{i\in I} \overline{A_i}$.

Next, let $x \in \bigcap\limits_{i\in I} \overline{A_i}$. Then $x \in \overline{A_i}$ for each $i \in I$. This means $x \notin A_i$ for each $i \in I$. Then

$$x \notin \{x \mid x \in A_i \text{ for } \textit{some } i \in I\} = \bigcup_{i\in I} A_i. \tag{4.5.25}$$

Thus, $x \in \overline{\bigcup\limits_{i\in I} A_i}$, proving that $\bigcap\limits_{i\in I} \overline{A_i} \subseteq \overline{\bigcup\limits_{i\in I} A_i}$. We proved earlier that $\overline{\bigcup\limits_{i\in I} A_i} \subseteq \bigcap\limits_{i\in I} \overline{A_i}$. Therefore, the two sets must be equal.

The proof of $\overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i}$ proceeds in a similar manner, and is left as an exercise.

Proof 2

We shall prove $\overline{\bigcup_{i\in I} A_i} = \bigcap_{i\in I} \overline{A_i}$. We leave out the explanations for you to fill in:

$$\begin{aligned} x \in \overline{\bigcup_{i\in I} A_i} &\Leftrightarrow \overline{x \in \bigcup_{i\in I} A_i} \\ &\Leftrightarrow \overline{x \in A_i \text{ for some } i} \\ &\Leftrightarrow x \notin A_i \text{ for all } i \\ &\Leftrightarrow x \in \overline{A_i} \text{ for all } i \\ &\Leftrightarrow x \in \bigcap_{i\in I} \overline{A_i}. \end{aligned}$$

The proof of $\overline{\bigcap_{i\in I} A_i} = \bigcup_{i\in I} \overline{A_i}$ is left as an exercise.

Partitions of Sets

Definition: Mutually Disjoint

Sets $A_1, A_2, A_3, \ldots$ are **mutually disjoint** (or **pairwise disjoint**) if and only if no two sets with distinct subscripts have any elements in common.

Specifically, for all $j = 1, 2, 3, \ldots$

$$A_i \cap A_j = \emptyset \text{ whenever } i \neq j. \tag{4.5.26}$$

Definition: Partition

A finite or infinite collection of non-empty sets $\{A_1, A_2, A_3, \ldots\}$ is a **partition** of set A if and only if

(1) A is the union of all the A_i.

(2) The sets $\{A_1, A_2, A_3, \ldots\}$ are mutually disjoint.

Example 4.5.8

Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Which of the following collections of sets are a partition of set S?

(a) $A = \{A_1, A_2\}$ with $A_1 = \{1, 3, 5, 7, 9\}, A_2 = \{2, 4, 6, 8, 10\}$

(b) $B = \{B_1, B_2, B_3\}$ with $B_1 = \{1, 2, 3, 4, 5, 6, 9\}, B_2 = \{7\}, B_3 = \{8, 9, 10\}$

(c) $C = \{C_1, C_2, C_3, C_4\}$ with $C_1 = \{8, 10\}, C_2 = \{3\}, C_3 = \{1, 4, 9\}, C_4 = \{2, 5, 6, 7\}$,

(d) $D = \{D_1, D_2, D_3, D_4\}$ with $D_1 = \{1\}, D_2 = \{2\}, D_3 = \{3\}, D_4 = \{4\}, D_5 = \{5, 6, 7, 8, 9, 10\}$,

(e) $E = \{E_1, E_2\}$ with $E_1 = \{1, 3, 5, 7, 9\}, E_2 = \{0, 2, 4, 6, 8, 10\}$

(f) $F = \{F_1, F_2, F_3\}$ with $F_1 = \{1, 2, 3, 4\}, F_2 = \{5, 6, 7\}, F_3 = \{9, 10\}$

Solution

(a), (c) & (d)

Summary and Review

- When dealing with arbitrary intersection or union of intervals, first identify the endpoints, then analyze the sets involved in the operation to determine whether an endpoint should be included or excluded.
- Intersection and union can be performed on a group of similar sets identified by subscripts belonging to an index set.
- Consequently, intersection or union can be formed by naming a specific index set.
- A collection of sets can be a partition of a set if it satisfies two conditions.

Exercises

Exercise 4.5.1

For each $n \in \mathbb{Z}^+$, define $A_n = \left(-\frac{1}{n}, 2n\right)$. Find $\bigcap_{n=1}^{\infty} A_n$ and $\bigcup_{n=1}^{\infty} A_n$.

Answer

$$\bigcap_{n=1}^{\infty} A_n = (0, 2), \bigcup_{n=1}^{\infty} A_n = (-1, \infty).$$

Exercise 4.5.2

For each $n \in \mathbb{Z}^+$, define $B_n = \{m \in \mathbb{Z} \mid -\frac{n}{2} \leq m \leq 3n\}$. Evaluate $\bigcap_{n=1}^{\infty} B_n$ and $\bigcup_{n=1}^{\infty} B_n$.

Exercise 4.5.3

Define $C_n = \{n, n+1, n+2, \ldots, 2n+1\}$ for each integer $n \geq 0$. Evaluate $\bigcap_{n=0}^{\infty} C_n$ and $\bigcup_{n=0}^{\infty} C_n$.

Answer

$$\bigcap_{n=0}^{\infty} C_n = \emptyset, \bigcup_{n=0}^{\infty} C_n = \mathbb{N} \cup \{0\}.$$

Exercise 4.5.4

For each $n \in I = \{1, 2, 3, \ldots, 100\}$, define $D_n = [-n, 2n] \cap \mathbb{Z}$. Evaluate $\bigcap_{n \in I} D_n$ and $\bigcup_{n \in I} D_n$.

Exercise 4.5.5

For each $n \in \mathbb{N}$, define $E_n = \{-n, -n+1, -n+2, \ldots, n^2\}$. Evaluate $\bigcap_{n \in \mathbb{N}} E_n$ and $\bigcup_{n \in \mathbb{N}} E_n$.

Answer

$$\bigcap_{n \in \mathbb{N}} E_n = E_1 = \{-1, 0, 1\}, \bigcup_{n \in \mathbb{N}} E_n = \mathbb{Z}.$$

Exercise 4.5.6

For each $n \in \mathbb{N}$, define $F_n = \left\{\frac{m}{n} \mid m \in \mathbb{Z}\right\}$. Evaluate $\bigcap_{n \in \mathbb{N}} F_n$ and $\bigcup_{n \in \mathbb{N}} F_n$.

Exercise 4.5.7

Let $I=(0,1)$, and define $A_i=\left[1,\frac{1}{i}\right]$ for each $i\in I$. For instance $A_{0.5}=[1,2]$ and $A_{\frac{\pi}{4}}=\left[1,\frac{4}{\pi}\right]$. Evaluate $\bigcup_{i\in I}A_i$ and $\bigcap_{i\in I}A_i$.

Answer

$\bigcup_{i\in I}A_i=[1,\infty), \bigcap_{i\in I}A_i=\{1\}$.

Exercise 4.5.8

Define $I=(0,1)$, and for each $i\in I$, let $B_i=(-i,\frac{1}{i})$. Evaluate $\bigcup_{i\in I}B_i=(-1,\infty)$ and $\bigcap_{i\in I}B_i$.

Exercise 4.5.9

Evaluate $\bigcap_{x\in(1,2)}(1-2x,x^2)$ and $\bigcup_{x\in(1,2)}(1-2x,x^2)$.

Answer

$\bigcap_{x\in(1,2)}(1-2x,x^2)=[-1,1]$, $\bigcup_{x\in(1,2)}(1-2x,x^2)=(-3.4)$.

Exercise 4.5.10

Evaluate $\bigcap_{x\in(0,1)}\left(x,\frac{1}{x}\right)$ and $\bigcup_{x\in(0,1)}\left(x,\frac{1}{x}\right)$.

Exercise 4.5.11

Let the universal set be $\mathbb{R}^2$. For each $r\in(0,\infty)$, define

$$A_r=\{(x,y)\mid y=rx^2\}; \tag{4.5.27}$$

that is, A_r is the set of points on the parabola $y=rx^2$, where $r>0$. Evaluate $\bigcap_{r\in(0,\infty)}A_r$ and $\bigcup_{r\in(0,\infty)}A_r$.

Answer

$\bigcap_{r\in(0,\infty)}A_r=\{(0,0)\}$, $\bigcup_{r\in(0,\infty)}A_r=\mathbb{R}^*\times\mathbb{R}^+\cup\{(0,0)\}$.

Exercise 4.5.12

Prove that $\overline{\bigcap_{i\in I}A_i}=\bigcup_{i\in I}\overline{A_i}$ for any nonempty index set I.

Exercise 4.5.13

Let $A_i=[-\frac{1}{i},5i]$ for $i\in\mathbb{Z}^+$.
Find:
(a) $A_1=$ (b) $A_3=$ (c) $A_6=$

Answer

(a) $A_1=[-1,5]$ (b) $A_3=[-\frac{1}{3},15]$ (c) $A_6=[-\frac{1}{6},30]$

Exercise 4.5.14

Let $A_i = [-\frac{1}{i}, 5i]$ for $i \in \mathbb{Z}^+$.

Find:

(a) $\bigcup_{i=1}^{n} A_i =$ $\qquad (b) \bigcap_{i=1}^{n} A_i =$

Exercise 4.5.15

Let $B_i = (0, \frac{1}{i})$ for $i \in \mathbb{Z}^+$.

Find:

(a) $B_1 =$ $\quad (b)\ B_3 = \quad (c)\ B_6 =$

Answer

(a) $B_1 = (0, 1)$ $\qquad (b)\ B_3 = (0, \frac{1}{3}) \qquad (c)\ A_6 = (0, \frac{1}{6})$

Exercise 4.5.16

Let $B_i = (0, \frac{1}{i})$ for $i \in \mathbb{Z}^+$.

Find:

(a) $\bigcup_{i=1}^{n} B_i =$ $\qquad (b) \bigcap_{i=1}^{n} B_i =$

(c) $\bigcup_{i=1}^{\infty} B_i =$ $\qquad (d) \bigcap_{i=1}^{\infty} B_i =$

CHAPTER OVERVIEW

5: Functions

5.1: Intro to Relations and Functions

Relations

Given two nonempty sets A and B, we are often interested in some sort of relationship between the elements from these two sets. A familiar example is the equality of two numbers. By saying $a = b$, we are proclaiming that the two numbers a and b are related by being equal in value. Likewise, $a \geq b$ is another example of a relation.

Example 5.1.1

Given $a, b \in \mathbb{R}^*$, declare a and b to be related if they have the same sign. For instance, 7.14 and e are related, so are $-\pi$ and $-\sqrt{2}$. However, 5 and -2 are not. Note that a is related to b implies that b is also related to a.

Example 5.1.2

For $a, b \in \mathbb{R}$, define "a is related to b" if and only if $a < b$. Take note that $3 < 5$, but $5 \not< 3$. This demonstrates that a is related to b does not necessarily imply that b is also related to a.

Example 5.1.3

Let A be a set of students, and let B be a set of courses. Given $a \in A$ and $b \in B$, define "a is related to b" if and only if student a is taking course b. While it could be possible that "John Smith is related to MATH 210" because John is taking MATH 210, it is certainly absurd to say that "MATH 210 is related to John Smith," because it does not make much sense to say that MATH 210 is taking John Smith. This again illustrates that a is related to b does not necessarily imply that b is also related to a.

In these examples, we see that when we say "a is related to b," the order in which a and b appear may make a difference. This suggests the following definition.

Definition

A ***relation*** from a set A to a set B is a subset of $A \times B$. Hence, a relation R consists of ordered pairs (a, b), where $a \in A$ and $b \in B$. If $(a, b) \in R$, we say that ***is related to*** , and we also write $a\,R\,b$.

Remark

We can also replace R by a symbol, especially when one is readily available. This is exactly what we do in, for example, $a < b$. To say it is not true that $a < b$, we can write $a \not< b$. Likewise, if $(a, b) \notin R$, then a is not related to b, and we could write $a \not R\, b$.

Since a relation is a set, we can describe a relation by listing its elements (that is, using the roster method).

Example 5.1.4

Let $A = \{1, 2, 3, 4, 5, 6\}$and $B = \{1, 2, 3, 4\}$. Define $(a, b) \in R$ if and only if $(a - b) \bmod 2 = 0$. Then

$$R = \{(1,1), (1,3), (2,2), (2,4), (3,1), (3,3), (4,2), (4,4), (5,1), (5,3), (6,2), (6,4)\}. \tag{5.1.1}$$

We note that R consists of ordered pairs (a, b) where a and b have the same parity. Be cautious, that $1 \leq a \leq 6$ and $1 \leq b \leq 4$. Hence, it is meaningless to talk about whether $(1, 5) \in R$ or $(1, 5) \notin R$.

hands-on Exercise 5.1.1

Let $A = \{2, 3, 4, 7\}$ and $B = \{1, 2, 3, \ldots, 12\}$. Define $a\,S\,b$ if and only if $a \mid b$. Use the roster method to describe S.

In the last example, 7 never appears as the first element (in the first coordinate) of any ordered pair. Likewise, 1, 5, 7, and 11 never appear as the second element (in the second coordinate) of any ordered pair.

Functions

The functions we studied in calculus are real functions, which are defined over a set of real numbers, and the results they produce are also real. In this chapter, we shall study their generalization over other sets. The definition could be difficult to grasp at the beginning, so we would start with a brief introduction.

Most students view real functions as computational devices. However, in the generalization, functions are not restricted to computation only. A better way to look at functions is their input-output relationship. Let f denote a function. Given an element (which need not be a number), we call the result from f the ***image under f***, and write $f(x)$, which is read as "f of x."

Imagine f as a machine. It takes the input value x, and returns $f(x)$ as the output value. This input-output relationship is depicted in Figure 6.1 in two different ways.

Figure 6.1: Two pictorial views of a function as a machine.

The question is: how could we obtain $f(x)$? A function need not involve any computation. Consequently, we cannot speak of "computing" the value of $f(x)$. Instead, we talk about what is the rule we follow to obtain $f(x)$. This rule can be described in many forms. We can, of course, use a computational rule. But a table, an algorithm, or even a verbal description also work as well.

Domain & Codomain

When we say a real function is defined over the real numbers, we mean the input values must be real numbers. The output values are also real numbers. In general, the input and output values need not be of the same type. The ***nearest integer function***, denoted $[x]$, rounds the real number x to the nearest integer. Here, the images (the output values) are integers. Consequently, we need to distinguish the set of input values from the set of possible output values. We call them the ***domain*** and the ***codomain***, respectively, of the function.

Example 5.1.5

When a professor reports the final letter grades for the students in her class, we can regard this as a function g. The domain is the set of students in her class, and the codomain could be the set of letter grades $\{A, B, C, D, F\}$.

Range & ONTO

We said the codomain is the set of *possible* output values, because not every element in the codomain needs to appear as the image of some element from the domain. If no student fails the professor's class in Example 5.1.5, no one will receive the final grade F. The collection of the images (the final letter grades) form a subset of the codomain. We call this subset the ***range*** of the function g. The range of a function can be a *proper* subset of the codomain. Hence, the codomain of a function is different from the set of its images. If the range of a function does equal to the codomain, we say that the function is ***onto***.

Definition: Range

The set of all images of a function is called the **range.**

Note: the range will be a subset of the codomain.

Example 5.1.6

For the nearest integer function $h(x) = [x]$, the domain is $\mathbb{R}$. The codomain is $\mathbb{Z}$, and the range is also $\mathbb{Z}$. Hence, the nearest integer function is onto.

Example 5.1.7

Let x be a real number. The ***greatest integer function*** $\lfloor x \rfloor$ returns the greatest integer less than or equal to x. For example,

$$\lfloor \sqrt{50} \rfloor = 7, \qquad \lfloor -6.34 \rfloor = -7, \qquad \text{and} \qquad \lfloor 15 \rfloor = 15. \tag{5.1.2}$$

Therefore, $\lfloor x \rfloor$ returns x if it is an integer, otherwise, it rounds x *down* to the next closest integer. Hence, it is also called the ***floor function*** of x. It is clear that its domain is $\mathbb{R}$, and the codomain and range are both $\mathbb{Z}$.

hands-on exercise 5.1.2

Let x be a real number. The ***least integer function*** $\lceil x \rceil$ returns the least integer greater than or equal to x. For example,

$$\lceil\sqrt{50}\,\rceil = 8, \qquad \lceil -6.34\rceil = -6, \qquad \text{and} \qquad \lceil 15\rceil = 15. \tag{5.1.3}$$

Thus, $\lceil x\rceil$ returns x if it is an integer, otherwise, it rounds x *up* to the next closest integer. Hence, it is also called the ***ceiling function*** of x. What is its domain and codomain?

We impose two restrictions on the input-output relationships that we call functions. For any fixed input value x, the output from a function must be the same every time we use the function. As a machine, it spits out the same answer every time we feed the same value x to it. As a calculator, it displays the same answer on its screen every time we enter the same value x, and push the button for the function. We call the output value the image of x, and write $f(x)$. The first important requirement for a function f is: the image $f(x)$ is *unique* for any fixed x-value.

A good machine must perform properly. In terms of a function f, we must be able to obtain $f(x)$ for any value x (and, of course, produce only one result for each x). This is perhaps a little bit too demanding. A remedy is to restrict our attention to those x's over which f would work. The set of legitimate input values is precisely what we call the domain of the function. Consequently, the second requirement says: for every element x from the domain, the output value $f(x)$ should be well-defined. This is the mathematical way of saying that the value $f(x)$ can be obtained, or the value $f(x)$ exists.

Example 5.1.8

Compare this to a calculator. If you enter a negative number and press the $\sqrt{\;}$ button, an error message will appear. To be able to compute the square root of a number, the number must be nonnegative. The domain of a function is the set of acceptable input values for which meaningful results can be found. For the square root function, the domain is $\mathbb{R}^+\cup\{0\}$, which is the set of nonnegative real numbers.

hands-on exercise 5.1.3

For the square root function, we may regard its codomain as $\mathbb{R}$. What is its range? Is the function onto?

hands-on exercise 5.1.4

For the square root function, can we say its domain is $\mathbb{R}^+\cup 0$? Explain.

The two conditions or requirements for a relation to be a function:

- every element in the domain has an image under f, and
- the image is unique.

In the next section, we shall present the complete formal definition.

Summary and Review

- Relations are generalizations of functions. A relation merely states that the elements from two sets A and B are related in a certain way.
- More formally, a relation is defined as a subset of $A\times B$. The domain is the set of elements in A and the codomain is the set of elements in B.
- The range of a relation is the set of elements in B that appear in the second coordinates of some ordered pairs.
- For brevity and for clarity, we often write $x\,R\,y$ if $(x,y)\in R$.
- Under this convention, the mathematical notations $\leq$, $\geq$, $=$, $\subseteq$, and their like, can be regarded as relational operators.
- A function is a rule that assigns to every element in the domain a unique image in the codomain.

Exercises

Exercise 5.1.1

Determine the arrow diagram that represents the relation R defined on $\{x\in\mathbb{Z}\mid -3\leq x\leq 3\}$ by

$$x\,R\,y \Leftrightarrow 3\mid(x-y). \tag{5.1.4}$$

Exercise 5.1.2

Determine the arrow diagram that represents the relation S defined on $\{1,2,4,5,10,20\}$by

$$x\,S\,y \Leftrightarrow (x < y \text{ and } x \text{ divides } y). \tag{5.1.5}$$

Exercise 5.1.3

Let $D = \{1, 2, 3, \ldots, 30\}$ be the set of dates in November, and let $W = \{$Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday$\}$ be the set of days of the week. For November of this year, define the relation T from D to W by

$$(x, y) \in T \Leftrightarrow x \text{ falls on } y. \tag{5.1.6}$$

List the ordered pairs in T. Is T a function from T to W?

Exercise 5.1.4

Let $\mathbb{R}$ be the domain and the codomain of the cube root function. Is it onto?

Exercise 5.1.5

For the square root function, how would you use the interval notation to describe the domain?

Answer

$[0, \infty)$

Exercise 5.1.6

Let $\mathbb{R}$ be the domain and the codomain of the absolute value function? Is it onto?

Exercise 5.1.7

Is the greatest integer function (or floor) from $\mathbb{R}$ to $\mathbb{Z}$ onto? Explain.

Answer

Yes, every integer will be the image of some real number input.
More specifically, let y be any integer. $\lfloor y \rfloor = y$, so for each $y \in \mathbb{Z}, \exists x \in \mathbb{R}$ (namely choose $x = y)(\lfloor x \rfloor = y)$.

Exercise 5.1.8

(a) $f : \mathbb{Z} \to \mathbb{Z}$ by the rule $f(x) = 3x$. Is f onto? Explain completely.

(b) $g : \mathbb{Z} \to \mathbb{Z}$ by the rule $g(x) = x^3$. Is g onto? Explain completely

Exercise 5.1.9

(a) $h : \mathbb{R} \to \mathbb{R}$ by the rule $h(x) = 3x$. Is h onto? Explain completely.

(b) $k : \mathbb{R} \to \mathbb{R}$ by the rule $k(x) = x^2$. Is k onto? Explain completely

Answer

(a) Yes. Let y be any real number. Choose $x = \frac{1}{3}y$. $x \in \mathbb{R}$ since the real numbers are closed under multiplication. Now, $h(x) = h(\frac{1}{3}y) = 3(\frac{1}{3}y) = y$. Thus every real number has a pre-image, and therefore h is onto.
(b) No. Consider $y = -25$. If y has a pre-image under k then there exists a real number, x such that $x^2 = -25$. Then $x = \sqrt{-25}$; however, $\sqrt{-25}$ is not a real number, hence $y = -25$ does not have a pre-image under k in the real numbers.

5.2: Definition of Functions

Definition: Function

Let A and B be nonempty sets. A ***function*** from A to B is a rule that assigns to *every element* of A a *unique* element in B. We call A the ***domain***, and B the ***codomain***, of the function. If the function is called f, we write $f:A\to B$. Given $x\in A$, its associated element in B is called its ***image*** under f. In other words, a function is a relation from A to B with the condition that for every element in the domain, there exists a unique image in the codomain (this is really two conditions: existence of an image and uniqueness of an image). We denote it $f(x)$, which is pronounced as " f of x."

A function is sometimes called a ***map*** or ***mapping***. Hence, we sometimes say f ***maps*** x to its image $f(x)$.

Example 5.2.1

The function $f:\{a,b,c\}$ to $\{1,3,5,9\}$is defined according to the rule

$$f(a)=1, \qquad f(b)=5, \qquad \text{and} \qquad f(c)=9. \tag{5.2.1}$$

It is a well-defined function. The rule of assignment can be summarized in a table:

x	a	b	c
$f(x)$	1	5	9

(5.2.2)

We can also describe the assignment rule pictorially with an ***arrow diagram***, as shown in Figure 6.2.

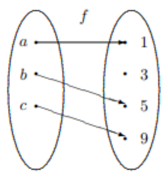


Figure 6.2: An example of a well-defined function.

The two key requirements of a function are

- every element in the domain has an image under f, and
- the image is unique.

You may want to remember that every element in A has exactly one "partner" in B.

Example 5.2.2

Figure 6.3 depicts two examples of non-functions. In the one on the left, one of the elements in the domain has no image associated with it; thus lacking existence of an image. In the one on the right, one of the elements in the domain has two images assigned to it; thus lacking uniqueness of an image. Both are not functions.

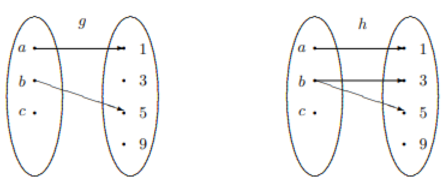


Figure 6.3: Two types of non-functions.

hands-on exercise 5.2.1

Do these rules

x	a	b	c
$f(x)$	5	3	3

x	b	c
$g(x)$	9	5

x	a	b	b	c
$h(x)$	1	5	3	9

(5.2.3)

produce functions from $\{a,b,c\}$ to $\{1,3,5,9\}$? Explain.

hands-on exercise 5.2.2

Does the definition

$$r(x) = \begin{cases} x & \text{if today is Monday,} \\ 2x & \text{if today is not Monday} \end{cases} \tag{5.2.4}$$

produce a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.

hands-on exercise 5.2.3

Does the definition

$$s(x) = \begin{cases} 5 & \text{if } x < 2, \\ 7 & \text{if } x > 3, \end{cases} \tag{5.2.5}$$

produce a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.

Example 5.2.3

The function $f:[0,\infty) \to \mathbb{R}$ is defined by

$$f(x) = \sqrt{x}. \tag{5.2.6}$$

Also the function $g:[2,\infty) \to \mathbb{R}$ is defined as

$$g(x) = \sqrt{x-2}. \tag{5.2.7}$$

Can you explain why the domain of g is $[2,\infty)$?

Example 5.2.4

Let A denote the set of students taking Discrete Mathematics, and $G=\{A,B,C,D,F\}$, and $\ell(x)$ is the final grade of student x in Discrete Mathematics. Every student should receive a final grade, and the instructor has to report one and only one final grade for each student. $\ell: A \to G$. This is precisely what we call a function.

Example 5.2.5

The function $n: \mathscr{P}(\{a,b,c,d\}) \to \mathbb{Z}$ is defined as $n(S)=|S|$. It evaluates the cardinality of a subset of $\{a,b,c,d\}$. For example,

$$n\big(\{a,c\}\big) = n\big(\{b,d\}\big) = 2. \tag{5.2.8}$$

Note that $n(\emptyset)=0$.

hands-on exercise 5.2.4

Consider Example 5.2.5. What other subsets S of $\{a,b,c,d\}$ also yield $n(S)=2$? What are the smallest and the largest images the function n can produce?

Example 5.2.6

Consider a function $f:\mathbb{Z}_7 \to \mathbb{Z}_5$. The domain and the codomain are,

$$\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}, \qquad \text{and} \qquad \mathbb{Z}_5 = \{0,1,2,3,4\}, \tag{5.2.9}$$

respectively. Not only are their elements different, their binary operations are different too. In the domain $\mathbb{Z}_7$, the arithmetic is performed modulo 7, but the arithmetic in the codomain $\mathbb{Z}_5$ is done modulo 5. So we need to be careful in describing the rule of assignment if a computation is involved. We could say, for example,

$$f(x)=z, \quad \text{where } z \equiv 3x \pmod 5. \tag{5.2.10}$$

Consequently, starting with any element x in $\mathbb{Z}_7$, we consider x as an ordinary integer, multiply by 3, and reduce the answer modulo 5 to obtain the image $f(x)$. For brevity, we shall write

$$f(x) \equiv 3x \pmod 5. \tag{5.2.11}$$

We summarize the images in the following table:

n	0	1	2	3	4	5	6
$f(n)$	0	3	1	4	2	0	3

(5.2.12)

Take note that the images start repeating after $f(4)=2$.

hands-on exercise 5.2.5

Tabulate the images of $g:\mathbb{Z}_{10} \to \mathbb{Z}_5$ defined by

$$g(x) \equiv 3x \pmod 5. \tag{5.2.13}$$

Definition: A Function as a Set of Ordered Pairs

A function $f: A \to B$ can be written as a set of ordered pairs (x,y) from $A \times B$ such that $y=f(x)$.

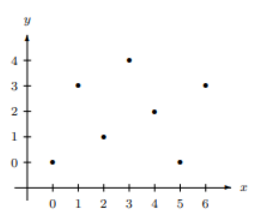
A function is, by definition, a set of *ordered pairs*, with certain restrictions.

Example 5.2.7

The function f in Example 5.26 can be written as the set of ordered pairs

$$\{(0,0),(1,3),(2,1),(3,4),(4,2),(5,0),(6,3)\}. \tag{5.2.14}$$

If one insists, we could display the graph of a function using an xy-plane that resembles the usual Cartesian plane. Keep in mind: the elements x and y come from A and B, respectively. We can "plot" the graph for f in Example 5.26 as shown below.



Besides using a graphical representation, we can also use a $(0,1)$-matrix. A $(0,1)$-matrix is a matrix whose entries are 0 and 1. For the function f, we use a 7×5 matrix, whose rows and columns correspond to the elements of A and B, respectively, and put one in the (i,j)th entry if $j=f(i)$, and zero otherwise. The resulting matrix is

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \tag{5.2.15}$$

We call it the ***incidence matrix*** for the function f.

hands-on exercise 5.2.6

"Plot" the graph of g in Hands-On Exercise 5.2.5

Summary and Review

- A function f from a set A to a set B (called the domain and the codomain, respectively) is a rule that describes how a value in the codomain B is assigned to an element from the domain A.
- But it is not just any rule; rather, the rule must assign to every element x in the domain a unique value in the codomain.
- This unique value is called the image of x under the function f, and is denoted $f(x)$.
- We use the notation $f : A \to B$ to indicate that the name of the function is f, the domain is A, and the codomain is B.
- A function $f : A \to B$ is the collection of all ordered pairs (x, y) from $A \times B$ such that $y = f(x)$.
- The graph of a function may not be a curve, as in the case of a real function. It can be just a collection of points.
- We can also display the images of a function in a table, or represent the function with an incidence matrix.

Exercises

exercise 5.2.1

What subset A of $\mathbb{R}$ would you use to make $f : A \to \mathbb{R}$ defined by $f(x) = \sqrt{3x-7}$ a function?

Answer

$\left[\frac{7}{3}, \infty\right)$

exercise 5.2.2

What subset A of $\mathbb{R}$ would you use to make

a. $g : A \to \mathbb{R}$, where $g(x) = \sqrt{(x-3)(x-7)}$
b. $h : A \to \mathbb{R}$, where $h(x) = \frac{x+2}{\sqrt{(x-2)(5-x)}}$

functions?

exercise 5.2.3

Which of these data support a function from $\{1,2,3,4\}$ to $\{1,2,3,4\}$? Explain.

x	1	2	3
$f(x)$	3	4	2

x	1	2	3	4
$g(x)$	2	4	3	2

x	1	2	3	3	4
$h(x)$	2	4	3	2	3

(5.2.16)

Answer

Only g is a function. The image $f(4)$ is undefined, and there are two values for $h(3)$. Hence, both f and h are not well-defined functions.

exercise 5.2.4

(a) Use arrow diagrams to show three different functions from $\{1,2,3,4\}$ to $\{1,2,3,4\}$.
(b) How many different functions from $\{1,2,3,4\}$ to $\{1,2,3,4\}$ are possible?

exercise 5.2.5

Determine whether these are functions. Explain.

a. $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = \frac{3}{x^2+5}$.
b. $g : (5, \infty) \to \mathbb{R}$, where $g(x) = \frac{7}{\sqrt{x-4}}$.
c. $h : \mathbb{R} \to \mathbb{R}$, where $h(x) = -\sqrt{7-4x+4x^2}$.

Answer

(a) Yes, because no division by zero will ever occur.

exercise 5.2.6

Determine whether these are functions. Explain.

a. $s : \mathbb{R} \to \mathbb{R}$, where $x^2 + [s(x)]^2 = 9$.
b. $t : \mathbb{R} \to \mathbb{R}$, where $|x - t(x)| = 4$.

exercise 5.2.7

Use arrow diagrams to show two different functions from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5, 6\}$

Answer

answers will vary

exercise 5.2.8

Let T be your family tree that includes your biological mother, your maternal grandmother, your maternal great-grandmother, and so on, and all of their female descendants. Determine which of the following define a function from T to T.

a. $h_1 : T \to T$, where $h_1(x)$ is the mother of x.
b. $h_2 : T \to T$, where $h_2(x)$ is x's sister.
c. $h_3 : T \to T$, where $h_3(x)$ is an aunt of x.
d. $h_4 : T \to T$, where $h_4(x)$ is the eldest daughter of x's maternal grandmother.

exercise 5.2.9

For each of the following functions, determine the image of the given x.

a. $k_1 : \mathbb{N} - \{1\} \to \mathbb{N}$, $k_1(x) =$ smallest prime factor of x , $x = 217$.
b. $k_2 : \mathbb{Z}_{11} \to \mathbb{Z}_{11}$, $k_2(x) \equiv 3x$ (mod 11), $x = 6$.
c. $k_3 : \mathbb{Z}_{15} \to \mathbb{Z}_{15}$, $k_3(x) \equiv 3x$ (mod 15), $x = 6$.

Answer

(a) 7 (b) 7 (c) 3

exercise 5.2.10

For each of the following functions, determine the images of the given x-values.

- $\ell_1 : \mathbb{Z} \to \mathbb{Z}$, $\ell_1(x) = x \bmod 7$, $x = 250$, $x = 0$, and $x = -16$.

Remark: Recall that, without parentheses, the notation "mod" means the binary operation mod.

$\ell_2 : \mathbb{Z} \to \mathbb{Z}$, $\ell_2(x) = \gcd(x, 24)$, $x = 100$, $x = 0$, and $x = -21$.

5.3: One-to-One Functions

We distinguish two special families of functions: one-to-one functions and onto functions. We shall discuss one-to-one functions in this section. Onto functions were introduced in section 5.2 and will be developed more in section 5.4.

One-to-One (Injective)

Recall that under a function each value in the domain has a unique image in the range. For a one-to-one function, we add the requirement that each image in the range has a unique pre-image in the domain.

Definition: One-to-One (Injection)

A function $f:A\to B$ is said to be ***one-to-one*** if

$$f(x_1)=f(x_2)\Rightarrow x_1=x_2 \tag{5.3.1}$$

for all elements $x_1,x_2\in A$. A one-to-one function is also called an ***injection***, and we call a function ***injective*** if it is one-to-one. A function that is not one-to-one is referred to as ***many-to-one***.

The contrapositive of this definition is: A function $f:A\to B$ is ***one-to-one*** if

$$x_1\neq x_2\Rightarrow f(x_1)\neq f(x_2) \tag{5.3.2}$$

Any function is either one-to-one or many-to-one. A function cannot be one-to-many because no element can have multiple images. The difference between one-to-one and many-to-one functions is whether there exist distinct elements that share the same image. There are no repeated images in a one-to-one function.

Definition: Identity Function

The ***identity function*** on any nonempty set A

$$I_A:A\to A,\qquad I_A(x)=x, \tag{5.3.3}$$

maps any element back to itself.

It is clear that all identity functions are one-to-one.

Example 5.3.1

The function $h:A\to A$ defined by $h(x)=c$ for some fixed element $c\in A$, is an example of a ***constant function***. It is a function with only one image. This is the exact opposite of an identity function. It is clearly *not* one-to-one unless $|A|=1$.

For domains with a small number of elements, one can use inspection on the images to determine if the function is one-to-one. This becomes impossible if the domain contains a larger number of elements.

In practice, it is easier to use the *contrapositive* of the definition to test whether a function is one-to-one:

$$f(x_1)=f(x_2)\Rightarrow x_1=x_2 \tag{5.3.4}$$

To prove a function is One-to-One

To prove $f:A\to B$ is one-to-one:

- Assume $f(x_1)=f(x_2)$
- Show it must be true that $x_1=x_2$
- Conclude: we have shown if $f(x_1)=f(x_2)$ then $x_1=x_2$, therefore f is one-to-one, by definition of one-to-one.

Example 5.3.2

Prove the function $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=3x+2$ is one-to-one.

Solution

Assume $f(x_1) = f(x_2)$, which means $3x_1 + 2 = 3x_2 + 2$.
Thus $3x_1 = 3x_2$
so $x_1 = x_2$.
We have shown if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Therefore f is one-to-one, by definition of one-to-one.

Hands-on exercise 5.3.1

Prove the function $g: \mathbb{R} \to \mathbb{R}$ defined by $g(x) = 5 - 7x$ is one-to-one.

Hands-on exercise 5.3.2

Determine whether the function $h: [2, \infty) \to \mathbb{R}$ defined by $h(x) = \sqrt{x-2}$ is one-to-one.

Interestingly, sometimes we can use calculus to determine if a real function is one-to-one. A real function f is ***increasing*** if

$$x_1 < x_2 \Rightarrow f(x_1) < f(x_2), \tag{5.3.5}$$

and ***decreasing*** if

$$x_1 < x_2 \Rightarrow f(x_1) > f(x_2). \tag{5.3.6}$$

Obviously, both increasing and decreasing functions are one-to-one. From calculus, we know that

- A function is increasing over an open interval (a, b) if $f'(x) > 0$ for all $x \in (a, b)$.
- A function is decreasing over an open interval (a, b) if $f'(x) < 0$ for all $x \in (a, b)$.

Therefore, if the derivative of a function is always positive, or always negative, then the function must be one-to-one.

Example 5.3.4

The function $p: \mathbb{R} \to \mathbb{R}$ defined by

$$p(x) = 2x^3 - 5 \tag{5.3.7}$$

is one-to-one, because $p'(x) = 6x^2 > 0$ for any $x \in \mathbb{R}^*$. Likewise, the function $q: \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$ defined by

$$q(x) = \tan x \tag{5.3.8}$$

is also one-to-one, because $q'(x) = \sec^2 x > 0$ for any $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$.

Hands-on exercise 5.3.3

Use both methods to show that the function $k: (0, \infty) \to \mathbb{R}$ defined by $k(x) = \ln x$ is one-to-one.

To prove a function is NOT one-to-one

To prove $f: A \to B$ is NOT one-to-one:

- Exhibit one case (a counterexample) where $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.
- Conclude: we have shown there is a case where $x_1 \neq x_2$ and $f(x_1) = f(x_2)$, therefore f is NOT one-to-one.

Example 5.3.5

Prove the function $h: \mathbb{R} \to \mathbb{R}$ given by $h(x) = x^2$ is not one-to-one.

Solution

Consider $a = 3$ and $b = -3$. Clearly $a \neq b$. However, $h(3) = 9$ and $h(-3) = 9$ so $h(a) = h(b)$.
we have shown there is a case where $a \neq b$ and $h(a) = h(b)$, therefore h is NOT one-to-one.

Example 5.3.6

The function $f:\mathbb{Z}\to\mathbb{Z}$ defined by

$$f(n)=\begin{cases}\frac{n}{2} & \text{if } n \text{ is even}\\ \frac{n+1}{2} & \text{if } n \text{ is odd}\end{cases} \tag{5.3.9}$$

is not one-to-one, because, for example, $f(0)=f(-1)=0$. The function $g:\mathbb{Z}\to\mathbb{Z}$ defined by

$$g(n)=2n \tag{5.3.10}$$

is one-to-one, because if $g(n_1)=g(n_2)$, then $2n_1=2n_2$ implies that $n_1=n_2$.

hands-on exercise 5.3.4

Show that the function $h:\mathbb{Z}\to\mathbb{N}$ defined by

$$h(n)=\begin{cases}2n+1 & \text{if } n\geq 0,\\ -2n & \text{if } n<0,\end{cases} \tag{5.3.11}$$

is one-to-one.

Example 5.3.7

Let A be the set of all married individuals from a monogamous community who are neither divorced nor widowed. Then the function $s:A\to A$ defined by

$$s(x)=\text{ spouse of } x \tag{5.3.12}$$

is one-to-one. The reason is, it is impossible to have $x_1\neq x_2$ and yet $s(x_1)=s(x_2)$.

