


Undergraduate Texts in Mathematics

UTM

Reading, Writing, and Proving

A Closer Look at Mathematics

Second Edition

 Springer

Undergraduate Texts in Mathematics

Editorial Board

S. Axler

K.A. Ribet

For further volumes:

<http://www.springer.com/series/666>

Ulrich Daepf • Pamela Gorkin

Reading, Writing, and Proving

A Closer Look at Mathematics

Second Edition



Springer

Ulrich Daepf
Department of Mathematics
Bucknell University
Lewisburg, PA 17837
USA
udaepf@bucknell.edu

Pamela Gorkin
Department of Mathematics
Bucknell University
Lewisburg, PA 17837
USA
pgorkin@bucknell.edu

Editorial Board:

S. Axler
Mathematics Department
San Francisco State University
San Francisco, CA 94132
USA
axler@sfsu.edu

K.A. Ribet
Mathematics Department
University of California at Berkeley
Berkeley, CA 94720
USA
ribet@math.berkeley.edu

ISSN 0172-6056
ISBN 978-1-4419-9478-3 e-ISBN 978-1-4419-9479-0
DOI 10.1007/978-1-4419-9479-0
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2011931085

© Springer Science+Business Media, LLC 2011

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

For Hannes and Madeleine

Preface

You are probably about to teach or take a “first course in proof techniques,” or maybe you just want to learn more about mathematics. No matter what the reason, a student who wishes to learn the material in this book likes mathematics and we hope to keep it that way. At this point, students have an intuitive sense of why things are true, but not the exposure to the detailed and critical thinking necessary to survive in the mathematical world. We have written this book to bridge this gap.

In our experience, students beginning this course have little training in rigorous mathematical reasoning; they need guidance. At the end, they are where they should be; on their own. Our aim is to teach the students to read, write, and do mathematics independently, and to do it with clarity, precision, and care. If we can maintain the enthusiasm they have for the subject, or even create some along the way, our book has done what it was intended to do.

Reading. This book was written for a course we teach to first- and second-year college students. The style is informal. A few problems require calculus, but these are identified as such. Students will also need to participate while reading proofs, prodded by questions (such as, “Why?”). Many detailed examples are provided in each chapter. Since we encourage the students to draw pictures, we include many illustrations as well. Exercises, designed to teach certain concepts, are also included. These can be used as a basis for class discussion, or preparation for the class. Students are expected to solve the exercises before moving on to the problems. Complete solutions to all of the exercises are provided at the end of each chapter. Problems of varying degrees of difficulty appear at the end of each chapter. Some problems are simply proofs of theorems that students are asked to read and summarize; others supply details to statements in the text. Though many of the remaining problems are standard, we hope that students will solve some of the unique problems presented in each chapter.

Writing. The bad news is that it is not easy to write a proof well. The good news is that with proper instruction, students quickly learn the basics of writing. We try to write in a way that we hope is worthy of imitation, but we also provide students

with “tips” on writing, ranging from the (what should be) obvious to the insider’s preference (“Don’t start a sentence with a symbol.”).

Proving. How can someone learn to prove mathematical results? There are many theories on this. We believe that learning mathematics is the same as learning to play an instrument or learning to succeed at a particular sport. Someone must provide the background: the tips, information on the basic skills, and the insider’s “know-how.” Then the student has to practice. Musicians and athletes practice hours a day, and it’s not surprising that most mathematicians do, too. We will provide students with the background; the exercises and problems are there for practice. The instructor observes, guides, teaches and, if need be, corrects. As with anything else, the more a student practices, the better she or he will become at solving problems.

Using this book. What should be in a book like this one? Even a quick glance at other texts on this subject will tell you that everyone agrees on certain topics: logic, quantifiers, basic set theoretic concepts, mathematical induction, and the definition and properties of functions. The depth of coverage is open to debate, of course. We try to cover logic and quantifiers fairly quickly, because we believe that students can only fully appreciate the fundamentals of mathematics when they are applied to interesting problems.

What is also apparent is that after these essential concepts, everyone disagrees on what should be included. Even we prefer to vary our approach depending on our students. We have tried to provide enough material for a flexible approach.

- *The Minimal Approach.* If you need only the basics, cover Chapters 1–18. (If you assume the well ordering principle, or decide to accept the principle of mathematical induction without proof, you can also omit Chapters 12 and 13.)
- *The Usual Approach.* This approach includes Chapters 1–18 and Chapters 21–24. (This is easily doable in a standard semester, if the class meets three hours per week.)
- *The Algebra Approach.* For an algebraic slant to the course, cover Chapters 1–18, omitting Chapter 13 and including Chapters 27 and 28.
- *The Analysis Approach.* For a slant toward analysis, cover Chapters 1–23. (Include Chapter 24, if time allows. This is what we usually cover in our course.) Include as much material from Chapters 25 and 26 as time allows. Students usually enjoy an introduction to metric spaces.
- *Projects.* We have included projects intended to let students demonstrate what they can do when they are on their own. We indicate prerequisites for each project, and have tried to vary them enough that they can be assigned throughout the semester. The results in these projects come from different areas that we find particularly interesting. Students can be guided to a project at their level. Since there are open-ended parts in each project, students can take these projects as far as they want. We usually encourage the students to work on these in groups.
- *Notation.* A word about some of our symbols is in order here. In an attempt to make this book user-friendly, we indicate the end of a proof with the well-known symbol \square . The end of an example or exercise is designated by \circ . If a problem is used later in the text, we designate it by **Problem**[#]. We also have a fair number

of “nonproofs.” These are “proofs” with errors, gaps, or both; the students are asked to find the flaw and to fix it. We conclude such “proofs” with the symbol \square . Every other symbol will be defined when we introduce you to it. Definitions are incorporated in the text for ease of reading and the terms defined are given in boldface type.

Presenting. We also hope that students will make the transition to thinking of themselves as members of a mathematical community. We encourage the students we have in this class to attend talks, give talks, go to conferences, read mathematical books, watch mathematical movies, read journal articles, and talk with their colleagues about the things in this course that interest them. Our (incomplete, but lengthy) list of references should serve a student well as a starting point. Each of the projects works well as the basis of a talk for students, and we have included some background material in each section. We begin the chapter on projects with some tips on speaking about mathematics.

What's new in this edition. We have made many changes to the first edition. First, all exercises now have solutions and every chapter, except for the first, has at least twenty problems of varying difficulty. As a result, the text has now roughly twice as many problems than before. As in the first edition, definitions are incorporated in the text. In this edition, all definitions newly introduced in a chapter appear again in a section with formal statements of the new definitions. We have included a detailed description of definitions by recursion and a recursion theorem. We've added axioms of set theory to the appendix. We have included new projects: one on the axiom of choice and one on complex numbers. We have added some interesting pieces to two projects, *Picture Proofs* and *The Best Number of All (and Some Other Pretty Good Ones)*.

Some chapters have been changed or added. The first edition's Chapter 12, which required more of students than previous chapters, has been broken into two chapters, now enumerated Chapters 12 and 13. If the instructor wishes, it is possible to simply assume the results in Chapter 13 and omit the chapter. We have also included a new chapter, Chapter 24, on the Cantor–Schröder–Bernstein theorem. We feel that this is the proper culmination to Chapters 21–23 and a wonderful way to end the course, but be forewarned that it is not an easy chapter.

Thanks to many of you who used the text, we were able to pinpoint areas where we could improve many of our explanations, provide more motivation, or present a different perspective. Our goal was to find simpler, more precise explanations, and we hope that we have been successful. One new feature of this text that may interest instructors of the course: We have written solutions to every third problem. These are available on our website (see below).

Of course, we have updated our reference list, made corrections to errors that appeared in the first version, and, most likely, introduced new errors in the second version. We hope you will send us corrections to errors that you find in the text, as well as any suggestions you have for improvement.

We hope that through reading, writing, proving, and presenting mathematics, we can produce students who will make good colleagues in every sense of the word.

Acknowledgments. Writing a book is a long process, and we wish to express our gratitude to those who have helped us along the way. We are, of course, grateful to the students at Bucknell University who suffered through the early versions of the manuscript, as well as those who used later versions. Their comments, suggestions, and detection of errors are most appreciated. We thank Andrew Shaffer for help with the illustrations. We also wish to express our thanks to our colleagues and friends, Gregory Adams, Thomas Cassidy, David Farmer, and Paul McGuire, for helpful conversations. We are particularly grateful to Raymond Mortini for his willingness to carefully read (and criticize) the entire text. The book is surely better for it. We also wish to thank our (former) student editor, Brad Parker. We simply cannot overstate the value of Brad's careful reading, insightful comments, and his suggestions for better prose. We thank Universität Bern, Switzerland for support provided during our sabbaticals. Finally, we thank Hannes and Madeleine Daepf for putting up with infinitely many dinner conversations about this text.

For the second edition, we wish to thank professors Paul Stanford at The University of Texas at Dallas, Matthew Daws at the University of Leeds, Raymond Boute at Ghent University, John M. Lee at the University of Washington, and Buster Thelen for many thoughtful suggestions. In addition to our colleagues who helped us with the first edition, we are grateful to John Bourke, Emily Dryden, and Allen Schweinsberg for their helpful comments. We wish to thank Peter McNamara, in particular, for spotting errors and inconsistencies, for suggestions for other references, and for pointing out sections that were potentially confusing for students. Again, we are grateful to all our colleagues and our students who have helped us to make this a better text.

We thank Hannes Daepf for creating a website to accompany the text. This website contains complete solutions to all problems numbered $3n$, where n is a positive integer. It also contains corrections to both editions of the text.

<http://www.facstaff.bucknell.edu/udaepf/readwriteprove/>

Lewisburg, PA
December 2010

Ulrich Daepf
Pamela Gorkin

Authors' e-mails: udaepf@bucknell.edu and pgorkin@bucknell.edu

Contents

Preface	vii
1 The How, When, and Why of Mathematics	1
Spotlight: George Pólya	8
Tips on Doing Homework	11
2 Logically Speaking	13
3 Introducing the Contrapositive and Converse	25
4 Set Notation and Quantifiers	33
Tips on Quantification	45
5 Proof Techniques	47
Tips on Definitions	56
6 Sets	59
Spotlight: Paradoxes	67
7 Operations on Sets	73
8 More on Operations on Sets	81
9 The Power Set and the Cartesian Product	89
Tips on Writing Mathematics	98
10 Relations	101
Tips on Reading Mathematics	110
11 Partitions	111
Tips on Putting It All Together	119
12 Order in the Reals	121

13 Consequences of the Completeness of \mathbb{R} 133
 Tips: You Solved It. Now What? 140

14 Functions, Domain, and Range 143
 Spotlight: The Definition of Function 151

15 Functions, One-to-One, and Onto 157

16 Inverses 167

17 Images and Inverse Images 181
 Spotlight: Minimum or Infimum? 187

18 Mathematical Induction 193

19 Sequences 209

20 Convergence of Sequences of Real Numbers 223

21 Equivalent Sets 235

22 Finite Sets and an Infinite Set 243

23 Countable and Uncountable Sets 251

24 The Cantor–Schröder–Bernstein Theorem 261
 Spotlight: The Continuum Hypothesis 270

25 Metric Spaces 277

26 Getting to Know Open and Closed Sets 289

27 Modular Arithmetic 301

28 Fermat’s Little Theorem 315
 Spotlight: Public and Secret Research 320

29 Projects 325
 Tips on Talking about Mathematics 325
 29.1 Picture Proofs 327
 29.2 The Best Number of All (and Some Other Pretty Good Ones). 330
 29.3 Set Constructions 332
 29.4 Rational and Irrational Numbers 334
 29.5 Irrationality of e and π 336
 29.6 A Complex Project 338
 29.7 When Does $f^{-1} = 1/f$? 342
 29.8 Pascal’s Triangle 343
 29.9 The Cantor Set 346

29.10 The Cauchy–Bunyakovsky–Schwarz Inequality	349
29.11 Algebraic Numbers	351
29.12 The Axiom of Choice	353
29.13 The RSA Code	357
Spotlight: Hilbert’s Seventh Problem	359
Appendix	363
Algebraic Properties of \mathbb{R}	363
Order Properties of \mathbb{R}	364
Axioms of Set Theory	364
Pólya’s List	366
References	367
Index	371

Chapter 1

The How, When, and Why of Mathematics

What is mathematics? Many people think of mathematics (incorrectly) as addition, subtraction, multiplication, and division of numbers. Those with more mathematical training may think of it as dealing with algorithms. But most professional mathematicians think of it as much more than that. While we certainly hope that our students will perform algorithms correctly, what we really want is for them to understand three things: how you do something, why it works, and when it works. The problems we present to you in this book concentrate on these three goals. If this is the first time you have been asked to prove theorems, you may find this to be quite a challenge. Not only will you be learning how to solve the problem, you will also be learning how to write up the solution. The necessary definitions and background to understand a problem, as well as a general plan of attack, will always be presented in the text. It's up to you to spend the time reading, trying various approaches, rereading, and reapproaching. You will probably be spending more time on fewer exercises than you ever have before. While you are now beyond the stage of being given steps to follow and practice, there are general rules that can assist you in your transition to doing higher mathematics. Many people have written about this subject before. The classic text on how to approach a problem is a wonderful book called *How to Solve It* by George Pólya, [84].

In his text, Pólya gives a list of guidelines for solving mathematical problems. He calls his suggestions “the list.” We have included the original in the Appendix on page 366. This list has served as a guide for several generations of mathematicians, and we suggest that you let it guide you as well. Here's a closer look at “the list” with some 21st-century modifications.

First. “Understanding the problem.” Easier said than done, of course. What should you do? Make sure you know what all the words mean. You may need to look something up in this book, or you may need to use another book. Look at the statement to figure out carefully what you are given and what you are supposed to figure out. If a picture will help, draw it. Will you be proving something? What? Will you have to obtain an example? Of what? Check all conditions. Will you have to show that something is false? Once you understand what you have to do, you can move on to the next step.

Second. "Devising a plan." How will you attack the problem? At this point, you understand what must be done (because you have completed Step 1). Have you seen something like it before? If you haven't looked over class notes, haven't read the text, or haven't done the previous homework assignments, the odds are slim that you have seen anything that will be helpful. Do all that first. Look over the text with the problem in mind, read over your notes with the problem in your head, look at previous exercises and theorems that sound similar. Maybe you can use some of the ideas in the proof of a theorem, or maybe you can use a previous homework problem. Mathematics builds on itself and the problems in the text will also. If you are truly stuck, try to answer a simpler, similar question. Once you decide on a method of approach, try it out.

Third. "Carrying out the plan." Solve the problem. Look at your solution. Is each sentence true? Sometimes it is difficult to catch an error right after you have "found a solution." Put the problem down and come back to it a few hours later. Is each sentence still true?

Fourth. "Looking back." Pólya suggests checking the result and the argument, or even looking for a different proof. If you are allowed (check with your teacher), one really good way to check a proof is to give it to someone else. You can present it to friends. Even if they don't understand a word you are saying, sometimes saying it out loud in a coherent manner will allow you to recognize an error you can't spot when you are reading. If you are permitted to work together, switch proofs and ask your partner for criticism of your proof.

When you are convinced that your argument is correct, it is time to write up a correct and neat solution to the problem.

Here is an example of the Pólya method at work in mathematics; we will decipher a message. A cipher is a system that is used to hide the meaning of a message by replacing the letters of the alphabet by other letters or symbols.

Exercise 1.1. The following message is encoded by a shift of the alphabet; that is, every letter is replaced by another one that has been shifted n places further down the alphabet. Once we reach the end of the alphabet, we start over. For instance, if n were 7, we would make the replacements $a \rightarrow h$, $b \rightarrow i$, \dots , $s \rightarrow z$, $t \rightarrow a$, \dots . Now the exercise: What does the message below say?

PDEO AJYKZEJC WHCKNEPDI EO YWHHAZ W YWAOWN YELDAN.
EP EO RANU AWOU PK XNAWG, NECDP?

Let's use the ideas from Pólya's list to solve this. If you have solved problems like this before, it might be a better exercise for you to try on your own to see how this fits Pólya's method before you read on.

1. *"Understanding the problem."* Each sequence of letters with no blank space between the letters represents one word. Each letter is shifted by the same number of places: namely, n . So n is the unknown in this problem and it is what we need to find. Once we know the value of n , we can decipher the whole message. In addition, once we know the meaning of one letter, we can find the value for n .

2. “*Devising a plan.*” A cipher text may have weak points. What are these? How about the short words? Looking at the short words, in some sense, substitutes an easier problem for the one we have.
3. “*Carrying out the plan.*” The short words are:

W;
 EO (which appears twice);
 EP;
 PK.

Try using the most common one- and two-letter words. For each guess, check the beginning of the cipher text to see if it makes sense. It shouldn’t take long for you to come up with the message.

4. “*Looking back.*” If your solution makes sense, then it is highly unlikely that a different replacement is also possible. So the solution is (with high probability) the only one.

Would there have been other solution methods? Sure. For instance, not all letters have the same frequency in the English language. One analysis of English texts showed the letter e occurring most frequently, followed by (in this order) t, a, o, i, n, s, h, and r. (See [99, p. 19].) We could have used this information to guess the assignment of letters.

We also could have simply tried one value of n after another until the message made sense.

Have you now solved the problem? If you know what the message says, then the answer to this question is *yes*. Are you done? Unless you solved the problem and wrote up a clear, complete solution, the answer to this second question is *no*. A solution consists of a report that tells the reader how you solved the problem and what the answer is. This needs to be done in clear English sentences. As you write up your solution, try to keep the reader in mind. You should explain things clearly and logically, so that the reader doesn’t have to spend time filling in gaps. ○

We now move on to a very different kind of example. Consider the set of points in three-space. In case you haven’t seen this before, these points are easily described. We take the familiar xy -plane, and place it parallel to the floor. The z -axis is the vertical line perpendicular to the xy -plane and passing through the origin of the xy -plane (see [Figure 1.1](#)). We’ll review the important concepts before we begin our example.

To locate a point, we will give three coordinates. The first coordinate is the x -coordinate and tells us the number of units to walk in the x -direction. The second is the y -coordinate, telling us how to move in the y -direction, and the third is the z -coordinate, telling us how far, up or down, to move. So a point in three-space is denoted by (x, y, z) . It is important to make sure you understand this. Try to think of how you would plot points. The point $(1, 0, 0)$ (plotted in [Figure 1.2](#)) would appear one unit in the positive direction on the x -axis (since it doesn’t move in the y -direction or z -direction at all). The point $(-1, 1, 0)$ would appear in the xy -plane,

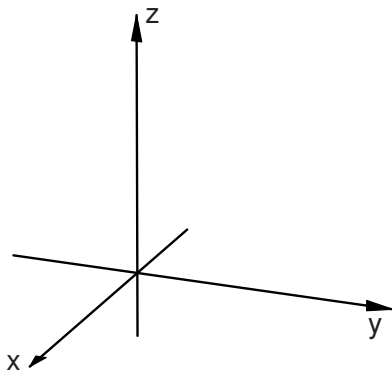


Fig. 1.1

one unit back on the x -axis and one unit in the positive y -direction. Finally the point $(2, -1, 3)$ is plotted in [Figure 1.2](#).

Let's go a bit further here. In two-space, what was $x = 0$? Since y does not appear in that equation, it is unrestricted and can be any real number. That's why $x = 0$ in two-space is the y -axis. What is $x = 3$? It is a line parallel to the y -axis through the point $(3, 0)$. So, let's try to generalize this to the situation in three-space. What's the plane $z = 0$? Recall that if a variable doesn't appear, then it may assume any value. So this means that z is fixed at 0 while x can take any value, as can y . Thus, the plane $z = 0$ is the xy -plane. Similarly, the yz -plane is the plane $x = 0$ and the xz -plane is the plane $y = 0$. These three planes are called the coordinate planes. What's the plane $z = 3$? $x = 2$? $y = y_0$? There's plenty to think about here, but let's start by asking what the distance is between two points in three-space.

Example 1.2. Given two points (x_0, y_0, z_0) and (x_1, y_1, z_1) in three-space, what is the distance between the two points?

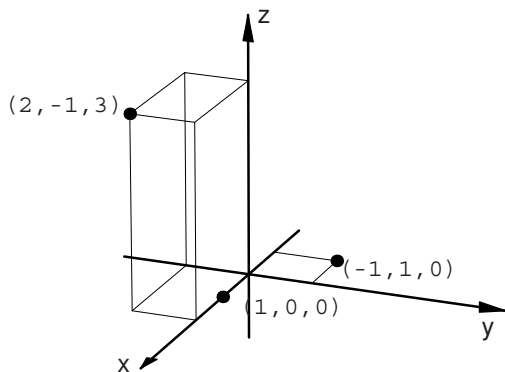


Fig. 1.2

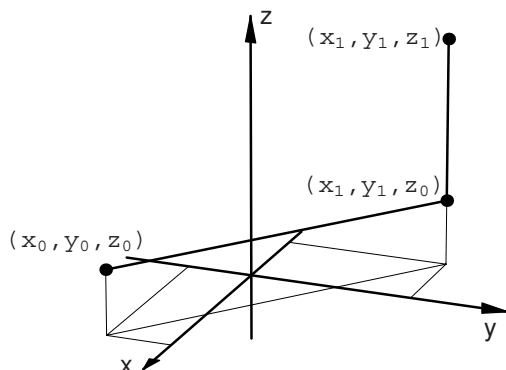


Fig. 1.3

We follow Pólya’s method to find the solution.

1. *“Understanding the problem.”* Before we begin, we make sure we really understand the meaning of each word and symbol above. We spent the last few paragraphs making sure we all understand the symbols, and all the words are familiar ones that appear in a standard English dictionary. But, wait—has “distance between two points” really been defined? We need to be sure that everyone means the same thing by this. The distance between these two arbitrary points would mean the length of the straight line segment joining the two points. That’s what we need to find. What were we given? Two points and their coordinates.
2. *“Devising a plan.”* How do we solve something like this? We haven’t covered anything yet, so what can the authors be thinking? If you have no idea how to get started, try thinking about finding the distance between two specific points. Of course, (and this is very important) this won’t give us a general formula because it is much too specific, but maybe we’ll get some ideas.

So what’s the distance between the two points $(1, 0, 0)$ and $(-1, 0, 0)$? That question is easier to answer—it’s two. What’s the distance between $(1, 1, 0)$ and $(-1, -2, 0)$? This seems to be just the distance between two points in the familiar xy -plane. We saw a formula for that at some point. It was obtained using the Pythagorean Theorem. What was it? If you can’t recall the formula, look it up or (better, yet) try to derive it again.

Our reasoning now brings us to a simpler, similar question. As you recall, this is precisely where Pólya suggested we look for a plan. So far, it seems we can find the distance between two points as long as they lie in a plane parallel to one of the coordinate planes. But in this problem, if we look at the two points, they need not lie in such a plane. We can try to insert a third point that helps us to reduce the problem to one we can already solve. Which point? A picture will help here, so we draw one in [Figure 1.3](#).

We see that (x_0, y_0, z_0) and (x_1, y_1, z_0) lie in the plane $z = z_0$, while (x_1, y_1, z_0) and (x_1, y_1, z_1) lie on the same vertical line, in the intersection of the two planes,

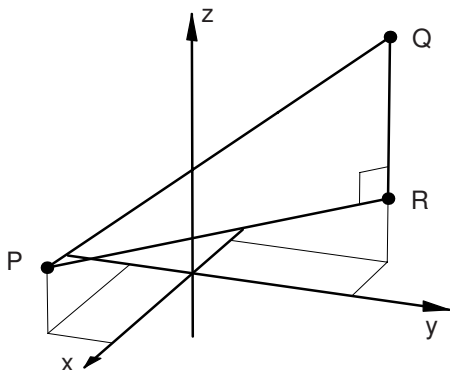


Fig. 1.4

$x = x_1$ and $y = y_1$. We “devise our plan” using these three points. Can we get the distance we are looking for from these three points? Look at Figure 1.3 and see if you can guess the rest before going on to Step 3. You probably noticed that the vertical line makes a right angle with every line in the plane $z = z_0$. This should suggest something to you—something like the Pythagorean Theorem.

3. “Carrying out the plan.” This is the only thing the reader will see. Everything that preceded this was to assist us in obtaining this solution. That means the reader doesn’t know what the points are; we have to tell him or her that. We should make sure we say why a sentence follows from the previous one and we should use equal signs between equal objects. When we think we are done, we should tell the reader that too.

Solution. Let $P = (x_0, y_0, z_0)$ and $Q = (x_1, y_1, z_1)$ be two points in space. We claim that the distance between these two points, denoted by $d(P, Q)$, is

$$d(P, Q) = \sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2 + (z_0 - z_1)^2}.$$

Proof. We introduce a third point with coordinates $R = (x_1, y_1, z_0)$. Since (x_0, y_0, z_0) and (x_1, y_1, z_0) both lie in the plane $z = z_0$, we can use the distance formula for two points in a plane to find the distance between them. Thus, the distance is given by

$$d(P, R) = \sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2}.$$

Now look at the distance between the two points (x_1, y_1, z_0) and (x_1, y_1, z_1) . Since these points lie on the same vertical line, the distance is given by

$$d(R, Q) = |z_0 - z_1|.$$

Now, the distance we are looking for is the length of the line segment PQ , which is the hypotenuse of the right triangle PQR (see Figure 1.4).

This is a right triangle, so we can obtain the length using the Pythagorean Theorem. So, we get

$$d(P, Q) = \sqrt{d(P, R)^2 + d(R, Q)^2} .$$

Substituting in what we found above, we obtain

$$d(P, Q) = \sqrt{(x_0 - x_1)^2 + (y_0 - y_1)^2 + (z_0 - z_1)^2} .$$

This completes the proof.

4. “*Looking back.*” What we have presented is our version of the proof. You may find that you need to include more details. By all means, go ahead. If you had to stop and say, “where did that come from?” make sure you answer yourself. Write it in the text (you aren’t going to sell this book back anyway, right?), or keep a notebook of “proofs with commentary.” Note that though we used pictures to illustrate the ideas in our argument, a picture will not, in general, substitute for a proof. However, it can really clarify an idea. Don’t rely on a picture, but don’t be afraid to use one either. ○

Solutions to Exercises

Solution (1.1). We are given that this code was created through a shift of the alphabet. Thus once we determine one letter, the other letters are easily found. Since we have a one-letter word, we’ll start with it. Thus “W” must represent the letter “I” or the letter “A.” Checking both shifts of the alphabet

$$(W \rightarrow I, X \rightarrow J, Y \rightarrow K, Z \rightarrow L, A \rightarrow M, B \rightarrow N, C \rightarrow O, \text{ etc.})$$

$$(W \rightarrow A, X \rightarrow B, Y \rightarrow C, Z \rightarrow D, A \rightarrow E, B \rightarrow F, C \rightarrow G, \text{ etc.})$$

we find that if “W” represents the letter “I,” then “E” must represent the letter “Q.” The fact that “EO” appears as a word and “O” would represent the letter “A” in our coded text implies that “EO” would be the word “QA,” which is an interesting combination of letters, but hardly a word. Thus, “W” cannot represent the letter “I” and therefore “W” represents “A.”

Using the shift described above and replacing the corresponding letters, we find that the code says the following.

“THIS ENCODING ALGORITHM IS CALLED A CAESAR CIPHER. IT IS VERY EASY TO BREAK, RIGHT?”

In fact, the Caesar cipher is quite easy to break. If this interests you, a very readable history of coding theory is presented by S. Singh in *The Code Book*, [99].

Spotlight: George Pólya

György Pólya (1887–1985), referred to as George Pólya in his later years, was born and raised in Hungary. He studied in Vienna and in Budapest, where he received his doctorate in 1912. One of his influential teachers was Leopold Fejér. In his book [85, p. 39], Pólya refers to Fejér as “an inspiring teacher who had a great deal of influence on Hungarian mathematicians of the time.” The two primary places where Pólya taught were the Eidgenössische Technische Hochschule (ETH) in Zürich, Switzerland, and Stanford University in Palo Alto, California.

Though Pólya’s mother tongue was Hungarian, he worked in the Swiss-German-speaking part of Switzerland and he spoke French with his wife from Neuchâtel, a city in the French-speaking part of Switzerland. In school he also learned Latin and Greek. (See [85, p. 11].) Pólya later emigrated to the United States where he taught and lectured in English. He published mathematical papers in Hungarian, German, French, English, Italian, and Danish.

Pólya contributed to original research in probability, geometry, number theory, real and complex analysis, graph theory, combinatorics, and mathematical physics. His name is connected to many mathematical ideas and constructions. To name just a few of his achievements, we mention that in probability there is a Pólya distribution and he is credited with introducing the idea and the term of “random walk.” But Pólya was not only recognized as an excellent scholar of mathematics, he was also an excellent teacher of mathematics. His heuristic approach to problem solving is outlined in *How to Solve It*. This book had a profound influence on the teaching of mathematics. It has sold over one million copies and is translated into over 20 languages. Records kept by the ETH in Zürich show that Pólya was the advisor of 14 thesis students there and, according to [78], he was the advisor of 9 more students at Stanford.

The Mathematical Association of America (MAA) gives an annual Pólya award. According to the MAA website, “This award, established in 1976, is named after the renowned teacher and writer, and is given for articles of expository excellence published in the *College Mathematics Journal*.”

To learn more about George Pólya and his approach to problem solving, we recommend reading his book *How to Solve It*, [84], the picture book [85] (which contains a short biography), or consulting the more in-depth account of Pólya’s life [4], written by his former student at Stanford. The article [110] is based on interviews with Pólya and appeared in an issue of *Mathematics Magazine* entirely devoted to Pólya and his work.

Problems

Problem 1.1. Here is a problem intended to help you work through “the list.” After this, you are on your own.

Find a word (written in standard capital letters) that is unchanged when reflected in a horizontal line and in a vertical line. The word must appear in a dictionary (in a language of your choice) in order to be a valid solution.

1. “*Understanding the problem.*” We need to find a word. We are given information about the letters that make up this word. There are two conditions: Two different reflections should not alter the word.
Try these two reflections on a word, say on SOLUTION, to make sure you understand the problem.
2. “*Devising a plan.*” We have to find the connection between what we are given and what we have to find.
Which letters of the alphabet satisfy each of the two conditions?
Both conditions?
Find a word that is not changed if it is reflected in a horizontal line.
Find a word that is not changed if it is reflected in a vertical line.
Formulate the exact conditions for this exercise; that is, state the letters that can be used and how they must be arranged.
3. “*Carrying out the plan.*” Find a word that satisfies the conditions given above.
4. “*Looking back.*” Are there other solutions?

Problem 1.2. Find a word (written in standard capital letters) that reads the same forward and backward and is still the same forward and backward when rotated around its center 180° . Your solution needs to appear in a standard dictionary of some language.

Problem 1.3. Solve the following anagrams. The first three are places (in the geographical sense), and the fourth is a place in which you might live. All can be rearranged to form a single word.

- (a) NOVA CURVE;
- (b) NINE SLAP NAVY;
- (c) I HELD A HIP PAL;
- (d) DIRTY ROOM.

Note: You may have to find out exactly what an anagram is. This is part of Pólya’s first point on the list.

Problem 1.4. Suppose n teams play in a single game elimination tournament. How many games are played?

An example of such tournaments are the various categories of the U. S. Open tennis tournament; for example, women’s singles.

Note: Pay special attention to the first entry of Pólya’s list: “Is it possible to satisfy the condition?”

Problem 1.5. Suppose you are all alone in a strange house. There are seven identical closed doors. The bathroom is behind exactly one of them. Is it more likely, less likely, or equally likely that you find the bathroom on the first try than on the third try? Why?

Problem 1.6. The following message is encoded using a shifted alphabet just as in Exercise 1.1. (Of course, the shift number n is not the same as in the exercise!) What does the message say?

RDSXCVIWT DGNXH UJCLTLXAAATPGCB DGT PQDJIXIAPITG

Problem 1.7. Give a detailed description of all points in three-space that are equidistant from the x -axis and the yz -plane. Once you decide on the answer, write the solution up carefully. Pay particular attention to your notation.

Problem 1.8. The following is a classic problem in mathematics. Though there are many variations of this problem, the standard one is the following.

You are given 12 coins that appear to be identical. However, one of the coins is counterfeit, and the weight of this coin is slightly different than that of the other 11. Using only a two-pan balance, what is the smallest number of weighings you would need to find the counterfeit coin? (Think about a simpler, similar problem.)

(See I. Peterson's website [82] for a discussion of this problem.)

Problem 1.9. Let n be an odd integer. Prove that $n^3 - n$ is divisible by 24.

The following two problems are only appropriate if you took at least two semesters of calculus. Though you may have worked these before, the idea is to work them again paying close attention to the final presentation. Make sure you define all variables. Use complete sentences, with proper punctuation.

Problem 1.10. Find the volume of a spherical cap if the height is 2 m and the radius of the rim of the cap is 5 m.

Problem 1.11. We have two circular right cylinders of radius 1 each. The axes of the two cylinders intersect at a right angle. Find the volume of the solid that both cylinders have in common.

Problem 1.12. Shlomo Sureshot started the basketball season with a free throw shooting percentage of below 75%. By the end of the season he brought it up to above 75%. Must there have been a time in the season (after a free throw attempt) when his free throw percentage was exactly 75%?

After having solved this problem and looking back at your solution, are there questions that you would like to answer? Can you answer them?

Problem 1.13. An old Spanish treasure is hidden away in a magical box with integer dimensions; that is, height, width, and length are all of integer values if measured in "braza," a unit of length. The volume of the box is 40 braza^3 . Though knowing the sum of the dimensions will not completely determine them, knowing (in addition) that the square front face is painted red will. What are the dimensions of the box?

Tips on Doing Homework

Your instructor will probably ask you to work many of the exercises and problems in this text. If there is one thing mathematicians agree on, it is that you learn mathematics by doing it. Here are some tips on how to get started.

- Make sure you know what the rules are. Some instructors do not want you to get help from someone else. Other instructors encourage working together in groups. Ask, if you are not clear about the policy.
- If you are permitted to work together, form a study group. A small group of two to four people usually works best. Get together on a regular basis and discuss the assigned problems.
- Read the questions carefully. If there is a term that you do not know, look it up.
- Before you get started, read over the text and the notes from class, paying particular attention to definitions, theorems, and previous exercises. It isn't unusual to spend several hours on a single problem at this point. Doing mathematics means pondering a problem for hours, days, weeks, even years (though we have tried not to pose problems that will take you years to solve). Working two hours on one problem, thinking about it as you go through your day and then spending another two hours on it the next day is fairly common practice for students at this level.
- Once you have read over the text, looked over the relevant definitions, worked through the examples, and tried to solve the problem, you will be well on your way toward understanding the problem. If you can't get started, at least you will know which questions to ask. Seek help from your instructor or other students (if your instructor allows this).
- Once you have a solution to a problem, look at it critically. Check that it is correct. Put it down. Come back to it later. Do you still understand everything? Is it still correct? (As you can imagine, this is very important.) Can you simplify it? If you work with someone else, have them read it over. *Never hand in your first draft of a solution to a problem.*
- Writing a solution means convincing a reader that the result is correct. There can be *no* gaps or errors. Explain each step—don't assume that the reader knows what you are thinking. Keep a reader in mind as you write, and remember that the instructor or anyone else who already knows the solution is *not* really your target audience. Though that may be the person for whom the solution is intended, it is your job to convince the reader that each step in your solution is correct. Perhaps a better audience to keep in mind is someone who knows the material from the class, but not the solution to the problem.
- Write up your final solution very carefully and neatly. The reader shouldn't find him- or herself proving things for you—you should do that for him or her. Staple pages together so that the reader may have the pleasure of reading your proof in the correct order and its entirety.

Chapter 2

Logically Speaking

“I know what you’re thinking about,” said Tweedledum; “but it isn’t so, nohow.” “Contrariwise,” continued Tweedledee, “if it was so, it might be; and if it were so, it would be; but as it isn’t, it ain’t. That’s logic.”—Lewis Carroll, [17, p. 139]

Suppose your friend tells you that Mr. Hamburger is German or Swiss. You happen to know that Mr. Hamburger is not Swiss. Using your powers of reasoning, you decide that Mr. Hamburger is German. Note that this argument can be generalized, because it doesn’t really depend on Mr. Hamburger being Swiss or German. If your friend said that “A or B is true” and you happened to know that “B is not true,” you would conclude that “A is true.” This is an example of a valid argument. Now suppose your friend tells you that Mr. French eats only pickles on Wednesday, and only chocolate on Monday. You know that Mr. French is eating chocolate that day. Now what can you say? While you may conclude that Mr. French has odd eating habits, you would not have used a logically valid argument to do so. In this example, there is really only one thing you can conclude. We’ll return to this at the end of this chapter.

In order to understand an argument, we must be able to read and comprehend the sentences that compose it. We need to be able to tell whether the sentences in our argument are true or false, and whether they follow logically from the previous ones. So now for a definition. A statement is a sentence that is true or false, but not both. “Two is not a prime number” is an example of a (false) statement. “Do you love me?” is not a statement. Below are some examples and some nonexamples of statements. These will be your first examples of nonexamples.

Exercise 2.1. Which of the sentences below are statements and which are not?

- (a) It is raining outside.
- (b) The professor of this class is a woman.
- (c) Two plus two is five.
- (d) $X + 6 = 0$.
- (e) Seven is a prime number.
- (f) All odd numbers are prime.

(g) This sentence is false.

○

Because English usage and mathematical usage may differ slightly, we must be certain that we understand our statements before we construct arguments. We now carefully study the truth or falsity of statements. Our treatment is brief. (See [69] for a more detailed study of mathematical logic.)

The rules of logic that we present in this chapter should work for all statements, and not just particular ones. For this reason, we introduce letters such as $P, Q, R,$ or S to represent statements. Thus P will have two possible truth values: true, denoted T , or false, denoted F . We can negate P or combine it with Q by saying things like:

Not P .

P and Q .

P or Q .

If P , then Q .

P if and only if Q .

Such symbolic sentences will be called statement forms. A precise definition of statement form will be given once we have precise definitions of the connectives “not,” “and,” “or,” “if . . . , then . . . ,” and “if and only if.”

In the English language we might say

It is raining.

It is not raining.

If it is raining, the sky is gray.

It is raining or it is snowing.

It is cold and it is snowing.

It is snowing if and only if it is cold.

Let’s start with the simplest case. Suppose your teacher says, “This book has a blue cover.” Taking a quick glance at the cover, you can decide on the truth value of that statement; namely, that it is false. In order to have a true statement, you could say, “This book does not have a blue cover.” If we have a statement form P , the negation of P is the statement form “not P .” Under what circumstances should the negation of P be true or false? We will always use the notation $\neg P$ for “not P .” If P is true, then $\neg P$ should be false. If P is false, then $\neg P$ should be true. We can summarize all the possibilities in a truth table as follows:

P	$\neg P$
T	F
F	T

What about combining two statement forms, P and Q , into one statement form as “ P or Q ”? In this sentence, it is particularly important to distinguish between mathematical usage of the word “or” and everyday speech. For example, if we say, “You can have cake or ice cream,” it could be that you can have both. If we say, “The door is open or closed,” it cannot be that the door is both open and closed. English

statements involving the word “or” are often ambiguous; in mathematics, ambiguity is generally frowned upon. The statement form “ P or Q ” is called a disjunction and is denoted $P \vee Q$. In mathematics, a disjunction is true when P alone is true, Q alone is true, or both P and Q are true. So in mathematics, you can always have your cake and ice cream.

Exercise 2.2. Complete the truth table for $P \vee Q$.

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



The statement form “ P and Q ” is called a conjunction and is denoted $P \wedge Q$. We will have you fill in the truth table for “ P and Q ” below. It should be clear that this will be true when both P and Q are true, and false otherwise.

Exercise 2.3. Complete this truth table.

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



Now consider the statement form “If P , then Q .” This statement form is called an implication and is often stated as “ P implies Q ” and written $P \rightarrow Q$. (Note that though English usage of the word “implies” may suggest a relationship between P and Q , our analysis of truth values has assumed no connection at all between P and Q .) There are equivalent ways of stating an implication, and some will require careful thinking on the reader’s part. Remember as you read on that “If P , then Q ” may also be stated as

- Q if P .
- P is sufficient for Q (meaning P is enough to make Q happen).
- Q is necessary for P (if P happened, then Q must have happened).
- P only if Q (same as above; if P happened, then Q must have happened).
- Q whenever P .

The statement form P in each of these formulations is called the antecedent, and Q is called the conclusion. Under what conditions is an implication true? false? Let’s begin with an example you are all familiar with. Suppose we say to our son,

“If you clean your room, then you can go to Henry’s house.”

Under what conditions would he feel that we had lied? In the example, the antecedent, P , is “you clean your room.” The conclusion, Q , is “you can go to Henry’s house.” Well, if our son cleans his room and we let him go to Henry’s, everybody is happy. That implication should be true. So, if P is true and Q is true, the whole statement should be true. Also, it should be as clear to you as it will be to our son, that if he cleans his room and we do not let him go to Henry’s, we lied. So, if P is true, and Q is false, the implication should be false. Now what if he doesn’t clean his room? We never discussed this possibility. So, no matter what we decide here, we have not lied. In this situation, the statement is not false; hence we consider it to be true. So, if P is false, no matter what the truth value is of the conclusion, we will consider the implication to be true.

Summarizing this discussion, the only way that the implication “If P , then Q ” can be false is if P is true and Q is false. In the exercise below you will sum up this discussion in the form of a truth table.

Exercise 2.4. Complete this truth table.

P	Q	$P \rightarrow Q$
T	T	
T	F	
F	T	
F	F	

○

It is often helpful to rephrase a statement, making sure that you maintain the same true and false values. The statement form “ P if and only if Q ” is called an equivalence, and we will write this as $P \leftrightarrow Q$. This is the same statement form as “(P only if Q) and (P if Q).” In view of the discussion above, we see that this is also $(P \rightarrow Q) \wedge (Q \rightarrow P)$. Thus the truth table for the equivalence is

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$P \leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Look down the final column and you’ll see that the equivalence is true precisely when P and Q are both true or both false.

The statement form “If P , then Q ” is also written as $P \Rightarrow Q$, and “ P if and only if Q ” might be written as $P \Leftrightarrow Q$ or “ P iff Q .”

Having studied the connectives, we are ready for our definition of a statement form. A statement form is a letter representing an unspecified statement or an expression built from such letters using connectives. Statement forms can be quite complicated. Assigning truth values to them can be done in a step-by-step fashion. The exercise below illustrates this.

Exercise 2.5. Find the truth table for the statement form

$$(P \rightarrow (\neg Q \vee R)) \wedge (R \vee Q) .$$

To solve this you must break the complicated form $(P \rightarrow (\neg Q \vee R)) \wedge (R \vee Q)$ into simpler parts. Once you have done this, you should find the truth value of each of the parts using the truth values of P , Q , and R . \circ

Now consider the two statement forms $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$. In the next exercise, you will find the truth table for each of these expressions and compare them.

Exercise 2.6. Write out the truth tables for $\neg(P \vee Q)$, $\neg P \wedge \neg Q$, and $(\neg(P \vee Q)) \leftrightarrow (\neg P \wedge \neg Q)$. What can you conclude? \circ

A statement form for which the final column in the truth table consists of all T 's is called a tautology. A statement form for which the final column is all F 's is called a contradiction. Two *statement forms*, P and Q , are said to be (logically) equivalent if $P \leftrightarrow Q$ is a tautology, and two *statements* are equivalent if they can be obtained from two equivalent statement forms by consistently replacing the letters by English statements.

In view of Exercise 2.6, we see that $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ are equivalent statement forms. Thus the statement "It is not the case that Rachel or Leah won the race" is equivalent to "Rachel did not win the race and Leah did not win the race." (Why?)

In Exercise 2.6 you noticed that the two statement forms $\neg(P \vee Q)$ and $\neg P \wedge \neg Q$ have the same truth table, and $(\neg(P \vee Q)) \leftrightarrow (\neg P \wedge \neg Q)$ is a tautology. This isn't something that happens in this one particular example. Whenever we notice that a statement is always true, we can state that fact as a theorem. Of course, we will need to give a conclusive argument for the statement's truth, and this is called a proof of the theorem. We'll present a theorem and a proof below, but remember: The statement forms, P and Q , might very well be complicated constructions with many connectives. For instance, P could be $R \rightarrow (S \vee (\neg T \wedge R))$. In fact, the theorem we present below is most interesting when P is complicated!

Theorem 2.7. *Two statement forms P and Q are equivalent if and only if they have the same truth table.*

Proof. Consider the truth table for the equivalence $P \leftrightarrow Q$:

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

We know that $P \leftrightarrow Q$ is a tautology if and only if $P \leftrightarrow Q$ has the truth value T (in the table above, this is row 1 and row 4). Finally, $P \leftrightarrow Q$ has the truth value T if and only if P and Q have the same truth value. Since P and Q are equivalent if and only if $P \leftrightarrow Q$ is a tautology, this establishes the theorem. \square

While it is very important to be able to restate something in an equivalent form, it is equally important that you be able to negate a statement. Some useful negations appear in the exercises and problems. The negation of an implication is particularly important in mathematics. If you think about integers and the sentence “If x is prime, then x is odd or $x = 2$,” you can see that even a relatively simple implication might be difficult to negate. Let’s begin with something simpler.

Exercise 2.8. Construct the truth table for $P \rightarrow Q$, and the truth table for $\neg P \vee Q$. What do you notice? Now construct a truth table for $(P \rightarrow Q) \leftrightarrow (\neg P \vee Q)$. What conclusion can you make? Finally, find an equivalent way to write $\neg(P \rightarrow Q)$. \circ

If all went well, you noticed that $P \rightarrow Q$ is equivalent to $\neg P \vee Q$, and therefore the negation of “If P , then Q ” is “ P and not Q .” Let’s return to

“If $\underbrace{x \text{ is prime}}_P$, then $\underbrace{x \text{ is odd or } x = 2}_Q$.”

Negating this leads to

“ $\underbrace{x \text{ is prime}}_P$ and it is $\underbrace{\text{not the case that } x \text{ is odd or } x = 2}_{\neg Q}$.”

While this is the negation, it isn’t really as helpful as it might be. So we now negate the disjunction “ x is odd or $x = 2$ ” and combine it with our previous work to obtain

“ x is prime and x is not odd and $x \neq 2$.”

Refining this further, we would probably say something like “ x is prime, even, and not equal to two.”

The negation of an implication is something you should learn well now because it arises frequently. In the theorem below, we summarize the five most important equivalences that we have covered so far. The first two are often referred to as DeMorgan’s laws.

Theorem 2.9. Let P and Q denote statement forms. The following are tautologies:

$$\begin{aligned} \text{(DeMorgan's laws)} \quad & \neg(P \vee Q) \leftrightarrow (\neg P \wedge \neg Q); \\ & \neg(P \wedge Q) \leftrightarrow (\neg P \vee \neg Q); \end{aligned}$$

$$\begin{aligned} \text{(Implication and its negation)} \quad & (P \rightarrow Q) \leftrightarrow (\neg P \vee Q); \\ & \neg(P \rightarrow Q) \leftrightarrow (P \wedge \neg Q); \end{aligned}$$

$$\text{(Double negation)} \quad \neg(\neg P) \leftrightarrow P.$$

Proof. In Exercise 2.6 we showed that the first tautology holds. You will establish the second in Problem 2.3. The third and fourth tautologies were the content of Exercise 2.8. Finally, you will establish the last tautology when you work Problem 2.2. \square

Here are some examples for you to try.

Exercise 2.10. Negate the following. It’s interesting to note that you can negate a statement even if you don’t understand what it says. It is easier to get it right, though, if you understand the statement.

- (a) If I go to the party, then he is there.
- (b) If x is even, then x is divisible by 2.
- (c) If a function is differentiable, then it is continuous.
- (d) If x is a natural number, then x is even or x is odd. ○

Exercise 2.11. Which of the following are equivalent to each other? All the answers have appeared in this chapter.

$$P \rightarrow Q, \neg(P \vee Q), \neg(P \wedge Q), P \wedge \neg Q, \neg(P \rightarrow Q),$$

$$P \vee \neg Q, \neg P \vee \neg Q, \neg P \wedge \neg Q, \neg P \vee Q. \quad \text{○}$$

So let’s apply what we have learned in this chapter to Mr. French, who eats only pickles on Wednesday and only chocolate on Monday. One statement is that “if it is Wednesday, then Mr. French eats only pickles.” We let W represent the statement “it is Wednesday,” and P the statement “Mr. French eats only pickles.” Thus, we know that $W \rightarrow P$ is true. (If you thought we should have said $W \wedge P$ is true, note that we do not know that the statement W is true, so we must use the implication here.) The second is “if it is Monday, then Mr. French eats only chocolate.” Letting M denote “it is Monday” and C the statement that “Mr. French eats only chocolate” we may write what we are given as $M \rightarrow C$. Finally we are told that “Mr. French is eating chocolate.” From this we can conclude that $\neg P$ is true. Let’s put this together.

1. $W \rightarrow P$,
2. $M \rightarrow C$, and
3. $\neg P$.

Now, it’s fairly clear that the second statement is irrelevant. So let us look at the truth tables for the first and third statements (for convenience, we combine the two tables):

W	P	$W \rightarrow P$	$\neg P$
<i>T</i>	<i>T</i>	<i>T</i>	<i>F</i>
<i>T</i>	<i>F</i>	<i>F</i>	<i>T</i>
<i>F</i>	<i>T</i>	<i>T</i>	<i>F</i>
F	F	T	T

We know that both $W \rightarrow P$ and $\neg P$ are true, and from our truth table we see that there is only one time that this happens: when both W and P are false. So there you have it. All we can conclude is that it is not Wednesday.

People differ in their approaches to problems. In the example above, you might have found it easier not to rewrite the problem. That’s fine. On the other hand, when

a problem starts to confuse you, looking at it as we have here will often help you figure out how to attack a problem.

Solutions to Exercises

Solution (2.1). All sentences are statements except (d) and (g).

Part (d) is not a statement because its truth depends on X , and X is a variable. So the sentence is sometimes true and sometimes false.

Part (g) is tricky. Suppose it were a statement. Then it would have to be true or false, but not both. Suppose “This sentence is false” were true. Then it would have to be false, but it cannot be both true and false. From this we conclude that the sentence has to be false. But reading the sentence tells us that if it is false, it must again be true as well. We conclude that it cannot be a statement, because we cannot assign a unique truth value to it.

Solution (2.2). The truth table for $P \vee Q$ is

P	Q	$P \vee Q$
<i>T</i>	<i>T</i>	<i>T</i>
<i>T</i>	<i>F</i>	<i>T</i>
<i>F</i>	<i>T</i>	<i>T</i>
<i>F</i>	<i>F</i>	<i>F</i>

Solution (2.3). The truth table for $P \wedge Q$ is

P	Q	$P \wedge Q$
<i>T</i>	<i>T</i>	<i>T</i>
<i>T</i>	<i>F</i>	<i>F</i>
<i>F</i>	<i>T</i>	<i>F</i>
<i>F</i>	<i>F</i>	<i>F</i>

Solution (2.4). The truth table for $P \rightarrow Q$ is

P	Q	$P \rightarrow Q$
<i>T</i>	<i>T</i>	<i>T</i>
<i>T</i>	<i>F</i>	<i>F</i>
<i>F</i>	<i>T</i>	<i>T</i>
<i>F</i>	<i>F</i>	<i>T</i>

This is the same as the truth table for $\neg P \vee Q$.

Solution (2.5). We will break the problem into parts in such a way that at each step we apply only one additional connective (except for the negation, which is handled easily in general).

P	Q	R	$\neg Q \vee R$	$P \rightarrow (\neg Q \vee R)$	$R \vee Q$	$(P \rightarrow (\neg Q \vee R)) \wedge (R \vee Q)$
T	T	T	T	T	T	T
T	T	F	F	F	T	F
T	F	T	T	T	T	T
T	F	F	T	T	F	F
F	T	T	T	T	T	T
F	T	F	F	T	T	T
F	F	T	T	T	T	T
F	F	F	T	T	F	F

Solution (2.6). We note that the last statement form is always true. (Note that the first and second statement forms have the same truth table.)

Solution (2.8). In the solution to Exercise 2.4, we noted that $P \rightarrow Q$ and $\neg P \vee Q$ are equivalent. Thus $\neg(P \rightarrow Q)$ is equivalent to $\neg(\neg P \vee Q)$, which is, as we have seen in Exercise 2.6, equivalent to $P \wedge \neg Q$. In words, the negation of “If P , then Q ” is “ P and not Q .”

Solution (2.10). More than one answer is possible but they must be equivalent, of course.

- (a) I go to the party and he is not there.
- (b) One answer is: x is even and x is not divisible by 2.
- (c) A function is differentiable and it is not continuous.
- (d) One answer is: x is a natural number and x is not even and x is not odd.
Equivalently, we could say: x is a natural number, and x is neither even nor odd.

Problems

Problem 2.1. In the following implications, identify the antecedent and the conclusion. (Don’t worry about whether the implication is true or false.)

- (a) If it is raining, I will stay home.
- (b) I wake up if the baby cries.
- (c) I wake up only if the fire alarm goes off.
- (d) If x is odd, then x is prime.
- (e) The number x is prime only if x is odd.
- (f) You can come to the party only if you have an invitation.
- (g) Whenever the bell rings, I leave the house.

Problem# 2.2. Construct a truth table for $\neg(\neg P)$. Is this what you expect? Why?

Problem# 2.3. Write out the truth tables for $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$. What can you conclude?