Summary and Review

- A function f is said to be one-to-one if $f(x_1)=f(x_2)\Rightarrow x_1=x_2$.
- No two images of a one-to-one function are the same.
- Know how to write a proof to show a function is one-to-one.
- To show that a function f is *not* one-to-one, all we need is to find two different x-values that produce the same image; that is, find $x_1\neq x_2$ such that $f(x_1)=f(x_2)$.

Exercises

Exercise 5.3.1

Which of the following functions are one-to-one? Explain.

(a) $f:\mathbb{R}\to\mathbb{R},\ f(x)=x^3-2x^2+1$.

(b) $g:[2,\infty)\to\mathbb{R},\ f(x)=x^3-2x^2+1$.

Solution

(a) No. For example, $f(0)=f(2)=1$
(b) Yes, since $g'(x)=3x^2-4x=x(3x-4)>0$ for $x>2$.

Exercise 5.3.2

Decide if this function is one-to-one or not. Then prove your conclusion.

$p:\mathbb{R}\to\mathbb{R},\ p(x)=|1-3x|$.

Exercise 5.3.3

Decide if this function is one-to-one or not. Then prove your conclusion.

$q: \mathbb{R} \to \mathbb{R}$, $q(x) = x^4$.

Solution

No. For example, $2 \neq -2$, but $q(2) = 16$ and $q(-2) = 16$.
We have shown a case where $x_1 \neq x_2$ and $q(x_1) = q(x_2)$, so q is NOT one-to-one.

Exercise 5.3.4

Decide if this function is one-to-one or not. Then prove your conclusion.

$f: \mathbb{R} \to \mathbb{R}$, $f(x) = 6 - 5x$.

Exercise 5.3.5

Determine which of the following are one-to-one functions.

a. $f: \mathbb{Z} \to \mathbb{Z}$; $f(n) = n^3 + 1$
b. $g: \mathbb{Q} \to \mathbb{Q}$; $g(x) = n^2$
c. $k: \mathbb{R} \to \mathbb{R}$; $k(x) = 5^x$

Solution

(a) One-to-one (b) Not one-to-one (c) One-to-one

Exercise 5.3.6

Determine which of the following are one-to-one functions and explain your answer.

a. $p: \mathscr{P}(\{1,2,3,\ldots,n\}) \to \{0,1,2,\ldots,n\}$; $p(S) = |S|$
b. $q: \mathscr{P}(\{1,2,3,\ldots,n\}) \to \mathscr{P}(\{1,2,3,\ldots,n\})$; $q(S) = \overline{S}$

Exercise 5.3.7

Determine which of the following functions are one-to-one.

a. $f_1: \{1,2,3,4,5\} \to \{a,b,c,d\}$; $f_1(1) = b$, $f_1(2) = c$, $f_1(3) = a$, $f_1(4) = a$, $f_1(5) = c$
b. $f_2: \{1,2,3,4\} \to \{a,b,c,d,e\}$; $f_2(1) = c$, $f_2(2) = b$, $f_2(3) = a$, $f_2(4) = d$

Solution

(a) Not one-to-one (b) One-to-one

Exercise 5.3.8

Determine which of the following functions are one-to-one.

a. $g_1: \{1,2,3,4,5\} \to \{a,b,c,d,e\}$; $g_1(1) = b$, $g_1(2) = b$, $g_1(3) = b$, $g_1(4) = a$, $g_1(5) = d$
b. $g_2: \{1,2,3,4,5\} \to \{a,b,c,d,e\}$; $g_2(1) = d$, $g_2(2) = b$, $g_2(3) = e$, $g_2(4) = a$, $g_2(5) = c$

Exercise 5.3.9

List all the one-to-one functions from $\{1,2\}$ to $\{a,b,c,d\}$.

Hint

List the images of each function.

Solution

There are twelve one-to-one functions from $\{1,2\}$ to $\{a,b,c,d\}$. The images of 1 and 2 under them are listed below.

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}
1	a	a	a	b	b	b	c	c	c	d	d	d
2	b	c	d	a	c	d	a	b	d	a	b	c

(5.3.13)

Exercise 5.3.10

Is it possible to find a one-to-one function from $\{1,2,3,4\}$to $\{1,2\}$? Explain.

Exercise 5.3.11

Determine which of the following functions are one-to-one.

a. $f:\mathbb{Z}_{10}\to\mathbb{Z}_{10}$; $h(n)\equiv 3n$ (mod 10).
b. $g:\mathbb{Z}_{10}\to\mathbb{Z}_{10}$; $g(n)\equiv 5n$ (mod 10).
c. $h:\mathbb{Z}_{36}\to\mathbb{Z}_{36}$; $h(n)\equiv 3n$ (mod 36).

Solution

(a) One-to-one (b) Not one-to-one (c) Not one-to-one

Exercise 5.3.12

Decide if this function is one-to-one or not. Then prove your conclusion.

$k:\mathbb{R}\to\mathbb{R}$ defined by $k(x)=3x^2-5$ is one-to-one.

Exercise 5.3.13

Decide if this function is one-to-one or not. Then prove your conclusion.

$f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=57$ is one-to-one.

Solution

No. For example, $8\neq 17$, but $f(8)=57$ and $f(17)=57$.
We have shown a case where $x_1\neq x_2$ and $f(x_1)=f(x_2)$, so f is NOT one-to-one.

Exercise 5.3.14

Give an example of a one-to-one function f from $\mathbb{N}$ to $\mathbb{N}$ that is not the identity function.

5.4: Onto Functions and Images/Preimages of Sets

One-to-one functions focus on the elements in the domain. We do not want any two of them sharing a common image. Onto functions focus on the codomain. We want to know if it contains elements not associated with any element in the domain.

Definition: ONTO (surjection)

A function $f : A \to B$ is ***onto*** if, for every element $b \in B$, there exists an element $a \in A$ such that

$$f(a) = b. \tag{5.4.1}$$

An onto function is also called a ***surjection***, and we say it is ***surjective***.

Example 5.4.1

The graph of the piecewise-defined functions $h : [1, 3] \to [2, 5]$ defined by

$$h(x) = \begin{cases} 3x - 1 & \text{if } 1 \leq x \leq 2, \\ -3x + 11 & \text{if } 2 < x \leq 3, \end{cases}$$

is displayed on the left in Figure 6.5. It is clearly onto, because, given any $y \in [2, 5]$, we can find at least one $x \in [1, 3]$ such that $h(x) = y$. Likewise, the function $k : [1, 3] \to [2, 5]$ defined by

$$k(x) = \begin{cases} 3x - 1 & \text{if } 1 \leq x \leq 2, \\ 5 & \text{if } 2 < x \leq 3, \end{cases}$$

is also onto. Its graph is displayed on the right of Figure 6.5.

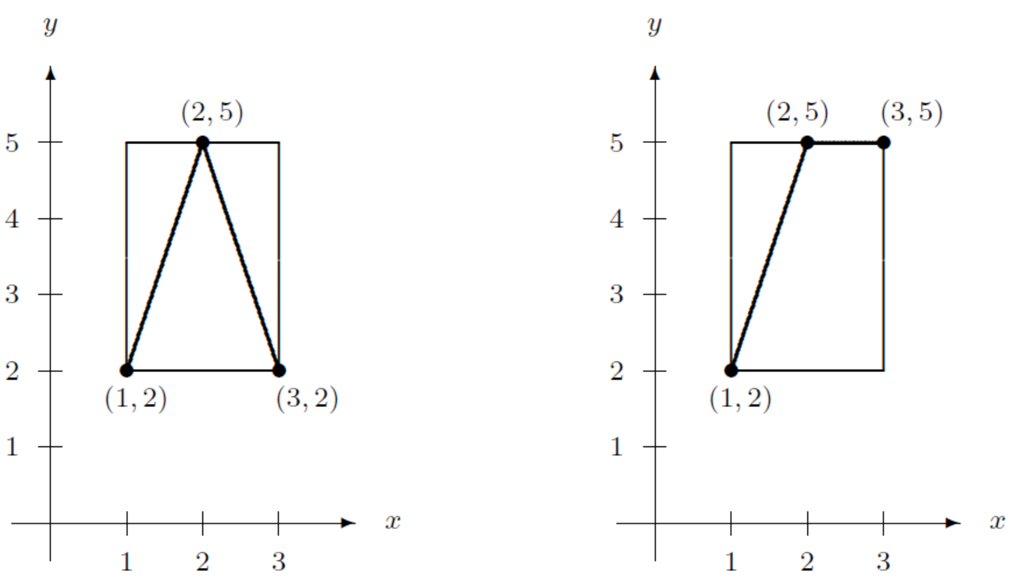


Figure 6.5: Two onto functions from $[1, 3]$ to $[2, 5]$.

Hands-on exercise 5.4.1

The two functions in Example 5.4.1 are onto but not one-to-one. Construct a one-to-one and onto function f from $[1, 3]$ to $[2, 5]$.

Hands-on exercise 5.4.2

Construct a function $g : [1, 3] \to [2, 5]$ that is one-to-one but not onto.

Hands-on exercise 5.4.3

Find a subset B of $\mathbb{R}$ that would make the function $s:\mathbb{R}\to B$ defined by $s(x)=x^2$ an onto function.

Example 5.4.2

Consider the function $g:\mathbb{R}\times\mathbb{R}\to\mathbb{R}$ defined by $g(x,y)=\frac{x+y}{2}$.

Is this function onto?

Remark

This function maps ordered pairs to a single real numbers. The image of an ordered pair is the average of the two coordinates of the ordered pair. To decide if this function is onto, we need to determine if every element in the codomain has a preimage in the domain.

Solution

Take any real number, $x\in\mathbb{R}$. Choose $(a,b)=(2x,0)$. $(a,b)\in\mathbb{R}\times\mathbb{R}$ since $2x\in\mathbb{R}$ because the real numbers are closed under multiplication and $0\in\mathbb{R}$. $g(a,b)=g(2x,0)=\frac{2x+0}{2}=x$. Thus, for any real number, we have shown a preimage $\mathbb{R}\times\mathbb{R}$ that maps to this real number. Therefore, this function is onto.

In general, how can we tell if a function $f:A\to B$ is onto? The key question is: given an element y in the codomain, is it the image of some element x in the domain? If it is, we must be able to find an element x in the domain such that $f(x)=y$. Mathematically, if the rule of assignment is in the form of a computation, then we need to solve the equation $y=f(x)$ for x. If we can *always* express x in terms of y, and if the resulting x-value is in the domain, the function is onto.

To prove a function is onto

For $f:A\to B$

- Let y be any element in the codomain, B.
- Figure out an element in the domain that is a preimage of y; often this involves some "scratch work" on the side.
- Choose $x=$ the value you found.
- Demonstrate x is indeed an element of the domain, A.
- Show $f(x)=y$.
- Conclude with: we have found a preimage in the domain for an arbitrary element of the codomain, so every element of the codomain has a preimage in the domain. Therefore f is onto, by definition of onto.

Example 5.4.3

The function $g:\mathbb{R}\to\mathbb{R}$ is defined as $g(x)=5x+11$. Prove that it is onto.

Scratch Work

We need to find an x that maps to y. Suppose $y=5x+11$; now we solve for x in terms of y. We find

$$x=\frac{y-11}{5}. \tag{5.4.2}$$

(We'll need to verify x is a real number - an element in the domain.)

That's the x we want to choose so that $g(x)=y$.

Now for the proof:

Proof

Let y be any element of $\mathbb{R}$.
Choose $x=\frac{y-11}{5}$.
Now, since the real numbers are closed under subtraction and non-zero division, $x\in\mathbb{R}$.

$g(x) = g(\frac{y-11}{5}) = 5(\frac{y-11}{5}) + 11 = y - 11 + 11 = y.$

Thus, we have found an $x \in \mathbb{R}$ such that $g(x) = y$.

So, given an arbitrary element of the codomain, we have shown a preimage in the domain.
Thus every element in the codomain has a preimage in the domain. Therefore, by the definition of onto, g is onto.

Hands-on exercise 5.4.4

Determine whether $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} 3x+1 & \text{if } x \leq 2 \\ 4x & \text{if } x > 2 \end{cases}$$

is an onto function.

Example 5.4.4

Is the function $u : \mathbb{Z} \to \mathbb{Z}$ defined by

$$u(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -n & \text{if } n < 0 \end{cases}$$

one-to-one? Is it onto?

Solution

Since $u(-2) = u(1) = 2$, the function u is not one-to-one. Since $u(n) \geq 0$ for any $n \in \mathbb{Z}$, the function u is not onto.

hands-on exercise 5.4.5

Is the function $v : \mathbb{N} \to \mathbb{N}$ defined by $v(n) = n + 1$ onto? Explain.

Images and Preimages of Sets

Definition: Image of a Set

Given a function $f : A \to B$, and $C \subseteq A$, the ***image of*** C ***under*** f is defined as

$$f(C) = \{f(x) \mid x \in C\}. \tag{5.4.3}$$

In words, $f(C)$ is the set of all the images of the elements of C.

A few remarks about the definition:

a. It is about the image of a *subset* C of the domain of A. Do not confuse it with the image of an *element* x from A.
b. Therefore, do not merely say “the image.” Be specific: the image of an element, or the image of a subset.
c. Better yet: include the notation $f(x)$ or $f(C)$ in the discussion.
d. While $f(x)$ is an *element* in the codomain, $f(C)$ is a *subset* of the codomain.
e. Perhaps, the most important thing to remember is:

If $y \in f(C)$, then $y \in B$, and there exists an $x \in C$
such that $f(x) = y$.

This key observation is often what we need to start a proof with.

Note:

Let $f : A \to B$ be a function. The ***image*** of set A is the ***range*** of f, which is the set of all possible images that f can assume.

Also, if the range of f is equal to B, then f is onto.

Example 5.4.5

For the function $f:\mathbb{R}\to\mathbb{R}$ defined by

$$f(x)=x^2,$$

we find the range of f is $[0,\infty)$. We also have, for example, $f\big([2,\infty)\big)=[4,\infty)$. It is clear that f is neither one-to-one nor onto.

Example 5.4.6

For the function $g:\mathbb{Z}\to\mathbb{Z}$ defined by

$$g(n)=n+3,$$

we find range of g is $\mathbb{Z}$, and $g(\mathbb{N})=\{4,5,6,\ldots\}$. The function g is both one-to-one and onto.

Example 5.4.7

Determine $f(\{(0,2),(1,3)\})$ where the function $f:\{0,1,2\}\times\{0,1,2,3\}\to\mathbb{Z}$ is defined according to

$$f(a,b)=a+b.$$

Remark: Strictly speaking, we should write $f((a,b))$ because the argument is an ordered pair of the form (a,b). However, we often write $f(a,b)$, because f can be viewed as a two-variable function. The first variable comes from $\{0,1,2\}$, the second comes from $\{0,1,2,3\}$, and we add them to form the image. Notice we are asked for the image of a set with two elements.

Solution

Because

$$f(0,2)=0+2=2,\qquad \text{and}\qquad f(1,3)=1+3=4, \tag{5.4.4}$$

we determine that $f(\{(0,2),(1,3)\})=\{2,4\}$a Set

Definition: Preimage of a Set

Given a function $f:A\to B$, and $D\subseteq B$, the *preimage* D *of under* f is defined as

$$f^{-1}(D)=\{x\in A\mid f(x)\in D\}. \tag{5.4.5}$$

Hence, $f^{-1}(D)$ is the set of elements in the domain whose images are in C. The symbol $f^{-1}(D)$ is also pronounced as "f inverse of D."

Some remarks about the definition:

a. The preimage of D is a subset of the domain A.

b. In particular, the preimage of B is always A.

c. The key thing to remember is:

> If $x\in f^{-1}(D)$, then $x\in A$, and $f(x)\in D$.

d. It is possible that $f^{-1}(D)=\emptyset$ for some subset D. If this happens, f is not onto.

e. Therefore, f is onto if and only if $f^{-1}(\{b\})\neq\emptyset$ for every $b\in B$.

Example 5.4.8

If $t:\mathbb{R}\to\mathbb{R}$ is defined by $t(x)=x^2-5x+5$, find $t^{-1}(\{-1\})$.

Solution

We want to find x such that $t(x)=x^2-5x+5=-1$. Hence, we have to solve the equation

$$0=x^2-5x+6=(x-2)(x-3).$$

The solutions are $x=2$ and $x=3$. Therefore, $t^{-1}(\{-1\})=\{2,3\}$.

hands-on Exercise 5.4.6

If $k:\mathbb{Q}\to\mathbb{R}$ is defined by $k(x)=x^2-x-7$, find $k^{-1}(\{3\})$.

Example 5.4.9

For the function $f:\{0,1,2\}\times\{0,1,2,3\}\to\mathbb{Z}$ defined by

$$f(a,b)=a+b, \tag{5.4.6}$$

we find

$$\begin{aligned} f^{-1}(\{3\}) &= \{(0,3),(1,2),(2,1)\}, \\ f^{-1}(\{4\}) &= \{(1,3),(2,2)\}. \end{aligned}$$

Since preimages are sets, we need to write the answers in set notation.

Summary and Review

- A function $f:A\to B$ is onto if, for every element $b\in B$, there exists an element $a\in A$ such that $f(a)=b$.
- Know how to prove f is an onto function.
- To show that a function is *not* onto, all we need is to find an element $y\in B$, and show that no x-value from A would satisfy $f(x)=y$.
- In addition to finding images & preimages of elements, we also find images & preimages of sets.
- Given a function $f:A\to B$, the image of $C\subseteq A$ is defined as $f(C)=\{f(x)\mid x\in C\}$.
    - If $y\in f(C)$, then $y\in B$, and there exists an $x\in C$ such that $f(x)=y$.
- The preimage of $D\subseteq B$ is defined as $f^{-1}(D)=\{x\in A\mid f(x)\in D\}$.
    - If $x\in f^{-1}(D)$, then $x\in A$, and $f(x)\in D$.

Exercises

exercise 5.4.1

Determine which of the following are onto functions.

a. $f:\mathbb{Z}\to\mathbb{Z}$; $f(n)=n^3+1$
b. $g:\mathbb{Q}\to\mathbb{Q}$; $g(x)=n^2$
c. $h:\mathbb{R}\to\mathbb{R}$; $h(x)=x^3-x$
d. $k:\mathbb{R}\to\mathbb{R}$; $k(x)=5^x$

Solution

(a) Not onto (b) Not onto (c) Onto (d) Not onto .

exercise 5.4.2

Determine which of the following are onto functions.

a. $p:\mathscr{P}(\{1,2,3,\ldots,n\})\to\{0,1,2,\ldots,n\}$; $p(S)=|S|$
b. $q:\mathscr{P}(\{1,2,3,\ldots,n\})\to\mathscr{P}(\{1,2,3,\ldots,n\})$; $q(S)=\overline{S}$

exercise 5.4.3

Determine which of the following functions are onto.

a. $f_1 : \{1,2,3,4,5\} \to \{a,b,c,d\}$; $f_1(1) = b$, $f_1(2) = c$, $f_1(3) = a$, $f_1(4) = a$, $f_1(5) = c$
b. $f_2 : \{1,2,3,4\} \to \{a,b,c,d,e\}$; $f_2(1) = c$, $f_2(2) = b$, $f_2(3) = a$, $f_2(4) = d$
c. $f_3 : \mathbb{Z} \to \mathbb{Z}$; $f_3(n) = -n$

Solution

f_1 and f_2 are not onto, f_3 is onto.

exercise 5.4.4

Determine which of the following functions are onto.

a. $g_1 : \{1,2,3,4,5\} \to \{a,b,c,d,e\}$; $g_1(1) = b$, $g_1(2) = b$, $g_1(3) = b$, $g_1(4) = a$, $g_1(5) = d$
b. $g_2 : \{1,2,3,4,5\} \to \{a,b,c,d,e\}$; $g_2(1) = d$, $g_2(2) = b$, $g_2(3) = e$, $g_2(4) = a$, $g_2(5) = c$

Exercise 5.4.5

Is it possible for a function from $\{1,2\}$ to $\{a,b,c,d\}$ to be onto? Explain.

Answer

No, because we have at most two distinct images, but the codomain has four elements.

exercise 5.4.6

List all the onto functions from $\{1,2,3,4\}$to $\{a,b\}$?

Hint

List the images of each function.

exercise 5.4.7

Determine which of the following functions are onto.

a. $f : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$; $h(n) \equiv 3n$ (mod 10).
b. $g : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$; $g(n) \equiv 5n$ (mod 10).
c. $h : \mathbb{Z}_{36} \to \mathbb{Z}_{36}$; $h(n) \equiv 3n$ (mod 36).

Solution

(a) Onto (b) Not onto (c) Not onto

exercise 5.4.8

Determine which of the following functions are onto.

a. $r : \mathbb{Z}_{36} \to \mathbb{Z}_{36}$; $r(n) \equiv 5n$ (mod 36).
b. $s : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$; $s(n) \equiv n + 5$ (mod 10).
c. $t : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$; $t(n) \equiv 3n + 5$ (mod 10).

exercise 5.4.9

Given a function $f : A \to B$, and $C \subset A$, since $f(C)$ is a subset of B, the preimage of this subset is indicated by the notation $f^{-1}(f(C))$. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$, and $C = \{0,1,2,3\}$.

(a) Find $f(C)$.

(b) Find $f^{-1}(f(C))$.

Solution

(a) $f(C) = \{0, 2, 4, 9\}$
(b) $f^{-1}(f(C)) = \{-3, -2, -1, 0, 1, 2, 3\}$

exercise 5.4.10

Give an example of a function $f : \mathbb{N} \to \mathbb{N}$ that is

a. neither one-to-one nor onto
b. one-to-one but not onto
c. onto but not one-to-one
d. both one-to-one and onto

Exercise 5.4.11

For each of the following functions, find the image of C, and the preimage of D.

(a) $f_1 : \{1, 2, 3, 4, 5\} \to \{a, b, c, d\}$; $f_1(1) = b$, $f_1(2) = c$, $f_1(3) = a$, $f_1(4) = a$, $f_1(5) = c$; $C = \{1, 3\}$, $D = \{a, c\}$.

(b) $f_2 : \{1, 2, 3, 4\} \to \{a, b, c, d, e\}$; $f_2(1) = c$, $f_2(2) = b$, $f_2(3) = a$, $f_2(4) = d$;$C = \{1, 3\}$, $D = \{b, d\}$.

(c) $f_3 : \{1, 2, 3, 4, 5\} \to \{a, b, c, d, e\}$; $f_3(1) = b$, $f_3(2) = b$, $f_3(3) = b$, $f_3(4) = a$, $f_3(5) = d$; $C = \{1, 3, 5\}$, $D = \{c\}$.

(d) $f_4 : \{1, 2, 3, 4, 5\} \to \{a, b, c, d, e\}$; $f_4(1) = d$, $f_4(2) = b$, $f_4(3) = e$, $f_4(4) = a$, $f_4(5) = c$; $C = \{3\}$, $D = \{c\}$.

Solution

(a) $f_1(C) = \{a, b\}$; $f_1^{-1}(D) = \{2, 3, 4, 5\}$
(b) $f_2(C) = \{a, c\}$; $f_2^{-1}(D) = \{2, 4\}$
(c) $f_3(C) = \{b, d\}$; $f_3^{-1}(D) = \emptyset$
(d) $f_4(C) = \{e\}$; $f_4^{-1}(D) = \{5\}$

Exercise 5.4.12

Define the $r : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$ according to $r(m, n) = 3^m 5^n$.

a. Find $r(\{1, 2, 3\} \times \{-1, 0, 1\})$
b. Find $r^{-1}\left(\left\{\frac{25}{27}\right\}\right)$.
c. Find $r^{-1}(D)$, where $D = \{3, 9, 27, 81, \ldots\}$

Exercise 5.4.13

The function $u : \mathbb{R} \to \mathbb{R}$ is defined as $u(x) = 3x + 11$, and the function $v : \mathbb{Z} \to \mathbb{R}$ is defined as $v(x) = 3x + 11$.

a. Find $u([3, 5))$ and $v(\{3, 4, 5\})$.
b. Find $u^{-1}((2, 7])$ and $v^{-1}((2, 7])$.

Solution

(a) $u([3, 5)) = [20, 26]$and $v(\{3, 4, 5\}) = \{20, 23, 26\}$
(b) $u^{-1}((2, 7]) = (-3, -\frac{4}{3}]$ and $v^{-1}((2, 7] = \{-2\})$.

Exercise 5.4.14

Is the function $h : \mathbb{Z} \to \mathbb{Z}$ defined by

$$h(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -n & \text{if } n < 0 \end{cases} \tag{5.4.7}$$

one-to-one? Is it onto?

Exercise 5.4.15

The function $f:\mathbb{R}\times\mathbb{R}\to\mathbb{R}\times\mathbb{R}$ is defined as $f(x,y)=(x+y,3y)$.

(a) Find $f(3,4)$, $f(-2,5)$, $f(2,0)$.

(b) Is f onto?

(c) Is f one-to-one?

Answer

(a) $f(3,4)=(7,12)$, $f(-2,5)=(3,15)$, $f(2,0)=(2,0)$.

(b) Consider any (a,b) in the codomain. Let $(x,y)=(a-\frac{b}{3},\frac{b}{3})$. Since $\mathbb{R}$ is closed under subtraction and non-zero division, $a-\frac{b}{3}\in\mathbb{R}$ and $\frac{b}{3}\in\mathbb{R}$, thus $(x,y)\in\mathbb{R}\times\mathbb{R}$.

Then $f(x,y)=f(a-\frac{b}{3},\frac{b}{3})=(a,b)$. So, every element in the codomain has a preimage in the domain and thus f is onto.

(c) Yes, if $f(x_1,y_1)=f(x_2,y_2)$ then $(x_1+y_1,3y_1)=(x_2+y_2,3y_2)$. This means $3y_1=3y_2$ and (dividing by 3) $y_1=y_2$.

Now, since $x_1+y_1=x_2+y_2$, subtract equals, y_1 and y_2 from both sides to get $x_1=x_2$. Because $x_1=x_2$ and $y_1=y_2$, we have $(x_1,y_1)=(x_2,y_2)$.

$f(x_1,y_1)=f(x_2,y_2)\to(x_1,y_1)=(x_2,y_2)$, so f is one-to-one.

5.5: Inverse Functions and Composition

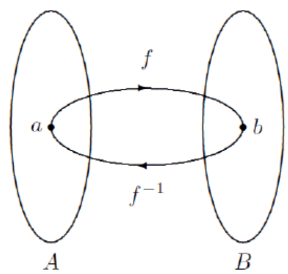
A ***bijection*** (or one-to-one correspondence) is a function that is both one-to-one and onto. Naturally, if a function is a bijection, we say that it is ***bijective***. If a function $f : A \to B$ is a bijection, we can define another function g that essentially reverses the assignment rule associated with f. Then, applying the function g to any element y from the codomain B, we are able to obtain an element x from the domain A such that $f(x) = y$. Let us refine this idea into a more concrete definition.

Definition: Inverse Function

Let $f : A \to B$ be a bijective function. Its *inverse function* is the function $f^{-1} : B \to A$ with the property that

$$f^{-1}(b) = a \Leftrightarrow b = f(a). \tag{5.5.1}$$

The notation f^{-1} is pronounced as "f inverse." See figure below for a pictorial view of an inverse function.



Why is $f^{-1} : B \to A$ a well-defined function? For it to be well-defined, every element $b \in B$ must have a unique image. This means given any element $b \in B$, we must be able to find one and only one element $a \in A$ such that $f(a) = b$. Such an a exists, because f is onto, and there is only one such element a because f is one-to-one. Therefore, f^{-1} is a well-defined function.

How to find f^{-1}

If a function f is defined by a computational rule, then the input value x and the output value y are related by the equation $y = f(x)$. In an inverse function, the role of the input and output are switched. Therefore, we can find the inverse function f^{-1} by following these steps:

- $f^{-1}(y) = x \iff y = f(x)$, so write $y = f(x)$, using the function definition of $f(x)$.
- Solve for x. That is, express x in terms of y. The resulting expression is $f^{-1}(y)$.
- Be sure to write the final answer in the form $f^{-1}(y) = \ldots$. Do not forget to include the domain and the codomain, and describe them properly.

Example 5.5.1

To find the inverse function of $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$, we start with the equation $y = 2x + 1$. Solving for x, we find $x = \frac{1}{2}(y - 1)$. Therefore, the inverse function is

$$f^{-1} : \mathbb{R} \to \mathbb{R}, \qquad f^{-1}(y) = \frac{1}{2}(y - 1). \tag{5.5.2}$$

It is important to describe the domain and the codomain, because they may not be the same as the original function.

Example 5.5.2

The function $s : \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \to [-1, 1]$ defined by $s(x) = \sin x$ is a bijection. Its inverse function is

$$s^{-1} : [-1, 1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right], \qquad s^{-1}(y) = \arcsin y. \tag{5.5.3}$$

The function $\arcsin y$ is also written as $\sin^{-1} y$, which follows the same notation we use for inverse functions.

hands-on Exercise 5.5.1

The function $f:[-3,\infty)\to[0,\infty)$ is defined as $f(x)=\sqrt{x+3}$. Show that it is a bijection, and find its inverse function

hands-on Exercise 5.5.2

Find the inverse function of $g:\mathbb{R}\to(0,\infty)$ defined by $g(x)=e^x$.

Remark

Exercise caution with the notation. Assume the function $f:\mathbb{Z}\to\mathbb{Z}$ is a bijection. The notation $f^{-1}(3)$ means the image of 3 under the inverse function f^{-1}. If $f^{-1}(3)=5$, we know that $f(5)=3$. The notation $f^{-1}(\{3\})$ means the preimage of the set $\{3\}$. In this case, we find $f^{-1}(\{3\})=\{5\}$. The results are essentially the same *if the function is bijective*.

If a function $g:\mathbb{Z}\to\mathbb{Z}$ is many-to-one, then it does not have an inverse function. This makes the notation $g^{-1}(3)$ meaningless. Nonetheless, $g^{-1}(\{3\})$ is well-defined, because it means the preimage of $\{3\}$. If $g^{-1}(\{3\})=\{1,2,5\}$, we know $g(1)=g(2)=g(5)=3$.

In general, $f^{-1}(D)$ means the preimage of the subset D under the function f. Here, the function f can be any function. If f is a bijection, then $f^{-1}(D)$ can also mean the image of the subset D under the inverse function f^{-1}. There is no confusion here, because the results are the same.

Example 5.5.3

The function $f:\mathbb{R}\to\mathbb{R}$ is defined as

$$f(x)=\begin{cases}3x & \text{if } x\leq 1,\\ 2x+1 & \text{if } x>1.\end{cases} \tag{5.5.4}$$

Find its inverse function.

Solution

Since f is a piecewise-defined function, we expect its inverse function to be piecewise-defined as well. First, we need to find the two ranges of input values in f^{-1}. The images for $x\leq 1$ are $y\leq 3$, and the images for $x>1$ are $y>3$. Hence, the codomain of f, which becomes the domain of f^{-1}, is split into two halves at 3. The inverse function should look like

$$f^{-1}(x)=\begin{cases}??? & \text{if } x\leq 3,\\ ??? & \text{if } x>3.\end{cases} \tag{5.5.5}$$

Next, we determine the formulas in the two ranges. We find

$$f^{-1}(x)=\begin{cases}\frac{1}{3}x & \text{if } x\leq 3,\\ \frac{1}{2}(x-1) & \text{if } x>3.\end{cases} \tag{5.5.6}$$

The details are left to you as an exercise.

hands-on Exercise 5.5.3

Find the inverse function of $g:\mathbb{R}\to\mathbb{R}$ defined by

$$g(x)=\begin{cases}3x+5 & \text{if } x\leq 6,\\ 5x-7 & \text{if } x>6.\end{cases} \tag{5.5.7}$$

Be sure you describe g^{-1} properly.

Example 5.5.4

Find the inverse function of $f:\mathbb{Z}\to\mathbb{N}\cup\{0\}$ defined by

$$f(n)=\begin{cases} 2n & \text{if } n\geq 0, \\ -2n-1 & \text{if } n<0. \end{cases} \tag{5.5.8}$$

Solution

In an inverse function, the domain and the codomain are switched, so we have to start with $f^{-1}:\mathbb{N}\cup\{0\}\to\mathbb{Z}$ before we describe the formula that defines f^{-1}. Writing $n=f(m)$, we find

$$n=\begin{cases} 2m & \text{if } m\geq 0, \\ -2m-1 & \text{if } m<0. \end{cases} \tag{5.5.9}$$

We need to consider two cases.

If $n=2m$, then n is even, and $m=\frac{n}{2}$.

If $n=-2m-1$, then n is odd, and $m=-\frac{n+1}{2}$.

Therefore, the inverse function is defined by $f^{-1}:\mathbb{N}\cup\{0\}\to\mathbb{Z}$ by:

$$f^{-1}(n)=\begin{cases} \frac{2}{n} & \text{if } n \text{ is even}, \\ -\frac{n+1}{2} & \text{if } n \text{ is odd}. \end{cases} \tag{5.5.10}$$

Verify this with some numeric examples.

hands-on Exercise 5.5.5

The function $f:\mathbb{Z}\to\mathbb{N}$ is defined as

$$f(n)=\begin{cases} -2n & \text{if } n<0, \\ 2n+1 & \text{if } n\geq 0. \end{cases} \tag{5.5.11}$$

Find its inverse.

Let A and B be finite sets. If there exists a bijection $f:A\to B$, then the elements of A and B are in one-to-one correspondence via f. Hence, $|A|=|B|$. This idea will be very important for our section on Infinite Sets and Cardinality.

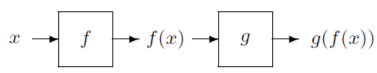
Composite Function

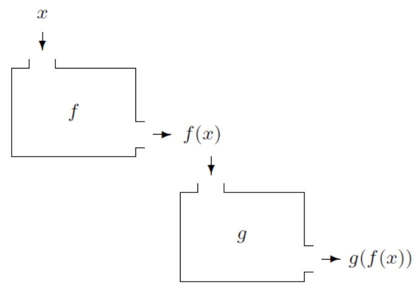
Given functions $f:A\to B'$ and $g:B\to C$ where $B'\subseteq B$, the ***composite function***, $g\circ f$, which is pronounced as "g after f", is defined as

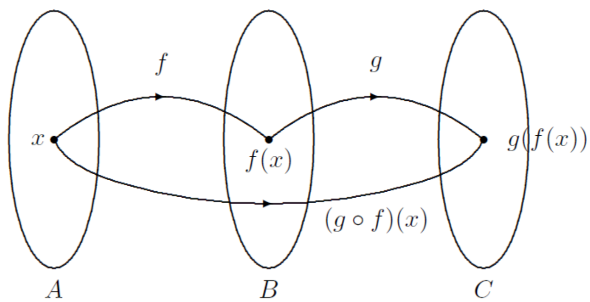
$$g\circ f:A\to C, \qquad (g\circ f)(x)=g(f(x)). \tag{5.5.12}$$

The image is obtained in two steps. First, $f(x)$ is obtained. Next, it is passed to g to obtain the final result. It works like connecting two machines to form a bigger one, see first figure below. We can also use an arrow diagram to provide another pictorial view, see second figure below.

Numeric value of $(g\circ f)(x)$ can be computed in two steps. For example, to compute $(g\circ f)(5)$, we first compute the value of $f(5)$, and then the value of $g(f(5))$. To find the algebraic description of $(g\circ f)(x)$, we need to compute and simplify the formula for $g(f(x))$. In this case, it is often easier to start from the "outside" function. More precisely, start with g, and write the intermediate answer in terms of $f(x)$, then substitute in the definition of $f(x)$ and simplify the result.







Example 5.5.5

Assume $f, g : \mathbb{R} \to \mathbb{R}$ are defined as $f(x) = x^2$, and $g(x) = 3x + 1$. We find

$$\begin{aligned}(g \circ f)(x) = g(f(x)) = 3[f(x)] + 1 = 3x^2 + 1, \\ (f \circ g)(x) = f(g(x)) = [g(x)]^2 = (3x+1)^2.\end{aligned} \tag{5.5.13}$$

Therefore,

$$g \circ f : \mathbb{R} \to \mathbb{R}, \qquad (g \circ f)(x) = 3x^2 + 1 \tag{5.5.14}$$

$$f \circ g : \mathbb{R} \to \mathbb{R}, \qquad (f \circ g)(x) = (3x+1)^2 \tag{5.5.15}$$

We note that, in general, $f \circ g \neq g \circ f$.

hands-on Exercise 5.5.6

If $p, q : \mathbb{R} \to \mathbb{R}$ are defined as $p(x) = 2x + 5$, and $q(x) = x^2 + 1$, determine $p \circ q$ and $q \circ p$. Do not forget to describe the domain and the codomain

Example 5.5.6

Define $f, g : \mathbb{R} \to \mathbb{R}$ as

$$f(x) = \begin{cases} 3x + 1 & \text{if } x < 0, \\ 2x + 5 & \text{if } x \geq 0, \end{cases} \tag{5.5.16}$$

and $g(x) = 5x - 7$. Find $g \circ f$.

Solution

Since f is a piecewise-defined function, we expect the composite function $g \circ f$ is also a piecewise-defined function. It is defined by

$$(g\circ f)(x) = g(f(x)) = 5f(x)-7 = \begin{cases} 5(3x+1)-7 & \text{if } x<0, \\ 5(2x+5)-7 & \text{if } x\geq 0. \end{cases} \tag{5.5.17}$$

After simplification, we find $g\circ f:\mathbb{R}\to\mathbb{R}$, by:

$$(g\circ f)(x) = \begin{cases} 15x-2 & \text{if } x<0, \\ 10x+18 & \text{if } x\geq 0. \end{cases} \tag{5.5.18}$$

In this example, it is rather obvious what the domain and codomain are. Nevertheless, it is always a good practice to include them when we describe a function.

hands-on Exercise 5.5.7

The functions $f:\mathbb{R}\to\mathbb{R}$ and $g:\mathbb{R}\to\mathbb{R}$ are defined by

$$f(x)=3x+2, \qquad \text{and} \qquad g(x) = \begin{cases} x^2 & \text{if } x\leq 5, \\ 2x-1 & \text{if } x>5. \end{cases} \tag{5.5.19}$$

Determine $f\circ g$

Example 5.5.7

Let $\mathbb{R}^*$ denote the set of nonzero real numbers. Suppose

$$f:\mathbb{R}^*\to\mathbb{R}, \qquad f(x)=\frac{1}{x} \tag{5.5.20}$$

$$g:\mathbb{R}\to(0,\infty), \qquad g(x)=3x^2+11. \tag{5.5.21}$$

Determine $f\circ g$ and $g\circ f$. Be sure to specify their domains and codomains.

Solution

To compute $f\circ g$, we start with g, whose domain is $\mathbb{R}$. Hence, $\mathbb{R}$ is the domain of $f\circ g$. The result from g is a number in $(0,\infty)$. The interval $(0,\infty)$ contains positive numbers only, so it is a subset of $\mathbb{R}^*$. Therefore, we can continue our computation with f, and the final result is a number in $\mathbb{R}$. Hence, the codomain of $f\circ g$ is $\mathbb{R}$. The image is computed according to $f(g(x)) = 1/g(x) = 1/(3x^2+11)$. We are now ready to present our answer:

$f\circ g:\mathbb{R}\to\mathbb{R}$, by:

$$(f\circ g)(x) = \frac{1}{3x^2+11}. \tag{5.5.22}$$

In a similar manner, the composite function $g\circ f:\mathbb{R}^*(0,\infty)$ is defined as

$$(g\circ f)(x) = \frac{3}{x^2}+11. \tag{5.5.23}$$

Be sure you understand how we determine the domain and codomain of $g\circ f$.

Identity Function relates to Inverse Functions

Recall the definition of the Identity Function:

The ***identity function*** on any nonempty set A maps any element back to itself:

$$I_A:A\to A, \qquad I_A(x)=x. \tag{5.5.24}$$

.

Theorem 5.5.1

For a bijective function $f:A\to B$,

$$f^{-1} \circ f = I_A, \qquad \text{and} \qquad f \circ f^{-1} = I_B, \tag{5.5.25}$$

where i_A and i_B denote the identity function on A and B, respectively.

Proof

To prove that $f^{-1} \circ f = I_A$, we need to show that $(f^{-1} \circ f)(a) = a$ for all $a \in A$. Assume $f(a) = b$. Then, because f^{-1} is the inverse function of f, we know that $f^{-1}(b) = a$. Therefore,

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a, \tag{5.5.26}$$

which is what we want to show. The proof of $f \circ f^{-1} = I_B$ procceds in the exact same manner, and is omitted here.

Example 5.5.8

Show that the functions $f, g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x+1$ and $g(x) = \frac{1}{2}(x-1)$ are inverse functions of each other.

Solution

The problem does not ask you to *find* the inverse function of f or the inverse function of g. Instead, the answers are given to you already. You job is to *verify* that the answers are indeed correct, that the functions are inverse functions of each other.

Form the two composite functions $f \circ g$ and $g \circ f$, and check whether they *both* equal to the identity function:

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) = 2g(x)+1 = 2\left[\tfrac{1}{2}(x-1)\right]+1 = x, \\ (g \circ f)(x) &= g(f(x)) = \tfrac{1}{2}\left[f(x)-1\right] = \tfrac{1}{2}[(2x+1)-1] = x. \end{aligned} \tag{5.5.27}$$

We conclude that f and g are inverse functions of each other.

hands-on Exercise 5.5.8

Verify that $f : \mathbb{R} \to \mathbb{R}^+$ defined by $f(x) = e^x$, and $g : \mathbb{R}^+ \to \mathbb{R}$ defined by $g(x) = \ln x$, are inverse functions of each other

Theorem 5.5.2

Suppose $f : A \to B$ and $g : B \to C$. Let I_A and I_B denote the identity function on A and B, respectively. We have the following results.

a. $f \circ I_A = f$ and $I_B \circ f = f$.
b. If both f and g are one-to-one, then $g \circ f$ is also one-to-one.
c. If both f and g are onto, then $g \circ f$ is also onto.
d. If $g \circ f$ is bijective, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof of (a)

To show that $f \circ I_A = f$, we need to show that $(f \circ I_A)(a) = f(a)$ for all $a \in A$. This follows from direct computation:

$$(f \circ I_A)(a) = f(I_A(a)) = f(a). \tag{5.5.28}$$

The proofs of $I_B \circ f = f$ and (b)–(d) are left as exercises.

Summary and Review

- A bijection is a function that is both one-to-one and onto.
- The inverse of a bijection $f : A \to B$ is the function $f^{-1} : B \to A$ with the property that

$$f(x) = y \Leftrightarrow x = f^{-1}(y). \tag{5.5.29}$$

- In brief, an inverse function reverses the assignment rule of f. It starts with an element y in the codomain of f, and recovers the element x in the domain of f such that $f(x) = y$.

- Given $B' \subseteq B$, the composition of two functions $f: A \to B'$ and $g: B \to C$ is the function $g \circ f: A \to C$ defined by $(g \circ f)(x) = g(f(x))$.
- If $f: A \to B$ is bijective, then $f^{-1} \circ f = I_A$ and $f \circ f^{-1} = I_B$.
- To check whether $f: A \to B$ and $g: B \to A$ are inverse of each other, we need to show that

a. $(g \circ f)(x) = g(f(x)) = x$ for all $x \in A$, *and*
b. $(f \circ g)(y) = f(g(y)) = y$ for all $y \in B$.

Exercises

Exercise 5.5.1

Find the inverse of each of the following bijections.

a. $u: \mathbb{Q} \to \mathbb{Q}$, $u(x) = 3x - 2$.
b. $v: \mathbb{Q} - \{1\} \to \mathbb{Q} - \{2\}$, $v(x) = \frac{2x}{x-1}$.
c. $w: \mathbb{Z} \to \mathbb{Z}$, $w(n) = n + 3$.

Solution

(a) $u^{-1}: \mathbb{Q} \to \mathbb{Q}$, $u^{-1}(x) = (x+2)/3$

Exercise 5.5.2

Find the inverse of the function $r: (0, \infty) \to \mathbb{R}$ defined by $r(x) = 4 + 3\ln x$.

Exercise 5.5.3

The images of the bijection $\alpha: \{1,2,3,4,5,6,7,8\} \to \{a,b,c,d,e,f,g,h\}$are given below.

x	1	2	3	4	5	6	7	8
$\alpha(x)$	g	a	d	h	b	e	f	c

(5.5.30)

Find its inverse function.

Solution

The images under $\alpha^{-1}: \{a,b,c,d,e,f,g,h\} \to \{1,2,3,4,5,6,7,8\}$are given below.

x	a	b	c	d	e	f	g	h
$\alpha^{-1}(x)$	2	5	8	3	6	7	1	4

(5.5.31)

Exercise 5.5.4

The function $h: (0, \infty) \to (0, \infty)$ is defined by $h(x) = x + \frac{1}{x}$. Determine $h \circ h$. Simplify your answer as much as possible.

Exercise 5.5.5

The functions $g, f: \mathbb{R} \to \mathbb{R}$ are defined by $f(x) = 1 - 3x$ and $g(x) = x^2 + 1$. Evaluate $f(g(f(0)))$.

Solution

We do not need to find the formula of the composite function, as we can evaluate the result directly: $f(g(f(0))) = f(g(1)) = f(2) = -5$.

Exercise 5.5.6

The functions $f, g: \mathbb{Z} \to \mathbb{Z}$ are defined by

$$f(n) = \begin{cases} 2n-1 & \text{if } n \geq 0 \\ 2n & \text{if } n < 0 \end{cases} \quad \text{and} \quad g(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ 3n & \text{if } n \text{ is odd} \end{cases} \tag{5.5.32}$$

Determine $g \circ f$

Exercise 5.5.7

Describe $g \circ f$.

a. $f : \mathbb{Z} \to \mathbb{N}$, $f(n) = n^2 + 1$; $g : \mathbb{N} \to \mathbb{Q}$, $g(n) = \frac{1}{n}$.
b. $f : \mathbb{R} \to (0,1)$, $f(x) = 1/(x^2+1)$; $g : (0,1) \to (0,1)$, $g(x) = 1 - x$.
c. $f : \mathbb{Q} - \{2\} \to \mathbb{Q}^*$, $f(x) = 1/(x-2)$; $g : \mathbb{Q}^* \to \mathbb{Q}^*$, $g(x) = 1/x$.
d. $f : \mathbb{R} \to [1, \infty)$,$f(x) = x^2 + 1$; $g : [1, \infty) \to [0, \infty)$ $g(x) = \sqrt{x-1}$.
e. $f : \mathbb{Q} - \{10/3\} \to \mathbb{Q} - \{3\}$,$f(x) = 3x - 7$; $g : \mathbb{Q} - \{3\} \to \mathbb{Q} - \{2\}$, $g(x) = 2x/(x-3)$.

Solution

(a) $g \circ f : \mathbb{Z} \to \mathbb{Q}$, $(g \circ f)(n) = 1/(n^2+1)$

(b) $g \circ f : \mathbb{R} \to (0,1)$, $(g \circ f)(x) = x^2/(x^2+1)$

Exercise 5.5.8

If $f : A \to B$ and $g : B \to C$ are functions and $g \circ f$ is one-to-one, must g be one-to-one? Prove or give a counter-example.

Exercise 5.5.9

If $f : A \to B$ and $g : B \to C$ are functions and $g \circ f$ is onto, must f be onto? Prove or give a counter-example.

Solution

No. Consider $f : \{2,3\} \to \{a,b,c\}$by $\{(2,a),(3,b)\}$and $g : \{a,b,c\} \to \{5\}$by $\{(a,5),(b,5),(c,5)\}$.
Then $f \circ g : \{2,3\} \to \{5\}$is defined by $\{(2,5),(3,5)\}$. Clearly $f \circ g$ is onto, while f is not onto.

Exercise 5.5.10

If $f : A \to B$ and $g : B \to C$ are functions and $g \circ f$ is one-to-one, must f be one-to-one? Prove or give a counter-example.

Exercise 5.5.11

If $f : A \to B$ and $g : B \to C$ are functions and $g \circ f$ is onto, must g be onto? Prove or give a counter-example.

Answer

Yes, if $f : A \to B$ and $g : B \to C$ are functions and $g \circ f$ is onto, then g must be onto.

Proof

If g is not onto, then $\exists c \in C$ such that there is no $b \in B$ such that $g(b) = c$.
However, since $g \circ f$ is onto, we know $\exists a \in A$ such that $(g \circ f)(a) = c$. This means $g(f(a)) = c$.
$f(a) \in B$ and $g(f(a)) = c$; let $b = f(a)$ and now there is a $b \in B$ such that $g(b) = c$.
Since every element in set C does have a pre-image in set B, by the definition of onto, g must be onto.

Exercise 5.5.12

Given the bijections f and g, find $f \circ g$, $(f \circ g)^{-1}$ and $g^{-1} \circ f^{-1}$.

a. $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n + 1$; $g : \mathbb{Z} \to \mathbb{Z}$, $g(n) = 2 - n$.
b. $f : \mathbb{Q} \to \mathbb{Q}$, $f(x) = 5x$; $g : \mathbb{Q} \to \mathbb{Q}$, $g(x) = \frac{x-2}{5}$.
c. $f : \mathbb{Q} - \{2\} \to \mathbb{Q} - \{2\}$, $f(x) = 3x - 4$; $g : \mathbb{Q} - \{2\} \to \mathbb{Q} - \{2\}$, $g(x) = \frac{x}{x-2}$.

Exercise 5.5.13

Prove part (b) of Theorem 5.5.2.

Statement of Theorem 5.5.2b

Given $f: A \to B$ and $g: B \to C$, if both f and g are one-to-one, then $g \circ f$ is also one-to-one.

Proof

Suppose $(g \circ f)(a_1) = (g \circ f)(a_2)$ for some $a_1, a_2 \in A$. WMST $a_1 = a_2$.
By definition of composition of functions, we have

$$g(f(a_1)) = g(f(a_2)). \tag{5.5.33}$$

$f(a_1) \in B$ and $f(a_2) \in B$. Let $b_1 = f(a_1)$ and $b_2 = f(a_2)$. Substituting into equation 5.5.3,

$$g(b_1) = g(b_2). \tag{5.5.34}$$

Since g is one-to-one, we know $b_1 = b_2$ by definition of one-to-one. Since $b_1 = b_2$ we have $f(a_1) = f(a_2)$.
Now, since f is one-to-one, we know $a_1 = a_2$ by definition of one-to-one.
Thus we have demonstrated if $(g \circ f)(a_1) = (g \circ f)(a_2)$ then $a_1 = a_2$ and therefore by the definition of one-to-one, $g \circ f$ is one-to-one.

Exercise 5.5.14

Prove part (c) of Theorem 5.5.2

Exercise 5.5.15

Prove part (d) of Theorem 5.5.

5.6: Infinite Sets and Cardinality

Preliminaries

$$\mathbb{N} = \{1, 2, 3, 4, \dots\} \text{ is the set of Natural Numbers, also known as the Counting Numbers.} \tag{5.6.1}$$

$\mathbb{N}$ is an infinite set and is the same as $\mathbb{Z}^+$.

In this section, we will see how the the Natural Numbers are used as a standard to test if an infinite set is "countably infinite".

$$\{1, 2, 3, \dots, n\} \text{ is a FINITE set of natural numbers from 1 to } n. \tag{5.6.2}$$

Recall: a one-to-one correspondence between two sets is a bijection from one of those sets to the other. A bijection is a function that is one-to-one and onto.

Finite Sets

Finite sets are either empty or have n elements. If a set has n elements, there exists a one-to-one correspondence with the set of natural numbers, $\{1, 2, 3, \dots, n\}$where $n \in \mathbb{N}$.

For example, $\{p, q, r\}$ can be put into a one-to-one correspondence with $\{1, 2, 3\}$. One such function is $p \to 1 \quad q \to 2 \quad r \to 3$.

If set S has n elements, then $|S| = n$. Also $|\emptyset| = 0$.

Infinite Sets

An infinite set is a non-empty set which cannot be put into a one-to-one correspondence with $\{1, 2, 3, \dots, n\}$for any $n \in \mathbb{N}$.

Cardinality

Cardinality is ***transitive*** (even for infinite sets).

$$\text{For all sets } A, B, C, \qquad \text{if } |A| = |B| \text{ and } |B| = |C| \text{ then } |A| = |C| \tag{5.6.3}$$

Same Cardinality

If set A and set B have the same cardinality, then there is a *one-to-one correspondence* from set A to set B.

For a finite set, the cardinality of the set is the number of elements in the set.

Example 5.6.1

Consider sets P and Q. $P = \{\text{olives, mushrooms, broccoli, tomatoes}\}$and $Q = \{\text{Jack, Queen, King, Ace}\}$.

Since $|P| = 4$ and $|Q| = 4$, they have the same cardinality and we can set up a one-to-one correspondence such as:

$$\text{olives} \to \text{Jack} \tag{5.6.4}$$

$$\text{mushrooms} \to \text{Ace} \tag{5.6.5}$$

$$\text{broccoli} \to \text{Queen} \tag{5.6.6}$$

$$\text{tomatoes} \to \text{King} \tag{5.6.7}$$

Theorem 5.6.1

An infinite set and one of its proper subsets could have the same cardinality.

An example:

The set of integers $\mathbb{Z}$ and its subset, set of even integers $E = \{\dots -4, -2, 0, 2, 4, \dots\}$.

The function $f:\mathbb{Z}\rightarrow E$ given by $f(n)=2n$ is one-to-one and onto.

So, even though $E\subset\mathbb{Z}$, $|E|=|\mathbb{Z}|$.

(This is an example, not a proof. It can be shown that this function is well-defined and a bijection.)

Countably and Uncountably Infinite

Countably Infinite

A set A is **countably infinite** if and only if set A has the same cardinality as $\mathbb{N}$ (the natural numbers).

If set A is **countably infinite**, then $|A|=|\mathbb{N}|$.

Furthermore, we designate the cardinality of countably infinite sets as $\aleph_0$ ("aleph null").

$|A|=|\mathbb{N}|=\aleph_0$.

Countable

A set is **countable** if and only if it is *finite* or *countably infinite*.

Uncountably Infinite

A set that is NOT countable is **uncountable** or **uncountably infinite.**

Example 5.6.2

$\mathbb{Z}$ is countable.

Initial thoughts

Thinking of how to match the natural numbers to the integers, I see how the even natural numbers could be used for the positive integers, like this:

$$2\rightarrow 1 \qquad 4\rightarrow 2 \qquad 6\rightarrow 3 \qquad 8\rightarrow 4 \qquad \text{etc.} \qquad \text{by } f(n)=\frac{n}{2}. \tag{5.6.8}$$

However, I realize zero will need a preimage, so I can adjust the function a bit:

$$2\rightarrow 0 \qquad 4\rightarrow 1 \qquad 6\rightarrow 2 \qquad 8\rightarrow 3 \qquad \text{etc.} \qquad \text{by } f(n)=\frac{n-2}{2}. \tag{5.6.9}$$

That takes care of the positive integers and zero.

For the negative integers, I need to use the odd natural numbers to get:

$$1\rightarrow -1 \qquad 3\rightarrow -2 \qquad 5\rightarrow -3 \qquad 7\rightarrow -4 \qquad \text{etc..} \tag{5.6.10}$$

Now I need to come up with a function to accomplish this mapping to the negative integers, and after some thinking, I come up with $f(n)=-\frac{n+1}{2}$.

These will need to fit together in a piece-wise function, with one piece if n is even and the other piece if n is odd.

Proof

Define $f:\mathbb{N}\to\mathbb{Z}$ by $f(n)=\begin{cases}\frac{n-2}{2} & \text{if } n \text{ is even}\\ -\frac{n+1}{2} & \text{if } n \text{ is odd}\end{cases}$

f is well-defined:

Case 1: n is even. $f(n)=\frac{n-2}{2}$ and since n is even, $n=2k$ for some integer k, by definition of even.
Now, $f(n)=\frac{2k-2}{2}=k-1$. Because the integers are closed under subtraction, $k-1\in\mathbb{Z}$ so $f(n)\in\mathbb{Z}$.

Case 2: n is odd. $f(n)=-\frac{n+1}{2}$ and since n is odd, $n=2j+1$ for some integer j, by definition of odd.
Now, $f(n)=-\frac{2j+1+1}{2}=-j-1$. Because the integers are closed under addition and multiplication, $-j-1\in\mathbb{Z}$ so $f(n)\in\mathbb{Z}$.

By the Parity Property, n must be either even or odd, so we have shown for all natural numbers n, $f(n)\in\mathbb{Z}$, thus f is well-defined.

f is one-to-one:

Let $f(x_1)=f(x_2)$ for some $x_1,x_2\in\mathbb{N}$. Since $f(x_1)=f(x_2)$, $f(x_1)$ and $f(x_2)$ are either both non-negative or both negative. If they are non-negative, then x_1 and x_2 are even and if they are negative, then x_1 and x_2 are odd.
Case 1: $f(x_1)$ and $f(x_2)$ are non-negative, x_1 and x_2 are even. $\frac{x_1-2}{2}=\frac{x_2-2}{2}$. Then $x_1-2=x_2-2$, so $x_1=x_2$ (by algebra).
Case 2: $f(x_1)$ and $f(x_2)$ are negative, x_1 and x_2 are odd. $-\frac{x_1+1}{2}=-\frac{x_2+1}{2}$. Then $x_1+1=x_2+1$, so $x_1=x_2$ (by algebra).
In both cases, if $f(x_1)=f(x_2)$ then $x_1=x_2$ and so, by definition of one-to-one, f is one-to-one.

f is onto:

Let $y\in\mathbb{Z}$. We must show there is an element in $\mathbb{N}$ whose image is y.
Case 1: y is non-negative; note: n is even. Choose $n=2y+2$. Since integers are closed under addition and multiplication, $2y+2$ is an integer. Furthermore, since $y\geq 0$, $2y\geq 0$ $2y+2>0$ so $2y+2\in\mathbb{Z}^+$. Thus $n\in\mathbb{N}$.
$f(n)=f(2y+2)=\frac{2y+2-2}{2}=y$.

Case 2: y is negative; note: n is odd. Choose $n=-2y-1$ Since integers are closed under subtraction and multiplication, $-2y-1$ is an integer. Furthermore, since $y<0$, $-2y>0$, $-2y-1>-1$. The smallest odd integer greater than -1 is 1 , thus $n\in\mathbb{N}$.
$f(n)=f(-2y-1)=-\frac{-2y-1+1}{2}=\frac{2y}{2}=y$.

By the Trichotomy Property, y is must be non-negative or negative, so we have shown for an arbitrary element y, of the codomain, there exists an element in $\mathbb{N}$ whose image is y and so, by definition of onto, f is onto.

Since f is a well-defined, one-to-one, onto function, we have demonstrated a one-to-one correspondence from $\mathbb{N}$ to $\mathbb{Z}$. Thus $|\mathbb{N}|=|\mathbb{Z}|$ and therefore the set of integers, $\mathbb{Z}$, is countable.

Theorem 5.6.2

Any subset of a countable set is countable.

If S is countably infinite and $A\subseteq S$ then A is countable.

Proof

If A is an finite set, then it is countable. Consider the case that A is an infinite subset of S. Since S is countably infinite, it can be enumerated: $S=\{x_0,x_1,x_2,\ldots\}$. Let n_i be the ith smallest index such that $x_{n_i}\in A$. Then $A=\{x_{n_0},x_{n_1},x_{n_2},\ldots\}$ and hence is countably infinite.

Corolary 5.6.3

A set with an uncountable subset is uncountable.

Theorem 5.6.4

$\mathbb{Q}$ is countable.

Sketch of a Proof

There is a nice proof you may have seen where all the fractions are listed in an endless matrix and it can be seen that a path can be drawn to cover all the fractions. This shows you can "line up" the rational numbers, and thus they can be "tagged" $1, 2, 3, 4, 5, \ldots$ and so the set is countable.

Theorem 5.6.5

$\mathbb{R}$ is uncountable.

Proof

We can show the set of real numbers in the interval $(0, 1)$ are uncountable as follows:
Suppose the real numbers in the interval $(0, 1)$ are countable. Then they can be written in a list, as the 1st, 2nd, etc.
Write this (infinite) list, and as it's written, we will create a number that is NOT on that list.
For example:
1st number: 0.345103592..... our number that we are creating 0.0
2nd number: 0.051023237..... our number that we are creating 0.00
3rd number: 0.840729312..... our number that we are creating 0.001
4th number: 0.859025839..... our number that we are creating 0.0011
5th number: 0.777888222..... our number that we are creating 0.00110
6th number: 0.001101111..... our number that we are creating 0.001100
7th number: 0.001100000..... our number that we are creating 0.0011001

Our scheme is to put a zero or a one in the i^{th} position depending on the digit in the i^{th} position of the i^{th} number in the list.
So, for the second number on the list, we see the second digit is a 5, and we choose a 0 for the second digit of our number being created.
So, for the third number on the list, we see the third digit is a 0, and we choose a 1 for the third digit of our number being created.
(We choose a 0 unless the digit we are comparing to is a 0 and then we choose a 1.)
Do you see that the number being created will never be on the list of real numbers?

More formally, if we describe the "wannabe" list of real numbers in the interval $(0, 1)$ using subscripts for each digit:

$0.a_{11}a_{12}a_{13}a_{14}a_{15}\ldots$
$0.a_{21}a_{22}a_{23}a_{24}a_{25}\ldots$
$0.a_{31}a_{32}a_{33}a_{34}a_{35}\ldots$
etc.

Then create $d_n = \begin{cases} 1 & \text{if } a_{nn} \neq 0 \\ 0 & \text{if } a_{nn} = 0 \end{cases}$
d is the created number which will never be on the list.
It is impossible to put all the real numbers in the interval $(0, 1)$ in a list (that number being created will always be left off the list), and thus that set of numbers is uncountable.

Since the interval $(0, 1)$ which is a subset of $\mathbb{R}$ is uncountable, then $\mathbb{R}$ is also uncountable (*Corollary 5.6.3*).

This proof is known as Cantor's Diagonalization Process. Georg Cantor was a pioneer in the field of different sizes of infinite sets.

Transfinite Numbers

As mentioned earlier, $\aleph_0$ is used to denote the cardinality of a countable set. Transfinite numbers are used to describe the cardinalities of "higher & higher" infinities.

$\aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$ cardinality of countably infinite sets.

$\aleph_1 = |\mathbb{R}| = |(0,1)| = |\mathscr{P}(\mathbb{N})|$ cardinality of the "lowest" uncountably infinite sets; also known as "cardinality of the continuum".

$\aleph_2 = |\mathscr{P}(\mathbb{R})| = |\mathscr{P}(\mathscr{P}(\mathbb{N}))|$ cardinality of the next uncountably infinite sets

From this we see that $2^{\aleph_0} = \aleph_1$.

Other strange math can be done with transfinite numbers such as $\aleph_1 + \aleph_0 = \aleph_1$.

The proof that a set cannot be mapped onto its power set is similar to the *Russell paradox*, named for Bertrand Russell.

The *continuum hypothesis* is the statement that there is no set whose cardinality is strictly between that of $\mathbb{N}$ and $\mathbb{R}$. The continuum hypothesis actually started out as the continuum *conjecture*, until it was shown to be consistent with the usual axioms of the real number system (by Kurt Gödel in 1940), and independent of those axioms (by Paul Cohen in 1963).

Summary and Review

- A bijection (one-to-one correspondence), a function that is both one-to-one and onto, is used to show two sets have the same cardinality.
- An infinite set that can be put into a one-to-one correspondence with $\mathbb{N}$ is countably infinite.
- Finite sets and countably infinite are called countable.
- An infinite set that cannot be put into a one-to-one correspondence with $\mathbb{N}$ is uncountably infinite.

- $\mathbb{Z}$ and $\mathbb{Q}$ are countably infinite sets.
- $\mathbb{R}$ is an uncountably infinite set.
- $|\mathbb{N}| = \aleph_0$
- $|\mathbb{R}| = \aleph_1$

Exercises

Exercise 5.6.1

Solution

Exercise 5.6.2

text needed

Exercise 5.6.3

text needed

Solution

text needed

Exercise 5.6.4

text needed

Exercise 5.6.5

text needed

Solution

text needed

Exercise 5.6.6

text needed

Exercise 5.6.7

text needed

Solution

text needed

Exercise 5.6.8

text needed

Exercise 5.6.9

text needed

Solution

text needed

Exercise 5.6.10

text needed

Exercise 5.6.11

text needed

Proof

text needed

Exercise 5.6.12

text needed

Exercise 5.6.13

text needed

Proof

text needed

Exercise 5.6.14

text needed

CHAPTER OVERVIEW

6: Relations

6.1: Relations on Sets

Definition: Relation

A ***relation*** from a set A to a set B is a subset of $A \times B$. Hence, a relation R consists of ordered pairs (a, b), where $a \in A$ and $b \in B$. If $(a, b) \in R$, we say that ***is related to*** , and we also write $a\,R\,b$.

Remark

We can also replace R by a symbol, especially when one is readily available. This is exactly what we do in, for example, $a < b$. To say it is not true that $a < b$, we can write $a \not< b$. Likewise, if $(a, b) \notin R$, then a is not related to b, and we could write $a \not R\, b$. But the slash may not be easy to recognize when it is written over an uppercase letter. In this regard, it may be a good practice to avoid using the slash notation over a letter. Alternatively, one may use the "bar" notation $\overline{a\,R\,b}$ to indicate that a and b are not related.

Example 6.1.1

Define $R = \{(a, b) \in \mathbb{R}^2 \mid a < b\}$, hence $(a, b) \in R$ if and only if $a < b$. Obviously, saying "$a < b$" is much clearer than "$a\,R\,b$." If a and b are not related, we could say $(a, b) \notin R$, or $a \not< b$.

Since a relation is a set, we can describe a relation by listing its elements (that is, using the roster method).

Example 6.1.2

Let $A = \{1, 2, 3, 4, 5, 6\}$and $B = \{1, 2, 3, 4\}$. Define $(a, b) \in R$ if and only if $(a - b) \bmod 2 = 0$. Then

$$R = \{(1, 1), (1, 3), (2, 2), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4), (5, 1), (5, 3), (6, 2), (6, 4)\}. \tag{6.1.1}$$

We note that R consists of ordered pairs (a, b) where a and b have the same parity. Be cautious, that $1 \leq a \leq 6$ and $1 \leq b \leq 4$. Hence, it is meaningless to talk about whether $(1, 5) \in R$ or $(1, 5) \notin R$.

hands-on Exercise 6.1.1

Let $A = \{2, 3, 4, 7\}$ and $B = \{1, 2, 3, \ldots, 12\}$. Define $a\,S\,b$ if and only if $a \mid b$. Use the roster method to describe S.

In the last example, 7 never appears as the first element (in the first coordinate) of any ordered pair. Likewise, 1, 5, 7, and 11 never appear as the second element (in the second coordinate) of any ordered pair.

Definition

The ***domain*** of a relation $R \subseteq A \times B$ is defined as

$$\text{domain of } R = \{a \in A \mid (a, b) \in R \text{ for some } b \in B\}, \tag{6.1.2}$$

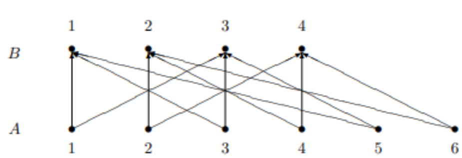
and the ***range*** is defined as

$$\text{range of } R = \{b \in B \mid (a, b) \in R \text{ for some } a \in A\}. \tag{6.1.3}$$

hands-on Exercise 6.1.5

Find domain of S and range of S, where S in Hands-On Exercise 1.

A relation $R \subseteq A \times B$ can be displayed graphically on an **arrow graph**, also called ***digraph*** (for ***directed graph***). Represent the elements from A and B by ***vertices*** or ***dots***, and use ***arrows*** (also called ***directed edges*** or ***arcs***) to connect two vertices if the corresponding elements are related. The figure below displays a graphical representation of the relation in Example 2.



hands-on Exercise 6.1.7

The courses taken by John, Mary, Paul, and Sally are listed below.

John:	MATH 211, CSIT 121, MATH 220
Mary:	MATH 230, CSIT 121, MATH 212
Paul:	CSIT 120, MATH 230, MATH 220
Sally:	MATH 211, CSIT 120

Represent, using an arrow graph, the relation R defined as $a\,R\,b$ if student a is taking course b.

Summary and Review

- Relations are generalizations of functions. A relation merely states that the elements from two sets A and B are related in a certain way.
- More formally, a relation is defined as a subset of $A \times B$.
- The domain of a relation is the set of elements in A that appear in the first coordinates of some ordered pairs, and the image or range is the set of elements in B that appear in the second coordinates of some ordered pairs.
- For brevity and for clarity, we often write $x\,R\,y$ if $(x, y) \in R$.
- Under this convention, the mathematical notations $\leq$, $\geq$, $=$, $\subseteq$, and their like, can be regarded as relational operators.

Exercises

Exercise 6.1.1

Let $A = \{A_1, A_2, A_3, A_4, A_5\}$ where $A_1 = \{1\}$ $\quad A_2 = \{5, 6, 7\}$ $\quad A_3 = \{1, 2, 3\}$ $\quad A_4 = \{4\}$ $\quad A_5 = \{10, 11\}$.

Define the relation R on the set A as $A_i\,R\,A_j$ iff $|A_i| \geq |A_j|$.

True or False?

(a) $A_2\,R\,A_3$

(b) $A_1\,R\,A_5$

(c) $A_3\,R\,A_5$

(d) $A_2\,R\,A_1$

(e) $A_5\,R\,A_2$

(f) $(A_1, A_3) \in R$

(g) $(A_1, A_4) \in R$

Solution

(a) True (b) False (c) True (d) True (e) False (f) False (g) True

Exercise 6.1.2

Let $A = \{A_1, A_2, A_3, A_4, A_5\}$ where $A_1 = \{1\}$ $\quad A_2 = \{5, 6, 7\}$ $\quad A_3 = \{1, 2, 3\}$ $\quad A_4 = \{4\}$ $\quad A_5 = \{10, 11\}$.

Define the relation R on the set A as $A_i\,R\,A_j$ iff $|A_i| \geq |A_j|$.

(a) List all the elements of A that are related to A_5.

(b) List all the elements of A that A_5 is related to

Exercise 6.1.3

Write out the relation R as a set of ordered pairs. $R : \mathscr{P}(\{1, 2\}) \to \mathscr{P}(\{1, 2\})$, where

$$(S,T) \in R \Leftrightarrow S \cap T = \emptyset. \tag{6.1.4}$$

Solution

$\{(\emptyset,\emptyset),(\emptyset,\{1\}),(\{1\},\emptyset),(\emptyset,\{2\}),(\{2\},\emptyset),(\emptyset,\{1,2\}),(\{1,2\},\emptyset),(\{1\},\{2\}),(\{2\},\{1\})\}$

Exercise 6.1.4

Represent each of the following relations from $\{1,2,3,6\}$to $\{1,2,3,6\}$using an arrow graph.

(a) $\{(x,y) \mid x = y\}$

(b) $\{(x,y) \mid x \neq y\}$

(c) $\{(x,y) \mid x < y\}$

Exercise 6.1.5

Find the domain and image of each relation in Problem Exercise 4.

Solution

(a) $\text{domain} = \text{range} = \{1,2,3,6\}$

(b) $\text{domain} = \text{range} = \{1,2,3,6\}$

(c) $\text{domain} = \{1,2,3\}$ $\text{range} = \{2,3,6\}$

Exercise 6.1.6

Represent each of the following relations from $\{1,2,3,6\}$to $\{1,2,3,6\}$using an arrow graph.

(a) $\{(x,y) \mid x^2 \leq y\}$

(b) $\{(x,y) \mid x \text{ divides } y\}$

(c) $\{(x,y) \mid x+y \text{ is even }\}$

Exercise 6.1.7

Find the domain and image of each relation in Problem 6.

Solution

(a) $\text{domain} = \{1,2\}$, $\text{range} = \{1,2,3,6\}$

(b) $\text{domain} = \text{range} = \{1,2,3,6\}$

(c) $\text{domain} = \text{range} = \{1,2,3,6\}$

Exercise 6.1.8

Create the arrow graph that represents the relation S defined on $\{1,2,4,5,10,20\}$by

$$x \, S \, y \Leftrightarrow (x < y \text{ and } x \text{ divides } y). \tag{6.1.5}$$

Exercise 6.1.9

Answer these questions about the relation S defined on $\{1, 2, 4, 5, 10, 20\}$by

$$x \, S \, y \Leftrightarrow (x < y \text{ and } x \text{ divides } y). \tag{6.1.6}$$

True or False?

(a) If $(x, y) \in S$, then $(y, x) \notin S$, for all $x, y \in S$.

(b) $(x, x) \in S$, for all $x \in S$.

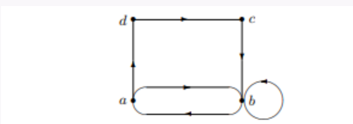
(c) If $(x, y) \in S$, and $(y, z) \in S$, then $(x, z) \in S$, for all $x, y, z \in S$.

Solution

(a) True (b) False (c) True

Exercise 6.1.10

For a relation $R \subseteq A \times A$, instead of using two rows of vertices in a digraph, we can use a digraph on the vertices that represent the elements of A. Hence, it is possible to have two directed arcs between a pair of vertices, and a loop may appear around a vertex x if $(x, x) \in R$. Write the set of ordered pairs for the relation represented by the following arrow diagram:



6.2: Properties of Relations

Note: If we say R is a relation "**on** set A" this means R is a relation from A to A; in other words, $R \subseteq A \times A$.

We will define three properties which a relation might have.

Definition: Reflexive Property

A relation R on A is **reflexive** if and only if for all $a \in A$, aRa.

example: consider $D : \mathbb{Z} \to \mathbb{Z}$ by $xDy \iff x|y$. Since $a|a$ for all $a \in \mathbb{Z}$ the relation D is reflexive.

Definition: Symmetric Property

A relation R on A is **symmetric** if and only if for all $a, b \in A$, if aRb, then bRa.

Clearly the relation $=$ is symmetric since $x = y \to y = x$. However, divides is not symmetric, since $5 \mid 10$ but $10 \nmid 5$.

Definition: Transitive Property

A relation R on A is **transitive** if and only if for all $a, b, c \in A$, if aRb and bRc, then aRc.

example: consider $G : \mathbb{R} \to \mathbb{R}$ by $xGy \iff x > y$. Since if $a > b$ and $b > c$ then $a > c$ is true for all $a, b, c \in \mathbb{R}$, the relation G is transitive.

Example 6.2.1

B is a relation on all people on Earth defined by xBy if and only if x is a brother of y.

Reflexive?

No, Jamal is not a brother to himself.

Symmetric?

No, Jamal can be the brother of Elaine, but Elaine is not the brother of Jamal.

Transitive?

Yes, if X is the brother of Y and Y is the brother of Z , then X is the brother of Z.

Example 6.2.2

Consider the relation R on the set $A = \{1, 2, 3, 4\}$ defined by

$$R = \{(1,1), (2,3), (2,4), (3,3), (3,4)\}. \tag{6.2.1}$$

Reflexive?

No, since $(2,2) \notin R$, the relation is not reflexive.

Symmetric?

No, we have $(2,3) \in R$ but $(3,2) \notin R$, thus R is not symmetric.

Transitive?

Yes. By going through all the ordered pairs in R, we verify that whether $(a,b) \in R$ and $(b,c) \in R$, we always have $(a,c) \in R$ as well. This shows that R is transitive.

Example 6.2.3

Define the relation S on the set $A = \{1,2,3,4\}$ according to

$$S = \{(2,3),(3,2)\}. \tag{6.2.2}$$

Reflexive?

No, since $(2,2) \notin R$, the relation is not reflexive.

Symmetric?

Yes. Since we have only two ordered pairs, and it is clear that whenever $(a,b) \in S$, we also have $(b,a) \in S$. Hence, S is symmetric.

Transitive?

Since $(2,3) \in S$ and $(3,2) \in S$, but $(2,2) \notin S$, the relation S is not transitive.

hands-on exercise 6.2.1

Define the relation R on the set $\mathbb{R}$ as

$$a\,R\,b \Leftrightarrow a \leq b. \tag{6.2.3}$$

Determine whether R is reflexive, symmetric, or transitive.

hands-on exercise 6.2.2

The relation S on the set $\mathbb{R}^*$ is defined as

$$a\,S\,b \Leftrightarrow ab > 0. \tag{6.2.4}$$

Determine whether S is reflexive, symmetric, or transitive.

Example 6.2.4

Here are two examples from geometry. Let $\mathcal{T}$ be the set of triangles that can be drawn on a plane. Define a relation S on $\mathcal{T}$ such that $(T_1, T_2) \in S$ if and only if the two triangles are similar. It is easy to check that S is reflexive, symmetric, and transitive.

Let $\mathcal{L}$ be the set of all the (straight) lines on a plane. Define a relation P on $\mathcal{L}$ according to $(L_1, L_2) \in P$ if and only if L_1 and L_2 are parallel lines. Again, it is obvious that P is reflexive, symmetric, and transitive.

Example 6.2.5

The relation T on $\mathbb{R}^*$ is defined as

$$a\,T\,b \Leftrightarrow \frac{a}{b} \in \mathbb{Q}. \tag{6.2.5}$$

Since $\frac{a}{a} = 1 \in \mathbb{Q}$, the relation T is reflexive.

The relation T is symmetric, because if $\frac{a}{b}$ can be written as $\frac{m}{n}$ for some nonzero integers m and n, then so is its reciprocal $\frac{b}{a}$, because $\frac{b}{a} = \frac{n}{m}$.

If $\frac{a}{b}, \frac{b}{c} \in \mathbb{Q}$, then $\frac{a}{b} = \frac{m}{n}$ and $\frac{b}{c} = \frac{p}{q}$ for some nonzero integers m, n, p, and q. Then $\frac{a}{c} = \frac{a}{b} \cdot \frac{b}{c} = \frac{mp}{nq} \in \mathbb{Q}$. Hence, T is transitive.

Therefore, the relation T is reflexive, symmetric, and transitive.

Definition: Equivalence Relation

A relation is an **equivalence relation** if and only if the relation is reflexive, symmetric and transitive.