Problem# 2.4. Find a statement form, S , equivalent to $\neg(P \vee Q)$ and show that it is logically equivalent by constructing the truth table for “ S if and only if $\neg(P \vee Q)$ ” and showing that this statement form is a tautology.

Problem 2.5. Write out the truth table for the statement form $P \rightarrow \neg(Q \wedge \neg P)$. Is this statement form a tautology, a contradiction, or neither?

Problem 2.6. Write out the truth table for the statement form $(P \rightarrow (\neg R \vee Q)) \wedge R$. Is this statement form a tautology, a contradiction, or neither?

Problem 2.7. Negate the sentences below and express the answer in a sentence that is as simple as possible.

- (a) I will do my homework and I will pass this class.
- (b) Seven is an integer and seven is even.
- (c) If T is continuous, then T is bounded.
- (d) I can eat dinner or go to the show.
- (e) If x is odd, then x is prime.
- (f) The number x is prime only if x is odd.

Problem 2.8. Negate the following.

- (a) If I am not home, then Sam will answer the phone and he will tell you how to reach me.
- (b) If the stars are green or the white horse is shining, then the world is eleven feet wide.
- (c) If we go swimming or bowling, then dinner will be late or Bob will bring veggie burgers.

Problem 2.9. Consider the statement form $(P \wedge \neg Q) \rightarrow R$.

- (a) Find the truth table for this statement form.
- (b) Construct a different statement form using P , Q , and R such that if you call your construction S , then $((P \wedge \neg Q) \rightarrow R) \leftrightarrow S$ is a tautology.

Problem 2.10. Consider the statement form $(P \vee \neg Q) \rightarrow (R \wedge Q)$.

- (a) Write out the truth table for this form.
- (b) Give a statement in English that is in this form.
- (c) Write the negation of your English statement, and simplify the sentence as much as possible.

Problem 2.11. For each of the cases below, write a tautology using the given statement form.

For example, if you are given $P \vee \neg Q$, you might write $(P \vee \neg Q) \leftrightarrow (Q \rightarrow P)$.

- (a) $\neg(\neg P)$;
- (b) $\neg(P \vee Q)$;
- (c) $\neg(P \wedge Q)$;

(d) $P \rightarrow Q$.

Problem 2.12. When we write, we should make certain that we say what we mean. If we write $P \wedge Q \vee R$, you may be confused, since we haven't said what to do when you are given a conjunction followed by a disjunction. Put parentheses in to create a statement form with the given truth table.

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

Problem 2.13. For each of the cases below, write a contradiction using the given statement form.

For example, if you are given $\neg(\neg P)$, you might write $\neg(\neg P) \leftrightarrow \neg P$.

- (a) $P \rightarrow Q$;
- (b) $\neg(P \vee Q)$;
- (c) $\neg P \vee \neg Q$;
- (d) $P \leftrightarrow Q$.

Problem 2.14. Consider the following statement: If f is not continuous at 1 and -1 , then the *group of invariants* is an *infinite cyclic group*, a *cyclic group of order 2*, or the *trivial group*.

You probably do not know what the words in italics mean, but you don't need to know in order to work this problem. Just think of them as describing different objects. This is an exercise in restating things you don't understand—something that might be useful in the future!

- (a) Write the form of this statement using P , Q , R , S , and T . (It's possible to use fewer variables and still have a correct solution.) Say precisely what each of your letters represent.
- (b) Write the negation of this statement in words. Use a phrase that is as simple and direct as possible.

Problem 2.15. Consider the statement “It snows or it is not sunny.”

- (a) Find a different statement that is equivalent to the given one.
- (b) Find a different statement that is equivalent to the negation of the given one.

Problem 2.16. The following problem is well known. Many different versions of this problem appear in [101].

On a certain island, each inhabitant is a truth-teller or a liar (and not both, of course). A truth-teller always tells the truth and a liar always lies. Arnie and Barnie live on the island.

- (a) Suppose Arnie says, “If I am a truth-teller, then each person living on this island is a truth-teller or a liar.” Can you say whether Arnie is a truth-teller or liar? If so, which one is he?
- (b) Suppose that Arnie had said, “If I am a truth-teller, then so is Bernie.” Can you tell what Arnie and Bernie are? If so, what are they?

Problem 2.17. Write a truth table for $(P \wedge (P \rightarrow Q)) \rightarrow Q$. What can you conclude?

Problem 2.18. Police at *Small Unnamed University* have received a report that a student was skateboarding in the hall. They rush to the scene of the crime to determine who the guilty party is, and they are met by three students: Alan, Bernard, and Charlotte. When questioned, Alan says, “If Bernard did not do it, then it was Charlotte.” Bernard says, “Alan and Charlotte did it together or Charlotte did it alone,” and Charlotte says, “We all did it together.”

- (a) If the police know that exactly one person committed the crime, and exactly one person is lying, who is the guilty party?
- (b) As it turns out, exactly one person committed the crime and all the students are lying. Who is the guilty party?

Problem 2.19. Show that if two statements, P and Q , are equivalent, then their negations, $\neg P$ and $\neg Q$, are also equivalent.

Problem 2.20. We know that each of the three statements below is correct. What can we conclude? Why?

1. If he was killed before noon, then his body temperature is at most 20°C .
2. His body temperature is at most 20°C and the police know who murdered him.
3. If the police know who murdered him, then he was killed before noon.

Problem 2.21. We have been avoiding the use of “either...or” in this text because the English language uses this construction ambiguously and the interpretation often depends on the context. Consider the following two statements:

1. “Either Peter or Paul ran in the race.”
 2. “You’re either with us or against us.”
- (a) Write the (intended) statement form for each of the two statements.
 - (b) Give two more examples of the use of “either A or B ” in the English language such that in the first of your examples both A and B occur, and in the second of your examples exactly one of A and B can occur.
 - (c) The symbol $\dot{\vee}$ is sometimes used for the “exclusive disjunction”; that is, a connective that yields a true statement if and only if exactly one of the two statements is true. Give an equivalent statement form of $P \dot{\vee} Q$ using only the connectives introduced earlier in this text.
 - (d) The negation “neither...nor” is interpreted exclusively as the negation of the regular disjunction in the English language. Give the truth table for the statement form “neither P nor Q ” and give a meaningful English statement that is in this form.

Chapter 3

Introducing the Contrapositive and Converse

In the last chapter (see Theorem 2.7) we saw that two statement forms, P and Q , that have the same truth table are equivalent. This was also expressed by showing that the equivalence, $P \leftrightarrow Q$, is a tautology. When you are confronted with a mathematical statement that you need to prove, you will often find it helpful to paraphrase it. You will use tautologies to do so, since you don't want to change the truth value of your statement. Some useful tautologies appeared in Theorem 2.9. More appear below and throughout this chapter.

Theorem 3.1. *Let P, Q , and R denote statement forms. Then the following are tautologies:*

$$\begin{aligned} \text{(Distributive property)} \quad & (P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R)); \\ & (P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R)); \end{aligned}$$

$$\begin{aligned} \text{(Associative property)} \quad & (P \wedge (Q \wedge R)) \leftrightarrow ((P \wedge Q) \wedge R); \\ & (P \vee (Q \vee R)) \leftrightarrow ((P \vee Q) \vee R); \end{aligned}$$

$$\begin{aligned} \text{(Commutative property)} \quad & (P \wedge Q) \leftrightarrow (Q \wedge P); \\ & (P \vee Q) \leftrightarrow (Q \vee P). \end{aligned}$$

At this point, you should be able to construct the truth tables for everything above and you should be able to show that all of them are tautologies.

Exercise 3.2. Negate the following:

- (a) $(P \wedge Q) \vee (P \wedge R)$;
- (b) $P \rightarrow (Q \wedge R)$.

○

Tautologies allow us to replace one statement by another. For example, suppose you want to show that an integer is odd or prime. You can show that the integer is prime or odd; that won't change things because these two statements are equivalent.

This is a fairly obvious change that usually won't make much of a difference. The same holds if you want to show x is prime and odd; you can show that it is odd and prime if that's easier and you will have accomplished the same thing. Similarly, if you want to show that it is not the case that x is prime and odd, you can show that x is not prime or not odd.

For implications, restating what you want to prove can really make a difference. We need to make sure, however, that what we have is equivalent to our original statement. So recall that we showed, in the last chapter, that $P \rightarrow Q$ is equivalent to $\neg P \vee Q$.

Now consider $\neg Q \rightarrow \neg P$, which is called the **contrapositive** of the implication $P \rightarrow Q$. We need to compare the two truth tables below:

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$\neg Q \rightarrow \neg P$
T	T	T
T	F	F
F	T	T
F	F	T

So the fact that the truth tables are the same and Theorem 2.7 tell us that the statement forms are logically equivalent. What this means to us is that, if we are trying to prove that an implication is true and we don't see how to do it, we should consider the contrapositive of that statement. Here's how it works in practice.

Theorem 3.3. *Let x be an integer. If x^2 is odd, then x is odd.*

First we need to understand the problem. What does it mean for a number x to be odd? Our definition of "odd number" is the following: An **integer x is odd** if there is an integer n such that $x = 2n + 1$. So we are assuming that $x^2 = 2n + 1$ for some integer n and trying to show $x = 2m + 1$ for some integer m . It's hard to see where to go from here, we think.

Remember that Pólya suggests restating the problem, so let's try that. Let P be the sentence " x^2 is odd" and Q be the sentence " x is odd." Then we see that we wish to prove that $P \rightarrow Q$ is true. But this is logically equivalent to $\neg Q \rightarrow \neg P$, which translates into "If x is not odd, then x^2 is not odd." We can do better than that, since an integer is odd or even. So we can show that "If x is even, then x^2 is even" and that will be equivalent. Let's see if that's easier.

Theorem (Contrapositive of the statement of Theorem 3.3). *Let x be an integer. If x is even, then x^2 is even.*

The first step is to understand the problem. The second step is to prove it. We'll do that here:

"*Understanding the problem.*" When is an integer even? Our definition of "even number" is the following: An **integer x is even** if there is an integer n such that $x = 2n$. So we need to show that $x^2 = 2m$, where m is an integer, assuming that $x = 2n$, where n is an integer. We began by understanding the problem, now we are ready to solve it.

Proof. Let x be even. Then there is an integer n such that $x = 2n$. Therefore, $x^2 = (2n)^2 = 2(2n^2)$. Let $m = 2n^2$. Then $x^2 = 2m$ and m is an integer. Therefore x^2 is even. \square

Of course, this takes care of the original theorem, since it is equivalent to the one we proved. Thus, using the contrapositive is one possible way to attempt to prove that an implication is true. We will soon have a number of ways to attack a problem. Try to keep them all in mind.

Some other related remarks: Notation is more important than it may seem. In the theorem above, we assume that x is even and try to show x^2 is even. If we assume that $x = 2n$ and accidentally try to show $x^2 = 2n$ (rather than $x^2 = 2m$), we're stuck because we assumed erroneously that $x = x^2$. In other words, our notation would force us to show that $x = 0$ or $x = 1$, which is not what we should be doing. We introduced an error because of poor notation. So it's important that one symbol be an n and one be an m .

Also, note that we begin the proof by saying what we are assuming, and end the proof by saying what we are concluding. That helps the reader too. Finally, we keep checking that m and n are integers. That's because that is very important; if they weren't integers, x wouldn't have to be even.

So the contrapositive was very helpful here. You do need to be careful though. It must be the contrapositive and not the converse. The converse of an implication $P \rightarrow Q$ is the statement form $Q \rightarrow P$. Looking at the truth tables for each of these given below,

P	Q	P \rightarrow Q	and	P	Q	Q \rightarrow P
T	T	T		T	T	T
T	F	F		T	F	T
F	T	T		F	T	F
F	F	T		F	F	T

we see that they are different. Unfortunately, though the contrapositive and converse of a statement are really very different, students often confuse them. We'll take just a moment to convince you that it is very important not to do this.

Suppose our statement is, "If I am a Hobbit, then I am under 5 feet tall." This is a true statement, as every Tolkien reader knows. The converse is "If I am under 5 feet tall, then I am a Hobbit." This latter statement is not true, since lots of children are under 5 feet tall, but most of them are not Hobbits. As a mathematical example, consider the sentence about integers "If x is seven, then x is prime," and its converse "If x is prime, then x is seven." Recall that an integer p is **prime** if $p > 1$ and p cannot be written as a product of two positive integers, both different from p . Thus, the original sentence is true for all x , while the converse above is not. On the other hand, you agree that for all x the contrapositive "If x is not prime, then x is not seven," is true, as it must be. But this is trickier when we don't really understand what we are saying as well as we understand this statement. Remember, make sure you understand the problem. We present some examples and exercises for you to try your hand at.

Example 3.4. Consider the slightly odd sentence: “If the sky is green, then $2 + 2 = 4$.” What are the converse and the contrapositive of this implication? Which of the following (if any) is true: the statement, the converse, or the contrapositive?

The converse is: “If $2 + 2 = 4$, then the sky is green.” The contrapositive is: “If $2 + 2 \neq 4$, then the sky is not green.”

To decide on the validity of the statements we have to agree on the truth of each part. We are quite confident that $2 + 2 = 4$, so this part is true. We abbreviate the statement with A (for arithmetic). Since we have never seen a (natural) green sky before, we suggest that “the sky is green,” abbreviated by S , should be considered as false. With this in place, we look at the relevant parts of the truth tables.

S	A	$S \rightarrow A$	A	S	$A \rightarrow S$	$\neg A$	$\rightarrow \neg S$
F	T	T	F	F	F	T	T

So the original statement and its contrapositive are true, while the converse is false. Of course we knew beforehand that the original statement and the contrapositive would have the same answer because they are equivalent statements. ○

Now it’s your turn.

Exercise 3.5. Consider the sentence “If n is odd, then $n^2 - n - 6$ is even.”

- (a) State the contrapositive.
- (b) State the converse. ○

We should also mention one more possibility that comes up frequently: the inverse of an implication $P \rightarrow Q$ is the statement form $\neg P \rightarrow \neg Q$. As you will show in the exercise below, this form is nothing new. The inverse of an implication can be expressed in terms of our earlier definitions.

Exercise 3.6. Consider the implication $P \rightarrow Q$.

- (a) Write the truth table for the inverse of $P \rightarrow Q$.
- (b) Express the inverse of an implication in terms of the converse and contrapositive in two different ways.
- (c) State the relation between the inverse of $P \rightarrow Q$ and the converse of $P \rightarrow Q$, and give a reason for your answer. ○

Definitions

Definition 3.1. An **integer** x is **odd** if there is an integer n such that $x = 2n + 1$.

Definition 3.2. An **integer** x is **even** if there is an integer n such that $x = 2n$.

Definition 3.3. An integer p is **prime** if $p > 1$ and p cannot be written as a product of two positive integers, both different from p .

Solutions to Exercises

Solution (3.2). The equivalences are given below.

(a) The negation may be stated as $(\neg P \vee \neg Q) \wedge (\neg P \vee \neg R)$, since

$$\begin{aligned} \neg((P \wedge Q) \vee (P \wedge R)) &\leftrightarrow (\neg(P \wedge Q) \wedge \neg(P \wedge R)) \\ &\leftrightarrow ((\neg P \vee \neg Q) \wedge (\neg P \vee \neg R)). \end{aligned}$$

(b) The negation may be stated as $P \wedge (\neg Q \vee \neg R)$, since

$$\begin{aligned} \neg(P \rightarrow (Q \wedge R)) &\leftrightarrow (P \wedge \neg(Q \wedge R)) \\ &\leftrightarrow (P \wedge (\neg Q \vee \neg R)). \end{aligned}$$

Solution (3.5).

- (a) The contrapositive is “If $n^2 - n - 6$ is odd, then n is even.”
- (b) The converse is “If $n^2 - n - 6$ is even, then n is odd.”

Solution (3.6).

(a)

P	Q	$\neg P \rightarrow \neg Q$
T	T	T
T	F	T
F	T	F
F	F	T

- (b) The inverse of an implication is the converse of the contrapositive of the implication and this, in turn, is equivalent to the contrapositive of the converse of the implication.
- (c) The inverse of the implication $P \rightarrow Q$ is equivalent to the converse of the implication $P \rightarrow Q$. To see this, compare the truth table of the inverse given in (a) with the truth table of the converse from page 27. They are the same and thus, by Theorem 2.7, the inverse is equivalent to the converse.

Problems

- Problem 3.1.** (a) Write a tautology involving only logical symbols, the implication $P \rightarrow Q$, its converse, and $P \leftrightarrow Q$.
- (b) Can you write a tautology involving only $P \rightarrow Q$ and its contrapositive? If so, how? If not, why not?

Problem# 3.2. (a) Let x be an integer. Prove that if x is odd, then x^2 is odd. Make sure you state your assumption as the first line and your conclusion as the last line.

- (b) State the contrapositive of what you just proved.
- (c) Combining the result of part (a) with Theorem 3.3 gives a stronger result. Say precisely what that result is.

Problem 3.3. For each of the following, write out the contrapositive and the converse of the sentence.

- (a) If you are the President of the United States, then you live in a white house.
- (b) If you are going to bake a soufflé, then you need eggs.
- (c) If x is a real number, then x is an integer.
- (d) If x is a real number, then $x^2 < 0$.

Problem 3.4. State the contrapositive of each of the following.

- (a) If it rains, then it pours.
- (b) If I had a bell, I would ring the bell in the morning.
- (c) The house is red, if the house is not blue.
- (d) Dinner is cooked only if I make it.

Problem 3.5. State the converse of each of the following.

- (a) If it rains, then it pours.
- (b) If I am young, then I am restless.
- (c) I am alone, if it is Saturday.
- (d) I eat fish only if it is cooked.

Problem 3.6. State the inverse of each of the following.

- (a) If it rains, then it pours.
- (b) If I am living abroad, then I need brownies.
- (c) To run quickly, it is sufficient to have long legs.
- (d) To make good chocolate chip cookies, it is necessary to have baking soda.

Problem 3.7. Consider the statement form $P \rightarrow Q$.

- (a) Write the negation of the converse of this statement form in as simple a form as possible.
- (b) Write the negation of the contrapositive of this statement form in as simple a form as possible.
- (c) Write the negation of the inverse of this statement form in as simple a form as possible.

Problem 3.8. Consider the sentence: “The horses eat the grass only if they are led to the pasture.”

- (a) Write the negation of the converse of this sentence. Your answer has to be simple and as eloquent as possible.
- (b) Is the sentence in (a) the same as the converse of the negation of the original sentence? Explain your answer.

Problem 3.9. Let x and y be real numbers. Show that if $x \neq y$, then $2x + 4 \neq 2y + 4$. (Hint: Use the contrapositive.)

Problem 3.10. Matilda always eats at least one of the following for breakfast: cereal, bread, or yogurt. On Monday, she is especially picky.

If she eats cereal and bread, she also eats yogurt. If she eats bread or yogurt, she also eats cereal. She never eats both cereal and yogurt. She always eats bread or cereal.

Can you say what Matilda eats on Monday? If so, what does she eat?

Problem 3.11. Consider the following statement.

If the coat is green, then the moon is full or the cow jumps over it.

- This odd statement is composed of several substatements. Identify each substatement, assign a letter to it, and write down the original statement as a statement form using these letters and logical connectives.
- Find the contrapositive of the original statement form from part (a). Use this to write the contrapositive of the *original* statement as an English sentence.
- Find the converse of the *original* statement form from part (a). Use this to write the converse of the *original* statement as an English sentence.
- Find the negation of the *original* statement form from part (a). Use this to write the negation of the *original* statement as an English sentence.
- Are some of the statements in this problem (the original or the ones you obtained) equivalent? If so, which ones?

Problem 3.12. Consider the two statement forms $P \rightarrow Q$ and $P \rightarrow (Q \vee \neg P)$.

- Make a truth table for each of these statement forms.
- What can you conclude from your solution to part (a)?

Problem 3.13. Karl's favorite brownie recipe uses semisweet chocolate, very little flour, and less than $1/4$ cup sugar. He has four recipes: one French, one Swiss, one German, and one American. Each of the four has at least two of the qualities Karl wants in a brownie recipe. Exactly three use very little flour, exactly three use semisweet chocolate, and exactly three use less than $1/4$ cup sugar.

The Swiss and the German recipes use different kinds of chocolate. The American and the German recipes use the same amount of flour, but different kinds of chocolate. The French and the American recipes use the same amount of flour. The German and American recipes do not both use less than $1/4$ cup sugar.

Karl is very excited because one of these is his favorite recipe. Which one is it?

Problem 3.14. Let n be an integer. Prove that if $3n$ is odd, then n is odd.

Problem 3.15. Let x be a natural number. Prove that if x is odd, then $\sqrt{2x}$ is not an integer.

Problem 3.16. Let x and y be real numbers. Show that if $x \neq y$ and $x, y \geq 0$, then $x^2 \neq y^2$.

Problem 3.17. In the statement below, G is a group and H is a normal subgroup of G . (You need not know what “group,” “normal subgroup,” or “p-group” mean to do this problem!)

“If H and G/H are p-groups, then G is a p-group.”

- State the converse of this statement.
- State the contrapositive of this statement.
- Consider the following: “ G is a p-group if and only if H and G/H are p-groups.” Write this in terms of your answers to the first two parts of this problem.

Problem 3.18. Prove that if the product of two integers x and y is odd, then both integers are odd. Describe your method of proof.

Problem 3.19. Consider the statement “If Simon takes German or French, then he cannot take Russian.”

- State the contrapositive of this implication.
- State the converse of this implication.

For parts (c) and (d), assume the original statement is true.

- Suppose someone tells you that Simon did not take German. What, if anything, can you conclude about Simon? Why?
- Suppose someone tells you that Simon took French. What, if anything, can you conclude about Simon? Why?

Problem 3.20. Consider the statement form $(P \vee \neg Q) \rightarrow (R \wedge Q)$.

- Write out the truth table for this form.
- Make up a meaningful English statement that has this form.
- Write the contrapositive of your English statement. Simplify the sentence as much as you can.

Chapter 4

Set Notation and Quantifiers

Consider the sentence “The equation $x^2 + 2x = 15$ has a unique solution.” Thus far, we’ve approached such things intuitively. It’s time now to tackle this head on. Is it true? False? It depends on which x we have in mind, of course. We turn to a rigorous way to make our sentence $x^2 + 2x = 15$ into a statement. But before we get to the heart of this chapter, it will be useful to have notation for the things with which we frequently work.

We will need to understand the possible set of values that the variable x can assume. Now we will follow the point of view that many mathematicians follow: while we think of a set as a collection of objects, we will define neither set nor object. What we will do instead is to say, carefully and precisely, how these two words can be used and we do so with axiomatic statements. (The system most people use now, the Zermelo–Fraenkel system together with the axiom of choice, is stated in the Appendix for reference. We will say much more about sets in Chapter 6 and in subsequent chapters.) At this point we will concentrate on understanding the notation and commonly used symbols.

We will write $x \in X$ to indicate that x is an element of X . (Some people read $x \in X$ as “ x belongs to X ,” others read it “ x is an element of X .”) Usually we will be considering things of a particular type. The set of all possible objects that are considered in the context in which we work is called the **universe**, which is also sometimes called the *domain of discourse*. We will usually denote the universe by X . In some cases the universe may consist of all real numbers, or it may consist of all right triangles; it might even consist of all cows living in France. The set may consist of all positive real numbers, all isosceles right triangles, or all white cows living in France. And the elements might be the real number π , the isosceles right triangle with legs of length 1, or Farmer Boursin’s white cow Elsie, which lives in Dijon, France, and produces a mighty fine cheese. Some people even allow the universe to be the “set of all sets,” even though this universe is no set at all (see the Spotlight: Paradoxes on page 67).

When it is clear, implicitly, what the universe is, we may not mention it explicitly. But when there is any doubt at all, we will carefully state what the universe is. Once we do that, we can denote a set by writing $S = \{x \in X : x \text{ satisfies } P\}$. The brackets

indicate that we are talking about a set of objects, called elements; $x \in X$ tells us where these elements live, and P is a property these elements have.

In this class, as well as others, some sets show up a lot and we have special notation for them. Notation should always be chosen carefully, as these have been. Most mathematicians agree on these, so don't make up your own notation and make sure you recognize what these are when they are used:

The natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

The integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

The rational numbers $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z} \text{ and } q \neq 0\}$.

The real numbers \mathbb{R} .

The complex numbers $\mathbb{C} = \{a + bi : i^2 = -1 \text{ and } a, b \in \mathbb{R}\}$.

If A is one of the sets \mathbb{Z} , \mathbb{Q} , or \mathbb{R} , then the set of the positive elements is denoted by $A^+ = \{x \in A : x > 0\}$ and the set of the negative elements is denoted by $A^- = \{x \in A : x < 0\}$. Thus we have defined \mathbb{Z}^+ , \mathbb{Z}^- , \mathbb{Q}^+ , \mathbb{Q}^- , \mathbb{R}^+ , and \mathbb{R}^- .

The plane $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$.

For $n \in \mathbb{Z}^+$, Euclidean n -space $\mathbb{R}^n = \{(x_1, x_2, \dots, x_n) : x_j \in \mathbb{R} \text{ for } j = 1, 2, \dots, n\}$.

Some authors include zero in \mathbb{N} and others don't. If you look in another text, make sure you know what convention they follow.

For real numbers a and b with $a \leq b$, the set $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ is called the closed interval from a to b . The sets $[a, \infty) = \{x \in \mathbb{R} : a \leq x\}$ and $(-\infty, b] = \{x \in \mathbb{R} : x \leq b\}$ are called unbounded closed intervals. For $a < b$, the set $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ is called the open interval from a to b . We shall see that (a, b) can be interpreted several ways, and you should be able to decide which from the way it is used. You've done this in the past. For example, you have certainly had courses where (x, y) denotes a point and, in the same course, (x, y) might denote an open interval. Unbounded open intervals are defined, with appropriate changes, in the same way that we defined unbounded closed intervals above.

Exercise 4.1. Find a (different) useful way to describe the following sets (your useful way could be a sketch):

(a) $\{x \in \mathbb{Z} : x^2 = 1\}$;

(b) $\{x \in \mathbb{N} : x^2 = 1\}$;

(c) $\{(x, y) \in \mathbb{R}^2 : y = 0\}$;

(d) $\{(x, y, z) \in \mathbb{R}^3 : z = 0\}$;

(e) $\{x \in \mathbb{Z} : x \text{ is even}\}$;

(f) $\{(m, n) : m, n \in \mathbb{Z}\}$. ○

Now we can talk about slightly more complicated sentences. Think of the difference between the statements "In every box there is a prize" and "In some box there is a prize." Obviously, if you had to choose (and if it were the same prize), you would go with the first one. In mathematics, in order to determine the truth or

falsity of a statement, we need to know whether we are talking about a particular x or all x . What we mean should be clear from the context. Letters like x that stand for elements of the universe are called variables. The phrases “for all,” “for every,” “for some,” or “there exists,” quantify variables. “For all,” or \forall , is the universal quantifier and “there exists,” or \exists , is the existential quantifier.

After agreeing that the universe consists of all real numbers, consider the following statement: “For all x it is the case that $x^2 - 1 \leq 0$.” We know that we are asking that for every x , something must happen. It just so happens that this statement is false, but it is still a clear statement. For all x is usually written $\forall x$. So we could write

$$\forall x, x^2 - 1 \leq 0.$$

What follows the words “For all x ” in our statement is another sentence that we could denote by p , but since p is a sentence involving x , we write $p(x)$. The statement above is of the form

$$\forall x, p(x).$$

One more remark about the example above. Suppose the universe is (still) the real numbers, but we want to make this a statement about positive integers only. In that case, we can express our statement symbolically as follows:

$$\forall x, (x \in \mathbb{Z}^+ \rightarrow (x^2 - 1 \leq 0)).$$

One very common error is to write $\forall x, (x \in \mathbb{Z}^+ \wedge (x^2 - 1 \leq 0))$ rather than what we have written above. But let’s think about what this would mean: This would say that “all real numbers are positive integers and satisfy the inequality $x^2 - 1 \leq 0$.” It is probably clear now that this is not what the original statement said.

For a different example, suppose that our universe is the set of integers and consider the sentence, “There is an integer x such that $x = 0$.” This, too, is a statement, and happens to be true. This statement can be expressed symbolically by

$$\exists x, (x = 0)$$

and is read as “there exists x such that $x = 0$.” This statement is of the form

$$\exists x, p(x).$$

One more remark about the last example. If we had chosen the set of the real numbers as the universe, we would express our statement symbolically as

$$\exists x, (x \in \mathbb{Z} \wedge x = 0).$$

Note that this time we are claiming that x exists, is an integer, and $x = 0$. To make all these things happen, we must use a conjunction rather than an implication. We have included tips on quantification that we hope will be a helpful guide (see Tips on Quantification on page 45), but remember to analyze your sentences carefully before translating them into symbols.

When you negate a statement, you must be 100% clear on what your universe is. You can easily see why, too: if you negate $x \in \mathbb{Z}$ and \mathbb{Z} is your universe, then there are no x left, but if you negate $x \in \mathbb{Z}$ and \mathbb{R} is your universe, there are still plenty of x left to worry about. So make sure that you give careful consideration to your universe before beginning a problem.

Let's return to the introductory example in this chapter and apply what we have learned.

Exercise 4.2. Our sentence was “The equation $x^2 + 2x = 15$ has a unique solution.”

- Write this statement in formal language.
- Describe a universe in which this statement is true. Explain briefly why your answer is correct.
- Describe a universe in which this statement is false. Explain briefly why your answer is correct. ○

Before proceeding to negations, a little more practice with quantifiers might be helpful.

Exercise 4.3. Write the statements below in symbols, assuming that the universe is \mathbb{R} throughout. Make sure that you quantify x ; is it “all x ” or “some x ”?

- For all x , it is the case that x is an integer.
- There exists an integer x such that $x > 0$.
- There is a rational number x such that $x^2 + 1 = 0$.
- For every real number x , there exists a real number y such that $x < y$.
- There is a real number y such that $x < y$ for all x .
- If x is a rational number, then $x^2 - \pi \neq 0$.
- A real number x satisfies $x^2 > 0$, if $x \neq 0$.
- If $x > 0$, then $x > 4$ or $x < 6$. ○

We negated conjunctions, disjunctions, and implications. Now we will think about the negation of a quantified statement.

Suppose we have the statement “Every cow is black.” How would we negate it? One pretty useless way is to say “Not every cow is black.” It's better to say “Some cow is not black.” So a useful negation of

$$\forall x, p(x)$$

is

$$\exists x, \neg p(x).$$

Similarly, if we say “There exists a black cow,” a useful negation is “No cow is black.” So a negation of

$$\exists x, p(x)$$

is

$$\forall x, \neg p(x).$$

You will find that sometimes you can negate a sentence directly and other times you need to convert to symbols. Here is another example.

Example 4.4. Negate the sentence “People who live in glass houses do not throw stones.”

We will assume that the universe is the set of all people. What does this say? First, it says something about all people who live in glass houses. So we will use the quantifier “for all” and x will denote a person. The notation $g(x)$ will mean that x lives in a glass house. The notation $t(x)$ will mean that x throws stones. So our sentence becomes “For all x , if $g(x)$, then $\neg t(x)$.” If you can negate it now, go ahead. If not, go through the steps below. You should provide reasons why each step below is correct:

1. $\neg(\forall x, (g(x) \rightarrow \neg t(x)))$;
2. $\exists x, \neg(g(x) \rightarrow \neg t(x))$;
3. $\exists x, \neg(\neg g(x) \vee \neg t(x))$;
4. $\exists x, (g(x) \wedge t(x))$.

The last sentence says that the negation of “People who live in glass houses do not throw stones” is “There exists a person who lives in a glass house and throws stones.” There’s another important thing to notice here. Though there is no obvious quantifier in the sentence “People who live in glass houses do not throw stones,” we all interpret the quantifier as a universal quantifier. If you, or someone else, do not explicitly include a quantifier, (all!) people will assume you meant to insert a universal quantifier. ○

We emphasize that while it is good to practice these symbolic manipulations, it is also important to understand what you are doing. Sometimes you will find it easier to use the symbolic notation and sometimes you won’t. Make sure you keep in mind what the sentence says, and whether or not your answer seems reasonable. Before you go off on your own, we’ll do a fairly complicated example together.

Example 4.5. Suppose our universe is the set of real numbers and we wish to negate the statement “For every rational number x , there exists an integer n that is greater than x .”

So let’s try it. First we note that “For every rational number x ” means that we are being told that “if x is a rational number” something will happen. What? There will exist an integer bigger than x . So this is an implication of the form “For all x , if x is a rational number, then there exists an n such that n is an integer and $n > x$.” Sometimes it is easier to understand a statement if we replace the various subsentences with symbolic representations. We use

$p(x)$ for x is a rational number,

$q(n)$ for n is an integer, and
 $r(n, x)$ for $n > x$.

Using this notation, we have

$$\forall x, (p(x) \rightarrow \exists n, (q(n) \wedge r(n, x))).$$

Let's try to negate this quantified statement form one step at a time, starting from the outside.

We know that when we negate "for all" it becomes "there exists." In other words, we can replace $\neg(\forall x, \dots)$ with $\exists x, \neg(\dots)$. So here's where we are now:

$$\neg(\forall x, (p(x) \rightarrow \exists n, (q(n) \wedge r(n, x))))$$

is equivalent to

$$\exists x, \neg(p(x) \rightarrow \exists n, (q(n) \wedge r(n, x))).$$

Now we negate the implication. From the last chapter we know that $\neg(P \rightarrow Q)$ is equivalent to $P \wedge \neg Q$. We're up to

$$\exists x, (p(x) \wedge \neg(\exists n, (q(n) \wedge r(n, x)))).$$

We still need to negate Q , which is the expression $\exists n, (q(n) \wedge r(n, x))$. At least this is simpler than what we started with! Now \exists will change to \forall and so we need only worry about $q(n) \wedge r(n, x)$. But that's a conjunction. So the final step is to negate that, and we know the negation of the conjunction will become $\neg q(n) \vee \neg r(n, x)$. So here's where we are now:

$$\exists x, (p(x) \wedge (\forall n, (\neg q(n) \vee \neg r(n, x)))).$$

We've done what we were asked to do, in a sense, but our answer is still in symbols. Let's translate back:

"There exists an x such that x is a rational number and for all n it is the case that n is not an integer or n is not greater than x ."

Well, that's certainly a mouthful. Let's try again (explain how we get the following):

"There is a rational number x such that for all n , if n is an integer, then $n \leq x$."

And finally (explain!):

"There is a rational number x such that for all integers n , $n \leq x$." ○

Not all negations are this complicated, but even in simpler statements there are things of which you should be wary. Consider the two statements about real numbers: $\forall x, \exists y, x + y = 0$ and $\exists y, \forall x, x + y = 0$. Assuming the universe is the set of real numbers, what's the difference between these two statements? In the first, we say that for each x we can find a y with $x + y = 0$. That's a statement you have known to be true for years, ever since you learned about $-x$. On the other hand, the second

statement says that there exists a y such that for all x , we have $x + y = 0$. That statement is false, because the same y would have to work for all x . What's the moral of this story? That the order of the quantifiers is very important.

Exercise 4.6. Negate the statements (a)–(h) of Exercise 4.3. ○

In order to provide you with lots of exercises, we will discuss the contrapositive, converse, and inverse of a statement with quantifiers, such as $\forall x, r(x)$ or of $\exists x, r(x)$. We use the following rules:

Given a statement of the form $\forall x, (p(x) \rightarrow q(x))$:

the converse is $\forall x, (q(x) \rightarrow p(x))$,

the contrapositive is $\forall x, (\neg q(x) \rightarrow \neg p(x))$,

and the inverse is $\forall x, (\neg p(x) \rightarrow \neg q(x))$.

Defined this way, the contrapositive will be true precisely when the original statement is true and, as before, this will not be true of the converse or inverse. For existential quantifiers, we follow the same procedure:

Given a statement of the form $\exists x, (p(x) \rightarrow q(x))$:

the converse is $\exists x, (q(x) \rightarrow p(x))$,

the contrapositive is $\exists x, (\neg q(x) \rightarrow \neg p(x))$,

and the inverse is $\exists x, (\neg p(x) \rightarrow \neg q(x))$.

Exercise 4.7. For each of the following state the contrapositive of the statement, the converse of the statement, the negation of the contrapositive of the statement, and the negation of the converse of the statement.

(a) $\forall x, ((p(x) \wedge q(x)) \rightarrow r(x))$.

(b) (Assume the universe for this is the real numbers.) If there is a real number strictly between 50 and 100, then that number is an integer with square root less than 8. ○

Solutions to Exercises

Solution (4.1). There are many possible answers. We list some below:

(a) $\{1, -1\}$;

(b) $\{1\}$;

(c) the x -axis in \mathbb{R}^2 ;

(d) the xy -plane in \mathbb{R}^3 ;

(e) $\{2n : n \in \mathbb{Z}\} = \{\dots, -2, 0, 2, \dots\}$;

(f) the set of all points in \mathbb{R}^2 such that both the x and y coordinates are integers.

Solution (4.2). Parts (b) and (c) have alternate solutions.

- (a) $\exists x, ((x^2 + 2x = 15) \wedge \forall y, (y^2 + 2y = 15 \rightarrow y = x))$
- (b) We choose \mathbb{N} as the universe for both, x and y . The statement is true because 3 is the only natural number that solves the equation, which we leave to you to check.
- (c) Now we use \mathbb{R} as the universe for both variables. The statement is then false because 3 and -5 are two different solutions.

Some people use the symbol $\exists!$ to indicate the existence of a unique element in the universe. With that notation, part (a) reads: $\exists!x, x^2 + 2x = 15$.

Solution (4.3). Note that the universe was assumed to be \mathbb{R} .

- (a) $\forall x, x \in \mathbb{Z}$.
- (b) $\exists x, ((x \in \mathbb{Z}) \wedge (x > 0))$.
- (c) $\exists x, ((x \in \mathbb{Q}) \wedge (x^2 + 1 = 0))$.
- (d) $\forall x, \exists y, (x < y)$.
- (e) $\exists y, \forall x, (x < y)$.
- (f) $\forall x, (x \in \mathbb{Q} \rightarrow x^2 - \pi \neq 0)$.
- (g) $\forall x, (\neg(x = 0) \rightarrow x^2 > 0)$.
- (h) $\forall x, (x > 0 \rightarrow ((x > 4) \vee (x < 6)))$.

Solution (4.6). Note that the universe was assumed to be \mathbb{R} .

- (a) There exists an x such that x is not an integer.
- (b) For all x , the real number x is not an integer or x is nonpositive. This is equivalent to: For all x , if x is an integer, then x is nonpositive.
- (c) For all x , if x is a rational number, then $x^2 + 1 \neq 0$.
- (d) There exists an x such that for all y we have $x \geq y$.
- (e) For all y , there exists an x such that $x \geq y$.
- (f) There is a rational number x such that $x^2 - \pi = 0$.
- (g) For some x , we have $x \neq 0$ and $x^2 \leq 0$.
- (h) There exists a positive real number x such that $x \leq 4$ and $x \geq 6$.

Solution (4.7).

- (a) For the contrapositive: $\forall x, (\neg r(x) \rightarrow (\neg p(x) \vee \neg q(x)))$.
For the converse: $\forall x, (r(x) \rightarrow (p(x) \wedge q(x)))$.
For the negation of the contrapositive: $\exists x, (\neg r(x) \wedge p(x) \wedge q(x))$.
For the negation of the converse: $\exists x, (r(x) \wedge (\neg p(x) \vee \neg q(x)))$.
- (b) We begin by writing the statement in formal language. The universe for this problem is the set of real numbers: $\exists x, (50 < x < 100 \rightarrow (x \in \mathbb{Z} \wedge \sqrt{x} < 8))$.
Now for the contrapositive: $\exists x, ((x \notin \mathbb{Z} \vee \sqrt{x} \geq 8) \rightarrow (x \leq 50 \vee x \geq 100))$. In words: There is a real number such that if it is not an integer or its square root is at least 8, then the number is at most 50 or at least 100.
For the converse: $\exists x, ((x \in \mathbb{Z} \wedge \sqrt{x} < 8) \rightarrow 50 < x < 100)$. In words: There is a real number such that if it is an integer and its square root is less than 8, then it is strictly between 50 and 100.

For the negation of the contrapositive: $\forall x, ((x \notin \mathbb{Z} \vee \sqrt{x} \geq 8) \wedge 50 < x < 100)$.
 In words: Every real number is strictly between 50 and 100 and at least one of the following occur: x is not an integer or the square root of x is at least 8.
 For the negation of the converse: $\forall x, (x \in \mathbb{Z} \wedge \sqrt{x} < 8 \wedge (x \leq 50 \vee x \geq 100))$.
 In words: Every real number is an integer, its square root is less than 8, and it is not strictly between 50 and 100.

Problems

Tips on Quantification on page 45 summarizes many of the major points in this chapter. You may find it helpful to read these tips before working the problems below.

Problem 4.1. Write the following statements symbolically.

- For every x , there is a y such that $x = 2y$.
- For every y , there is an x such that $x = 2y$.
- For every x and for every y , it is the case that $x = 2y$.
- There exists an x such that for some y the equality $x = 2y$ holds.
- There exists an x and a y such that $x = 2y$.

Problem 4.2. Which of the statements in Problem 4.1 are true if the universe for both x and y is the set of the real numbers?

Problem 4.3. Which of the statements in Problem 4.1 are true if the universe for x is the set of the real numbers and the universe for y is the set of the integers?

Problem 4.4. Negate the statements in Problem 4.1.

Problem 4.5. Negate the following sentences. If you don't know how to negate it, change it to symbols and then negate. State the universe, if appropriate.

- For all $x \in \mathbb{R}$, we have $x^2 > 0$.
- Every odd integer is nonzero.
- If I am hungry, then I eat chocolate.
- For every girl there is a boy she doesn't like.
- There exists x such that $g(x) > 0$.
- For every x there is a y such that $xy = 1$.
- There is a y such that $xy = 0$ for every x .
- If $x \neq 0$, then there exists y such that $xy = 1$.
- If $x > 0$, then $xy^2 \geq 0$ for all y .
- For all $\varepsilon > 0$, there exists $\delta > 0$ such that if x is a real number with $|x - 1| < \delta$, then $|x^2 - 1| < \varepsilon$.
- For all real numbers M , there exists a real number N such that $|f(n)| > M$ for all $n > N$.

Problem 4.6. What are the sets, A and B , described by the following statements?

- (a) $\forall x, (x \in A \leftrightarrow \exists n, (n \in \mathbb{Z} \wedge x = 2n))$.
- (b) $\forall x, (x \in B \leftrightarrow \exists n, (n \in \mathbb{Z} \wedge x = 2n + 1))$.

Problem 4.7. Consider the statement of Exercise 4.2 on page 36.

- (a) Write the negation of that statement using symbols.
- (b) Write the negation of that statement as an English sentence.

Problem 4.8. Consider the following statement.

For all positive integers x , there exists a real number y such that for all real numbers z , we have $y = z^x$ or $z = y^x$.

- (a) Write this statement using symbols and appropriate quantification. Use \mathbb{R} for the universe of all variables.
- (b) Once you have written this statement in symbols, negate the (symbolic) statement that you obtained.

Problem 4.9. Consider the following statement:

$$\forall x, ((x \in \mathbb{Z} \wedge \neg(\exists y, (y \in \mathbb{Z} \wedge x = 7y))) \rightarrow (\exists z, (z \in \mathbb{Z} \wedge x = 2z))).$$

- (a) Negate this statement.
- (b) Write the original statement as an English sentence.
- (c) Which statement is true, the original one or the negation? Explain your answer.

Problem 4.10. Write each of the statements below using symbolic notation. In this problem, use \mathbb{R} as the universe for all variables involved.

- (a) There is an integer that is bigger than its square.
- (b) Every rational number is the product of two irrational numbers. (Note: A real number x is irrational if $x \notin \mathbb{Q}$.)
- (c) There are integers m and n such that for each rational number x , we have $m < nx$ or $n < mx$.
- (d) Every rational number is the solution of an equation $ax + b = 0$, where a and b are integers.

Problem 4.11. Why is this joke supposed to be funny? A physicist, a chemist, and a mathematician are traveling through Switzerland. From the train they spot a cow grazing in the field. The chemist gazes out the window and says, "Ah, all the cows in Switzerland are brown." The physicist says, "No, no. You can't conclude that. You can only say that some of the cows in Switzerland are brown." The mathematician says, "No, no, no. All you can say is that there is a cow in Switzerland that is brown on one side."

Problem 4.12. For each of the following, state

1. the negation of the statement;
2. the converse of the statement;
3. the negation of the converse;
4. the contrapositive of the statement; and
5. the negation of the contrapositive.

State the universe, if appropriate, and quantify anything that is quantifiable.

- (a) Madeleine waters the rosebush only if it is Tuesday.
- (b) If I ski, I will fall.
- (c) Windows break if you throw balls through them.
- (d) If I negate a sentence, then I always do it wrong.
- (e) I will come only if you invite me.
- (f) For all positive real numbers x , there exists an integer n such that $1/n < x$. (For the universe on x and n , use the real numbers.)
- (g) If x is a nonzero real number, then $x^2 \neq 0$.
- (h) If x is a nonzero real number, then there exists a real number y such that $x \cdot y = 1$.
- (i) If x and y are even integers, then $x + y$ is an even integer.

Problem 4.13. Find a different useful description of each of the following:

- (a) $\{x \in \mathbb{R} : x^2 = 2\}$;
- (b) $\{(x, y) \in \mathbb{R}^2 : x = y\}$;
- (c) $\{x \in \mathbb{N} : x \leq 0\}$;
- (d) $\{x \in \mathbb{Z} : x^2 > 0\}$.

Problem 4.14. Write each of the following in set notation.

- (a) The set of all odd integers.
- (b) The set of all points in the xy -plane above the line $y = x$.
- (c) The set of all points in the xy -plane that are inside the circle of radius one.
- (d) The set of all irrational numbers.

Problem 4.15. Assume that the universe for the variables below is \mathbb{R} . Consider the statement form $\exists M, ((M \in \mathbb{Z}) \wedge \forall x, (x^2 \leq M))$.

- (a) Negate this statement.
- (b) Which is true, the statement or its negation?

Problem 4.16. Consider the statement “All odd positive integers are prime.”

- (a) Write this statement using logic symbols and standard set notation only. You may use \mathcal{P} for the set of all prime numbers. Make sure you include the proper quantifiers.
- (b) Negate the statement.
- (c) Prove the statement of part (a) or (b), whichever is correct.

Problem 4.17. Let a, b , and c be fixed real numbers, and consider the statement “For all real numbers x , if x is greater than a or equal to b , then x does not equal c .”

- (a) Write this sentence in symbols.
- (b) Negate the symbolic statement.
- (c) Translate the statement back into a (coherent) English sentence.

Problem 4.18. For an integer x consider the statement: “If 8 does not divide $x^2 - 1$, then x is even.”

- (a) State an appropriate universe for x .
- (b) Write the statement in symbols.
- (c) Negate the statement.

Problem 4.19. Assume that the universe for all variables below is the set of the real numbers, \mathbb{R} . Consider the statement:

$$\forall x, (\exists y, (x^3 = y^2)) \vee \forall z, (z^2 < 0 \rightarrow x^3 \neq z^2).$$

- (a) Negate this statement (keeping the symbolic notation).
- (b) Which statement is true, the original or the negation? Give a very brief argument for your choice.

Problem 4.20. Decide whether statement (3) is true if statements (1) and (2) are both true. Give reasons for your answers.

- (a) The three statements are:
 - (1) Everyone who loves Bill loves Sam.
 - (2) I don't love Sam.
 - (3) I don't love Bill.
- (b) The three statements are:
 - (1) If Susie goes to the ball in the red dress, I will stay home.
 - (2) Susie went to the ball in the green dress.
 - (3) I did not stay home.
- (c) The three statements are:
 - (1) If l is a positive real number, then there exists a real number m such that $m > l$.
 - (2) Every real number m is less than t .
 - (3) The real number t is not positive.
- (d) The three statements are:
 - (1) Every little breeze seems to whisper Louise or my name is Igor.
 - (2) My name is Stewart.
 - (3) Every little breeze seems to whisper Louise.
- (e) The three statements are:
 - (1) There is a house on every street such that if that house is blue, the one next to it is black.

- (2) There is no blue house on my street.
 (3) There is no black house on my street.
- (f) Let x and y be real numbers.
- (1) If $x > 5$, then $y < 1/5$.
 (2) We know $y = 1$.
 (3) So $x \leq 5$.
- (g) Let M and n be real numbers.
- (1) If $n > M$, then $n^2 > M^2$.
 (2) We know $n < M$.
 (3) So $n^2 \leq M^2$.
- (h) Let x, y , and z be real numbers.
- (1) If $y > x$ and $y > 0$, then $y > z$.
 (2) We know that $y \leq z$.
 (3) Then $y \leq x$ or $y \leq 0$.

Tips on Quantification

- Check the universe for each of the variables. Write it down, if it is not self-evident.
- When a quantifier on a variable in a statement is a universal quantifier, writers sometimes omit it. For example, you may read a statement about real numbers such as “If x is negative, then x^2 is positive.” Because the quantifier is not explicitly stated, we assume the author meant, “For every real number x , if x is negative, then x^2 is positive.” If you want to say that *there exists* such an x , you must include the existential quantifier.
- Suppose a statement restricts the variable x to a proper subset A of the universe as in the statement form, “For all $x \in A$, property $p(x)$ holds.” Since x is universally quantified, this is an implication of the form

$$\forall x, (x \in A \rightarrow p(x)).$$

- Suppose a statement restricts the variable x to a proper subset A of the universe as in the statement form, “For some $x \in A$, property $p(x)$ holds.” Since x is existentially quantified, this is a conjunction of the form

$$\exists x, (x \in A \wedge p(x)).$$

- Simple statements are usually easy to negate. Just do it.

- Complicated statements will often resist a “just do.” Write them out in symbols first. Make sure you know what the quantifier is on every variable. Check for the various ways one can say “if..., then...”
- Do not use logical connectives ($\neg, \wedge, \vee, \rightarrow, \leftrightarrow$) between quantifiers. (Do not write “ $\forall x \vee \forall y \dots$ ” or “ $\forall x \wedge \forall y \dots$.”)
- Know the rules. You must know how to negate statements involving existential quantifiers, universal quantifiers, conjunctions, disjunctions, and implications. The most important negation is also the one students frequently forget: the negation of an implication.
- Practice: Every time you get a definition or theorem, try negating it. If you can't, this might indicate that you do not fully understand it.

If you think you need more practice, here it is. In what follows, unless otherwise stated, all variables are real numbers, and ε and δ represent positive real numbers. Negate all of these.

- Let a be a fixed element of \mathbb{R} . For every ε there exists δ such that for every $x \in \mathbb{R}$, if $|x - a| < \delta$, then $|x^2 - a^2| < \varepsilon$.
- For all x , we have $x < x + \varepsilon$ for every ε .
- For every integer n , there exists $x > n$ such that $x^2 > n^2$.
- For all x, y , and z , if $x < y$ and $z < 0$, then $zx > zy$.
- For every ε , there exists an integer N such that $1/n < \varepsilon$ for all $n \geq N$.
- For all x , we have $x < 0$ or $x > 0$.
- For all x , there exists an integer n such that $n > x$.
- For all x and y , if $x < y + \varepsilon$ for all ε , then $x \leq y$.
- For every ε , there exists δ such that $\delta < \varepsilon$.

We provide solutions (which you should not look at until you try the negation!) for the first four exercises below.

- Let a be a fixed element of \mathbb{R} . There exists ε such that for every δ there exists x for which $|x - a| < \delta$ and $|x^2 - a^2| \geq \varepsilon$.
- There exist x and ε such that $x \geq x + \varepsilon$.
- There exists an integer n such that for all x , if $x > n$, then $x^2 \leq n^2$.
- There exist x, y , and z such that $x < y, z < 0$, and $zx \leq zy$. ○

Chapter 5

Proof Techniques

The fact that Adolphe Sax invented the saxophone hardly proves that William Tell invented the telephone.—Markus M. Ronner (Swiss journalist)¹

In this chapter, we introduce you to some of the most common proof techniques. The three methods we will examine in this section are:

- direct proof (just get started and keep going),
- proof by contradiction (show that the negation of the statement you wish to prove implies the impossible), and
- proof in cases (which may be used when conditions dictate that different situations occur).

There are many more. For example, another proof technique that you may be familiar with from the study of calculus is the method of exhaustion, such as computing area or volume calculations by “filling up the object” with a sequence of more familiar smaller sets. Sometimes these techniques are used in combination. Some other methods, such as proof of existence and uniqueness of an object or proof by induction, will appear in subsequent chapters.

The first example is a direct proof. We want to show that “If A , then B is true.” So we do it in our most direct manner: We start with A and keep going until we get to B . Before getting started, we make sure we know the meaning of every word in the implication and we try to make sure that the implication is true.

Theorem 5.1. *If a, b , and c are integers such that a divides b and a divides c , then a divides $b + c$.*

“*Understanding the problem.*” Okay, before we get started, let’s identify the hypothesis and conclusion. What are they? The hypothesis is a, b , and c are integers such that a divides b and a divides c . We get to start with that. What does a divides b mean? We say that a nonzero integer a **divides** b if there is an integer n such that $b = an$. There is even a standard symbol for this, namely, $a|b$. Since we have already

¹ The translation is ours.

defined everything here, we understand the problem and we feel confident—raring to go, in fact. What’s the conclusion we need to come to? The conclusion is a divides $b + c$, and we know what this means because we understand “divides.”