Example 6.2.6

The relation U on $\mathbb{Z}$ is defined as

$$a\,U\,b \Leftrightarrow 5 \mid (a+b). \tag{6.2.6}$$

Is U an equivalence relation?

Answer

If $5 \mid (a+b)$, it is obvious that $5 \mid (b+a)$ because $a+b=b+a$. Thus, U is symmetric.
However, U is not reflexive, because $5 \nmid (1+1)$.
Therefore U is not an equivalence relation

hands-on exercise 6.2.3

Determine whether the following relation V on some universal set $\mathcal{U}$ is an equivalence relation:

$$(S,T) \in V \Leftrightarrow S \subseteq T. \tag{6.2.7}$$

Example 6.2.7

Consider the relation V on the set $A=\{0,1\}$ is defined according to

$$V=\{(0,0),(1,1)\}. \tag{6.2.8}$$

Is V an equivalence relation?

Answer

The relation V is reflexive, because $(0,0) \in V$ and $(1,1) \in V$.
It is clearly symmetric, because $(a,b) \in V$ always implies $(b,a) \in V$.
Because V consists of only two ordered pairs, both of them in the form of (a,a), V is transitive.
Therefore, V is an equivalence relation.

hands-on exercise 6.2.4

Determine whether the following relation W on a nonempty set of individuals in a community is an equivalence relation:

$$a\,W\,b \Leftrightarrow a \text{ and } b \text{ have the same last name.} \tag{6.2.9}$$

Example **6.2.8** Congruence Modulo 5

Consider the relation R on $\mathbb{Z}$ defined by $xRy \iff 5 \mid (x-y)$.

Note: (1) R is called Congruence Modulo 5. (2) We have proved $a \mod 5 = b \mod 5 \iff 5 \mid (a-b)$.

Prove R is an equivalence relation.

Proof:

Reflexive: Consider any integer a. $a-a=0$. $5 \mid 0$ by the definition of divides since $5(0)=0$ and $0 \in \mathbb{Z}$.
So, $5 \mid (a=a)$ thus aRa by definition of R.
$\therefore R$ is reflexive.

Symmetric: Let $a,b \in \mathbb{Z}$ such that aRb. We must show that bRa.
Since aRb, $5 \mid (a-b)$ by definition of R. By definition of divides, there exists an integer k such that

$$5k=a-b.$$

By algebra:

$$-5k = b - a$$

$$5(-k) = b - a.$$

$-k \in \mathbb{Z}$ since the set of integers is closed under multiplication. So, $5 \mid (b-a)$ by definition of divides. bRa by definition of R.
$\therefore R$ is symmetric.

Transitive: Let $a, b, c \in \mathbb{Z}$ such that aRb and bRc. We must show that aRc.
$5 \mid (a-b)$ and $5 \mid (b-c)$ by definition of R. By definition of divides, there exists an integers j, k such that

$$5j = a - b.$$

$$5k = b - c.$$

Adding the equations together and using algebra:

$$5j + 5k = a - c$$

$$5(j+k) = a - c.$$

$j + k \in \mathbb{Z}$ since the set of integers is closed under addition. So, $5 \mid (a-c)$ by definition of divides. aRc by definition of R.
$\therefore R$ is transitive.

Thus, by definition of equivalence relation, R is an equivalence relation.

Summary and Review

- A relation from a set A to itself is called a relation **on** set A.
- Given any relation R on a set A, we are interested in three properties that R may or may not have.
- The relation R is said to be reflexive if every element is related to itself, that is, if $x\,R\,x$ for every $x \in A$.
- The relation R is said to be symmetric if the relation can go in both directions, that is, if $x\,R\,y$ implies $y\,R\,x$ for any $x, y \in A$.
- Finally, a relation is said to be transitive if we can pass along the relation and relate two elements if they are related via a third element.
- More precisely, R is transitive if $x\,R\,y$ and $y\,R\,z$ implies that $x\,R\,z$.

Exercises

Exercise 6.2.1

Let S be a nonempty set and define the relation A on $\mathscr{P}(S)$ by

$$(X, Y) \in A \Leftrightarrow X \cap Y = \emptyset. \tag{6.2.10}$$

It is clear that A is symmetric.

a) Explain why A is not reflexive.

b) Is A transitive? Explain.

c) Let $S = \{a, b, c\}$. Draw the directed (arrow) graph for A.

Answer:

(a) Since set S is not empty, there exists at least one element in S, call one of the elements x. The power set must include $\{x\}$ and $\{x\} \cap \{x\} = \{x\}$ and thus is not empty. So we have shown an element which is not related to itself; thus S is not reflexive.

(b) Consider these possible elements of the power set: $S_1 = \{w, x, y\}$, $S_2 = \{a, b\}$, $S_3 = \{w, x\}$. $S_1 \cap S_2 = \emptyset$ and $S_2 \cap S_3 = \emptyset$, but $S_1 \cap S_3 \neq \emptyset$. We have shown a counter example to transitivity, so A is not transitive.

(c) Here's a sketch of some of the diagram should look:

-There are eight elements on the left and eight elements on the right

-This relation is symmetric, so every arrow has a matching cousin. i.e there is \{a,c\}\right arrow\{b}\} and also \{b\}\right arrow\{a,c}\}.

-The empty set is related to all elements including itself; every element is related to the empty set.

Exercise 6.2.2

For each of these relations on $\mathbb{N} - \{1\}$, determine which of the three properties are satisfied.

a) $A_1 = \{(x, y) \mid x \text{ and } y \text{ are relatively prime}\}$

b) $A_2 = \{(x, y) \mid x \text{ and } y \text{ are not relatively prime}\}$

Exercise 6.2.3

For each of the following relations on $\mathbb{N}$, determine which of the three properties are satisfied.

a) $B_1 = \{(x, y) \mid x \text{ divides } y\}$

b) $B_2 = \{(x, y) \mid x + y \text{ is even }\}$

c) $B_3 = \{(x, y) \mid xy \text{ is even }\}$

Answer:

(a) reflexive, transitive

(b) reflexive, symmetric, transitive

(c) symmetric

Exercise 6.2.4

For each of the following relations on $\mathbb{N}$, determine which of the three properties are satisfied.

a) $D_1 = \{(x, y) \mid x + y \text{ is odd }\}$

b) $D_2 = \{(x, y) \mid xy \text{ is odd }\}$

Exercise 6.2.5

For each of the following relations on $\mathbb{Z}$, determine which of the three properties are satisfied.

a) $U_1 = \{(x, y) \mid 3 \text{ divides } x + 2y\}$

b) $U_2 = \{(x, y) \mid x - y \text{ is odd }\}$

Answer:

(a) reflexive, symmetric and transitive (try proving this!)

(b) symmetric

Exercise 6.2.6

For each of the following relations on $\mathbb{Z}$, determine which of the three properties are satisfied.

a) $V_1 = \{(x, y) \mid xy > 0\}$

b) $V_2 = \{(x, y) \mid x - y \text{ is even }\}$

c) $V_3 = \{(x, y) \mid x \text{ is a multiple of } y\}$

6.3: Equivalence Relations and Partitions

Recall:

A relation on a set A is an ***equivalence relation*** if it is reflexive, symmetric, and transitive. We often use the tilde notation $a \sim b$ to denote a relation.

Also, when we specify just one set, such as $a \sim b$ is a relation on set B, that means the domain & codomain are both set B.

For an equivalence relation, due to transitivity and symmetry, all the elements related to a fixed element must be related to each other. Thus, if we know one element in the group, we essentially know all its "relatives."

Definition: Equivalence Class

Let R be an equivalence relation on set A. For each $a \in A$ we denote the **equivalence class** of a as $[a]$ defined as:

$$[a] = \{x \in A \mid xRa\}. \tag{6.3.1}$$

Example 6.3.1

Define a relation $\sim$ on $\mathbb{Z}$ by

$$a \sim b \Leftrightarrow a \bmod 4 = b \bmod 4. \tag{6.3.2}$$

Find the equivalence classes of $\sim$.

Answer

Two integers will be related by $\sim$ if they have the same remainder after dividing by 4. The possible remainders are 0, 1, 2, 3.

$[0] = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$

$[1] = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$

$[2] = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$

$[3] = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$

hands-on exercise 6.3.1

Define a relation $\sim$ on $\mathbb{Z}$ by

$$a \sim b \Leftrightarrow a \bmod 3 = b \bmod 3. \tag{6.3.3}$$

Find the equivalence classes of $\sim$.

example 6.3.2

Let $S = \mathscr{P}(\{1,2,3\}) = \big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\big\}$.

For convenience, label

$S_0 = \emptyset$, $S_1 = \{1\}$, $S_2 = \{2\}$, $S_3 = \{3\}$, $S_4 = \{1,2\}$, $S_5 = \{1,3\}$, $S_6 = \{2,3\}$, $S_7 = \{1,2,3\}$.

Define this equivalence relation $\sim$ on S by

$$S_i \sim S_j \Leftrightarrow |S_i| = |S_j|. \tag{6.3.4}$$

Find the equivalence classes of $\sim$.

Answer

Two sets will be related by $\sim$ if they have the same number of elements.

$[S_0]=\{S_0\}$

$[S_2]=\{S_1,S_2,S_3\}$

$[S_4]=\{S_4,S_5,S_6\}$

$[S_7]=\{S_7\}$

The element in the brackets, [ ] is called the representative of the equivalence class. An equivalence class can be represented by any element in that equivalence class. So, in *Example 6.3.2*, $[S_2]=[S_3]=[S_1]=\{S_1,S_2,S_3\}$. This equality of equivalence classes will be formalized in Lemma 6.3.1.

Notice an equivalence class is a set, so a collection of equivalence classes is a collection of sets.

Take a closer look at *Example 6.3.1*. All the integers having the same remainder when divided by 4 are related to each other. The equivalence classes are the sets

$$\begin{array}{rcl} [0] &=& \{n\in\mathbb{Z}\mid n \bmod 4=0\} &=& 4\mathbb{Z}, \\ [1] &=& \{n\in\mathbb{Z}\mid n \bmod 4=1\} &=& 1+4\mathbb{Z}, \\ [2] &=& \{n\in\mathbb{Z}\mid n \bmod 4=2\} &=& 2+4\mathbb{Z}, \\ [3] &=& \{n\in\mathbb{Z}\mid n \bmod 4=3\} &=& 3+4\mathbb{Z}. \end{array} \tag{6.3.5}$$

It is clear that every integer belongs to exactly one of these four sets. Hence,

$$\mathbb{Z}=[0]\cup[1]\cup[2]\cup[3]. \tag{6.3.6}$$

These four sets are pairwise disjoint. From this we see that $\{[0],[1],[2],[3]\}$ is a partition of $\mathbb{Z}$.

Equivalence Classes form a partition (idea of Theorem 6.3.3)

The overall idea in this section is that given an equivalence relation on set A, the collection of equivalence classes forms a partition of set A, (Theorem 6.3.3).

The converse is also true: given a partition on set A, the relation "induced by the partition" is an equivalence relation (Theorem 6.3.4).

As another illustration of Theorem 6.3.3, look at *Example 6.3.2*.

$$[S_0]\cup[S_2]\cup[S_4]\cup[S_7]=S \tag{6.3.7}$$

$$\big\{[S_0],[S_2],[S_4],[S_7]\big\} \text{ is pairwise disjoint} \tag{6.3.8}$$

Thus, $\big\{[S_0],[S_2],[S_4],[S_7]\big\}$ is a partition of set S.

In order to prove Theorem 6.3.3, we will first prove two lemmas.

Lemma 6.3.1

If R is an equivalence relation on A, then $aRb\to[a]=[b]$.

Proof

Let R be an equivalence relation on A with aRb.
First we will show $[a]\subseteq[b]$.
Let $x\in[a]$, then xRa by definition of equivalence class. Now we have xRa and aRb,
thus xRb by transitivity (since R is an equivalence relation). Since xRb, $x\in[b]$, by definition of equivalence classes.
We have shown if $x\in[a]$ then $x\in[b]$, thus $[a]\subseteq[b]$, by definition of subset.

Next we will show $[b] \subseteq [a]$.
Let $x \in [b]$, then xRb by definition of equivalence class. Since aRb, we also have bRa, by symmetry.
Now we have xRb and bRa, thus xRa by transitivity. Since xRa, $x \in [a]$, by definition of equivalence classes.
We have shown if $x \in [b]$ then $x \in [a]$, thus $[b] \subseteq [a]$, by definition of subset.

$\therefore [a] = [b]$ by the definition of set equality.

One may regard equivalence classes as objects with many aliases. Every element in an equivalence class can serve as its representative. So we have to take extra care when we deal with equivalence classes. Do not be fooled by the representatives, and consider two apparently different equivalence classes to be distinct when in reality they may be identical.

Example 6.3.3

Define $\sim$ on a set of individuals in a community according to

$$a \sim b \Leftrightarrow a \text{ and } b \text{ have the same last name.} \tag{6.3.9}$$

We can easily show that $\sim$ is an equivalence relation. Each equivalence class consists of all the individuals with the same last name in the community. Hence, for example, Jacob Smith, Liz Smith, and Keyi Smith all belong to the same equivalence class. Any Smith can serve as its representative, so we can denote it as, for example, [Liz Smith].

Example 6.3.4

Define $\sim$ on $\mathbb{R}^+$ according to

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}. \tag{6.3.10}$$

Hence, two positive real numbers are related if and only if they have the same decimal parts. It is easy to verify that $\sim$ is an equivalence relation, and each equivalence class $[x]$ consists of all the positive real numbers having the same decimal parts as x has. Notice that

$$\mathbb{R}^+ = \bigcup_{x \in (0,1]} [x], \tag{6.3.11}$$

which means that the equivalence classes $[x]$, where $x \in (0,1]$, form a partition of $\mathbb{R}$.

hands-on exercise 6.3.2

Prove that the relation $\sim$ in Example 6.3.4 is indeed an equivalence relation.

Lemma 6.3.2

Given an equivalence relation R on set A, if $a, b \in A$ then either $[a] \cap [b] = \emptyset$ or $[a] = [b]$

Proof

Let R be an equivalence relation on set A with $a, b \in A$.

Case 1: $[a] \cap [b] = \emptyset$
In this case $[a] \cap [b] = \emptyset$ or $[a] = [b]$ is true.

Case 2: $[a] \cap [b] \neq \emptyset$
$\exists x (x \in [a] \wedge x \in [b])$ by definition of empty set & intersection.
xRa and xRb by definition of equivalence classes. Also since xRa, aRx by symmetry.
We have aRx and xRb, so aRb by transitivity. Since aRb, $[a] = [b]$ by Lemma 6.3.1.
In this case $[a] \cap [b] = \emptyset$ or $[a] = [b]$ is true.

These are the only possible cases. So, if $a, b \in A$ then either $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

Theorem 6.3.3 and Theorem 6.3.4 together are known as the ***Fundamental Theorem on Equivalence Relations***.

Theorem 6.3.3

If R is an equivalence relation on any non-empty set A, then the distinct set of equivalence classes of R forms a partition of A.

Proof

Suppose R is an equivalence relation on any non-empty set A. Denote the equivalence classes as $A_1, A_2, A_3, \ldots$.
WMST $A_1 \cup A_2 \cup A_3 \cup \ldots = A$.
First we will show $A_1 \cup A_2 \cup A_3 \cup \ldots \subseteq A$.
If $x \in A_1 \cup A_2 \cup A_3 \cup \ldots,$ then x belongs to at least one equivalence class, A_i by definition of union.
By the definition of equivalence class, $x \in A$. Thus $A_1 \cup A_2 \cup A_3 \cup \ldots \subseteq A$.
Next we show $A \subseteq A_1 \cup A_2 \cup A_3 \cup \ldots$.
If $x \in A$, then xRx since R is reflexive. Thus $x \in [x]$.
$[x] = A_i,$ for some i since $[x]$ is an equivalence class of R.
So, $A \subseteq A_1 \cup A_2 \cup A_3 \cup \ldots$ by definition of subset. And so, $A_1 \cup A_2 \cup A_3 \cup \ldots = A,$ by the definition of equality of sets.

Now WMST $\{A_1, A_2, A_3, \ldots\}$ is pairwise disjoint.
For any i, j, either $A_i = A_j$ or $A_i \cap A_j = \emptyset$ by Lemma 6.3.2. So, $\{A_1, A_2, A_3, \ldots\}$ is mutually disjoint by definition of mutually disjoint.

We have demonstrated both conditions for a collection of sets to be a partition and we can conclude
if R is an equivalence relation on any non-empty set A, then the distinct set of equivalence classes of R forms a partition of A.

Conversely, given a partition $\mathcal{P}$, we could define a relation that relates all members in the same component. This relation turns out to be an equivalence relation, with each component forming an equivalence class. This equivalence relation is referred to as the ***equivalence relation induced by*** $\mathcal{P}$.

Definition

Given $P = \{A_1, A_2, A_3, \ldots\}$ is a partition of set A, the **relation, R, induced by the partition, P,** is defined as follows:

$$\text{For all } x, y \in A, xRy \leftrightarrow \exists A_i \in P(x \in A_i \wedge y \in A_i). \tag{6.3.12}$$

Example 6.3.5

Consider set $S = \{a, b, c, d\}$ with this partition: $\{\{a, b\}, \{c\}, \{d\}\}$.

Find the ordered pairs for the relation R, induced by the partition.

Proof

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

Theorem 6.3.4

If A is a set with partition $P = \{A_1, A_2, A_3, \ldots\}$ and R is a relation induced by partition P, then R is an equivalence relation.

Proof

Let A be a set with partition $P = \{A_1, A_2, A_3, \ldots\}$ and R be a relation induced by partition P. WMST R is an equivalence relation.

Reflexive
Let $x \in A$. Since the union of the sets in the partition $P = A,$ x must belong to at least one set in P.
$\exists i(x \in A_i)$. Since $x \in A_i \wedge x \in A_i,$ xRx by the definition of a relation induced by a partition.

$\therefore R$ is reflexive.

Symmetric
Suppose xRy. $\exists i(x \in A_i \wedge y \in A_i)$ by the definition of a relation induced by a partition.
Since $y \in A_i \wedge x \in A_i, \qquad yRx$.
$\therefore R$ is symmetric.

Transitive
Suppose $xRy \wedge yRz$.
$\exists i(x \in A_i \wedge y \in A_i)$ and $\exists j(y \in A_j \wedge z \in A_j)$ by the definition of a relation induced by a partition.
Because the sets in a partition are pairwise disjoint, either $A_i = A_j$ or $A_i \cap A_j = \emptyset$.
Since y belongs to both these sets, $A_i \cap A_j \neq \emptyset$, thus $A_i = A_j$.
Both x and z belong to the same set, so xRz by the definition of a relation induced by a partition.
$\therefore R$ is transitive.

We have shown R is reflexive, symmetric and transitive, so R is an equivalence relation on set A.
$\therefore$ if A is a set with partition $P = \{A_1, A_2, A_3, \ldots\}$ and R is a relation induced by partition P, then R is an equivalence relation.

Example 6.3.6

Over $\mathbb{Z}^*$, define

$$R_3 = \{(m,n) \mid m,n \in \mathbb{Z}^* \text{ and } mn > 0\}. \tag{6.3.13}$$

It is not difficult to verify that R_3 is an equivalence relation. There are only two equivalence classes: $[1]$ and $[-1]$, where $[1]$ contains all the positive integers, and $[-1]$ all the negative integers. It is obvious that $\mathbb{Z}^* = [1] \cup [-1]$.

hands-on exercise 6.3.3

The relation S defined on the set $\{1,2,3,4,5,6\}$is known to be

$$\begin{aligned} S = \{&(1,1),(1,4),(2,2),(2,5),(2,6),(3,3), \\ &(4,1),(4,4),(5,2),(5,5),(5,6),(6,2),(6,5),(6,6)\}. \end{aligned} \tag{6.3.14}$$

Confirm that S is an equivalence relation by studying its ordered pairs. Determine the contents of its equivalence classes.

Example 6.3.7

Consider the equivalence relation R induced by the partition

$$\mathcal{P} = \{\{1\},\{3\},\{2,4,5,6\}\} \tag{6.3.15}$$

of $A = \{1,2,3,4,5,6\}$.

(a) Write the equivalence classes for this equivalence relation. (b) Write the equivalence relation as a set of ordered pairs.

Answer

(a) $[1] = \{1\} \qquad [2] = \{2,4,5,6\} \qquad [3] = \{3\}$

(b) From the two 1-element equivalence classes $\{1\}$ and $\{3\}$, we find two ordered pairs $(1,1)$ and $(3,3)$ that belong to R. From the equivalence class $\{2,4,5,6\}$ any pair of elements produce an ordered pair that belongs to R. Therefore,

$$\begin{aligned} R = \quad &\{(1,1),(3,3),(2,2),(2,4),(2,5),(2,6),(4,2),(4,4),(4,5),(4,6), \\ &(5,2),(5,4),(5,5),(5,6),(6,2),(6,4),(6,5),(6,6)\}. \end{aligned}$$

Summary Review

- A relation R on a set A is an equivalence relation if it is reflexive, symmetric, and transitive.
- If R is an equivalence relation on the set A, its equivalence classes form a partition of A.
- In each equivalence class, all the elements are related and every element in A belongs to one and only one equivalence class.
- The relation R determines the membership in each equivalence class, and every element in the equivalence class can be used to represent that equivalence class.
- In a sense, if you know one member within an equivalence class, you also know all the other elements in the equivalence class because they are all related according to R.
- Conversely, given a partition of A, we can use it to define an equivalence relation by declaring two elements to be related if they belong to the same component in the partition.

Exercises

Exercise 6.3.1

Find the equivalence classes for each of the following equivalence relations $\sim$ on $\mathbb{Z}$.

a) $m \sim n \Leftrightarrow |m-3| = |n-3|$

b) $m \sim n \Leftrightarrow m+n$ is even

Answer

(a) The equivalence classes are of the form $\{3-k, 3+k\}$ for some integer k. For instance, $[3] = \{3\}$, $[2] = \{2,4\}$, $[1] = \{1,5\}$, and $[-5] = \{-5,11\}$.

(b) There are two equivalence classes: $[0] = \text{the set of even integers}$, and $[1] = \text{the set of odd integers}$.

Exercise 6.3.2

For this relation $\sim$ on $\mathbb{Z}$ defined by $m \sim n \Leftrightarrow 3 \mid (m+2n)$:

a) show $\sim$ is an equivalence relation.

b) find the equivalence classes for $\sim$.

Exercise 6.3.3

Let T be a fixed subset of a nonempty set S. Define the relation $\sim$ on $\mathscr{P}(S)$ by

$$X \sim Y \Leftrightarrow X \cap T = Y \cap T, \tag{6.3.16}$$

Show that $\sim$ is an equivalence relation. In particular, let $S = \{1,2,3,4,5\}$ and $T = \{1,3\}$.

a) True or false: $\{1,2,4\} \sim \{1,4,5\}$?

b) How about $\{1,2,4\} \sim \{1,3,4\}$?

c) Find $[\{1,5\}]$

d) Describe $[X]$ for any $X \in \mathscr{P}(S)$.

Answer

(a) True

(b) False

(c) $[\{1,5\}] = \big\{\{1\},\{1,2\},\{1,4\},\{1,5\},\{1,2,4\},\{1,2,5\},\{1,4,5\},\{1,2,4,5\}\big\}$

(d) $[X]=\{(X\cap T)\cup Y \mid Y\in\mathscr{P}(\overline{T})\}$. In other words, $S\sim X$ if S contains the same element in $X\cap T$, plus possibly some elements not in T.

Exercise 6.3.4

For each of the following relations $\sim$ on $\mathbb{R}\times\mathbb{R}$, determine whether it is an equivalence relation. For those that are, describe geometrically the equivalence class $[(a,b)]$.

1. $(x_1,y_1)\sim(x_2,y_2) \Leftrightarrow y_1-x_1^2=y_2-x_2^2$.
2. $(x_1,y_1)\sim(x_2,y_2) \Leftrightarrow (x_1-1)^2+y_1^2=(x_2-1)^2+y_2^2$

Exercise 6.3.5

For each of the following relations $\sim$ on $\mathbb{R}\times\mathbb{R}$, determine whether it is an equivalence relation. For those that are, describe geometrically the equivalence class $[(a,b)]$.

1. $(x_1,y_1)\sim(x_2,y_2) \Leftrightarrow x_1+y_2=x_2+y_1$
2. $(x_1,y_1)\sim(x_2,y_2) \Leftrightarrow (x_1-x_2)(y_1-y_2)=0$

Answer

(a) Yes, with $[(a,b)]=\{(x,y)\mid y=x+k \text{ for some constant } k\}$. In other words, the equivalence classes are the straight lines of the form $y=x+k$ for some constant k.

(b) No. For example, $(2,5)\sim(3,5)$ and $(3,5)\sim(3,7)$, but $(2,5)\nsim(3,7)$. Hence, the relation $\sim$ is not transitive.

Exercise 6.3.6

For each of the following relations $\sim$ on $\mathbb{R}\times\mathbb{R}$, determine whether it is an equivalence relation. For those that are, describe geometrically the equivalence class $[(a,b)]$.

1. $(x_1,y_1)\sim(x_2,y_2) \Leftrightarrow |x_1|+|y_1|=|x_2|+|y_2|$
2. $(x_1,y_1)\sim(x_2,y_2) \Leftrightarrow x_1y_1=x_2y_2$

Exercise 6.3.7

Define the relation $\sim$ on $\mathbb{Q}$ by

$$x\sim y \Leftrightarrow 2(x-y)\in\mathbb{Z}. \tag{6.3.17}$$

$\sim$ is an equivalence relation. Describe the equivalence classes $[0]$ and $\left[\frac{1}{4}\right]$.

Answer

We find $[0]=\frac{1}{2}\mathbb{Z}=\{\frac{n}{2}\mid n\in\mathbb{Z}\}$, and $[\frac{1}{4}]=\frac{1}{4}+\frac{1}{2}\mathbb{Z}=\{\frac{2n+1}{4}\mid n\in\mathbb{Z}\}$.

Exercise 6.3.8

Define the relation $\sim$ on $\mathbb{Q}$ by

$$x\sim y \Leftrightarrow \frac{x-y}{2}\in\mathbb{Z}. \tag{6.3.18}$$

Show that $\sim$ is an equivalence relation. Describe the equivalence classes $[0]$, $[1]$ and $\left[\frac{1}{2}\right]$.

Exercise 6.3.9

Consider the following relation on $\{a,b,c,d,e\}$:

$$\begin{aligned} R=\{&(a,a),(a,c),(a,e),(b,b),(b,d),(c,a),(c,c),(c,e),\\ &(d,b),(d,d),(e,a),(e,c),(e,e)\}. \end{aligned} \tag{6.3.19}$$

This is an equivalence relation. Describe its equivalence classes.

Answer

$[a]=\{a,c,e\}$
$[b]=\{b,d\}$

Exercise 6.3.10

Each part below gives a partition of $A=\{a,b,c,d,e,f,g\}$. Find the equivalence relation (as a set of ordered pairs) on A induced by each partition.

(a) $\mathcal{P}_1=\{\{a,b\},\{c,d\},\{e,f\},\{g\}\}$

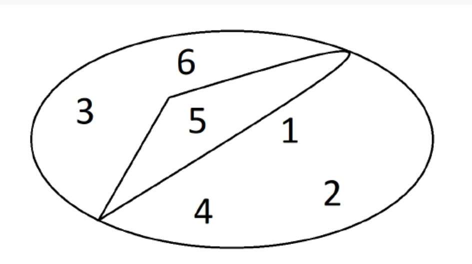
(b) $\mathcal{P}_2=\{\{a,c,e,g\},\{b,d,f\}\}$

(c) $\mathcal{P}_3=\{\{a,b,d,e,f\},\{c,g\}\}$

(d) $\mathcal{P}_4=\{\{a,b,c,d,e,f,g\}\}$

Exercise 6.3.11

Write out the relation, R induced by the partition below on the set $A=\{1,2,3,4,5,6\}$.



Answer

$R=\{(1,2),(2,1),(1,4),(4,1),(2,4),(4,2),(1,1),(2,2),(4,4),(5,5),(3,6),(6,3),(3,3),(6,6)\}$

Exercise 6.3.12

Consider the relation, R induced by the partition on the set $A=\{1,2,3,4,5,6\}$shown in exercises 6.3.11 (above).

Answer these questions True or False.

(a) Every element in set A is related to every other element in set A.

(b) $(2,3)\in R$.

(c) $(2,1)\in R$.

(d) Every element in set A is related to itself.

(e) The relation, R, is transitive.

(f) $5\,R\,6$

(g) $1\,R\,4$

(h) $[3]=\{6\}$

(i) $R\subseteq A\times A$

(j) $A\cap R=\emptyset$

CHAPTER OVERVIEW

7: Combinatorics

7.1: Intro, Probability and Pigeonhole Principle

Intro: What is Combinatorics?

Combinatorics studies the arrangements of objects according to some rules. The questions that can be asked include

- *Existence*. Do the arrangements exist?
- *Classification*. If the arrangements exist, how can we characterize and classify them?
- *Enumeration*. How many arrangements are there?
- *Construction*. Is there an algorithm for constructing all the arrangements?

Example 7.1.1

In how many ways can five people be seated at a round table? What if a certain pair of them refuses to sit next to one another? What if there are n people?

Example 7.1.2

A ***binary string*** is a sequence of digits, each of which being 0 or 1. Let a_n be the number of binary strings of length n that do not contain consecutive 1s. It is easy to check that $a_1 = 2$, $a_2 = 3$, and $a_3 = 5$. What is the general formula for a_n?

Example 7.1.3

The complexity of an algorithm tells us how many operations it requires. By comparing the complexity of several algorithms for solving the same problem, we can determine which one is most efficient. Let b_n be the number of operations required to solve a problem of size n. If it is known that

$$b_n = 2b_{n-1} + 3b_{n-2}, \qquad n \geq 3, \tag{7.1.1}$$

where $b_1 = 1$ and $b_2 = 3$, what is the general formula for b_n?

Consider the number of integers from 2 to 5, inclusive. You might think there 3 integers since $5-2=3$. However, if we include the 1st and last integer, our set is $\{2,3,4,5\}$and you can see there are 4 integers.

Theorem $\mathbf{7.1.1}$: Counting Natural Numbers

If $m, n \in \mathbb{Z}$ and $m \geq n$ then the number of integers from n to m is $m-n+1$.

Example 7.1.4

How many four-digit codes exist from 1000 to 9999?

Solution

$9999-1000+1=9000$ so there are 9000 four-digit codes from 1000 to 9999.

Probability

Definition: Sample Space

A sample space is the set of all possible outcomes. For example, the sample space for rolling a die is:

$$1 \qquad 2 \qquad 3 \qquad 4 \qquad 5 \qquad 6 \tag{7.1.2}$$

which is the set of the six possible results from tossing a die.

Definition: Event

An **event** is a subset of a sample space. For example, an event for rolling two dice is: the sum is 9, i.e.

$$3\,6 \qquad 6\,3 \qquad 4\,5 \qquad 5\,4 \tag{7.1.3}$$

Definition: Probability for Equally Likely outcomes

If E is an event, then the **probability of that event, $P(E)$ is:**

$$P(E)=\frac{\text{the number of outcomes in E}}{\text{the total number of outcomes in the sample space}}. \tag{7.1.4}$$

For example, there are 36 outcomes for rolling two dice, so $P(\text{sum of } 9)=\frac{4}{36}=\frac{1}{9}$.

Since an event is a subset of the sample space, the largest number of elements in an event is the number of elements in the sample space.

Thus the maximum probability of an event is 1. The smallest number of elements in an event is zero, so the minimum probability of an event is 0.

$P(E_1)=1$ means event E_1 will always happen.

$P(E_2)=0$ means event E_2 will never happen.

Example 7.1.1

Pick a card from a standard 52-card deck. What is the probability that the number of the card is

(a) a six

(b) a number less than 20

(c) a number greater than 15

Solution

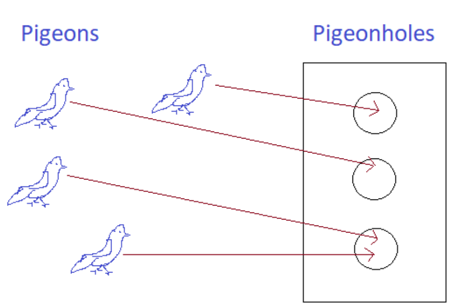
(a) $\frac{1}{13}$

(b) 1

(c) 0

Pigeonhole Principle

The Pigeonhole Principle says that if you have more pigeons than pigeonholes, then at least one pigeonhole will get two pigeons.



If you have a function from a finite set to a smaller finite set, then the function cannot be one-to-one; in other words, there must be at least two elements in the domain with the same image in the codomain.

More formally,

Theorem 7.1.2 Pigeonhole Principle

If $f: X \to Y$ where X and Y are finite sets with $|X| > |Y|$, then f is not one-to-one.

Example 7.1.5

Without looking, you pull socks out of a drawer that has just 5 blue socks and 5 white socks. How many do you need to pull to be certain you have two of the same color?

Solution

You could have two socks of different colors, but once you pull out three socks, there must be at least two of the same color. The answer is *three socks.*

Example 7.1.6

in a group of 30 people, each person picks a number from 1 to 10. What is the minimum number of people needed to be sure you have two people with the same number?

Solution

11

Summary and Review

- This chapter is about combinatorics, which is a study of arrangements of objects.
- We have a theorem to find the size of a set of consecutive integers.
- The probability of a event is the # of ways it can happen divided by the total # of outcomes.
- Probability is a number from 0 to 1, inclusive.
- The Pigeonhole Principle says if you have more pigeons than pigeonholes, at least 2 pigeons must cuddle up.

Exercises

exercise 7.1.1

A random number is picked from 80 to 600.

(a) How many numbers are there to pick?

(b) What is the probability of picking the number 220?

Answer

(a) $600 - 80 + 1 = 521$ so there are 521 numbers
(b) $\frac{1}{521}$

Exercise 7.1.2

Are you able to answer any of the 1st three examples in this section?

If so, tell your professor what you came up with. If not, look back after you have done more work in this chapter

Exercise 7.1.3

In a group of 100 people, each person picks a number from 100 to 120. What is the minimum number of people you need to be sure two of them have the same number?

Answer

22

Exercise 7.1.4

In a group of 20 people, each person has one pet that is a cat, a dog or a goat. What is the minimum number of people you need to be sure two of them have the same type of pet?

Exercise 7.1.5

How many cards do you need to pick from a standard 52-card deck to be sure to get a red card?

Answer

27, because if you pick all of the 26 black cards, the next one must be red.

Exercise 7.1.6

In a school of 600 students, do there have to be two students with the same birthday (month and day)? Why?

Exercise 7.1.7

How many integers do you need to pick to be sure that at least two of them have the same remainder after dividing by 5?

Answer

6, because there are 5 possible remainders: 0, 1, 2, 3, 4

Exercise 7.1.8

How many cards do you need to pick from a standard 52-card deck to be sure to get two cards of the same suit?

Exercise 7.1.9

If you pick one card from a standard 52-card deck, what is the probability it will be a diamond?

Answer

$\frac{1}{4}$

Exercise 7.1.10

If you pick one card from a standard 52-card deck, what is the probability it will be

(a) a two or three

(b) a two and a three

(c) a red card or a black card

Exercise 7.1.11

If you pick one card from a standard 52-card deck, what is the probability it will be

(a) an eight or a nine or a ten?

(b) an eight and a nine?

Answer

(a) $\frac{3}{13}$

(b) 0

7.2: Addition and Multiplication Principles

Addition Principle

Preliminaries

Recall that the cardinality of a finite set A, denoted $|A|$, is the number of elements it contains.

Example 7.2.1

If $A=\{-1,0,2\}$, then $|A|=3$. Also,

$$\begin{aligned} |\{2\}| &= 1, \\ |\{2,5,-1,-3\}| &= 4, \\ |\{x\in\mathbb{R}\mid x^2=1\}| &= 2. \end{aligned}$$

Notice that $|\emptyset|=0$, because an empty set does not contain any element.

It becomes more interesting when we consider the cardinality* of a union or an intersection of two or more sets.

**This cardinality link will take you to a not completely edited, but interesting dive into cardinality of infinite sets.*

Example 7.2.2

Determine $|A\cup B|$ and $|A\cap B|$ if $A=\{2,5\}$ and $B=\{7,9,10\}$.

Solution

Since $A\cup B=\{2,5,7,9,10\}$, and $A\cap B=\emptyset$, it is clear that $|A\cup B|=5$, and $|A\cap B|=0$.

Example 7.2.3

Determine $|A\cup B|$ and $|A\cap B|$ if $A=\{2,5\}$ and $B=\{5,9,10\}$.

Solution

Since $A\cup B=\{2,5,9,10\}$, and $A\cap B=\{5\}$, it is clear that $|A\cup B|=4$, and $|A\cap B|=1$.

hands-on exercise 7.2.1

Let $A=\{n\in\mathbb{Z}\mid -5\leq n\leq 3\}$, and $B=\{n\in\mathbb{Z}\mid -3\leq n\leq 5\}$. Evaluate $|A\cap B|$ and $|A\cup B|$.

The difference between the last two examples is whether the two sets A and B have a nonempty intersection. Two sets A and B are ***disjoint*** if $A\cap B=\emptyset$. A collection of sets $A_1,A_2,\ldots,A_n$ is said to be ***pairwise disjoint*** if $A_i\cap A_j=\emptyset$ whenever $i\neq j$.

Example 7.2.4

Let $A=\{1,0,-1\}$, $B=\{-2,0,2\}$, $C=\{-2,2\}$ and $D=\{3,4,5\}$. Then A, C, and D are pairwise disjoint, so are B and D, but A, B, and C are not.

Theorem 7.2.1: Addition Principle

If the finite sets $A_1,A_2,\ldots,A_n$ are pairwise disjoint, then

$$|A_1\cup A_2\cup\cdots\cup A_n|=|A_1|+|A_2|+\cdots+|A_n|. \tag{7.2.1}$$

Use the addition principle if we can break down the problems into *cases*, and count how many items or choices we have in each case. The total number is the sum of these individual counts. The idea is, instead of counting a large set, we divide it up into several smaller subsets, and count the size of each of them. The cardinality of the original set is the sum of the cardinalities of the smaller subsets. This divide-and-conquer approach works perfectly only when the sets are pairwise disjoint.

Example 7.2.5

To find the number of students present at a lecture, the teacher counts how many students there are in each row, then adds up the numbers to obtain the total count.

When the sets are not disjoint, the addition principle does not give us the right answer because the elements belonging to the intersection are counted more than once. We have to compensate the over-counting by subtracting the number of times these elements are over-counted. The simplest case covers two sets.

Theorem 7.2.2: Principle of Inclusion-Exclusion (PIE)

For any finite sets A and B, we have

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{7.2.2}$$

Proof

Observe that $A \cup B$ is the *disjoint union* of three sets

$$A \cup B = (A - B) \cup (A \cap B) \cup (B - A). \tag{7.2.3}$$

It is clear that $|A - B| = |A| - |A \cap B|$, and $|B - A| = |B| - |A \cap B|$. Therefore,

$$\begin{aligned} |A \cup B| &= |A - B| + |A \cap B| + |B - A| \\ &= (|A| - |A \cap B|) + |A \cap B| + (|B| - |A \cap B|) \\ &= |A| + |B| - |A \cap B|, \end{aligned}$$

which is what we have to prove.