“*Devising a plan.*” So we know that, in the notation we used above, $b = am$ and $c = an$ where m and n are both integers. We need to show that a divides $b + c$, or that there is an integer j with $b + c = aj$. Looking at what we were given and what the desired conclusion is should suggest the plan.

Proof. Since a, b , and c are integers such that $a|b$ and $a|c$, we know that there exist integers m and n such that $b = am$ and $c = an$. Therefore, $b + c = am + an = a(m + n)$. Since $m + n$ is an integer and $a \neq 0$, we conclude that $a|(b + c)$. \square

“*Looking back.*” Let’s admire this proof for a minute. It’s so lovely. There are complete sentences, periods, and all symbols are carefully defined. We say where we are starting; that is, what the assumption is, and we end by saying what the conclusion is. Just in case the reader hasn’t noticed, though, we indicate that we are done by adding the little box, \square . Other people use Q.E.D. (*quod erat demonstrandum* which is Latin for *which was to be demonstrated*). Your proofs should be just as appealing as the one above.

What follows is an example of a proof by contradiction, sometimes referred to as *reductio ad absurdum*. The idea of such a proof is that we suppose that what we wish to conclude is false and show that something really silly happens (hence the absurdum). Below is an example of this idea that goes back to the Pythagoreans. This is one of two proofs presented by G. H. Hardy in his famous book *A Mathematician’s Apology* [45], as an example of a beautiful proof. (The first proof in Hardy’s text is in the problems. If you haven’t read his book, it is another one that we highly recommend.)

Theorem 5.2. *The number $\sqrt{2}$ is not rational.*

“*Understanding the problem.*” Before we begin, we make sure that we know what all the words mean, what we are assuming, and what we are trying to prove. A rational number is a number of the form p/q where p and q are integers, and q is nonzero. So we need to show that $\sqrt{2}$ is not of this form; that is, there are no integers p and q (with q nonzero) such that $\sqrt{2} = p/q$. That may seem like a tall order, since it seems to mean we have to look through all possible integers! This leads directly to:

“*Devising a plan.*” Perhaps it would be easiest to assume $\sqrt{2} = p/q$ (with p and q integers and $q \neq 0$) and see what, if anything, happens. This is precisely the idea behind proof by contradiction.

Proof. Suppose, to the contrary, that $\sqrt{2}$ is rational. Then there exist integers p and q (with q nonzero) such that $\sqrt{2} = p/q$. We may assume that p and q have no common factor, for if they did, we would simplify and begin again. Now, we have that $\sqrt{2}q = p$. Squaring both sides, we obtain $2q^2 = p^2$. Thus p^2 is even. Since p^2 is even, we know from Problem 3.2 that p must be even. Therefore, $p = 2m$ for some integer m . This means that $2q^2 = 4m^2$. Dividing, we see that $q^2 = 2m^2$. But this

means that q^2 is even. Again we know from Problem 3.2 that q is even. So p and q have a common factor 2, which is completely absurd, since we assumed they had no common factor. Therefore our assumption that $\sqrt{2}$ is rational must be wrong and we have completed the proof of the theorem. \square

“Looking back.” Note that we slipped in a reference to Problem 3.2. If we hadn’t, you would have read “Since p^2 is even, p must be even.” Your reaction to this could have been “Oh yeah, we did that already.” That’s fine. But you could also have stopped, tried to think about why it is true, tried to prove it, and so on. That’s fine too, in some sense, but you don’t want to re-prove everything we have already done. So if the writer tells the reader why something is true, it saves the reader valuable time. Or, you could also have skipped right over it, never worrying about why it is true. That’s not fine. You need to understand each sentence in a proof!

Knowing how to split a proof into cases, which we will refer to as a “proof in cases,” is something that will be extremely useful too. Here is an example of something defined in cases. Once we understand this definition, we’ll prove something using it.

For a real number x , the **absolute value** of x is defined in cases by

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} .$$

Is this what you were expecting the definition to be? If not, let’s make sure it agrees with what you were expecting. If $x = 3$, then $x \geq 0$, and we conclude that $|3| = 3$. If $x = -3$, then $x < 0$, and we conclude that $|-3| = -(-3) = 3$. If you feel comfortable with this definition, you are ready to move on to the theorem. If not, work out a few more examples and then move on.

Theorem 5.3. *Let x and y be real numbers. Then $|xy| = |x||y|$.*

We made sure that we understood the definition of absolute value before proceeding to the theorem, so we understand the problem. Let’s think about devising a plan.

“Devising a plan.” Absolute value was defined in cases, and therefore $|xy|$ depends on whether $xy \geq 0$ or $xy < 0$. The first, $xy \geq 0$, is actually two cases again: $xy > 0$ or $xy = 0$. What are the possibilities? Well, $xy > 0$ would mean that both $x > 0$ and $y > 0$, or both $x < 0$ and $y < 0$. The case $xy = 0$ would mean that $x = 0$ or $y = 0$. The final possibility, $xy < 0$, would mean that one of the two, x or y , is negative and the other is positive. It seems that we have four cases to consider: both x and y positive, both negative, at least one of the numbers is zero, and one of the two numbers negative while the other is positive.

Proof. First, suppose that $x > 0$ and $y > 0$. Then $xy > 0$ and we have $|xy| = xy$, $|x| = x$, and $|y| = y$. Therefore,

$$|xy| = xy = |x||y| ,$$

and we have established the result in this case.

Second, suppose that $x < 0$ and $y < 0$. Then $xy > 0$ and we have $|xy| = xy$, $|x| = -x$, and $|y| = -y$. Therefore,

$$|xy| = xy = (-x)(-y) = |x||y|,$$

and we have the result for this case as well.

Third, suppose that $x = 0$ or $y = 0$. Then $xy = 0$ and we have $|xy| = 0$. Also, $|x| = 0$ or $|y| = 0$. Therefore,

$$|xy| = 0 = |x||y|,$$

establishing the result in this case too.

For our final case, suppose that one number is positive and the other is negative. Thus, we may assume that $x < 0$ and $y > 0$. Then $xy < 0$ and we have $|xy| = -(xy)$, $|x| = -x$, and $|y| = y$. Therefore,

$$|xy| = -(xy) = (-x)y = |x||y|.$$

We have now established the result for all four possible cases and we may conclude that $|xy| = |x||y|$ for all real numbers x and y . \square

Once again, look at the form of the proof. There are four cases and we tell the reader which case we are discussing before we discuss it. We can conclude something in each case, but it isn't until we cover all four possible cases that we can write "we may conclude that $|xy| = |x||y|$ for all real numbers x and y ."

It will also be helpful to know how to show something is not true. A statement whose truth is anticipated, but for which we have no proof yet is called a conjecture. There are many different ways that one might arrive at a conjecture. It can be due to the intuition or insight of a great mathematician, or it can be a generalization of observations gleaned from many examples. The latter has become more common in recent years, in part due to the capabilities of powerful calculators and computers. Once we find a proof, the conjecture turns into a theorem. One of the most famous examples in recent history is a proof by Andrew Wiles. In 1995, Wiles turned Fermat's last conjecture into Fermat's last theorem, [111]. Fermat's last theorem was a conjecture for over 350 years. (Watch the excellent Nova episode "The Proof" for the full story on the history of Fermat's last theorem, [10].)

Another recent and major achievement was the proof of the 100-year-old Poincaré conjecture by Grigori Perelman. In 2002 and 2003, Perelman made three papers available on the Internet and, by 2006, experts were convinced that Perelman's papers provided a positive answer to the Poincaré conjecture. Such an achievement was well worthy of the Fields Medal, one of the top two honors a mathematician can receive and often considered the equivalent of the Nobel Prize (with the other award being the Abel Prize). Perelman declined the Fields Medal. Because the Poincaré conjecture is one of the seven millennium problems for which the Clay Mathematics Institute has offered a one million dollar award for the solution, Perelman was offered this award. As expected, he declined this prize, too. There is a biography of Grigori Perelman and the culture of Russian mathematicians in the 20th century,

[33]. The Clay Institute has a website with all seven problems listed, and some of them are formulated as conjectures. (See [19].)

It's important to note that just because you believe something might be true, doesn't mean that it necessarily is true. Sometimes you will find that a conjecture someone else has made (or even one that you have made) is, in fact, false. In these cases, you need to find an example of something that satisfies the hypotheses of your conjecture, but not the conclusion. An example is the following conjecture of Pierre de Fermat—one of the very few of his conjectures that turned out to be wrong.

Consider numbers of the form $2^{2^m} + 1$, where m is a natural number. The first number, $2^{2^0} + 1 = 3$, is prime. The second, $2^{2^1} + 1 = 5$, is also prime, as are the third, fourth, and fifth numbers. In fact, Fermat conjectured that if m is a nonnegative integer, then $2^{2^m} + 1$ is prime. In 1732, the Swiss mathematician Leonhard Euler showed that this was false by showing that the sixth number in this list, $2^{2^5} + 1 = 4294967297$, can be factored. In fact, our calculator tells us that

$$2^{2^5} + 1 = 641 \cdot 6700417.$$

Thus Fermat's conjecture is false.

An example that shows that a statement is false is called a counterexample. You only need one to show something is false!

We end this chapter by discussing one final statement form that appears frequently in mathematics, and this is a statement of the form “ A if and only if B .” This is a really convenient way of saying two things: A if B and B if A . In other words, it's two statements in one! We have already seen examples of this; for example, in Problem 3.2 (c) you summarized a result as

An integer x is odd if and only if x^2 is odd.

We proved this statement in two installments. First we showed the implication of Theorem 3.3: *For all real numbers x , if x^2 is odd, then x is odd.* We proved the converse in Problem 3.2 (a): *For all real numbers x , if x is odd, then x^2 is odd.* This approach, proving the necessity and sufficiency, is what you will do each and every time. So whenever you have to prove an “if and only if” statement you should rejoice: You get to give two proofs for one problem. To make your proof clear and easy to follow, it's a good idea to break the proof into two parts, indicate clearly which part you are proving, and indicate clearly when you have finished proving each part. Here's an example.

Example 5.4. Show that for a real number x , we get $-2 \leq x < 1$ if and only if $(2x + 1)/(x - 1) \leq 1$.

“*Devising a plan.*” We have to prove an equivalence, so we have two separate problems, each of which is an implication. We will first show that for all real numbers x , if $-2 \leq x$ and $x < 1$, then $(2x + 1)/(x - 1) \leq 1$. A direct proof should work here. Then we will prove the converse: For all real numbers x , if $(2x + 1)/(x - 1) \leq 1$, then $-2 \leq x$ and $x < 1$. We will find it convenient to multiply the inequality by

$x - 1$. Since we don't know whether $x - 1$ is positive or negative, we will need to consider two cases. Consequently, we expect this proof to be a proof in cases.

Proof. We first assume that $-2 \leq x$ and $x < 1$. Adding $x + 1$ to the first inequality, $-2 \leq x$, we get $x - 1 \leq 2x + 1$. Subtracting 1 from the inequality $x < 1$ leads to $x - 1 < 0$. Therefore, when we divide by $x - 1$, this “flips the sign.” As a result we obtain $(2x + 1)/(x - 1) \leq 1$, as required.

For the converse we assume that $(\star)(2x + 1)/(x - 1) \leq 1$. Note first that this implies that $x \neq 1$. Now our proof will be in cases, $x - 1 > 0$ and $x - 1 < 0$. So first suppose that $x - 1 > 0$. Multiplying (\star) by $x - 1$, we get $2x + 1 \leq x - 1$. This, and our assumption that $x - 1 > 0$, implies $0 < x - 1 \leq -3$. This is a contradiction and shows that this case is impossible. Now consider the remaining case, namely, $x - 1 < 0$, or equivalently, $x < 1$. As before, this implies that $2x + 1 \geq x - 1$. This, in turn, implies that $x \geq -2$. We conclude that $-2 \leq x < 1$, completing the proof of the converse.

Since we have proved both the statement “ $-2 \leq x < 1$ implies $(2x + 1)/(x - 1) \leq 1$,” and its converse, we have completed the proof of the result. \square

“*Looking back.*” Reviewing the structure of the proof above, we note that we have proved an implication and its converse. We use certain phrases for the benefit of the reader; for example, when we say “We will first show that...” this is to let the reader know what's coming. Of course, the astute reader would figure it out, eventually, without being told. But most people like to be told where they are going before they get to their destination, and the same is true in mathematics. After indicating clearly what our hypothesis is, we work until we obtain the desired conclusion and we say when we have reached our conclusion. There are, sometimes, “if and only if” proofs in which each step of the proof is reversible, and some authors will work both directions simultaneously to save time and space. Even in this case, it is less confusing for the reader if you prove one direction and, after carefully checking that all steps are reversible, say something on the order of “since all the steps above are reversible, the converse follows.” \circ

It's very convenient, when taking notes or writing quickly, to follow the lead of many mathematicians and write “iff” for “if and only if.” While it can be a real time saver, we don't recommend it in formal writing.

Definitions

Definition 5.1. A nonzero integer a **divides** an integer b if there is an integer n such that $b = an$. We write this as $a|b$.

Definition 5.2. For a real number x , the **absolute value** of x is defined to be

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} .$$

Problems

Problem 5.1. Below is the other proof Hardy chose to present ([45, pp. 92–94]). This theorem and its proof were known to Euclid, and appear in the *Elements* IX 20, [47]. Can you read and understand this proof? Read the whole thing. Underline anything you don't understand the first time. Reread it slower this time. Underline anything you can't figure out. You may need to spend 10 minutes on each sentence; you may not. Then write the general idea of the proof in "street talk." A bright, interested twelve-year-old should be able to follow your outline of the proof.

Before you begin, make sure you understand what will be assumed and what we will try to do. Make sure you know what all the words mean. "Infinite" has not yet been defined; prime number has.

Theorem 5.5. *There are infinitely many prime numbers.*

Proof. To prove this statement, suppose, to the contrary, that there are finitely many primes. Then we may write these finitely many primes in ascending order as

$$2, 3, 5, \dots, N,$$

where N is the largest prime. Now consider the number M defined by

$$M = (2 \cdot 3 \cdot 5 \cdots N) + 1.$$

If M is prime, then M is a prime that is larger than the largest prime N . Therefore, we must conclude that M is not prime, and so it is divisible by some prime number, P . However, P must appear in the list of primes

$$2, 3, 5, \dots, N,$$

which we gave earlier. But when we divide M by P , we obtain a remainder of 1. Therefore, P cannot be a factor of M , and we have contradicted our assumption that there are finitely many primes. Thus, there exist infinitely many primes. \square

Problem 5.2. Prove that if n is an integer, then $4n^2 + 4n + 8$ is an even integer. What kind of proof did you use?

Problem 5.3. Prove that if n is an integer, then $n^2 + 3n + 2$ is an even integer. What method of proof did you use?

Problem 5.4. In this problem, we outline a proof of the following theorem:

Theorem 5.6. *Let x and y be real numbers. If $xy > 1/2$, then $x^2 + y^2 > 1$.*

Your mission is to fill in the gaps and blanks, leaving no detail omitted.

Proof. The proof will proceed by (insert name of proof technique or description of proof strategy here). So suppose that $x^2 + y^2 \leq 1$. Now we know that $(x - y)^2 \geq 0$. (Insert missing steps of proof here.) Therefore $xy \leq 1/2$, and the proof is complete. \square

Problem 5.5. In this problem, we outline a proof of the following theorem:

Theorem 5.7. *If n and m are nonzero integers, then $n^2 - m^2 \neq 1$*

Your mission is to fill in the gaps and blanks, leaving no detail omitted.

Proof. The proof will proceed by (*insert name of proof technique or description of proof strategy here*). So suppose that $n^2 - m^2 = 1$. Then $(n - m)(n + m) = 1$. Since (*insert relevant reason here*), we conclude that both factors, $(n - m)$ and $(n + m)$, are equal. Now we cannot have $n - m = n + m$, because (*insert reason here*). Therefore (*insert concluding sentence*). \square

Problem 5.6. Consider the two statements about real numbers x and y .

Statement 1. If the product, xy , is not a rational number, then x or y must be an irrational number.

Statement 2. If x is a rational number and y is an irrational number, then $x + y$ is irrational.

- What method(s) of proof would you use to prove Statement 1? Statement 2? Why?
- Prove Statement 1 in the most efficient way possible. Do you need to modify your answer to the previous part of the problem? Explain.
- Prove Statement 2 in the most efficient way possible. Do you need to modify your answer to the previous part of the problem? Explain.

Your first proof of these statements may not be the best one. Run through the various techniques until you come up with the nicest proof of each statement!

Problem 5.7. Provide counterexamples to each of the following.

- Every odd number is prime.
- Every prime number is odd.
- For every real number x , we have $x^2 > 0$.
- For every real number $x \neq 0$, we have $1/x > 0$.
- Every function $f : \mathbb{R} \rightarrow \mathbb{R}$ is linear (of the form $mx + b$).

Problem 5.8. Define two sets, A and B , by

$$A = \{x \in \mathbb{Z} : x = 2n \text{ for some } n \in \mathbb{Z}\} \text{ and}$$

$$B = \{x \in \mathbb{Z} : x = 2m + 1 \text{ for some } m \in \mathbb{Z}\}.$$

- Using these definitions, give a rigorous proof that A and B have no element in common. Make sure you write out all details.
- What type of proof did you use in part (a)?

Problem 5.9. Let n be an integer. Prove that if n^2 is divisible by 3, then n is divisible by 3.

Problem 5.10. Show that $\sqrt{3}$ is not rational. (You may want to use the result of Problem 5.9 to work this problem.)

Problem 5.11. Prove that $\sqrt{2} + \sqrt{3}$ is not a rational number.

Problem 5.12. Prove that the square of an integer cannot be of the form $3k + 2$, where k is an integer.

Problem 5.13. Prove that $\sin^2 x \leq |\sin x|$ for all $x \in \mathbb{R}$.

Problem# 5.14. Let x be a real number.

- Prove that $-|x| \leq x \leq |x|$.
- Let $a \geq 0$. Prove that $|x| \leq a$ if and only if $-a \leq x \leq a$.
- Use parts (a) and (b) to prove the theorem below.

Theorem 5.8 (The triangle inequality). Let x and y be real numbers. Then

$$|x + y| \leq |x| + |y|.$$

Problem 5.15. Prove the lower triangle inequality: Let x and y be real numbers. Then

$$||x| - |y|| \leq |x - y|.$$

There are many ways to do this, but we would like to firmly suggest using the triangle inequality (see Theorem 5.8 above).

Problem 5.16. Prove that for real numbers z and w ,

$$|(1 + z)(1 + w) - 1| \leq (1 + |z|)(1 + |w|) - 1.$$

Problem 5.17. Prove or refute the following conjecture. There are no positive integers x and y such that $x^2 - y^2 = 10$.

Problem 5.18. Prove or refute the following conjecture. There are no positive integers x and y such that $x^2 - 3xy + 2y^2 = 10$.

Problem 5.19. Prove that for all real numbers x , we have $x \leq -5$ if and only if $1 \leq (2x + 3)/(x - 2) \leq 2$.

Problem 5.20. Find all points in the xy -plane that lie on the surface

$$4 = 5(x - 3)^2 + 3(y - \pi)^2 + 2(z + 2)^2.$$

Write up your solution carefully. What method of proof did you use?

Problem 5.21. Let n be an integer. Prove that if $n^2 - (n - 2)^2$ is not divisible by 8, then n is even.

Problem 5.22. Let $n \in \mathbb{Z}^+$, $a_0, \dots, a_n \in \mathbb{R}$, and $a_n \neq 0$. Prove that the polynomial $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ can have at most n different roots. (Some remarks are in order here. To work this problem, you must understand it. Recall that $c \in \mathbb{R}$ is a root of a polynomial p if $p(c) = 0$. In order to solve the problem, you also need to recall that if c is a root of p , then $x - c$ is a factor of p .)

Problem 5.23. Let a_1, \dots, a_{10} be real numbers and $y = (x - a_1) \cdots (x - a_{10})$ be the equation of a curve in the plane \mathbb{R}^2 . Prove that this curve has a horizontal tangent at $x = a_1$ if and only if $a_1 = a_j$ for some j in $\{2, 3, \dots, 10\}$. (Note: This problem requires knowledge of calculus.)

Problem 5.24. Consider the following statement.

$$\forall x, (x \in \mathbb{Z}^+ \rightarrow \exists y, \exists z, ((y \in \mathbb{Q}) \wedge (z \in \mathbb{Q}) \wedge (yz \neq 0) \wedge (x^2 = y^2 + z^2))).$$

- Change this symbolic statement to an English sentence.
- Prove the statement you found in (a).

Tips on Definitions

“When I use a word,” Humpty Dumpty said, in a rather scornful tone, “it means just what I choose it to mean—neither more nor less.”—Lewis Carroll, [17, p. 163]

In your previous courses, you may or may not have had to memorize definitions. Now it becomes essential that you memorize them, understand them, and investigate them before venturing on to use them. Here are some suggestions on how to do these things.

- The first step is to make sure you know the definition. This does not mean that you highlight it with a marker and read it over a few times. It means that you, first of all, understand it, and, second of all, memorize it. You must know whether the quantifiers are “for all” or “there exist,” you must know what order they come in, you must watch the order on implications, and you must be sure that what you write is correct. Every single itty bitty detail must be correct or chances are that your definition is wrong.
- It’s very difficult to memorize something you don’t understand. So once you see a definition (in bold black print in this book) write it down and think about what it means.
- Give many examples, until you feel that you know what an example looks like.
- Negate the definition and try to find nonexamples (that show when things won’t satisfy the definition).

- Go back and see if you can write out the definition without looking at it. Wait a few hours and do that again. If anything is out of place, ask yourself if it matters. If it does, repeat the appropriate steps here.
- Definitions are often stated as implications. This leads students to ask if the definition is an equivalence. The answer is “yes.” Consider the following definition: “An integer m is even if there exists an integer n such that $m = 2n$.” Since this is how we defined “even,” we also mean that “if m is even, then there exists an integer n such that $m = 2n$.”
- Note that you either have defined something correctly or not; you can’t “get close” to a definition unless you get it right. For example, suppose you are asked to define *cat*. Let’s say your definition is “A carnivorous mammal, domesticated since early times.” Fair enough, it seems. Now suppose that working with this definition you try to purchase a mail-order cat and you receive a large St. Bernard. While this might upset you, it shouldn’t surprise you. Your definition was close enough that you didn’t receive a mail-order minivan, for example, but it was also wrong. In the same way, mathematicians will be upset if your definition includes things it shouldn’t. Be very careful.

Some teachers and students find it helpful to make definition notebooks. In such a notebook, you will do all the steps above as often as necessary. We heartily recommend such an approach.

In this text, we summarize the definitions at the end of each chapter. This is intended to *help* you with a definition notebook; it is not meant to replace the notebook. Working the following additional problems will help you appreciate the value of a good definition.

Problem 5.25. Consider an object that all of you know well: A *car*.

- (a) Define a *car*. (You may not say, “A car is an automobile.” Why are we ruling this out?)
- (b) Give an example.
- (c) Give a few nonexamples. Your nonexample should be close to the definition of “car” but not close enough to be correct.

Problem 5.26. Definition. We will call a natural number an *s-difference* if it is the difference of the squares of two natural numbers.

- (a) Give three different examples of s-differences.
- (b) Write the definition symbolically. What should the universe be?
- (c) Give two nonexamples from the universe that you chose in (b).

Problem 5.27. See Problem 5.26 for the definition of an s-difference.

Definition. We will call an s-difference *simply even*, if it is even but not a multiple of 4.

- (a) Give an example of a simply even s-difference.
- (b) Give two nonexamples.

- (c) Is this a useful definition? Why or why not?

Problem 5.28. At the beginning of Chapter 4 we noted that *set* is an undefined expression. Some texts define *set* to be “a collection of objects.” Why is this “definition” not satisfactory?

Problem 5.29. For the first three parts of this problem, you will need to use your knowledge of calculus.

- (a) Consider the following: A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is differentiable if it is continuous. Is this a definition of *differentiable*? Why or why not?
- (b) Consider the following: A *sequence of real numbers* is a list of real numbers. Is this a definition of a *sequence of real numbers*? Why or why not?
- (c) We found the following “definition” of *tangent line* online: “A line that touches a curve at a point without crossing over.” What’s wrong with this definition? (Say as much as you can!)
- (d) Is this a definition of *perfect square*? A real number is a *perfect square* if there exists n such that $x = n^2$.

Chapter 6

Sets

In Chapter 4 we introduced the terms *set* and *element of a set*. In order to have some flexibility and to avoid the slightly awkward phrase *set of sets*, we will use the word *collection* as a synonym for set. In particular, we will usually speak of a collection of sets, which is just a set of sets. Just as you worked with points and lines in geometry without having a rigorous definition of those terms, we will ask you to use your intuition as you work with the terms *set* and *element*. It's important to note that you will need to exercise care when you use these words. Mathematics describes very carefully and exactly what you can do with *sets* and when you can use the words *element of a set*. In particular, the construction of “the set of all sets” is forbidden, as this would lead to contradictions. In order to get around such contradictions, mathematicians have developed axioms. These are listed in the Appendix as the Zermelo–Fraenkel system together with the axiom of choice (ZFC, for short). At this point, we will introduce our subject in a less formal way, leaving a more axiomatic treatment for a later course in set theory.

The objects that make up a set are called the elements or members of the set. A set has a defining property, and it is used to determine whether or not an element belongs to the set: To decide whether or not x is in the set S , you need to see whether x satisfies this defining property p . The **empty set** is the set with no elements, and is denoted by \emptyset .

Once we have the defining property, there are often several ways to describe a set. If there aren't too many elements in the set, then we can list all elements: $B = \{Benny, Betty, Billy, Bobby\}$. If the elements come from a well-known larger set X and satisfy a defining property p , we may write $\{x \in X : p(x)\}$. This is read “the set of all elements of X satisfying property p .” We may think of X as the universe in this context.

Example 6.1. We will frequently use sets such as the set of all even integers, the set of all odd integers, or the set of integers that are divisible by three. We will denote these sets by $2\mathbb{Z}$, $2\mathbb{Z} + 1$, or $3\mathbb{Z}$, respectively. Define these sets using the format suggested above; that is, by choosing appropriate X and p so that each set is described by $\{x \in X : p(x)\}$.

For the set of even integers, we write $2\mathbb{Z} = \{x \in \mathbb{Z} : x = 2n \text{ for some } n \in \mathbb{Z}\}$. The set of odd integers can be written as $2\mathbb{Z} + 1 = \{x \in \mathbb{Z} : x = 2n + 1 \text{ for some } n \in \mathbb{Z}\}$. Finally, the set of all integers that are divisible by three is $3\mathbb{Z} = \{x \in \mathbb{Z} : x = 3n \text{ for some } n \in \mathbb{Z}\}$. ○

Note that a set is described by its elements—not by the order we put the elements in the set, or whether we put an element in more than once. Thus the set $\{1, 2, 3\}$ is the same as the set $\{1, 1, 3, 2\}$.

Exercise 6.2. For each of the following sets, say what the universe is and write out the defining property. For example, if we wish to describe the set of all women, the universe might be all people, and the defining property would be “ x is a woman.” Use complete sentences.

- (a) The collection A of all members of the school band.
- (b) The collection B of all irrational numbers.
- (c) The collection of all prime numbers greater than or equal to 4 and less than 7. ○

Exercise 6.3. Care needs to be used when creating a defining property. What is wrong with each of the following?

- (a) The collection C of all pretty people in Luxembourg.
- (b) The collection D of all collections that do not contain themselves as an element. ○

The notation we have described so far in this chapter is not the only acceptable notation. For example, if we know what our universe is, there may be no reason to repeat it in the notation. Therefore, we may write $\{x \in X : p(x)\}$, or we may simply write $\{x : p(x)\}$. The next exercise introduces you to a slightly different way of describing a set.

Exercise 6.4. Let $S = \{x \in \mathbb{Z} : x = 2n + 1 \text{ for some } n \in \mathbb{Z}\}$ and $T = \{s^2 : s \in S\}$. The notation for T is different from the notation we have discussed thus far in the chapter, yet you can still determine T . Write out a description of T using the same notation as the one used for S . Then write out a description of S using the same notation as the one used for T . ○

Exercise 6.5. Consider the set A of nonzero integers.

- (a) Write this set using the notation $A = \{x \in S : p(x)\}$.

Use what you learned in previous chapters to answer the following questions.

Define a new “multiplication” on A by $x \star y = 2xy$ for $x, y \in A$. For parts (b) and (c) below, prove the statement or give a counterexample to it. (If you find you cannot answer the questions below, read the discussion following part (c).)

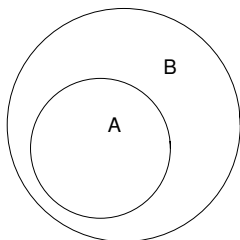


Fig. 6.1 $A \subseteq B$

- (b) If $x, y \in A$, then $x \star y \in A$.
- (c) There exists an element $y \in A$ such that $x \star y = x$ for every $x \in A$.

If you really can't get started, then you probably didn't understand the problem. One way to begin is to pick numbers for x and y and try them out until you get a feel for this new multiplication. Once you understand it, try rewriting the statements so that they make sense to you. For example, in (b), replace the conclusion $x \star y$ by its definition to obtain "If $x, y \in A$, then $2xy \in A$." All this should help. Remember, the most important thing is to get started. \circ

A set A is a **subset** of a set B or, equivalently, A is **contained** in B , if every element of A is an element of B . We will write $A \subseteq B$ to indicate that A is a subset of B . This is depicted in [Figure 6.1](#).

Notice that A is always a subset of itself: $A \subseteq A$. However, a subset can also be truly smaller, and we often find it necessary to use our notation to emphasize this. We say that A is a **proper subset** of B if $A \subseteq B$ and $A \neq B$, and we will write $A \subset B$.

Showing that a set A is contained in another set B turns out to be one of the most important tasks in mathematics. One way to show that a set A is contained in a set B is to do exactly what the definition says; take an arbitrary element of the set A and then show that this element is in set B . We need not worry about whether or not there is an element in the set A . The definition of subset requires only the implication ($x \in A$ implies $x \in B$) to be true, not the antecedent ($x \in A$).

Example 6.6. In Exercise 6.4 we used two sets, S and T , where $S = \{2n + 1 : n \in \mathbb{Z}\}$ and $T = \{s^2 : s \in S\}$. Show that $T \subseteq S$. Is T a proper subset of S ?

Remember, to prove set inclusion we have to take an arbitrary element in the set T and then show that this element is in the set S . So, for our proof of containment, we will begin with $x \in T$, and attempt to end our proof with $x \in S$.

As we will see in future chapters, we can often devise a plan for a proof of this type by writing out what we know ($x \in T$) at the top of the page, and what we want to show ($x \in S$) at the bottom. You have probably attempted proving things this way before: you work from the top down, and from the bottom up. So our plan might look like

$$x \in T,$$

large space

$$x \in S.$$

But $x \in T$ means that $x = s^2$ for some $s \in S$, and $x \in S$ means that $x = 2n + 1$ for some $n \in \mathbb{Z}$. So our plan (a few minutes later) might look like

$$x \in T,$$

$$x = s^2, \text{ for some } s \in S,$$

smaller space

$$x = 2n + 1, \text{ for some } n \in \mathbb{Z},$$

$$x \in S.$$

We keep filling things in, making sure that each line follows logically from the previous one, until we see how to complete the proof. Here's what we end up with.

Proof. (Inclusion) We claim that $T \subseteq S$. Now, if $x \in T$, then $x = s^2$ for some $s \in S$. By the definition of S , there exists $n \in \mathbb{Z}$ such that $s = 2n + 1$. Hence $x = s^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$. Now let $m = 2n^2 + 2n$. Then $m \in \mathbb{Z}$ and $x = 2m + 1$. Therefore $x \in S$. Thus $T \subseteq S$, as desired.

(Proper subset) In fact, T is a proper subset of S . To show this we need to exhibit an element that is in S , but not in T . Consider the number -1 . Then $-1 = 2(-1) + 1$ and $-1 \in \mathbb{Z}$. Thus, -1 satisfies the defining property for S , so $-1 \in S$. On the other hand, the elements of T are squares of real numbers. Consequently all of them are nonnegative. Hence $-1 \notin T$, and the inclusion is proper. \square

If you remember the result of Problem 3.2, then you know that you already showed that s^2 is odd if and only if s is odd. If you refer the reader to this result (carefully referencing it, so the reader can find it easily), you can significantly shorten the proof of inclusion. Given two proofs written with equal clarity and insight, most people will prefer the shorter of the two. If the reader remembers the result, reading it again may detract from the proof. So, as long as you tell the reader what you are using and where to find it if he or she needs to, you can (and should) refer to previous results. \circ

We now return to the subject of this chapter. Notice that we just told you how to show that a set A is contained in a set B . All you need to do is show that *for all* x , *if* $x \in A$, *then* $x \in B$. So we also just told you how to show that A is not contained in B —negate the definition of containment.

Exercise 6.7. Negate the statement: “For all x , if $x \in A$, then $x \in B$.” \circ

Two sets are equal if they have precisely the same elements. This can be defined a bit more formally as follows. A set A is **equal** to B , written $A = B$, if $A \subseteq B$ and $B \subseteq A$. To show that two sets are equal is therefore a two-step task: First you show

that one set is contained in the other ($A \subseteq B$). Then you reverse the order of the sets and show inclusion again ($B \subseteq A$).

Note that when A is a subset of B we use the symbol \subseteq , but when x is an element of A we use the symbol \in . Choose your symbols carefully and don't mix them up! If x is not in A , then we write $x \notin A$. If A is not a subset of B , then we write $A \not\subseteq B$.

Exercise 6.8. Write a definition of set equality that reverts back to membership in a set, rather than set containment. \circ

Example 6.9. Show that $\{(x, y) \in \mathbb{R}^2 : x^2 - x = y^2 = 0\} = \{(0, 0), (1, 0)\}$.

Devising a plan. According to the definition of equality above, we have to show two separate things. The first is to show that the set on the left is contained in the set on the right. For this part of the proof, we will begin with an arbitrary element $(w, z) \in \{(x, y) \in \mathbb{R}^2 : x^2 - x = y^2 = 0\}$ and we will try to show that $(w, z) = (0, 0)$ or $(w, z) = (1, 0)$. Then we must show that the set on the right is contained in the set on the left. So for this part, we will begin with $(a, b) = (0, 0)$ or $(a, b) = (1, 0)$ and try to show that it is in the set on the left.

Before beginning any problem, make sure you understand exactly what kind of objects are under consideration. In this example, our elements are in \mathbb{R}^2 , and therefore they are "points" with an x - and a y -coordinate. Thus, when we discuss elements, we will not talk about an element like "z," but rather one of the form (x, y) . You'll progress more quickly if you use the particular form of the elements in your problem.

Proof. If $(w, z) \in \{(x, y) \in \mathbb{R}^2 : x^2 - x = y^2 = 0\}$, then $w^2 - w = w(w - 1) = 0$ and $z^2 = 0$. Hence $w = 0$ or $w = 1$ and in both cases, $z = 0$. Thus $(w, z) = (0, 0)$ or $(w, z) = (1, 0)$. This implies that $(w, z) \in \{(0, 0), (1, 0)\}$ and therefore we can conclude that $\{(x, y) \in \mathbb{R}^2 : x^2 - x = y^2 = 0\} \subseteq \{(0, 0), (1, 0)\}$.

If $(w, z) \in \{(0, 0), (1, 0)\}$, then $w = 0$ or $w = 1$ and thus $w(w - 1) = w^2 - w = 0$. We also have $z = 0$ and thus $z^2 = 0$. Hence $(w, z) \in \{(x, y) \in \mathbb{R}^2 : x^2 - x = y^2 = 0\}$ and therefore $\{(0, 0), (1, 0)\} \subseteq \{(x, y) \in \mathbb{R}^2 : x^2 - x = y^2 = 0\}$.

By the definition of equality, $\{(x, y) \in \mathbb{R}^2 : x^2 - x = y^2 = 0\} = \{(0, 0), (1, 0)\}$. \square

Exercise 6.10. Let $A = \{1, 3, 5\}$, $B = \{3, 4, 6\}$, $C = \{5\}$, and $D = \{1, 3\}$. Which sets are subsets of the others? For which sets S do we have $1 \in S$? $1 \notin S$? Which sets are not subsets of each other? \circ

Theorem 6.11. Let A be a set. Then $\emptyset \subseteq A$.

Proof. We must show that for every x , if $x \in \emptyset$, then $x \in A$. Since there are no elements in the empty set, the antecedent is always false. Therefore the implication is always true, completing the proof. \square

Suppose A is a set and we wish to show that $A = \emptyset$. One inclusion, $A \subseteq \emptyset$, will suffice because the reverse inclusion is always true. In fact, such a proof will often be

done by assuming that there exists $x \in A$ and then obtaining a contradiction. When showing that a set $A = \emptyset$, then, it will look like we are proving that two sets are equal by establishing only one containment. That's only because the other containment is obvious!

Exercise 6.12. Prove the following.

- (a) For $A = \{x \in \mathbb{R} : x^2 + x + 1 = 0\}$, show that $A = \emptyset$, using the comments in the preceding paragraph.
- (b) For $B = \{x \in \mathbb{N} : \exists y \in \mathbb{R}, x = y^2\}$, show that $B = \mathbb{N}$. ○

We will now present a list of very important definitions, using two sets, A and B , to create other sets. Some examples will be presented (briefly) here, and more can be found in the exercises. In what follows, we assume that all variables x belong to a universe, X .

The **union** of two sets A and B is defined by $A \cup B = \{x : x \in A \text{ or } x \in B\}$. For example, if A denotes the set of even integers, and B denotes the set of odd integers, then $A \cup B = \mathbb{Z}$.

The **intersection** of A and B is $A \cap B = \{x : x \in A \text{ and } x \in B\}$. If A and B are two sets such that $A \cap B = \emptyset$, then we say that A and B are **disjoint**. For example, if A is the set of even integers and B is the set of odd integers, then A and B are disjoint.

The **set difference** of B in A is $A \setminus B = \{x \in A : x \notin B\}$. A comment is in order here. We can never look for objects “not in B ” unless we know where to start looking. So we use A to tell us where to look for elements not in B . If X is the universe, we will write B^c for $X \setminus B$. This is referred to as the **complement** of B . For example, let A be the set of integers. If $B = \mathbb{Z}^+$, then $A \setminus B$ is the set of elements of A (integers) that are not in B (that are not positive integers). Thus $A \setminus B = \{x \in \mathbb{Z} : x \leq 0\}$. On the other hand, if $A = \mathbb{N}$, then $A \setminus B = \{0\}$.

It is possible to visualize these sets using a representation called a Venn diagram. These diagrams are often helpful in sorting out the relationship between sets. The universe is usually indicated by a rectangle containing the sets. The idea is illustrated in [Figures 6.2 and 6.3](#). You might enjoy the pretty Venn diagrams in [93] and the book *Cogwheels of the Mind: The Story of Venn Diagrams*, [24].

A word of warning: Be careful—pictures can be deceiving. Use the Venn diagram to get your intuition going, but check everything carefully using the techniques we have developed thus far.

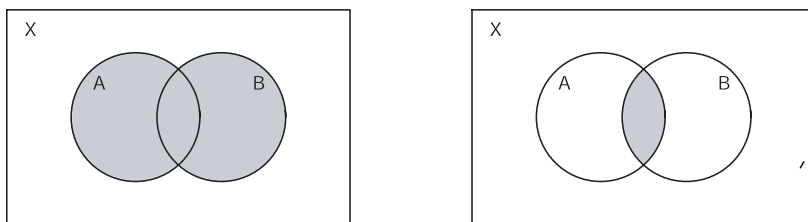


Fig. 6.2 $A \cup B$ and $A \cap B$

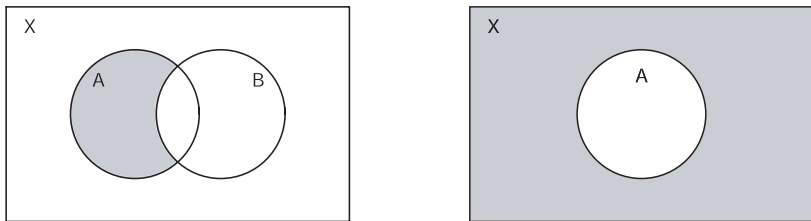


Fig. 6.3 $A \setminus B$ and A^c

Exercise 6.13. Use the sets in Exercise 6.10 to answer the following questions: What is $A \setminus B$? $A \setminus C$? Which sets are disjoint? If the universe is $\{1, 2, 3, 4, 5, 6\}$, what is A^c ? Find $A \cup B$ and $A \cap B$. ○

Exercise 6.14. Write a definition of union for three sets. Write a definition of intersection for three sets. Can you write a definition of set difference for three sets? Why or why not? ○

Definitions

Definition 6.1. The **empty set**, denoted \emptyset , is the set that contains no element.

Definition 6.2. The set A is a **subset** of set B , denoted $A \subseteq B$, if for all x it is the case that $x \in A$ implies that $x \in B$.

Definition 6.3. The set A is a **proper subset** of set B , denoted $A \subset B$, if $A \subseteq B$ and $A \neq B$.

Definition 6.4. Two sets A and B are **equal** if $A \subseteq B$ and $B \subseteq A$.

Definition 6.5. The **union** of the sets A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

Definition 6.6. The **intersection** of the sets A and B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

Definition 6.7. Two sets A and B are **disjoint** if $A \cap B = \emptyset$.

Definition 6.8. The **set difference** of set B in set A is the set $A \setminus B = \{x \in A : x \notin B\}$.

Definition 6.9. If the set X is the universe and A is a subset of X , then the **complement** of A is the set $A^c = X \setminus A$.

Solutions to Exercises

Solution (6.2). Here is the answer to (b): The universe is the set of all real numbers. The defining property is “ $x \in \mathbb{R} \setminus \mathbb{Q}$.”

Solution (6.3).

- (a) The adjective “pretty” is subjective and it is unclear whether a person from Luxembourg is a member of the set C or not.
- (b) Consider the following question: Is the collection D an element of D or not? If it is an element of D , then it must satisfy the defining property, which says that D is not an element of D ; in other words, in this case it would have to be both in the set and not in the set. On the other hand, if D is not an element of the collection D , then it does just what the defining property says. Thus it must be in the set D ; in other words, in this case it would have to be both in the set and not in the set. Hence, this property is contradictory.

Solution (6.4). We can write $T = \{x \in \mathbb{Z} : x = (2n + 1)^2 \text{ for some } n \in \mathbb{Z}\}$ and $S = \{2n + 1 : n \in \mathbb{Z}\}$.

Solution (6.5). Let A be the set of nonzero integers.

- (a) $A = \{x \in \mathbb{Z} : x \neq 0\}$.
- (b) Let x and y be elements of A . Then $x \star y = 2xy$. Since x, y , and 2 are all integers, $x \star y \in \mathbb{Z}$. Furthermore, since x and y are elements of A , they are nonzero. Therefore $x \star y = 2xy \neq 0$. Consequently $x \star y \in A$, as desired.
- (c) This is false. Suppose to the contrary that there were such an element y in A . Then $x \star y = x$ for every $x \in A$. Choosing $x = 1$, we see that $1 = 1 \star y = 2(1)(y) = 2y$. The only solution to this equation is $y = 1/2$, which is not an integer and therefore not an element of A . This contradiction shows that no such y can exist.

Solution (6.7). The negation is “There exists an x such that $x \in A$ and $x \notin B$.”

Solution (6.8). Two sets A and B are equal if for all x we have $x \in A$ if and only if $x \in B$.

Solution (6.10). The following statements hold:

- $C \subseteq A$ and $D \subseteq A$;
- no other sets are subsets of each other;
- $1 \in A, 1 \in D, 1 \notin B$, and $1 \notin C$.

Solution (6.12).

- (a) Suppose there exists $x \in A$. Then $x \in \mathbb{R}$ and $x^2 + x + 1 = 0$. This implies that $x = (-1 + \sqrt{3}i)/2$ or $x = (-1 - \sqrt{3}i)/2$. In both cases, $x \notin \mathbb{R}$ leading to a contradiction. Hence $A = \emptyset$. Alternatively, we might recall the technique of completing the square to note that

$$x^2 + x + 1 = x^2 + x + \frac{1}{4} + \frac{3}{4} = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4} > 0,$$

establishing a contradiction.

- (b) We need only show that $\mathbb{N} \subseteq B$ (why?). If $n \in \mathbb{N}$, then $n \in \mathbb{R}$ and $n \geq 0$. Thus $y = \sqrt{n} \in \mathbb{R}$ and $n = y^2$. Hence $y \in B$. This shows that $\mathbb{N} = B$.

Solution (6.13). The following statements hold:

- $A \setminus B = \{1, 5\}$, $A \setminus C = \{1, 3\}$;
 sets B and C are disjoint, and sets C and D are disjoint;
 if the universe is as given, then $A^c = \{2, 4, 6\}$;
 $A \cup B = \{1, 3, 4, 5, 6\}$, and $A \cap B = \{3\}$.

Solution (6.14). Let A, B , and C be sets and let the universe be denoted by X . Then $A \cup B \cup C = \{x \in X : x \in A \text{ or } x \in B \text{ or } x \in C\}$ and $A \cap B \cap C = \{x \in X : x \in A \text{ and } x \in B \text{ and } x \in C\}$. While the union and intersection of three sets makes sense, the set difference of three sets does not. In order to answer this question, we would need to reduce it to a set difference of two sets by including parentheses. For example, you can define the following set differences: $(A \setminus B) \setminus C$ and $A \setminus (B \setminus C)$ (try it!). Work out what these last two sets are when A, B , and C are as in Exercise 6.10.

Spotlight: Paradoxes

You may already have seen paradoxes in mathematics. For example, you may have seen Zeno's paradoxes, the most famous of which is the story of Achilles and the tortoise, in your calculus class. Another well-known paradox comes from the following: what is the sum of

$$1 - 1 + 1 - 1 + 1 - \dots?$$

You might argue that this sum should be $(1 - 1) + (1 - 1) + \dots = 0$. Or, you might just as well argue that this sum should be $1 + (-1 + 1) + (-1 + 1) + \dots = 1$. You might even argue (as Luigi Guido Grandi did [27, p. 135]) that since the sums 0 and 1 are equally probable, the answer should be the average of 0 and 1; in other words, $1/2$. This paradox forces us to look closely at exactly what we mean by summing infinitely many numbers.

Bertrand Russell pointed out a paradox in set theory. He also presented a popular form of this paradox, called the barber problem. The problem is the following. Suppose there is a town with one barber, and this barber says that he shaves those people, and only those, who do not shave themselves. The question is: Who shaves the barber? (You'll recognize the set theoretic form of this problem in Exercise 6.3.)

Paradoxes serve a very useful purpose. They point out where the foundations of mathematics are shaky (or even faulty!). To learn more about them, and how they

have been handled, we recommend reading [26, Chapter 15], [57, Chapter 18], or [59, Chapter 51].

Problems

Problem 6.1. “Order” the following sets, using the appropriate symbol from among $=, \subseteq, \subset$:

$$\mathbb{N}, \mathbb{R}, \mathbb{Z}^+, \mathbb{Z}, \mathbb{Q}.$$

Problem[#] 6.2. Let A, B , and C be sets. Prove that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$. (We say that set containment is transitive.)

Problem 6.3. Recall that \mathbb{N} denotes the set of natural numbers, \mathbb{Z} the set of integers, and \mathbb{R} the set of real numbers.

- Write the phrase “ x belongs to \mathbb{R} ” in symbols.
- Write the phrase “ \mathbb{Z} is a proper subset of \mathbb{R} ” in symbols.
- Write the phrase “If x is an element of \mathbb{Z} , then x or $-x$ is an element of \mathbb{N} ” in symbols.
- Use set notation to describe the set of squares of all multiples of 3.

Problem 6.4. In this problem our universe is \mathbb{R} , the set of real numbers.

- Give an example of subsets A and B of \mathbb{R} that are disjoint.
- Give an example of subsets A and B of \mathbb{R} that are not disjoint and find $A \setminus B$ and $B \setminus A$.
- Give an example of subsets A and B of \mathbb{R} such that $A \subseteq B$.
- Give an example of subsets A, B , and C of \mathbb{R} such that

$$A \cup (B \cap C) \neq (A \cup B) \cup (A \cup C).$$

Problem 6.5. The universe in this problem is \mathbb{R} . Let A be the closed interval $[0, 2]$ and let B be the closed interval $[-1, 1]$. Find $A \setminus B$, $B \setminus A$, A^c , B^c , $A^c \cap B^c$, $(A \cup B)$, and $(A \cup B)^c$.

Problem 6.6. Find an expression for each of the shaded sets in the Venn diagrams of [Figure 6.4](#).

Problem 6.7. (a) Consider the set S of nonzero real numbers. Write S in set notation.

- Define a new “multiplication” on this set by $x \heartsuit y = x/y$. If $x, y \in S$, is $x \heartsuit y \in S$? Is there an element $y \in S$ such that $x \heartsuit y = x$ for all $x \in S$?
- Repeat parts (a) and (b), replacing the set S by the set T of negative real numbers.
- Repeat parts (a) and (b), replacing the set S by the set V of nonzero rational numbers.

Problem 6.8. Define two sets A and B as follows: $A = \{(2n + 1)^3 : n \in \mathbb{Z}\}$ and $B = \{2n + 1 : n \in \mathbb{Z}\}$.

- (a) Prove that $A \subset B$.
- (b) Suppose we redefine A and B , replacing \mathbb{Z} by \mathbb{R} ; in other words, let $A = \{(2n + 1)^3 : n \in \mathbb{R}\}$ and $B = \{2n + 1 : n \in \mathbb{R}\}$. What is the relation between these two sets? State and prove your answer.

Problem 6.9. Find an expression for each of the shaded sets in the Venn diagrams of Figure 6.5.

Problem 6.10. Is the following statement true or false: $\{\emptyset\} = \emptyset$? Why?

Problem 6.11. Show that $\{x \in \mathbb{R} : x^2 - 1 = 0\} = \{1, -1\}$.

Problem 6.12. Let $A = \{x \in \mathbb{Z} : 6 \text{ divides } x\}$, $B = \{x \in \mathbb{Z} : 21 \text{ divides } x\}$, and $C = \{x \in \mathbb{Z} : 42 \text{ divides } x\}$. Prove that $A \cap B = C$.

Problem 6.13. Let $A = \{(x, y) \in \mathbb{R}^2 : x - y = 0\}$, $B = \{(x, y) \in \mathbb{R}^2 : x + y = 0\}$, and $C = \{(x, y) \in \mathbb{R}^2 : x^2 - y^2 = 0\}$. Prove that $A \cup B = C$.

Problem 6.14. Let $A = \mathbb{Z}$, $B = \{x \in \mathbb{Z} : x = 2n + 5 \text{ for some } n \in \mathbb{Z}\}$ and, $C = \{x \in \mathbb{Z} : x = -2m \text{ for some } m \in \mathbb{Z}\}$. Prove that $A \setminus B = C$.

Problem 6.15. Let S be the set of nonzero real numbers. Define a new “addition” on this set by $x \# y = x + y + 1$. If you add two numbers in S , do you end up with a number in S ? (In other words, if $x, y \in S$, is $x \# y \in S$?)

Problem 6.16. Prove that $A = B$ in each of the following.

- (a) Let A and B be the sets defined by $A = \{x \in \mathbb{R} : \sin(\pi x) = 0\}$ and $B = \mathbb{Z}$.
- (b) Let $x \in \mathbb{R}$. Define $A = \{(ax + b)/(cx + d) : a, b, c, d \in \mathbb{Z} \text{ and } cx + d \neq 0\}$ and $B = \{(px + q)/(rx + s) : p, q, r, s \in \mathbb{Q} \text{ and } rx + s \neq 0\}$.

Problem 6.17. Let $A = \{x \in \mathbb{R} : ax^2 + bx + c = 0 \text{ for some integers } a, b, \text{ and } c, \text{ with at least one of } a, b, c \text{ nonzero}\}$ and let $B = \{x \in \mathbb{R} : px^2 + qx + r = 0 \text{ for some rational numbers } p, q, \text{ and } r, \text{ with at least one of } p, q, r \text{ nonzero}\}$.

- (a) Prove that $2 \in A$.



Fig. 6.4

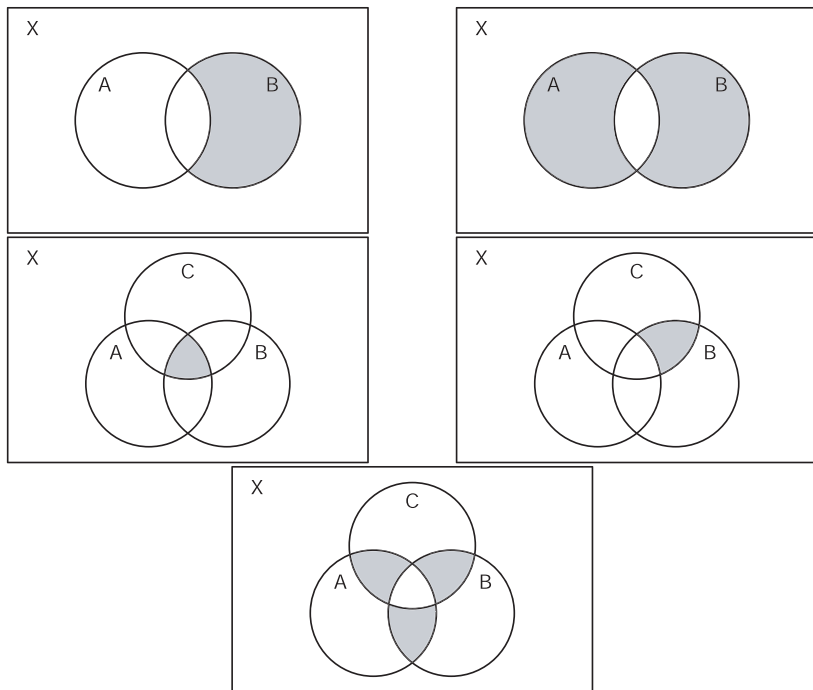


Fig. 6.5

- (b) Prove that $\sqrt{2} \in A$.
- (c) Give an example of a real number y such that $y \notin A$. (You do not need to prove that $y \notin A$.)
- (d) Prove that $A = B$.
- (e) Prove that $\mathbb{Q} \subseteq A$.

The following problems deal with sets of points in the plane. We remind you of the notation introduced in Chapter 4. The set of all points in the plane is denoted by $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$. Subsets of \mathbb{R}^2 will be studied in more generality in Chapter 9.

Problem 6.18. Define a set A by $A = \{(x, y) \in \mathbb{R}^2 : y \neq 0\}$.

- (a) Give a geometric description of A .
- (b) Suppose we tell you that if you have two elements of this set A , you can “add” them according to the following rule:

$$(x, y) \diamond (z, w) = (xw + zy, wy).$$

The symbol $+$ here denotes usual addition. Show that the object that results when we add two elements of our set A is again an object in our set A .

- (c) Continuing, find an element (a, b) in A such that $(a, b) \diamond (x, y) = (x, y)$ for every (x, y) in A .
- (d) This “new” addition probably looks somewhat odd to you, but you have seen it before. What is it?

Problem 6.19. In each part of this problem, two sets, A and B , are defined. Prove that $A \subseteq B$ in each of the following:

- (a) $A = \{x^2 : x \in \mathbb{Z}\}$ and $B = \mathbb{Z}$;
 (b) $A = \mathbb{R}$ and $B = \{2x : x \in \mathbb{R}\}$;
 (c) $A = \{(x, y) \in \mathbb{R}^2 : y = (5 - 3x)/2\}$ and $B = \{(x, y) \in \mathbb{R}^2 : 2y + 3x = 5\}$.

Problem 6.20. Prove that $\{n^2 + n + 1 : n \in \mathbb{N}\} \subseteq \{2n + 1 : n \in \mathbb{N}\}$.

Problem 6.21. Let

$$A = \{x \in \mathbb{N} : x < x^2 \text{ and for all } y \in \mathbb{Z}, \text{ if } y|x, \text{ then } y^2|x\}.$$

Prove that $A = \emptyset$.

Problem 6.22. Prove that one set is a proper subset of the other one in each of the following:

- (a) $A = \{(x, y) \in \mathbb{R}^2 : xy > 0\}$ and $B = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 > 0\}$;
 (b) $A = \emptyset$ and $B = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 0\}$.

Problem 6.23. Consider the sets

$$A = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\} \text{ and } B = \{(x, y) \in \mathbb{R}^2 : |x| + |y| \leq 1\}.$$

Is one of the two sets properly contained in the other one? Justify your answer.

Problem 6.24. Define the following three sets:

$$\begin{aligned} A &= \{(x, y) \in \mathbb{R}^2 : xy > 0\}; \\ B &= \{(x, y) \in \mathbb{R}^2 : y > |x|\}; \\ C &= \{(x, y) \in \mathbb{R}^2 : 0 < x < y\}. \end{aligned}$$

Carefully prove that $A \cap B = C$.

Chapter 7

Operations on Sets

By an operation on sets we mean the construction of a new set from the given ones. As we saw in the last chapter, these new sets may be formed using unions, intersections, set differences, or complements of given sets. In this section, we will look at many important properties of operations on sets. We end the chapter with a summarizing list of identities. In the exercises and problems you will be given the opportunity to prove the most important ones and then commit them to memory, so you don't have to re-prove them every time you need them.

The Venn diagrams introduced in the previous chapter can be helpful in deciding what is true and what is false, and they can be part of understanding the problem. If the arrangement of your sets in the diagram is a so-called “typical” one (see [103]), it is even possible to use the Venn diagram as a proof. However, in this text, we (and you) will use Venn diagrams to guide us, but we will write our proofs without relying on them. When you prove these properties you may not always need to start from the definition. Sometimes you can use what you know, and once you have proven everything in Theorem 7.4, you will know a lot.

The first theorem is a good example of a proof in cases. It keeps things tidy. Now remember, if we use the definition to show two sets A and B are equal, then we must show that if $x \in A$, then $x \in B$ and if $x \in B$, then $x \in A$.

Theorem 7.1 (The distributive property). *Let A, B , and C be sets. Then*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Before reading the proof, let's use Pólya's method.

“*Understanding the problem.*” Draw two Venn diagrams representing the left and right sides of the equality above. Each diagram will have three sets, appropriately labeled A, B , and C . Shade in the area described by the left side of the equation in one diagram and then shade the right side in the other diagram. They should look the same. While this should convince you that you are on the right track, it is not enough to convince someone else.

“*Devising a plan.*” We wish to show that two sets are equal. Using the definition of equality of sets, we know that we must show two things. The first thing to show

is that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. So our first line will begin

$$\text{If } x \in A \cup (B \cap C),$$

and our last line (for this part of the proof) will look like

$$\text{Thus } x \in (A \cup B) \cap (A \cup C).$$

Now we just have to figure out how to get from the first line to the last one. Let's fill in some things, making sure that each line follows logically from the previous one. Working down from the top we get

$$x \in A \cup (B \cap C),$$

$$x \in A \text{ or } x \in B \cap C,$$

and working up from the bottom leads to

$$x \in A \cup B \text{ and } x \in A \cup C,$$

$$x \in (A \cup B) \cap (A \cup C).$$

Looking at what we are missing in our proof suggests that we use a proof in cases; one that depends on whether $x \in A$ or $x \in B \cap C$.

Once we are done with the proof above, we must show that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. We use the same method to devise our plan for a proof of this set containment: We write down our first line and look to see where it takes us. Then we'll write down our last line and try to figure out how to get there. That leads to

$$x \in (A \cup B) \cap (A \cup C),$$

$$x \in A \cup B \text{ and } x \in A \cup C,$$

[stuff]

$$x \in A \text{ or } x \in B \cap C,$$

$$x \in A \cup (B \cap C).$$

It looks like if $x \in A$, we have our proof. But what if $x \notin A$? This again suggests a proof in cases; one that depends on whether $x \in A$ or $x \notin A$. If you see what to do now, you can write up the proof. If you still do not see what to do, continue using this method until you see the solution.

Once you see the solution, fill in the missing steps and write the proof up carefully using complete sentences, as we do below.

Proof. If $x \in A \cup (B \cap C)$, then $x \in A$ or $x \in B \cap C$. Suppose first that $x \in A$. Then $x \in A \cup B$ and $x \in A \cup C$. In this first case, we see that $x \in (A \cup B) \cap (A \cup C)$. Now suppose that $x \in B \cap C$. Then $x \in B$ and $x \in C$. Since $x \in B$, we see that $x \in A \cup B$. Since we also have $x \in C$, we see that $x \in A \cup C$. Therefore, $x \in (A \cup B) \cap (A \cup C)$

in this case as well. In both cases $x \in (A \cup B) \cap (A \cup C)$ and we may conclude that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

To complete the proof, we must now show that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. So if $x \in (A \cup B) \cap (A \cup C)$, then $x \in A \cup B$ and $x \in A \cup C$. It is, once again, helpful to break this into two cases, since we know that $x \in A$ or $x \notin A$. Now if $x \in A$, then $x \in A \cup (B \cap C)$. If $x \notin A$, then the fact that $x \in A \cup B$ implies that x must be in B . Similarly, the fact that $x \in A \cup C$ implies that x must be in C . Therefore, $x \in B \cap C$. Hence $x \in A \cup (B \cap C)$. In both cases $x \in A \cup (B \cap C)$ and we may conclude that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Since we proved containment in both directions we may conclude that the two sets are equal. \square

Look at the proof above. It has complete sentences, variables are identified, we know when we are in one case and then the other, and we know when the proof is complete. You should use the form as a model, but remember that each proof will be unique.

The following theorem involves an “if and only if” statement. Remember that an “if and only if” statement requires that you prove *both* the “if” *and* the “only if.”

Theorem 7.2. *Let A and B be sets. Then $A \cup B = A$ if and only if $B \subseteq A$.*

Proof. First we’ll show that if $A \cup B = A$, then $B \subseteq A$. So assume $A \cup B = A$. If $x \in B$, then $x \in A \cup B$. Using the assumption that $A \cup B = A$ we have $x \in A$. This shows that $B \subseteq A$.

Now we will prove that if $B \subseteq A$, then $A \cup B = A$. So let us assume that $B \subseteq A$. We must show that $A \cup B \subseteq A$ and $A \subseteq A \cup B$. To prove the first containment, we have that if $x \in A \cup B$, then $x \in A$ or $x \in B$. If $x \in A$, then x is where it needs to be and we have nothing more to prove. If $x \in B$, then we use the assumption that $B \subseteq A$ to conclude that $x \in A$. In both cases we get $x \in A$ and therefore have $A \cup B \subseteq A$. To prove the second containment, let $x \in A$. Then $x \in A \cup B$ and we conclude that $A \subseteq A \cup B$. Together we have proven that $A \cup B = A$. \square

The structure of the proof of Theorem 7.2 is more complicated than the proof of the distributive property. First, as we said above, there are two things to prove: the “if” and the “only if.” Next, both of these statements have hypotheses and conclusions. In each case, you must be aware of what you are assuming and what you are proving. What’s even more important, though, is that you *use* what you are assuming to get to your desired conclusion. If you don’t use your assumption, then your original statement was poorly constructed, you proved more than you thought you did, or your proof was in error. In fact, in the proof above, we did not use our assumption that $B \subseteq A$ to prove $A \subseteq A \cup B$. Did we make an error, or did we prove more than we said we did?

Now that you have seen two examples of how to write such a proof, it is time for you to try it by yourself. Try proving one of the two DeMorgan’s laws below.

Exercise 7.3. Let A and B be subsets of the set X . Then

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B).$$

- (a) Devise your plan. (Include a Venn diagram.)
 (b) Write up your proof. ○

We now give the promised list of some of the properties of set operations. We proved three of them above. In the problems you will be asked to work more of the proofs.

Theorem 7.4. *Let X denote a set, and $A, B,$ and C denote subsets of X . Then*

1. $\emptyset \subseteq A$ and $A \subseteq A$.
2. $(A^c)^c = A$.
3. $A \cup \emptyset = A$.
4. $A \cap \emptyset = \emptyset$.
5. $A \cap A = A$.
6. $A \cup A = A$.
7. $A \cap B = B \cap A$. (*Commutative property*)
8. $A \cup B = B \cup A$. (*Commutative property*)
9. $(A \cup B) \cup C = A \cup (B \cup C)$. (*Associative property*)
10. $(A \cap B) \cap C = A \cap (B \cap C)$. (*Associative property*)
11. $A \cap B \subseteq A$.
12. $A \subseteq A \cup B$.
13. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. (*Distributive property*)
14. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. (*Distributive property*)
15. $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$. (*DeMorgan's law*)
 (When X is the universe we also write $(A \cup B)^c = A^c \cap B^c$.)
16. $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$. (*DeMorgan's law*)
 (When X is the universe we also write $(A \cap B)^c = A^c \cup B^c$.)
17. $A \setminus B = A \cap B^c$.
18. $A \subseteq B$ if and only if $(X \setminus B) \subseteq (X \setminus A)$.
 (When X is the universe we also write $A \subseteq B$ if and only if $B^c \subseteq A^c$.)
19. $A \subseteq C$ and $B \subseteq C$ if and only if $A \cup B \subseteq C$.
20. $C \subseteq A$ and $C \subseteq B$ if and only if $C \subseteq A \cap B$.
21. $A \cup B = A$ if and only if $B \subseteq A$.
22. $A \cap B = B$ if and only if $B \subseteq A$.

Many results can be proved using the methods demonstrated thus far in this chapter. Once you have proven these statements, though, it is a good idea to use them in other proofs. Practice using the results in Theorem 7.4 in the next exercise.

Exercise 7.5. Let $A, B,$ and C be sets. Prove the following using relevant statements from Theorem 7.4: If $C^c \subseteq B$, then $(A \setminus B) \cup C = C$. ○

Definition

Definition 7.1 (for Problems 7.6 through 7.10). The **symmetric difference** of sets A and B is the set $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Solutions to Exercises

Solution (7.3). First we show that

$$X \setminus (A \cup B) \subseteq (X \setminus A) \cap (X \setminus B).$$

If $x \in X \setminus (A \cup B)$, then $x \notin A \cup B$. Therefore $x \notin A$ and $x \notin B$. Consequently, $x \in X \setminus A$ and $x \in X \setminus B$. Thus $x \in (X \setminus A) \cap (X \setminus B)$. We conclude that $X \setminus (A \cup B) \subseteq (X \setminus A) \cap (X \setminus B)$.

We now show that

$$(X \setminus A) \cap (X \setminus B) \subseteq X \setminus (A \cup B).$$

If $x \in (X \setminus A) \cap (X \setminus B)$, then $x \in X \setminus A$ and $x \in X \setminus B$. Thus, $x \in X$ and $x \notin A$, and $x \in X$ and $x \notin B$. So, $x \in X$ and $x \notin A$ and $x \notin B$. This implies that $x \in X$ and $x \notin A \cup B$. Therefore, $x \in X \setminus (A \cup B)$, and we see that $(X \setminus A) \cap (X \setminus B) \subseteq X \setminus (A \cup B)$. Thus, the two sets are equal.

Solution (7.5). Since $C^c \subseteq B$, statements 18 and 2 of Theorem 7.4 imply $B^c \subseteq C$, and thus $B^c \cup C = C$ by statement 19 of the same theorem. The rest of the proof now follows from the following string of equalities (numbers indicate the relevant statements from Theorem 7.4):

$$\begin{aligned} (A \setminus B) \cup C &= (A \cap B^c) \cup C && \text{(by 17)} \\ &= (A \cup C) \cap (B^c \cup C) && \text{(by 8 and 13)} \\ &= (A \cup C) \cap C && \text{(since } B^c \cup C = C \text{ as shown)} \\ &= C && \text{(by 8, 12, and 20).} \end{aligned}$$

Problems

In all the problems below, X denotes a set; A, B , and C denote subsets of X .

Problem 7.1. In this problem we refer to statements of Theorem 7.4.

- Prove statement 2.
- Prove statement 14.
- Prove statement 16.
- Prove statement 18.

- (e) Prove statement 20.
- (f) Prove statement 22.

Problem 7.2. Prove that $A \cap B = \emptyset$ if and only if $B \subseteq (X \setminus A)$.

Problem 7.3. Prove that $A = B$ if and only if $(X \setminus A) = (X \setminus B)$. Make sure you use statements from Theorem 7.4 rather than going back to the definition.

Problem 7.4. Prove the following using the results stated in Theorem 7.4:

- (a) $(A \cup B) \cap B = B$;
- (b) $(A \cap B) \cup B = B$.

Problem 7.5. Show that $(A \setminus B) \cup (B \cap A^c) = (A \cup B) \setminus (B \cap A)$ in two different ways, by completing the two parts below.

- (a) Prove this equality using only the definition of set containment.
- (b) Using theorems from the text, give a different proof of the equality above. If you use a result that has a name, state the name of the result.

Problem 7.6. Draw the Venn diagram for the symmetric difference $A \Delta B$ of two sets A and B and prove that

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Problem 7.7. For sets A and B prove the following.

- (a) $A \Delta A = \emptyset$;
- (b) $A \Delta \emptyset = A$;
- (c) $A \Delta B = B \Delta A$. (The symmetric set difference is commutative.)

Problem 7.8. Prove that for sets A , B , and C , we have $(A \Delta B) \Delta C = A \Delta (B \Delta C)$. (The symmetric set difference is associative.)

Problem 7.9. Prove that for sets A and B , we have $A \Delta B = A \setminus B$ if and only if $B \subseteq A$.

Problem 7.10. Prove that for sets A and B , we have $(A \cup B) \Delta (A \cap B) = A \Delta B$.

Problem 7.11. Sketch Venn diagrams of the set on the left and the set on the right side of the equation

$$(A \setminus (B \cap C)) \cup (B \setminus C) = (A \cup B) \setminus (B \cap C).$$

Once you have done that, prove that the equality above holds.

Problem 7.12. Consider the following sets:

- (i) $A \setminus (A \cup B \cup C)$,
- (ii) $A \setminus A \cap B \cap C$,
- (iii) $A \cap B^c \cap C^c$,
- (iv) $A \setminus (B \cup C)$, and
- (v) $(A \setminus B) \cap (A \setminus C)$.

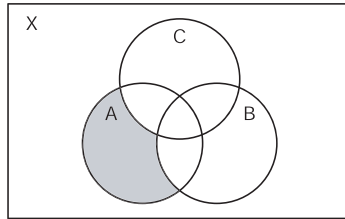


Fig. 7.1

- (a) Which of the sets above are written ambiguously, if any?
- (b) Of the ones that make sense, which of the sets above agree with the shaded set in Figure 7.1?
- (c) Prove that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Problem 7.13. Consider the following sets:

- (i) $(A \cap B) \setminus (A \cap B \cap C)$,
- (ii) $A \cap B \setminus (A \cap B \cap C)$,
- (iii) $A \cap B \cap C^c$,
- (iv) $(A \cap B) \setminus C$, and
- (v) $(A \setminus C) \cap (B \setminus C)$.

- (a) Which of the sets above are written ambiguously, if any?
- (b) Of the sets above that make sense, which ones equal the set sketched in Figure 7.2?
- (c) Prove that $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$.

Problem# 7.14. In this problem you will prove that the union of two sets can be rewritten as the union of two disjoint sets.

- (a) Prove that the two sets $A \setminus B$ and B are disjoint.
- (b) Prove that $A \cup B = (A \setminus B) \cup B$.

Problem 7.15. Prove that $A^c \cup B^c = X$ if and only if A and B are disjoint.

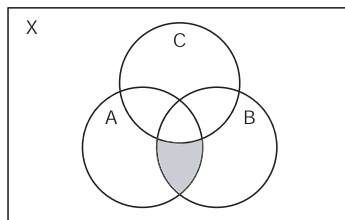


Fig. 7.2

Problem 7.16. Prove that $(A \setminus B) \cup (B \setminus C) \subseteq A \setminus C$ if and only if $A \cap C \subseteq A \cap B$ and $B \cap C^c \subseteq A$.

Problem 7.17. Prove or disprove: If $A \cup B = A \cup C$, then $B = C$.

Problem 7.18. Prove or give a counterexample for the following statement.

Let X be the universe and $A, B \subseteq X$. If $A \cap Y = B \cap Y$ for all $Y \subseteq X$, then $A = B$.

Problem 7.19. Prove that $A \cap (B^c \cap C^c) = \emptyset$ if and only if $A \subseteq B \cup C$.

Problem 7.20. Prove that $(A \cup B) \setminus (C \cup D) = (A \setminus (C \cup D)) \cup (B \setminus (C \cup D))$.

Chapter 8

More on Operations on Sets

Most of what we did in the last two chapters was concerned with operations on two sets. In Exercise 6.14 we defined unions and intersections of three sets. In general, we may have two or three sets, as many sets as there are integers, or even more sets than that. We'll need a new definition and special notation. In this chapter, we will introduce the notation that will allow us to keep track of these sets. Unfortunately, a rigorous definition will have to wait until Chapter 14.

Let n be a positive integer and suppose that we have sets A_1, A_2, \dots, A_n . How can we talk about the union of these n sets? the intersection? For example, when we have three sets, if we write $\bigcup_{j=1}^3 A_j = A_1 \cup A_2 \cup A_3$, we would be referring to the set of x in our universe that lie in at least one of our sets, A_1, A_2 , or A_3 . Of course, there is nothing special about three sets; that is, for every positive integer, n , we can write

$$\bigcup_{j=1}^n A_j = A_1 \cup A_2 \cup \dots \cup A_n \text{ and } \bigcap_{j=1}^n A_j = A_1 \cap A_2 \cap \dots \cap A_n.$$

The first set would be the set of all x in the universe that lie in at least one of the A_j for $j = 1, 2, \dots, n$, while the second would be the set of x that lie in all of the sets A_j . If we have a set A_j for each positive integer j and we want to take the union and intersection over all positive integers, then we write

$$\bigcup_{j=1}^{\infty} A_j = A_1 \cup A_2 \cup \dots \text{ and } \bigcap_{j=1}^{\infty} A_j = A_1 \cap A_2 \cap \dots.$$

This is probably a good time to look at some examples.

Example 8.1. We can write the union in different ways. For example,

$$\bigcup_{j=1}^{10} [0, j] = [0, 1] \cup [0, 2] \cup \dots \cup [0, 10] = [0, 10].$$

Similarly,

$$\bigcap_{j=1}^{10} [0, j] = [0, 1] \cap [0, 2] \cap \cdots \cap [0, 10] = [0, 1].$$

○

In Example 8.1, we had unions and intersections of finitely many sets (ten, to be precise). We now take a look at what can happen when we take unions and intersections of even more sets.

Example 8.2. (a) For each $q \in \mathbb{Z}^+$ define the set $A_q = \{p/q : p \in \mathbb{Z}\}$. These sets can be used to define the union $\bigcup_{q \in \mathbb{Z}^+} A_q$.

(b) This time we define, for each $i \in \mathbb{N}$, the set $B_i = \{p/3^i, p \in \mathbb{Z}\}$. These sets may be used to define the intersection $\bigcap_{i \in \mathbb{N}} B_i$. ○

Exercise 8.3. Write the sets $\bigcup_{j=1}^{\infty} [j, j+1]$ and $\bigcap_{j=1}^{\infty} [j, j+1]$ in their simplest form, by listing the first few sets in the union or intersection until the pattern is established, and then stating your guess. (You don't have to prove that your guess is correct.) ○

Let X denote our universe and let \mathcal{A} be a collection of subsets of X . Then the **union of the collection** and **intersection of the collection** are defined just as you might expect: The union is defined by

$$\bigcup_{A \in \mathcal{A}} A = \{x \in X : x \in A \text{ for some } A \in \mathcal{A}\}$$

and, for a nonempty collection \mathcal{A} , the intersection by

$$\bigcap_{A \in \mathcal{A}} A = \{x \in X : x \in A \text{ for all } A \in \mathcal{A}\}.$$

In some situations, it will be helpful to label our sets. We often label objects in real life; for example, we label runners in order of their finish in a race. Why not do this with sets? We could label the set we think of first as A_1 , the runner-up would be set A_2 , and so on. Sometimes this is possible, as in Example 8.2 above, but other times it is not. For example, sometimes we do not know how many sets we have and other times we will have so many sets that it is impossible to tell which “came first.” While this may seem odd, it happens all the time.

So again let X be our universe and suppose we have a set I . Suppose further that for each $\alpha \in I$ there is a unique set $A_\alpha \subseteq X$ corresponding to it. The set I is called an **index set**, each $\alpha \in I$ is called an **index**, and the set $\{A_\alpha : \alpha \in I\}$ is called an **indexed set** or an indexed collection. Thus, an index set is a set that labels the members of another set \mathcal{A} . We may also write $\{A_\alpha\}_{\alpha \in I}$ for an indexed collection of sets.

In this setting, our definition of union and intersection will look a bit different from the one presented above. So recall the notation: X denotes our universe and we let $\{A_\alpha : \alpha \in I\}$ be an indexed collection of sets with $A_\alpha \subseteq X$ for all α in an index set I . Then the union of the indexed collection $\{A_\alpha : \alpha \in I\}$ is just

$$\bigcup_{\alpha \in I} A_\alpha = \{x \in X : x \in A_\alpha \text{ for some } \alpha \in I\},$$

and for $I \neq \emptyset$, the intersection of the indexed collection $\{A_\alpha : \alpha \in I\}$ is

$$\bigcap_{\alpha \in I} A_\alpha = \{x \in X : x \in A_\alpha \text{ for all } \alpha \in I\}.$$

Exercise 8.4. Find the simplest way to describe the following sets (you may find sketches helpful):

- (a) $\bigcup_{x \in \mathbb{R}^+} (0, x)$;
- (b) $\bigcup_{n \in \mathbb{N}} [0, n]$;
- (c) $\bigcap_{n \in \mathbb{N}} [0, n]$. ○

Note that the index notation and the general definition of union and intersection given here include the cases in Chapter 6 and the ones we mentioned in the beginning of this chapter. For instance, if $I = \{1, 2\}$, then $\bigcap_{i \in I} A_i = A_1 \cap A_2$.

Some more practice with this notation will probably be very helpful at this point.

- Exercise 8.5.** (a) Write $\bigcup_{j=0}^\infty [0, j]$ using an appropriate index set.
 (b) Write $\bigcup_{j=1}^\infty (0, j)$ using an appropriate index set. ○

Some sets are more easily described with index notation, others without such notation. Let's go back and look at the sets in Example 8.2.

Example 8.6. Consider the indexed collection of sets $\{A_q\}_{q \in \mathbb{Z}^+}$ defined in Example 8.2 (a). Then $\bigcup_{q \in \mathbb{Z}^+} A_q = \mathbb{Q}$.

Proof. If $x \in \bigcup_{q \in \mathbb{Z}^+} A_q$, then $x \in A_q$ for some $q \in \mathbb{Z}^+$. Thus, there exist $q \in \mathbb{Z}^+$ and $p \in \mathbb{Z}$ such that $x = p/q$. Hence $x \in \mathbb{Q}$, and we have shown that $\bigcup_{q \in \mathbb{Z}^+} A_q \subseteq \mathbb{Q}$.

Conversely, if $x \in \mathbb{Q}$, then $x = p/q$ for some $p, q \in \mathbb{Z}$ with $q \neq 0$. Now (for reasons that you will explain) we may choose q so that $q > 0$. For this q we have $q \in \mathbb{Z}^+$ and therefore $x \in A_q$. Hence $x \in \bigcup_{q \in \mathbb{Z}^+} A_q$. So, $\mathbb{Q} \subseteq \bigcup_{q \in \mathbb{Z}^+} A_q$, and therefore $\bigcup_{q \in \mathbb{Z}^+} A_q = \mathbb{Q}$. □

Example 8.7. Consider the indexed collection of sets $\{B_i\}_{i \in \mathbb{N}}$ defined in Example 8.2 (b). We claim that $\bigcap_{i \in \mathbb{N}} B_i = \mathbb{Z}$.

Proof. If $x \in \bigcap_{i \in \mathbb{N}} B_i$, then $x \in B_i$ for all $i \in \mathbb{N}$. In particular, $x \in B_0$. Therefore $x = p/3^0 = p$ for some $p \in \mathbb{Z}$. So $x \in \mathbb{Z}$, and thus $\bigcap_{i \in \mathbb{N}} B_i \subseteq \mathbb{Z}$.

Now let $x \in \mathbb{Z}$. For each $i \in \mathbb{N}$, we may write $x = (3^i x)/3^i$. Of course, $3^i x \in \mathbb{Z}$, since $x \in \mathbb{Z}$. Hence $x \in B_i$ for all $i \in \mathbb{N}$. This shows that $x \in \bigcap_{i \in \mathbb{N}} B_i$ and therefore $\mathbb{Z} \subseteq \bigcap_{i \in \mathbb{N}} B_i$.

Combining the two arguments we obtain the desired equality, $\bigcap_{i \in \mathbb{N}} B_i = \mathbb{Z}$. □

Exercise 8.8. What's the difference between "an infinite union of sets" and "a union of infinite sets"? Give an example of each, showing how these two phrases differ. (While we haven't given a rigorous definition of infinite here, your intuition should suffice to solve this problem.) ○

You already know that one of DeMorgan's laws for two sets can be stated as

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B).$$

This can be rephrased in words as "the complement of a union is the intersection of the complements." DeMorgan's laws do not depend on the number of sets that we have, and that is the point of the next exercise.

Exercise 8.9. Show that the general DeMorgan's laws hold: For every universe X , nonempty index set I , and indexed collection of sets $\{A_\alpha : \alpha \in I\}$, we have

- (i) $X \setminus \bigcup_{\alpha \in I} A_\alpha = \bigcap_{\alpha \in I} (X \setminus A_\alpha)$ and
 (ii) $X \setminus \bigcap_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I} (X \setminus A_\alpha)$. ○

Exercise 8.10. Suppose $A_\alpha \subseteq B$ for each $\alpha \in I$. Show that $\bigcup_{\alpha \in I} A_\alpha \subseteq B$. ○

Definitions

Definition 8.1. Let X denote the universe and \mathcal{A} a collection of subsets of X . Then the **union of the collection** is defined as

$$\bigcup_{A \in \mathcal{A}} A = \{x \in X : x \in A \text{ for some } A \in \mathcal{A}\}.$$

Definition 8.2. Let X denote the universe and \mathcal{A} a nonempty collection of subsets of X . Then the **intersection of the collection** is defined as

$$\bigcap_{A \in \mathcal{A}} A = \{x \in X : x \in A \text{ for all } A \in \mathcal{A}\}.$$

Definition 8.3. A set I is called an **index set for a set** \mathcal{A} , if for each $\alpha \in I$ there is an element $A_\alpha \in \mathcal{A}$ corresponding to α , and every element in \mathcal{A} is labeled in this way.

Definition 8.4. Given an index set I and corresponding sets A_α that are defined for each $\alpha \in I$, the set $\{A_\alpha : \alpha \in I\}$ is said to be an **indexed set** or **indexed collection** of sets.

Definition 8.5 (for Problem 8.18). A collection of sets \mathcal{A} is said to be **pairwise disjoint** if the following is satisfied: For all $X, Y \in \mathcal{A}$, if $X \cap Y \neq \emptyset$, then $X = Y$.

Solutions to Exercises

Solution (8.3). You can see that $\bigcup_{j=1}^{\infty} [j, j+1] = [1, 2] \cup [2, 3] \cup [3, 4] \cup \dots = [1, \infty)$ and $\bigcap_{j=1}^{\infty} [j, j+1] = [1, 2] \cap [2, 3] \cap [3, 4] \cap \dots = \emptyset$.

Solution (8.4). You can check the following:

- (a) $\bigcup_{x \in \mathbb{R}^+} (0, x) = (0, \infty)$;
- (b) $\bigcup_{n \in \mathbb{N}} [0, n] = [0, \infty)$;
- (c) $\bigcap_{n \in \mathbb{N}} [0, n] = \{0\}$.

Solution (8.5). You can check the following:

- (a) $\bigcup_{j=0}^{\infty} [0, j] = \bigcup_{j \in \mathbb{N}} [0, j]$;
- (b) $\bigcup_{j=1}^{\infty} (0, j) = \bigcup_{j \in \mathbb{Z}^+} (0, j)$.

Solution (8.8). An infinite union of sets would mean that we take the union over infinitely many sets (but the sets themselves may be finite); in other words, the index set is infinite. For example, $\bigcup_{n \in \mathbb{N}} \{n\}$ would be an infinite union of (finite) sets. On the other hand, a union of infinite sets would mean that the sets themselves must be infinite (while the index set may be finite). For example, the union of the even integers, $2\mathbb{Z}$, with the odd integers, $2\mathbb{Z} + 1$, would be a union of two infinite sets.

Solution (8.9). We will show part (i) and will leave part (ii) for you to do. So we need to show that

$$X \setminus \left(\bigcup_{\alpha \in I} A_{\alpha} \right) = \bigcap_{\alpha \in I} (X \setminus A_{\alpha}).$$

If $x \in X \setminus \left(\bigcup_{\alpha \in I} A_{\alpha} \right)$, then $x \in X$ and $x \notin \bigcup_{\alpha \in I} A_{\alpha}$. By the definition of union this means that $x \in X$ and $x \notin A_{\alpha}$ for every $\alpha \in I$. Hence, $x \in X \setminus A_{\alpha}$ for all $\alpha \in I$, and therefore $x \in \bigcap_{\alpha \in I} (X \setminus A_{\alpha})$. Thus, $X \setminus \left(\bigcup_{\alpha \in I} A_{\alpha} \right) \subseteq \bigcap_{\alpha \in I} (X \setminus A_{\alpha})$.

Now if $x \in \bigcap_{\alpha \in I} (X \setminus A_{\alpha})$, then $x \in X \setminus A_{\alpha}$ for all $\alpha \in I$. This implies that $x \in X$ and $x \notin A_{\alpha}$ for every $\alpha \in I$. Hence, we have $x \in X$ and $x \notin \bigcup_{\alpha \in I} A_{\alpha}$. It follows that $x \in X \setminus \left(\bigcup_{\alpha \in I} A_{\alpha} \right)$ and thus $\bigcap_{\alpha \in I} (X \setminus A_{\alpha}) \subseteq X \setminus \left(\bigcup_{\alpha \in I} A_{\alpha} \right)$.

The two subset relations give the desired equality between the sets.

Solution (8.10). If $x \in \bigcup_{\alpha \in I} A_{\alpha}$, then there exists α_0 such that $x \in A_{\alpha_0}$. Since we suppose that $A_{\alpha_0} \subseteq B$, we know that $x \in B$. Thus $\bigcup_{\alpha \in I} A_{\alpha} \subseteq B$.

Problems

Problem 8.1. For positive integers n , consider the intervals of real numbers given by $A_n = [0, 1/n)$, $B_n = [0, 1/n]$, and $C_n = (0, 1/n)$.

- (a) Find $\bigcup_{n=1}^{\infty} A_n$, $\bigcup_{n=1}^{\infty} B_n$, and $\bigcup_{n=1}^{\infty} C_n$.
- (b) Find $\bigcap_{n=1}^{\infty} A_n$, $\bigcap_{n=1}^{\infty} B_n$, and $\bigcap_{n=1}^{\infty} C_n$.
- (c) Does $\bigcup_{n \in \mathbb{N}} A_n$ make sense? Why or why not?

Problem 8.2. If $A_x = [-x, x]$, find $\bigcup_{x \in \mathbb{R}^+} A_x$ and $\bigcap_{x \in \mathbb{R}^+} A_x$.

Problem 8.3. Find simpler notation for the two sets

$$A = \bigcup_{j=0}^{\infty} [j, j+1] \quad \text{and} \quad B = \bigcap_{j \in \mathbb{Z}} (\mathbb{R} \setminus (j, j+1)).$$

Problem 8.4. Let I be a nonempty index set and suppose that $B \subseteq A_\alpha$ for all $\alpha \in I$. Show that $B \subseteq \bigcap_{\alpha \in I} A_\alpha$.

Problem 8.5. Let $I \neq \emptyset$ and $\{A_\alpha : \alpha \in I\}$ be an indexed collection. Prove that for all $\beta \in I$

$$\bigcap_{\alpha \in I} A_\alpha \subseteq A_\beta \subseteq \bigcup_{\alpha \in I} A_\alpha.$$

Problem 8.6. Prove or give a counterexample: Let $\{A_n : n \in \mathbb{Z}^+\}$ and $\{B_n : n \in \mathbb{Z}^+\}$ be two indexed collections of sets. If $A_n \subset B_n$ for all $n \in \mathbb{Z}^+$, then

$$\bigcap_{n=1}^{\infty} A_n \subset \bigcap_{n=1}^{\infty} B_n.$$

(Recall that $A \subset B$ means strict inclusion; that is, $A \subseteq B$ and $A \neq B$.)

Problem 8.7. Let I be a set and let $\{A_\alpha : \alpha \in I\}$, and $\{B_\alpha : \alpha \in I\}$ be two indexed collections of sets such that $A_\alpha \subseteq B_\alpha$ for all $\alpha \in I$. Prove that

$$\bigcup_{\alpha \in I} A_\alpha \subseteq \bigcup_{\alpha \in I} B_\alpha.$$

Problem 8.8. Prove the following set inclusion.

$$\bigcup_{b \in \mathbb{R}^+} \{(x, y) \in \mathbb{R}^2 : x + y = b\} \subseteq \bigcap_{s \in \mathbb{R}^-} \{(x, y) \in \mathbb{R}^2 : x + y > s\}.$$

Problem 8.9. For $n \in \mathbb{Z}^+$ define

$$A_n = \{x \in \mathbb{R} : \frac{1}{n} < x \leq 2\} \quad \text{and} \quad B_n = \{x \in \mathbb{R} : 0 < x < \frac{3}{n} + 2\}.$$

Prove that $\bigcup_{n \in \mathbb{Z}^+} A_n \subseteq \bigcap_{n \in \mathbb{Z}^+} B_n$.

Problem 8.10. Let I and J be nonempty sets such that $J \subseteq I$, and let $\{A_\alpha : \alpha \in I\}$ be an indexed collection. Prove that

- (a) $\bigcup_{\alpha \in J} A_\alpha \subseteq \bigcup_{\alpha \in I} A_\alpha$ and
- (b) $\bigcap_{\alpha \in I} A_\alpha \subseteq \bigcap_{\alpha \in J} A_\alpha$.

Problem 8.11. Let $\{A_r : r \in \mathbb{R}\}$ and $\{B_r : r \in \mathbb{R}\}$ be two indexed collections of sets. Prove that

$$\left(\bigcap_{r \in \mathbb{R}} A_r\right) \cup \left(\bigcap_{r \in \mathbb{R}} B_r\right) \subseteq \bigcap_{r \in \mathbb{R}} (A_r \cup B_r).$$

Provide an example showing that this inclusion can be proper.

Problem# 8.12. Let I be a nonempty set, $\{A_\alpha : \alpha \in I\}$ an indexed collection of sets, and let B be a set.

(a) Prove the distributive property:

$$\left(\bigcup_{\alpha \in I} A_\alpha\right) \cap B = \bigcup_{\alpha \in I} (A_\alpha \cap B).$$

(b) State and prove a distributive property for $(\bigcap_{\alpha \in I} A_\alpha) \cup B$.

Problem# 8.13. Suppose that $\{A_\alpha : \alpha \in I\}$ is a nonempty indexed collection of subsets of a set X .

- (a) If $A_{\alpha_0} = \emptyset$ for some $\alpha_0 \in I$, prove that $\bigcap_{\alpha \in I} A_\alpha = \emptyset$.
- (b) If $A_{\alpha_0} = X$ for some $\alpha_0 \in I$, prove that $\bigcup_{\alpha \in I} A_\alpha = X$.

Problem 8.14. Define

$$A = \mathbb{R} \setminus \bigcap_{n \in \mathbb{Z}^+} (\mathbb{R} \setminus \{-n, -n+1, \dots, 0, \dots, n-1, n\}).$$

The set A should be familiar to you. Guess what it is and then prove that your guess is correct.

Problem 8.15. Guess a simpler way to express the set A defined as

$$A = \mathbb{Q} \setminus \bigcap_{n \in \mathbb{Z}} (\mathbb{R} \setminus \{2n\}),$$

and then prove that your guess is correct.

Problem 8.16. Suppose that X is a set with more than one element. What is $\bigcup_{x \in X} \{x\}$? What is $\bigcap_{x \in X} \{x\}$?

Problem 8.17. For every $\alpha \in \mathbb{R}$ and for every $m, n \in \mathbb{Z}^+$ define

$$A_\alpha = \{x \in \mathbb{Z}^+ : x < \alpha\} \quad \text{and} \quad B_{mn} = \{x \in \mathbb{R} : |x - m| < \frac{1}{n}\}.$$

Prove that

$$\bigcup_{\alpha \in \mathbb{R}} A_\alpha \subseteq \bigcup_{m \in \mathbb{Z}^+} \left(\bigcap_{n \in \mathbb{Z}^+} B_{mn}\right).$$

Problem# 8.18. A collection of sets \mathcal{A} is said to be **pairwise disjoint** if the following is satisfied: For all $X, Y \in \mathcal{A}$, if $X \cap Y \neq \emptyset$, then $X = Y$.

A comment about this definition may be in order: Speaking informally, a collection of sets is pairwise disjoint if whenever we choose two sets from the collection, they are disjoint or they are equal.

- Give an example of a pairwise disjoint collection of infinitely many sets.
- What is the contrapositive of “if $X \cap Y \neq \emptyset$, then $X = Y$ ”?
- What is the converse of “if $X \cap Y \neq \emptyset$, then $X = Y$ ”?
- If \mathcal{A} is a pairwise disjoint collection of sets, does the assertion you found in (b) hold for all $X, Y \in \mathcal{A}$?
- If the assertion that you found in (b) holds for all X and Y in some set \mathcal{A} , is \mathcal{A} a pairwise disjoint collection of sets?
- Suppose that \mathcal{B} is a pairwise disjoint collection of sets. Can we conclude that $\bigcap_{X \in \mathcal{B}} X = \emptyset$?
- Suppose that $\bigcap_{X \in \mathcal{B}} X = \emptyset$. Is \mathcal{B} necessarily a pairwise disjoint collection of sets?

Problem 8.19. For $n \in \mathbb{N}$ we define $A_n = \{x \in \mathbb{N} : \frac{n}{2} - 1 < x \leq \frac{n}{2}\}$. We use these sets for two collections of sets: $\mathcal{A} = \{A_n : n \in \mathbb{N}\}$ and $\mathcal{B} = \{A_n : n \in 2\mathbb{N}\}$ (where $2\mathbb{N}$ denotes the set of even nonnegative integers).

- Is the collection \mathcal{A} pairwise disjoint? Prove or give a counterexample.
- Is the collection \mathcal{B} pairwise disjoint? Prove or give a counterexample.
- Is \mathcal{A} contained in \mathcal{B} ? Are the sets equal?

Problem 8.20. An indexed collection of sets $\{A_n : n \in \mathbb{Z}^+\}$ is said to be *increasing* if $A_n \subseteq A_{n+1}$ for each $n \in \mathbb{Z}^+$. The indexed collection is said to be *strictly increasing* if $A_n \subset A_{n+1}$ for each $n \in \mathbb{Z}^+$.

- Give an example of an increasing indexed collection of sets (consisting of subsets of \mathbb{R}) that is not strictly increasing.
- Find an increasing indexed collection of sets $\{A_n : n \in \mathbb{Z}^+\}$ (consisting of subsets of \mathbb{R}) such that $\bigcup_{n \in \mathbb{Z}^+} A_n = [0, 1]$ and $\bigcap_{n \in \mathbb{Z}^+} A_n = \{0\}$.
- Find a strictly increasing indexed collection of sets $\{B_n : n \in \mathbb{Z}^+\}$ (consisting of subsets of \mathbb{R}) such that $\bigcup_{n \in \mathbb{Z}^+} B_n = [0, 1]$.

Problem 8.21. Find an example of an indexed collection of sets $\{A_j : j \in \mathbb{Z}^+\}$ such that $A_{j+1} \subset A_j$ for each $j \in \mathbb{Z}^+$, and $\bigcap_{j=1}^{\infty} A_j \neq \emptyset$.

Chapter 9

The Power Set and the Cartesian Product

Now that we know about sets, we can construct some new ones from old ones in even more ways than we did before. In this section we look closely at two special sets: the first is called the power set, and the second is called the Cartesian product of two sets.

Let S be a set. Then the **power set** of S is the set of all subsets of S . We shall denote the power set by $\mathcal{P}(S)$. When working with the power set, the following observation will be extremely useful: $A \in \mathcal{P}(S)$ if and only if $A \subseteq S$.

Before we begin, note that the power set is again a set and its elements are also sets. The power set is never empty. Why?

Example 9.1. Consider the set $S = \{0, 1\}$. We look for all subsets of S . They are \emptyset , $\{0\}$, $\{1\}$, and $\{0, 1\}$. Then the power set of S is $\mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$. \circ

As you probably noticed, the notation is tricky here. You have to distinguish very carefully between “element of” (\in) and “subset of” (\subseteq). Until you get really good at this distinction, we suggest that you ask yourself each time you use \in or \subseteq whether you chose the correct symbol. It’s time for some practice with this notation.

Exercise 9.2. Let A be a set. Which of the following are true, which are false? Explain.

- (a) $A \in \mathcal{P}(A)$;
- (b) $\emptyset \subseteq \mathcal{P}(A)$;
- (c) $\emptyset = \mathcal{P}(\emptyset)$;
- (d) $\{\emptyset\} = \mathcal{P}(\emptyset)$;
- (e) if $a \in A$, then $\{a\} \subseteq \mathcal{P}(A)$.

Now we are ready to explore the power set construction further.

Exercise 9.3. Let $A = \{1, 2, 3\}$, $B = \{2, 5\}$, $C = \{0, 1\}$.

- (a) Find $\mathcal{P}(B)$ and $\mathcal{P}(C)$. Do these two sets have elements in common?
- (b) Find $\mathcal{P}(A)$, $\mathcal{P}(B)$, $\mathcal{P}(A \cap B)$, and $\mathcal{P}(A \cup B)$.

(c) Compute $\mathcal{P}(A) \cup \mathcal{P}(B)$ and $\mathcal{P}(A) \cap \mathcal{P}(B)$. ○

Remember to use element notation when you are thinking of the set as an element and subset notation when you are showing containment of sets.

In the next exercise, we will ask you to prove that two sets are equal. We've done this many times in the previous chapters, and so you know one way to begin: use an element-chasing argument. Ask yourself if your set plays the role of a set or the role of an element, and use the corresponding notation.

Exercise 9.4. Let A and B be sets. Prove that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$. ○

When we talk about a set, it is understood that if we discuss the set $\{1, 3\}$ we are discussing the set $\{3, 1\}$ as well. A set is determined by its elements and there is no notion of order associated with what we have defined so far. When there is an order, such as when we plot points and need to know which is the x coordinate and which is the y coordinate, we use the notion of an ordered pair. The next set we will consider is called the Cartesian product of two sets X and Y , and it is constructed using ordered pairs.

Here is our informal definition: An **ordered pair** (x, y) is a pair of objects in which there is a first object x and a second object y . The very important property of ordered pairs is that $(x, y) = (z, w)$ if and only if $x = z$ and $y = w$.

We may now define the **Cartesian product** of X and Y , denoted $X \times Y$, to be the set of all ordered pairs in which the first element comes from X and the second from Y ; that is,

$$X \times Y = \{(x, y) : x \in X, y \in Y\}.$$

For example, if $X = [0, 1]$ and $Y = [0, 2]$, then

$$X \times Y = \{(x, y) : 0 \leq x \leq 1, 0 \leq y \leq 2\}.$$

This is the rectangle in \mathbb{R}^2 with base along the interval $[0, 1]$ and height along the interval $[0, 2]$ sketched in [Figure 9.1](#).

Perhaps you are wondering why we said “informal definition” when we presented our definition of ordered pair. Since this is probably the definition you were expecting, it most likely looks formal. It turns out that there is a rigorous definition of ordered pair; one that can be presented without referring to the “first” and “second” coordinates. The reason we do not present it here is that, in our opinion, a rigorous definition is mostly confusing rather than helpful at this point. If you have a strong desire to know more about this, you can work Problem 9.23 in this chapter.

It's time for a few more examples of Cartesian products.

Exercise 9.5. (a) Write out all the elements in $\{0, 1\} \times \{2, 3\}$ and $\{2, 3\} \times \{0, 1\}$.
 (b) Sketch the Cartesian products $[0, 1] \times [2, 3]$ and $[2, 3] \times [0, 1]$ as sets of points in the plane.

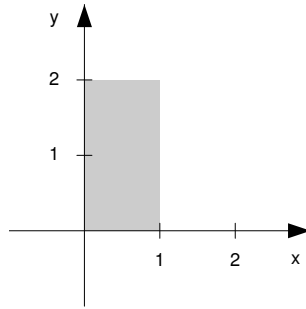


Fig. 9.1 $[0, 1] \times [0, 2]$

- (c) Recall that we defined $\mathbb{R}^2 = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\}$. Write \mathbb{R}^2 using the Cartesian product notation.
- (d) Having done that, can you describe \mathbb{R}^3 as a Cartesian product of two sets? (You might have more than one description that seems reasonable to you.)
- (e) The set of even integers is denoted by $2\mathbb{Z}$ (see Example 6.1). Make sketches that describe the sets $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times 2\mathbb{Z}$, and $2\mathbb{Z} \times \mathbb{Z}$. ○

When we prove that two sets defined using Cartesian products are equal, we can still use the method of “element-chasing.” Remember that we need to use the special form of the element, namely, that it looks like an ordered pair. If you don’t use the form of an element, you may lose valuable information and, as a consequence, proving your result will be tougher than it has to be. As you read the proofs below, pay attention to where we use the fact that the element we consider is an ordered pair.

Theorem 9.6. *Let A be a set. Then $A \times \emptyset = \emptyset$.*

Proof. Suppose, to the contrary, that $A \times \emptyset \neq \emptyset$. Then there exists an element $(x, y) \in A \times \emptyset$. Therefore, by our definition of Cartesian product, $x \in A$ and $y \in \emptyset$. But this contradicts the fact that \emptyset is the empty set. Thus $A \times \emptyset = \emptyset$. □

Theorem 9.7. *Let A, B, C , and D be sets. Then*

$$(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D).$$

Proof. If $z \in (A \times B) \cup (C \times D)$, then $z = (x, y)$ where $(x, y) \in A \times B$ or $(x, y) \in C \times D$. Suppose first that $(x, y) \in A \times B$. Then $x \in A$ and $y \in B$. In this case $x \in A \cup C$ and $y \in B \cup D$, so by definition $(x, y) \in (A \cup C) \times (B \cup D)$. Now suppose that $(x, y) \in C \times D$. Then $x \in C$ and $y \in D$. Therefore $x \in A \cup C$ and $y \in B \cup D$. So $(x, y) \in (A \cup C) \times (B \cup D)$. Hence $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$, as desired. □

Again, notice how quickly we changed from z to (x, y) in the proof. That’s because we can’t do anything if we don’t realize that z is really an ordered pair.

Now consider the following nontheorem.

Nontheorem. Let A, B, C , and D be sets. Then

$$(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D).$$

Not a proof. If $(x, y) \in (A \cup C) \times (B \cup D)$, then $x \in A \cup C$ and $y \in B \cup D$. Thus $x \in A$ or $x \in C$, and $y \in B$ or $y \in D$. Hence $x \in A$ and $y \in B$ or $x \in C$ and $y \in D$. So $(x, y) \in A \times B$ or $(x, y) \in C \times D$. Thus $(x, y) \in (A \times B) \cup (C \times D)$. \square

Exercise 9.8. Find the error in the nonproof above and show that Nontheorem 9 really is not a theorem because the statement is false. (Find sets for which the statement does not hold.) \circ

In these problems and all that follow, you will begin with an element in your set. It will be helpful to you to think about the form of your element. Is it a set? an ordered pair? If you rush through these proofs, as we did in Nontheorem 9, you will prove things that are false. This is generally frowned upon in mathematics. Go slowly, be careful, and check each step.

We will now define relations. We will soon see that there is a connection between functions (something you probably feel familiar with) and relations (something you may not feel terribly familiar with). We begin with a definition.

Suppose that X and Y are two sets. A **relation from X to Y** is a subset of $X \times Y$. A relation from X to X is called a **relation on X** .

Exercise 9.9. For the following, decide whether or not they are relations from a set X to a set Y . If they are, say what X is and what Y is. Then describe each set pictorially (as a set of points in the plane) or in words:

- (a) $\{(x, y) \in \mathbb{R}^2 : x \leq y\}$;
- (b) $\{x/y : x, y \in \mathbb{Z} \text{ and } y \neq 0\}$;
- (c) $\{(x, y) \in \mathbb{R}^2 : x, y \in \mathbb{Z} \text{ and } x + y = 0\}$. \circ

We will learn more about relations in Chapter 10.

Definitions

Definition 9.1. The **power set** of a set S is the set of all subsets of S . It is denoted by $\mathcal{P}(S)$.

Definition 9.2 (see **Problem 9.23 for a formal definition**). The **ordered pair** of the objects x and y is the object (x, y) in which x is considered to be the first object and y the second object.

Definition 9.3. The **Cartesian product** of sets X and Y is the set of ordered pairs $X \times Y = \{(x, y) : x \in X, y \in Y\}$.

Definition 9.4. A **relation from a set X to a set Y** is a subset of $X \times Y$. If $Y = X$, we say the relation is a **relation on X** .

Solutions to Exercises

Solution (9.2).

- (a) True. We have $A \subseteq A$ and thus $A \in \mathcal{P}(A)$.
- (b) True (e.g., by Theorem 6.11).
- (c) False. Since $\emptyset \subseteq \emptyset$ we get $\emptyset \in \mathcal{P}(\emptyset)$ and thus $\mathcal{P}(\emptyset) \neq \emptyset$.
- (d) True. See the argument for (c) and note that if $B \subseteq \emptyset$, then $B = \emptyset$.
- (e) False. Here is a counterexample: Let $A = \{0\}$, then $\mathcal{P}(A) = \{\emptyset, \{0\}\}$ and $0 \in A$ but $\{0\} \notin \mathcal{P}(A)$.

Solution (9.3).

- (a) $\mathcal{P}(B) = \{\emptyset, \{2\}, \{5\}, \{2, 5\}\}$, $\mathcal{P}(C) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$, and the empty set is an element of both sets.
- (b) You can check that $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$ and $\mathcal{P}(A \cap B) = \{\emptyset, \{2\}\}$. We leave $\mathcal{P}(A \cup B)$ to you.
- (c) $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset, \{2\}\}$. We leave $\mathcal{P}(A) \cup \mathcal{P}(B)$ to you.

Solution (9.4). If $x \in \mathcal{P}(A \cap B)$, then $x \subseteq A \cap B$. Thus $x \subseteq A$ and $x \subseteq B$. This implies that $x \in \mathcal{P}(A)$ and $x \in \mathcal{P}(B)$, so $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Since x was an arbitrarily chosen element, $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$. Each of these steps is reversible, so the containment $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$ follows as well.