The principle of inclusion-exclusion also works if A and B are disjoint, because in such an event, $|A \cap B| = 0$, reducing PIE to the addition principle.

Example 7.2.6

Assume the current enrollment at a college is 4689, with 60 students taking MATH 210, 42 taking CSIT 260, and 24 taking both. Together, how many different students are taking these two courses? In other words, determine the number of students who are taking either MATH 210 or CSIT 260.

Solution

Let A be the set of students taking MATH 210, and B the set of students taking CSIT 260, Then, $|A| = 60$, $|B| = 42$, and $|A \cap B| = 24$. We want to find $|A \cup B|$. According to PIE,

$$|A \cup B| = |A| + |B| - |A \cap B| = 60 + 42 - 24 = 78. \tag{7.2.4}$$

Therefore, 78 students are taking either MATH 210 or CSIT 260.

Example 7.2.7

Among 4689 students, 2112 of them have earned at least 60 credit hours and 2678 of them have earned at most 60 credit hours. How many students are there who have accumulated exactly 60 hours?

Solution

Let A be the set of students who have earned at least 60 credit hours, and B be the set of students who have earned at most 60 credit hours. We want to find $|A \cap B|$. According to PIE,

$$4689 = |A \cup B| = |A| + |B| - |A \cap B| = 2112 + 2678 - |A \cap B|. \tag{7.2.5}$$

Hence,

$$|A \cap B| = (2112 + 2678) - 4689 = 101. \tag{7.2.6}$$

There are 101 students who have accumulated exactly 60 credit hours.

hands-on exercise 7.2.2

The attendance at two consecutive college football games was 72397 and 69211 respectively. If 45713 people attended both games, how many different people have watched the games?

hands-on exercise 7.2.3

The attendance at two consecutive college football games was 72397 and 69211 respectively. If 93478 different individuals attended these two games, how many have gone to both?

Sometimes, it is easy to work with the complement of a set.

Lemma 7.2.3

For any finite set S, we have

$$|\bar{S}| = |\mathcal{U}| - |S|, \tag{7.2.7}$$

where $\mathcal{U}$ is the universal set containing S.

Example 7.2.8

In Example 6 since there are 78 students taking either MATH 210 or CSIT 260, the number of students taking neither is $4689 - 78 = 4611$.

The principle of inclusion-exclusion can be extended to any number of sets. The situation is more complicated, because some elements may be double-counted, some triple-counted, etc. To give you a taste of the general result, here is the principle of inclusion-exclusion for three sets.

Theorem 7.2.1

For any three finite sets A, B and C,

$$|A \cup B \cup B| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Proof

The union $A \cup B \cup C$ is the disjoint union of seven subsets:

$$\begin{gathered} A-(B \cup C), \quad B-(C \cup A), \quad C-(A \cup B), \quad (A \cap B)-(A \cap B \cap C), \\ (B \cap C)-(A \cap B \cap C), \quad (C \cap A)-(A \cap B \cap C), \quad \text{and} \quad A \cap B \cap C. \end{gathered}$$

We can apply an argument similar to the one used in the union of two sets to complete the proof. We leave the details as an exercise.

hands-on exercise 7.2.4

A group of students claims that each of them had seen at least one part of the *Back to the Future* trilogy. A quick show of hands reveals that

- 47 had watched Part I;
- 43 had watched Part II;
- 32 had watched Part III;
- 33 had watched both Parts I and II;
- 27 had watched both Parts I and III;
- 25 had watched both Parts II and III;
- 22 had watched all three parts.
- How many students are there in the group?

  Hint: A Venn Diagram can be helpful with this exercise.

Multiplication Principle

Another useful counting technique is the multiplication principle.

Theorem 7.2.5 (Multiplication Principle)

For any finite sets A and B, we have

$$|A \times B| = |A| \cdot |B|. \tag{7.2.8}$$

Clearly, this can be extended to an n-fold Cartesian product.

Theorem 7.2.6

For any finite sets $A_1, A_2, \ldots, A_n$, we have

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|.$$

In many applications, it may be helpful to use an equivalent form.

Theorem 7.2.7 (Multiplication Principle: Alternate Form)

If a task consists of k steps, and if there are n_i ways to finish step i, then the entire job can be completed in $n_1 n_2 \ldots n_k$ different ways.

Now that we have two counting techniques, the addition principle and the multiplication principle, which one should we use? The major difference between them is whether

- the jobs can be divided into *cases*, *groups*, or *categories*; or
- each job can be broken up into *steps*.

In practice, it helps to draw a picture of the configurations that we are counting.

Example 7.2.9

How many different license plates are there if a standard license plate consists of three letters followed by three digits?

Solution

We need to decide how many choices we have in each position. Draw a picture to show the configuration. Draw six lines to represent the six positions. Above each line, describe briefly the possible candidates for that position, and under each line, write the the number of choices.

	any	any	any	any	any	any
choices:	letter	letter	letter	digit	digit	digit
	———	———	———	———	———	———
# of choices:	26	26	26	10	10	10

This left-to-right configuration suggests that the multiplication principle should be used. The answer is $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 260^3$.

As you become more experienced, you can argue directly, as follows. There are 26 choices for each of the three letters, and 10 choices for each digit. So there are $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 260^3$ different license plates.

Example 7.2.10

Find the number of positive integers not exceeding 999 that end with 7.

Solution 1

The integers can have one, two, or three digits, so we have to analyze three cases.

Case 1. There is only one integer with one digit, namely, the integer 7.

Case 2. If there are two digits, the first could be any digit between 1 and 9, and the last digit must be 7.

choices:	1–9	7
	___	___
# of choices:	9	1

This gives us nine choices.

- *Case 3*. If there are three digits, the first digit could be any digit between 1 and 9, the second any digit between 0 and 9, and the last digit must be 7.

		any	
choices:	1–9	digit	7
	___	___	___
# of choices:	9	10	1

Hence, there are 90 integers in this case.

Combining the three cases, we have a total of $1+9+90=100$ integers that meet the requirements.

Solution 2

The integers could be written as three-digit integers if we allow 0 as the leading digits. For instance, 7 can be written as 007, and 34 as 034. Under this agreement, we have to fill three positions where the last one is always occupied by the digit 7. The first two digits are $0, 1, 2, \ldots, 8$ or 9, so there are 10 choices for each position.

	any	any	
choices:	digit	digit	7
	___	___	___
# of choices:	10	10	1

Together, there are $10 \cdot 10 = 100$ such integers.

hands-on exercise 7.2.5

How many natural numbers less than 1000000 are there that end with the digit 3?

hands-on exercise 7.2.6

How many natural numbers less than 10000 are there that end with the digit 0?

Example 7.2.11

Determine the number of four-digit positive integers without repeated digits.

Solution

We want to determine how many choices there are for each place value. The first digit has nine choices because it cannot be 0. Once the first digit is chosen, there are nine choices left for the second digit; and then eight choices for the next digit, and seven choices for the last digit. Together, we have $9 \cdot 9 \cdot 8 \cdot 7 = 4536$ four-digit positive integers that do not contain any repeated digits. Question: Can we start counting from the last digit?

hands-on exercise 7.2.7

How many six-digit natural numbers are there that do not have any repeated digit?

Example 7.2.12

How many two-digit positive integers do not have consecutive 5s?

Solution 1

There are three *disjoint* cases:

both digits are not 5,

only the first digit is 5, and

only the last digit is 5.

There are $8 \cdot 9 + 9 + 8 = 89$ integers that meet the requirement.

Solution 2

An easier solution is to consider the complement of the problem. There is only one integer with consecutive 5s, namely, the integer 55. There are 90 two-digit integers, hence $90 - 1 = 89$ of them do not have consecutive 5s.

hands-on exercise 7.2.8

How many three-digit natural numbers are there that do not have consecutive 4s?

Example 7.2.13

In how many ways can we draw a sequence of three cards from a standard deck of 52 cards?

Solution

This is a trick question! The answer depends on whether we can return a drawn card to the deck. With replacement, the answer is 52^3; without replacement, it is $52 \cdot 51 \cdot 50$.

Example 7.2.14

A standard New York State license plate consists of three letters followed by four digits. Determine the number of standard New York State license plates with K as the first letter *or* 8 as the first digit.

Solution

The keyword “or” suggests that we are looking at a union, hence, we have to apply PIE. We need to analyze three possibilities:

- There are $26^2 \cdot 10^4$ license plates with K as the first letter.
- There are $26^3 \cdot 10^3$ license plates with 8 as the first digit.
- There are $26^2 \cdot 10^3$ license plates with K as the first letter *and* 8 as the first digit.

The answer is $26^2 \cdot 10^4 + 26^3 \cdot 10^3 - 26^2 \cdot 10^3$.

hands-on exercise 7.2.9

To access personal account information, a customer could log in to the bank’s web site with a PIN consisting of two letters followed by

exactly four digits,

at most six digits,

at least two but at most 6 digits.

How many different PINs are there in each case?

Summary and Review

- Use the addition principle if the problem can be divided into cases. Make sure the cases do not overlap.
- If the cases overlap, the number of objects belonging to the overlapping cases must be subtracted from the total to obtain the correct count.
- In particular, the principle of inclusion-exclusion states that $|A\cup B| = |A|+|B|-|A\cap B|$.
- Use the multiplication principle if the problem can be solved in several steps.
- How can we get started? Imagine you want to list all the possibilities, what is a systematic way of doing so? Follow the steps, and count how many objects you would end up with.
- It may be helpful to use a schematic diagram. Draw one line for each step. Above the lines, write the choices. Below the lines, write the number of choices. Apply the multiplication principle to finish the problem.
- If there are other cases involved, repeat, and add the results from all the possible cases.

Exercises

exercise 7.2.1

A professor surveyed the 98 students in her class to count how many of them had watched at least one of the three films in *The Lord of the Rings* trilogy. This is what she found:

- 74 had watched Part I;
- 57 had watched Part II;
- 66 had watched Part III;
- 52 had watched both Parts I and II;
- 51 had watched both Parts I and III;
- 45 had watched both Parts II and III;
- 43 had watched all three parts.

How many students did not watch any one of these three movies?

(Hint: A Venn Diagram may be helpful.)

Solution

6

exercise 7.2.2

Forty-six students in a film class told the professor that they had watched at least one of the three films in *The Godfather* trilogy. Further inquiry led to the following data:

- 41 had watched Part I;
- 37 had watched Part II;
- 33 had watched Part III;
- 33 had watched both Parts I and II;
- 30 had watched both Parts I and III;
- 29 had watched both Parts II and III.

1. How many students had watched all three films?
2. How many students had watched only Part I?
3. How many students had watched only Part II?
4. How many students had watched only Part III?

exercise 7.2.3

Joe has 10 dress shirts and seven bow ties. In how many ways can he match the shirts with bow ties?

Solution

70

exercise 7.2.4

A social security number is a sequence of nine digits. Determine the number of social security numbers that satisfy the following conditions:

1. There are no restrictions.
2. The digit 8 is never used.
3. The sequence does not begin or end with 8.
4. No digit is used more than once.

exercise 7.2.5

A professor has seven books on discrete mathematics, five on number theory, and four on abstract algebra. In how many ways can a student borrow two books not both on the same subject?

Hint

Which two subjects would the student choose?

Solution

$7 \cdot 5 + 7 \cdot 4 + 5 \cdot 4$

exercise 7.2.6

How many different collections of cans can be formed from five identical Cola-Cola cans, four identical Seven-Up cans, and seven identical Mountain Dew cans?

Hint

How many cans of Cola-Cola, Seven-Up, and Mountain Dew would you pick?

exercise 7.2.7

How many five-letter words (technically, we should call them strings, because we do not care if they make sense) can be formed using the letters A, B, C, and D, with repetitions allowed. How many of them do not contain the substring BAD?

Hint

For the second question, consider using a complement.

Solution

4^5, $4^5 - 3 \cdot 4^2$

exercise 7.2.8

How many different five-digit integers can be formed using the digits 1, 3, 3, 3, 5?

Hint

The three digits 3 are identical, so we cannot tell the difference between them. Consequently, what really matters is where we put the digits 1 and 5. Once we place the digits 1 and 5, the remaining three positions must be occupied by the digits 3.

exercise 7.2.9

Four cards are chosen at random from a standard deck of 52 playing cards, with replacement allowed. This means after choosing a card, the card is return to the deck, and the deck is reshuffled before another card is selected at random. Determine the number of such four-card sequences if

1. There are no restrictions.
2. None of the cards can be spades.
3. All four cards are from the same suit.
4. The first card is an ace and the second card is not a king.
5. At least one of the four cards is an ace.

Solution

(a) 52^4 (b) 39^4 (c) $4 \cdot 13^4$ (d) $4 \cdot 48 \cdot 52^2$ (e) $52^4 - 48^4$

exercise 7.2.10

Three different mathematics final examinations and two different computer science final examinations are to be scheduled during a five-day period. Determine the number of ways to schedule these final examinations from 11 AM to 1 PM if (are these one-hour exams?)

1. There are no restrictions.
2. No two examinations can be scheduled on the same day.
3. No two examinations from the same department can be scheduled on the same day.
4. Each mathematics examination must be the only examination for the day on which it is scheduled.

exercise 7.2.11

Determine the number of four-digit positive integers that satisfy the following conditions:

1. There are no restrictions.
2. No integer contains the digit 8.
3. Every integer contains the digit 8 at least once.
4. Every integer is a palindrome (A positive integer is a palindrome if it remains the same when read backward, for example, 3773 and 47874).

Solution

(a) $9 \cdot 10^3$ (b) $8 \cdot 9^3$ (c) $9 \cdot 10^3 - 8 \cdot 9^3$ (d) $9 \cdot 10$

exercise 7.2.12

A box contains 12 distinct colored balls (for instance, we could label them as 1, 2, …, 12 to distinguish them). Three of them are red, four are yellow, and five are green. Three balls are selected at random from the box, with replacement. Determine the number of sequences that satisfy the following conditions:

1. There are no restrictions.
2. The first ball is red, the second is yellow, and the third is green.
3. The first ball is red, and the second and third balls are green.
4. Exactly two balls are yellow.
5. All three balls are green.
6. All three balls are the same color.
7. At least one of the three balls is red.

exercise 7.2.13

Let $A = \{a, b, c, d, e, f\}$ and $B = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Determine the number of functions $f : A \to B$ that satisfy the following conditions:

1. There are no restrictions.

2. f is one-to-one.
3. f is onto.
4. $f(x)$ is odd for at least one x in A.
5. $f(a) = 3$ and $f(b)$ is odd.
6. $f^{-1}(4) = \{a\}$.

Solution

(a) 8^6 (b) $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$ (c) 0 (d) $8^6 - 4^6$ (e) $4 \cdot 8^4$ (f) 7^5

exercise 7.2.14

How many onto functions are there from an n-element set A to $\{a, b\}$?

7.3: Permutations

Let A be a finite set with n elements. For $1 \leq r \leq n$, an ***r*-permutation** of A is an *ordered* selection of r distinct elements from A. In other words, it is the *linear* arrangement of r distinct objects $a_1 a_2 \ldots a_r$, where $a_i \in A$ for each i. The number of r-permutations of an n-element set is denoted by $P(n,r)$. It also appears in many other forms and names.

- The number of permutations of n objects, taken r at a time without replacement.
- The number of ways to arrange n objects (in a sequence), taken r at a time without replacement.

All of them refer to the same number $P(n,r)$. The keywords are:

1. "*Permutation*" or "*arrangement*," both of which suggest that order does matter.
2. "*Without replacement*" means the entries in the permutation/arrangement are distinct.

In some textbooks and on some calculators, the notation $P(n,r)$ is also written as P_r^n or ${}_nP_r$.

Example 7.3.1

The 1-permutations of $\{a,b,c,d\}$ are

$$a, \quad b, \quad c, \quad d.$$

Consequently, $P(4,1) = 4$. The 2-permutations of $\{a,b,c,d\}$ are

$$\begin{array}{ccc} ab, & ac, & ad, \\ ba, & bc, & bd, \\ ca, & cb, & cd, \\ da, & db, & dc. \end{array}$$

Hence, $P(4,2) = 12$. What are the 3-permutations and 4-permutations of $\{a,b,c,d\}$? Can you explain why the numbers of 3-permutations and 4-permutations are equal?

Computing the value of $P(n,r)$ is easy. We want to arrange r objects in a sequence. These r objects are to be selected from a pool of n items. Hence there are n ways to fill the first position. Once we settle with the first position, whatever we put there cannot be used again. We are left with $n-1$ choices for the second position. Likewise, once it is filled, there are only $n-2$ choices for the third position. Now it is clear that $P(n,r)$ is the product of r numbers of the form $n, n-1, n-2, \ldots$. What is the last number in this list? There are $r-1$ numbers before it, so it must be $n-(r-1) = n-r+1$.

$P(n,r)$ formula

Theorem 7.3.1

For all integers n and r satisfying $1 \leq r \leq n$,

$$P(n,r) = n(n-1)\cdots(n-r+1) = \frac{n!}{(n-r)!}. \tag{7.3.1}$$

Although the formula $P(n,r) = \frac{n!}{(n-r)!}$ is rather easy to remember, the other form

$$P(n,r) = \underbrace{n(n-1)\cdots(n-r+1)}_{r} \tag{7.3.2}$$

is actually more useful in numeric computation, especially when it is done by hand. We multiply n by the next smaller integer $n-1$, and then the next smaller integer $n-2$, and so forth, until we have a product of r consecutive factors. For instance,

$$P(4,2) = 4 \cdot 3 = 12, \qquad \text{and} \qquad P(9,3) = 9 \cdot 8 \cdot 7 = 504. \tag{7.3.3}$$

How about $P(n,1)$ and $P(n,2)$?

Example 7.3.2

How would you compute the value of $P(278,3)$ by hand, or if your calculator does not have that ${}_nP_r$ button?

Solution

We find $P(278,3) = 278 \cdot 277 \cdot 276 = 21253656$

hands-on Exercise 7.3.1

Compute $P(21,4)$ by hand.

Remark

It follows from the first version of the formula that $P(n,n) = n!$. The second version reduces to

$$n! = P(n,n) = \frac{n!}{0!}. \tag{7.3.4}$$

Consequently, to make the second version works, we have to define $0! = 1$.

Remark

In your homework assignments, quizzes, tests, and final exam, it is perfectly fine to use the notation $P(n,r)$ in your answers. In fact, leaving the answers in terms of $P(n,r)$ gives others a clue to how you obtained the answer.

It is often easier and less confusing if we use the multiplication principle. Once you realize the answer involves $P(n,r)$, it is not difficult to figure out the values of n and r. A good start, *before jumping into any calculation*, is to ask yourself, how would you list the possible arrangements? Also, try constructing some examples. These can give you an idea of how many choices you have in each position.

Example 7.3.3

A police station has 12 police officers on duty. In how many ways can they be assigned to foot patrol in five different districts, assuming that we assign only one police officer per district.

Solution

Imagine you are the officer who schedules the assignments. You have to assign someone to the first district, and then another officer to the second district, and so forth.

district:	first	second	third	fourth	fifth
			another		
	any	another	different	…	…
choices:	officer	officer	officer		
	___	___	___	___	___
# of choices:	12	11	10	9	8

There are 12 choices for the first district, 11 for the second, etc. The multiplication principle implies that the answer is $12 \cdot 11 \cdots$, which is in the form of $P(n,r)$. Since the product starts with 12, and we need a product of 5 consecutive numbers, the answer is $P(12,5)$.

hands-on Exercise 7.3.2

A school sends a team of six runners to a relay game. In how many ways can they be selected to participate in the 4×100 m relay?

Example 7.3.4

From a collection of 10 flags of different patterns, how many three-flag signals can we put on a pole?

Solution

Since the flags are arranged on a flag pole, the order is important. There are 10 choices for the top flag, 9 for the second, and 8 for the third. Therefore, $10 \cdot 9 \cdot 8 = P(10, 3)$ different signals can be formed.

Z_n

$Z_n = \{0, 1, 2, 3, \ldots, n-1\}$.

For example, $Z_6 = \{0, 1, 2, 3, 4, 5\}$ or $Z_{22} = \{0, 1, 2, 3, \ldots, 21\}$.

Example 7.3.5

Determine the number of functions $f : \{1, 3, 4, 7, 9\} \to \mathbb{Z}_{22}$ if

1. There are no restrictions.
2. f is one-to-one.
3. f is onto.

Solution

To distinguish one function from another function, we have to compare their images. Hence, a function is completely determined by its images (surprise: not by its formula!). After all, we may not even know the formula behind a function, so we cannot and should not rely on the formula alone.

To determine how many functions there are from $\{1, 3, 4, 7, 9\}$ to $\mathbb{Z}_{22}$, we have to determine the number of ways to assign values to $f(1)$, $f(3)$, $f(4)$, $f(7)$ and $f(9)$.

images:	$f(1)$	$f(3)$	$f(4)$	$f(7)$	$f(9)$
choices:					
# of choices:					

(a) If there are no restrictions, we have 22 choices for each of these five images. Hence there are $22 \cdot 22 \cdot 22 \cdot 22 \cdot 22 = 22^5$ functions.

(b) If f is one-to-one, we cannot duplicate the images. So we have 22 choices for $f(1)$, 21 for $f(3)$, and so on. There are $P(22, 5)$ one-to-one functions.

(c) There are at most five distinct images, but $\mathbb{Z}_{22}$ has 22 elements, so at least 17 of them will be left unused. Hence f can never be onto. The number of onto functions is therefore zero.

hands-on Exercise 7.3.3

How many functions are there from $\{2, 4, 6, 8, 10\}$ to $\mathbb{Z}_{15}$? How many of them are one-to-one?

Example 7.3.6

Let A and B be finite sets, with $|A| = s$ and $|B| = t$. Determine the number of one-to-one functions from A to B.

Solution

How can we come up with a one-to-one function from A to B? We have to specify the image of each element in A. There are t choices for the first element. Since repeated images are not allowed, we have only $t-1$ choices for the image of the second element in A, and $t-2$ choices for the third image, and so forth. The answer is $P(t, s)$.

What if $t < s$? We know that in such an event, there does not exist any one-to-one function from A to B because there are not enough distinct images. Does $P(t, s)$ still make sense? The product version of the formula says that $P(t, s)$ is a product of s consecutive numbers. Hence, for example,

$$P(3,6) = 3\cdot 2\cdot 1\cdot 0\cdot(-1)\cdot(-2) = 0, \tag{7.3.5}$$

which means there is no one-to-one function from A to B.

Not all problems use $P(n,r)$. In many situations, we have to use $P(n,r)$ together with other numbers. The safest approach is to rely on the addition and multiplication principles.

Example 7.3.7

How many four-digit integers are there that do not contain repeated digits?

Solution

There are 10 choices for each digit, but the answer is not $P(10,4)$, because we cannot use 0 as the first digit. To ensure that we have a four-digit integer, the first digit must be nonzero. This leaves us 9 choice for the first digit. Then we have 9 choices for the second digit, 8 and 7 for the next two. The answer is $9\cdot 9\cdot 8\cdot 7$.

Example 7.3.8

Twelve children are playing "musical chairs," with 9 chairs arranged in a circle on the floor. In how many ways can they be seated?

Solution

The answer is not $P(12,9)$ because any position can be the first position in a ***circular permutation***. What matters is the relative placement of the selected objects, all we care is who is sitting next to whom. The correct answer can be found in the next theorem.

Theorem 7.3.1

The number of circular r-permutations of an n-element set is $P(n,r)/r$.

Proof

Compare the number of circular r-permutations to the number of linear r-permutations. Start at any position in a circular r-permutation, and go in the clockwise direction; we obtain a linear r-permutation. Since we can start at any one of the r positions, each circular r-permutation produces r linear r-permutations. This means that there are r times as many circular r-permutations as there are linear r-permutations. Therefore, the number of circular r-permutations is $P(n,r)/r$.

Alternate Proof

Let A be the set of all linear r-permutations of the n objects, and let B be the set of all circular r-permutations. Define a function from A to B as follows. Given any r-permutation, form its image by joining its "head" to its "tail." It becomes clear, using the same argument in the proof above, that f is an r-to-one function, which means f maps r distinct elements from A to the same image in B. Therefore A has r times as many elements as in B. This means $|A| = r\cdot|B|$. Since $|A| = P(n,r)$, we find $|B| = P(n,r)/r$.

hands-on Exercise 7.3.4

A circular cardboard has eight dots marked along its rim. In how many ways can we glue eight beads of different colors, one on each dot?

hands-on Exercise 7.3.5

In how many ways can we form a necklace with eight beads of different color?

Remark: When a necklace is flipped around, it is still the same necklace. Thus, the orientation of the necklace does not matter: we can count the beads clockwise, or counterclockwise.

Example 7.3.9

In how many ways can we arrange 20 knights at a round table? What if two of them refuse to sit next to each other?

Solution

Without any restriction, there are $20!/20 = 19!$ ways to seat the 20 knights. To solve the second problem, use complement. If two of them always sit together, we in effect are arranging 19 objects in a circle. Among themselves, these two knights can be seated in two ways, depending on who is sitting on the left. Hence, there are $2 \cdot 19!/19 = 2 \cdot 18!$ ways to seat the 20 knights, with two of them always together. Therefore, the final answer to the second problem is $19! - 2 \cdot 18!$.

Summary and Review

- Use permutation if order matters: the keywords arrangement, sequence, and order suggest that we should use permutation.
- It is often more effective to use the multiplication principle directly.
- The number of ways to arrange n objects linearly is $n!$, and the number of ways to arrange them in a circle is $(n-1)!$.

Exercises

Exercise 7.3.1

How many eight-character passwords can be formed with the 26 letters in the English alphabet, each of which can be in uppercase or lowercase, and the 10 digits? How many of can be formed if they do not have any repeated characters?

Solution

62^8, $P(62,8)$.

Exercise 7.3.2

How many functions are there from $\mathbb{Z}_6$ to $\mathbb{Z}_{12}$? How many of them are one-to-one?

Exercise 7.3.3

The school board of a school district has 14 members. In how many ways can the chair, first vice-chair, second vice-chair, treasurer, and secretary be selected?

Solution

$P(14,5)$.

Exercise 7.3.4

The wrestling teams of two schools have eight and 10 members respectively. In how many ways can three matches be made up between them?

Exercise 7.3.5

Six students in the class will sit in a group in a circle.

(a) How many arrangements are there?

(b) How many arrangements are there if two students insist on sitting next to each other?

Solution

(a) $\frac{6!}{6} = 5!$
(b) $2 \cdot \frac{5!}{5} = 2 \cdot 4!$

Exercise 7.3.6

A teacher takes her AP calculus class of 8 students to lunch. They sit around a circular dining table.

1. How many seating arrangements are possible?
2. How many seating arrangements are there if the teacher has to sit on the chair closest to the soda fountain?
3. Among the students are one set of triplets. How many seating arrangements are there without all three of them sitting together?

Exercise $7.3.7$

Eleven students go to lunch. There are two circular tables in the dining hall, one can seat 7 people, the other can hold 4. In how many ways can they be seated?

Solution

$P(11,7)\cdot 3!/7.$

Exercise $7.3.8$

Five couples attend a wedding banquet. They are seated on a long table. How many seating arrangements that alternate men and women? What if the table is circular in shape?

7.4: Combinations

In many counting problems, the order of arrangement or selection does not matter. In essence, we are selecting or forming subsets.

If we are choosing 3 people out of 20 Discrete students to be president, vice-president and janitor, then the order makes a difference. The choice of:

Steve, Ahmet, Liz (SAL) v.s Liz, Ahmet, Steve (LAS) would make quite a difference for Liz and Steve. Permutations include all the different arrangements, so we say "order matters" and there are $P(20,3)$ ways to choose 3 people out of 20 to be president, vice-president and janitor.

Now, change the scenario to chose 3 people out of 20 to get an A for the course. This time SAL and LAS are not considered different choices; here we say "order does not matter". This scenario is the number of combinations (basically subsets) and we call this one "20 choose 3". With permutations, each set of 3 letters, such as SAL, will be rearranged $3!$ or 6 times. For combinations, we only use a set of 3 letters once (since order does not matter) and so the number of combinations in this case will be $\frac{P(20,3)}{3!}$.

Example 7.4.1

Determine the number of ways to choose 4 values from 1, 2, 3, …, 20, in which the order of selection does not matter.

Solution

Let N be the number of ways to choose the 4 numbers. Since the order in which the numbers are selected does not matter, these are *not* sequences (in which order of appearance matters). We can change a selection of 4 numbers into a sequence. The 4 numbers can be arranged in $P(4,4)=4!$ ways. Therefore, all these 4-number selections together produce $N\cdot 4!$ sequences. The number of 4-number sequences is $P(20,4)$. Thus, $N\cdot 4!=P(20,4)$, or equivalently, $N=P(20,4)/4!$.

Definition: combinations

The number of r-element subsets in an n-element set is denoted by

$$C(n,r) \qquad \text{or} \qquad \binom{n}{r}, \tag{7.4.1}$$

where $\binom{n}{r}$ is read as "n choose r." It determines the number of ***combinations*** of n objects, taken r at a time (without replacement). Alternate notations such as ${}_nC_r$ and C_r^n can be found in other textbooks and some calculators. Do *not* write it as $(\frac{n}{r})$; this notation has a completely different meaning.

Recall that $\binom{n}{r}$ counts the number of ways to *choose* or *select* r objects from a pool of n objects in which the order of selection does not matter. Hence, r-combinations are subsets of size r.

Example 7.4.2

The 2-combinations of $S=\{a,b,c,d\}$ are

$$\{a,b\}, \quad \{a,c\}, \quad \{a,d\}, \quad \{b,c\}, \quad \{b,d\}, \quad \text{and} \quad \{c,d\}. \tag{7.4.2}$$

Therefore $\binom{4}{2}=6$. What are the 1-combinations and 3-combinations of S? What can you say about the values of $\binom{4}{1}$ and $\binom{4}{3}$?

Solution

The 1-combinations are the singleton sets $\{a\}$, $\{b\}$, $\{c\}$, and $\{d\}$. Hence, $\binom{4}{1}=4$. The 3-combinations are

$$\{a,b,c\}, \quad \{a,b,d\}, \quad \{a,c,d\}, \quad \text{and} \quad \{b,c,d\}. \tag{7.4.3}$$

Thus, $\binom{4}{3}=4$.

C(n,r) formula

Theorem 7.4.1

For all integers n and r satisfying $0\leq r\leq n$, we have

$$\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{r!\,(n-r)!}. \tag{7.4.4}$$

Proof

The idea is similar to the one we used in the alternate proof of Theorem [thm:circperm]. Let A be the set of all r-permutations, and let B be the set of all r-combinations. Define \fcn$fAB$ to be the function that converts a permutation into a combination by "unscrambling" its order. Then f is an $r!$-to-one function because there are $r!$ ways to arrange (or shuffle) r objects. Therefore

$$|A| = r! \cdot |B|. \tag{7.4.5}$$

Since $|A| = P(n,r)$, and $|B| = \binom{n}{r}$, it follows that $\binom{n}{r} = P(n,r)/r!$.

Example 7.4.3

There are $\binom{40}{5}$ ways to choose 5 numbers, without repetitions, from the integers $1,2,\ldots,40$. To compute its numeric value by hand, it is easier if we first cancel the common factors in the numerator and the denominator. We find

$$\binom{40}{5} = \frac{40\cdot 39\cdot 38\cdot 37\cdot 36}{5\cdot 4\cdot 3\cdot 2\cdot 1} = 13\cdot 38\cdot 37\cdot 36, \tag{7.4.6}$$

which gives $\binom{40}{5} = 658008$.

hands-on Exercise 7.4.1

Compute $\binom{12}{3}$ by hand.

hands-on Exercise 7.4.2

A three-member executive committee is to be selected from a group of seven candidates. In how many ways can the committee be formed?

hands-on Exercise 7.4.3

How many subsets of $\{1,2,\ldots,23\}$have five elements?

$\binom{n}{r} = \binom{n}{n-r}$

Theorem 7.4.2

For $0 \leq r \leq n$, we have $\binom{n}{r} = \binom{n}{n-r}$.

Proof

According to Theorem 7.4.1 we have

$$\binom{n}{n-r} = \frac{n!}{(n-r)!\,(n-(n-r))!} = \frac{n!}{(n-r)!\,r!}, \tag{7.4.7}$$

which is precisely $\binom{n}{r}$.

Example 7.4.4

To compute the numeric value of $\binom{50}{47}$, instead of computing the product of 47 factors as indicated in the definition, it is much faster if we use

$$\binom{50}{47} = \binom{50}{3} = \frac{50\cdot 49\cdot 48}{3\cdot 2\cdot 1}, \tag{7.4.8}$$

from which we obtain $\binom{50}{47} = 19600$.

hands-on Exercise 7.4.4

Compute, by hand, the numeric value of $\binom{529}{525}$.

Pascal's Triangle

In this section we will cover

- how to construct Pascal's Triangle
- how to read values for combinations from Pascal's Triangle

In a later section, we will prove that this construction does give the values for combinations.

Start with a 1, then two more 1's. Notice how the spacing is offset on each row.

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 1 & & \\ & 1 & & 2 & & 1 & \\ 1 & & 3 & & 3 & & 1 \end{array} \tag{7.4.9}$$

To create the next row, start with a 1 and then add the two entries just above. So under the $1 \quad 3 \quad 3 \quad 1$ row, start with a 1, then add $1+3=4$ to get the next entry, then $3+3=6$, etc. Notice the symmetry; this relates to Theorem 7.4.2.

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array} \tag{7.4.10}$$

Here's more of the triangle:

$$\begin{array}{ccccccccccccc} & & & & & & 1 & & & & & & \\ & & & & & 1 & & 1 & & & & & \\ & & & & 1 & & 2 & & 1 & & & & \\ & & & 1 & & 3 & & 3 & & 1 & & & \\ & & 1 & & 4 & & 6 & & 4 & & 1 & & \\ & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\ 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \end{array} \tag{7.4.11}$$

From the top, these rows are the 0-row, the 1-row, the 2-row, etc.

The 5-row consists of:

$$\begin{array}{cccccc} 1 & 5 & 10 & 10 & 5 & 1 \end{array} \tag{7.4.12}$$

These numbers correspond to:

$$\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5} \quad . \tag{7.4.13}$$

The symmetry of the triangle shows the symmetric values, such as $\binom{5}{1} = \binom{5}{4}$

Example 7.4.5

Use Pascal's Triangle to find $\binom{7}{3}$.

Answer

After the 6-row (see above) create the 7-row.

$$\begin{array}{cccccccc} 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \end{array} \tag{7.4.14}$$

Count over, $\binom{7}{0}=1$, $\binom{7}{1}=7$, $\binom{7}{2}=21$, so the answer is

$$\binom{7}{3}=35. \tag{7.4.15}$$

Now we are ready to look at some mixed examples. In all of these examples, sometimes we have to use permutation, other times we have to use combination. Very often we need to use both, together with the addition and multiplication principles. You may ask, how can I figure out what to do? We suggest asking yourself these questions:

1. Use the construction approach. If you want to list all the configurations that meet the requirement, how are you going to do it systematically?
2. Are there several cases involved in the problem? If yes, we need to list them first, *before* we go through each of them one at a time. Finally, add the results to come up with the final answer.
3. Do we allow repetitions or replacements? This question can also take the form of whether the objects are distinguishable or indistinguishable.
4. Does order matter? If yes, we have to use permutation. Otherwise, use combination.
5. Sometimes, it may be easier to use the multiplication principle instead of permutation, because repetitions may be allowed (in which case, we cannot use permutation, although we can still use the multiplication principle). Try drawing a schematic diagram and decide what we need from it. If the analysis suggests a pattern that follows the one found in a permutation, you can then use the formula for permutation.
6. Do not forget: it may be easier to work with the complement.

It is often not clear how to get started because there seem to be several ways to start the construction. For example, how would you distribute soda cans among a group of students? There are two possible approaches:

- From the perspective of the students. Imagine you are one of the students, which soda would you receive?
- From the perspective of the soda cans. Imagine you are holding a can of soda, to whom would you give this soda?

Depending on the actual problem, usually only one of these two approaches would work.

Example 7.4.5

Suppose we have to distribute 10 different soda cans to 20 students. It is clear that some students may not get any soda. In fact, some lucky students could receive more than one soda (the problem does not say this cannot happen). Hence, it is easier to start from the perspective of the soda cans.

Solution

We can give the first soda to any one of the 20 students, and we can also give the second soda to any one of the 20 students. In fact, we always have 20 choices for each soda. Since we have 10 sodas, there are $\underbrace{20\cdot 20\cdots 20}_{10}=20^{10}$ ways to distribute the sodas.

Example 7.4.6

In how many ways can a team of three representatives be selected from a class of 885 students? In how many ways can a team of three representatives consisting of a chairperson, a vice-chairperson, and a secretary be selected?

Solution

If we are only interested in selecting three representatives, order does not matter. Hence, the answer would be $\binom{885}{3}$. If we are concerned about which offices these three representative will hold, then the answer should be $P(885,3)$.

hands-on Exercise 7.4.5

Mike needs some new shirts, but he has only enough money to purchase five of the eight that he likes. In how many ways can he purchase the five shirts by choosing them at random?

hands-on Exercise 7.4.6

Mary wants to purchase four shirts for her four brothers, and she would like each of them to receive a different shirt. She finds ten shirts that she thinks they will like. In many ways can she select them?

Playing cards provide excellent examples for counting problems. Just in case you are not familiar with them, let us briefly review what a deck of playing cards contains.

- There are 52 playing cards, each of them is marked with a suit and a rank.
- There are four suits: spades ($\spadesuit$), hearts ($\heartsuit$), diamonds ($\diamondsuit$) and clubs ($\clubsuit$).
- Each suit has 13 ranks, labeled A, 2, 3, …, 9, 10, J, Q, and K, where A means ace, J means jack, Q means queen, and K means king.
- Each rank has 4 suits (see above).

hands-on Exercise 7.4.7

Determine the number of five-card poker hands that can be dealt from a deck of 52 cards.

Solution

All we care is which five cards can be found in a hand. This is a selection problem. The answer is $\binom{52}{5}$.

hands-on exercise 7.4.7

In how many ways can a 13-card bridge hand be dealt from a standard deck of 52 cards?

Example 7.4.8

In how many ways can a deck of 52 cards be dealt in a game of bridge? (In a bridge game, there are four players designated as North, East, South and West, each of them is dealt a hand of 13 cards.)

Solution

The difference between this problem and the last example is that the order of distributing the four bridge hands makes a difference. This is a problem that combines permutations and combinations. As we had suggested earlier, the best approach is to start from scratch, using the addition and/or multiplication principles, along with permutation and/or combination whenever it seems appropriate.

There are $\binom{52}{13}$ ways to give 13 cards to the first player. Now we are left with 39 cards, from which we select 13 to be given to the second player. Now, out of the remaining 26 cards, we have to give 13 to the third player. Finally, the last 13 cards will be given to the last player (there is only one way to do it). The number of ways to deal the cards in a bridge game is $\binom{52}{13}\binom{39}{13}\binom{26}{13}$.