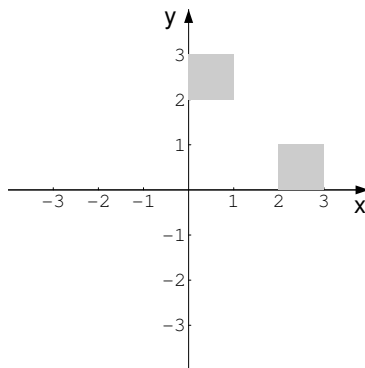


Fig. 9.2 $[0, 1] \times [2, 3]$ and $[2, 3] \times [0, 1]$

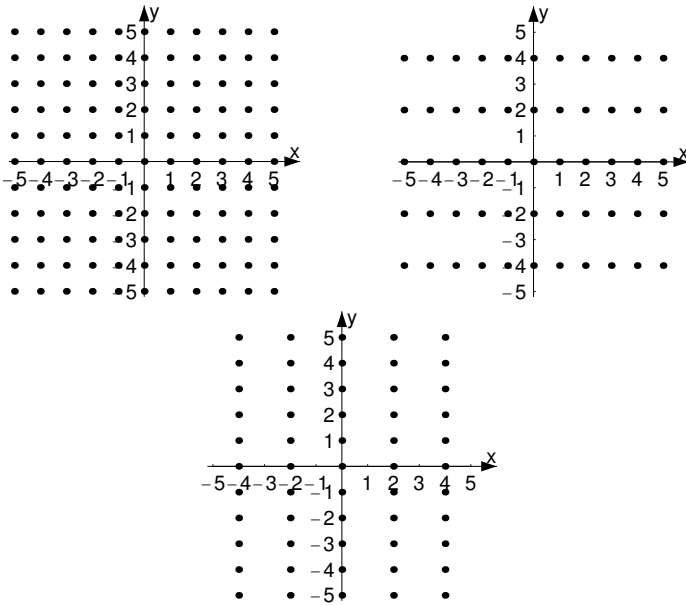


Fig. 9.3 $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times 2\mathbb{Z}$, and $2\mathbb{Z} \times \mathbb{Z}$

Solution (9.5).

(a) The two sets are

$$\{0, 1\} \times \{2, 3\} = \{(0, 2), (0, 3), (1, 2), (1, 3)\}$$

and

$$\{2, 3\} \times \{0, 1\} = \{(2, 0), (3, 0), (2, 1), (3, 1)\}.$$

(b) The two sets are sketched in [Figure 9.2](#).

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

(d) One answer might be $\mathbb{R}^2 \times \mathbb{R}$.

(e) These are sketched in [Figure 9.3](#).

Solution (9.8). Our “Not a proof” claims that “ $x \in A$ or $x \in C$, and $y \in B$ or $y \in D$. Hence $x \in A$ and $y \in B$ or $x \in C$ and $y \in D$.” This conclusion is not justified: it could also be that $x \in A$ and $y \in D$, or $x \in C$ and $y \in B$.

As an example, let $A = D = \emptyset$ and $B = C = \mathbb{R}$. Then $(A \cup C) \times (B \cup D) = \mathbb{R} \times \mathbb{R}$, while $(A \times B) \cup (C \times D) = \emptyset$.

Solution (9.9).

(a) This is a relation from $X = \mathbb{R}$ to $Y = \mathbb{R}$, consisting of the set of points in \mathbb{R}^2 lying above or on the line $y = x$.

- (b) This is not a subset of $X \times Y$ for any choice of X and Y , hence this is not a relation.
- (c) This is a relation from $X = \mathbb{Z}$ to $Y = \mathbb{Z}$, and consists of the points for which x is an integer and $y = -x$; that is, this is the set $\{(x, -x) : x \in \mathbb{Z}\}$.

Problems

Problem 9.1. Let $S = \{a, b, c\}$. Find $\mathcal{P}(S)$.

Problem 9.2. Replace ? by the proper symbol, choosing from among the following: $\in, \subseteq, \text{ or } \subset$.

- (a) $\mathbb{N} ? \mathbb{Z}$;
- (b) $\{1, 2, 3\} ? \mathbb{Z}$;
- (c) $\{5\} ? \mathbb{Z}$;
- (d) $\mathbb{Z}^+ ? \mathcal{P}(\mathbb{Z})$;
- (e) $\{1, 2, 3\} ? \mathcal{P}(\{1, 2, 3\})$;
- (f) $5 ? \mathbb{Z}$;
- (g) $\emptyset ? \mathbb{Z}$;
- (h) $\emptyset ? \mathcal{P}(\mathbb{Z})$.

Problem 9.3. Give an explicit description of $\mathcal{P}(\mathcal{P}(\{1\}))$ by listing all its elements.

Problem 9.4. Say whether the following are true or false and give a reason for your answer.

- (a) $\{\emptyset\} \subseteq A$ for all sets A .
- (b) $\emptyset \subset \mathcal{P}(A)$ for all sets A .
- (c) If $A = \{x, y\}$, then $\mathcal{P}(A) = \{\{x\}, \{y\}, \{x, y\}, \{\emptyset\}\}$.
- (d) If $A = \{x, y\}$, $\mathcal{P}(\{A\}) = \{\{x\}, \{y\}, \{x, y\}, \emptyset\}$.
- (e) If $A_0 = \{\emptyset\}$, then $A_0 \in \mathcal{P}(A)$ for all sets A .

Problem 9.5. (a) Show that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

(b) Show that $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$ in general, by exhibiting two concrete sets, A and B , for which the aforementioned inequality holds.

Problem 9.6. (a) Let X be a nonempty set in $\mathcal{P}(A \setminus B)$. Must $X \in \mathcal{P}(A) \setminus \mathcal{P}(B)$?

(b) Prove that it is never the case that $\mathcal{P}(A \setminus B) = \mathcal{P}(A) \setminus \mathcal{P}(B)$.

Problem 9.7. Let $2\mathbb{Z}$ denote the even integers and $2\mathbb{Z} + 1$ denote the odd integers. What is $\mathcal{P}(2\mathbb{Z}) \cap \mathcal{P}(2\mathbb{Z} + 1)$?

Problem 9.8. Show that $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Problem 9.9. For every set I and for every indexed collection of sets $\{A_\alpha : \alpha \in I\}$, prove that

$$\bigcup_{\alpha \in I} \mathcal{P}(A_\alpha) \subseteq \mathcal{P}\left(\bigcup_{\alpha \in I} A_\alpha\right).$$

Problem 9.10. Let $\{A_\alpha : \alpha \in I\}$ be a nonempty indexed collection of sets. Prove that $\mathcal{P}\left(\bigcap_{\alpha \in I} A_\alpha\right) = \bigcap_{\alpha \in I} \mathcal{P}(A_\alpha)$.

Problem 9.11. How many elements are there in the power set of $\{1, 2, 3, 4\}$? How many elements are in the power set of $\{1, 2, 3, 4, 5\}$? State a general result. You'll be able to prove it later.

Problem 9.12. Describe the following relations pictorially (as a set of points in the plane) or in words:

- (a) $\{(x, y) \in \mathbb{N} \times \mathbb{Z} : x \geq y\}$;
- (b) $\{(x, y) \in \mathbb{R}^2 : x = y\}$;
- (c) $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x + y \in 2\mathbb{Z}\}$;
- (d) $\{0, 1\} \times \mathbb{N}$;
- (e) $\{(x, x^2) : x \in \mathbb{R}\}$;
- (f) $\{(\sqrt{x}, x) : x \in \mathbb{Z}^+\}$.

Problem 9.13. Describe the following Cartesian products:

- (a) $\emptyset \times \mathbb{N}$;
- (b) $\mathbb{Z} \times \emptyset$;
- (c) $\mathbb{R} \times \mathbb{R}$;
- (d) $\mathbb{R} \times \mathbb{Z}$.

Problem 9.14. Which of the following sets can be written as the Cartesian product of two subsets of \mathbb{R} ? (Either give the two sets or explain why two such sets do not exist.)

- (a) $\{(x, y) : 0 \leq y \leq 5\}$;
- (b) $\{(x, y) : x > y\}$;
- (c) $\{(x, y) : x^2 + y^2 = 1\}$.

Problem 9.15. Show that $\mathbb{N} \times \mathbb{N} \subseteq \mathbb{Z} \times \mathbb{Z}$.

Problem 9.16. (a) In the plane, sketch the set $[0, 1] \times ([1, 3] \cup [2, 4])$.

(b) Sketch $([0, 1] \cup [1, 4]) \times ([0, 1] \cup [2, 4])$.

Problem 9.17. Let A , B , C , and D be nonempty sets. Then $A \times B = C \times D$ if and only if $A = C$ and $B = D$.

- (a) Prove this statement.
- (b) One of the two implications does not require the sets to be nonempty. Which one?
- (c) If we do not require the sets to be nonempty, then the statement is false. Give examples of sets A, B, C , and D to show the necessity of the assumption that the sets be nonempty.

Problem 9.18. Suppose A, B, C , and D are four sets. If $A \times B \subseteq C \times D$, must $A \subseteq C$ and $B \subseteq D$? Why or why not?

Problem 9.19. Let A, B , and C be sets. If the statements below are true, prove them. If they are false, give a counterexample:

- (a) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
- (b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Problem 9.20. Let $A = \{1, \{1\}, \{1, \{1\}\}\}$.

- (a) Find $A \times A$.
- (b) Find $A \cap \mathcal{P}(A)$.

Problem 9.21. Let $A = \{0, 1\}$. We define a relation R from A to the power set of A by $R = \{(x, y) \in A \times \mathcal{P}(A) : x \in y\}$. List all elements of R .

Problem 9.22. Let $\{A_\alpha : \alpha \in I\}$ and $\{B_\beta : \beta \in J\}$ be two indexed collections with nonempty index sets I and J . Prove that

$$\bigcap_{\alpha \in I} \left(\bigcup_{\beta \in J} (A_\alpha \times B_\beta) \right) = \left(\bigcap_{\alpha \in I} A_\alpha \right) \times \left(\bigcup_{\beta \in J} B_\beta \right).$$

Problem 9.23. This problem introduces rigorous definitions of an ordered pair and Cartesian product. Let A be a set and $a, b \in A$. We define the ordered pair of a and b with first coordinate a and second coordinate b as

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Using this definition prove the following.

- (a) If $(a, b) = (x, y)$, then $a = x$ and $b = y$.
- (b) If $a \in A$ and $b \in B$, then $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$.

Now we are able to define the Cartesian product of the two sets A and B as the set

$$A \times B = \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) : x = (a, b) \text{ for some } a \in A \text{ and some } b \in B\}.$$

- (c) Using the definitions introduced in this problem, prove that if $A \subseteq C$ and $B \subseteq D$, then $A \times B \subseteq C \times D$.

This is a pretty complicated definition. It is also not our idea, but rather an idea that was born from axioms. P. Halmos's book, [41], is an excellent reference for this subject.

Tips on Writing Mathematics

This letter is longer than usual simply because I could not spare the time to make it shorter.—Blaise Pascal, [80, p. 865]¹

After this point in the course the work will change. You'll find that you are writing more in words than in symbols. How you write is as important as what you write. Here are some things to think about as you write your proofs.

- In mathematics, it is always important that the reader know what the variables stand for. This was true in algebra in high school, geometry, and calculus, and it is true here too. If you use symbols—any symbols—make sure the meaning is clear to the reader *before* you use them.
- Think about your notation, and choose notation that is easy on the reader.
- A variable should only be assigned one meaning in your proof. For example, if you used C to denote the complex numbers, don't use C again to denote a different set.
- Try for a good blend of symbols and words. Don't juxtapose unrelated symbols if you don't have to. For example, consider the sentence "So $1 \leq p, q \geq 2$." You might find this confusing and (unnecessarily) difficult to read. If we say "So $1 \leq p$ and $q \geq 2$," the sentence is clear. It's often easier to read things if you put a word, even a little one, between symbols.
- Avoid starting a sentence with a symbol. This often confuses the reader unnecessarily. For example, consider the following sentence.

Thus $x \in A$. A is a subset of B .

First, the $A.A$ just doesn't look nice. Second, it's hard to read.

- Every sentence should start with a capital letter and end with a period, just like sentences are supposed to begin and end.
- All grammatical rules apply. Make sure your sentence has a noun and a verb, for example.
- Strive for clarity. Always keep the reader in mind. If something follows from a definition, say so. The reader will appreciate this and will know what you are thinking *and*, what's more, you will know why what you say is true. If something follows from Theorem 10.1, say so. It is extremely important for you to be aware of when you are using a result. For one thing, it means that you are more likely to notice if you are using a result that you do not have. (This would be wrong. Don't do it.) For another, it helps the reader who may not fully understand what you are doing.
- Certain phrases are particularly helpful in guiding a reader through your proof. For example, "Suppose to the contrary, ..." tells the reader that your proof will be done by contradiction. As a second example, if you are proving "A if and only if B," your reader will understand everything better if you say, "Suppose A. ... Then we have B." And then say, "Suppose B. ... Then we have A." You should

¹ The translation is ours.

alert the reader to a proof that will be in cases, or a proof that will proceed using the contrapositive. You should not only tell the reader how you will begin the proof, you should also tell the reader when you believe you have completed the proof. Words like “thus, we have established the desired result” will let the reader know that you think you are done now and it’s his or her turn to understand why. Other examples of phrases that you may use to guide your reader will come up as we learn new techniques.

- If you can find a shorter, clearer solution, do so.
- Perhaps the most difficult thing about writing a proof is to find a balance between the main ideas in the proof and the details. You’ll often find that the more you explain, the more you hide the main ideas. On the other hand, if you don’t explain enough, you might overlook an important detail or confuse your reader. It’s not easy to strike the right balance. This is why we suggest waiting a bit, and then rereading your proof. If you can’t figure out why you did something, it’s unlikely that someone else will.
- If you have a partner in the class, it is an excellent idea to exchange papers and see if things are clear to each of you. (Check with your teacher to make sure this is allowed, of course.)

Exercise 9.10. Here’s a student’s proof of the following theorem: Let x and y be real numbers. Show that $xy \leq x^2/2 + y^2/2$.

Proof (Student version).

$$\begin{aligned}(x - y)^2 &\geq 0 \\ x^2 - 2xy + y^2 &\geq 0 \\ x^2 + y^2 &\geq 2xy \\ x^2/2 + y^2/2 &\geq xy\end{aligned}\quad \square$$

Criticize the student’s solution and rewrite the proof, paying close attention to the tips presented here. ○

Example 9.11 (Adapting an idea of [112]). If you are trying to publish a paper, you should think carefully about your exposition. Strive for clarity. Here’s an example of how to improve mathematical writing:

Theorem (Steiner’s Theorem I). *Given any triangle, there is a unique ellipse inscribed in the triangle that passes through the midpoints of the sides of the triangle and is tangent to the sides of the triangle at these three midpoints.*

Let’s see. We’ve used the word “triangle” four times. Let’s try to eliminate that repetition.

Theorem (Steiner’s Theorem II). *Given any triangle T , there is a unique ellipse inscribed in T that passes through the midpoints of the sides of T and is tangent to the sides of T at these three midpoints.*

Now, if the ellipse is tangent to the sides of T , then it must pass through those points as well. So, it looks like that's a phrase we can omit. Let's try it.

Theorem (Steiner's Theorem III). *Given a triangle T , there is a unique ellipse inscribed in T that is tangent to each of the sides of T at the three midpoints.*

This looks simpler than our previous statement. Is there anything else we can do to shorten this? Well, yes. Yes there is. The "unique ellipse inscribed in T " is too wordy. If we say that the ellipse is tangent to each of the sides of T at the midpoints, then T must be the circumscribing triangle. Now, do we really have to say "three" midpoints? One argument in favor of "three" is that the reader will immediately see that we are talking about all possible midpoints. But we've got that covered: we said "tangent to each of the sides." So how about:

Theorem (Steiner's Theorem IV). *Given a triangle T , there is a unique inscribed ellipse that is tangent to each of the sides of T at the midpoints.*

Is this the shortest possible version? If a convex figure is tangent to each side of a triangle, then it is necessarily "inscribed." Thus we can drop this word, as it does not convey additional information.

Theorem (Steiner's Theorem V). *Given a triangle T , there is a unique ellipse that is tangent to each of the sides of T at the midpoints.*

Is the last statement really the "best" one? It certainly is the shortest. The reader may have to think for a moment before realizing that the ellipse is inscribed. If we state this explicitly rather than implicitly, it will most likely aid the reader. Most statements that we found of this theorem include the word "inscribed," perhaps for this reason. *Shortest* is not necessarily equivalent to *clearest!* In this case, we vote for version IV as the clearest.

Steiner's Theorem is, by the way, a beautiful theorem. You can find a lot about it on the Web by doing a search for "Steiner inellipse" or in the book [2, pp. 52–53].



For other (not necessarily independent) views on writing see [42], [62], and [112].

Chapter 10

Relations

In the last chapter we introduced relations. We will now look at three useful properties of relations.

Recall that “ S is a relation on a set X ” is one way of saying that S is a subset of $X \times X$, and therefore the elements of S are ordered pairs, (x, y) . Many authors write $x \sim y$ rather than $(x, y) \in S$. Sometimes we will write $x \sim y$ and other times we will write $(x, y) \in S$, and this is exactly the same thing. So why do it? Because sometimes one notation is more convenient than the other. Use the next exercise to familiarize yourself with both notations.

Exercise 10.1. Let $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x > y\}$.

- (a) Sketch the set S .
- (b) With this relation is $1 \sim 2$?
- (c) With this relation is $3.5 \sim 2$? ○

At this point, we investigate one more relation that will be familiar to you.

Exercise 10.2. Let X be a nonempty set. We consider the usual set inclusion \subset on the set $\mathcal{P}(X)$.

- (a) Using the ordered pair notation and calling this relation R , describe the set R .
- (b) Give an example of a set X and two sets $A, B \in \mathcal{P}(X)$ such that $A \subset B$.
- (c) Give an example of a set X and two different sets $A, B \in \mathcal{P}(X)$ such that $A \not\subset B$.
- (d) If $A, B \in \mathcal{P}(X)$ with $A \neq B$, can you conclude that $A \subset B$ or $B \subset A$? ○

You will learn more about the relation in Exercise 10.2 above in Chapter 13. We now turn to another important type of relation.

A relation on a set X is said to be **reflexive** if $x \sim x$ for all $x \in X$. The relation is **symmetric** if for all $x, y \in X$, whenever $x \sim y$, then $y \sim x$. Finally, the relation is **transitive** if for all $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$. If a relation is reflexive, symmetric, and transitive, then the relation is said to be an **equivalence relation**.

For the remainder of this chapter, we will look at examples and nonexamples of equivalence relations. There's something to note before we begin. To show that a relation is reflexive, we show that $x \sim x$ for all $x \in X$. But to show it is symmetric, we must choose two arbitrary elements of X , suppose that $x \sim y$, and then show that $y \sim x$. If we don't use the fact that $x \sim y$, we probably haven't done it correctly. Finally, to show that a relation is transitive, we must choose three arbitrary elements, suppose that $x \sim y$ and $y \sim z$, and then show that $x \sim z$. Remember to use your assumptions to show that a relation is symmetric or transitive.

Example 10.3. Define a relation on the real numbers \mathbb{R} by $x \sim y$ if and only if $x - y \in \mathbb{Z}$. Show that this relation is an equivalence relation.

Before we begin to show that this is an equivalence relation, we will do appropriate things to understand this definition. Here are a few examples of pairs that satisfy the relation:

$$3 \sim 4, 0 \sim -2384, 7 \sim 7, \pi \sim \pi + 7, -3.7 \sim 4.3.$$

On the other hand, the following pairs do not satisfy the relation:

$$3 \not\sim 3.5, 0 \not\sim \pi, -3.7 \not\sim 3.7.$$

If you have a sense of what the relation does, you are ready to move on to the proof. (If you don't have a sense of what is happening, look for more examples and nonexamples.)

Proof. To show that this relation is reflexive, let $x \in \mathbb{R}$. Then $x - x = 0$. Since $0 \in \mathbb{Z}$, we see that $x - x \in \mathbb{Z}$. Therefore, $x \sim x$ for all $x \in \mathbb{R}$ and \sim is reflexive.

To show that this relation is symmetric, let $x, y \in \mathbb{R}$. If $x \sim y$, then $x - y \in \mathbb{Z}$. But $y - x = -(x - y) \in \mathbb{Z}$, and therefore $y \sim x$. Hence this relation is symmetric.

To show that this relation is transitive, let $x, y, z \in \mathbb{R}$. If $x \sim y$ and $y \sim z$, then $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$. Now the sum of two integers is an integer and therefore $x - z = (x - y) + (y - z) \in \mathbb{Z}$. In other words, $x \sim z$. Thus \sim is transitive. \square

Exercise 10.4. Let R be a relation on a set X . Write the definition of each of the following in symbolic notation: R is reflexive, symmetric, and transitive on X . Once you have completed this task, negate each of your (symbolic) definitions. \circ

In Example 10.3 it's interesting to try to describe, in words, the set of numbers that are related to 0, $1/2$, π , and x . As is the case with our examples and nonexamples appearing above, we hope that describing these sets will help us to more fully understand this relation.

For 0, we look for $\{x \in \mathbb{R} : x \sim 0\} = \{x \in \mathbb{R} : x - 0 \in \mathbb{Z}\}$. Thus, the set of elements related to 0 is just \mathbb{Z} .

For $1/2$, we look for $\{x \in \mathbb{R} : x \sim 1/2\} = \{x \in \mathbb{R} : x - 1/2 \in \mathbb{Z}\}$. Thus, the set of all elements related to $1/2$ is the set $\{1/2 + k : k \in \mathbb{Z}\}$.

For π , we look for $\{x \in \mathbb{R} : x - \pi \in \mathbb{Z}\}$. Thus, the set of all elements related to π is the set $\{\pi + k : k \in \mathbb{Z}\}$.

In general it appears that for every $x \in \mathbb{R}$, the set of all elements related to x is the set $\{x + k : k \in \mathbb{Z}\}$.

Once we have an equivalence relation on a set X , we define the **equivalence class** of an element $x \in X$ to be the set E_x where $E_x = \{y \in X : x \sim y\}$. It might help to think of equivalence classes as houses. “Being in the household of” is the equivalence relation on the people in the town and the houses form the equivalence classes. Saying the relation is reflexive is the same as saying each person lives in the same house as herself. The fact that the relation is symmetric implies that if Barbara lives in the same house as Bob, then Bob lives in the same house as Barbara. Finally, the fact that the relation is transitive implies that if Louis lives in the same house as Lois and Lois lives in the same house as Lilly, then Louis and Lilly live in the same house. If David, Esther, Florian, and Gregg all live in the house and David is your best friend, you’ll probably call the house David’s house. If Esther is your best buddy, though, you might call it Esther’s house. No matter what you call the house, it’s the same house and the same four people live there. And these are the main things to remember: equivalence classes are nonempty, x is always in the same class as x , if x is in the same class as y , then y is in the same class as x , and if x is in the same class as y and y is in the same class as z , then x and z are in the same class. When x and y are in the class, you might call the class E_x or you might call it E_y ; either way, it will be the same class, as we will show more precisely below. It’s time for a little practice with this new definition.

Using the equivalence class notation, we see that the sets of points related to 0, $1/2$, π , and x following Example 10.3 were actually descriptions of E_0 , $E_{1/2}$, E_π , and E_x .

Exercise 10.5. Write each relation below using set notation. Then decide whether or not the following relations are reflexive, symmetric, or transitive. If they are all three, prove it and describe the equivalence classes. If they are not, give a particular example to show why the property fails to hold.

- Define a relation on \mathbb{Z} by $x \sim y$ if and only if $x = -y$.
- Define a relation on \mathbb{Z} by $x \sim y$ if and only if $x - y$ is even.
- Define a relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by $(x, y) \sim (w, z)$ if and only if $xz = yw$. \circ

Example 10.6. We look at $R = \{(1, 1), (2, 2), (3, 3), (1, 3)\}$. This is a relation on the set $X = \{1, 2, 3\}$. We can represent this relation with a diagram. Such a diagram is obtained using a point for each element of X , and these will be the vertices of the diagram. If $(x, y) \in R$, then we will sketch an arrow from x to y . These arrows are the directed edges of the diagram (that is, they are edges with an indicated direction). [Figure 10.1](#) shows the diagram of our relation R . (Such a diagram is usually called a directed graph or a digraph in graph theory. Since we will soon use the term graph for something else, we will call such a picture a diagram.) \circ

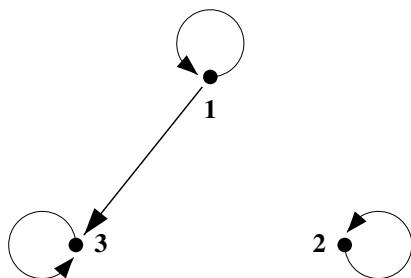


Fig. 10.1 Diagram of a relation on $\{1, 2, 3\}$

Exercise 10.7. Give a detailed description of a diagram that came from an equivalence relation; that is, give precise conditions that a diagram must satisfy in order to fulfill each of the conditions an equivalence relation must satisfy. How can you identify the equivalence classes in the diagram? \circ

Definitions

Definition 10.1. A relation \sim on a set X is **reflexive** if $x \sim x$ for all $x \in X$.

Definition 10.2. A relation \sim on a set X is **symmetric** if for all $x, y \in X$, whenever $x \sim y$, then $y \sim x$.

Definition 10.3. A relation \sim on a set X is **transitive** if for all $x, y, z \in X$, whenever $x \sim y$ and $y \sim z$, then $x \sim z$.

Definition 10.4. A relation on a set X is an **equivalence relation** if it is reflexive, symmetric, and transitive.

Definition 10.5. Given an equivalence relation \sim on a set X , the **equivalence class** of $x \in X$ is the set $E_x = \{y \in X : x \sim y\}$.

Solutions to Exercises

Solution (10.1). The set S is represented by the shaded area of [Figure 10.2](#).

Using the defined relation, $(1, 2) \notin S$ but $(3.5, 2) \in S$. Thus, the answer to (b) is no, and the answer to (c) is yes.

Solution (10.2).

- (a) The relation is $R = \{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) : A \subset B\}$.

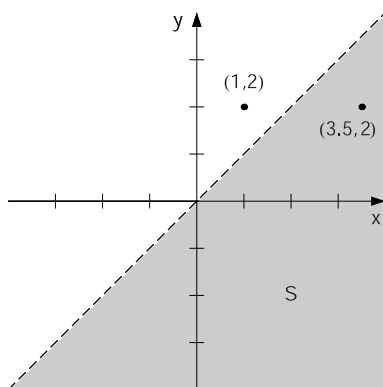


Fig. 10.2 $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x > y\}$

- (b) For our example, we may take X to be any nonempty set. Then \emptyset and X are different, both are in $\mathcal{P}(X)$, and $\emptyset \subset X$.
- (c) Using the same sets as above, we have $X \not\subset \emptyset$.
- (d) In general, we cannot conclude from $A, B \in \mathcal{P}(X)$ with $A \neq B$ that $A \subset B$ or $B \subset A$. To see this, let $\{a, b\} \subseteq X$ with $a \neq b$. Then $\{a\}, \{b\} \in \mathcal{P}(X)$ and $\{a\} \neq \{b\}$. But, $\{a\} \not\subset \{b\}$ and $\{b\} \not\subset \{a\}$. However, the conclusion does hold if X contains only one element. In that case $\mathcal{P}(X) = \{\emptyset, X\}$ and $\emptyset \subset X$.

Solution (10.4). Since R is a relation on the set X , we have $R \subseteq X \times X$. The universe for all variables below is the set X . Then,

R is reflexive, if $\forall x, (x, x) \in R$.

R is symmetric, if $\forall x, \forall y, ((x, y) \in R \rightarrow (y, x) \in R)$.

R is transitive, if $\forall x, \forall y, \forall z, (((x, y) \in R \wedge (y, z) \in R) \rightarrow (x, z) \in R)$.

R is not reflexive, if $\exists x, (x, x) \notin R$.

R is not symmetric, if $\exists x, \exists y, ((x, y) \in R \wedge (y, x) \notin R)$.

R is not transitive, if $\exists x, \exists y, \exists z, ((x, y) \in R \wedge (y, z) \in R \wedge (x, z) \notin R)$.

Solution (10.5).

- (a) This relation is neither reflexive nor transitive (but it is symmetric). It is not reflexive because, for example, $1 \neq -1$ and therefore $1 \not\sim 1$. It is not transitive because $1 \sim -1$ and $-1 \sim 1$, but $1 \not\sim 1$.
- (b) This relation is an equivalence relation. To see this, let $x \in \mathbb{Z}$. Then $x - x = 0$ and therefore $x \sim x$, which shows that \sim is reflexive. To show symmetry, let $x, y \in \mathbb{Z}$. If $x \sim y$, then $x - y$ is even. Since $y - x = -(x - y)$, it follows that $y - x$ is even. Therefore $y \sim x$, and \sim is symmetric. For transitivity, let $x, y, z \in \mathbb{Z}$. If $x \sim y$ and $y \sim z$, then $x - y$ and $y - z$ are both even; in other words, there exist integers m and n such that $x - y = 2m$ and $y - z = 2n$. Now, $x - z = (x - y) + (y - z) = 2m + 2n = 2(m + n)$, and $m + n \in \mathbb{Z}$. Thus $x - z$ is even. Therefore $x \sim z$, and \sim is transitive. We conclude that the relation is an equivalence relation.

What are the equivalence classes? You can check that if x is even, then the equivalence class corresponding to x is the set of even numbers. If x is odd, then the equivalence class corresponding to x is the set of odd numbers.

(c) This relation is an equivalence relation.

If $(x, y) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, then $xy = yx$. Therefore, $(x, y) \sim (x, y)$. Thus, the relation is reflexive.

If $(x, y), (w, z) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ and $(x, y) \sim (w, z)$, then $xz = yw$. This implies that $wy = zx$. Thus, $(w, z) \sim (x, y)$. This shows that the relation is symmetric.

Suppose $(x, y), (u, v)$, and (w, z) are elements of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ such that $(x, y) \sim (u, v)$ and $(u, v) \sim (w, z)$. By definition, y, v , and z are all nonzero, $xv = yu$, and $uz = vw$. We need to show that $xz = yw$. Multiplying both sides of the equation $xv = yu$ by z and both sides of the equation $uz = vw$ by y , we obtain the two equations $xvz = yuz$ and $uzv = vwy$. Therefore $xvz = vwy$. Now v is nonzero, so we may cancel to obtain $xz = yw$, which shows that $(x, y) \sim (w, z)$. Therefore \sim is transitive.

Finally, $E_{(x,y)} = \{(w, z) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) : xz = yw\}$. If we think of (x, y) as the rational number x/y , then $(w, z) \sim (x, y)$ if and only if $x/y = w/z$. So this relation is a way of identifying all fractions with the same value.

Solution (10.7). A relation is reflexive if and only if its diagram has an arrow from each vertex to itself. It is symmetric if and only if whenever we have an arrow between two different vertices, then there is also an arrow in the other direction between these two vertices. Finally, a relation is transitive if and only if whenever an arrow goes from a vertex x to a vertex y and a second arrow from vertex y to a vertex z , then there is an arrow directly from x to z . The relation is an equivalence relation on the set of the vertices of the diagram, if the diagram satisfies the three conditions outlined above.

Two vertices are in the same equivalence class if and only if there is an arrow between them. Thus two vertices are in different equivalence classes if and only if there is no arrow between them. In a diagram representing an equivalence relation, we call a subset of the vertices with the property that any two vertices of the subset are connected by arrows a component of the diagram. With this language, the equivalence classes are the components of the diagram.

Problems

Problem 10.1. We define several relations on \mathbb{R}^2 below. Prove that each is an equivalence relation and give a geometric description of the equivalence classes.

- We define $(x, y) \sim (w, z)$ if and only if $x + y = w + z$.
- We define $(x, y) \sim (w, z)$ if and only if $x^2 + y^2 = w^2 + z^2$.
- We define $(x, y) \sim (w, z)$ if and only if $3x + y = 3w + z$.
- We define $(x, y) \sim (w, z)$ if and only if $x = w$.

Problem 10.2. Decide whether or not the following relations are reflexive, symmetric, or transitive. If a property holds, prove that it does. If a property does not hold, prove that it does not hold. If the relation is an equivalence relation, give the equivalence class of a general point $x \in X$.

- On \mathbb{R} , we define $x \sim y$ if and only if $x < y$.
- On \mathbb{R} , we define $x \sim y$ if and only if $x \leq y$.
- On \mathbb{Z} , we define $x \sim y$ if and only if $x - y$ is divisible by 3.
- If X is a nonempty set, define a relation on $\mathcal{P}(X)$ by $A \sim B$ if and only if $A \subseteq B$.
- If X is a nonempty set, define a relation on $\mathcal{P}(X)$ by $A \sim B$ if and only if $A \setminus B \neq \emptyset$.
- On \mathbb{Z} , we define $x \sim y$ if and only if $|x| = |y|$.
- On \mathbb{Z}^+ , we define $x \sim y$ if and only if there exists a rational number m such that $x = y^m$.

Problem 10.3. Define three relations on \mathbb{R} by $x \sim y$ if and only if there exists $n \in \mathbb{Z}$ such that

- $x, y \in [n, n + 1]$;
- $x, y \in [n, n + 1)$;
- $x, y \in [n, n + 2)$.

In each case, determine whether we have defined an equivalence relation or not. Give reasons for your answers.

Problem 10.4. If $a, b \in \mathbb{C}$, say that $a \sim b$ if and only if $a^k = b^k$ for some positive integer k . Prove that this is an equivalence relation.

Problem 10.5. We define a relation \sim on \mathbb{R}^2 by $(x_1, y_1) \sim (x_2, y_2)$ if and only if $y_2 - y_1 \in 2\mathbb{Z}$ (see Example 6.1 for the definition of $2\mathbb{Z}$). Show that the relation \sim is an equivalence relation and describe the equivalence class of the point $(0, 1)$.

Problem 10.6. Define an equivalence relation on \mathbb{Z} that has exactly three equivalence classes.

Problem 10.7. Let $X = \{1, 2, 3, 4, 5\}$.

- If possible, define a relation on X that is an equivalence relation.
- If possible, define a relation on X that is reflexive, but neither symmetric nor transitive.
- If possible, define a relation on X that is symmetric, but neither reflexive nor transitive.
- If possible, define a relation on X that is transitive, but neither reflexive nor symmetric.

Problem 10.8. Define a relation \sim on \mathbb{R} as follows: For $x, y \in \mathbb{R}$, we say $x \sim y$ if and only if $x^2 - y^2 \in \mathbb{Z}$.

- (a) Prove that \sim as defined above is an equivalence relation on \mathbb{R} .
 (b) Give five different real numbers that are in the equivalence class $E_{\sqrt{2}}$.

Problem 10.9. Define a relation \sim on \mathbb{R}^2 as follows: For $(x_1, x_2), (y_1, y_2) \in \mathbb{R}^2$, we say that $(x_1, x_2) \sim (y_1, y_2)$ if and only if both $x_1 - y_1$ and $x_2 - y_2$ are even integers. Is this relation an equivalence relation? Why or why not?

Problem[#] 10.10. Let X be a nonempty set with an equivalence relation \sim on it. Prove that for all elements x and y in X , the equality $E_x = E_y$ holds if and only if $x \sim y$.

Problem 10.11. What, if anything, is wrong with the following argument?

We claim that if a relation on a set X is symmetric and transitive, then it is reflexive. Here's a proof of this claim:

Proof. Let $x \in X$. Let $y \in X$ with $x \sim y$. By symmetry we have $y \sim x$. We now use transitivity to conclude that $x \sim x$. □

Problem 10.12. Give an example of a relation on $\mathbb{Z} \times \mathbb{Z}$ that is not transitive, but is reflexive and symmetric.

Problem 10.13. Recall that a **polynomial** p over \mathbb{R} is an expression of the form $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$ where each $a_j \in \mathbb{R}$ and $n \in \mathbb{N}$. The largest integer j such that $a_j \neq 0$ is the **degree** of p . We define the degree of the constant polynomial $p = 0$ to be $-\infty$. (A polynomial over \mathbb{R} defines a function $p : \mathbb{R} \rightarrow \mathbb{R}$.)

- (a) Define a relation on the set of polynomials by $p \sim q$ if and only if $p(0) = q(0)$. Is this an equivalence relation? If so, what is the equivalence class of the polynomial given by $p(x) = x$?
- (b) Define a relation on the set of polynomials by $p \sim q$ if and only if the degree of p is the same as the degree of q . Is this an equivalence relation? If so, what is E_r if $r(x) = 3x + 5$?
- (c) Define a relation on the set of polynomials by $p \sim q$ if and only if the degree of p is less than or equal to the degree of q . Is this an equivalence relation? If so, what is E_r , where $r(x) = x^2$?

Problem 10.14. Figure 10.3 shows the diagram of a relation on $X = \{a, b, c, d, e, f\}$. Is this the diagram of an equivalence relation on X ? Give reasons for your answer. If it is an equivalence relation, find all equivalence classes of the relation.

Problem 10.15. We define a relation on a subset X of \mathbb{Z} as follows. For $x, y \in X$, $x \sim y$ if and only if there is a prime number p such that $p|x$ and $p|y$. For each of the two choices of X below, draw a diagram of the relation. From the diagram determine whether or not the relation on X is an equivalence relation. If it is an equivalence relation, use the diagram to find all equivalence classes. How many are there?

- (a) $X = \{x \in \mathbb{Z} : 1 \leq x \leq 10\}$;
 (b) $X = \{4, 5, 6, 8, 11, 12, 35, 143\}$.

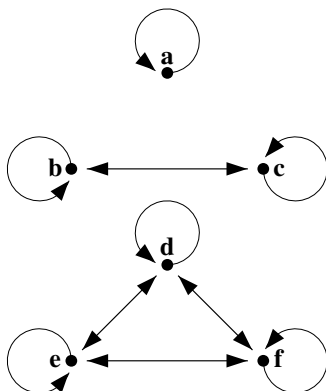


Fig. 10.3

Problem 10.16. Prove that if x and y are two vertices of a diagram that represents an equivalence relation on a set X and x is in the same equivalence class as y , then there are arrows pointing in both directions between x and y .

Problem 10.17. We say that a relation \sim on a set X is antisymmetric if for all $x, y \in X$, whenever $x \sim y$ and $y \sim x$, then $x = y$. How can you see from the diagram of a relation that it is antisymmetric? Explain. Draw a nontrivial example (at least one arrow between two different vertices) of such a diagram using $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Problem# 10.18. Let X be a nonempty set and suppose that there is an equivalence relation defined on X . Prove that the union of all equivalence classes is X .

Problem# 10.19. Given an equivalence relation on a nonempty set X , prove that no equivalence class is empty.

Problem 10.20. Given three sets A, B , and C we can define a 3-adic relation among them in the following way. We first define the triple product of the sets A, B , and C by $A \times B \times C = \{(a, b, c) : a \in A, b \in B, \text{ and } c \in C\}$. This notation presumes that $(a_1, b_1, c_1) = (a_2, b_2, c_2)$ if and only if $a_1 = a_2, b_1 = b_2$, and $c_1 = c_2$. A 3-adic relation among sets A, B , and C is a subset of $A \times B \times C$. Give a meaningful example of a 3-adic relation on $A = B = C = \mathbb{Z}$. Give two triples that are related in your example and two triples that are not related.

Tips on Reading Mathematics

Don't just read it; fight it! Ask your own questions, look for your own examples, discover your own proofs. Is the hypothesis necessary? Is the converse true? What happens in the classical special case? What about the degenerate cases? Where does the proof use the hypothesis?—Paul R. Halmos, [44]

- Be an active reader. Open to the page you need to read, get out some paper and a pencil.
- If notation is defined, make sure you know what it means. Your pencil and paper should come in handy here.
- Look up the definitions of all words that you do not understand.
- Read the statement of the theorem, corollary, lemma, or example. Can you work through the details of the proof by yourself? Try. Even if it feels like you are making no progress, you are gaining a better understanding of what you need to do.
- Once you truly understand the statement of what is to be proven, you may still have trouble reading the proof—even someone's well-written, clear, concise proof. Try to get the overall idea of what the author is doing, and then try (again) to prove it yourself.
- If a theorem is quoted in a proof and you don't know what it is, look it up. Check that the hypotheses apply, and that the conclusion is what the author claims it is.
- Don't expect to go quickly. You need to get the overall idea as well as the details. This takes time.
- If you are reading a fairly long proof, try doing it in bits.
- If you can't figure out what the author is doing, try to (if appropriate) choose a more specific case and work through the argument for that specific case.
- Draw a picture, if appropriate.
- If you really can't get it, do what comes naturally—put the book down and come back to it later. You might want to take this time to read similar proofs or some examples.
- After reading a theorem, see if you can restate it. Make sure you know what the theorem says, what it applies to, and what it does not apply to.
- After you read the proof, try to outline the technique and main idea the author used. Try to explain it to a willing listener. If you can't do this without looking back at the proof, you probably didn't fully understand the proof. Read it again.
- Can you prove anything else using a similar proof? Does the proof remind you of something else? What are the limits of this proof? This theorem?
- If your teacher is following a book, read over the proofs before you go to class. You'll be glad you did.

As we proceed, you will have plenty of opportunities to try these tips out and find some others of your own.

Chapter 11

Partitions

It is sometimes helpful to split a nonempty set into disjoint smaller pieces. For example, we might have reason to split the integers into positive integers, negative integers, and the set containing zero alone. We often split the real numbers into rational numbers and irrational numbers, or we might want to break \mathbb{R}^2 down into distinct vertical lines. All of these are examples of partitioning a space.

Though we have an intuitive feel for what a partition is, we need a precise definition. We turn to that now. A **partition of a nonempty set** X is a collection \mathcal{A} of subsets of X that satisfies the following three conditions.

- (i) Every set $A \in \mathcal{A}$ is nonempty,
- (ii) $\bigcup_{A \in \mathcal{A}} A = X$, and
- (iii) for all $A, B \in \mathcal{A}$, if $A \cap B \neq \emptyset$, then $A = B$.

Looking back at the example of the integers that we discussed earlier, we see that the collection $\mathcal{A} = \{\mathbb{Z}^+, \mathbb{Z}^-, \{0\}\}$ is a partition of \mathbb{Z} .

Figure 11.1 provides a diagram of a partition of $X = \{a, b, c, d, e, f\}$ into sets A_1 , A_2 , and A_3 , defined by

$$A_1 = \{a, b\}, \quad A_2 = \{c, d, e\}, \quad \text{and} \quad A_3 = \{f\}.$$

While it is often clear that the sets in the collection are nonempty, you should still check. Condition (ii) says that every element of X is in at least one of the sets in the collection. It's a sort of existence statement: for each element x of X , there exists a set A in \mathcal{A} of which x is a member. The third condition is a fancy way of saying that two of the sets in the partition are disjoint or they are equal. This is a sort of uniqueness statement: if x belongs to two sets A and B , then the sets must be equal.

We hope the examples below will clarify these concepts.

Example 11.1. For each $x \in \mathbb{R}$, define $A_x = \{y \in \mathbb{R} : |x| = |y|\}$. We will show that $\{A_x : x \in \mathbb{R}\}$ forms a partition of \mathbb{R} .

Before we begin, note that our proposed partition is an indexed collection of sets, and that in this case it is possible that two different indices give rise to the same set.

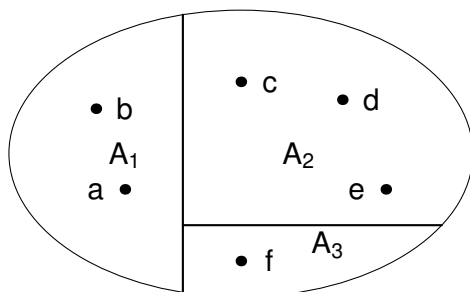


Fig. 11.1 A partition of $\{a, b, c, d, e, f\}$

For example, $A_1 = \{1, -1\}$ and $A_{-1} = \{-1, 1\}$, so $A_1 \cap A_{-1} \neq \emptyset$. That will not be a problem though, and it does illustrate why we stated condition (iii) the way we did. It happens that $A_1 \cap A_{-1} \neq \emptyset$, but $A_1 = A_{-1}$, as required.

Proof. We note that all the sets A_α are nonempty. So there are two things left to show, namely, conditions (ii) and (iii) of the definition of partition. We begin by showing that (ii) holds; that is, $\bigcup_{x \in \mathbb{R}} A_x = \mathbb{R}$. First, $\bigcup_{x \in \mathbb{R}} A_x \subseteq \mathbb{R}$ since each $A_x \subseteq \mathbb{R}$. We show the reverse containment using an element-chasing argument. Let $y \in \mathbb{R}$. Then $|y| = |y|$, so $y \in A_y$. Since $y \in A_x$ for some x (namely, $x = y$), we may conclude that $y \in \bigcup_{x \in \mathbb{R}} A_x$. Thus $\bigcup_{x \in \mathbb{R}} A_x = \mathbb{R}$.

Next, suppose that $A_x \cap A_y \neq \emptyset$. Then we must show that $A_x = A_y$. By our assumption, there exists $z \in \mathbb{R}$ such that $z \in A_x \cap A_y$. Therefore, $|x| = |z|$ and $|y| = |z|$. In particular, $|x| = |y|$. So,

$$A_x = \{w \in \mathbb{R} : |x| = |w|\} = \{w \in \mathbb{R} : |y| = |w|\} = A_y. \quad \square$$

Well, we showed the two sets A_x and A_y are equal with nary an element-chasing argument in sight. What happened? We certainly could have started with an element from one side and showed it was in the other, switched sides, repeated what we did, and then concluded we were done. But this is somewhat cumbersome and doesn't show us what is really going on. So from now on, even though we can use element-chasing, we are going to use whatever produces the most elegant or enlightening proof.

Exercise 11.2. For each $n \in \mathbb{N}$, let $A_n = [-n, n]$. Show that the collection $\mathcal{A} = \{A_n : n \in \mathbb{N}\}$ does not form a partition of \mathbb{R} . However, if we define $B_n = [n, n + 1)$, then the collection $\mathcal{B} = \{B_n : n \in \mathbb{Z}\}$ does partition \mathbb{R} . \circ

In Example 11.1 and Exercise 11.2, the third condition may have reminded you of transitivity. If so, then it may not surprise you to learn that there is a connection between equivalence relations and partitions. As we have already seen, every equivalence relation on a set X gives rise to equivalence classes in a natural way. These equivalence classes are sets and as we will see, these sets partition our set X .

Conversely, a collection of sets that partitions a set X gives rise to an equivalence relation on X . How? Well, we say two elements in X are related if they belong to the same set of the partition. We shall now show that this relation is an equivalence relation. We can shorten our proof of this theorem, if we first prove something less ambitious. A helpful result that is used to prove a theorem is called a lemma. Lemmas are sometimes of independent interest.

Lemma 11.3. *Let X be a nonempty set and let \sim be an equivalence relation on X . For two arbitrary elements x and y in X , if $E_x \cap E_y \neq \emptyset$, then $E_x = E_y$.*

The very first thing we should probably ask ourselves before beginning our proof is: What is E_x ? If we don't know, we can't understand the proof. So, before reading the proof, we recall the definition:

$$E_x = \{z \in X : x \sim z\}.$$

Now the proof should be easy.

Proof. Let $z \in E_x$. Hence $x \sim z$. Since we assume that $E_x \cap E_y \neq \emptyset$, we may choose $w \in E_x \cap E_y$. Thus $w \in E_x$, and therefore $x \sim w$. Similarly, $w \in E_y$ and therefore $y \sim w$. By symmetry, $w \sim x$. So $y \sim w, w \sim x$, and $x \sim z$. By transitivity, $y \sim z$. Thus, $z \in E_y$, and we may conclude that $E_x \subseteq E_y$.

Exactly the same argument (*) shows that $E_y \subseteq E_x$. Hence $E_x = E_y$. □

One comment on the proof above: When we use the words “exactly the same argument,” as in (*), that means nothing would be changed except (possibly) the symbols. If you use words to that effect (like “similarly” or “exactly as above”), make sure that what you say is true. Now that we have our lemma, we turn to the proof of our main theorem.

Theorem 11.4. *Let \sim be an equivalence relation on a nonempty set X . Then the indexed collection of equivalence classes $\{E_x : x \in X\}$ is a partition of X . Furthermore, if \mathcal{A} is a partition of a nonempty set X and for $x, y \in X$ we define $x \sim y$ if and only if $x, y \in A$ for some $A \in \mathcal{A}$, then \sim is an equivalence relation on X .*

Before beginning the proof, let's reflect on what we need to do. For the first assertion (“ $\{E_x : x \in X\}$ is a partition”) we need to show that the sets are nonempty, and satisfy conditions (ii) and (iii) in the definition of partition.

What do we expect to use? Our assumptions, of course. We are assuming \sim is an equivalence relation, so we should use the fact that \sim is reflexive, symmetric, and transitive. But that's only one direction—this would show that an equivalence relation gives rise to equivalence classes and these, in turn, form a partition of our set.

For the other direction, we want to show that if we have a relation defined by a partition \mathcal{A} , then the relation is an equivalence relation. So that means we must show that \sim is reflexive, symmetric, and transitive. How will we do that? Well, probably the first thing to do is to make sure we know what \sim is. Remember, $x \sim y$ if and only if there exists $A \in \mathcal{A}$ such that $x, y \in A$. Now, finally, we may begin.

Proof. First we'll show that given an equivalence relation on X , the indexed collection of sets $\{E_x : x \in X\}$ forms a partition of X . We first show that each E_x is nonempty. Since the relation is reflexive, $x \sim x$ for each $x \in X$. Thus $x \in E_x$ for each $x \in X$, and $E_x \neq \emptyset$.

Now we need to check condition (ii): that $\bigcup_{y \in X} E_y = X$. If $x \in X$, then we have just seen that $x \in E_x$. This shows that $x \in \bigcup_{y \in X} E_y$. Thus $X \subseteq \bigcup_{y \in X} E_y$. Since the opposite inclusion follows from the fact that $E_y \subseteq X$ for each $y \in X$, we know that $X = \bigcup_{y \in X} E_y$. Thus, condition (ii) holds.

To show that condition (iii) holds, suppose that for $x, y \in X$, we have $E_x \cap E_y \neq \emptyset$. By Lemma 11.3, we conclude that $E_x = E_y$, and condition (iii) holds. Thus, the set of equivalence classes $\{E_x : x \in X\}$ satisfies conditions (i), (ii), and (iii) and therefore forms a partition of X .

To prove the converse, suppose that \mathcal{A} is a partition of X . By condition (ii), $X = \bigcup_{A \in \mathcal{A}} A$. Thus, for $x \in X$, there exists $A \in \mathcal{A}$ such that $x \in A$. Since x is in the same set as itself, $x \sim x$. Since x was arbitrary, \sim is reflexive.

Suppose now that $x, y \in X$ and $x \sim y$. Then there exists $A \in \mathcal{A}$ such that $x, y \in A$. But if $x, y \in A$, then $y, x \in A$. Consequently, $y \sim x$. Therefore \sim is symmetric.

Finally, suppose that $x, y, z \in X$ where $x \sim y$ and $y \sim z$. We must show that $x \sim z$. By the definition of \sim we see that there exists $A \in \mathcal{A}$ such that $x, y \in A$, and there exists $B \in \mathcal{A}$ such that $y, z \in B$. Therefore, $A \cap B \neq \emptyset$. By property (iii) of partitions, $A = B$. Thus $x, z \in A$. Therefore, $x \sim z$, as desired. We conclude that the partition gives rise to an equivalence relation, since \sim is symmetric, transitive, and reflexive. \square

We will illustrate this connection between partitions and equivalence relations with two very simple examples.

Example 11.5. (a) Consider the set $X = \{1, 2, 3, 4, 5\}$, then the collection of sets $\mathcal{A} = \{\{1, 2\}, \{3\}, \{4, 5\}\}$ is a partition of X . Describe the corresponding equivalence relation.

We have exactly the following relations (and no others):

$$1 \sim 1, 2 \sim 2, 3 \sim 3, 4 \sim 4, 5 \sim 5, 1 \sim 2, 2 \sim 1, 4 \sim 5, 5 \sim 4$$

By Theorem 11.4, this relation is an equivalence relation.

- (b) We consider the set $Y = \{1, 2, 3\}$ and define an equivalence relation on $\mathcal{P}(Y)$ by $A \sim B$ if and only if the number of elements of A is equal to the number of elements of B , for $A, B \in \mathcal{P}(Y)$.

This is clearly an equivalence relation and Theorem 11.4 shows that the following collection of sets, \mathcal{B} , is a partition of $\mathcal{P}(Y)$:

$$\mathcal{B} = \{\{\emptyset\}, \{\{1\}, \{2\}, \{3\}\}, \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}, \{\{1, 2, 3\}\}\}. \quad \circ$$

Theorem 11.4 shows how one can obtain a partition from an equivalence relation and vice versa. Now suppose we start with a partition \mathcal{A}_1 and use the theorem to get a

corresponding equivalence relation. Then we use that equivalence relation to obtain a second partition \mathcal{A}_2 . What's the relation between \mathcal{A}_1 and \mathcal{A}_2 ? And what about turning this procedure around: Say we start with an equivalence relation R_1 , and we use it to determine a partition. Then we use this partition to obtain an equivalence relation R_2 . What's the relation between R_1 and R_2 ? You're probably thinking that in both cases you will end up where you started. If you work Problems 11.14 and 11.15 you will find out that your intuition is correct: \mathcal{A}_1 and \mathcal{A}_2 will be the same, and so will R_1 and R_2 . We say that Theorem 11.4 provides a one-to-one correspondence between the equivalence relations on a nonempty set X and the partitions of the set X .

Exercise 11.6. For $r \in \mathbb{R}$, let $A_r = \{(x, y) \in \mathbb{R}^2 : x + y = r\}$. Show that $\{A_r : r \in \mathbb{R}\}$ is a partition of \mathbb{R}^2 . Then describe the equivalence relation and equivalence classes associated with this partition. \circ

Definition

Definition 11.1. A **partition of a nonempty set** X is a collection \mathcal{A} of subsets of X that satisfies the following three conditions.

- (i) Every set $A \in \mathcal{A}$ is nonempty,
- (ii) $\bigcup_{A \in \mathcal{A}} A = X$, and
- (iii) for all $A, B \in \mathcal{A}$, if $A \cap B \neq \emptyset$, then $A = B$.

Solutions to Exercises

Solution (11.2). The collection \mathcal{A} does not partition \mathbb{R} because condition (iii) is not satisfied: $A_1 \cap A_2 \neq \emptyset$, but $A_1 \neq A_2$. The collection \mathcal{B} does partition \mathbb{R} : For each $n \in \mathbb{Z}$, the set B_n is nonempty, the union of the sets satisfies

$$\bigcup_{B \in \mathcal{B}} B = \bigcup_{n \in \mathbb{Z}} B_n = \bigcup_{n \in \mathbb{Z}} [n, n+1) = \mathbb{R},$$

and if $B_n, B_m \in \mathcal{B}$ with $B_n \cap B_m \neq \emptyset$, then $[n, n+1) \cap [m, m+1) \neq \emptyset$. Since m and n are integers, the intervals $[n, n+1)$ and $[m, m+1)$ are either equal or disjoint. We conclude that $[n, n+1) = [m, m+1)$; in other words, $B_n = B_m$.

Solution (11.6). Note that for $r \in \mathbb{R}$, the ordered pair $(0, r)$ satisfies the condition $0 + r = r$. Thus $(0, r) \in A_r$ and A_r is nonempty. Since it is clear that $\bigcup_{r \in \mathbb{R}} A_r \subseteq \mathbb{R}^2$, we check the reverse inclusion. If $(u, v) \in \mathbb{R}^2$, then $s = u + v \in \mathbb{R}$ and consequently $(u, v) \in A_s$. Thus $(u, v) \in \bigcup_{r \in \mathbb{R}} A_r$, and $\bigcup_{r \in \mathbb{R}} A_r = \mathbb{R}^2$, completing the proof of condition (ii) in the definition of partition. Finally, suppose that $A_r \cap A_s \neq \emptyset$. Then there

exists $(u, v) \in A_r \cap A_s$. By the definition of A_r and A_s this means that $r = u + v = s$. Thus, $A_r = A_s$, as desired.

We associate an equivalence relation on \mathbb{R}^2 as follows. For $(x, y), (u, v) \in \mathbb{R}^2$, we will say $(x, y) \sim (u, v)$ if and only if $x + y = u + v$. By our work above and Theorem 11.4, this is an equivalence relation on \mathbb{R}^2 . The equivalence classes are the lines with slope -1 .

In the two exercises in this chapter, the third condition (of partition) is satisfied because the indices (n and m in Exercise 11.2, and r and s in Exercise 11.6) are equal. Though this can happen, Example 11.1 shows that the two sets can be equal without the indices being equal. Condition (iii) in the definition of partition requires that we show that the two sets are equal—not the two indices.

Problems

Problem 11.1. For each of the relations in Problem 10.2 that you determined to be equivalence relations, describe the partition associated with it.

Problem 11.2. Determine whether or not the following are equivalence relations on \mathbb{R}^2 . If they are, describe the partition associated with each:

- (a) $(x, y) \sim (w, z)$ if and only if $y = w$;
- (b) $(x, y) \sim (w, z)$ if and only if $x^2 = w^2$;
- (c) $(x, y) \sim (w, z)$ if and only if $xw = yz$.

Problem 11.3. None of the following partitions \mathbb{R} . Say precisely why the collection of sets fails to be a partition of \mathbb{R} .

- (a) $\{\{x \in \mathbb{R} : |x| = r\} : r \in \mathbb{R}\}$;
- (b) $\{\{x \in \mathbb{R} : n < |x| \leq n + 1\} : n \in \mathbb{N}\}$;
- (c) $\{\mathbb{R} \setminus \mathbb{R}^+, \mathbb{R} \setminus \mathbb{R}^-\}$.

Problem 11.4. (a) For each $r \in \mathbb{R}$, let $A_r = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = r\}$. Is this a partition of \mathbb{R}^3 ? If so, give a geometric description of the partitioning sets.

- (b) For each $r \in \mathbb{R}$, let $A_r = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = r^2\}$. Is this a partition of \mathbb{R}^3 ? If so, give a geometric description of the partitioning sets.

Problem 11.5. (a) Let $A = \{1, 2, \dots, 10\}$. Describe a partition of A that gives rise to five distinct partitioning sets.

- (b) Describe a partition of \mathbb{Z} that gives rise to five distinct partitioning sets.
- (c) Can you describe a partition of \mathbb{R} that gives rise to five distinct partitioning sets?

Problem 11.6. (a) Suppose that we partition \mathbb{R}^3 into horizontal planes. What equivalence relation is associated with this partition?

- (b) Suppose that we partition \mathbb{R}^3 into concentric spheres, centered at $(0,0,0)$. What equivalence relation is associated with this partition?

Problem 11.7. Suppose that we look at the set X containing all circles in the plane. Define an equivalence relation on this set of circles by $c \sim d$ if and only if the circles c and d have the same center. Describe the partition associated with this equivalence relation.

Problem 11.8. Consider the set P of polynomials with real coefficients. Decide whether or not each of the following collection of sets determines a partition of P . If you decide that it does determine a partition, show it carefully. If you decide that it does not determine a partition, list the part(s) of the definition that is (are) not satisfied and justify your claim with an example. (See Problem 10.13 for more information about polynomials.)

- For $m \in \mathbb{N}$, let A_m denote the set of polynomials of degree m . The collection of sets is $\{A_m : m \in \mathbb{N}\}$.
- For $c \in \mathbb{R}$, let A_c denote the set of polynomials p such that $p(0) = c$. The collection of sets is $\{A_c : c \in \mathbb{R}\}$.
- For a polynomial q , let A_q denote the set of all polynomials p such that q is a factor of p ; that is, there is a polynomial r such that $p = qr$. The collection of sets is $\{A_q : q \in P\}$.
- For $c \in \mathbb{R}$, let A_c denote the set of polynomials p such that $p(c) = 0$. The collection of sets is $\{A_c : c \in \mathbb{R}\}$.

Problem 11.9. For two nonempty disjoint sets, I and J , let $\{A_\alpha : \alpha \in I\}$ be a partition of \mathbb{R}^+ and $\{A_\alpha : \alpha \in J\}$ be a partition of $\mathbb{R}^- \cup \{0\}$. Prove that $\{A_\alpha : \alpha \in I \cup J\}$ is a partition of \mathbb{R} .

Problem 11.10. Let X be a nonempty set and $\{A_\alpha : \alpha \in I\}$ be a partition of X .

- Let B be a subset of X such that $A_\alpha \cap B \neq \emptyset$ for every $\alpha \in I$. Is $\{A_\alpha \cap B : \alpha \in I\}$ a partition of B ? Prove it or give a counterexample.
- Suppose further that $A_\alpha \neq X$ for every $\alpha \in I$. Is $\{X \setminus A_\alpha : \alpha \in I\}$ a partition of X ? Prove it or show that it is not a partition. (Make sure you consider each of the following cases: the partition $\{A_\alpha : \alpha \in I\}$ has zero, one, two, or at least three elements.)

Problem 11.11. Recall that for an integer n , the symbol $3|n$ means that there exists $m \in \mathbb{Z}$ such that $n = 3m$. For each integer i , where $i = 0, 1, 2$, we define the set $A_i = \{x \in \mathbb{Z} : 3|(x-i)\}$. Show that $\{A_i : i = 0, 1, 2\}$ is a partition of \mathbb{Z} .

Problem 11.12. Let $A = \{x \in \mathbb{R} : x > 0\}$ and $B = \{x \in \mathbb{R} : x \leq 0\}$. Describe the equivalence relation on \mathbb{R} that is associated with the partition $\{A, B\}$ of \mathbb{R} .

Problem 11.13. For each $r \in \mathbb{R}$ define a subset of \mathbb{R}^3 by

$$A_r = \{(x, y, z) : y^2 + z^2 = r^2\}.$$

- (a) Prove that $\{A_r : r \in \mathbb{R}\}$ is a partition of \mathbb{R}^3 .
 (b) Describe the equivalence relation associated with this partition geometrically.

Problem 11.14. Let X be a nonempty set with an equivalence relation \sim on it. According to Theorem 11.4, this equivalence relation gives rise to a partition on X which in turn defines a new equivalence relation $\tilde{\sim}$ on X . Prove that \sim and $\tilde{\sim}$ are the same equivalence relation on X .

Problem 11.15. Let \mathcal{A} be a partition of a nonempty set X . By Theorem 11.4, this partition gives rise to an equivalence relation on X and this equivalence relation, in turn, defines a new partition \mathcal{B} of X . Prove that $\mathcal{A} = \mathcal{B}$.

Problem 11.16. Let $X = \{x \in \mathbb{Z}^+ : x \leq 100\}$; that is, X is the set of all integers from 1 to 100. For each $Y \in \mathcal{P}(X)$ we define $A_Y = \{Z \in \mathcal{P}(X) : Y \text{ and } Z \text{ have the same number of elements}\}$.

- (a) Prove that $\{A_Y : Y \in \mathcal{P}(X)\}$ partitions $\mathcal{P}(X)$.
 (b) Let \sim denote the equivalence relation on $\mathcal{P}(X)$ that is associated with this partition (according to Theorem 11.4). If possible, find A, B , and C such that
1. $A \sim \{1, 2, 3\}$ and $A \neq \{1, 2, 3\}$
 2. $B \not\sim \{7, 8, 9\}$
 3. $C \sim X$ and $C \neq X$.

Problem 11.17. Let the collection $\mathcal{S} = \{A_\alpha : \alpha \in I\}$ be a partition of a nonempty set A and $\mathcal{T} = \{B_\beta : \beta \in J\}$ be a partition of a nonempty set B . We define the following collection of sets $\mathcal{W} = \{A_\alpha \times B_\beta : \alpha \in I \text{ and } \beta \in J\}$.

- (a) Give a “small” example of this situation using $A = B = \mathbb{R}$ and two different partitions \mathcal{S} and \mathcal{T} , each having exactly two sets. (Specify \mathcal{S} , \mathcal{T} , and \mathcal{W} .)
 (b) Does the collection \mathcal{W} for your example above partition the plane $\mathbb{R} \times \mathbb{R}$? (No proof needed for this part, just state your answer.)
 (c) Prove that with \mathcal{S} , \mathcal{T} , and \mathcal{W} as defined at the beginning of this problem, \mathcal{W} is a partition of $A \times B$.

Problem 11.18. Let X be a nonempty set and \mathcal{A} a partition of X . Is $\{\mathcal{P}(A) : A \in \mathcal{A}\}$ a partition of $\mathcal{P}(X)$? If it is, prove it. If it isn’t, give a simple example of sets X and \mathcal{A} such that $\{\mathcal{P}(A) : A \in \mathcal{A}\}$ is not a partition of $\mathcal{P}(X)$.

Problem 11.19. Consider the set consisting of all three-letter “words” that you can make with the two letters O and T, so that

$$S = \{OOO, TOO, OTO, OOT, OTT, TOT, TTO, TTT\}.$$

- (a) Define an equivalence relation on the set S of “words” by saying that $x \sim y$ for $x, y \in S$ if it is possible to rearrange the letters in x to obtain y . Show that this is an equivalence relation and find the partition \mathcal{A} associated with \sim .

- (b) Now define $x \sim_1 y$ for $x, y \in S$ if and only if there is a set $A \in \mathcal{A}$ such that $x, y \in A$. Is this an equivalence relation? If so, find the associated equivalence classes.
- (c) Is your answer to part (b) what you expected? Why or why not? (If a theorem applies, state it.)

Problem 11.20. Do there exist sets X for which $\mathcal{P}(X)$ is a partition of X ? If so, give an example of such a set X . If there do not exist such sets, prove that $\mathcal{P}(X)$ is not a partition of X for all sets X .

Problem 11.21. For $k \in \mathbb{Z}$, we define $A_k = \{x \in \mathbb{Z} : x = 5\ell + k \text{ for some } \ell \in \mathbb{Z}\}$.

- (a) Prove that $\{A_k : k \in \mathbb{Z}\}$ partitions \mathbb{Z} .
- (b) We denote by \sim the equivalence relation on \mathbb{Z} that is obtained from the partition of part (a). Give as simple a description of \sim as possible; that is, given two elements x and y in \mathbb{Z} , find a simple condition “ $C(x, y)$ ” on x and y so that $x \sim y$ if and only if “ $C(x, y)$ ” holds.

Tips on Putting It All Together

In my own writing, I average about five pages a day. Unfortunately, they’re all the same page.—Michael Alley [5, p. 246]

Now we will build upon the foundations we have created.

- In each section, work through the definitions. (Check “Tips on Definitions.”) If you don’t know the definitions, you cannot get started. So the first step is to make sure that you have *mastered* them.
- Next, learn and understand all theorems. You don’t have to memorize their number, of course, but you should know by name each theorem that has a name. Make sure you can restate every theorem in the text correctly.
- If you are asked to prove something, look for a proof or theorem that reminds you of your problem. Read it over.
- If your problem is too difficult, try a simpler one first.
- Whenever you claim something is true, say why (at least to yourself, if it is minor, and to the reader, if it is major). Is it a definition? a theorem? Are the techniques the same as in a proof everyone has already seen? If you are writing up your homework, tell the grader which theorem (now you should give a number) or what definition you are using.
- If you can check your solution, do so. Is your answer reasonable?
- Does your theorem make sense? Does it agree with other theorems in the text? (It’s supposed to agree, of course!) Does your proof use everything you were given?
- Your first draft is precisely that. No one should have to read someone else’s first draft. Work out the solution, write it up, put it away, read it again, and rewrite it.

Chapter 12

Order in the Reals

You've seen numbers ever since you've been in school, and you know a lot about them. It is possible to give them a careful mathematical foundation. In fact, it's possible to construct the natural numbers (and you can do so in Project 29.3). Then, if you try to introduce operations like addition and subtraction, you'll find that you are missing something: the negative numbers. So you look at the integers, and try again. Now, trying to introduce multiplication and division, you'll find you are missing something again: multiplicative inverses. So you look at the rational numbers, and you'll find you are missing something yet again. That brings you to the real numbers. Our ultimate goal will be to discuss what's missing in \mathbb{Q} , and to show you why \mathbb{R} has what's missing. This is known as completeness of \mathbb{R} . In this and the next chapter, we'll show you some wonderful applications of completeness.

What do we mean by this property "completeness," that \mathbb{R} has, but \mathbb{Q} doesn't? If we take a stroll along the real number line, we can walk right up to any real number and it will be there waiting for us. In contrast to this, if we walk along the real line, this time stepping on rational numbers only, we might walk right up to where we'd expect $\sqrt{2}$ to be, but it will be out having lunch with other irrationals. We'll make this precise by the end of the chapter. We remind you that in this text we are assuming that the real numbers satisfy the algebraic and order properties listed in the Appendix on pages 363–364. We now turn to the important terminology that we need.

A nonempty subset A of \mathbb{R} is **bounded above** if there is a real number M such that $x \leq M$ for all $x \in A$. We call a real number M satisfying $x \leq M$ for all $x \in A$ an **upper bound** of A . The nonempty subset A of \mathbb{R} is **bounded below** if there is a real number m such that $m \leq x$ for all $x \in A$. We call a real number m satisfying $m \leq x$ for all $x \in A$ a **lower bound** of A . We say a nonempty set is **bounded** if it is bounded above and below. For example, the open interval $(0, 1)$ is bounded above, since every $x \in (0, 1)$ satisfies $x \leq 1$. The number 1 is an upper bound, and so is the real number 1.5. In fact, every number greater than or equal to 1 is an upper bound. Similarly, since $x \geq 0$ for all $x \in (0, 1)$, the set $(0, 1)$ is bounded below and 0 is an example of a lower bound of the set. Since $(0, 1)$ is bounded above and below, it is an example of a bounded set.

Exercise 12.1. For each of the following sets of real numbers, decide whether it is bounded above, bounded below, and (consequently) whether or not it is bounded. If the set is bounded above, give three different examples of upper bounds in \mathbb{R} . If the set is bounded below, give three different examples of lower bounds in \mathbb{R} . Use your intuition; we'll prove things rigorously later. The sets are:

- (a) $\{x \in \mathbb{R} : x^2 \leq 5\}$;
- (b) $\{x \in \mathbb{R} : x^3 < 5\}$;
- (c) $\{x \in \mathbb{N} : x \leq 5\}$;
- (d) $\{x \in \mathbb{Q} : x^2 < 2\}$.

○

Sometimes a subset of \mathbb{R} that is bounded above contains a largest element, and we give this element a special name: a maximum. The real number M is a **maximum** of the set A , if $M \in A$ and $x \leq M$ for all $x \in A$. We will write $M = \max A$ for a maximum of the set A . Note that a maximum is an upper bound that lies in the set A . Likewise, a real number m is a **minimum** of the set A , if $m \in A$ and $m \leq x$ for all x in A . We will write $m = \min A$ to denote a minimum of the set A . Again, notice that a minimum is a lower bound that lies in the set A .

It should now be clear that if a set A has a maximum, then A must be bounded above, and if the set has a minimum, then A must be bounded below. What about the converse?

Example 12.2. Give an example of a bounded set that has neither a maximum nor a minimum.

We claim that the set $(0, 2)$ is bounded and has neither a maximum nor a minimum.

Proof. For each $x \in (0, 2)$, we know that $0 < x < 2$. Therefore 0 is a lower bound of the set and 2 is an upper bound. Thus, $(0, 2)$ is bounded. To see that it has no maximum, suppose to the contrary that s is a maximum of the set $(0, 2)$. Then, by definition of maximum, s must be in the set, so $0 < s < 2$. But (as you can check) $0 < s < (2 + s)/2 < 2$, and therefore $(2 + s)/2$ is in the set $(0, 2)$ and larger than s , a contradiction. In a similar fashion, you can check that there is no minimum. \square

It turns out that there is an upper bound that can help us when we don't have a maximum (called the supremum), and a lower bound that can help us when we don't have a minimum (called the infimum). We define these below.

Let A be a nonempty set of real numbers that is bounded above. Then a real number U is said to be a **supremum** of A or **least upper bound** of A if

- (i) $a \leq U$ for all $a \in A$, and
- (ii) if $M \in \mathbb{R}$ satisfies $a \leq M$ for all $a \in A$, then $U \leq M$.

Note that (i) says that U is an upper bound, while (ii) says that U is least among all upper bounds. While the phrase "least upper bound" is more descriptive, most authors prefer the term "supremum."

The following lemma tells us that the supremum, when it exists, is unique.

Lemma 12.3. *If a nonempty subset of \mathbb{R} has a supremum, then the supremum is unique.*

We first try to understand the problem. Let's call our set S . We are not asking whether or not a supremum of S exists. What we are trying to do is to show that there cannot exist two different real numbers a and b , such that both a and b fulfill the properties of supremum of S . (We've seen examples of sets with more than one upper bound. Maybe there are sets with more than one least upper bound.)

So we turn to devising a plan. Let's suppose that there are two such numbers a and b , and try to show that they must be equal.

Proof. Let S be a nonempty subset of \mathbb{R} . Suppose a and b are two real numbers that satisfy properties (i) and (ii) in the definition of supremum. Then a is an upper bound. Since b is a supremum, property (ii) implies that $b \leq a$. On the other hand, since b is an upper bound and a is a supremum, property (ii) implies that $a \leq b$. Thus $a = b$, and we conclude that there is at most one supremum. \square

From here on in, we will refer to “the” supremum, and we will denote the supremum of a nonempty set A by $\sup A$.

The last proof was your first proof of uniqueness. This particular proof is fairly standard. You'll frequently be able to prove uniqueness by supposing that you have two such objects, and showing that they must be equal.

Exercise 12.4. Return to Exercise 12.1. Use your intuition to decide which of the sets have a supremum in \mathbb{R} . For the sets that you decide have a supremum, find a real number that you believe is the supremum. At this point, you may use your intuition to find an answer. We will ask you to prove that your answer is correct later. \circ

So we have defined two notions, supremum and maximum. What are the differences and what are the similarities? A close look at the definition shows that the maximum of a set A must be in A , while the supremum of A need not. On the other hand, we also have the following.

Exercise 12.5. Let A be a nonempty subset of real numbers that is bounded above. Show that if A has a maximum M , then M is the supremum of A . Conclude that a maximum of a set is unique and thus we can speak of “the” maximum of a set A —if it exists. \circ

In the following exercise you will define and investigate the infimum (or greatest lower bound) of a set. This is an important exercise, and we will refer to it frequently.

Exercise 12.6. Let A be a nonempty subset of \mathbb{R} that is bounded below.

- Define **infimum** (or **greatest lower bound**) of the set A .
- Do what you always do when confronted with a new definition: Find examples and nonexamples. \circ

The infimum of a set A , denoted $\inf A$, is also unique (Problem 12.17) and hence we can speak of “the” infimum. If a set A has a minimum, then this minimum is the infimum of the set. Thus, $\min A$ is also unique, if it exists.

Some students find the words supremum and infimum difficult to remember. But once you get used to it, these words will sound like what they are: If the supremum is in the set, it’s the maximum. If it’s not in the set, the supremum (as suggested by the word “superior”) lies above the set. Similarly, if the infimum is in the set, it’s the minimum. If it’s not in the set, then the infimum (as suggested by the word “inferior”) lies below the set.

The next example shows how to prove rigorously that a particular number is the infimum (or supremum) of a set. Remember that to show ℓ is the infimum, we must show that it is a lower bound, and that if y is another lower bound, then $y \leq \ell$. We will actually show the contrapositive of this last assertion: if $y > \ell$, then y is not a lower bound.

Example 12.7. Show that $\inf(3, 4] = 3$.

Proof. We note that $3 \leq x$ for all $x \in (3, 4]$. Therefore, 3 is a lower bound.

To see that it is the infimum, we will show that nothing larger can be a lower bound. To this end, let y be chosen so that $3 < y$. If $y > 4$, then y is not a lower bound of $(3, 4]$. If $y \leq 4$, then $(3 + y)/2$ is a real number such that $3 < (3 + y)/2 < y \leq 4$. Therefore $(3 + y)/2 \in (3, 4]$ and $(3 + y)/2 < y$. Thus, y is not a lower bound of $(3, 4]$. Hence, 3 is the infimum of $(3, 4]$. \square

There is one point in the proof above that is very important and, unfortunately, very easy to overlook. When we checked that “nothing larger than 3 can be a lower bound,” we chose $y > 3$ and showed that $(3 + y)/2 < y$. This, alone, will not convince someone that y is not a lower bound of $(3, 4]$; if $(3 + y)/2$ is not in the set $(3, 4]$, it won’t help us at all. That’s why we also checked that $(3 + y)/2 \in (3, 4]$. Our point is this: to show y_0 is *not* a lower bound of a set S , you must find something in the set S that is smaller than y_0 . (Keep this in mind when you solve the problems; in particular, when you solve Problem 12.1.)

Example 12.7 provides us with an example of a bounded set that has no minimum, but does have an infimum.

Exercise 12.8. Return to Exercise 12.4 and assume for now that the real numbers $\sqrt{5}$ and $5^{1/3}$ are irrational. (We will discuss this assumption in the next chapter.) If the set has an infimum, say what you think the infimum is. Then give an argument that shows that your answers for supremum (from Exercise 12.4) and infimum for the first three sets are correct.

We saw in Example 12.2 that there are sets that are bounded, but have no maximum or minimum. Since a maximum is a supremum, it may seem that there exist sets that are bounded above but have no supremum in \mathbb{R} . It turns out that in \mathbb{R} this is not the case; the real numbers are constructed to guarantee the existence of a supremum of every bounded nonempty set. This will not be proved; in a way it is an agreement. The technical term for such a statement is axiom.

The completeness axiom of the reals. *Every nonempty subset of real numbers that is bounded above has a supremum.*

Exercise 12.9. State a version of the completeness axiom of \mathbb{R} replacing the word “supremum” by the word “infimum.” What conditions, if any, must be placed on the set? Prove that the two versions are equivalent. (Once you have your version of the completeness axiom, you may use Problem 12.7 to complete this exercise.) \circ

Here’s an extremely useful consequence of the work we have built up in this chapter:

Theorem 12.10 (Archimedean property of \mathbb{R}). *Let a and b be two positive real numbers. Then there exists a positive integer n such that $a < nb$.*

Proof. Suppose that this is not true; that is, suppose that there are two positive real numbers, a and b , such that $a \geq nb$ for all $n \in \mathbb{N}$. This means that a/b is an upper bound of \mathbb{N} . Therefore, by the completeness axiom of \mathbb{R} , it follows that \mathbb{N} has a supremum, which we will call u . Now consider $u - 1$. Since this is less than the supremum u , it can’t be an upper bound of \mathbb{N} . So there exists $m \in \mathbb{N}$ with $m > u - 1$. Therefore, $m + 1 \in \mathbb{N}$ and $m + 1 > u$. Since no element of \mathbb{N} can be greater than the upper bound u , this is a contradiction. \square

When we have a result that follows from a theorem that we just proved, we call it a corollary. You will show, in Problem 12.14, that the following is indeed a corollary of the Archimedean property.

Corollary 12.11. *For every real number a , there is an integer n such that $a < n$.*

We now turn to the well-ordering principle of \mathbb{N} , which is concerned with a fundamental property of the natural numbers. There is another important principle, called the principle of mathematical induction, which we will introduce in Chapter 18 and Project 29.3. If you work the project, you will learn that induction is one of the five Peano axioms that can be used to construct the natural numbers. For now, we will state and use the well-ordering principle without proof. In Chapter 18, we will show that the well-ordering principle of \mathbb{N} and the principle of mathematical induction are equivalent.

Well-ordering principle of the natural numbers. *Every nonempty subset of the natural numbers contains a minimum.*

As a consequence of the well-ordering principle, we obtain an interesting theorem about where the rationals “live.” The next theorem suggests that they can really fill up space! The curious thing about them, which we will return to in Chapter 23, is that there really aren’t that many of them.

Theorem 12.12. *Let a and b be two real numbers satisfying $a < b$. Then there is a rational number c such that $a < c < b$.*

The proof of this result will be much easier to follow if you understand the basic idea. It's this: if the difference between a and b were greater than one, then there would have to be an integer m with $a < m < b$ and we would be done. Of course, the difference does not have to be greater than one, but we can sort of force it to be: Look at $b - a$ and multiply by an integer n so that $n(b - a) > 1$. Now the difference between nb and na is greater than one, so there has to be an integer m between them (but this needs proof). So we will prove that there exists an integer m with $na < m < nb$. Divide by n to obtain the desired rational number, m/n .

Proof. As you will show in Problem 12.21, we may assume without loss of generality that $a > 0$. By Theorem 12.10 there is an integer n such that $n(b - a) > 1$. Thus,

$$nb > 1 + na. \quad (12.1)$$

Now consider the subset A of \mathbb{N} defined by $A = \{r \in \mathbb{N} : na < r\}$. By Corollary 12.11, A is nonempty. The well-ordering principle implies that A has a minimum, which we call m . Thus $m \in A$, and from the definition of A we see that $na < m$; in other words, $a < m/n$. Let c be the rational number m/n . Then we have the lower inequality, $a < c$, and we are halfway there. For the upper inequality, note that $m - 1$ is not in the set A (what would happen if it were?) so $na \geq m - 1$. So, putting this together with equation 12.1 we get

$$nb > 1 + na \geq 1 + (m - 1).$$

So $nb > m$, and $b > m/n$. Now $c = m/n$ is a rational number between a and b , and this completes the proof. \square

Definitions

Definition 12.1. A nonempty subset A of \mathbb{R} is **bounded above**, if there is a real number M such that $x \leq M$ for all $x \in A$. We say a nonempty subset A of \mathbb{R} is **bounded below**, if there is a real number m such that $m \leq x$ for all $x \in A$.

Definition 12.2. A nonempty subset of \mathbb{R} is **bounded** if it is bounded above and bounded below.

Definition 12.3. Let A be a nonempty subset of \mathbb{R} . A real number M that satisfies $x \leq M$ for all $x \in A$ is called an **upper bound** of A . We call a real number m that satisfies $m \leq x$ for all $x \in A$ a **lower bound** of A .

Definition 12.4. The real number M is the **maximum** of the subset A of \mathbb{R} , written $M = \max A$, if $M \in A$ and $x \leq M$ for all $x \in A$.

Definition 12.5. The real number m is the **minimum** of the subset A of \mathbb{R} , written $m = \min A$, if $m \in A$ and $m \leq x$ for all x in A .

Definition 12.6. Let A be a nonempty set of real numbers that is bounded above. Then a real number U is said to be the **supremum** of A or **least upper bound** of A , written $U = \sup A$, if

- (i) $a \leq U$ for all $a \in A$, and
- (ii) if $M \in \mathbb{R}$ satisfies $a \leq M$ for all $a \in A$, then $U \leq M$.

Definition 12.7. Let A be a nonempty set of real numbers that is bounded below. Then a real number ℓ is said to be the **infimum** of A or **greatest lower bound** of A , written $\ell = \inf A$, if

- (i) $\ell \leq b$ for all $b \in A$, and
- (ii) if $m \in \mathbb{R}$ satisfies $m \leq b$ for all $b \in A$, then $m \leq \ell$.

Solutions to Exercises

Solution (12.1). We include brief answers to each part here.

- (a) This set is bounded, and therefore bounded above and below. Some possible upper bounds are $\sqrt{5}$, 3, and 121. Some possible lower bounds are $-\sqrt{5}$, -10 , and -2π .
- (b) This set is bounded above, and it is not bounded below. Some possible upper bounds are $5^{1/3}$, 10, and 21.3.
- (c) This set is bounded, and therefore bounded above and below. Some possible upper bounds are 5, 121, and 1000. Some possible lower bounds are 0, -3 , and -12 .
- (d) This set is bounded above and below, and therefore bounded. Every real number greater than or equal to $\sqrt{2}$ will work as an upper bound, and every real number less than or equal to $-\sqrt{2}$ will work as a lower bound.

Solution (12.4). Our intuition tells us that we have $\sup\{x \in \mathbb{R} : x^2 \leq 5\} = \sqrt{5}$, $\sup\{x \in \mathbb{R} : x^3 < 5\} = 5^{1/3}$, $\sup\{x \in \mathbb{N} : x \leq 5\} = 5$, and $\sup\{x \in \mathbb{Q} : x^2 < 2\} = \sqrt{2}$.

Solution (12.5). Let $M = \max A$. Then $a \leq M$ for all $a \in A$ and property (i) of the definition of supremum is fulfilled. Now suppose that K is a real number satisfying $a \leq K$ for all $a \in A$. Since M is in A we have in particular that $M \leq K$. Thus, property (ii) holds and $M = \sup A$.

By Lemma 12.3, the supremum of A is unique. Since $\max A$ is the supremum of A , it is also unique.

Solution (12.6).

- (a) Let A be a nonempty set of real numbers that is bounded below. A real number m is the infimum (or greatest lower bound) of A if
 - (i) $a \geq m$ for all $a \in A$, and
 - (ii) if y is a real number satisfying $a \geq y$ for all $a \in A$, then $m \geq y$.

- (b) Let $A = \{x \in \mathbb{R} : x > 10\}$. Then A is bounded below (e.g., by 0), nonempty (e.g., $20 \in A$), and $\inf A = 10$. This can be seen as follows.
- (i) $a \geq 10$ for all $a \in A$ by the definition of A .
 - (ii) If y is a real number satisfying $a \geq y$ for all $a \in A$ and $y > 10$, then $10 < (y + 10)/2 < y$. Thus $(y + 10)/2 \in A$ and $(y + 10)/2 \not\geq y$. This is a contradiction and it follows that $y \leq 10$.

These two conditions imply that $\inf A = 10$.

Using the set A above, $0 \neq \inf A$ and $20 \neq \inf A$, giving two nonexamples.

We do not seem to be able to find a nonempty set that is bounded below and does not have an infimum. That no such set exists will follow from Exercise 12.9 below.

Solution (12.8).

In this problem we assume that there is a real number, x , with the property that $x^2 = 5$. Similarly, we assume that there is a real number y with the property that $y^3 = 5$. A rigorous argument for the existence of x will be given in Theorem 13.2.

First, let $S = \{x \in \mathbb{R} : x^2 \leq 5\}$. We claim that $m = -\sqrt{5} = \inf S$. If $x \in S$, then $x^2 \leq 5 = m^2$. Thus, $|x| \leq |m|$. Since $m < 0$, we have $m \leq |x| \leq -m$. So we conclude that $m \leq x$. Thus m is a lower bound of S . If v is any other lower bound of S , then $v \leq -\sqrt{5}$ because $-\sqrt{5} \in S$. Thus $v^2 \geq 5 = m^2$ and hence $v \leq m$. This establishes the claim. (This illustrates Exercise 12.5. We could also have used the result of this exercise and we will, from here on.) An entirely similar proof shows that $\sup S = \sqrt{5}$.

For the second set, $T = \{x \in \mathbb{R} : x^3 < 5\}$, note that T is not bounded below. Hence it has no infimum. In Exercise 12.4 we claimed that $\sup T = 5^{1/3}$. Set $M = 5^{1/3}$. If $x \in T$, then $x^3 < 5 = M^3$. Hence $x < M$, showing that M is an upper bound. Suppose that U is an upper bound of T and that $U < M$. Then $U < (U + M)/2 < M$. Thus $(U + M)/2 \in T$. This shows that U cannot be an upper bound and implies that $M = \sup T$.

Finally, the third set is simply $W = \{0, 1, 2, 3, 4, 5\}$. We see that 0 is the minimum and 5 is the maximum. From Exercise 12.5, we conclude that the infimum is 0 and the supremum is 5.

We note here that the fourth set is more complicated because of the requirement that x be a member of \mathbb{Q} .

Solution (12.9). Completeness axiom of \mathbb{R} ; infimum version. *Every nonempty subset of real numbers that is bounded below has an infimum.*

To show the equivalence of the two versions we first assume that every nonempty set of real numbers that is bounded above has a supremum. Let S be a nonempty subset of the reals that is bounded below. Define $T = \{x \in \mathbb{R} : -x \in S\}$. By the result of Problem 12.7, we conclude that T is bounded above. By the completeness axiom of \mathbb{R} , the set T has a supremum. Again using the result of Problem 12.7, we conclude that the set S has an infimum. This establishes the infimum version of the axiom.

A similar proof establishes the fact that the infimum version of the completeness axiom implies the supremum version.

Problems

Problem 12.1. A student solved the following problem: Let $S = \mathbb{Q} \cap (0, 4)$. Show that $\sup S = 4$. Below is the student's solution. Criticize it.

Not a proof (Student Solution). First we show that 4 is an upper bound. Let $x \in S$. Then $0 < x < 4$, so 4 is clearly an upper bound. Suppose to the contrary that 4 is not the supremum. Then there exists an upper bound u with $u < 4$. But $u < (u + 4)/2$, and we have shown that u is not an upper bound of S . This shows that 4 must be the supremum. \square

Problem 12.2. Consider the sets below. For each one, decide whether the set is bounded above. If it is, give the supremum in \mathbb{R} . Then decide whether or not the set is bounded below. If it is, give the infimum. Finally, decide whether or not the supremum is a maximum, and whether or not the infimum is a minimum:

- The closed interval $[0, 4]$;
- The open interval $(0, 4)$;
- The natural numbers \mathbb{N} ;
- The set $[0, \sqrt{2}] \cap \mathbb{Q}$.

Problem 12.3. Consider the interval $(1, 4)$ in \mathbb{R} . Show in detail

- that 4 is the supremum, and
- that 1.1 is not a lower bound.

Problem 12.4. Let $X = \mathcal{P}(\mathbb{N}) \setminus \{\emptyset\}$. For $R, S \in X$ we define $R \sim S$ if and only if $\min R = \min S$.

- Give an example of two different elements of X that are related to each other with respect to the relation \sim defined above.
- Prove that \sim as defined above is an equivalence relation on X .

Problem 12.5. Show that $\inf\{1/n : n \in \mathbb{Z}^+\} = 0$.

Problem 12.6. Show that $\sup\{1 - 1/n : n \in \mathbb{Z}^+\} = 1$.

Problem[#] 12.7. Let $S \subseteq \mathbb{R}$ and define $T = \{x \in \mathbb{R} : -x \in S\}$.

- Prove that if S is nonempty and bounded below, then T is bounded above. Further, prove that if $\sup T$ exists, then $\inf S$ exists and $\inf S = -\sup T$.
- Prove that if S is nonempty and bounded above, then T is bounded below. Further, prove that if $\inf T$ exists, then $\sup S$ exists and $\sup S = -\inf T$.

Problem[#] 12.8. Let S be a nonempty subset of \mathbb{R} . Prove that S is bounded if and only if there exists $M \in \mathbb{R}$ such that $|x| \leq M$ for all $x \in S$.

Problem[#] 12.9. Let S be a nonempty bounded subset of \mathbb{R} . Show that $\inf S \leq \sup S$. Under what conditions on S would you have $\inf S = \sup S$?

Problem 12.10. Let S be a nonempty bounded subset of \mathbb{R} and let u be a real number such that $u < \sup S$. Show that there exists $s \in S$ such that $u < s$.

Problem 12.11. Let S and T be nonempty bounded subsets of \mathbb{R} .

- Show that $\sup(S \cup T) \geq \sup S$, and $\sup(S \cup T) \geq \sup T$.
- Show that $\sup(S \cup T) = \max\{\sup S, \sup T\}$.
- Try to state the results of (a) and (b) in English, without using mathematical symbols.

Problem 12.12. Let $x \in \mathbb{R}$ and let S be a nonempty subset of \mathbb{R} that is bounded above. We define a new set, $x + S$, by $x + S = \{x + s : s \in S\}$.

- Prove that $x + S$ is bounded above.
- Prove that $x + \sup S$ is an upper bound of $x + S$. Using this result, conclude that $\sup(x + S) \leq x + \sup S$.
- Prove that $x + \sup S = \sup(x + S)$.

Problem 12.13. Let A and B denote nonempty bounded subsets of \mathbb{R} and define $A \oplus B = \{x + y : x \in A, y \in B\}$.

- Prove that $A \oplus B$ is also a nonempty bounded subset of \mathbb{R} .
- Let $A = [1, 3]$ and $B = [2, 4]$. Find $A \oplus B$, $\sup A$, $\sup B$, and $\sup(A \oplus B)$.
- Show that $\sup(A \oplus B) \leq \sup A + \sup B$.
- Show that $\sup A + \sup B \leq \sup(A \oplus B)$.

Problem# 12.14. Prove Corollary 12.11.

Problem 12.15. Find the supremum and infimum of the set $(0, 2) \cap \mathbb{Q}$ and justify your answer. (If you haven't worked Problem 12.1, you might want to work it before solving this problem.)

Problem 12.16. Let ε be a positive real number. Prove that for every real number a , there exists a rational number b (depending on a) such that $|a - b| < \varepsilon$.

Problem# 12.17. Prove that if a subset A of the reals has an infimum, then the infimum is unique.

Problem 12.18. Prove that every nonempty bounded subset of \mathbb{N} has a maximum.

Problem 12.19. Show that there does not exist a real number b such that $a \leq b$ for all $a \in \mathbb{R}$.

Problem 12.20. Let $a \in \mathbb{Q}$, $a \neq 0$, and $b \in \mathbb{R} \setminus \mathbb{Q}$. Prove the following:

- $a + b \in \mathbb{R} \setminus \mathbb{Q}$;
- $ab \in \mathbb{R} \setminus \mathbb{Q}$;
- $1/b \in \mathbb{R} \setminus \mathbb{Q}$.

Problem# 12.21. Suppose that we have established Theorem 12.10 for the case when $a > 0$; that is, suppose we know that if a and b are real numbers and $0 < a < b$, then there exists a rational number r with $a < r < b$. Show that it follows that for all real numbers x and y with $x < y$, there is a rational number s with $x < s < y$. (This is what we meant by “we may assume without loss of generality that $a > 0$.” We suggest you add an appropriate real number M to x and y to reduce your problem to the case $0 < a < b$.)

Chapter 13

Consequences of the Completeness of \mathbb{R}

We have now reached the point at which we can give rigorous proofs of two facts you have known for some time. We mention the second first; that is, we will conclude this chapter by showing that there is a nonempty bounded subset of \mathbb{Q} that does not have a supremum in \mathbb{Q} . As an exercise, you will show that there is also a nonempty bounded subset of \mathbb{Q} that does not have an infimum in \mathbb{Q} . In this sense, \mathbb{Q} is not complete. Since \mathbb{R} is complete, there must be numbers in \mathbb{R} that are not in \mathbb{Q} . We know what these numbers are, of course; they are the irrational numbers. Thus far we haven't proven that a particular real number is irrational. But now we can! This will be the first fact that we prove. Here's a rough outline: We will show that if a is a positive real number, then a has a positive square root; that is, there exists $x \in \mathbb{R}^+$ such that $x^2 = a$. But Theorem 5.2 told us that $\sqrt{2}$ is not rational. Thus, we know $\sqrt{2}$ exists and we know it is not rational. Therefore, we have a rigorous proof that $\sqrt{2}$ is irrational.

This might be a good time to put in a plug for a project: It's much harder than you might think to prove that a particular number is irrational. We take for granted that e and π are irrational, but proving this is really not so easy. You can do so if you work Project 29.5.

Before we get to the heart of this chapter, we will get a little more practice with least and greatest lower bound. You should solve the exercise below before proceeding to the next theorem.

Exercise 13.1. Let $a = \sup\{w \in \mathbb{R}^+ : w^2 < 2\}$. Show that if $0 < c < a$, then $c^2 < 2$. ○

Theorem 13.2 (Existence of square roots in \mathbb{R}^+). *There exists a positive real number a such that $a^2 = 2$.*

In order to help you better understand this proof, we'll indicate how we "devised a plan." The basic idea is that the square root should be the supremum of the set $A = \{w \in \mathbb{R}^+ : w^2 < 2\}$. The completeness axiom tells us this supremum exists, so we'll call it a . How do we show that a is the square root of 2? Well, we need to

show that $a^2 = 2$. If $a^2 > 2$, our intuition tells us that we should be able to subtract something off of a , which we'll call x , and come up with something smaller than a that is still an upper bound of the set. Thus $a - x$ would be an upper bound smaller than the supremum, and this would contradict the fact that a is the least upper bound. So we now have to worry about the case in which $a^2 < 2$. In this case, our intuition tells us that we should be able to add just a little bit to a , which we'll call y , and find an element of A , namely, $a + y$, that is bigger than the upper bound a . This now contradicts the fact that a is an upper bound. So, since neither of these two cases can occur, the only other possibility, $a^2 = 2$, must be the one that holds.

Proof. Let $A = \{w \in \mathbb{R}^+ : w^2 < 2\}$. Then A is a nonempty subset of \mathbb{R} (since $1 \in A$), and A is bounded above (by, for example, 2). By the completeness axiom A has a supremum, which we denote by a . What we know so far is that a is a real number, and $1 \leq a \leq 2$. We will show that $a^2 = 2$.

We know that one of the following three cases must occur: $a^2 > 2$, $a^2 < 2$, or $a^2 = 2$. We'll show that the first two cases are impossible.

Case 1. Suppose that $a^2 > 2$. Let $x = (a^2 - 2)/(2a)$. (We'll explain the choice of this x after the proof.) Then, as you can check, $0 < a - x < a$. By Exercise 13.1 we know that $(a - x)^2 < 2$. But

$$(a - x)^2 = a^2 - 2a + x^2 \geq a^2 - 2ax = 2.$$

So $(a - x)^2 < 2$ and $(a - x)^2 \geq 2$. This is impossible and we conclude that Case 1 cannot occur.

Case 2. Suppose that $a^2 < 2$. Let $y = (2 - a^2)/(3a)$. (You'll explain the choice of this y in Problem 13.10, after you have read our explanation for the choice of x for Case 1.) Then $y > 0$, and therefore $a + y > a$. Since a is an upper bound of A , we see that $a + y \notin A$. Thus $(a + y)^2 \geq 2$. We will show that $y < a$, and then use this to obtain our contradiction. To this end, note that because $1 \leq a$ we have

$$a - y = (4a^2 - 2)/(3a) > 0.$$

Thus, $y < a$, as claimed. Since $y < a$, we also know that $y^2 < ay$. Thus,

$$(a + y)^2 = a^2 + 2ay + y^2 < a^2 + 2ay + ay = a^2 + 3ay = 2.$$

So, $(a + y)^2 \geq 2$ and $(a + y)^2 < 2$. This is impossible, and we conclude that Case 2 cannot occur.

Thus we conclude that the only remaining possibility holds, and therefore $a^2 = 2$. \square

We promised an explanation for our choice of x . Here it is: We wanted x to satisfy two conditions, $0 < x < a$ and $(a - x)^2 \geq 2$. The second condition is difficult to solve (without resorting to $\sqrt{2}$). Let's concentrate on $(a - x)^2 \geq 2$. Once we know which x satisfy this inequality, we'll worry about satisfying $0 < x < a$. So we want to solve $(a - x)^2 \geq 2$, and we will do so by following Pólya's advice about simplifying the problem. We note that $(a - x)^2 = a^2 - 2ax + x^2 \geq a^2 - 2ax$. Now, if we make

$a^2 - 2ax = 2$, then we have also made $(a - x)^2 \geq 2$. So, now we have arrived at an easier problem: Find x such that $a^2 - 2ax = 2$. Solving this we get $x = (a^2 - 2)/2a$. This will be our first guess for x . If it doesn't satisfy $0 < x < a$, we'll need to adjust it. But we know that $1 \leq a \leq 2$ so $x < 2$, and we suppose that $a^2 > 2$ so $0 < x$. Thus, $0 < x < 2$, as desired. The proof shows that, in fact, this choice does everything it needs to do.

A similar proof can be used to show that for every $x > 0$ and every positive integer n , there exists a unique real number $a > 0$ such that $a^n = x$. Uniqueness follows easily from the fact that if $a, b > 0$ and $a < b$, then $a^n < b^n$. (See [92, p. 10] for a proof of the existence and uniqueness of n th roots.) This real number is sometimes called the principal n th root of x . From here on, we will assume the existence of n th roots and we will use the usual rules of exponentiation.

The completeness axiom of \mathbb{R} says that if we start with a nonempty set that is bounded above, we can find its supremum. In \mathbb{Q} , this is not the case: We can find a nonempty subset of \mathbb{Q} that is bounded above but has no supremum in \mathbb{Q} . In other words, there is no completeness axiom for \mathbb{Q} . There are simpler examples of sets that are not complete and we provide one such example below.

Exercise 13.3. Show that if $S = [0, 1) \cup (1, 2]$, there is a nonempty bounded subset T of S for which there is no $b \in S$ that satisfies both

- (i) $x \leq b$ for all $x \in T$, and
- (ii) if $c \in S$ and $x \leq c$ for all $x \in T$, then $b \leq c$. ○

There are many subsets of \mathbb{R} that are complete and there are many that are not complete, but it is not our goal in this chapter to discuss the completeness properties of all subsets of \mathbb{R} . Dealing with subsets can be a bit tricky, and we prefer not to get into the details in this text. Instead, we will focus on one of the most important subsets of \mathbb{R} —the rationals.

Example 13.4. Show that the set \mathbb{Q} is not complete; that is, show that there is a nonempty set B of rational numbers that is bounded above, but no rational number b satisfies both

- (i) $x \leq b$ for all $x \in B$, and
- (ii) if $c \in \mathbb{Q}$ and $x \leq c$ for all $x \in B$, then $b \leq c$.

Proof. Let $B = \{x \in \mathbb{Q}^+ : x^2 < 2\}$. Then B is nonempty ($1 \in B$) and bounded above (2 is an upper bound). Suppose to the contrary that the rational number b satisfies conditions (i) and (ii) above. If such a rational number b exists, it must satisfy one of the following three things: $b = \sqrt{2}$, $b > \sqrt{2}$, or $b < \sqrt{2}$. We'll show that no rational number can satisfy one of these.

We know from Theorem 5.2 that $\sqrt{2}$ is not rational, and we know from our assumptions that b is rational. So $b \neq \sqrt{2}$.

Suppose that $b > \sqrt{2}$. By Theorem 12.12, there is a rational number c such that $\sqrt{2} < c < b$. Now the supremum of the set $A = \{x \in \mathbb{R}^+ : x^2 < 2\}$ is, as we have just seen in Theorem 13.2, $\sqrt{2}$. For every $x \in B$ we know that $x \in A$ and consequently

$x \leq \sqrt{2} < c$. Thus c satisfies the hypotheses of (ii). But $c < b$, and therefore c does not satisfy the conclusion of (ii). This implies that this case cannot occur.

Now suppose that $b < \sqrt{2}$. By Theorem 12.12, there is a rational number c with $b < c < \sqrt{2}$. The right side of this inequality (together with the fact that $c > 0$) tells us that $c^2 < 2$ and therefore $c \in B$. But $c > b$, and this contradicts the fact that b satisfies condition (i) above. This implies that this case cannot occur.

Thus we conclude that there is no rational number satisfying conditions (i) and (ii) above. \square

Exercise 13.5. We showed that \mathbb{Q} is not complete by showing that when we consider the set $B = \{x \in \mathbb{Q}^+ : x^2 < 2\}$, there is no $b \in \mathbb{Q}$ satisfying (i) and (ii) of Example 13.4. Using that result, show that there is a nonempty bounded set C in \mathbb{Q} for which there is no $u \in \mathbb{Q}$ satisfying

- (i) $w \geq u$ for all $w \in C$, and
- (ii) if $z \in \mathbb{Q}$ and $w \geq z$ for all $w \in C$, then $u \geq z$. \circ

By the way, there is still something “missing” in \mathbb{R} —the square root of -1 . So you might decide to look at complex numbers ... but that’s another story. If it’s a story you are interested in learning more about, you can begin by looking at Project 29.6 and the references that appear there.

Definitions

Definition 13.1 (for Problems 13.13 through 13.15). The relation \preceq on a nonempty set S is called a **partial order** if the following three conditions are satisfied:

- (i) (Reflexive property) For all $x \in S$, we have $x \preceq x$.
- (ii) (Transitive property) For all $x, y, z \in S$, if $x \preceq y$ and $y \preceq z$, then $x \preceq z$.
- (iii) (Antisymmetric property) For all $x, y \in S$, if $x \preceq y$ and $y \preceq x$, then $x = y$.

Definition 13.2 (for Problems 13.13 through 13.15). The relation \preceq on a nonempty set S is called a **total order** if it is a partial order with the following additional property:

- (iv) For all $x, y \in S$, we have $x \preceq y$ or $y \preceq x$.

Solutions to Exercises

Solution (13.1). Since $c < a$, we know that $c \neq \sup\{w \in \mathbb{R}^+ : w^2 < 2\}$. Therefore, there exists $w \in \mathbb{R}^+$ such that $w^2 < 2$ and $c < w$. Since $c > 0$, we have $c^2 < cw$. Since $w > 0$, we have $cw < w^2$. Putting this together, we have $c^2 < w^2 < 2$, as desired.

Solution (13.3). Claim: If $T = [0, 1)$, then there is no element $b \in S = [0, 1) \cup (1, 2]$ satisfying the stated conditions for this T : Suppose there were such an element. We cannot have $b = 1$, because $b \in S$ and $1 \notin S$. Thus, $b < 1$ or $b > 1$.

Suppose $b < 1$, then $(b+1)/2 < 1$ and, since $b \in S$, we have $(b+1)/2 > 0$. So $(b+1)/2 \in T$ and $(b+1)/2 > b$, which contradicts (i).

Therefore, we must have $b > 1$. In this case, we consider $(b+1)/2 > 1$. Then $1 < (b+1)/2 < b \leq 2$. But then $c = (b+1)/2 \in S$ and $t \leq c$ for all $t \in T$. Therefore c satisfies the hypothesis of (ii), but not the conclusion since $c < b$. This completes the proof.

Solution (13.5). We define the set $C = \{w \in \mathbb{Q}^- : w^2 < 2\}$. Suppose to the contrary that there exists $u \in \mathbb{Q}$ that satisfies conditions (i) and (ii) stated in this exercise. Let $b = -u$ and note that $b \in \mathbb{Q}$. We will show that b satisfies conditions (i) and (ii) of Example 13.4.

If $x \in B$, we let $w = -x$. Then $w^2 = (-x)^2 = x^2 < 2$. Since $x \in \mathbb{Q}^+$, we have $w \in \mathbb{Q}^-$. Hence $w \in C$. Condition (i) shows that $u \leq w$. Thus $x = -w \leq -u = b$. Hence for all $x \in B$, we have $x \leq b$. Therefore, condition (i) of Example 13.4 is satisfied.