We could have said the answer is

$$\binom{52}{13}\binom{39}{13}\binom{26}{13}\binom{13}{13}. \tag{7.4.16}$$

The last factor $\binom{13}{13}$ is the number of ways to give the last 13 cards to the fourth player. Numerically, $\binom{13}{13}=1$, so the two answers are the same. Do not dismiss this extra factor as redundant. Take note of the nice pattern in this answer. The bottom numbers are 13, because we are selecting 13 cards to be given to each player. The top numbers indicate how many cards are still available for distribution at each stage of the distribution. The reasoning behind the solution is self-explanatory!

[eg:combin-08]

Example 7.4.9

Determine the number of five-card poker hands that contain three queens. How many of them contain, in addition to the three queens, another pair of cards?

Solution

(a) The first step is to choose the three queens in $\binom{4}{3}$ ways, after which the remaining two cards can be selected in $\binom{48}{2}$ ways. Therefore, there are altogether $\binom{4}{3}\binom{48}{2}$ hands that meet the requirements.

Solution

(b) As in part (a), the three queens can be selected in $\binom{4}{3}$ ways. Next, we need to select the pair. We can select any card from the remaining 48 cards (therefore, there are 48 choices), after which we have to select one from the remaining 3 cards of the same rank. This gives $48 \cdot 3$ choices for the pair, right? The answer is *NO*!

The first card we picked could be $\heartsuit 8$, and the second could be $\clubsuit 8$. However, the first card could have been $\clubsuit 8$, and the second $\heartsuit 8$. These two selections are counted as *different* selections, but they are actually the same pair! The trouble is, we are considering "first," and "second" cards, which in effect imposes an ordering among the two cards, thereby turning it into a sequence or an *ordered* selection. We have to divide the answer by 2 to overcome the double-counting. The answer is therefore $\frac{48 \cdot 3}{2}$.

Here is a better way to count the number of pairs. An important question to ask is

> *Which one should we pick first: the suit or the rank?*

Here, we want to pick the rank first. There are 12 choices (the pair cannot be queens) for the rank, and among the four cards of that rank, we can pick the two cards in $\binom{4}{2}$ ways. Therefore, the answer is $12\binom{4}{2}$. Numerically, the two answers are identical, because $12\binom{4}{2} = 12 \cdot \frac{4 \cdot 3}{2} = \frac{48 \cdot 3}{2}$. In summary: the final answer is $\binom{4}{3} \cdot 12\binom{4}{2}$.

hands-on Exercise 7.4.8

How many bridge hands contain exactly four spades?

hands-on Exercise 7.4.9

How many bridge hands contain exactly four spades and four hearts?

hands-on Exercise 7.4.10

How many bridge hands are there containing exactly four spades, three hearts, three diamonds, and three clubs?

Example 7.4.10

How many positive integers not exceeding 99999 contain exactly three 7s?

Solution

Regard each legitimate integer as a sequence of five digits, each of them selected from 0, 1, 2, …, 9. For example, the integer 358 can be considered as 00358. Three out of the five positions must be occupied by 7. There are $\binom{5}{3}$ ways to select these three slots. The remaining two positions can be filled with any of the other nine digits. Hence, there are $\binom{5}{3} \cdot 9^2$ such integers.

Example 7.4.11

How many five-digit positive integers contain exactly three 7s?

Solution

Unlike the last example, the first of the five digits cannot be 0. Yet, the answer is *not* $\binom{5}{3} \cdot 9 \cdot 8$. Yes, there are $\binom{5}{3}$ choices for the placement of the three 7s, but some of these selections may have put the 7s in the last four positions. This leaves the first digit unfilled. The nine choices counted by 9 allows a zero to be placed in the first position. The result is, at best, a four-digit number. The correct approach is to consider two cases:

Case 1. If the first digit is not 7, then there are eight ways to fill this slot. Among the remaining four positions, three of them must be 7, and the last one can be any digit other than 7. So there are $8 \cdot \binom{4}{3} \cdot 9$ integers in this category.

Case 2. If the first digit is 7, we still have to put the other two 7s in the other four positions. There are $\binom{4}{2} \cdot 9^2$ such integers.

Together, the two cases give a total of $8 \cdot \binom{4}{3} \cdot 9 + \binom{4}{2} \cdot 9^2 = 774$ integers.

hands-on Exercise 7.4.11

Five balls are chosen from a bag of eight blue balls, six red balls, and five green balls. How many of these five-ball selections contain exactly two blue balls?

Example 7.4.12

Find the number of ways to select five balls from a bag of six red balls, eight blue balls and four yellow balls such that the five-ball selections contain exactly two red balls *or* two blue balls.

Solution

The keyword "or" suggests this is a problem that involves the union of two sets, hence, we have to use PIE to solve the problem.

- How many selections contain two red balls? Following the same argument used in the last example, the answer is $\binom{6}{2}\binom{12}{3}$.
- How many selections contain two blue balls? The answer is $\binom{8}{2}\binom{10}{3}$.
- According to PIE, the final answer is

$$\binom{6}{2}\binom{12}{3}+\binom{8}{2}\binom{10}{3}-\binom{6}{2}\binom{8}{2}\binom{4}{1}. \tag{7.4.17}$$

  In each term, the upper numbers always add up to 18, and the sum of the lower numbers is always 5. Can you explain why?
- How many selections contain two red balls *and* 2 blue balls? The answer is $\binom{6}{2}\binom{8}{2}\binom{4}{1}$.

Example 7.4.13

We have 11 balls, five of which are blue, three of which are red, and the remaining three are green. How many collection of four balls can be selected such that at least two blue balls are selected? Assume that balls of the same color are indistinguishable.

Solution

The keywords "at least" mean we could have two, three, or four blue balls. There are

$$\binom{5}{2}\binom{6}{2}+\binom{5}{3}\binom{6}{1}+\binom{5}{4}\binom{6}{0} \tag{7.4.18}$$

ways to select four balls, with at least two of them being blue.

hands-on Exercise 7.4.12

Jerry bought eight cans of Pepsi, seven cans of Sprite, three cans of Dr. Pepper, and six cans of Mountain Dew. He want to bring 10 cans to his pal's house when they watch the basketball game tonight. Assuming the cans are distinguishable, say, with different expiration dates, how many selections can he make if he wants to bring

1. Exactly four cans of Pepsi?
2. At least four cans of Pepsi?
3. At most four cans of Pepsi?
4. Exactly three cans of Pepsi, and at most three cans of Sprite?

The proof of the next result uses what we call a combinatorial or counting argument. In general, a combinatorial argument does not rely on algebraic manipulation. Rather, it uses the combinatorial significance of the situations to solve the problem.

$\sum_{r=0}^{n}\binom{n}{r}=2^n$

Theorem 7.4.3

Prove that $\sum_{r=0}^{n}\binom{n}{r}=2^n$ for all nonnegative integers n.

Proof

Since $\binom{n}{r}$ counts the number of r-element subsets selected from an n-element set S, the summation on the left is the sum of the number of subsets of S of all possible cardinalities. In other words, this is the total number of subsets in S. We learned earlier that S has 2^n subsets, which establishes the identity immediately.

Summary and Review

- Use permutation if order matters, otherwise use combination.
- The keywords arrangement, sequence, and order suggest using permutation.
- The keywords selection, subset, and group suggest using combination.
- It is best to start with a construction. Imagine you want to list all the possibilities, how would you get started?
- We may need to use both permutation and combination, and very likely we may also need to use the addition and multiplication principles.

Exercises

Exercise 7.4.1

If the Buffalo Bills and the Cleveland Browns have eight and six players, respectively, available for trading, in how many ways can they swap three players for three players?

Solution

$\binom{6}{3}\binom{8}{3}$.

Exercise 7.4.2

In the game of Mastermind, one player, the codemaker, selects a sequence of four colors (the “code”) selected from red, blue, green, white, black, and yellow.

a) How many different codes can be formed?

b) How many codes use four different colors?

c) How many codes use only one color?

d) How many codes use exactly two colors?

e) How many codes use exactly three colors?

Exercise 7.4.3

Becky likes to watch DVDs each evening. How many DVDs must she have if she is able to watch every evening for 24 consecutive evenings during her winter break?

a) A different subset of DVDs?

b) A different subset of three DVDs?

Solution

(a) at least 5 (b) at least 7

Exercise 7.4.4

Bridget has n friends from her bridge club. Every Thursday evening, she invites three friends to her home for a bridge game. She always sits in the north position, and she decides which friends are to sit in the east, south, and west positions. She is able to do this for 200 weeks without repeating a seating arrangement. What is the minimum value of n?

Exercise 7.4.5

Bridget has n friends from her bridge club. She is able to invite a different subset of three of them to her home every Thursday evening for 100 weeks. What is the minimum value of n?

Solution

10.

Exercise 7.4.6

How many five-digit numbers can be formed from the digits 1, 2, 3, 4, 5, 6, 7? How many of them do not have repeated digits?

Exercise 7.4.7

The Mathematics Department of a small college has three full professors, seven associate professors, and four assistant professors. In how many ways can a four-member committee be formed under these restrictions:

a) There are no restrictions.

b) At least one full professor is selected.

c) The committee must contain a professor from each rank.

Solution

(a) $\binom{14}{4}$ (b) $\binom{14}{4}-\binom{11}{4}$ (c) $\binom{3}{2}\binom{7}{1}\binom{4}{1}+\binom{3}{1}\binom{7}{2}\binom{4}{1}+\binom{3}{1}\binom{7}{1}\binom{4}{2}$

Exercise 7.4.8

A department store manager receives from the company headquarters 12 football tickets to the same game (hence they can be regarded as "identical"). In how many ways can she distribute them to 20 employees if no one gets more than one ticket? What if the tickets are for 12 different games?

Exercise 7.4.9

A checkerboard has 64 distinct squares arranged into eight rows and eight columns.

a) In how many ways can eight identical checkers be placed on the board so that no two checkers can occupy the same row or the same column?

b) In how many ways can two identical red checkers and two identical black checkers be placed on the board so that no two checkers of the same color can occupy the same row or the same column?

Solution

(a) 8! (b) $\binom{8}{2}P(8,2)\left[\binom{6}{2}P(8,2)+2\cdot7\cdot6\cdot7+7\cdot6\right]$

Exercise 7.4.10

Determine the number of permutations of $\{A,B,C,D,E\}$ that satisfy the following conditions:

a) A occupies the first position.

b) A occupies the first position, and B the second.

c) A appears before B.

Exercise 7.4.11

A binary string is a sequence of digits chosen from 0 and 1. How many binary strings of length 16 contain exactly seven 1s?

Solution

$\binom{16}{7}$.

Exercise 7.4.12

In how many ways can a nonempty subset of people be chosen from eight men and eight women so that every subset contains an equal number of men and women?

Exercise 7.4.13

A poker hand is a five-card selection chosen from a standard deck of 52 cards. How many poker hands satisfy the following conditions?

a) There are no restrictions.

b) The hand contains at least one card from each suit.

c) The hand contains exactly one pair (the other three cards all of different ranks).

d) The hand contains three of a rank (the other two cards all of different ranks).

e) The hand is a full house (three of one rank and a pair of another).

f) The hand is a straight (consecutive ranks, as in 5, 6, 7, 8, 9, but not all from the same suit).

g) The hand is a flush (all the same suit, but not a straight).

h) The hand is a straight flush (both straight and flush).

Solution

(a) $\binom{52}{5}$ (b) $4\binom{13}{2}13^3$ (c) $13\binom{4}{2}\binom{12}{3}4^3$ (d) $13\binom{4}{3}\binom{12}{2}4^2$
(e) $13\binom{4}{3}12\binom{4}{2}$ (f) $10\cdot(4^5-4)$ (g) $4\left[\binom{13}{5}-10\right]$ (h) $4\cdot 10$

Exercise 7.4.14

A local pizza restaurant offers the following toppings on their cheese pizzas: extra cheese, pepperoni, mushrooms, green peppers, onions, sausage, ham, and anchovies.

a) How many kinds of pizzas can one order?

b) How many kinds of pizzas can one order with exactly three toppings?

c) How many kinds of vegetarian pizza (without pepperoni, sausage, or ham) can one order?

Exercise 7.4.15

Write the numbers for the 8-row for Pascal's Triangle.

Solution

$$1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1 \tag{7.4.19}$$

Exercise 7.4.16

In terms of selecting objects and Pascal's Triangle, explain why

(a) $\binom{8}{0} = \binom{8}{8}$

(b) $\binom{8}{1} = 8$

(c) $\binom{8}{2}$ is the third number in the 8-row rather than the second number

Exercise 7.4.17

Use the 8-row of Pascal's Triangle to find

(a) $\binom{8}{4}$

(b) $\binom{8}{6}$

(c) $\binom{8}{5} = \binom{?}{?}$

Solution

(a) 70 (b) 28 (c) $\binom{8}{5} = \binom{8}{3}$

7.5: Combinations WITH Repetitions

Consider our choice of 3 people out of 20 Discrete students.

Permutations include all the different arrangements, so we say "order matters" and there are $P(20,3)$ ways to choose 3 people out of 20 to be president, vice-president and janitor. Steve, Ahmet, Liz (SAL) v.s Liz, Ahmet, Steve (LAS) are two different arrangements.

For combinations, we chose 3 people out of 20 to get an A for the course so order does not matter. This is "20 choose 3", the number of sets of 3 where order does not matter. SAL and LAS are the same arrangement. This one is $\binom{20}{3}$.

In both permutations and combinations, repetition is not allowed. LLA is not a choice.

Now we move to combinations with repetitions. Here we are choosing 3 people out of 20 Discrete students, but we allow for repeated people. These are combinations, so SAL and LAS are still the same choice, but we have other distinct choices such as LLA, SSS, WAW, SWW, and many more!

Example $7.5.1$ First example

Determine the number of ways to choose 3 tea bags to put into the teapot. You have 100 each of these six types of tea: Black tea, Chamomile, Earl Grey, Green, Jasmine and Rose. (Essentially you have an unlimited number of each type of tea.). You can repeat types of tea.

For example, some choices are: CEJ, CEE, JJJ, GGR, etc.

type of tea:	Black	Chamomile	Earl Grey	Green	Jasmine	Rose
choices:	x		xx			
# of choices:	1	0	2	0	0	0

This arrangement is BEE.

type of tea:	Black	Chamomile	Earl Grey	Green	Jasmine	Rose
choices:				xx		x
# of choices:	0	0	0	2	0	1

This arrangement is GGR.

Reduce this table as follows: Black | Chamomile | Earl Grey | Green | Jasmine | Rose

to just dividers: | | | | |

Our 6 types of tea gives us 5 dividers.

We are choosing 3 tea bags, so we need 3 x's along with the 5 dividers.

Here are the two choices on the tables above: x | | x x | | | and | | | x x | | x.

What are the letters for these two choices? | | | | xx|x and x| | x | x | | .

Answer

JJR and BEG

We are arranging 8 objects (5 dividers and 3 choices of tea bags), so we have 8 spots to put the 3 tea bags.

______ ______ ______ ______ ______ ______ ______ ______

Once we place the 3 tea bags, the placement of the 5 dividers is automatically determined.

There are $\binom{8}{3}$ ways to pick the 3 tea bags.

Where did the 8 and 3 come from? See the following theorem.

Combination with Repetition formula

Theorem 7.5.1

If we choose a set of r items from n types of items, where repetition is allowed and the number items we are choosing from is essentially unlimited, the number of selections possible:

$$\binom{n+r-1}{r}. \tag{7.5.1}$$

Example 7.5.2 Example with Restrictions

From an unlimited selection of five types of soda, one of which is Dr. Pepper, you are putting 25 cans on a table.

(a) Determine the number of ways you can select 25 cans of soda.

Solution

This is the case with no restrictions. $\binom{5+25-1}{25}=\binom{29}{25}=23751$
There are 23751 ways to select 25 cans of soda with five types.

(b) Determine the number of ways you can select 25 cans of soda if you must include at least seven Dr. Peppers.

Solution

Here figure seven Dr. Peppers are already selected, so you are really choosing $25-7=18$ cans. $\binom{5+18-1}{18}=\binom{22}{18}=7315$
There are 7315 ways to select 25 cans of soda with five types, with at least seven of one specific type.

(c) Determine the number of ways you can select 25 cans of soda if it turns out there are only three Dr. Peppers available.

Solution

This is harder to do directly, and easier to use the complement. The complement is "four or more Dr. Peppers" which is at least four Dr. Peppers.
Following our reasoning in (b), the number of ways to select 25 cans with at least four Dr. Peppers is $\binom{5+21-1}{21}=\binom{25}{21}=12650.$
So there are 12650 ways to get four or more Dr. Peppers. We need to subtract that from the total in order to get the number of three or less Dr. Peppers.
$\binom{5+25-1}{25}-\binom{5+21-1}{21}=\binom{29}{25}-\binom{25}{21}=23751-12650=11101.$
There are 11101 ways to select 25 cans of soda with five types, with no more than three of one specific type.

Summary and Review

- Permutations: order matters, repetitions are not allowed.
- (regular) Combinations: order does NOT matter, repetitions are not allowed.
- Combinations WITH Repetitions: order does NOT matter, repetitions ARE allowed.

Exercises

Exercise 7.5.1

Lollypop Farm has cats, dogs, goats, ducks and horses. How many ways can you select three pets to take home?

Solution

$\binom{7}{3} = 35$

Exercise 7.5.2

You are going to bring two bags of chips to a party. In the chip aisle, you see regular potato chips, barbecue potato chips, sour cream and onion potato chips, corn chips and scoopable corn chips. How many selections can you make?

Exercise 7.5.3

(a) Compute $\binom{5+7-1}{7}$ (to an integer).

(b) If you had to compute $\binom{5+7-1}{7}$ without a calculator, how could you simplify the calculations?

(c) Fill in the blanks to create a problem whose solution is the formula in (a):

You are sitting with a number of friends and go to get ____________cans of soda for your table. There are __________types of soda. How many selections can you make?

Solution

(a) 330
(b) $\binom{5+7-1}{7} = \binom{11}{7} = \binom{11}{4} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{4 \cdot 3 \cdot 2 \cdot 1} = \frac{11 \cdot 10 \cdot 9}{3} = 11 \cdot 10 \cdot 3 = 110 \cdot 3 = 330$
(c) get 7 cans of soda; 5 types of soda

Exercise 7.5.4

You are setting out 30 cans of drinks. There are six types of drinks, and one type is seltzer.

(a) How many ways can you choose drinks to set out?

(b) How many ways can you choose drinks to set out that include at least 8 cans of seltzer?

(c) How many ways can you choose drinks to set out if there are only 5 cans of seltzer available?

Exercise 7.5.5

Twenty batteries will be put on the display. The types of batteries are: AAA, AA, C, D, and 9-volt.

(a) How many ways can we choose the twenty batteries?

(b) How many ways can we choose the twenty batteries but be sure that at least four batteries that are are 9-volt batteries?

(c) How many ways can we choose the twenty batteries but have no more than two batteries that are 9-volt batteries?

Solution

(a) $\binom{24}{20} = 10626$

(b) $\binom{20}{16} = 4845$

(c) $\binom{24}{20} - \binom{21}{17} = 4641$

Exercise 7.5.6

Use the tea bags from Example 7.5.1: Black, Chamomile, Earl Grey, Green, Jasmine and Rose for these questions.

(a) You are making a cup of tea for the Provost, a math professor and a student. How many ways can you do this?

(b) You are making a cup of tea for the Provost, a math professor and a student. Each person will have a different flavor. How many ways can you do this?

(c) You are making a pot of tea with four tea bags. How many ways can you do this?

(d) You are making a pot of tea with four tea bags, each a different flavor. How many ways can you do this?

(e) You are setting out 30 tea bags. How many ways can you do this?

(f) You are setting out 30 tea bags, but there are only five Rose tea bags available. How many ways can you do this?

(g) You are setting out 30 tea bags and will include at least 10 Earl Grey. How many ways can you do this?

Exercise 7.5.7

How many non-negative integer solutions are there to this equation:

$$x_1 + x_2 + x_3 + x_4 = 18? \tag{7.5.2}$$

Solution

$\binom{21}{18} = 1330$

Exercise 7.5.8

How many non-negative solutions are there to this equation:

$$x_1 + x_2 + x_3 + x_4 + x_5 = 26? \tag{7.5.3}$$

7.6: The Binomial Theorem

A binomial is a polynomial with exactly two terms. The ***binomial theorem*** gives a formula for expanding $(x+y)^n$ for any positive integer n.

How do we expand a product of polynomials? We pick one term from the first polynomial, multiply by a term chosen from the second polynomial, and then multiply by a term selected from the third polynomial, and so forth. In the special case of $(x+y)^n$, we are selecting either x or y from each of the n binomials $x+y$ to form a product. Some of these products will be identical, hence, we need to collect their coefficients. The expansion of $(x+y)^3$ is demonstrated below.

We find

$$\begin{aligned}(x+y)^3 &= (x+y)(x+y)(x+y) \\ &= xxx+xxy+xyx+xyy+yxx+yxy+yyx+yyy \\ &= x^3+x^2y+x^2y+xy^2+x^2y+xy^2+xy^2+y^3 \\ &= x^3+3x^2y+3xy^2+y^3.\end{aligned}$$

What happens when we expand $(x+y)^n$?

If we select y from k copies of the $(x+y)$s, and x from the other $n-k$ copies, their product will be $x^{n-k}y^k$. Therefore, in the expansion of $(x+y)^n$, a typical term will be of the form $x^{n-k}y^k$, where $0 \leq k \leq n$. The question is, what is its coefficient in the expansion, after we collect like terms? This coefficient is the number of times the product $x^{n-k}y^k$ appears when we multiply out $(x+y)^n$ in the way described above. It depends on which k copies of the $(x+y)$s we will choose y from. There are $\binom{n}{k}$ choices, hence, the product $x^{n-k}y^k$ appears $\binom{n}{k}$ times. Thus, the coefficient is $\binom{n}{k}$. For this reason, we also call $\binom{n}{k}$ the ***binomial coefficients***.

Theorem 7.6.1 (Binomial Theorem)

For any positive integer n,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k.$$

Because of the symmetry in the formula, we can interchange x and y. In addition, we also have $\binom{n}{k} = \binom{n}{n-k}$. Consequently, the binomial theorem can be written in three other forms:

$$\begin{aligned}(x+y)^n &= \sum_{k=0}^{n} \binom{n}{n-k} x^{n-k}y^k, \\ (x+y)^n &= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}, \\ (x+y)^n &= \sum_{k=0}^{n} \binom{n}{n-k} x^k y^{n-k}.\end{aligned}$$

You need not worry which one to use. They are all the same! This is how to remember these four different forms. In each term, the powers of x and y always add up to n. If the power of one of the two variables is k, where $0 \leq k \leq n$, then the power of the other must be $n-k$, and we need to multiply the coefficient $\binom{n}{k}$, which is the same as $\binom{n}{n-k}$, to their product.

When expanding $(x+y)^n$, it may be helpful if you first lay out all the terms x^n, $x^{n-1}y$, $x^{n-2}y^2$, and so forth. Then you fill in with the binomial coefficients. For instance, to expand $(x+y)^3$, we first list all the terms that we expect fo find:

$$(x+y)^3 = \_x^3 + \_x^2y + \_xy^2 + \_y^3.$$

Next we fill in the binomial coefficients:

$$(x+y)^3 = \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3.$$

Finally, evaluate the binomial coefficients and simplify the result.

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.$$

In a similar way, we also find $(x-y)^3 = x^3 - 3x^2y + 3xy^2 - y^3$. Note the similarity between the two expansions.

Example 7.6.1

Compute $(x+y)^4$.

Solution

Following the steps we outlined above, we find

$$\begin{aligned}(x+y)^4 &= \binom{4}{0}x^4 + \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 + \binom{4}{3}xy^3 + \binom{4}{4}y^4 \\ &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.\end{aligned}$$

Since $\binom{n}{0} = \binom{n}{n} = 1$, the expansion always starts with x^n and ends with y^n.

Example 7.6.2

Compute $(x-y)^4$.

Solution

We find

$$\begin{aligned}(x-y)^4 &= [x+(-y)]^4 \\ &= \binom{4}{0}x^4 + \binom{4}{1}x^3(-y) + \binom{4}{2}x^2(-y)^2 + \binom{4}{3}x(-y)^3 + \binom{4}{4}(-y)^4 \\ &= x^4 - 4x^3y + 6x^2y^2 - 4xy^3 + y^4.\end{aligned}$$

Take note of the alternating signs in the expansion. This suggests that we could expand $(A-B)^n$ the exact same way we would with $(A+B)^n$, except that the signs alternate.

We can carry out the expansion by following these steps. First, list all the terms we expect to find

$$(x+y)^4 = \_x^4 \quad \_x^3y \quad \_x^2y^2 \quad \_xy^3 \quad \_y^4. \tag{7.6.1}$$

Next, fill in the signs:

$$(x+y)^4 = \_x^4 - \_x^3y + \_x^2y^2 - \_xy^3 + \_y^4, \tag{7.6.2}$$

and then the binomial coefficients:

$$(x+y)^4 = \binom{4}{0}x^4 - \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 - \binom{4}{3}xy^3 + \binom{4}{4}y^4. \tag{7.6.3}$$

Finally, compute the binomial coefficients to finish the expansion.

Example 7.6.3

Expand $(2x-3y)^5$.

Solution

The expansion yields

$$(2x)^5 - \binom{5}{1}(2x)^4(3y) + \binom{5}{2}(2x)^3(3y)^2 - \binom{5}{3}(2x)^2(3y)^3 + \binom{5}{4}(2x)(3y)^4 - (3y)^5. \tag{7.6.4}$$

Therefore, $(2x-3y)^5 = 32x^5 - 240x^4y + 720x^3y^2 - 1080x^2y^3 + 810xy^4 - 243y^5$.

hands-on Exercise 7.6.1

Use the binomial theorem to expand $(3x-5y)^4$.

Example 7.6.4

Find the coefficient of x^3 in the expansion of $(1+x)^{102}$.

Solution

Since

$$(1+x)^{102} = \sum_{k=0}^{102} \binom{102}{k} x^k, \tag{7.6.5}$$

the term containing x^3 is $\binom{102}{3}x^3$. Therefore, the coefficient is $\binom{102}{3}$. Depending on which form of the binomial theorem you use, you may end up with the term $\binom{102}{99}x^3$. Numerically, this gives us the same coefficient, because $\binom{102}{99} = \binom{102}{102-99} = \binom{102}{3}$.
$\binom{102}{3} = 171700.$

Example 7.6.5

What is the coefficient of t^4 in the expansion of $(2+3t)^9$?

Solution

Since

$$(2+3t)^9 = \sum_{k=0}^{9} \binom{9}{k} 2^{9-k}(3t)^k, \tag{7.6.6}$$

we need $k=4$. The coefficient is $\binom{9}{4}2^5 \cdot 3^4 = 126 \cdot 32 \cdot 81 = 326,592.$

Example 7.6.6

What is the coefficient of t^5 in the expansion of $(3-2t)^7$?

Solution

Since $(3-2t)^7 = \sum_{k=0}^{7} \binom{7}{k} 3^{7-k}(-2t)^k$, we need $k=5$, and the coefficient is $\binom{7}{5}3^2 \cdot (-2)^5 = -\binom{7}{5}3^2 \cdot 2^5 = -21 \cdot 9 \cdot 32 = -6048$.

hands-on Exercise 7.6.2

What is the coefficient of t^5 in $(1+3t)^8$?

hands-on Exercise 7.6.3

What is the coefficient of t^4 in the expansion of $(2-5t)^9$?

Example 7.6.7

What is the coefficient of t^6 in the expansion of $(4+5t^2)^8$?

Solution

The general term in the expansion is $\binom{8}{k}4^{8-k}(5t^2)^k = \binom{8}{k}4^{8-k} \cdot 5^k t^{2k}$. Hence, we need $k=3$, and the coefficient is $\binom{8}{3}4^5 \cdot 5^3 = 56 \cdot 1024 \cdot 125 = 7,168,000$

hands-on Exercise 7.6.4

What is the coefficient of t^9 in the expansion of $(3-2t^3)^8$?

The constant term in an expansion does not contain any variable. It can be interpreted as the term containing x^0.

Example 7.6.8

What is the term with y^3 in $(3x+5y)^8$?

Solution

The general term in the expansion is

$$\binom{8}{k}(3x)^{8-k}(5y)^k. \tag{7.6.7}$$

Since $k=3$, the term is $\binom{8}{3}(3x)^5(5y)^3$.
This is $56\cdot(243)x^5\cdot(125)\,y^3$.

Therefore, the term is $1701000x^5y^3$.

Pascal's Triangle

(See an introduction to Pascal's Triangle in *section 7.4*)

To compute the binomial coefficients quickly, one may use the ***Pascal triangle***, in which the nth row $(n\geq 0)$ consists of the binomial coefficients $\binom{n}{k}$, where $0\leq k\leq n$:

$$\begin{array}{ccccccccccccc} &&&&&&1&&&&&& \\ &&&&&1&&1&&&&& \\ &&&&1&&2&&1&&&& \\ &&&1&&3&&3&&1&&& \\ &&1&&4&&6&&4&&1&& \\ &1&&5&&10&&10&&5&&1& \\ 1&&6&&15&&20&&15&&6&&1 \end{array} \tag{7.6.8}$$

Constructing the Pascal triangle is easy. We generate the rows one at a time. The extreme ends are always 1. Each of the interior entries is the sum of the two entries right above it in the preceding row. For instance, the next row (for $n=7$) should be

$$\begin{array}{cccccccc} 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \end{array} \tag{7.6.9}$$

Such computations produce the right binomial coefficients, because of the next result.

Theorem 7.6.2 (Pascal's Identitity)

For all integers n and k satisfying $1\leq k\leq n$,

$$\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}.$$

(Analytic Proof)

It follows from the definition of binomial coefficients that

$$\begin{aligned}\binom{n-1}{k-1}+\binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!\,(n-k)!}+\frac{(n-1)!}{k!\,(n-k-1)!} \\ &= \frac{(n-1)!}{(k-1)!\,(n-k-1)!}\left(\frac{1}{n-k}+\frac{1}{k}\right) \\ &= \frac{(n-1)!}{(k-1)!\,(n-k-1)!}\cdot\frac{n}{k(n-k)} \\ &= \frac{n!}{k!\,(n-k)!}.\end{aligned}$$

This completes the proof.

(Combinatorial Proof)

Let A be an n-element set. Then $\binom{n}{k}$ counts the number of k-element subsets of A. These subsets can be classified according to whether they contain a fixed element, say x. If a subset contains x, then the other $k-1$ elements must be selected from the remaining $n-1$ elements of A. Otherwise, if the subset does not contain x, then all its k elements must be selected from the other $n-1$ elements of A. The numbers of these two kinds of subsets are given by $\binom{n-1}{k-1}$ and $\binom{n-1}{k}$, respectively. The theorem now follows immediately by applying the addition principle.

hands-on Exercise 7.6.7

Determine the 8th and the 9th rows in the Pascal's triangle.

Example 7.6.10

Use the Pascal's triangle to expand

a. $(C-D)^5$
b. $(2A+5B)^3$
c. $(3C-4B)^4$

Solution

Draw the values of $\binom{n}{k}$ from the Pascal triangle directly. The answers are:

a. $(C-D)^5 = C^5-5C^4D+10C^3D^2-10C^2D^3+5CD^4-D^5$.
b. $(2a+5B)^3 = 8A^3+60A^2B+150AB^2+125B^3$.
c. $(3C-4B)^4 = 81C^4-432C^3B+864C^2B^2-768CB^3+256B^4$.

Summary and Review

- The binomial theorem can be expressed in four different but equivalent forms.
- The expansion of $(x+y)^n$ starts with x^n, then we decrease the exponent in x by one, meanwhile increase the exponent of y by one, and repeat this until we have y^n.
- The next few terms are therefore $x^{n-1}y$, $x^{n-2}y^2$, etc., which end with y^n.
- In general, the sum of exponents in x and y is always n. Hence, the general term is x^ky^{n-k}, whose coefficient is $\binom{n}{k}$.
- The expansion of $(x+y)^n$ and $(x-y)^n$ look almost identical, except that the signs in $(x-y)^n$ alternate.

Exercises

Exercise 7.6.1

Expand $(x-2y)^4$

Answer

$x^4-8x^3y+24x^2y^2-32xy^3+16y^4$

Exercise 7.6.2

Find the coefficient of $x^{11}y^3$ in $(x+y)^{14}$.

Exercise 7.6.3

Find the coefficient of x^4y^7 in $(2x-y)^{11}$.

Answer

The term is $\binom{11}{4}2^4 \cdot x^4(-1)^7y^7$, so the coefficient is $330 \cdot 16 \cdot -1 = -5280$.

Exercise 7.6.4

Expand $(3a-b)^5$

Exercise 7.6.5

Find the coefficient of y^5 in $(2x+3y)^7$.

Answer

The term is $\binom{7}{5}2^2 \cdot x^2 \cdot 3^5y^5$, so the coefficient is $21 \cdot 4 \cdot 243 = 20,412$.

Exercise 7.6.6

Find the coefficient of y^3 in $(5x-2y)^5$.

Exercise 7.6.7

What is the term in $(2x+7y)^6$ with y^2?

Answer

The term is $\binom{6}{2}2^4 \cdot x^4 \cdot 7^2y^2$, so the term is $15 \cdot 16 \cdot 49x^4y^2 = 11760x^4y^2$

Exercise 7.6.8

What is the term in $(x-3y)^8$ with x^5?

CHAPTER OVERVIEW

8: Big O

8.1: Big O

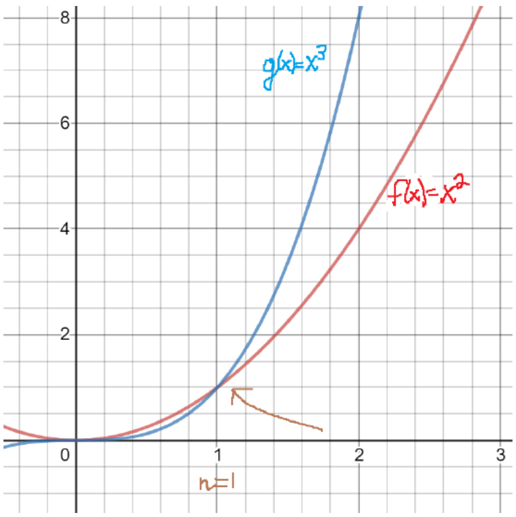
Big O

The idea of Big O is to characterize functions according to their growth rates. The O refers to the order of a function. In computer science, Big O is used to classify algorithms for their running time or space requirements.

Notice in the figure below that $f(x) > g(x)$ right before $x = 1$. However, for $x > 1$, we see that $g(x) > f(x)$. In the long run (namely after $x > 1$) $g(x)$ overtakes $f(x)$.

We say "f is of order at most g" or "$f(x)$ is Big O of $g(x)$" .

We write: $f(x) = O\big(g(x)\big)$.



In our definition of Big O notation, there are certain parameters.

- We use x greater than a certain initial value, n; in the diagram above, $n = 1$.
- We use absolute value for both functions.
- We use k as a constant multiplied by the function inside the O.

Definition: Big O Notation

$$f(x) = O\big(g(x)\big). \tag{8.1.1}$$

if and only if there exist real numbers k, n with $k > 0, n \geq 0$ such that

$$|f(x)| \leq k|g(x)| \qquad \forall x > n. \tag{8.1.2}$$

Example 8.1.1

Take this statement and express it in Big O notation: $|7x^5 + 4x^3 + x| \leq 14|x^5|$ for $x > 1$.

Solution

$(7x^5 + 4x^3 + x)$ is $O(x^5)$

Comparing orders of common functions

A constant function, such as $f(x) = 6$ does not grow at all. Logarithmic functions grow very slowly. Here is a list of some common functions in increasing order of growth rates.

constant function, logarithmic function, polynomial function, exponential function

Example 8.1.2

Put these functions in order of increasing growth rates:

$$\log_6 x, \quad x^5, \quad 2^x, \quad x^2, \quad \log_{15} x, \quad 100x^4, \quad 64x+1000, \quad x^5\log_6 x, \quad 5^x, \quad 6 \tag{8.1.3}$$

Solution

$$6, \quad \log_6 x, \quad \log_{15} x, \quad 64x+1000, \quad x^2, \quad 100x^4, \quad x^5, \quad x^5\log_6 x, \quad 2^x, \quad 5^x \tag{8.1.4}$$

Proofs

We will be using the Triangle Inequality Theorem which is

$$|x+y| \leq |x|+|y|. \tag{8.1.5}$$

Example 8.1.3

Prove: $4x^3-11x^2+3x-2=O(x^3)$

Proof

Choose $n=1$, i.e. $x\geq 1$.

$$\begin{aligned} |4x^3-11x^2+3x-2| &\leq |4x^3|+|-11x^2|+|3x|+|-2| \qquad \text{by the Triangle Inequality Theorem} \\ &= 4x^3+11x^2+3x+2 \qquad \text{applying absolute value; note: } x \text{ is positive} \\ &\leq 4x^3+11x^3+3x^3+2x^3 \qquad \text{since } x \text{ is positive and greater than 1} \\ &= 20x^3 \\ &= 20|x^3| \qquad \text{since } x \text{ is positive and greater than 1} \end{aligned}$$

Thus for all $x\geq 1$, $|4x^3-11x^2+3x-2|\leq 20|x^3|$

Therefore, using $n=1$ and $k=20$, $4x^3-11x^2+3x-2=O(x^3)$ by the definition of Big O.

Summary and Review

- Big O is used to compare the growth rates of functions.
- Be sure to understand the examples here.

Exercises

exercise 8.1.1

True or False?

(a) $11x^3=O(87x^2)$

(b) $x^{13}=O(3^x)$

(c) $-2x=O(58\log_{35} x)$

Answer

(a) false
(b) true
(c) false

Exercise 8.1.2

True or False?

(a) $4x^3+12x^2+36=O(x^3)$

(b) $.01x^5=O(48x^4)$

(c) $4^x=O(x^7)$

(d) $3x\log_2 x=O(25x)$

Exercise 8.1.3

True or False?

(a) $23\ln x=O(3x)$

(b) $7x^5=O(x^5)$

(c) $x^5=O(7x^5)$

Answer

all true

Exercise 8.1.4

Prove: $2x^5+3x^4-x^3+5x=O(x^5)$

Example 8.1.5

Put these functions in order of increasing growth rates:

$$x^7,\qquad 6^x,\qquad 78x^2,\qquad x^2\log x,\qquad 1000x,\qquad 7,\qquad \log_{11} x \tag{8.1.6}$$

Answer

$$7,\qquad \log_{11} x,\qquad 1000x,\qquad 78x^2,\qquad x^2\log x,\qquad x^7,\qquad 6^x \tag{8.1.7}$$

Exercise 8.1.6

Take this statement and express it in Big O notation: $|2x^4-5x^3+x^2-5|\leq 13|x^4|\quad \text{for } x>1.$

CHAPTER OVERVIEW

Appendices

A.1: Cardinality-additional info

Basic Theory

Definitions

Suppose that $\mathscr{S}$ is a non-empty collection of sets. We define a relation $\approx$ on $\mathscr{S}$ by $A \approx B$ if and only if there exists a one-to-one function f from A onto B. The relation $\approx$ is an equivalence relation on $\mathscr{S}$. That is, for all $A, B, C \in \mathscr{S}$,

a. $A \approx A$, the reflexive property
b. If $A \approx B$ then $B \approx A$, the symmetric property
c. If $A \approx B$ and $B \approx C$ then $A \approx C$, the transitive property

Proof

a. The identity function I_A on A, given by $I_A(x) = x$ for $x \in A$, maps A one-to-one onto A. Hence $A \approx A$.

b. If $A \approx B$ then there exists a one-to-one function f from A onto B. But then f^{-1} is a one-to-one function from B onto A, so $B \approx A$.

c. Suppose that $A \approx B$ and $B \approx C$. Then there exists a one-to-one function f from A onto B and a one-to-one function g from B onto C. But then $g \circ f$ is a one-to-one function from A onto C, so $A \approx C$.