Now suppose $c \in \mathbb{Q}$ and $x \leq c$ for all $x \in B$. If $w \in C$, let $x = -w$. Note that $x^2 = (-w)^2 = w^2 < 2$ and $x \in \mathbb{Q}^+$. Thus, $x \in B$ and $x \leq c$. So $w = -x \geq -c$. Taking $z = -c$ in condition (ii), we have shown that $w \geq z$ for all $w \in C$. We conclude that $u \geq z$. Thus $b = -u \leq -z = c$; that is, $b \leq c$ and condition (ii) of Example 13.4 is satisfied.

The existence of the rational number b contradicts the result of Example 13.4. Hence there can be no rational number u corresponding to the set C that satisfies the two conditions of this exercise.

Problems

Problem 13.1. Find the supremum and infimum (in \mathbb{R}) of the subset $T = [0, \pi) \cap \mathbb{Q}$ of \mathbb{R} . Justify your answers! You may assume that π is irrational, if that is helpful.

Problem 13.2. Let T be a nonempty subset of $[0, 1]$. Then T has an infimum m and a supremum M in \mathbb{R} . Show that m and M belong to $[0, 1]$.

Problem 13.3. Consider the subset $S = \mathbb{R} \setminus \mathbb{Z}$ of \mathbb{R} . Give an example of a subset T_1 of S that has an infimum and supremum in S and a bounded subset T_2 of S that has neither an infimum nor supremum in S .

Problem 13.4. Suppose S is a nonempty bounded subset of \mathbb{R} and u is the infimum of S . Let $v = \inf\{x \in S : x > u\}$. Show that $v \geq u$.

Problem 13.5. Show that the set $S = [0, 1] \cap \mathbb{Q}$ is not complete by showing that there is a nonempty bounded subset T of S for which there is no element $b \in S$ satisfying

- (i) $x \leq b$ for all $x \in T$, and
- (ii) if $c \in S$ and $x \leq c$ for all $x \in T$, then $b \leq c$.

Problem 13.6. Let x and y be two real numbers and let $S = \{x, y\}$.

- (a) Prove that

$$\max\{x, y\} = \frac{|x - y| + x + y}{2}.$$

- (b) Find a similar formula for the minimum.
- (c) Explain why these formulas also yield formulas for $\inf S$ and $\sup S$.

Problem 13.7. If A and B are subsets of \mathbb{R} for which $\sup A = \sup B$ and $\inf A = \inf B$, must $A = B$? Either prove this or give a counterexample.

Problem 13.8. Suppose that A and B are disjoint bounded intervals in \mathbb{R} . Prove that $\inf A \geq \sup B$ or $\inf B \geq \sup A$. You may use the fact that if $a_1, a_2 \in A$ with $a_1 < a_2$, then the interval $[a_1, a_2] \subseteq A$. (Of course, you may use the corresponding fact for B .)

Problem 13.9. For each of the following, either prove the statement or provide a counterexample.

- (a) Let S be a subset of \mathbb{R} consisting of 20 positive integers. Then S has a supremum U and an infimum u and both u and U belong to S .
- (b) Suppose that S is a nonempty subset of \mathbb{R} and S has a supremum U . Let $T = \{x \in S : x \leq U\}$. Then $T = S$.
- (c) Suppose S is a nonempty bounded subset of \mathbb{R} and $U = \sup S$. Suppose further that there exists an $x \in S$ with $x < U$. Let $v = \sup\{x \in S : x < U\}$. Then $v < U$.

Problem 13.10. In the proof of Theorem 13.2, we let $y = (2 - a^2)/(3a)$ for the case $a^2 < 2$.

Explain this choice of y along the lines of the explanation for the choice of x following the proof of Theorem 13.2. (We need a real number y satisfying $0 < y < a$ and $(a + y)^2 \leq 2$. Solve a simpler problem.)

Problem 13.11. Prove that if a is a rational number, then there is an irrational number b such that $a < b$.

Problem 13.12. Prove that for two arbitrary real numbers a and b with $a < b$, there is an irrational number c such that $a < c < b$. (Hint: Consider $a/\sqrt{2}$ and $b/\sqrt{2}$.)

Problem 13.13. Let \preceq denote a relation on a nonempty set S . The relation \preceq is called a **partial order** if the following three conditions are satisfied.

- (i) (Reflexive property) For all $x \in S$, we have $x \preceq x$.
- (ii) (Transitive property) For all $x, y, z \in S$, if $x \preceq y$ and $y \preceq z$, then $x \preceq z$.
- (iii) (Antisymmetric property) For all $x, y \in S$, if $x \preceq y$ and $y \preceq x$, then $x = y$.

The relation \preceq is a **total order** on the nonempty set S if, in addition, (iv) below is satisfied.

(iv) For all $x, y \in S$, we have $x \preceq y$ or $y \preceq x$.

The last condition says that we can always compare two elements x and y in S using the relation. (A partially ordered set is sometimes called a poset. It's much less common to call a totally ordered set a toset.)

Show that the usual \leq relation defines a total order on \mathbb{R} .

Problem 13.14. This problem uses the definitions introduced in Problem 13.13.

Let A be a set containing at least two elements. We define an order on $\mathcal{P}(A)$ using set inclusion \subseteq . Show that \subseteq is a partial order, but not a total order on $\mathcal{P}(A)$.

Problem 13.15. This problem uses the definitions introduced in Problem 13.13. Consider the relation $<$ on \mathbb{R} . Show that this is not a total order by exhibiting counterexamples for each property ((i)–(iv)) violated in the definition of total order.

Problem 13.16. Prove that there exists $x \in \mathbb{R}^+$ with $x^2 = 3$.

Problem 13.17. Prove that there is no $x \in \mathbb{Q}$ with $x^2 = 12$, but there is an $x \in \mathbb{R}^+$ such that $x^2 = 12$. (You might find Problem 13.16 helpful.)

Problem 13.18. In Problem 13.14 you showed that $(\mathcal{P}(\mathbb{Z}), \subseteq)$ is a partial order. For every nonempty subset \mathcal{A} of $\mathcal{P}(\mathbb{Z})$ we say that $U \in \mathcal{P}(\mathbb{Z})$ is an upper set of \mathcal{A} , if $X \subseteq U$ for all $X \in \mathcal{A}$. A nonempty set $\mathcal{A} \subseteq \mathcal{P}(\mathbb{Z})$ will be called an upper bounded set if there is an upper set of \mathcal{A} in $\mathcal{P}(\mathbb{Z})$. We say $U_0 \in \mathcal{P}(\mathbb{Z})$ is a least upper set if (i) U_0 is an upper set of \mathcal{A} and (ii) if U is another upper set of \mathcal{A} , then $U_0 \subseteq U$.

- Let $\mathcal{B} = \{\{1, 2, 5, 7\}, \{2, 8, 10\}, \{2, 5, 8\}\}$. Show that \mathcal{B} is an upper bounded set and find a least upper set of \mathcal{B} , if there is one.
- Prove that every nonempty subset of $\mathcal{P}(\mathbb{Z})$ is upper bounded.
- Define “lower set,” “lower bounded set,” and “greatest lower set.”
- Let \mathcal{A} be a nonempty subset of $\mathcal{P}(\mathbb{Z})$. Using union and intersection, find an expression for least upper set of \mathcal{A} and greatest lower set of \mathcal{A} .
- Prove that $(\mathcal{P}(\mathbb{Z}), \subseteq)$ has the “least upper set property” (in other words, show every upper bounded set has a least upper set).

Problem 13.19. Prove that (\mathbb{Z}, \leq) is complete in the following sense: If A is a nonempty set of integers that is bounded above, then there is an integer a such that $a = \sup A$.

Problem 13.20. Let S be a nonempty subset of \mathbb{R} , and $x \in \mathbb{R}$. Suppose that there exists $y \in S$ with $y < x$. Let $y_0 = \sup\{y \in S : y < x\}$.

- Give an example of such a set S and real number x .
- Show that $y_0 \leq x$.
- Give an example to show that y_0 may equal x .
- Give an example to show that y_0 may be strictly less than x .

Problem 13.21. Prove the following statement: For every positive irrational real number a with $\sqrt{a} < 10000$, there is a positive integer n such that

$$\frac{10000}{n} < \sqrt{a} < \frac{10000}{n-1}.$$

Problem# 13.22. To practice some of the more challenging theorems in this and the previous chapter, we use some of the techniques we have discussed to establish the division algorithm in \mathbb{Z} . We wish to prove:

Theorem 13.6 (Division algorithm). *Let m and n be integers with $n \neq 0$. Then there exist $q, r \in \mathbb{Z}$ satisfying $m = nq + r$, where $0 \leq r < |n|$ and q and r are unique.*

We outline the proof below. You should complete the details.

- Let $A = \{m - nx : x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Show that A is nonempty.
- Explain why there exists $r \in \mathbb{Z}$ such that $r = \min A$.
- Explain why $0 \leq r < |n|$.
- Use your work above to prove that there are $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r < |n|$.
- We now need to show uniqueness. Recall that to show q and r are unique, we will assume that there exist q_1 and r_1 satisfying several properties. Write out the properties.
- Show that $|n| \mid (r - r_1)$ and that $-|n| < r - r_1 < |n|$.
- Finish the proof.

Tips: You Solved It. Now What?

Let's say we are now at the point where you solved the given problem and wrote up your first draft.

- Look over your solution. Does it use everything you are given?
- Is the answer reasonable?
- If there were places where you were unsure of your argument, check over those arguments carefully. You might find it helpful to write the solution, take a break, and then check the solution. (We say that a lot, don't we?)
- Is your argument clear? Did you choose your notation well? Is your notation clear and unambiguous? Did you introduce all notation before you used it?
- Is there a shorter or more intuitive argument?
- Do you fully understand what you did? Spend some time thinking about the method and what you proved. Could you have gotten a better result?
- When do these methods work? What are the restrictions? Where have you seen them before?
- If the problem was hard for you to solve, what made it hard? What were the important ideas that you were missing?

- This is a good opportunity to learn about yourself, too. Which problems do you like best? Why?

Chapter 14

Functions, Domain, and Range

What is a function? You've probably gotten a definition of this somewhere along the way. We will state the definition of function in terms of relations, which is probably different than the way you have seen it stated.

Let A and B be sets. A **function f from A to B** is a relation f from A to B satisfying

- (i) for all $a \in A$, there exists $b \in B$ such that $(a, b) \in f$, and
- (ii) for all $a \in A$, and all $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

A function is often called a **map** or **mapping**. We usually write $f : A \rightarrow B$ to indicate that f is a function from A to B . The sets A and B may be explicitly identified, but they are often understood from the context. (See Problem 14.4.)

When we know what the two sets are and that the two conditions are satisfied, we say f is a well-defined function. If the object we try to define does not satisfy these properties, it isn't a function, and we often say that f (which we shouldn't call a function) is not well-defined.

Condition (i) makes sure that each element in A is related to some element of B , while condition (ii) makes sure that no element of A is related to more than one element of B . Note that it may be the case that an element of B has no element of A to which it is related; or an element of B could be related to more than one element of A . The set A is called the **domain**, and denoted by $\text{dom}(f)$, and the set B is called the **codomain**, and denoted $\text{cod}(f)$.

As a first example, consider the function that assigns to a citizen of the United States his or her height measured in inches on a particular day at a particular time. We'll assume that people are at most 20 feet tall. This is a function because we have a *domain* (the set of the citizens of the United States on a particular day at a particular time), a *codomain* (the set of real numbers between 0 and 240 inches), *condition (i)* (each person has a height), and *condition (ii)* (each person has exactly one height on that day, at that time). Now let's turn to a nonexample. We still consider the domain to be the set of citizens of the United States, but this time let the codomain consist of all the countries in the world (on a particular day, at a particular time). Consider the relation that assigns to each person in the domain his or her country

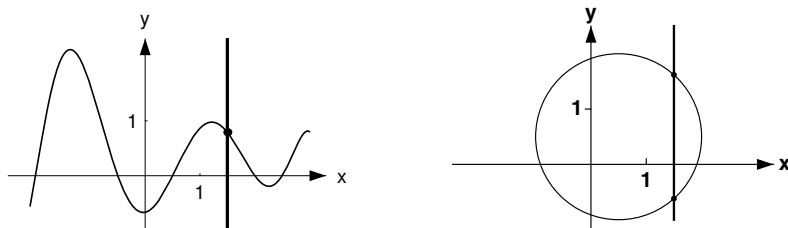


Fig. 14.1

(countries) of citizenship. This is not a function because a United States citizen can be a citizen of more than one country. Though (i) is satisfied because each person in the domain is a U.S. citizen, (ii) is not.

Exercise 14.1. Let $A = \{1, 2, 3\}$ and $B = \{2, 4, 6\}$. Which of the following are functions from A to B ? If they are not functions, explain which rule is violated.

- (a) The relation f is $\{(1, 2), (2, 4), (3, 4)\}$.
- (b) The relation f is $\{(1, 2), (1, 4), (2, 2), (3, 6)\}$.
- (c) The relation f is $\{(1, 2), (3, 4)\}$.
- (d) The relation f is $\{(2, 4), (1, 2), (3, 6)\}$.

Exercise 14.2. You probably learned that a function $f : \mathbb{R} \rightarrow \mathbb{R}$ can be represented by a graph, and that there is a vertical line test to determine whether or not f is a function (see Figure 14.1). Which condition in the definition corresponds to the vertical line test? Why?

In Exercise 14.1, you probably recognized (d) as a function from A to B . It is more usual to write $f(1) = 2$, $f(2) = 4$, and $f(3) = 6$. Since each x in the domain is related to a unique y in the codomain, we will write $f(x) = y$ rather than $(x, y) \in f$.

Exercise 14.3. Rewrite the definition of a function using the notation introduced in the paragraph above.

Here are some more examples and nonexamples of functions.

Exercise 14.4. Decide which of the following are functions and which are not, giving reasons for your answers.

- (a) Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = 3x + 2$.
- (b) Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = 1/x^2$.
- (c) Let $f : \mathbb{R} \rightarrow \mathbb{R}^2$ be defined by $f(x) = (x, x)$.
- (d) Let $f : \mathbb{Q} \rightarrow \mathbb{Q}$ be defined by $f(p/q) = 1/q$, where p and q are integers and $q \neq 0$.
- (e) Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be defined by $f(x, y) = (x, 3)$.

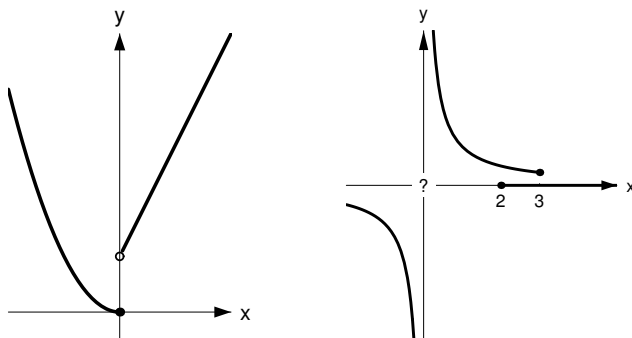


Fig. 14.2 The graph on the left is of f , the one on the right is of g

You have seen many examples of functions. One particular type of example, that of a function defined in cases, allows us to explicitly illustrate many of the ideas discussed in this section. Before you begin working with a function that is defined in cases, make sure that you understand the function. If you can, graph it. Remember that the best thing to do is to work with concrete objects (like trying $x = 2$ or $x = -3$) until you get a feel for what is happening. For functions that are defined in cases we have to be particularly careful to check that the cases don't overlap; or if they do, that the function is defined in a unique way for all the elements in the domain that are in the overlap. Of course, we are not changing the rules here. All you really have to do is check that you know what the domain and codomain are, and that conditions (i) and (ii) of the definition hold. Here are some examples.

Example 14.5. We will check to see whether each of the objects defined below and graphed in Figure 14.2 is a function.

(a) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = \begin{cases} x^2 & \text{if } x \leq 0 \\ 2x + 1 & \text{if } x > 0 \end{cases}.$$

(b) Let $g: \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$g(x) = \begin{cases} 0 & \text{if } x \geq 2 \\ 1/x & \text{if } x \leq 3 \end{cases}.$$

For (a) note that the domain is \mathbb{R} and the codomain is also \mathbb{R} . From the definition of f it is easy to see that f is defined for all $x \in \mathbb{R}$. Hence condition (i) of the definition of a function holds.

Now let $a \in \mathbb{R}$ and suppose that there exist real numbers b and c with $f(a) = b$ and $f(a) = c$. The most orderly way to check condition (ii) is the following: If $a \leq 0$, then $b = f(a) = a^2$ and $c = f(a) = a^2$, so $b = c$. If $a > 0$, then $b = f(a) = 2a + 1$ and $c = f(a) = 2a + 1$. Hence $b = c$. In either case, $b = c$. So condition (ii) holds. Since both (i) and (ii) are satisfied, f is well-defined.

The formula given in part (b) does not define a function for two reasons. First note that 0 is in the domain. Since $0 \leq 3$, we see that $g(0)$ is not defined to be an element in the codomain. Hence condition (i) is violated, and we conclude that g is not a function.

We mention here that there is a second problem with the definition of g : consider a real number a such that $2 \leq a \leq 3$. For instance, let $a = 2.5$. Then $g(2.5) = 0$ (since $2.5 \geq 2$) and $g(2.5) = 2/5$ (since $2.5 \leq 3$). This violates condition (ii) of the definition of a function. Thus g does not satisfy condition (i) or (ii). Therefore, the object defined above is not a function, for two reasons.

Although the example above violates both (i) and (ii), keep in mind that it is enough that (i) or (ii) alone be violated to ensure that f is not a function. \circ

Exercise 14.6. For each of the two examples below decide whether or not the object so defined is a function. Give reasons for your answers.

(a) Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = \begin{cases} x^2 & \text{if } x \geq 0 \\ -(x^2) & \text{if } x \leq 0 \end{cases}.$$

(b) Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be defined by

$$f(x) = \begin{cases} 1 & \text{if } x \in 2\mathbb{Z} \\ 2 & \text{if } x \text{ is prime} \\ 3 & \text{otherwise} \end{cases}.$$

\circ

One very important example of a function defined in cases is the familiar absolute value function.

Example 14.7. The absolute value function $f : \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = |x|$. It is easy to check that this does define a function on \mathbb{R} . \circ

When you define a new mathematical concept, it's always a good idea to think about it and pose questions. Of course, it's also a good idea to answer those questions, if you can. We now turn to some questions that we find interesting. See if you can think of some questions on your own.

What does it mean to say that two functions $f : A \rightarrow B$ and $g : A \rightarrow B$ are equal? Since this is a very important concept that we will need again later, we provide the answer here. But try to think about how this answer follows from the definition of a function.

Two functions $f : A \rightarrow B$ and $g : A \rightarrow B$ are equal if and only if $f(x) = g(x)$ for all $x \in A$.

Here's a second question: What is the function's relationship to elements of the domain, and how does this differ from the function's relationship to elements of the

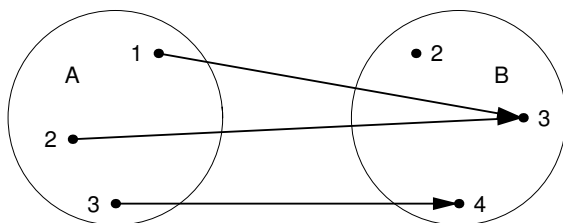


Fig. 14.3

codomain? We must be able to evaluate f for every element in the domain, while elements in $\text{cod}(f)$ may or may not be associated with elements of the domain. The elements of the codomain that are related to elements of $\text{dom}(f)$ are obviously important in understanding the function. For this reason, we look at the set called the range of f , which consists precisely of these points.

Given a function $f : A \rightarrow B$, the **range** of f , denoted $\text{ran}(f)$, is defined by

$$\text{ran}(f) = \{b \in B : \text{there exists at least one } a \in A \text{ such that } f(a) = b\}.$$

Sometimes it is fairly easy to determine the range, but it generally requires a method (demonstrated below) that we think of as working backwards. You'll start with $b \in B$ and try to find $a \in A$. Then, to show that $b \in \text{ran}(f)$, you have two things to check: The element a must map to b under f (that is, $f(a) = b$), and a must be an element of A . This latter statement is often obvious, but don't forget to check it!

It's always easier to start with small sets and see if you understand what is happening. You can do this visually as well. For example, say $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, and the function $f : A \rightarrow B$ is defined by $f(1) = 3, f(2) = 3$, and $f(3) = 4$. We can "see" the action of f by drawing a little picture as in [Figure 14.3](#)

From this picture we can see easily that f sends two things to 3, one thing to 4, and nothing to 2. So we can "see" that though 2 is in the codomain, it is not in the range. If you are asked for examples or counterexamples, remember that small sets will sometimes do the trick!

Our next example is really a method. Once we complete the example, we will review exactly what you must do in similar circumstances. But one thing we will mention in advance: you will always need to devise a plan as we do below.

Example 14.8. Let $f : \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R}$ be defined by $f(x) = (x+1)/(x-3)$. Determine the range of f .

"*Devising a plan.*" We need to figure out which $y \in \mathbb{R}$ come from something under f . It's a bit difficult to simply gaze at f , or even the graph of f , and see what comes out of it, so we'll try working backwards to see what y might be. (Though the graph of f provides a good way to see if your answer is reasonable, it does not provide a proof.) So, suppose $y \in \mathbb{R}$ did come from something in the domain. That would mean

$$y = f(x), \text{ for some } x \in \mathbb{R} \setminus \{3\};$$

in other words, $y = (x + 1)/(x - 3)$. Since we need to figure out what x is, we should solve for it. Multiplying through by $x - 3$, we get $(x + 1) = yx - 3y$. Collecting all terms involving x yields $x - yx = -3y - 1$. Factoring out x , dividing, simplifying, and ignoring potential problems (like what?), we get $x = (3y + 1)/(y - 1)$. So if y came from some x at all, y had to come from $x = (3y + 1)/(y - 1)$. That's fine, as long as $y \neq 1$ (that was a potential problem). So $\text{ran}(f)$ “appears to be”

$$\{y \in \mathbb{R} : y \neq 1\} = \mathbb{R} \setminus \{1\}.$$

The reason for saying “appears to be” is that we started by assuming y came from something called x , and then found out what x had to be. But the definition of range really requires us to start with an x and show that $f(x) = y$. So we need to check that everything we did above is reversible, and that the two sets $\text{ran}(f)$ and $\mathbb{R} \setminus \{1\}$ are equal. All of this was helpful in deciding what the range is, but the actual proof is still to come. The proof below is the form you should follow. When we write it, we need to pretend the reader has not seen the work we just completed.

Proof. We will show that $\text{ran}(f) = \mathbb{R} \setminus \{1\}$. Let $y \in \text{ran}(f)$. Then, clearly, $y \in \mathbb{R}$. So $\text{ran}(f) \subseteq \mathbb{R}$. To show that $y \neq 1$, suppose that this is not the case; so we will suppose $y = 1 \in \text{ran}(f)$ and see what happens. Since $y \in \text{ran}(f)$, there exists a point x in the domain with $f(x) = y = 1$. Using the definition of f , we find that $1 = f(x) = (x + 1)/(x - 3)$. Therefore, $x + 1 = x - 3$. This would mean that $1 = -3$, which is not possible. So $y \in \text{ran}(f)$ implies $y \in \mathbb{R}$ and $y \neq 1$. Thus, $\text{ran}(f) \subseteq \mathbb{R} \setminus \{1\}$.

Now let $y \in \mathbb{R} \setminus \{1\}$. Let $x = (3y + 1)/(y - 1)$. Since $y \neq 1$, we see that $x \in \mathbb{R}$. Remember that we need to check that $x \in \text{dom}(f)$. We know that $x \in \mathbb{R}$. Could we possibly have $x = 3$? Suppose we do, then $3 = (3y + 1)/(y - 1)$ which implies $3y - 3 = 3y + 1$. Thus we would have $-3 = 1$, which is impossible. So $x \in \text{dom}(f)$ and we can evaluate f at x to obtain

$$f(x) = \frac{\frac{3y+1}{y-1} + 1}{\frac{3y+1}{y-1} - 3} = \frac{3y + 1 + y - 1}{3y + 1 - 3y + 3} = y.$$

It follows that $\mathbb{R} \setminus \{1\} \subseteq \text{ran}(f)$. Therefore $\text{ran}(f) = \mathbb{R} \setminus \{1\}$, completing the proof. \square

Before going on, we will make two remarks. If you hadn't read “*Devising a plan*” above the proof, the definition of $x = (3y + 1)/(y - 1)$ would probably look bizarre. Remember that we didn't guess it; we worked backwards to see what x had to be. One other thing to note is that $\text{ran}(f) \neq \mathbb{R}$, but $\text{ran}(f) = \mathbb{R} \setminus \{1\}$. So f maps into \mathbb{R} but it doesn't “hit” the value 1. We'll come back to this in the next chapter. \circ

So what must we do when we have to find the range of a function? First, we need to take out a different sheet of paper and figure out what the set should be. Let's say we decide the range is a set called B . Then we need to show the reader that the two sets are equal. There are often many ways to do it, but one way is to start with an

element in the range (tell the reader you are doing this) and show it is in B . Then start with an element y in B (tell the reader you are doing this, too) and find an x (which you found somewhere else, but the reader doesn't necessarily need to see that) that satisfies two things: x is in the domain of your function and $f(x) = y$. Write your proof up carefully, identifying variables before you use them, and always checking that your variables are in the appropriate sets.

Exercise 14.9. What is the range of each of the functions below? A picture, when appropriate, is a lovely addition and is heartily encouraged. It does not, however, substitute for the real thing. Write out everything explicitly.

- (a) The function $f : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ defined by $f(x) = 1/x$.
- (b) The function $f : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \rightarrow \mathbb{R}$ defined by $f(x, y) = x/y$.
- (c) The function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2 + 4x + 5$. ○

Definitions

Definition 14.1. Let A and B be sets. A **function f from A to B** is a relation f from A to B satisfying

- (i) for all $a \in A$, there exists $b \in B$ such that $(a, b) \in f$, and
- (ii) for all $a \in A$, and all $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

The standard notation is $f : A \rightarrow B$ and $b = f(a)$ for $(a, b) \in f$. A function is also called a **map** or a **mapping**.

Definition 14.2. Given a function $f : A \rightarrow B$, the set A is called the **domain** of f , denoted by $\text{dom}(f)$, and the set B is called the **codomain** of f , and denoted by $\text{cod}(f)$.

Definition 14.3. Given a function $f : A \rightarrow B$, the **range** of f , denoted $\text{ran}(f)$, is defined by

$$\text{ran}(f) = \{b \in B : \text{there exists at least one } a \in A \text{ such that } f(a) = b\}.$$

Definition 14.4 (for Problems 14.6 through 14.9). Let X be a nonempty set and let A be a subset of X . The **characteristic function** or **indicator function** of the set A in X is

$$\chi_A : X \rightarrow \{0, 1\} \text{ defined by } \chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \in X \setminus A \end{cases}.$$

Definition 14.5 (for Problems 14.7 through 14.9). Let I be an interval of \mathbb{R} (open, closed, half open, or all of \mathbb{R}). A **step function** is a function $f : I \rightarrow \mathbb{R}$ of the form

$$f = \sum_{k=1}^n a_k \chi_{A_k},$$

where, for $k = 1, \dots, n$, we have $a_k \in \mathbb{R}$ and intervals A_k (any type, including I itself or containing just one point) such that $\{A_k : k \in \{1, \dots, n\}\}$ forms a partition of I and has the additional property that $A_j \cap A_\ell = \emptyset$ if $j \neq \ell$.

Definition 14.6 (for Problems 14.11 through 14.13). For $x \in \mathbb{R}$ we define the **greatest integer** of x by $\lfloor x \rfloor = n$, where $n \in \mathbb{Z}$ and $n \leq x < n + 1$. The **greatest integer function** or **floor function** is the function $f : \mathbb{R} \rightarrow \mathbb{Z}$, defined by $f(x) = \lfloor x \rfloor$.

Solutions to Exercises

Solution (14.1). The relations in (a) and (d) are functions, those in (b) and (c) are not.

Solution (14.2). Condition (ii) corresponds to the vertical line test, since it says that if we draw the vertical line $x = a$, it should pass through the graph of f at most once.

Solution (14.3). A function **f** from a set **A** to a set **B** is a relation $f : A \rightarrow B$ satisfying

- (i) for all $a \in A$, there exists $b \in B$ such that $f(a) = b$, and
- (ii) for all $a \in A$, and all $b, c \in B$, if $f(a) = b$ and $f(a) = c$, then $b = c$.

Solution (14.4). Parts (a), (c), and (e) define functions. The others do not. In (b), we have not defined $f(0)$ as an element of \mathbb{R} . In (d) note that if, for example, we consider $a = 2/1 = 4/2$, then $f(2/1) = 1$, while $f(4/2) = 1/2$. Thus $(2, 1)$ and $(2, 1/2)$ are both elements of the relation and condition (ii) is violated.

Solution (14.6). For part (a), the domain and codomain are both \mathbb{R} and both conditions in the definition of a function are satisfied. Note that though $x = 0$ appears twice in the definition of f , in both cases $f(0) = 0$. For part (b), consider $x = 2$. Since $x = 2 \in 2\mathbb{Z}$, we have $f(2) = 1$. On the other hand, 2 is also prime, so $f(2) = 2$. Thus $(2, 1)$ and $(2, 2)$ are both elements of the relation, but $1 \neq 2$, and condition (ii) is violated.

Solution (14.9). For (a) we claim that $\text{ran}(f) = \mathbb{R} \setminus \{0\}$. Clearly, $\text{ran}(f) \subseteq \mathbb{R} \setminus \{0\}$. So suppose that $y \in \mathbb{R} \setminus \{0\}$. Let $x = 1/y$. Then $x \in \mathbb{R}$ and $x \neq 0$. Thus, $x \in \text{dom}(f)$. Furthermore, $f(x) = 1/(1/y) = y$. Therefore, $y \in \text{ran}(f)$ and $\mathbb{R} \setminus \{0\} \subseteq \text{ran}(f)$, completing the proof.

For (b) we claim that $\text{ran}(f) = \mathbb{Q}$. If $z \in \text{ran}(f)$, then there exists $(x, y) \in \text{dom}(f) = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ with $z = f(x, y) = x/y \in \mathbb{Q}$. Thus $\text{ran}(f) \subseteq \mathbb{Q}$. Conversely, if $z \in \mathbb{Q}$, then $z = p/q$ for some $p, q \in \mathbb{Z}$ and $q \neq 0$. Hence $(p, q) \in \text{dom}(f)$ and $f(p, q) = p/q = z$. Thus $z \in \text{ran}(f)$ and $\mathbb{Q} \subseteq \text{ran}(f)$. The two parts together establish the claim.

For (c) we claim that $\text{ran}(f) = \{z \in \mathbb{R} : z \geq 1\}$. (We went to another sheet of paper to come up with this claim. A sketch (see [Figure 14.4](#)) is also helpful here, but it is *not* a proof.)

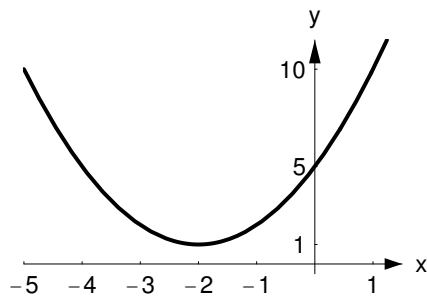


Fig. 14.4 $f(x) = x^2 + 4x + 5$

Proof. First note that if $y \in \text{ran}(f)$, then there exists $x \in \mathbb{R}$ such that $y = x^2 + 4x + 5$. Completing the square, we get $y = (x + 2)^2 + 1$. Since $(x + 2)^2 \geq 0$, we see that $y \geq 1$. Therefore, $y \in \{z \in \mathbb{R} : z \geq 1\}$, and hence $\text{ran}(f) \subseteq \{z \in \mathbb{R} : z \geq 1\}$.

Now suppose that $y \in \{z \in \mathbb{R} : z \geq 1\}$. Let $x = \sqrt{y - 1} - 2$. (We worked backwards to get this, of course.) Since $y \geq 1$, we have $x \in \mathbb{R}$. So $x \in \text{dom}(f)$. Furthermore, $f(x) = f(\sqrt{y - 1} - 2) = (\sqrt{y - 1} - 2)^2 + 4(\sqrt{y - 1} - 2) + 5$. Thus (as the reader can check) $f(x) = y - 1 - 4\sqrt{y - 1} + 4 + 4\sqrt{y - 1} - 8 + 5 = y$. Therefore, $y \in \text{ran}(f)$ and $\{z \in \mathbb{R} : z \geq 1\} \subseteq \text{ran}(f)$, as desired. \square

Spotlight: The Definition of Function

It's probably difficult to imagine that there could be any debate about the definition of function. In fact, the development of the definition of function is quite interesting. For example, Leonhard Euler first defined a function as follows [94, p. 72]: "A function of a variable quantity is an analytical expression composed in any manner from that variable quantity and numbers or constant quantities." Euler later revised his definition because of work on a problem known as the vibrating string problem. Discussion ensued, and Dirichlet is now often credited with providing us with roughly the definition we use today.

Once this discussion appeared to be settled, people could then concentrate on studying various kinds of functions; including, for example, continuous, discontinuous, differentiable, or even nowhere differentiable functions. Dirichlet also introduced the following example (now called the Dirichlet function):

$$D(x) = \begin{cases} c & \text{if } x \in \mathbb{Q} \\ d & \text{if } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases},$$

where c and d are distinct real numbers. This was the first example of many things, including the first example of a function that is discontinuous everywhere (see [58]). In a very interesting article written around 1940 (or, rather, the English translation of

this article), Luzin points out that not everyone agreed that Dirichlet had completely answered the question of what a function is. According to Luzin [65, p. 263], some mathematicians found the definition perfect, others found it too broad, and still others found it meaningless. Even as late as 1928, Hermann Weyl [109, p. 22] stated that no one can explain what a function is; then Weyl finishes the paragraph by telling us what a function is: “A function is given if by some definite rule to each real number a there is assigned a real number b (as e.g. by the formula $b = 2a + 1$). One then says that b is the value of the function f for the value a of the argument.”¹

For an overview of the definition of the concept of function, we recommend R uthing’s entertaining paper [94], where definitions (from 1718 to 1939) attributed to various authors are presented in their original language, with translation and without comment. You will notice that the final definition, due to N. Bourbaki and given in 1939, agrees with our definition.

The history of the vibrating string problem is described in [59, pp. 503–518]. In [57, p. 724], Katz presents the definition of function used by Johann Bernoulli, an earlier and later definition used by Euler, and definitions attributed to Lacroix, Fourier, Heine, and Dedekind. For a complete and readable overview on this topic, we recommend the papers of Luzin (both [64] and [65]), Youschkevitch [113], and Kleiner [58]. Kleiner’s paper also has an extensive bibliography.

Problems

Problem 14.1. Complete the following: A relation $f : A \rightarrow B$ is not a function if . . .

Problem 14.2. Suppose that $f : X \rightarrow Y$. Recall that the definition of $\text{ran}(f)$ was stated in the text. State carefully what it means when we say $y \in Y$ is not in the range of f .

Problem 14.3. Which of the following are functions from the set A to the set B ? Give reasons for your answers.

- Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by the relation $f = \{(x, y) : x^2 + y^2 = 4\}$ on \mathbb{R} .
- Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = 1/(x + 1)$.
- Define $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ by $f(x, y) = x + y$.
- The domain of f is the set of all closed intervals of real numbers of the form $[a, b]$, where $a, b \in \mathbb{R}$, $a \leq b$, the codomain of f is \mathbb{R} , and f is defined by $f([a, b]) = a$.
- Define $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{R}$ by $f(n, m) = m$.
- Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by

$$f(x) = \begin{cases} 0 & \text{if } x \geq 0 \\ x & \text{if } x \leq 0 \end{cases}.$$

¹ The translation is ours.

(g) Define $f : \mathbb{Q} \rightarrow \mathbb{R}$ by

$$f(x) = \begin{cases} x + 1 & \text{if } x \in 2\mathbb{Z} \\ x - 1 & \text{if } x \in 3\mathbb{Z} \\ 2 & \text{otherwise} \end{cases} .$$

(See Example 6.1 for the definitions of $2\mathbb{Z}$ and $3\mathbb{Z}$.)

- (h) The domain of f is the set of all circles in the plane \mathbb{R}^2 , the codomain is \mathbb{R} , and if c is a circle in the domain, define f by $f(c) =$ the circumference of c .
- (i) (For students with a background in calculus.) The domain and codomain of f are the set of all polynomials with real coefficients, and f is defined by $f(p) = p'$. (Here p' is the derivative of p .)
- (j) (For students with a background in calculus.) The domain of f is the set of all polynomials, the codomain is \mathbb{R} , and f is defined by $f(p) = \int_0^1 p(x) dx$. (Here $\int_0^1 p(x) dx$ is the definite integral of p .)

Problem 14.4. A function $f : A \rightarrow \mathbb{R}$ is often called a real-valued function. Thus, authors will often say, “Let f be a real-valued function.” Sometimes, A is explicitly defined. Other times, it is understood that the codomain is \mathbb{R} and that the domain is the largest set A for which all values under f result in real numbers. For all real-valued functions below, specify the implied domain, assuming that $A \subseteq \mathbb{R}$.

- (a) $f(x) = \frac{3+x}{x-2}$;
- (b) $g(x) = \ln(2x^2 + x - 6)$;
- (c) $h(x) = \sqrt{8x - 15 - x^2}$;
- (d) $k(x) = \sqrt{\frac{(x-3)(2x+5)}{x(x+2)(x-5)}}$.

Problem 14.5. Let $f : \mathcal{P}(\mathbb{R}) \rightarrow \mathbb{Z}$ be defined by

$$f(A) = \begin{cases} \min(A \cap \mathbb{N}) & \text{if } A \cap \mathbb{N} \neq \emptyset \\ -1 & \text{if } A \cap \mathbb{N} = \emptyset \end{cases} .$$

Prove that f above is a well-defined function.

Problem 14.6. Let X be a nonempty set and let A be a subset of X . The **characteristic function** or **indicator function** of the set A in X is

$$\chi_A : X \rightarrow \{0, 1\} \text{ defined by } \chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \in X \setminus A \end{cases} .$$

- (a) Since this is called the characteristic function, it probably is a function, but check this carefully anyway.
- (b) Determine the domain and range of this function. Make sure you look at all possibilities for A and X .

Problem 14.7. Using the characteristic function from Problem 14.6 we can define another useful type of function:

Let I be an interval of \mathbb{R} (open, closed, half open, or all of \mathbb{R}). A **step function** is a function $f : I \rightarrow \mathbb{R}$ of the form

$$f = \sum_{k=1}^n a_k \chi_{A_k},$$

where, for $k = 1, \dots, n$, we have $a_k \in \mathbb{R}$ and intervals A_k (any type, including I itself or containing just one point) such that $\{A_k : k \in \{1, \dots, n\}\}$ forms a partition of I and has the additional property that $A_j \cap A_\ell = \emptyset$ if $j \neq \ell$.

- Prove that a step function as defined above is a function.
- Find the range of the step function.
- Can the range of a step function have infinitely many elements? Explain.
- Suppose that we have a function $g : I \rightarrow \mathbb{R}$, where I is an interval of \mathbb{R} and the range of g is finite. Is g necessarily a step function? If it is, prove it; if it isn't, give a counterexample.

Problem 14.8. For each of the step functions below, sketch the graph and identify the range. (Step functions are introduced in Problem 14.7.)

- $f : [-5, 5] \rightarrow \mathbb{R}$ defined by $f(x) = 2\chi_{[-5, -1]} - 3\chi_{(-1, 1)} + 5\chi_{\{1\}} + \chi_{(1, 3)} + 2\chi_{[3, 5]}$;
- $g : [-3, 4) \rightarrow \mathbb{R}$ defined by $g(x) = \sum_{k=-3}^3 2^k \chi_{[k, k+1)}$.

Problem 14.9. Write each of the following functions as a sum of products of characteristic functions and other well-known functions. Say whether or not your function is a step function and explain your answer. (Characteristic functions are introduced in Problem 14.6 and step functions in Problem 14.7.)

- $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = \begin{cases} 2-x & \text{if } x \leq 0 \\ 2 & \text{if } 0 < x < 2; \\ x & \text{else} \end{cases}$;
- $g : [0, 12] \rightarrow \mathbb{R}$ given by the graph of [Figure 14.5](#) below;

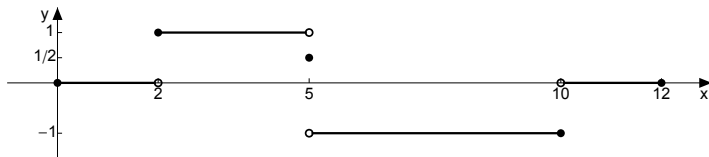


Fig. 14.5

- $h : \mathbb{R} \rightarrow \mathbb{R}$ defined by $h(x) = \begin{cases} \sin x & \text{if } 0 \leq x \leq 2\pi \\ 0 & \text{otherwise} \end{cases}$.

Problem 14.10. Let X be a bounded nonempty subset of \mathbb{R} . Suppose that we define $g: \mathcal{P}(X) \setminus \{\emptyset\} \rightarrow \mathbb{R}$ by $g(S) = \sup S$. Is g a well-defined function? Why or why not?

Problem 14.11. For $x \in \mathbb{R}$ we define the **greatest integer** of x by $\lfloor x \rfloor = n$, where $n \in \mathbb{Z}$ and $n \leq x < n + 1$. The **greatest integer function** or **floor function** is the function $f: \mathbb{R} \rightarrow \mathbb{Z}$, defined by $f(x) = \lfloor x \rfloor$.

- Find $\lfloor 1/2 \rfloor$, $\lfloor \pi \rfloor$, $\lfloor -3.5 \rfloor$, and $\lfloor -10 \rfloor$.
- Prove that f is a well-defined function.
- What is the range of f ? (Show all work!)
- Sketch the graph of the greatest integer (floor) function if it is restricted to $-5 \leq x \leq 5$.

Problem 14.12. See Problems 14.6, 14.7, and 14.11 for the definitions.

- Write the greatest integer function as a sum of characteristic functions (there may be more than one way to do this). Depending on your solution, the sum will “appear to have infinitely many terms,” but to calculate a particular value you will be adding only finitely many nonzero terms.
- Is the greatest integer function a step function? Explain your answer.

Problem 14.13. We use the notation of Problem 14.11 and define $g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) = \lfloor x \rfloor + \lfloor -x \rfloor$. Find $\text{ran}(g)$, and prove that your answer is correct.

Problem 14.14. (a) If possible, give an example of a function $f: \mathbb{N} \rightarrow \mathbb{R}$, with $\text{ran}(f) = \text{dom}(f)$.

- If possible, give an example of a function $f: \mathbb{N} \rightarrow \mathbb{R}$, with $\text{ran}(f) = \mathbb{Z}^+$.
- If possible, give an example of a function $f: \mathbb{N} \rightarrow \mathbb{R}$, with $\text{ran}(f) = \mathbb{Z}$.

Problem 14.15. Let $f: \mathbb{R} \setminus \{2\} \rightarrow \mathbb{R}$ be defined by $f(x) = 1/(x-2)$. Find $\text{ran}(f)$ and prove that your answer is correct.

Problem 14.16. Consider the (well-defined) function $f: \mathbb{R} \setminus \{3/2\} \rightarrow \mathbb{R}$ defined by $f(x) = (x-5)/(2x-3)$. Carefully prove that $\text{ran}(f) = \mathbb{R} \setminus \{1/2\}$.

Problem 14.17. Consider the (well-defined) function $f: \mathbb{R} \setminus \{3/7\} \rightarrow \mathbb{R}$ defined by $f(x) = (x+2)/(7x-3)$. Find $\text{ran}(f)$ and prove that your solution is correct.

Problem 14.18. (a) Give an example of a function f from $\mathbb{R} \times \mathbb{R}$ to \mathbb{R}^+ .

- Give an example of a function f from $\mathbb{Z} \times \mathbb{Z}$ to \mathbb{N} such that $\text{ran}(f) = \mathbb{N}$. (Prove that f is a function and $\text{ran}(f) = \mathbb{N}$.)
- Give an example of a function f from $\mathbb{Z} \times \mathbb{Z}$ to \mathbb{N} such that $\text{ran}(f) \neq \mathbb{N}$. (Prove that f is a function and $\text{ran}(f) \neq \mathbb{N}$.)

Problem 14.19. Let a, b, c , and d be real numbers with $a < b$ and $c < d$. Let $[a, b]$ and $[c, d]$ be two closed intervals. Find a function f such that $f: [a, b] \rightarrow [c, d]$ and $\text{ran}(f) = [c, d]$. Prove everything.

Problem 14.20. (a) Define $f: \mathbb{Z} \rightarrow \mathbb{N}$ by $f(x) = |x|$. Is f a function? If so, determine $\text{ran}(f)$.

(b) Define $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ by $f(x, y) = x$. Is f a function? If so, determine $\text{ran}(f)$.

Problem 14.21. Suppose that f is a function from a set A to a set B . Thus, we know that f is a subset of $A \times B$. Is the relation $\{(y, x) : (x, y) \in f\}$ necessarily a function from B to A ? Why or why not? (Say as much as is possible to say with the given information.)

Problem 14.22. Which of the following functions equal $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $f(x) = |x|$? Prove your answers (make sure you show that the functions below either equal f or do not equal f).

- (a) The function $g : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $g(x) = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$.
- (b) The function $h : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $h(x) = \sqrt{x^2}$.
- (c) The function $k : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $k(x) = \begin{cases} x^2/|x| & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$.

Problem 14.23. Let X be a nonempty set. Find all relations on X that are both equivalence relations on X and functions from X to X .

Problem 14.24. We can now define the indexing process more rigorously than we were able to in Chapter 8. Let I and X be sets and $f : I \rightarrow X$ be a function. Then we call the domain I an index set and an element of I an index. The range of the function, denoted here $\{f(j) : j \in I\}$, is called an indexed set. If the set $X \subseteq \mathcal{P}(Y)$ for some set Y (and thus $f : I \rightarrow \mathcal{P}(Y)$), then $\{f(j) : j \in I\}$ is usually called an indexed collection of sets.

As a specific example, consider

$$f : \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{R}) \text{ defined by } f(n) = \{x \in \mathbb{R} : \pi - 2n \leq x \leq \pi + 2/n\}.$$

- (a) Find $\bigcup_{n \in \mathbb{Z}^+} f(n)$.
- (b) Find $\bigcap_{n \in \mathbb{Z}^+} f(n)$.

Chapter 15

Functions, One-to-One, and Onto

Functions can map elements from the domain to the codomain in many ways. A function may “hit” every element in the codomain, or it may “miss” some. It may assign more than one x to a y or it may assign exactly one x to each y . We will understand our function better if we know which of these things it does. Precise formulations of these ideas will be given in a moment. It’s a mouthful, though, and really requires practice.

To say that a function $f : A \rightarrow B$ is **one-to-one** means that for all $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$, then $a_1 = a_2$. A function $f : A \rightarrow B$ is **onto** if $\text{ran}(f) = B$. If a function has this property, then we say that f maps A onto B . Some authors use the word **injective** rather than one-to-one and **surjective** rather than onto. If a function is both one-to-one and onto (or injective and surjective), then we say the function is **bijective**.

Diagrams using small sets may help illustrate the ideas involved in these definitions. We sketch two functions that are not one-to-one in [Figure 15.1](#) and two functions that are not onto in [Figure 15.2](#). Can you make a diagram for a function that is bijective?

Before moving on, let’s think about these definitions. The definition of one-to-one is an implication with quantifiers on elements of the domain A . It moves “forward,” in the sense that we start with elements in A and see where f maps them. The definition of onto, on the other hand, requires that we show something about every element in the set B . It will require us to move “backward,” in the sense that we will start with something in B and see what element of A is mapped to it under f .

If you want to show that a function is onto, we said that you must check that $\text{ran}(f) = B$. Technically that would mean showing $\text{ran}(f) \subseteq B$ and $B \subseteq \text{ran}(f)$. But if we are showing that a function $f : A \rightarrow B$ is onto, we already know that $\text{ran}(f) \subseteq B$; that is, we get that half for free. So if we know we have a function $f : A \rightarrow B$ (maybe it was given to us; maybe we showed it), to show that f maps A onto B , we only have to check that $B \subseteq \text{ran}(f)$. And what does this mean? The answer is given in the lemma below.

Lemma 15.1. *Let $f : A \rightarrow B$ be a function. Then f maps A onto B if and only if for all $b \in B$ there exists (at least one) $a \in A$ such that $f(a) = b$.*

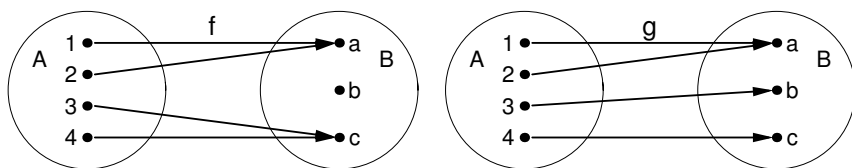


Fig. 15.1 The function f does not map onto B , but the function g does. Neither function is one-to-one

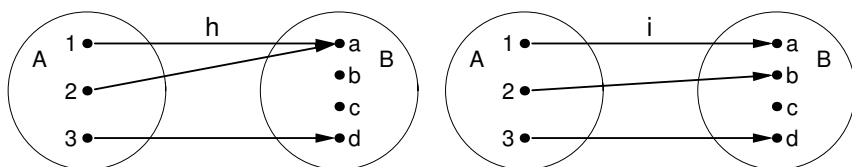


Fig. 15.2 The function h is not one-to-one, but the function i is. Neither function maps onto B

Since this lemma is just a reformulation of the definition of onto, we will often use it without explicitly referencing it.

Let's run through some of these ideas in slow motion. We'll begin with a simple example, and move on to a more challenging one.

Example 15.2. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = 2x + 5$. Then f is one-to-one.

Proving a function is one-to-one is often easier than proving it is onto, because one-to-one doesn't have that backwards quality. To prove it, we assume that (for two arbitrary points x_1 and x_2 in the domain) $f(x_1) = f(x_2)$, and show that $x_1 = x_2$. So now we'll just dive in here. Don't forget that the definition of one-to-one is an implication and therefore we expect to use our assumption.

Proof. Let $x_1, x_2 \in \mathbb{R}$. If $f(x_1) = f(x_2)$, then $2x_1 + 5 = 2x_2 + 5$. Simplification yields $x_1 = x_2$, as desired. Therefore f is one-to-one. \square

We turn to a more interesting example. Note that even though the functions in these two examples are quite different, the proofs that they are one-to-one are quite similar.

Example 15.3. In Example 14.8, we considered $f : \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R}$ defined by $f(x) = (x + 1)/(x - 3)$. We started with an element y and solved for x . We found an x that corresponded to y , but there may be others. Is the function one-to-one (meaning there aren't any others)?

We claim that $f : \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R}$ defined by $f(x) = (x + 1)/(x - 3)$ is one-to-one.

Proof. Let $x_1, x_2 \in \mathbb{R} \setminus \{3\}$. If $f(x_1) = f(x_2)$, then

$$\frac{x_1 + 1}{x_1 - 3} = \frac{x_2 + 1}{x_2 - 3}.$$

Multiplying through yields $x_1x_2 + x_2 - 3x_1 - 3 = x_2x_1 + x_1 - 3x_2 - 3$. Canceling, combining, and dividing by 4, we find that $x_1 = x_2$, as desired. Therefore f is one-to-one. \square

Note that $f : \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R}$ is not onto. This follows from our work in Example 14.8, where we showed that $\text{ran}(f) = \mathbb{R} \setminus \{1\} \neq \mathbb{R}$. The work of that example together with the proof above show that $f : \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R} \setminus \{1\}$ is a bijection. \circ

Exercise 15.4. What do you need to do in order to show that a function is not one-to-one? Use what you just decided to show that the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$ is not one-to-one. \circ

Exercise 15.5. In Exercise 14.9, which of the functions are one-to-one? If they are not one-to-one, show that carefully as well. \circ

It is now time to investigate what it really means when we say that a function maps a set A onto a set B .

Example 15.6. Prove that the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined in Example 15.2 by $f(x) = 2x + 5$ is onto.

We first devise our plan.

“*Devising a plan.*” We have checked that $f : \mathbb{R} \rightarrow \mathbb{R}$ is well-defined, so (in view of Lemma 15.1) we let $y \in \mathbb{R}$. We must show that $y = f(x)$ for some $x \in \mathbb{R}$. Thus, we must show that $y = 2x + 5$ for some $x \in \mathbb{R}$. It is now easy to see that $x = (y - 5)/2$ will work. Remember, when we write this up, we will act as though the reader has not seen this work.

Proof. Let $y \in \mathbb{R}$ and let $x = (y - 5)/2$. Then $x \in \mathbb{R} = \text{dom}(f)$ and

$$f(x) = 2 \left(\frac{y - 5}{2} \right) + 5 = y.$$

Since $f : \mathbb{R} \rightarrow \mathbb{R}$ is a well-defined function, f is onto (by Lemma 15.1). \square

Functions that are defined in cases will play an important role in the rest of this course. They are also illuminating examples, because they show just how much one-to-one depends on “what goes into f ” and just how much onto depends on “what comes out.” Showing that they are one-to-one and onto is a bit tricky. We’ll go through one example carefully first.