A one-to-one function f from A onto B is sometimes called a *bijection*. Thus if $A \approx B$ then A and B are in *one-to-one* correspondence and are said to have the same *cardinality*. The equivalence classes under this equivalence relation capture the notion of having the same number of elements.

Let $\mathbb{N}_0 = \emptyset$, and for $k \in \mathbb{N}_+$, let $\mathbb{N}_k = \{0, 1, \ldots k-1\}$. As always, $\mathbb{N} = \{0, 1, 2, \ldots\}$is the set of all natural numbers.

Suppose that A is a set.

a. A is *finite* if $A \approx \mathbb{N}_k$ for some $k \in \mathbb{N}$, in which case k is the cardinality of A, and we write $\#(A) = k$.
b. A is *infinite* if A is not finite.
c. A is *countably infinite* if $A \approx \mathbb{N}$.
d. A is *countable* if A is finite or countably infinite.
e. A is *uncountable* if A is not countable.

In part (a), think of $\mathbb{N}_k$ as a *reference set* with k elements; any other set with k elements must be equivalent to this one. We will study the cardinality of finite sets in the next two sections on Counting Measure and Combinatorial Structures. In this section, we will concentrate primarily on infinite sets. In part (d), a countable set is one that can be *enumerated* or *counted* by putting the elements into one-to-one correspondence with $\mathbb{N}_k$ for some $k \in \mathbb{N}$ or with all of $\mathbb{N}$. An uncountable set is one that cannot be so counted. Countable sets play a special role in probability theory, as in many other branches of mathematics. Apriori, it's not clear that there *are* uncountable sets, but we will soon see examples.

Preliminary Examples

If S is a set, recall that $\mathscr{P}(S)$ denotes the power set of S (the set of all subsets of S). If A and B are sets, then A^B is the set of all functions from B into A. In particular, $\{0,1\}^S$ denotes the set of functions from S into $\{0,1\}$.

If S is a set then $\mathscr{P}(S) \approx \{0,1\}^S$.

Proof

The mapping that takes a set $A \in \mathscr{P}(S)$ into its indicator function $\mathbf{1}_A \in \{0,1\}^S$ is one-to-one and onto. Specifically, if $A, B \in \mathscr{P}(S)$ and $\bs1_A = \bs1_B$, then $A = B$, so the mapping is one-to-one. On the other hand, if $f \in \{0,1\}^S$ then $f = \bs1_A$ where $A = \{x \in S : f(x) = 1\}$. Hence the mapping is onto.

Next are some examples of countably infinite sets.

The following sets are countably infinite:

a. The set of even natural numbers $E = \{0, 2, 4, \ldots\}$
b. The set of integers $\mathbb{Z}$

Proof

a. The function $f : \mathbb{N} \to E$ given by $f(n) = 2n$ is one-to-one and onto.

b. The function $g : \mathbb{N} \to \mathbb{Z}$ given by $g(n) = \frac{n}{2}$ if n is even and $g(n) = -\frac{n+1}{2}$ if n is odd, is one-to-one and onto.

At one level, it might seem that E has only half as many elements as $\mathbb{N}$ while $\mathbb{Z}$ has twice as many elements as $\mathbb{N}$. as the previous result shows, that point of view is incorrect: $\mathbb{N}$, E, and $\mathbb{Z}$ all have the same cardinality (and are countably infinite). The next example shows that there are indeed uncountable sets.

If A is a set with at least two elements then $S = A^{\mathbb{N}}$, the set of all functions from $\mathbb{N}$ into A, is uncountable.

Proof

The proof is by contradiction, and uses a nice trick known as the *diagonalization method*. Suppose that S is countably infinite (it's clearly not finite), so that the elements of S can be enumerated: $S = \{f_0, f_1, f_2, \ldots\}$. Let a and b denote distinct elements of A and define $g : \mathbb{N} \to A$ by $g(n) = b$ if $f_n(n) = a$ and $g(n) = a$ if $f_n(n) \mathbb{N}ea$. Note that $g \mathbb{N}ef_n$. for each $n \in \mathbb{N}$, so $g \mathbb{N}otinS$. This contradicts the fact that S is the set of *all*functions from $\mathbb{N}$ into A.

Subsets of Infinite Sets

Surely a set must be as least as large as any of its subsets, in terms of cardinality. On the other hand, by example (4), the set of natural numbers $\mathbb{N}$, the set of even natural numbers E and the set of integers $\mathbb{Z}$ all have exactly the same cardinality, even though $E \subset \mathbb{N} \subset \mathbb{Z}$. In this subsection, we will explore some interesting and somewhat paradoxical results that relate to subsets of infinite sets. Along the way, we will see that the countable infinity is the “smallest” of the infinities.

If S is an infinite set then S has a countable infinite subset.

Proof

Select $a_0 \in S$. It's possible to do this since S is infinite and therefore nonempty. Inductively, having chosen $\{a_0, a_1, \ldots, a_{k-1}\} \subseteq S$, select $a_k \in S \setminus \{a_0, a_1, \ldots, a_{k-1}\}$. Again, it's possible to do this since S is not finite. Manifestly, $\{a_0, a_1, \ldots\}$ is a countably infinite subset of S.

A set S is infinite if and only if S is equivalent to a proper subset of S.

Proof

If S is finite, then S is not equivalent to a proper subset by the “pigeonhole principle”. If S is infinite, then S has countably infinite subset $\{a_0, a_1, a_2, \ldots\}$ by the previous result. Define the function $f : S \to S$ by f \left(a_n\mathbb{R}ight) = a_{2 n} for $n \in \mathbb{N}$ and $f(x) = x$ for $x \in S \setminus \{a_0, a_1, a_2, \ldots\}$. Then f maps S one-to-one onto $S \setminus \{a_1, a_3, a_5, \ldots\}$.

When S was infinite in the proof of the previous result, not only did we map S one-to-one onto a proper subset, we actually threw away a countably infinite subset and still maintained equivalence. Similarly, we can *add* a countably infinite set to an infinite set S without changing the cardinality.

If S is an infinite set and B is a countable set, then $S \approx S \cup B$.

Proof

Consider the most extreme case where B is countably infinite and disjoint from S. Then S has a countably infinite subset $A = \{a_0, a_1, a_2, \ldots\}$ by the result above, and B can be enumerated, so $B = \{b_0, b_1, b_2, \ldots\}$. Define the function

$f: S \to S \cup B$ by f\left(a_n\mathbb{R}ight) = a_{n/2} if n is even, f\left(a_n\mathbb{R}ight) = b_{(n-1)/2} if n is odd, and $f(x) = x$ if $x \in S \setminus \{a_0, a_1, a_2, \ldots\}$. Then f maps S one-to-one onto $S \cup B$.

In particular, if S is uncountable and B is countable then $S \cup B$ and $S \setminus B$ have the same cardinality as S, and in particular are uncountable. In terms of the dichotomies *finite-infinite* and *countable-uncountable*, a set is indeed at least as large as a subset. First we need a preliminary result.

If S is countably infinite and $A \subseteq S$ then A is countable.

Proof

It suffices to show that if A is an infinite subset of S then A is countably infinite. Since S is countably infinite, it can be enumerated: $S = \{x_0, x_1, x_2, \ldots\}$. Let n_i be the ith smallest index such that $x_{n_i} \in A$. Then $A = \{x_{n_0}, x_{n_1}, x_{n_2}, \ldots\}$ and hence is countably infinite.

Suppose that $A \subseteq B$.

a. If B is finite, then A is finite.
b. If A is infinite, then B is infinite.
c. If B is countable, then A is countable.
d. If A is uncountable, then B is uncountable.

Proof

a. This is clear from the definition of a finite set.

b. This is the contrapositive of (a).

c. If A is finite, then A is countable. If A is infinite, then B is infinite by (b) and hence is countably infinite. But then A is countably infinite by (9).

d. This is the contrapositive of (c).

Comparisons by one-to-one and onto functions

We will look deeper at the general question of when one set is “at least as big” as another, in the sense of cardinality. Not surprisingly, this will eventually lead to a partial order on the cardinality equivalence classes.

First note that if there exists a function that maps a set A one-to-one into a set B, then in a sense, there is a copy of A contained in B. Hence B should be at least as large as A.

Suppose that $f: A \to B$ is one-to-one.

a. If B is finite then A is finite.
b. If A is infinite then B is infinite.
c. If B is countable then A is countable.
d. If A is uncountable then B is uncountable.

Proof

Note that f maps A one-to-one onto $f(A)$. Hence $A \approx f(A)$ and $f(A) \subseteq B$. The results now follow from (10):

a. If B is finite then $f(A)$ is finite and hence A is finite.

b. If A is infinite then $f(A)$ is infinite and hence B is infinite.

c. If B is countable then $f(A)$ is countable and hence A is countable.

d. If A is uncountable then $f(A)$ is uncountable and hence B is uncountable.

On the other hand, if there exists a function that maps a set A onto a set B, then in a sense, there is a copy of B contained in A. Hence A should be at least as large as B.

Suppose that $f : A \to B$ is onto.

a. If A is finite then B is finite.
b. If B is infinite then A is infinite.
c. If A is countable then B is countable.
d. If B is uncountable then A is uncountable.

Proof

For each $y \in B$, select a specific $x \in A$ with $f(x) = y$ (if you are persnickety, you may need to invoke the axiom of choice). Let C be the set of chosen points. Then f maps C one-to-one onto B, so $C \approx B$ and $C \subseteq A$. The results now follow from (11):

a. If A is finite then C is finite and hence B is finite.

b. If B is infinite then C is infinite and hence A is infinite.

c. If A is countable then C is countable and hence B is countable.

d. If B is uncountable then C is uncountable and hence A is uncountable.

The previous exercise also could be proved from the one before, since if there exists a function f mapping A onto B, then there exists a function g mapping B one-to-one into A. This duality is proven in the discussion of the axiom of choice. A simple and useful corollary of the previous two theorems is that if B is a given countably infinite set, then a set A is countable if and only if there exists a one-to-one function f from A into B, if and only if there exists a function g from B onto A.

If A_i is a countable set for each i in a countable index set I, then $\bigcup_{i \in I} A_i$ is countable.

Proof

Consider the most extreme case in which the index set I is countably infinite. Since A_i is countable, there exists a function f_i that maps $\mathbb{N}$ onto A_i for each $i \in \mathbb{N}$. Let M = \left\{2^i 3^j: (i, j) \in \mathbb{N} \times \mathbb{N}\mathbb{R}ight\}. Note that the points in M are distinct, that is, $2^i 3^j \mathbb{N}e 2^m 3^n$ if (i, j), $(m, n) \in \mathbb{N} \times \mathbb{N}$ and $(i, j) \mathbb{N}e (m, n)$. Hence M is infinite, and since $M \subset \mathbb{N}$, M is countably infinite. The function f given by f\left(2^i 3^j\mathbb{R}ight) = f_i(j) for $(i, j) \in \mathbb{N} \times \mathbb{N}$ maps M onto $\bigcup_{i \in I} A_i$, and hence this last set is countable.

If A and B are countable then $A \times B$ is countable.

Proof

There exists a function f that maps $\mathbb{N}$ onto A, and there exists a function g that maps $\mathbb{N}$ onto B. Again, let M = \left\{2^i 3^j: (i, j) \in \mathbb{N} \times \mathbb{N} \mathbb{R}ight\} and recall that M is countably infinite. Define $h : M \to A \times B$ by h\left(2^i 3^j\mathbb{R}ight) = \left(f(i), g(j)\mathbb{R}ight). Then h maps M onto $A \times B$ and hence this last set is countable.

The last result could also be proven from the one before, by noting that

$$A \times B = \bigcup_{a \in A} \{a\} \times B \tag{A.1.1}$$

Both proofs work because the set M is essentially a copy of $\mathbb{N} \times \mathbb{N}$, embedded inside of $\mathbb{N}$. The last theorem generalizes to the statement that a finite product of countable sets is still countable. But, from (5), a product of *infinitely* many sets (with at least 2 elements each) will be uncountable.

The set of rational numbers $\mathbb{Q}$ is countably infinite.

Proof

The sets $\mathbb{Z}$ and $\mathbb{N}_+$ are countably infinite and hence the set $\mathbb{Z} \times \mathbb{N}_+$ is countably infinite. The function $f : \mathbb{Z} \times \mathbb{N}_+ \to \mathbb{Q}$ given by $f(m, n) = \frac{m}{n}$ is onto.

A real number is *algebraic* if it is the root of a polynomial function (of degree 1 or more) with integer coefficients. Rational numbers are algebraic, as are rational roots of rational numbers (when defined). Moreover, the algebraic numbers are closed under addition, multiplication, and division. A real number is *transcendental* if it's not algebraic. The numbers e and π are transcendental, but we don't know very many other transcendental numbers by name. However, as we will see, most (in the sense of cardinality) real numbers are transcendental.

The set of algebraic numbers $\mathbb{A}$ is countably infinite.

Proof

Let $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$ and let $\mathbb{Z}_n = \mathbb{Z}^{n-1} \times \mathbb{Z}_0$ for $n \in \mathbb{N}_+$. The set $\mathbb{Z}_n$ is countably infinite for each n. Let $C = \bigcup_{n=1}^\infty \mathbb{Z}_n$. Think of C as the set of coefficients and note that C is countably infinite. Let P denote the set of polynomials of degree 1 or more, with integer coefficients. The function $(a_0, a_1, \ldots, a_n) \mapsto a_0 + a_1 x + \cdots + a_n x^n$ maps C onto P, and hence P is countable. For $p \in P$, let A_p denote the set of roots of p. A polynomial of degree n in P has at most n roots, by the *fundamental theorem of algebra*, so in particular A_p is finite for each $p \in P$. Finally, note that $\mathbb{A} = \bigcup_{p \in P} A_p$ and so $\mathbb{A}$ is countable. Of course $\mathbb{N} \subset \mathbb{A}$, so $\mathbb{A}$ is countably infinite.

Now let's look at some uncountable sets.

The interval $[0, 1)$ is uncountable.

Proof

Recall that $\{0,1\}^{\mathbb{N}^+}$ is the set of all functions from $\mathbb{N}^+$ into $\{0,1\}$, which in this case, can be thought of as infinite sequences or *bit strings*:

$$\{0,1\}^{\mathbb{N}^+} = \left\{\bs x = (x_1, x_2, \ldots) : x_n \in \{0,1\} \text{ for all } n \in \mathbb{N}^+\right\} \tag{A.1.2}$$

By (5), this set is uncountable. Let N = \left\{\bs{x} \in \{0, 1\}^{\mathbb{N}_+}: x_n = 1 \text{ for all but finitely many } n\mathbb{R}ight\}, the set of bit strings that eventually terminate in all 1s. Note that $N = \bigcup_{n=1}^\infty N_n$ where N_n = \left\{\bs{x} \in \{0, 1\}^{\mathbb{N}_+}: x_k = 1 \text{ for all } k \ge n\mathbb{R}ight\}. Clearly N_n is finite for all $n \in \mathbb{N}_+$, so N is countable, and therefore $S = \{0,1\}^{\mathbb{N}_+} \setminus N$ is uncountable. In fact, $S \approx \{0,1\}^{\mathbb{N}_+}$. The function

$$\bs x \mapsto \sum_{n=1}^\infty \frac{x_n}{2^n} \tag{A.1.3}$$

maps S one-to-one onto $[0,1)$. In words every number in $[0,1)$ has a unique *binary expansion* in the form of a sequence in S. Hence $[0,1) \approx S$ and in particular, is uncountable. The reason for eliminating the bit strings that terminate in 1s is to ensure uniqueness, so that the mapping is one-to-one. The bit string $x_1 x_2 \cdots x_k 0111 \cdots$ corresponds to the same number in $[0,1)$ as the bit string $x_1 x_2 \cdots x_k 1000 \cdots$.

The following sets have the same cardinality, and in particular all are uncountable:

a. $\mathbb{R}$, the set of real numbers.
b. Any interval I of $\mathbb{R}$, as long as the interval is not empty or a single point.
c. $\mathbb{R} \setminus Q$, the set of irrational numbers.
d. $\mathbb{R} \setminus \mathbb{A}$, the set of transcendental numbers.
e. $\mathscr{P}(\mathbb{N})$, the power set of $\mathbb{N}$.

Proof

a. The mapping $x \mapsto \frac{2x-1}{x(1-x)}$ maps $(0,1)$ one-to-one onto $\mathbb{R}$ so $(0,1) \approx \mathbb{R}$. But $(0,1) = [0,1) \setminus \{0\}$, so $(0,1] \approx (0,1) \approx \mathbb{R}$, and all of these sets are uncountable by the previous result.

b. Suppose $a, b \in \mathbb{R}$ and $a < b$. The mapping $x \mapsto a + (b-a)x$ maps $(0,1)$ one-to-one onto (a,b) and hence $(a,b) \approx (0,1) \approx \mathbb{R}$. Also, $[a,b) = (a,b) \cup \{a\}$, $(a,b] = (a,b) \cup \{b\}$, and $[a,b] = (a,b) \cup \{a,b\}$, so $(a,b) \approx [a,b) \approx (a,b] \approx [a,b] \approx \mathbb{R}$. The function $x \mapsto e^x$ maps $\mathbb{R}$ one-to-one onto $(0,\infty)$, so $(0,\infty) \approx \mathbb{R}$. For $a \in \mathbb{R}$, the function $x \mapsto a + x$ maps $(0,\infty)$ one-to-one onto (a,∞) and the mapping $x \mapsto a - x$ maps $(0,\infty)$ one to one onto $(-\infty,a)$ so $(a,\infty) \approx (-\infty,a) \approx (0,\infty) \approx \mathbb{R}$. Next, $[a,\infty) = (a,\infty) \cup \{a\}$ and $(-\infty,a] = (-\infty,a) \cup \{a\}$, so $[a,\infty) \approx (-\infty,a] \approx \mathbb{R}$.

c. $\setminus Q$ is countably infinite, so $\mathbb{R} \setminus \setminus Q \approx \mathbb{R}$.

d. Similarly, $\setminus A$ is countably infinite, so $\mathbb{R} \setminus \mathbb{A} \approx \mathbb{R}$.

e. If S is countably infinite, then by the previous result and (a), $\mathscr{P}(S) \approx \mathscr{P}(\mathbb{N}_+) \approx \{0,1\}^{\mathbb{N}_+} \approx [0,1)$.

The Cardinality Partial Order

Suppose that $\mathscr{S}$ is a nonempty collection of sets. We define the relation $\preceq$ on $\mathscr{S}$ by $A \preceq B$ if and only if there exists a one-to-one function f from A into B, if and only if there exists a function g from B onto A. In light of the previous subsection, $A \preceq B$ should capture the notion that B is at least as big as A, in the sense of cardinality.

The relation $\preceq$ is reflexive and transitive.

Proof

For $A \in \mathscr{S}$, the identity function $I_A : A \to A$ given by $I_A(x) = x$ is one-to-one (and also onto), so $A \preceq A$. Suppose that $A, B, C \in \mathscr{S}$ and that $A \preceq B$ and $B \preceq C$. Then there exist one-to-one functions $f : A \to B$ and $g : B \to C$. But then $g \circ f : A \to C$ is one-to-one, so $A \preceq C$.

Thus, we can use the construction in the section on on Equivalence Relations to first define an equivalence relation on $\mathscr{S}$, and then extend $\preceq$ to a true partial order on the collection of equivalence classes. The only question that remains is whether the equivalence relation we obtain in this way is the same as the one that we have been using in our study of cardinality. Rephrased, the question is this: *If there exists a one-to-one function from A into B and a one-to-one function from B into A, does there necessarily exist a one-to-one function from A* ***onto*** *B?* Fortunately, the answer is yes; the result is known as the *Schröder-Bernstein Theorem*, named for Ernst Schröder and Sergi Bernstein.

If $A \preceq B$ and $B \preceq A$ then $A \approx B$.

Proof

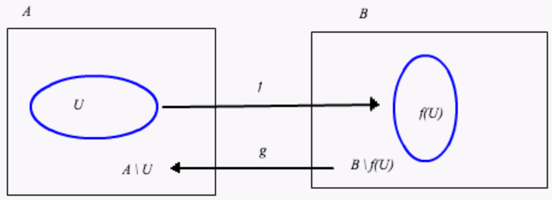
Set inclusion $\subseteq$ is a partial order on $\mathscr{P}(A)$ (the power set of A) with the property that every subcollection of $\mathscr{P}(A)$ has a supremum (namely the union of the subcollection). Suppose that f maps A one-to-one into B and g maps B one-to-one into A. Define the function $h : \mathscr{P}(A) \to \mathscr{P}(A)$ by $h(U) = A \setminus g[B \setminus f(U)]$ for $U \subseteq A$. Then h is increasing:

$$U \subseteq V \implies f(U) \subseteq f(V) \implies B \setminus f(V) \subseteq B \setminus f(U) \tag{A.1.4}$$

$$\implies g[B \setminus f(V)] \subseteq g[B \setminus f(U)] \implies A \setminus g[B \setminus f(U)] \subseteq A \setminus g[B \setminus f(U)] \tag{A.1.5}$$

From the fixed point theorem for partially ordered sets, there exists $U \subseteq A$ such that $h(U) = U$. Hence $U = A \setminus g[B \setminus f(U)]$ and therefore $A \setminus U = g[B \setminus f(U)]$. Now define $F : A \to B$ by $F(x) = f(x)$ if $x \in U$ and $F(x) = g^{-1}(x)$ if $x \in A \setminus U$.

f maps U one-to-one onto $f(U)$; g maps $B \setminus f(U)$ one-to-one onto $A \setminus U$



Next we show that F is one-to-one. Suppose that $x_1,\, x_2 \in A$ and $F(x_1) = F(x_2)$. If $x_1,\, x_2 \in U$ then $f(x_1) = f(x_2)$ so $x_1 = x_2$ since f is one-to-one. If $x_1,\, x_2 \in A \setminus U$ then $g^{-1}(x_1) = g^{-1}(x_2)$ so $x_1 = x_2$ since g^{-1} is one-to-one. If $x_1 \in U$ and $x_2 \in A \setminus U$. Then $F(x_1) = f(x_1) \in f(U)$ while $F(x_2) = g^{-1}(x_2) \in B \setminus f(U)$, so $F(x_1) = F(x_2)$ is impossible.

Finally we show that F is onto. Let $y \in B$. If $y \in f(U)$ then $y = f(x)$ for some $x \in U$ so $F(x) = y$. If $y \in B \setminus f(U)$ then $x = g(y) \in A \setminus U$ so $F(x) = g^{-1}(x) = y$.

We will write $A \prec B$ if $A \preceq B$, but $A \mathbb{N}ot \approx B$, That is, there exists a one-to-one function from A into B, but there does not exist a function from A onto B. Note that $\prec$ would have its usual meaning if applied to the equivalence classes. That is, $[A] \prec [B]$ if and only if $[A] \preceq [B]$ but $[A] \mathbb{N}e [B]$. Intuitively, of course, $A \prec B$ means that B is strictly larger than A, in the sense of cardinality.

$A \prec B$ in each of the following cases:

a. A and B are finite and $\#(A) < \#(B)$.
b. A is finite and B is countably infinite.
c. A is countably infinite and B is uncountable.

We close our discussion with the observation that for any set, there is always a larger set.

If S is a set then $S \prec \mathscr{P}(S)$.

Proof

First, it's trivial to map S one-to-one *into* $\mathscr{P}(S)$; just map x to $\{x\}$. Suppose now that f maps S onto $\mathscr{P}(S)$ and let $R = \{x \in S : x \mathbb{N}otin f(x)\}$. Since f is onto, there exists $t \in S$ such that $f(t) = R$. Note that $t \in f(t)$ if and only if $t \mathbb{N}otin f(t)$.

The proof that a set cannot be mapped onto its power set is similar to the *Russell paradox*, named for Bertrand Russell.

The *continuum hypothesis* is the statement that there is no set whose cardinality is strictly between that of $\mathbb{N}$ and $\mathbb{R}$. The continuum hypothesis actually started out as the continuum *conjecture*, until it was shown to be consistent with the usual axioms of the real number system (by Kurt Gödel in 1940), and independent of those axioms (by Paul Cohen in 1963).

If S is uncountable, then there exists $A \subseteq S$ such that A and A^c are uncountable.

Proof

There is an easy proof, assuming the continuum hypothesis. Under this hypothesis, if S is uncountable then $[0, 1) \preceq S$. Hence there exists a one-to-one function $f : [0, 1) \to S$. Let A = f\left[0, \frac{1}{2}\mathbb{R}ight). Then A is uncountable, and since f\left[\frac{1}{2}, 1\mathbb{R}ight) \subseteq A^c, A^c is uncountable.

There is a more complicated proof just using the axiom of choice.

Answers

Answers to Selected Exercises

Section 2.1

1. Only (a), (c), and (e) are statements.
2. (a) false (b) false (c) false (d) true
3. (a) $\pi \notin \mathbb{Z}$ (b) $1^3+2^3+3^3 \neq 3^2 \cdot 4^2/4$ (c) u is not a vowel

   (d) This statement is either true or false.
4. (a) true (b) true (c) true (d) false (e) false (f) true
5. By definition, a rational number can be written as a ratio of two integers. After multiplying the numerator by 7, we still have a ratio of two integers. Conversely, given any rational number x, we can multiply the denominator by 7, we obtain another rational number y such that $7y = x$. Hence, the two sets $7\mathbb{Q}$ and $\mathbb{Q}$ contain the same collection of rational numbers. In contrast, $0\mathbb{Q}$ contains only one number, namely, 0. Therefore, $0\mathbb{Q} \neq \mathbb{Q}$.

Section 2.2

1. (a) $p \wedge q$ (b) $\overline{q} \wedge r$ (c) $\overline{p} \vee \overline{q}$ (d) $(p \vee q) \wedge \overline{p \wedge q}$
2. (a) $p \wedge q$; always false regardless of the value of r.

   (b) $p \vee q$; always true regardless of the value of r.

   (c) $(p \wedge q) \vee r$; true if r is true, and false if r is false.

   (d) $\overline{q} \wedge r$; true if r is true, and false if r is false.
3. (a) false (b) true
4. (a) $(4 \leq x) \wedge (x \leq 7)$ (b) $(4 < x) \wedge (x \leq 7)$ (c) $(4 \leq x) \wedge (x < 7)$

Section 2.3

1. (a) $p \Rightarrow q$ (b) $r \Rightarrow p$ (c) $\overline{p} \Rightarrow q$ (d) $\overline{p} \Rightarrow r$ (e) $(\overline{p} \wedge q) \Rightarrow r$
2. (a) $p \Rightarrow q$, which is false.

   (b) $p \Rightarrow r$, which is true if r is true, and is false if r is false.

   (c) $(p \vee q) \Rightarrow r$, which is true if r is true, and is false if r is false.
3. (a) $x^3-3x^2+x-3=0 \Rightarrow x=3$

   (b) $x^3-3x^2+x-3=0 \Rightarrow x=3$

   (c) $x=3 \Rightarrow x^3-3x^2+x-3=0$
4.

p	q	r	$p \wedge q$	$(p \wedge q) \vee r$
T	T	T	T	T
T	T	F	T	T
T	F	T	F	T
T	F	F	F	F
F	T	T	F	T
F	T	F	F	F
F	F	T	F	T
F	F	F	F	F

p	q	r	$p \vee q$	$p \wedge r$	$(p \vee q) \Rightarrow (p \wedge r)$
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	T	T	T
T	F	F	T	F	F
F	T	T	T	F	F
F	T	F	T	F	F
F	F	T	F	F	T
F	F	F	F	F	T

5. (a) Using a truth table, we find that the implication $(p \wedge q) \Rightarrow (q \vee r)$ is always true. Hence, no truth value of p would make $(p \wedge q) \Rightarrow (q \vee r)$ false.

   (b) From a truth table, we find that, $(q \wedge r) \Rightarrow (p \wedge q)$ is false only when p is false. We can draw the same conclusion without using any truth table. An implication is false only when its hypothesis (in this case, $q \wedge r$) is true *and* its conclusion (in this case, $p \wedge q$) is false. For $q \wedge r$ to be true, we need both q and r to be true. Now q is true and $p \wedge q$ is false require p to be false.

Section 2.4

1. (a) $p \Leftrightarrow q$ (b) $r \Leftrightarrow \overline{p}$ (c) $r \Leftrightarrow (q \wedge \overline{p})$ (d) $r \Leftrightarrow (p \wedge q)$
2. (a) $p \Leftrightarrow q$, which is false.

   (b) $p \Leftrightarrow r$, which is true if r is true, and is false if r is false.

   (c) $(p \vee q) \Leftrightarrow r$, which is true if r is true, and is false if r is false.
3. (a) true (b) false (c) false (d) false
4. We say n is odd if and only if $n = 2q+1$ for some integer q.

Section 2.5

1.

p	q	$p \vee q$	$\overline{p \vee q}$	$\overline{p}$	$\overline{q}$	$\overline{p} \wedge \overline{q}$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
T	T	T	F	T	F	F
T	F	F	T	T	T	T

2. Only (b) is a tautology, as indicated in the truth tables below.

   (a)

p	q	$\overline{p}$	$\overline{p} \vee q$	$(\overline{p} \vee q) \Rightarrow p$
T	T	F	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	T	F

(b)

p	q	$p \Rightarrow q$	$\overline{q}$	$p \Rightarrow \overline{q}$	$(p \Rightarrow q) \vee (p \Rightarrow \overline{q})$
T	T	T	F	F	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	F	T	T	T

(c)

p	q	r	$p \Rightarrow q$	$(p \Rightarrow q) \Rightarrow r$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	T
T	F	F	F	T
F	T	T	T	T
F	T	F	T	F
F	F	T	T	T
F	F	F	T	F

3. The proofs are displayed below without explanations. Be sure to fill them in.

(b)
$$
\begin{aligned}
(p \wedge q) \Rightarrow r &\equiv \overline{p \wedge q} \vee r \\
&\equiv (\overline{p} \vee \overline{q}) \vee r \\
&\equiv \overline{p} \vee (\overline{q} \vee r) \\
&\equiv p \Rightarrow (\overline{q} \vee r)
\end{aligned}
$$

(c)
$$
\begin{aligned}
(p \Rightarrow \overline{q}) \wedge (p \Rightarrow \overline{r}) &\equiv (\overline{p} \vee \overline{q}) \wedge (\overline{p} \vee \overline{r}) \\
&\equiv \overline{p} \vee (\overline{q} \wedge \overline{r}) \\
&\equiv \overline{p} \vee \overline{q \vee r} \\
&\equiv \overline{p \wedge (q \vee r)}
\end{aligned}
$$

4. (a)

Converse:	If triangle ABC is a right triangle, then ABC is isosceles
	and contains an angle of 45 degrees.
Inverse:	If triangle ABC is not isosceles or does not contain an angle
	of 45 degrees, then ABC is not a right triangle.
Contrapositive:	If triangle ABC is not a right triangle, then ABC is not isosceles
	or does not contain an angle of 45 degrees.

(b)

Converse:	If quadrilateral $ABCD$ is both a rectangle and a rhombus,
	then $ABCD$ is a square.
Inverse:	If quadrilateral $ABCD$ is not a square,
	then it is not a rectangle or not a rhombus.
Contrapositive:	If quadrilateral $ABCD$ is not a rectangle or not a rhombus,
	then $ABCD$ is not a square.

5. (a) true (b) true (c) false

6. Only (b).

7. (a) $p \wedge q$ (b) $p \wedge \overline{q}$ (c) $p \wedge q$

Section 2.6

1. (a) There exists an integer n such that n is prime and n is even.

(b) For all integers n, if $n > 2$, then n is prime or n is even.

(c) There exists an integer n such that n is prime, and either n is even or $n > 2$.

(d) For all integers n, if n is prime and n is even, then $n \leq 2$.

2. (a) true (b) true (c) false (d) false (e) true

3. (a) $\exists x < 0 \; \exists y, z \in \mathbb{R} \; (y < z \wedge xy \leq xz)$

(b) $\exists x \in \mathbb{Z} \; [\overline{p(x)} \wedge \overline{q(x)}]$

(c) $\exists x, y \in \mathbb{R} \; [p(x, y) \wedge \overline{q(x, y)}]$

4. (a)

$\forall x, y \in \mathbb{R} \, (x + y = y + x)$
$\exists x, y \in \mathbb{R} \, (x + y \neq y + x)$
There exist real numbers x and y such that $x + y \neq y + x$.

(b)

$\forall x \in \mathbb{R}^{+} \; \exists y \in \mathbb{R} \, (y^2 = x)$
$\exists x \in \mathbb{R}^{+} \; \forall y \in \mathbb{R} \, (y^2 \neq x)$
There exists a positive real number x such that for all real numbers y, $y^2 \neq x$.

(c)

$\exists y \in \mathbb{R}\, \forall x \in \mathbb{Z}\, (2x^2+1 > x^2 y)$	
$\forall y \in \mathbb{R}\, \exists x \in \mathbb{Z}\, (2x^2+1 \leq x^2 y)$	
For every real number y, there exists an integer x such that $2x^2+1 \leq x^2 y$.	

5. The statement "a square must be a parallelogram" means, symbolically,

$$\forall PQRS\, (PQRS \text{ is a square} \Rightarrow PQRS \text{ is a parallelogram}), \tag{1}$$

but the statement "a square must not be a parallelogram" means

$$\forall PQRS\, (PQRS \text{ is a square} \Rightarrow PQRS \text{ is not a parallelogram}). \tag{2}$$

The second statement is not the negation of the first. The correct negation, in symbol, is

$$\exists PQRS\, (PQRS \text{ is a square} \wedge PQRS \text{ is a parallelogram}). \tag{3}$$

In words, it means "there exists a square that is not a parallelogram."

Section 3.1

1. Placing six dominoes horizontally in each row covers the entire chessboard.
2. Let $f(x) = x^3 - 12x + 2$. From the following chart

x	-4	-3	-2	-1	0	1	2	3	4
$f(x)$	-14	12	18	13	2	-9	-14	-7	18

(4)

we conclude there $x^3 - 12x + 2 = 0$ has a solution between -4 and -3, another one between 0 and 1, and a third one between 3 and 4. So it has at least three real solutions.

Remark. The Fundamental Theorem of Algebra asserts that a real polynomial of degree n has at most n real roots. Hence, the given equation has exactly three real solutions.

3. $n = 3$.

Section 3.2

1. No, $2^3 + 1 = 9$ is composite.
2. According to (i), the number $\sqrt{2}$ is irrational. It follows from (ii) that $\sqrt[4]{2} = \sqrt{\sqrt{2}}$ is also irrational. Applying (ii) one more time, we conclude that $\sqrt[8]{2} = \sqrt{\sqrt[4]{2}}$ is irrational.
3. (a) The statement is false, because $(-3)^2 > (-2)^2$, but $-3 \not> -2$.

(b) The statement is false, because when $n = 41$,

$$n^2 + n + 41 = 41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \cdot 43 \tag{5}$$

is composite.

Section 3.3

(a) We will prove the contrapositive of the given statement. That is, we will prove that if n is odd, then n^2 is odd. If n is odd, we can write $n = 2q + 1$ for some integer q. Then

$$n^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 2(2q^2 + 2q) + 1, \tag{6}$$

where $2q^2 + 2q$ is an integer. This shows that n^2 is odd.

(b) Suppose the given statement is false. That is, suppose n^2 is even, but n is odd. Since n is odd, $n = 2q + 1$ for some integer q. Then

$$n^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 2(2q^2 + 2q) + 1, \tag{7}$$

where $2q^2 + 2q$ is an integer. This shows that n^2 is odd, which contradicts the assumption that n^2 is even. Therefore, the given statement must be true.

Suppose there exist some numbers $a \neq b$ such that $a^2 + b^2 = 2ab$. Then

$$0 = a^2 - 2ab + b^2 = (a-b)^2 \tag{8}$$

would have implied that $a = b$. This contradicts the assumption that $a \neq b$. Therefore, $a^2 + b^2 \neq 2ab$.

Suppose $(p \Rightarrow q) \vee (p \Rightarrow \overline{q})$ is false for some logical statements p and q. For a disjunction to be false, we need

$p \Rightarrow q$ to be false, and

$p \Rightarrow \overline{q}$ to be false.

They in turn require

p to be true and q to be false, and

p to be true and $\overline{q}$ to be false.

Having $\overline{q}$ false would imply q is true, which contradicts what we found. Therefore, the given logical formula is always true, hence, a tautology.

Section 3.4

1. We proceed by induction on n. When $n = 1$, the left-hand side of the identity reduces to $1^3 = 1$, and the right-hand side becomes $\frac{1^2 \cdot 2^2}{4} = 1$. Hence, the identity holds when $n = 1$. Assume the identity holds when $n = k$ for some integer $k \geq 1$; that is, assume

$$1^3 + 2^3 + 3^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4} \tag{9}$$

for some integer $k \geq 1$. We want to show that it also holds when $n = k + 1$; that is, we want to show that

$$1^3 + 2^3 + 3^3 + \cdots + (k+1)^3 = \frac{(k+1)^2(k+2)^2}{4}. \tag{10}$$

Using the inductive hypothesis, we find

$$\begin{aligned}
1^3+2^3+3^3+\cdots+(k+1)^3 &= 1^3+2^3+3^3+\cdots+k^3+(k+1)^3 \\
&= \frac{k^2(k+1)^2}{4}+(k+1)^3 \\
&= \frac{(k+1)^2[k^2+4(k+1)]}{4} \\
&= \frac{(k+1)^2(k^2+4k+4)}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4}.
\end{aligned}$$

Therefore, the identity also holds when $n=k+1$. This completes the induction.

Section 3.5

1. We proceed by induction on n. When $n=1$, the product $n(n+1)(n+2)$ becomes $1\cdot2\cdot3=6$, which is obviously a multiple of 3. Hence, the claim holds when $n=1$. Assume the claim holds when $n=k$ for some integer $k\geq1$; that is, assume that $k(k+1)(k+2)$ is a multiple of 3 for some integer $k\geq1$. Then we can write

$$k(k+1)(k+2)=3q \tag{11}$$

for some integer q. We want to show that the claim is still valid when $n=k+1$. That is, we want to show that $(k+1)(k+2)(k+3)$ is also a multiple of 3. So we want to find an integer Q such that

$$(k+1)(k+2)(k+3)=3Q. \tag{12}$$

We note that, using the inductive hypothesis,

$$\begin{aligned}
(k+1)(k+2)(k+3) &= k(k+1)(k+2)+3(k+1)(k+2) \\
&= 3q+3(k+1)(k+2) \\
&= 3\,[q+(k+1)(k+2)],
\end{aligned}$$

where $q+(k+1)(k+2)$ is an integer. Hence, $(k+1)(k+2)(k+3)$ is a multiple of 3. This completes the induction.

2. (b) $S_n=1-\frac{1}{(n+1)!}$ for all integers $n\geq1$.

3. (b) $T_n=\frac{n+1}{2n+3}$ for all integers $n\geq0$.

Section 3.6

1. We proceed by induction on n. When $n=1$, the left-hand side of the identity reduces to $F_1^2=1^2=1$, and the right-hand side becomes $F_1F_2=1\cdot1=1$. Hence, the identity holds when $n=1$. Assume the identity holds when $n=k$ for some integer $k\geq1$; that is, assume

$$F_1^2+F_2^2+F_3^2+\cdots+F_k^2=F_kF_{k+1} \tag{13}$$

for some integer $k\geq1$. We want to show that it also holds when $n=k+1$; that is, we want to show that

$$F_1^2+F_2^2+F_3^2+\cdots+F_{k+1}^2=F_{k+1}F_{k+2}. \tag{14}$$

Using the inductive hypothesis, we find

$$\begin{aligned}
F_1^2+F_2^2+F_3^2+\cdots+F_{k+1}^2 &= F_1^2+F_2^2+F_3^2+\cdots+F_k^2+F_{k+1}^2 \\
&= F_kF_{k+1}+F_{k+1}^2 \\
&= F_{k+1}(F_k+F_{k+1}) \\
&= F_{k+1}F_{k+2}.
\end{aligned}$$

Therefore, the identity also holds when $n=k+1$. This completes the induction.

Section 4.1

1. (a) $\{-5,-4,-3,-2,-1,0,1,2,3\}$(b) $\{1,2,3\}$(c) $\{0,-2,3\}$(d) $\{-3,3\}$
2. (a) $\{n\in\mathbb{Z}\mid n<0\}$

   (b) \{n\in\mathbb{Z} \mid \mbox{\)n\(is a perfect cube}\}

   (c) \{n\in\mathbb{Z} \mid \mbox{\)n\(is a perfect square}\}
3. (a) $\mathbb{Z}^-$ (d) $5\mathbb{Z}$ (f) $4+6\mathbb{Z}$

   Remark. We cannot write (b) as $\mathbb{Z}^3$ and (c) as $\mathbb{Z}^2$, because $\mathbb{Z}^3$ and $\mathbb{Z}^2$ mean something else. If we drop 0 from (e), then $\{4,8,12,\ldots\}=4\mathbb{N}$ However, the inclusion of 0 makes it harder to describe (d) in the form of $4S$.
4. (a) $(-4,7)$ (b) $(-4,7]$ (c) $(0,7]$
5. (a) 10 (b) 11 (c) 7
6. (a) true (b) true (c) true (d) false
7. (a) It is incorrect to write $(3,7]=3<x\leq7$ because $(3,7]$ is a set, but $3<x\leq7$ is a logical statement.

   (b) No, because both $\{x\in\mathbb{R}\mid x^2<0\}$ and $\emptyset$ are sets, so we should use an equal sign to compare them. The notation $\equiv$ only applies to logical statements. The correct way to say it is "$\{x\in\mathbb{R}\mid x^2<0\}=\emptyset$."

Section 4.2

1. (a) true (b) true (c) true (d) true (e) true (f) false
2. We have $\mathbb{Z}\subseteq\mathbb{N}$ because every integer n is also a rational number, as we can write it as the rational number $\frac{n}{1}$.
3. Yes, this is the transitive property.
4. (e) $\{\emptyset,\{a\},\{\{b\}\},\{a,\{b\}\}\}$
5. (a) False, because the set $\{a\}$ cannot be found in $\{a,b,c\}$ as an element.

   (b) False, because a, the sole element in $\{a\}$, cannot be found in $\{\{a\},b,c\}$ as an element.

   (c) False. For $\{a\}\in\wp(\{\{a\},b,c\})$, the set $\{a\}$ must be a subset of $\{\{a\},b,c\}$. This means a must belong to $\{\{a\},b,c\}$, which is not true.

Section 4.3

1. (a) $\{-4,-3,-2,-1,0,1,2,3,4\}$

   (b) $\{-3,-2,-1,0,1,2,3,4\}$

(c) $\{-3,-2,-1,0,1,2,3,\ldots\}$

2. (a) false (b) false
3. (a) $E\cap D$ (b) $\overline{E}\cup B$
4. For example, take $A=\{x\}$, and $B=\{\{x\},x\}$.
5. Assume $A\subseteq C$ and $B\subseteq C$, we want to show that $A\cup B\subseteq C$. In this regard, let $x\in A\cup B$, we want to show that $x\in C$ as well. Since $x\in A\cup B$, the definition of set union asserts that either $x\in A$ or $x\in B$.
   - Case 1: If $x\in A$, then $A\subseteq C$ implies that $x\in C$.
   - Case 2: If $x\in B$, then $B\subseteq C$ implies that $x\in C$.

   In both cases, we find $x\in C$. This proves that $A\cup B\subseteq C$.
6. (a) The notation $\cap$ is used to connect two sets, but "$x\in A$" and "$x\in B$" are both logical statements. We should also use $\Leftrightarrow$ instead of $\equiv$. The statement should have been written as "$x\in A\wedge x\in B\Leftrightarrow x\in A\cap B$."

   (b) If we read it aloud, it sounds perfect:

$$\text{If } x \text{ belongs to } A \text{ and } B, \text{ then } x \text{ belongs to } A\cap B. \tag{15}$$

   The trouble is, every notation has its own meaning and specific usage. In this case, $\wedge$ is not exactly a replacement for the English word "and." Instead, it is the notation for joining two logical statements to form a conjunction. Before $\wedge$, we have "$x\in A$," which is a logical statement. But, after $\wedge$, we have "B," which is a set, and not a logical statement. It should be written as "$x\in A\wedge x\in B\Rightarrow x\in A\cap B$."

Section 4.4

1. (a) $\{(-2,0),(-2,4),(2,0),(2,4)\}$

   (b) $\{(-2,-3),(-2,0),(-2,3),(-2,-3),(-2,0),(-2,3)\}$
2. $2\cdot 2\cdot 2\cdot 3=24$.
3. (a) $\{(-2,\emptyset),(-2,\{-2\}),(-2,\{2\}),(-2,\{-2,2\}),(2,\emptyset),(2,\{-2\}),(2,\{2\}),(2,\{-2,2\})\}$

Section 4.5

1. $\bigcap_{n=1}^{\infty}A_n=[0,2)$, $\bigcup_{n=1}^{\infty}A_n=(-1,\infty)$.
2. $\bigcap_{n=0}^{\infty}C_n=\emptyset$, $\bigcup_{n=0}^{\infty}C_n=\mathbb{N}\cup\{0\}$.
3. $\bigcap_{n\in\mathbb{N}}E_n=E_0=\{0\}$, $\bigcup_{n\in\mathbb{N}}E_n=\mathbb{Z}$.
4. $\bigcup_{i\in I}A_i=[1,\infty)$, $\bigcap_{i\in I}A_i=\{1\}$.
5. $\bigcap_{x\in(1,2)}(1-2x,x^2)=[-1,1]$, $\bigcup_{x\in(1,2)}(1-2x,x^2)=(-3.4)$.
6. $\bigcap_{r\in(0,\infty)}A_r=\{(0,0)\}$, $\bigcup_{r\in(0,\infty)}A_r=\mathbb{R}^*\times\mathbb{R}^+\cup\{(0,0)\}$.

Section 5.1

1. (a) 3 (b) 3 (c) 3 (d) 1
2. We claim that the subset $(3,5)$ does not have a smallest element. To see why, suppose it has a smallest element x. The midpoint between 3 and x is the number $\frac{3+x}{2}$, and

$$3<\frac{3+x}{2}<x<5. \tag{16}$$

   This means $\frac{3+x}{2}$ is also inside the interval $(3,5)$, and is smaller than x. This contradicts the minimality of x. Thus, the interval $(3,5)$ does not have a smallest element. Consequently, the interval $(3,5]$ is not well-ordered.
3. We know that $\mathbb{N}$ is well-ordered. Since $2\mathbb{N}$ is a subset of $\mathbb{N}$, and $2\mathbb{N}$ is clearly nonempty, we conclude from Problem [ex:PWO-04] that $2\mathbb{N}$ is also well-ordered.

Section 5.2

1. (a) 23, 1 (b) -11, 1 (c) -6, 13
2. This is an immediate consequence of Corollary [cor:divalgo].
3. (a) Let n be any integer. Then $n \bmod 3=0,1,2$.
   - Case 1: if $n \bmod 3=0$, then $n=3q$ for some integer q, and

$$n^3-n=(3q)^3-3q=27q^3-3q=3(9q^2-q), \tag{17}$$

     where $9q^2-q$ is an integer.
   - Case 2: if $n \bmod 3=1$, then $n=3q+1$ for some integer q, and

$$n^3-n=(3q+1)^3-(3q+1)=27q^3+27q^2+6q=3(9q^3+9q^2+2q), \tag{18}$$

     where $9q^3+9q^2+2q$ is an integer.
   - Case 2: if $n \bmod 3=2$, then $n=3q+2$ for some integer q, and

$$n^3-n=(3q+2)^3-(3q+2)=27q^3+54q^2+33q+6=3(9q^3+18q^2+11q+2), \tag{19}$$

     where $9q^3+18q^2+11q+2$ is an integer.

   In all three cases, we have shown that n^3-n is a multiple of 3.

   (b) We note that

$$n^3-n=n(n^2-1)=n(n-1)(n+1)=(n-1)n(n+1) \tag{20}$$

   is a product of three consecutive integers. As we have seen in Problem [ex:divalgo-04], any three consecutive integers must contain a multiple of 3. It follows that their product is also a multiple of 3.
4. (a) $s+t$ (b) 4

Section 5.3

Assume $a\mid b$ and $c\mid(-a)$. There exist integers x and y such that $b=ax$ and $-a=cy$. Then

$$b=ax=(-a)(-x)=cy\cdot(-x)=(-c)\cdot xy, \tag{21}$$

where xy is an integer. Thus, $(-c) \mid b$.

There are three cases, depending on the remainder when an integer is divided by 3.

$(3q)^2 = 9q^2 = 3 \cdot 3q^2$.

$(3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$.

$(3q+2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1$.

In each case, we have shown that the square of an integer is of the form $3k$ or $3k+1$.

Section 5.4

1. (a) $1 \cdot 27 + 0 \cdot 81 = 27$ (b) $-3 \cdot 24 + 1 \cdot 84 = 12$ (c) $-35 \cdot 1380 + 16 \cdot 3020 = 20$
2. 1, 2, 17, and 34.

Section 5.5

1. Since

$$-3 \cdot (2n+1) + 2 \cdot (3n+2) = 1, \tag{22}$$

we deduce that $\gcd(2n+1, 3n+2) = 1$.

2. Let a, b, and c be positive integers such that $a \mid c$, $b \mid c$, and $\gcd(a,b) = 1$. Then there exist integers x and y such that $c = ax$ and $c = by$; and there exist integers s and t such that $sa + tb = 1$. It follows that

$$c = c \cdot 1 = c(sa+tb) = csa + ctb. \tag{23}$$

Using $c = ax$ and $c = by$, we find

$$c = csa + ctb = by \cdot sa + ax \cdot tb = ab(ys + xt), \tag{24}$$

where $ys + xt$ is an integer. Thus, $ab \mid c$.

Section 5.6

1. (a) $3^2 \cdot 5^2 \cdot 7$ (b) $2 \cdot 3^2 \cdot 7^2 \cdot 11$
2. (a) 81 (b) 168
3. Every 50 days.
4. Assume $x \in 10\mathbb{Z} \cap 15\mathbb{Z}$, then $x \in 10\mathbb{Z}$ and $x \in 15\mathbb{Z}$. This means x is a multiple of both 10 and 15. Consequently, x is a multiple of \lcm$(10,15) = 30$, which means $x \in 30\mathbb{Z}$. Thus, $10\mathbb{Z} \cap 15\mathbb{Z} \subseteq 30\mathbb{Z}$.

   Next, assume $x \in 30\mathbb{Z}$, then x is a multiple of 30. Consequently, x is a multiple of 10, as well as a multiple of 15. This means $x \in 10\mathbb{Z}$, and $x \in 15\mathbb{Z}$. As a result, $x \in 10\mathbb{Z} \cap 15\mathbb{Z}$. Thus, $30\mathbb{Z} \subseteq 10\mathbb{Z} \cap 15\mathbb{Z}$. Together with $10\mathbb{Z} \cap 15\mathbb{Z} \subseteq 30\mathbb{Z}$, we conclude that $10\mathbb{Z} \cap 15\mathbb{Z} = 30\mathbb{Z}$.
5. (a) When p is divided by 4, its remainder is 0, 1, 2, or 3. But p is odd, hence, p is of the form $4k+1$ or $4k+3$ for some integer k. Since $p \geq 3$, we also need k to be a nonnegative integer.

   (b) When p is divided by 6, its remainder is 0, 1, 2, 3, 4, or 5. But p is odd, hence, p is of the form $6k+1$, $6k+3$, or $6k+5$. We rule out the form $6k+3$ because this would make p a multiple of 3. Hence, p is of the form $6k+1$ or $6k+5$ for some nonnegative integer k.

Section 5.7

1. The addition and multiplication tables for $\mathbb{Z}_8$ are listed below.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	2	5	4	3	2	1

(25)

   Only 1, 3, 5, and 7 have multiplicative inverses. In fact,$1^{-1} = 1$, $3^{-1} = 3$, $5^{-1} = 5$, and $7^{-1} = 7$.
2. The sum is 9, and the product is 7.
3. From the following computation

m (mod-7)	m^2+1 (mod-7)
0	$0^2+1=1$
±1	$1^2+1=2$
±2	$2^2+1=5$
±3	$3^2+1=10\equiv3$

(26)

   we determine that $m^2+1 \not\equiv 0$ (mod 7). Hence, m^2+1 is not a multiple of 7 for all integers m.
4. Both methods give $4^{45} = 1$ in $\mathbb{Z}_{11}$.
5. (a) 9

Section 6.1

1. -24pt

x	5.7	π	e	-7.2	-0.8	9
$\lfloor x \rfloor$	5	3	2	-8	-1	9
$\lceil x \rceil$	6	4	3	-7	0	9
$[x]$	6	3	3	-7	-1	9

2. $[0, \infty)$.

Section 6.2

1. $\left[\frac{7}{3}, \infty\right)$.

2. Only g is a well-defined function. The image $f(4)$ is undefined, and there are two values for $h(3)$. Hence, both f and h are not well-defined functions.
3. (a) Yes, because no division by zero will ever occur.
4. -24pt

x	1	2	3	4
$p(x)$	3	1	2	2

0.4in

x	1	2	3	4
$q(x)$	2	3	1	3

5. (a) 7 (b) 7 (c) 3

Section 6.3

1. (a) No. For example, $f(0) = f(2) = 1$.
   (b) Yes, since $g'(x) = 3x^2 - 4x = x(3x-4) > 0$ for $x > 2$.
2. Because the domain and the codomain are half-open intervals, we need to be careful with the inclusion and exclusion of the endpoints. We can use the graph displayed below on the left.
   We find $f(x) = \frac{3}{2}x + \frac{1}{2}$.
3. (a) One-to-one (b) Not one-to-one
4. (a) Not one-to-one (b) One-to-one
5. There are twelve one-to-one functions from $\{1,2\}$ to $\{a,b,c,d\}$. The images of 1 and 2 under them are listed below.

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}
1	a	a	a	b	b	b	c	c	c	d	d	d
2	b	c	d	a	c	d	a	b	d	a	b	c

(27)

6. (a) One-to-one (b) Not one-to-one (c) Not one-to-one

Section 6.4

1. (a) Yes! It is not easy to express x in terms of y from the equation $y = x^3 - 2x^2 + 1$. However, from its graph, we can tell that the y-values cover all the possible real values in the codomain.
   (b) No, because $g(x) \geq 1$.
2. (b) Not onto (c) Onto
3. (b) Not onto (c) Onto
4. No, because we have at most two distinct images, but the codomain has four elements.
5. (a) Onto (b) Not onto (c) Not onto

Section 6.5

1. (a) $f_1(A) = \{a,b\}$, $f_1^{-1}(B) = \{2,3,4,5\}$
   (b) $f_2(A) = \{a,c\}$, $f_2^{-1}(B) = \{2,4\}$
   (c) $f_3(A) = \{b,d\}$, $f_3^{-1}(B) = \emptyset$
   (d) $f_4(A) = \{e\}$, $f_4^{-1}(B) = \{5\}$
2. The images of s are tabulated below.

x	0	1	2	3	4	5	6	7	8	9	10	11
$s(x)$	7	11	3	7	11	3	7	11	3	7	11	3

(28)

   (a) $\{3,11\}$(b) $\{0,3,6,9\}$(c) $\{3,7,11\}$
3. (a) $[20,26)$; $\{20,23,26\}$(b) $[-3,-\frac{4}{3})$; $\{-2\}$
4. (a) $\{\frac{3}{5},\frac{9}{5},\frac{27}{5},3,9,27,15,45,135\}$(b) $\{(-3,2)\}$ (c) $\mathbb{N}\times\{0\}$
5. For a function to be well-defined, each row sum must be 1. For the function to be one-to-one, each column sum must be at most 1. For the function to be onto, each column sum must be at least 1 (hence, no column sum is zero).
6. Let $y \in f(C_1) - f(C_2)$, we want to show that $y \in f(C_1 - C_2)$ as well. Since $y \in f(C_1) - f(C_2)$, we know there exists $x \in A$ such that $f(x) = y$. Having $y \in f(C_1) - f(C-2)$ means $y \in f(C_1)$ but $y \notin f(C_2)$. Hence, $x \in C_1$ but $x \notin C_2$. In other words, $x \in C_1 - C_2$. This leads to $y = f(x) \in f(C_1 - C_2)$. This completes the proof that $f(C_1) - f(C_2) \subseteq f(C_1 - C_2)$.
7. $\{0,1,4,9\}$; $\{0,\pm1,\pm2,\pm3\}$.

Section 6.6

1. Only (e) is bijective.
2. Their inverse functions $f^{-1}, g^{-1} : (4,7) \to (1,3)$ are defined by

$$f^{-1}(x) = \frac{2}{3}\left(x - \frac{5}{2}\right), \qquad \text{and} \qquad g^{-1}(x) = -\frac{2}{3}\left(x - \frac{17}{2}\right). \tag{29}$$

3. $g^{-1} :\to [4,7][1,3]$, where g^{-1}(x) = \cases{ x-3 & if\)4x < 5\(, \cr \textstyle \frac{1}{2}(11-x) & if\)5x7\(. \cr}
4. $s^{-1} : (-\infty,-3) \to \mathbb{R}$, where $s^{-1}(x) = \frac{1}{2}\ln\left(\frac{4-x}{7}\right)$.
5. (a) $u^{-1} : \mathbb{Q} \to \mathbb{Q}$, $u^{-1}(x) = (x+2)/3$
6. The images under $\alpha^{-1} : \{a,b,c,d,e,f,g,h\} \to \{1,2,3,4,5,6,7,8\}$are given below.

x	a	b	c	d	e	f	g	h
$\alpha^{-1}(x)$	2	5	8	3	6	7	1	4

(30)

Section 6.7

1. Both $f\circ g$ and $g\circ f$ are from $\mathbb{R}$ to $\mathbb{R}$, where $(f\circ g)(x) = 15x^2 + 19$, and $(g\circ f)(x) = 75x^2 - 30x + 7$.
2. We do not need to find the formula of the composite function, as we can evaluate the result directly: $f(g(f(0))) = f(g(1)) = f(2) = -5$.
3. (a) $g\circ f : \mathbb{Z} \to \mathbb{Q}$, $(g\circ f)(n) = 1/(n^2+1)$
   (b) $g\circ f : \mathbb{R} \to (0,1)$, $(g\circ f)(x) = x^2/(x^2+1)$
4. (a) $g\circ f : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$,
   $(g\circ f)(1) = 2$, $(g\circ f)(2) = 5$, $(g\circ f)(3) = 1$, $(g\circ f)(4) = 3$, $(g\circ f)(5) = 4$

5. $g\circ f:\mathbb{Z}\to\mathbb{Z}$, (g\circ f)(n) = \cases{ 3(2n-1) & if\)n0\(, \cr 2n+1 & if\)n < 0\(. \cr}

6. (a) $f\circ g:\mathbb{Z}\to\mathbb{Z}$, $(f\circ g)(n)=3-n$

{(f\circ g)^{-1}}:{\mathbb{Z}}\to{\mathbb{Z}}\), $(f\circ g)^{-1}(n)=3-n$

$f^{-1}:\mathbb{Z}\to\mathbb{Z}$, $f^{-1}(n)=2-n$

$g^{-1}:\mathbb{Z}\to\mathbb{Z}$, $g^{-1}(n)=n-1$

$g^{-1}\circ:f^{-1}\mathbb{Z}\to\mathbb{Z}$, $(g^{-1}\circ f^{-1})(n)=3-n$

Section 7.1

1. (a)

\noalign\medskip

	1	2	3	6
1	1	0	0	0
2	0	1	0	0
3	0	0	1	0
6	0	0	0	1

(b)

0pt

(140,60)(-10,-10) (0, 0)(40,0)4 (0,40)(40,0)4 (-10,-20)(20,20)1 (-10,40)(20,20)1 (30,-20)(20,20)2 (30,40)(20,20)2 (70,-20)(20,20)3 (70,40)(20,20)3 (110,-20)(20,20)6 (110,40)(20,20)6 (0,0)(1,1) 40 (40,0)(-1,1) 40 (0,0)(2,1) 80 (40,0)(1,1) 40 (0,0)(3,1)120 (40,0)(2,1) 80 (80,0)(-2,1) 80 (120,0)(-3,1)120 (80,0)(-1,1) 40 (120,0)(-2,1) 80 (80,0)(1,1) 40 (120,0)(-1,1) 40

0.6in

0pt \noalign\medskip

	1	2	3	6
1	0	1	1	1
2	1	0	1	1
3	1	1	0	1
6	1	1	1	0

(c)

0pt

(140,60)(-10,-10) (0, 0)(40,0)4 (0,40)(40,0)4 (-10,-20)(20,20)1 (-10,40)(20,20)1 (30,-20)(20,20)2 (30,40)(20,20)2 (70,-20)(20,20)3 (70,40)(20,20)3 (110,-20)(20,20)6 (110,40)(20,20)6 (0,0)(1,1) 40 (0,0)(2,1) 80 (40,0)(1,1) 40 (0,0)(3,1)120 (40,0)(2,1) 80 (80,0)(1,1) 40

0.6in

0pt \noalign\medskip

	1	2	3	6
1	0	1	1	1
2	0	0	1	1
3	0	0	0	1
6	0	0	0	0

2. (a) domain $=$ image $=\{1,2,3,6\}$.

(b) domain $=$ image $=\{1,2,3,6\}$.

(c) domain $=\{1,2,3\}$, image $=\{2,3,6\}$.

3. 0pt

(220,60)(-10,-10) (0, 0)(40,0)6 (0,40)(40,0)6 (-10,-20)(20,20) 1 (-10,40)(20,20) 1 (30,-20)(20,20) 2 (30,40)(20,20) 2 (70,-20)(20,20) 4 (70,40)(20,20) 4 (110,-20)(20,20) 5 (110,40)(20,20) 5 (150,-20)(20,20)10 (150,40)(20,20)10 (190,-20)(20,20)20 (190,40)(20,20)20 (0,0)(1,1) 40 (40,0)(1,1) 40 (0,0)(2,1) 80 (0,0)(3,1)120 (40,0)(3,1)120 (0,0)(4,1)160 (40,0)(4,1)160 (0,0)(5,1)200 (80,0)(3,1)120 (120,0)(1,1) 40 (120,0)(2,1) 80 (160,0)(1,1) 40

0pt \noalign\medskip

	1	2	4	5	10	20
1	0	1	1	1	1	1
2	0	0	1	0	1	1
4	0	0	0	0	0	1
5	0	0	0	0	1	1
10	0	0	0	0	0	1
20	0	0	0	0	0	0

4. \noalign\medskip

	$\emptyset$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\emptyset$	0	0	0	0
$\{1\}$	0	1	0	1
$\{2\}$	0	0	1	1
$\{1,2\}$	0	1	1	1

Section 7.2

1. (a) Reflexive, symmetric, antisymmetric, and transitive.

(b) Irreflexive, and symmetric.

(c) Irreflexive, and transitive.

2. (a) Antisymmetric.

(b) Reflexive, symmetric, and transitive.

(c) Irreflexive, symmetric, and transitive.

3. Reflexive, symmetric, and transitive.

4. Antisymmetric, and transitive.

5. Irreflexive, and antisymmetric.

6. Symmetric.

7. (a) A is not reflexive because $(X,X) \notin A$ if $X \neq \emptyset$.

   (b) A is not irreflexive because $(\emptyset,\emptyset) \in A$.

   (c) No. For example, consider $S=\{a,b,c\}$, $X=\{a\}$, $Y=\{b\}$, and $Z=\{a,c\}$. Then $(X,Y) \in A$, $(Y,Z) \in A$, but $(X,Z) \notin A$.

   (d)

   0pt

   (300,60)(-10,-10) (0, 0)(40,0)8 (0,40)(40,0)8 (-10,-20)(20,20)$\emptyset$ (-10, 40)(20,20)$\emptyset$ (30,-20)(20,20)$\{a\}$ (30, 40)(20,20)$\{a\}$ (70,-20)(20,20)$\{b\}$ (70, 40)(20,20)$\{b\}$ (110,-20)(20,20)$\{c\}$ (110, 40)(20,20)$\{c\}$ (140,-20)(40,20)$\{a,b\}$ (140, 40)(40,20)$\{a,b\}$ (180,-20)(40,20)$\{a,c\}$ (180, 40)(40,20)$\{a,c\}$ (220,-20)(40,20)$\{b,c\}$ (220, 40)(40,20)$\{b,c\}$ (260,-20)(40,20)$\{a,b,c\}$ (260, 40)(40,20)$\{a,b,c\}$ (0, 0)(0,1) 40 (0, 0)(1,1) 40 (0, 0)(5,1)200 (0, 0)(2,1) 80 (0, 0)(6,1)240 (0, 0)(3,1)120 (0,0, 280,40) (0, 0)(4,1)160 (40, 0)(-1,1) 40 (40, 0)(1,1) 40 (40, 0)(2,1) 80 (40, 0)(5,1)200 (80, 0)(-2,1) 80 (80, 0)(-1,1) 40 (80, 0)(2,1) 80 (80, 0)(1,1) 40 (120, 0)(-3,1)120 (120, 0)(-1,1) 40 (120, 0)(-2,1) 80 (120, 0)(1,1) 40 (160, 0)(-1,1) 40 (160, 0)(-4,1)160 (200, 0)(-3,1)120 (200, 0)(-5,1)200 (240, 0)(-6,1)240 (240, 0)(-5,1)200 (280,0, 0,40)

   18pt

   0pt

   \rotatebox90\)\(\rotatebox90\)a\(\rotatebox90\)b\(\rotatebox90\)c\(\rotatebox90\)a,b\(\rotatebox90\)a,c\(\rotatebox90\)$b,$

   \noalign\medskip $\begin{matrix} \emptyset \\ \{a\} \\ \{b\} \\ \{c\} \\ \{a,b\} \\ \{a,c\} \\ \{b,c\} \\ \{a,b,c\} \end{matrix}$ \setlength\arraycolsep$7.7pt$ $\begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 1&0&1&1&0&0&1&0 \\ 1&1&0&1&0&1&0&0 \\ 1&1&1&0&1&0&0&0 \\ 1&0&0&1&0&0&0&0 \\ 1&0&1&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0 \end{pmatrix}$

8. (a) Symmetric.

   (b) Reflexive, and symmetric.

9. (a) Reflexive, antisymmetric, and transitive.

   (b) Reflexive, symmetric, and transitive.

   (c) Symmetric.

10. (a) Reflexive, antisymmetric, and transitive.

    (b) Symmetric.

    (c) Symmetric, and transitive.

11. (a) Reflexive, and transitive.

    (b) Symmetric,

    (c) Reflexive, symmetric, and transitive.

12. (a) Symmetric, and transitive.

    (b) Reflexive, symmetric, and transitive.

    (c) Reflexive, and transitive.

Section 7.3

1. (a) The equivalence classes are of the form $\{3-k, 3+k\}$ for some integer k. For instance, $[3]=\{3\}$, $[2]=\{2,4\}$, $[1]=\{1,5\}$, and $[-5]=\{-5,11\}$.

   (b) There are three equivalence classes: $[0]=3\mathbb{Z}$, $[1]=1+3\mathbb{Z}$, and $[2]=2+3\mathbb{Z}$.

2. (a) True

   (b) False

   (c) $[\{1,5\}]=\big\{\{1\},\{1,2\},\{1,4\},\{1,5\},\{1,2,4\},\{1,2,5\},\{1,4,5\},\{1,2,4,5\}\big\}$

   (d) $[X]=\{(X\cap T)\cup Y \mid Y \in \wp(\overline{T})\}$. In other words, $S \sim X$ if S contains the same element in $X \cap T$, plus possibly some elements not in T.

3. (a) Yes, with [(a,b)] = \{(x,y) \mid y=x+k \mbox{ for some constant\)k\(}\} . In other words, the equivalence classes are the straight lines of the form $y=x+k$ for some constant k.

   (b) No. For example, $(2,5) \sim (3,5)$ and $(3,5) \sim (3,7)$, but $(2,5) \nsim (3,7)$. Hence, the relation $\sim$ is not transitive.

4. We find $[0]=\frac{1}{2}\mathbb{Z}=\{\frac{n}{2} \mid n \in \mathbb{Z}\}$, and $[\frac{1}{4}]=\frac{1}{4}+\frac{1}{2}\mathbb{Z}=\{\frac{2n+1}{4} \mid n \in \mathbb{Z}\}$.

Section 7.4

1. The Hasse diagram is shown below.

   (180,230) (80,20)(80, 70)2(0,0)(0,70)2(-6,5)60 (20,90)(80,-70)2(0,0)(0,70)2(6,5)60 (10,90)(80,-70)2(0,0)(80,70)2(0,1)50 (80, 0)(20,20) 1 (0, 70)(20,20) 2 (80, 70)(20,20) 3 (160, 70)(20,20) 5 (-10,140)(40,20) 6 (70,140)(40,20)10 (150,140)(40,20)15 (70,210)(40,20)30

2. Let $a \in B$, since $B \subseteq A$, we also find $a \in A$. Since $(A, \preceq)$ is a poset, the relation $\preceq$ on A is reflexive, hence, $a \preceq a$. This shows that $\preceq$ is still reflexive when restricted to B. Antisymmetry and transitivity are proved with a similar argument.

3. (b) The Hasse diagram is shown below.

   (180,160) (10,90)(160,0)2(0,1)50 (80,20)(-6,5)60 (100,20)(6,5)60 (160,90, 20,140) (20,90, 160,140) (80, 0)(20,20)0 (0, 70)(20,20)-1 (160, 70)(20,20)1 (0,140)(20,20)-2 (160,140)(20,20)2

4. $B=\big\{\emptyset,\{a\},\{a,b\},\{a,b,c\},\{a,b,c,d\}\big\}$.

Section 8.2

1. 6.
2. 70.
3. $7\cdot 5+7\cdot 4+5\cdot 4$
4. 4^5, $4^5-3\cdot 4^2$
5. (a) 52^4 (b) 39^4 (c) $4\cdot 13^4$ (d) $4\cdot 48\cdot 52^3$ (e) 52^4-48^4
6. (a) $9\cdot 10^3$ (b) $8\cdot 9^3$ (c) $9\cdot 10^3-8\cdot 9^3$ (d) $9\cdot 10$

7. (a) 8^6 (b) $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$ (c) 0 (d) $8^6 - 4^6$ (e) $4 \cdot 8^4$ (f) 7^5

Section 8.3

1. 62^8, $P(62,8)$.
2. $P(14,5)$.
3. $p(7,3) \cdot P(10,3) + P(7,3) \cdot P(11,3) + P(10,3) \cdot P(11,3)$.
4. $P(11,7) \cdot 3!/7$.

Section 8.4

1. $\binom{6}{3}\binom{8}{3}$.
2. (a) at least 5 (b) at least 7
3. 10.
4. (a) $\binom{14}{4}$ (b) $\binom{14}{4} - \binom{11}{4}$ (c) $\binom{3}{2}\binom{7}{1}\binom{4}{1} + \binom{3}{1}\binom{7}{2}\binom{4}{1} + \binom{3}{1}\binom{7}{1}\binom{4}{2}$
5. (a) 8! (b) $\binom{8}{2} P(8,2) \left[\binom{6}{2} P(8,2) + 2 \cdot 7 \cdot 6 \cdot 7 + 7 \cdot 6\right]$
6. $\binom{16}{7}$.
7. (a) $\binom{52}{5}$ (b) $4\binom{13}{2} 13^3$ (c) $13\binom{4}{2}\binom{12}{3} 4^3$ (d) $13\binom{4}{3}\binom{12}{2} 4^2$
   (e) $13\binom{4}{3} 12\binom{4}{2}$ (f) $10 \cdot (4^5 - 1)$ (g) $4\left[\binom{13}{5} - 10\right]$ (h) $4 \cdot 10$

Section 8.5

1. (a) $x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$
   (b) $s^6 - 6s^5t + 15s^4t^2 - 20s^3t^3 + 15s^2t^4 - 6st^5 + t^6$
   (c) $a^4 + 12a^3b + 54a^2b^2 + 108ab^3 + 81b^4$
2. (a) $\binom{4}{2} = 6$ (b) $-\binom{9}{3} 3^6 \left(\frac{2}{5}\right)^3 = -\frac{489888}{125}$ (c) 0 (d) $-\binom{6}{3} 3^3 \left(\frac{5}{7}\right)^3 = -\frac{67500}{343}$
3. $\sum_{k=0}^{n} \binom{n}{k} r^k = (1+r)^n$
4. (c) $k^2 = 2\binom{k}{2} + \binom{k}{1}$ (d) $\sum_{k=1}^{n} k^2 = \frac{1}{6}\, n(n+1)(2n+1)$

Index

Glossary

Sample Word 1 | Sample Definition 1

Detailed Licensing

Overview

Title: MTH 220 Discrete Math

Webpages: 64

Applicable Restrictions: Noncommercial

All licenses found:

- CC BY-NC-SA 4.0: 78.1% (50 pages)
- Undeclared: 20.3% (13 pages)
- CC BY-NC-SA 3.0: 1.6% (1 page)

By Page

- MTH 220 Discrete Math - *Undeclared*
  - Front Matter - *Undeclared*
    - TitlePage - *Undeclared*
    - InfoPage - *Undeclared*
    - Table of Contents - *Undeclared*
    - Licensing - *Undeclared*
  - 1: Introduction to Discrete Mathematics - *CC BY-NC-SA 4.0*
    - 1.0 Preface - *CC BY-NC-SA 4.0*
    - 1.1: An Overview of Discrete Mathematics - *CC BY-NC-SA 4.0*
    - 1.2: Suggestions to Students - *CC BY-NC-SA 4.0*
    - 1.3: How to Read and Write Mathematics - *CC BY-NC-SA 4.0*
    - 1.4: Proving Identities - *CC BY-NC-SA 4.0*
    - 1.5: Introduction to Sets and Real Numbers - *Undeclared*
  - 2: Logic - *CC BY-NC-SA 4.0*
    - 2.1: Propositions - *CC BY-NC-SA 4.0*
    - 2.2: Conjunctions and Disjunctions - *CC BY-NC-SA 4.0*
    - 2.3: Implications - *CC BY-NC-SA 4.0*
    - 2.4: Biconditional Statements - *CC BY-NC-SA 4.0*
    - 2.5: Logical Equivalences - *CC BY-NC-SA 4.0*
    - 2.6 Arguments and Rules of Inference - *Undeclared*
    - 2.7: Quantifiers - *CC BY-NC-SA 4.0*
    - 2.8: Multiple Quantifiers - *CC BY-NC-SA 4.0*
  - 3: Proof Techniques - *CC BY-NC-SA 4.0*
    - 3.1: An Introduction to Proof Techniques - *CC BY-NC-SA 4.0*
    - 3.2: Direct Proofs - *CC BY-NC-SA 4.0*
    - 3.3: Q-R Theorem and Mod - *CC BY-NC-SA 4.0*
    - 3.4: Indirect Proofs - *CC BY-NC-SA 4.0*
    - 3.5: The Euclidean Algorithm - *CC BY-NC-SA 3.0*
    - 3.6: Mathematical Induction - An Introduction - *CC BY-NC-SA 4.0*
    - 3.7: The Well-Ordering Principle - *CC BY-NC-SA 4.0*
    - 3.8: More on Mathematical Induction - *CC BY-NC-SA 4.0*
  - 4: Sets - *CC BY-NC-SA 4.0*
    - 4.1: An Introduction to Sets - *CC BY-NC-SA 4.0*
    - 4.2: Subsets and Power Sets - *CC BY-NC-SA 4.0*
    - 4.3: Unions and Intersections - *CC BY-NC-SA 4.0*
    - 4.4: Cartesian Products - *CC BY-NC-SA 4.0*
    - 4.5: Index Sets and Partitions - *CC BY-NC-SA 4.0*
  - 5: Functions - *CC BY-NC-SA 4.0*
    - 5.1: Intro to Relations and Functions - *CC BY-NC-SA 4.0*
    - 5.2: Definition of Functions - *CC BY-NC-SA 4.0*
    - 5.3: One-to-One Functions - *CC BY-NC-SA 4.0*
    - 5.4: Onto Functions and Images/Preimages of Sets - *CC BY-NC-SA 4.0*
    - 5.5: Inverse Functions and Composition - *CC BY-NC-SA 4.0*
    - 5.6: Infinite Sets and Cardinality - *CC BY-NC-SA 4.0*
  - 6: Relations - *CC BY-NC-SA 4.0*
    - 6.1: Relations on Sets - *CC BY-NC-SA 4.0*
    - 6.2: Properties of Relations - *CC BY-NC-SA 4.0*
    - 6.3: Equivalence Relations and Partitions - *CC BY-NC-SA 4.0*
  - 7: Combinatorics - *CC BY-NC-SA 4.0*
    - 7.1: Intro, Probability and Pigeonhole Principle - *CC BY-NC-SA 4.0*
    - 7.2: Addition and Multiplication Principles - *CC BY-NC-SA 4.0*
    - 7.3: Permutations - *CC BY-NC-SA 4.0*
    - 7.4: Combinations - *CC BY-NC-SA 4.0*
    - 7.5: Combinations WITH Repetitions - *CC BY-NC-SA 4.0*
    - 7.6: The Binomial Theorem - *CC BY-NC-SA 4.0*
  - 8: Big O - *CC BY-NC-SA 4.0*