Example 15.7. We will show that $f : \mathbb{Z} \rightarrow \mathbb{N}$ as defined below and graphed in [Figure 15.3](#) is a bijective function:

$$f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -2n - 1 & \text{if } n < 0 \end{cases}.$$

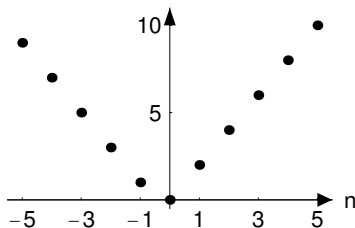


Fig. 15.3

We should mention something before we begin. We, the authors of this text, checked that the f in this example is really a function from \mathbb{Z} to \mathbb{N} . But don't trust us; check it again. Remember to check that f assigns a value in \mathbb{N} to each element of \mathbb{Z} , and that f assigns at most one value in \mathbb{N} to each integer. We now begin our example.

“Devising a plan.” Now to prove that f is one-to-one, we must show that if m and n are integers, and $f(m) = f(n)$, then $m = n$. But it's sort of confusing here, since we have more than one choice for $f(m)$ and $f(n)$. The problem seems to be that the function is defined in cases, and it's not immediately clear which case to use. The choice depends on whether m and n are negative or nonnegative. So we'll break this into all possible cases. Let's see. Both could be nonnegative (case 1), both negative (case 2), or one nonnegative, one negative (case 3). So let's check them all.

Proof. [Proof that f is one-to-one] Let $m, n \in \mathbb{Z}$ and suppose that $f(m) = f(n)$.

Case 1. Suppose that $m \geq 0$ and $n \geq 0$. Then $f(m) = 2m$ and $f(n) = 2n$. Thus $2m = 2n$, and therefore $m = n$.

Case 2. Suppose that $m < 0$ and $n < 0$. Then $f(m) = -2m - 1$ and $f(n) = -2n - 1$. Thus, $-2m - 1 = -2n - 1$, and therefore $m = n$.

Case 3. Suppose that one of the two, say m , is nonnegative, and the other is negative. Then $f(m) = 2m$ and $f(n) = -2n - 1$. Thus $2m = -2n - 1$. But this means that an even number, $2m$, is equal to an odd number, $-2n - 1$, which is impossible.

Therefore, if $f(m) = f(n)$, only cases 1 and 2 can occur. In either of these cases, we have shown that $m = n$. Thus f is one-to-one. \square

Now we will show that f maps \mathbb{Z} onto \mathbb{N} .

“Devising a plan.” Recall that to show f is onto, we must show that $\text{ran}(f) = \mathbb{N}$. We (you, actually) already checked that f is a well-defined function from \mathbb{Z} to \mathbb{N} , so $\text{ran}(f) \subseteq \mathbb{N}$. So let $k \in \mathbb{N}$. We wish to find m such that $f(m) = k$ and $m \in \mathbb{Z}$. Again, because there are cases, this is a bit confusing. So let's try to think about this before we really begin. We'll try to do this for a few specific points. Though this won't prove anything, it may tell us how to begin our proof. So moving along in the spirit of showing something is onto, if $f(m) = 4$, what's m ? (It's 2.) If $f(m) = 3$, what's m ? (It's -2 .) Now maybe you see it. If you don't, keep trying until you do. After a while, you should see that our choice of m depends on whether k is even or odd.

Proof. [Proof that f maps \mathbb{Z} onto \mathbb{N}] Let $k \in \mathbb{N}$. If k is even, then $k = 2m$ for some $m \in \mathbb{Z}$ with $m \geq 0$. Thus, $m \in \mathbb{Z}$ and $f(m) = 2m = k$. If k is odd, then $k + 1$ is even. Hence $m = (k + 1)/(-2) \in \mathbb{Z}$. Since $k \geq 1$, we have $m < 0$. Thus, $f(m) = -2m - 1 = -2((k + 1)/(-2)) - 1 = k$. We conclude that for all $k \in \mathbb{N}$, there exists $m \in \mathbb{Z}$ such that $f(m) = k$. Since $f : \mathbb{Z} \rightarrow \mathbb{N}$ is a well-defined function, f maps \mathbb{Z} onto \mathbb{N} . \square

Note that though the functions in the last two examples are quite different, the proofs that they are onto are quite similar.

What about an example of a function $f : A \rightarrow B$ that does not map A onto B ? Our Lemma 15.1 is quite handy here: Let $f : A \rightarrow B$ be a function. Then f is not onto if there exists $b \in B$ such that $f(a) \neq b$ for every $a \in A$.

For example, consider the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$. Then to show that f does not map onto \mathbb{R} , we note that $-1 \in \mathbb{R}$, but there exists no $a \in \mathbb{R}$ such that $f(a) = -1$. You should be able to show that f does map \mathbb{R} onto the nonnegative real numbers.

Exercise 15.8. In Exercise 14.9, which of the functions map onto their codomain? If they do not map onto, show that carefully as well. \circ

We now turn to a concrete example of a function f and a special way to construct a function (called the restriction) that is related to f in a very special way.

Suppose that the set A contains all the buses in the city of Bern, Switzerland, and the function $f : A \rightarrow \mathbb{Z}^+$ enumerates them by assigning a positive integer to each one. We will let C denote the subset of A that contains all the buses that run on biogas. There are now enough biogas buses available to serve the city on a regular day and, therefore, we are interested in enumerating just the biogas buses. If we wish to select only the biogas buses, we would be interested in the enumeration of the set C ; that is, we use the old function but consider only buses in the set C . This is easily done, by restricting the function f from A to C . Formally speaking, the restriction is the following: Let $f : A \rightarrow B$ be a function and $C \subseteq A$. The **restriction** of f to C is the function $f|_C : C \rightarrow B$ defined by $f|_C(x) = f(x)$ for all $x \in C$.

Exercise 15.9. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a function.

- (a) Give an example of a function f and a nonempty subset A of \mathbb{R} such that f is not one-to-one, but $f|_A$ is one-to-one.
- (b) Give an example of a function f and a nonempty subset A of \mathbb{R} such that $f|_A : A \rightarrow \mathbb{R}$ is not onto, but f is onto.
- (c) Are there examples of f and $A \subseteq \mathbb{R}$ such that f is a bijection, but $f|_A : A \rightarrow \mathbb{R}$ is not? Give an example or explain why none exists.
- (d) Are there examples of f and $A \subseteq \mathbb{R}$ such that $f|_A : A \rightarrow \mathbb{R}$ is a bijection, but f is not? Give an example or explain why none exists.

Definitions

Definition 15.1. A function $f : A \rightarrow B$ is **one-to-one** or **injective** if for all $a_1, a_2 \in A$, whenever $f(a_1) = f(a_2)$, then $a_1 = a_2$.

Definition 15.2. A function $f : A \rightarrow B$ is **onto** or **surjective** if $\text{ran}(f) = B$.

Definition 15.3. A function $f : A \rightarrow B$ is **bijective** if it is injective and surjective (or, equivalently, one-to-one and onto).

Definition 15.4. Let $f : A \rightarrow B$ be a function and $C \subseteq A$. The **restriction** of f to C is the function $f|_C : C \rightarrow B$ defined by $f|_C(x) = f(x)$ for all $x \in C$.

Solutions to Exercises

Solution (15.4). Carefully negating the definition, we see that to show a function $f : A \rightarrow B$ is not one-to-one, we must show that there exist x_1 and x_2 in A with $f(x_1) = f(x_2)$ and $x_1 \neq x_2$. For the particular function $f(x) = x^2$ given above, we note that the numbers 1 and -1 are both real numbers with $f(1) = f(-1)$, but $1 \neq -1$. Therefore f is not one-to-one.

Solution (15.5). Only the function defined in (a) is one-to-one: If $x_1, x_2 \in \mathbb{R} \setminus \{0\}$ and $f(x_1) = f(x_2)$, then $1/x_1 = 1/x_2$. Therefore, $x_1 = x_2$, showing that f is one-to-one.

For part (b) consider $(1, 1), (2, 2) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \text{dom}(f)$. Then $(1, 1) \neq (2, 2)$, but $f(1, 1) = 1 = f(2, 2)$. This shows that f is not one-to-one.

For part (c), let $-1, -3 \in \mathbb{R} = \text{dom}(f)$. Then $f(-1) = 2 = f(-3)$ and hence f is not one-to-one.

Solution (15.8). None of the functions maps onto their codomain. The range of each function was presented in the solution to Exercise 14.9.

Solution (15.9). We will need only two functions to solve all four parts of this problem. Of course, many other examples are possible.

(a) Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = \begin{cases} x & \text{if } x \leq 0 \\ x - 1 & \text{if } x > 0 \end{cases}$$

and let $A = \mathbb{R} \setminus (0, 1] \subseteq \mathbb{R}$. Clearly f is not one-to-one, but $f|_{\mathbb{R} \setminus (0, 1]}$ is.

(b) Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x$ and let $A = \mathbb{Z}$. Then f is onto but $f|_{\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{R}$ is not.

(c) The example presented in part (b) works here also.

(d) The example presented in part (a) works here also.

Problems

Problem 15.1. For each of the following, you are asked to give an example of a function. (You should always state the domain, codomain, and the associated rule of your function.)

- Give an example of a function that is both one-to-one and onto.
- Give an example of a function that is one-to-one, but not onto.
- Give an example of a function that is not one-to-one, but is onto.
- Give an example of a function that is neither one-to-one nor onto.

Problem 15.2. (a) Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^2$. Show that f is not onto.

- Show that f , as defined above, maps \mathbb{R} onto $\{x \in \mathbb{R} : x \geq 0\}$.
- Consider the function $g : \mathbb{Z} \rightarrow \mathbb{N}$ defined by $g(x) = x^2$. Is g onto?
- Both g and f take elements of the domain and square them. Why did we use the letter g in the previous part of this problem, rather than the letter f ?

Problem 15.3. Is the absolute value function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = |x|$ one-to-one? Why or why not?

Problem 15.4. (a) Is there a one-to-one function from the set $\{1, 2, 3\}$ to the set $\{1, 3\}$? Why or why not?

- Is there a function mapping $\{1, 2, 3\}$ onto the set $\{1, 3\}$? Why or why not?
- Is there a one-to-one function mapping the open interval $(0, 2)$ to the open interval $(0, 1)$?
- Is there a one-to-one function mapping the set $\{x \in \mathbb{R} : x > 0\}$ to the open interval $(0, 1)$?
- Is there a function mapping the set $\{x \in \mathbb{R} : x > 0\}$ onto the open interval $(0, 1)$?

Problem 15.5. Recall Definition 15.1 of one-to-one.

- State the contrapositive of the definition.
- By negating the contrapositive, complete the following definition. A function $f : X \rightarrow Y$ is not one-to-one if ...

Problem 15.6. Criticize the following “definition” of onto. “A function $f : X \rightarrow Y$ is onto if there exists an $x \in X$ such that for each $y \in Y$ we have $f(x) = y$.”

Problem 15.7. Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = 5 + (x - 3)^2$.

- Prove that f is not injective.
- Find $\text{ran}(f)$ and prove that your conjecture is correct.

Problem 15.8. We define $f : \mathbb{R} \rightarrow \mathbb{R}$ by

$$f(x) = \begin{cases} x^2 - 4x + 7 & \text{if } x \leq 1 \\ 5 - x^2 & \text{if } x > 1 \end{cases}.$$

This function is well-defined and you may assume this without proving it. Prove that this function is bijective.

Problem 15.9. We define $f : \mathbb{R} \rightarrow \mathbb{R}$ by

$$f(x) = \begin{cases} x^2 + 2x + 4 & \text{if } x \leq -2 \\ -2x & \text{if } -2 < x < 2 \\ -2 - x & \text{if } x \geq 2 \end{cases} .$$

This function is well-defined and you may assume this without proving it. Prove that this function is bijective.

Problem 15.10. For each of the functions below, determine whether or not the function is one-to-one and whether or not the function is onto. If the function is not one-to-one, give an explicit example to show what goes wrong. If it is not onto, determine the range.

- Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = 1/(x^2 + 1)$.
- Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = \sin(x)$. (Assume familiar facts about the sine function.)
- Define $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ by $f(n, m) = nm$.
- Define $f : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ by $f((x, y), (u, v)) = xu + yv$. (Do you recognize this function?)
- Define $f : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ by $f((x, y), (u, v)) = \sqrt{(x-u)^2 + (y-v)^2}$. (Do you recognize this function?)
- Let A and B be nonempty and $b \in B$. Define $f : A \rightarrow A \times B$ by $f(a) = (a, b)$.
- Let X be a nonempty set. Define $f : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ by $f(A) = X \setminus A$.
- Let B be a fixed proper subset of a nonempty set X . We define a function $f : \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ by $f(A) = A \cap B$.
- Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by

$$f(x) = \begin{cases} 2 - x & \text{if } x < 1 \\ 1/x & \text{otherwise} \end{cases} .$$

Problem 15.11. Definition 14.4 introduced the characteristic function χ_A of a subset A of a set X .

- Under what conditions on the sets A and X is the function $\chi_A : X \rightarrow \{0, 1\}$ onto? Justify your answer.
- Under what conditions on the sets A and X is the function $\chi_A : X \rightarrow \{0, 1\}$ one-to-one? Justify your answer.
- Under what conditions on the sets A and X is the function $\chi_A : X \rightarrow \{0, 1\}$ bijective? Justify your answer.

Problem 15.12. For each of the following, determine whether or not $f : A \rightarrow B$ is a function from the set A to the set B . If it is, prove that f is one-to-one, or give an example to show that f is not one-to-one. Then prove that f is onto, or give an example of an element in the codomain that is not in the range to show that f is not onto.

- (a) Define $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ by $f(x, y) = (y, x)$.
 (b) Define $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ by $f(x, y) = x^2 + y^2$.
 (c) Let $y \in \mathbb{R}$. Define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = y \cdot x$. (Does your answer depend on y ?)
 (d) Define $f : \mathcal{P}(\mathbb{Z}) \rightarrow \mathbb{Z}$ by $f(S) = \max S$.

Problem# 15.13. Let $f : \mathbb{R} \rightarrow (-1, 1)$ be defined by

$$f(x) = \frac{x}{1 + |x|}.$$

Prove that f is a bijective function, mapping \mathbb{R} onto the open interval $(-1, 1)$.

Problem 15.14. Let a, b, c , and d be real numbers with $a < b$ and $c < d$. Define a bijection from the closed interval $[a, b]$ onto the closed interval $[c, d]$ and prove that your function is a bijection.

Problem 15.15. Let $F([0, 1])$ denote the set of all real-valued functions defined on the closed interval $[0, 1]$. Define a new function $\phi : F([0, 1]) \rightarrow \mathbb{R}$ by $\phi(f) = f(0)$. Is ϕ a function from $F([0, 1])$ to \mathbb{R} ? Is it one-to-one? Is it onto? Remember to prove all claims, and to provide examples where appropriate.

Problem 15.16. Find a function $f : \mathbb{R} \rightarrow \mathbb{R}^+$ that is one-to-one.

Problem 15.17. Let f be a function, $f : \mathbb{R} \rightarrow \mathbb{R}$. Define a new function $f \cdot f : \mathbb{R} \rightarrow \mathbb{R}$ by $(f \cdot f)(x) = f(x) \cdot f(x)$. Prove that $f \cdot f$ is a function. Then do the remaining parts of the problem. (You may wish to work Problem 15.16, if you haven't already done so.)

- (a) Does there exist a function f for which $f \cdot f$ is one-to-one? If not, why not? If there is, what is an example?
 (b) Does there exist a function f for which $f \cdot f$ maps onto \mathbb{R} ? If not, what is $\text{ran}(f \cdot f)$? Your answer will be in terms of $\text{ran}(f)$.

Problem 15.18. Let $f : A \rightarrow B$ be a function and $C \subseteq A$. Prove that $f|_C$ is a well-defined function.

Problem# 15.19. Let $f : A \rightarrow B$ be a function and $C \subseteq A$.

- (a) Prove that if f is one-to-one, then $f|_C$ is one-to-one.
 (b) Prove that if $f|_C$ is onto, then f is onto.

Problem 15.20. Let $f : X \rightarrow Y$ and $g : X \rightarrow Y$ be functions and let \mathcal{A} denote a partition of X . Show that if $f|_A = g|_A$ for all $A \in \mathcal{A}$, then $f = g$.

Problem 15.21. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be $f(x) = x^3 - 3x$ and $A = (-\infty, -\sqrt{3}) \cup [\sqrt{3}, \infty)$. Is f a bijection? Is $f|_A : A \rightarrow \mathbb{R}$ a bijection? (Your solution may involve the intermediate value theorem.)

Problem 15.22. Show that the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = |x| + 2x$ is bijective. You might find it more convenient to write f as a function defined in cases.

Problem# 15.23. Define $f : (-1, 1) \rightarrow \mathbb{R}$ by

$$f(x) = \frac{x}{x^2 - 1}.$$

- (a) Show that f is injective.
- (b) Show that f is surjective.

Problem 15.24. Let a, b, c , and d be real numbers, not both of c and d zero. Further, let $X = \{x \in \mathbb{R} : cx + d \neq 0\}$. The function $f : X \rightarrow \mathbb{R}$ defined by

$$f(x) = \frac{ax + b}{cx + d},$$

is well-defined (you need not prove that).

- (a) Under what conditions (i.e., restrictions on a, b, c, d) will f be one-to-one? Prove your conjecture.
- (b) Assume that the conditions that you proposed in part (a) hold and that, in addition, $c = 0$. Show that in this case, f is a bijection from \mathbb{R} to \mathbb{R} .

Problem 15.25. Let \sim be an equivalence relation on a nonempty set X . We denote the set of all equivalence classes of \sim by \mathcal{C} . Define $f : X \rightarrow \mathcal{C}$ by $f(x) = E_x$. Thus, an element $x \in X$ is mapped to the equivalence class containing x .

- (a) Prove that f is a well-defined function.
- (b) Prove that f is surjective.
- (c) Give necessary and sufficient conditions on the equivalence relation for f to be bijective.

Problem 15.26. Let $f : A \rightarrow B$ be a surjective function. For $x, y \in A$, we say $x \sim y$ if and only if $f(x) = f(y)$.

- (a) Prove that \sim is an equivalence relation on A .

We denote the collection of all equivalence classes of \sim by \mathcal{C} . Define $g : \mathcal{C} \rightarrow B$ by $g(E_x) = f(x)$.

- (b) Prove that g is a well-defined function.
- (c) Prove that g is bijective.

Chapter 16

Inverses

Given functions $f : A \rightarrow B$ and $g : C \rightarrow D$ with $\text{ran}(f) \subseteq C$, we can define a third function called the **composite function** from A to D . (We will usually call this the **composition**, rather than the composite function.) This composition is the function $g \circ f : A \rightarrow D$ defined by $(g \circ f)(x) = g(f(x))$. So, for example, if $f : \mathbb{R} \rightarrow \mathbb{R}$ and $g : \mathbb{R} \rightarrow \mathbb{R}$ are defined by $f(x) = x^2$ and $g(x) = \sin(x)$, then $(g \circ f)(x) = g(f(x)) = g(x^2) = \sin(x^2)$. Note that the order really matters here. Using f and g as above, for example, $(f \circ g)(x) = f(g(x)) = f(\sin(x)) = (\sin(x))^2$. You can check pretty easily that these two functions are different. (Check this pretty easily.) So composition of functions is not commutative.

Consider the two functions in [Figure 16.1](#). Here $f : A \rightarrow B$, where $A = \{a, b, c\}$ and $B = \{1, 2, 3, 4\}$, while $g : C \rightarrow D$, where $C = \{2, 3, 4, 5, 6\}$ and $D = \{\alpha, \beta, \gamma\}$. Then $\text{ran}(f) \subset C$, so the composition $g \circ f$ is defined. To determine the action of $g \circ f$ algebraically, use the definition of each. For example, $(g \circ f)(a) = g(f(a)) = g(2) = \beta$. To determine the action visually, follow the arrows, remembering that f goes first.

Take this opportunity to check that the composition of three functions satisfies the associative property. In other words, if we have three functions f, g , and h so that the composition makes sense (what would that mean?), then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

We'll use this result in this chapter.

Sometimes it is useful to “undo” the action of a function f . If f maps 3 to 5, we might wish to “undo” that by finding a function that takes 5 back to 3. This is most useful when we can undo the action of f on the whole range, not at just one point, because then every element ends up back where it started. For example, if f cubes all the values in its domain, we can “reverse” that action by taking the cube root. Mathematically what this means is that if $f : \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = x^3$, then $g : \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = x^{1/3}$ satisfies two things: $(g \circ f)(x) = x$ for all $x \in \text{dom}(f)$, and $(f \circ g)(y) = y$ for all $y \in \text{dom}(g)$.

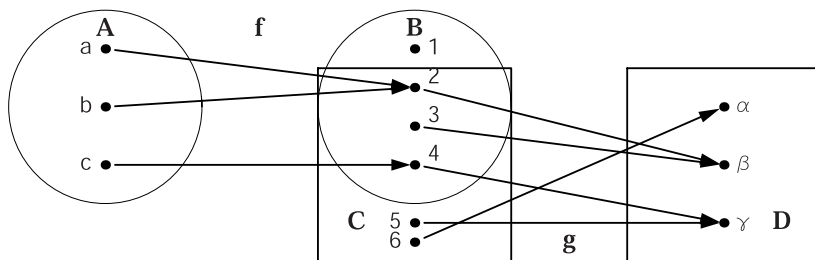


Fig. 16.1 $g \circ f : A \rightarrow D$

But what happens if $f : \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = x^2$? If we want g to “undo” this action, then we want g to satisfy $(g \circ f)(x) = x$ for all $x \in \mathbb{R}$. But if $x = 2$, we need $(g \circ f)(2) = g(4) = 2$ and, if $x = -2$, we need $(g \circ f)(-2) = g(4) = -2$ (see Figure 16.2). What’s the problem here? Well, g is not allowed to assign two different values to the number 4. So we can’t do this for all functions. When can we do it? (Think first, read on later.)

Suppose that a function is bijective. Then, rather than looking in the domain and asking what x gets mapped to, we can look in the range at y and ask where it came from. Since the function is onto, y came from some x . Since the function is one-to-one, y came from exactly one x . So we can define an inverse function as follows.

Let $f : A \rightarrow B$ be a bijective function. The **inverse** of f is the function $f^{-1} : B \rightarrow A$ defined by

$$f^{-1}(y) = x \text{ if and only if } f(x) = y.$$

Whenever we define a function, we have to ask ourselves: “Is it well-defined?” Is it? The domain is defined to be B . By definition, the value of an element of B under f^{-1} is some $x \in A$. Hence A qualifies as a codomain of f^{-1} . Now we check condition (i) of the definition of a function. Let $b \in B$. Since f is onto, there exists an element $a \in A$ such that $f(a) = b$. Hence $f^{-1}(b) = a$ is defined and property (i) holds. For property (ii) we assume that there is an element $b \in B$, and elements a and c in A such that $f^{-1}(b) = a$ and $f^{-1}(b) = c$. By the definition of f^{-1} we have $f(a) = b$

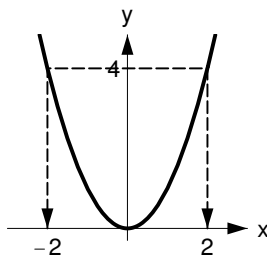


Fig. 16.2 $f(x) = x^2$

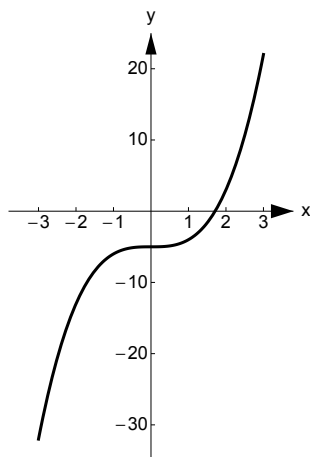


Fig. 16.3 $f(x) = x^3 - 5$

and $f(c) = b$. Hence $f(a) = f(c)$ and since f is one-to-one, $a = c$. This shows that property (ii) holds and we conclude that f^{-1} is well-defined. Note that this function is only defined in the case when f is bijective.

The discussion in the last paragraph shows that f^{-1} is indeed a function. Thus we have shown that if $f : A \rightarrow B$ is a bijective function, then there exists an inverse function $g : B \rightarrow A$. The remainder of this chapter will be spent understanding inverse functions. In particular, we will show that an inverse function is unique and we will speak of “the” inverse of f .

Example 16.1. We define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = x^3 - 5$. Graph the function f . Then prove that f is one-to-one and onto. Once you have done that, decide what f^{-1} is.

“*Devising a plan.*” Assume for the moment that we know that f is bijective, so that we know that f^{-1} exists. To find f^{-1} , we use what we know: $f^{-1}(y) = x$ if and only if $f(x) = y$. Thus we must solve $x^3 - 5 = y$ for x . Once we solve this equation, we find that $x = (y + 5)^{1/3}$. Now we are ready to solve this problem.

Proof. We first prove that f is one-to-one. So let x_1 and x_2 be real numbers. If $f(x_1) = f(x_2)$, then $x_1^3 - 5 = x_2^3 - 5$. Hence $x_1^3 = x_2^3$. We factor the difference to get $x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2)$. Thus, $x_1 = x_2$ or $x_1^2 + x_1x_2 + x_2^2 = 0$. In the latter case, we write $x_1^2 + x_1x_2 + x_2^2 = (x_1 + x_2)^2 - x_1x_2 = 0$. So, we would have $x_1x_2 = (x_1 + x_2)^2 \geq 0$, and this would mean that all three terms in $x_1^2 + x_1x_2 + x_2^2$ are nonnegative. The only way this sum can be zero is if each summand is zero. Thus $x_1 = x_2 = 0$. Therefore $x_1 = x_2$ and we may conclude that f is one-to-one. (Alternatively, you can use the remark following the discussion and proof of Theorem 13.2.)

Now we show that f is onto. Let $y \in \mathbb{R}$ and set $x = (y + 5)^{1/3}$. (See the remark on the existence of n th roots following the discussion and proof of Theorem 13.2.) Then $x \in \mathbb{R}$, and $f(x) = ((y + 5)^{1/3})^3 - 5 = y$. Since $f : \mathbb{R} \rightarrow \mathbb{R}$ is a well-defined function, Lemma 15.1 implies that f is onto.

Finally, we claim that $f^{-1} : \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f^{-1}(y) = (y + 5)^{1/3}$. So let $g(y) = (y + 5)^{1/3}$. If we can show that $g(y) = x$ if and only if $f(x) = y$, then g satisfies the definition of inverse function and we can conclude that $g = f^{-1}$. So let $y \in \mathbb{R}$. Then $x = g(y) = (y + 5)^{1/3}$ if and only if $x^3 = y + 5$. The last equality holds if and only if $y = x^3 - 5 = f(x)$. Therefore $x = g(y)$ if and only if $y = f(x)$ and $f^{-1}(y) = g(y) = (y + 5)^{1/3}$. \square

We'll have another way to show that a function g is the inverse of a function f as soon as we prove Theorem 16.4 below. That theorem will make our life easier. However, until we prove that theorem, we'll have to resort to the definition because it's all we have.

The example above brings up an important point. Students often confuse the notation f^{-1} with $1/f$. In the example above $1/f$ would be the function defined for $x \neq 5^{1/3}$ by $1/(x^3 - 5)$, while we have seen that f^{-1} is defined on all of \mathbb{R} by $f^{-1}(x) = (x + 5)^{1/3}$. These two functions are really quite different! In fact, f^{-1} and $1/f$ are rarely the same. (See Project 29.7 for more information.)

You may also be wondering whether the original function will always be defined in terms of x and the inverse function in terms of y . The answer is: Of course not. For one thing, there is nothing "original" about the first function; we might just as well have started with the "inverse" function in the example above (see Problem 16.9). What we decide to call the variable is irrelevant: For example, the functions $g : \mathbb{R} \rightarrow \mathbb{R}$ and $h : \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = (x + 5)^{1/3}$ and $h(y) = (y + 5)^{1/3}$ are the same function.

Example 16.2. Let $f : \mathbb{R} \setminus \{3\} \rightarrow \mathbb{R} \setminus \{1\}$ be defined by $f(x) = (x + 1)/(x - 3)$. (You should graph the function f , and compare it to our graph in Figure 16.4.) We'll find $f^{-1} : \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R} \setminus \{3\}$.

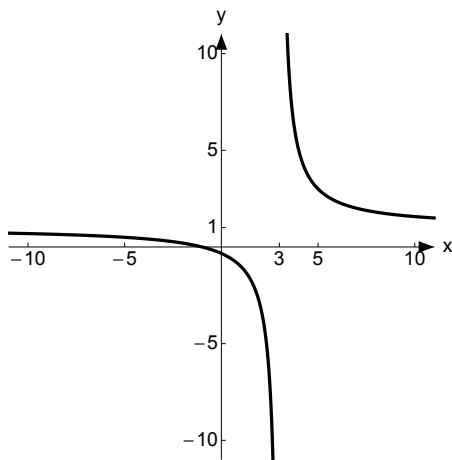


Fig. 16.4 $f(x) = (x + 1)/(x - 3)$

Before you read our solution, use Examples 14.8 and 15.3 to check that this function is bijective and that the domain and range are also appropriate for f^{-1} .

To find an expression for f^{-1} , let $y \in \mathbb{R} \setminus \{1\}$. Then there exists (exactly one) $x \in \mathbb{R} \setminus \{3\}$ such that $f(x) = y$. Further, $f(x) = y$ if and only if $(x+1)/(x-3) = y$, and this happens if and only if $x = (3y+1)/(y-1)$.

Therefore $f^{-1}(y) = x = (3y+1)/(y-1)$. ○

In our examples and exercises thus far, you probably noticed us repeating the same steps: We first check that $f : A \rightarrow B$ is bijective. If it is, then we know f^{-1} exists. To find f^{-1} , we choose $y \in B$ and solve for the unique x such that $f(x) = y$. Then, by definition, $f^{-1}(y) = x$, and we are done.

Now you should be ready to do a more challenging example as an exercise.

Exercise 16.3. Let $f : \mathbb{Z} \rightarrow \mathbb{N}$ be defined by

$$f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -2n - 1 & \text{if } n < 0 \end{cases}.$$

We showed in Example 15.7 that this function is bijective. Find a formula for f^{-1} . (You might find it helpful to reexamine the graph of f in [Figure 15.3](#).) ○

If A is a set, one very important function mapping A to itself is the identity function. So, the **identity function** i_A is the function $i_A : A \rightarrow A$ defined by $i_A(x) = x$ for all $x \in A$. You should check that i_A is well-defined, is both one-to-one and onto, and is its very own inverse. In addition, this function is easy to use. For example, if A and B are sets and f is a function such that $f : A \rightarrow B$, then $f \circ i_A = f$, while $i_B \circ f = f$.

Theorem 16.4. Let $f : A \rightarrow B$ be a bijective function. Then

- (i) $f \circ f^{-1} = i_B$; that is, $(f \circ f^{-1})(y) = y$ for all $y \in B$.
- (ii) $f^{-1} \circ f = i_A$; that is, $(f^{-1} \circ f)(x) = x$ for all $x \in A$.
- (iii) f^{-1} is a bijective function.
- (iv) If $g : B \rightarrow A$ is a function satisfying $f \circ g = i_B$ or $g \circ f = i_A$, then $g = f^{-1}$.

The last part of this theorem says that if we know that our function has an inverse, then f^{-1} is the one and only function satisfying the identities in (iv). This can come in quite handy. Consider the following.

Sometimes, as in Exercise 16.3, it is difficult to compute f^{-1} . In these cases it is nice to check your answer. Theorem 16.4 tells you one way to do so: Suppose you know that f is bijective, and you are claiming that g is the inverse. If you find that $g \circ f = i_A$ or $f \circ g = i_B$, you know you have the right answer!

We also remark here that (i) and (ii) above really follow from the definition of inverse function: $f(x) = y$ if and only if $f^{-1}(y) = x$.

Proof. (i) If $y \in B$, let $z = f^{-1}(y)$. By definition $f^{-1}(y) = z$ if and only if $f(z) = y$. Therefore

$$(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(z) = y.$$

(ii) If $x \in A$, let $z = f(x)$. By definition $f(x) = z$ if and only if $f^{-1}(z) = x$. Therefore,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(z) = x.$$

(iii) We leave this for you to do in Problem 16.9.

(iv) We note first that $\text{dom}(g) = \text{dom}(f^{-1}) = B$.

First suppose that $g \circ f = i_A$. Then, using the associative property of composition and (i) above, we have

$$f^{-1} = i_A \circ f^{-1} = (g \circ f) \circ f^{-1} = g \circ (f \circ f^{-1}) = g \circ i_B = g.$$

In exactly the same way (except we use (ii) in place of (i)), we can show that if $f \circ g = i_B$, then $g = f^{-1}$. \square

Before applying Theorem 16.4 make sure that you check that f really is bijective. It is one of the hypotheses, after all!

Exercise 16.5. For each of the functions and their inverses in Example 16.1, Example 16.2, and Exercise 16.3 check that $f^{-1} \circ f = i_{\text{dom}(f)}$ and $f \circ f^{-1} = i_{\text{ran}(f)}$. \circ

The theorem above includes the basic facts about inverses. But there are more theorems that will be useful as we move along.

Theorem 16.6. Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be bijective functions. Then $g \circ f$ is bijective and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Before we begin, let's make sure we understand the function and think about what we need to prove. We note that $g \circ f : A \rightarrow C$. To show that the composition is bijective, we must show that it is one-to-one and onto. To find the inverse, if we have a guess for what it should be, we can use Theorem 16.4 (iv), which (in this case) says that if $g \circ f$ is bijective and h is a function such that $(h \circ (g \circ f))(x) = x$ for all x in A or $((g \circ f) \circ h)(y) = y$ for all y in B , then h must be $(g \circ f)^{-1}$. So all we need to do is think of a good candidate for h (the object we want to show is the inverse) and show it works. But the statement of the theorem gives us a candidate for h . Now that we have the plan, we can try to carry it out.

Proof. First we'll show that the composition $g \circ f$ is one-to-one. So let $x_1, x_2 \in A$. If $(g \circ f)(x_1) = (g \circ f)(x_2)$, then $g(f(x_1)) = g(f(x_2))$. Now since g is one-to-one, $f(x_1) = f(x_2)$. But f is also one-to-one, and therefore $x_1 = x_2$, as desired.

To see that the composition is onto, let $z \in C$. Since g is onto, there exists a $y \in B$ such that $g(y) = z$. Since $y \in B$ and f is onto, there exists $x \in A$ such that $f(x) = y$. Therefore, $x \in A$ and

$$(g \circ f)(x) = g(f(x)) = g(y) = z.$$

Since $g \circ f : A \rightarrow C$, we conclude that $g \circ f$ is onto.

Now we will show that $f^{-1} \circ g^{-1}$ is the inverse of $g \circ f$ by applying (iv) of Theorem 16.4 to $g \circ f$. We just showed that $g \circ f$ is bijective. Now we check the hypotheses of part (iv) of the theorem. First, note that the domain is correct; that is, $f^{-1} \circ g^{-1} : C \rightarrow A$.

We now show that $((f^{-1} \circ g^{-1}) \circ (g \circ f))(z) = z$ for all $z \in A$. By (ii) of Theorem 16.4 applied twice (as well as the associative property of composition), for every $z \in A$ we have

$$((f^{-1} \circ g^{-1}) \circ (g \circ f))(z) = f^{-1}(g^{-1}(g(f(z)))) = f^{-1}(f(z)) = z.$$

Using (iv) of Theorem 16.4 we may conclude that $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$. \square

Remember that Pólya suggests that after solving a problem, we should look back and see whether we can use the result or the method to solve a different problem. Here's a good chance to try that out: Use the proof above to establish the following.

Theorem 16.7. *Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions.*

- (i) *If f and g are one-to-one, then $g \circ f$ is one-to-one.*
- (ii) *If f and g are onto, then $g \circ f$ is onto.*

The converses of the two statements in the theorem above are not true. However, two corresponding weaker statements can be made. In addition, part (iii) of Theorem 16.8 provides a useful characterization of the inverse.

Theorem 16.8. *Let $f : A \rightarrow B$ and $g : B \rightarrow C$ be functions.*

- (i) *If $g \circ f$ is onto, then g is onto.*
- (ii) *If $g \circ f$ is one-to-one, then f is one-to-one.*
- (iii) *Suppose now that $f : A \rightarrow B$ and $g : B \rightarrow A$. If $f \circ g = i_B$ and $g \circ f = i_A$, then $g = f^{-1}$.*

How does (iii) in Theorem 16.8 differ from part (iv) in Theorem 16.4? Well, both are implications, but the antecedent in one is a disjunction and the antecedent in the other is a conjunction. In addition, in Theorem 16.8, we do not assume that f or g is bijective. You will need to show that the conditions in (iii) imply that f and g are, in fact, bijective. If you already know that one of your functions f and g is bijective, Theorem 16.4 will usually be easier to use than Theorem 16.8.

Exercise 16.9. Prove Theorem 16.8. \circ

Definitions

Definition 16.1. Given functions $f : A \rightarrow B$ and $g : C \rightarrow D$ with $\text{ran}(f) \subseteq C$, we define the **composition** of f and g as the function $g \circ f : A \rightarrow D$, where $(g \circ f)(x) = g(f(x))$. The composition is also called the **composite function** from A to D .

Definition 16.2. Let $f : A \rightarrow B$ be a bijective function. The **inverse** of f is the function $f^{-1} : B \rightarrow A$ defined by

$$f^{-1}(y) = x \text{ if and only if } f(x) = y.$$

Definition 16.3. The **identity function** on a set A is the function $i_A : A \rightarrow A$, defined by $i_A(x) = x$.

Solutions to Exercises

Solution (16.3). This problem only asks for a formula for f^{-1} , which we will give here. You need to think about how we obtained this formula. You should check that $f^{-1} : \mathbb{N} \rightarrow \mathbb{Z}$ defined by

$$f^{-1}(m) = \begin{cases} m/2 & \text{if } m \text{ is even} \\ -(m+1)/2 & \text{if } m \text{ is odd} \end{cases}$$

really is the inverse of f .

Solution (16.5). For the function in Example 16.1 we calculate

$$(f^{-1} \circ f)(x) = f^{-1}(x^3 - 5) = ((x^3 - 5) + 5)^{1/3} = (x^3)^{1/3} = x = i_{\mathbb{R}}(x)$$

and

$$(f \circ f^{-1})(x) = f((x+5)^{1/3}) = \left((x+5)^{1/3}\right)^3 - 5 = x + 5 - 5 = x = i_{\mathbb{R}}(x).$$

For the function in Example 16.2 the calculations are

$$(f^{-1} \circ f)(x) = f^{-1}\left(\frac{x+1}{x-3}\right) = \frac{3\frac{x+1}{x-3} + 1}{\frac{x+1}{x-3} - 1} = \frac{4x}{4} = x = i_{\mathbb{R} \setminus \{3\}}(x)$$

and

$$(f \circ f^{-1})(x) = f\left(\frac{3x+1}{x-1}\right) = \frac{\frac{3x+1}{x-1} + 1}{\frac{3x+1}{x-1} - 3} = \frac{4x}{4} = x = i_{\mathbb{R} \setminus \{1\}}(x).$$

Finally, for the function in Exercise 16.3 the calculations are as follows.

First, for $f^{-1} \circ f$, we use the two cases that f forces upon us. So suppose that $n \in \mathbb{Z}$ and $n \geq 0$. Then

$$(f^{-1} \circ f)(n) = f^{-1}(2n) = (2n)/2 = n,$$

since $2n$ is even.

Now suppose that $n < 0$. Then

$$(f^{-1} \circ f)(n) = f^{-1}(-2n - 1) = -((-2n - 1) + 1)/2 = n,$$

since $m = -2n - 1$ is odd. Therefore $(f^{-1} \circ f)(n) = n = i_{\mathbb{Z}}(n)$, completing the first part of the problem.

Now, for $f \circ f^{-1}$, we use the two cases f^{-1} forces upon us. So suppose that $m \in \mathbb{N}$ is even. Then

$$(f \circ f^{-1})(m) = f(m/2) = 2(m/2) = m,$$

since $m/2 \geq 0$. If m is odd, then

$$(f \circ f^{-1})(m) = f(-(m+1)/2) = -2(-(m+1)/2) - 1 = m,$$

since $-(m+1)/2 < 0$. Therefore $(f \circ f^{-1})(m) = m = i_{\mathbb{N}}(m)$, as required.

Solution (16.9). (i) If $c \in C$, then the fact that $g \circ f$ is onto implies that there exists $a \in A$ such that $(g \circ f)(a) = c$. Therefore $g(f(a)) = c$. Since $f(a) \in B$, we have shown that there is an element $b = f(a)$ in B such that $g(b) = c$. Since $g : B \rightarrow C$, we conclude that g is onto.

(ii) If a_1 and a_2 are in A and $f(a_1) = f(a_2)$, then $g(f(a_1)) = g(f(a_2))$. Therefore $(g \circ f)(a_1) = (g \circ f)(a_2)$. Since $g \circ f$ is one-to-one, $a_1 = a_2$ and f is one-to-one, as desired.

(iii) Since $g \circ f$ is one-to-one, (ii) implies that f is one-to-one. Since $f \circ g$ is onto, (i) implies that f is onto. Thus f is bijective. Consequently, (iii) follows from Theorem 16.4 (iv). \square

Problems

Problem 16.1. Find the compositions $f \circ g$ and $g \circ f$ assuming the domain of each is the largest set of real numbers for which the functions f , g , $f \circ g$, and $g \circ f$ make sense. In your solution to each of the following, give the compositions and the corresponding domain and range:

- $f(x) = 1/(1+x)$, $g(x) = x^2$;
- $f(x) = x^2$, $g(x) = \sqrt{x}$ (simplify this one);
- $f(x) = 1/x$, $g(x) = x^2 + 1$;
- $f(x) = |x|$, $g(x) = f(x)$.

Problem 16.2. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^3 + 4$. Use Theorem 16.8 to show that if $g : \mathbb{R} \rightarrow \mathbb{R}$ is defined by $g(x) = (x - 4)^{1/3}$, then $g = f^{-1}$.

Problem 16.3. Let $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ be defined by $f(x, y) = x + y$. Prove that there is no function $g : \mathbb{R} \rightarrow \mathbb{R}^2$ such that $g \circ f = i_{\mathbb{R}^2}$.

Problem 16.4. Let $f : \mathbb{R} \rightarrow \mathbb{R}^2$ be defined by $f(x) = (x, 0)$. Show that there is no function $g : \mathbb{R}^2 \rightarrow \mathbb{R}$ such that $f \circ g = i_{\mathbb{R}^2}$.

Problem 16.5. Functions $f : A \rightarrow B$ are given below. For each of them find the range of f . Further, if possible, find $f^{-1} : B \rightarrow A$. Rigorous proofs are not required, but you should provide explanations for each of your statements.

- The function $f : \mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ is defined by $f(x) = 1/x$.
- The function $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ is defined by $f(x, y) = x + y$.
- The function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ is defined by $f(x, y) = (y, x)$.
- The function $f : \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = \sin x$.
- The function $f : \{x \in \mathbb{R} : -\pi/2 < x < \pi/2\} \rightarrow \mathbb{R}$ is defined by $f(x) = \tan x$.

Problem 16.6. The functions $f : \mathbb{R} \setminus \{-2\} \rightarrow \mathbb{R} \setminus \{1\}$ and $g : \mathbb{R} \setminus \{1\} \rightarrow \mathbb{R} \setminus \{-2\}$ defined by

$$f(x) = \frac{x-3}{x+2} \quad \text{and} \quad g(x) = \frac{3+2x}{1-x}$$

are well-defined (you need not check this).

- Calculate $f \circ g$ and $g \circ f$.
- What can you conclude about f and g from your result in part (a)? If you use a theorem, give a reference.

Problem 16.7. (a) If possible, find examples of functions $f : A \rightarrow B$ and $g : B \rightarrow A$ such that $f \circ g = i_B$ when:

- $A = \{1, 2, 3\}$, $B = \{4, 5\}$;
- $A = \{1, 2\}$, $B = \{4, 5\}$;
- $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$.

Draw diagrams of A and B in each case above.

- Give an example of sets A and B , and functions $f : A \rightarrow B$ and $g : B \rightarrow A$ such that $f \circ g = i_B$, but $g \circ f \neq i_A$. (Thus the existence of a function g such that $f \circ g = i_B$ is *not* enough to conclude that f has an inverse!) Why doesn't this contradict Theorem 16.4, part (iv)?
- Give an example of sets A and B , and functions $f : A \rightarrow B$ and $g : B \rightarrow A$ such that $g \circ f = i_A$, but $f \circ g \neq i_B$. (Thus the existence of a function g such that $g \circ f = i_A$ is not enough to conclude that f has an inverse!) Why doesn't this contradict Theorem 16.4, part (iv)?
- Let A and B be two sets, and let $f : A \rightarrow B$ be a function. Assume further that there exists a function $g : B \rightarrow A$ such that $f \circ g = i_B$. Must f be one-to-one? onto?

- (e) Looking over your work above, what should be your strategy in solving a question like (d) above? Whatever you decide, use it to solve the following: Let f and g be as above and suppose $g \circ f = i_A$. Must f be one-to-one? onto?

Problem 16.8. Consider the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by $f(x, y) = (x, x + y)$. Show that f has an inverse and find the inverse function.

Problem# 16.9. Let $f : A \rightarrow B$ be a bijective function. Prove part (iii) of Theorem 16.4 and show that $(f^{-1})^{-1} = f$.

The following theorem is quite often useful. It provides an alternate way to prove that a function is bijective.

Theorem 16.10. *If $f : A \rightarrow B$, then the following are equivalent.*

1. *The function f is a bijection.*
2. *The function f has an inverse.*
3. *There exists a function $h : B \rightarrow A$ such that $h \circ f = i_A$ and $f \circ h = i_B$.*

Problem 16.10. Prove Theorem 16.10. (One way to do this is to prove that 1 implies 2; 2 implies 3; and 3 implies 1.)

Problem 16.11. Prove that $f : \mathbb{R}^+ \rightarrow \mathbb{R}$ defined by $f(x) = \ln x$ is bijective. (You may use properties of the logarithm function and exponential function.)

- Problem 16.12.** (a) Give an example of a function $f : A \rightarrow A$ such that $f \neq i_A$, but $f \circ f = i_A$. Must such a function f be one-to-one? onto?
- (b) Give an example of a nonzero function $f : \mathbb{R} \rightarrow \mathbb{R}$ such that $(f \circ f)(x) = 0$ for all $x \in \mathbb{R}$. Can such a function be one-to-one? onto?

Problem 16.13. Let $f : A \rightarrow A$ be a function. Suppose that $f \circ f : A \rightarrow A$ is a bijection. Must such a function f be a bijection? (Prove this or give a counterexample.)

Problem 16.14. Suppose that $f : A \rightarrow B$ and g_1 and g_2 are functions from B to A such that $f \circ g_1 = f \circ g_2$. Show that if f is bijective, then $g_1 = g_2$. If $g_1 \circ f = g_2 \circ f$ and f is bijective, must $g_1 = g_2$?

Problem 16.15. Let $f : A \rightarrow A$ be a function. Define a relation on A by $a \sim b$ if and only if $f(a) = f(b)$. Is this an equivalence relation? If f is one-to-one, what is the equivalence class of a point $a \in A$?

Problem 16.16. Let $f : A \rightarrow A$ be a function. Define a relation on A by $a \sim b$ if and only if $f(a) = b$. Is this an equivalence relation for an arbitrary function f ? If not, is there a function for which it is an equivalence relation?

Problem# 16.17. Let A, B, C , and D be nonempty sets. Let $f : A \rightarrow B$ and $g : C \rightarrow D$ be functions.

- (a) Prove that if f and g are one-to-one, then $H : A \times C \rightarrow B \times D$ defined by

$$H(a, c) = (f(a), g(c))$$

is a one-to-one function. (Check that it is one-to-one and a function.)

- (b) Prove that if f and g are onto, then H is also onto.

Problem# 16.18. Let A, B, C , and D be nonempty sets. Let $f : A \rightarrow B$ and $g : C \rightarrow D$ be functions. Consider H defined on $A \cup C$ by

$$H(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in C \end{cases}.$$

Show that there exist sets A, B, C , and D for which H is *not* a function, but there also exist such sets for which H is a function. What conditions can we place on A and C to ensure that H is a function?

Problem 16.19. Let $a \in \mathbb{R}$ with $|a| < 1$. Define f on the set $\{x \in \mathbb{R} : |x| < 1\}$ by

$$f(x) = \frac{a-x}{1-ax}.$$

- Show that the range of f is contained in the set $\{x \in \mathbb{R} : |x| < 1\}$.
- Does f map onto the set $\{x \in \mathbb{R} : |x| < 1\}$?
- Prove that f is one-to-one.
- Compute $f \circ f$.
- Find f^{-1} .

Problem 16.20. Let $\mathbb{R}[x]$ denote the set of all polynomials with real coefficients. (See Problem 10.13.)

- Define a function f on $\mathbb{R}[x]$ by $f(p) = p(0)$. What is the range of f ? Is f one-to-one?
- Define a function g on the nonzero polynomials in $\mathbb{R}[x]$ by $g(p) = \text{degree of } p$. Is g a function? Is it one-to-one? What is the range of g ?
- Recall that a value z is a root of a polynomial p if $p(z) = 0$. Define F on $\mathbb{R}[x]$ by $F(p) = \text{a root of } p$. Is F a function? Why or why not?
- Define h on $\mathbb{R}[x]$ by $(h(p))(x) = xp(x)$. Is h a function? If so, is it one-to-one? What is the range of h ?
- Define $k : \mathbb{R}[x] \rightarrow \mathbb{R}[x]$ by $k(p) = p \circ p$. Show that k is neither one-to-one nor onto.

Problem 16.21. For each part give examples of functions $f : A \rightarrow B$ and $g : B \rightarrow C$ satisfying the stated conditions.

- The composition $g \circ f$ is onto, but f is not onto.
- The composition $g \circ f$ is one-to-one, but g is not one-to-one.

Problem 16.22. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a function such that f is onto and $f \circ f \circ f = f$. Prove that f is bijective.

Problem 16.23. Let A, B, C , and D be nonempty sets with $B \subseteq C$ and $D \subseteq A$. Suppose that both functions $f: A \rightarrow B$ and $g: C \rightarrow D$ are onto and $f \circ g \circ f = f$. (Note that the compositions $g \circ f$ and $f \circ g$ are both defined.)

- (a) Show that $(f \circ g)|_B$ is one-to-one.
- (b) Give an example to show that $(g \circ f)|_D$ is not necessarily one-to-one.

Chapter 17

Images and Inverse Images

In the last chapter, we looked at where points in the domain are mapped to under a function f and where points in the range come from under f . But sometimes we need to look at where f maps a whole set, or where an entire set comes from. So here are two definitions that are waiting to be understood.

Let $f : X \rightarrow Y$ be a function and let $A \subseteq X$. Then the **image** of A under f is the set

$$f(A) = \{f(a) : a \in A\}.$$

Note that $f(A)$ is the notation we use for this set, and that this set is a subset of Y . In “street talk” the image of A under f is where the elements of A were taken by f .

Exercise 17.1. It’s good to start small. So let’s begin with the two sets $A = \{1, 2, 4\}$ and $B = \{-1, 1, -2, 3\}$. Find each of the requested images under the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$.

- (a) What is $f(A)$?
- (b) What is $f(B)$?
- (c) What is $f(A \cap B)$?
- (d) What is $f(A) \cap f(B)$?

We’ll solve (a) for you here, so you can see what we are asking you to do. We claim that $f(A) = \{1, 4, 16\}$. To see this, we use the definition:

$$f(A) = \{f(a) : a \in A\} = \{f(1), f(2), f(4)\} = \{1, 4, 16\}. \quad \circ$$

Small sets are easier because you can often list the values, just as we did above. This won’t be possible, in general, as you will see below.

We are also interested in where sets in the codomain come from. This is called the inverse image of a set (because we are going backwards) and there is one unfortunate thing about it: the notation involves the symbol f^{-1} , which we have used only when f is bijective. Well, here f may not be bijective, and therefore, f^{-1} may not be a function. Though this may be confusing at first, this is generally agreed upon

notation and you (the reader) must check carefully on the context. Having said all that, we now define the inverse image.

Let $f : X \rightarrow Y$ be a function and let $B \subseteq Y$. Then the **inverse image** of B under f is the set

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

In other words, the inverse image of B is *the subset of X* consisting of all the elements in the domain that get mapped into B . Note that when f is *not* bijective, the notation $f^{-1}(y)$ makes no sense (why?). If you want to talk about the inverse image of a set with just one element, say so by writing $f^{-1}(\{y\})$. (You may find texts in which the authors use the notation $f^{-1}(y)$, but we find that it often introduces unnecessary confusion.)

Exercise 17.2. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^2$. Find:

- (a) $f^{-1}(\{4\})$;
- (b) $f^{-1}(\{1, 2, 4\})$;
- (c) $f^{-1}(f(A))$, where $A = \{1, 2\}$.

Again, we will do (a) here, so you can see what we are asking you to do. By definition,

$$f^{-1}(\{4\}) = \{x \in \mathbb{R} : f(x) \in \{4\}\} = \{x \in \mathbb{R} : f(x) = 4\}.$$

Replacing f by what it equals, we have

$$f^{-1}(\{4\}) = \{x \in \mathbb{R} : x^2 = 4\} = \{-2, 2\}.$$

○

Since the sets above are small, we can list all the elements. We ask that you now check your understanding with more challenging sets, but still using the same function as in the previous exercises.

By carefully writing out the definitions of the sets in Exercise 17.3, it is possible to guess what the answers are. We provide rigorous proofs for several parts at the end of this chapter. If you wish to try them yourself first (which you are certainly encouraged to do), make sure that you work from the inside out on parts (e)–(h). So in part (e), for example, first find $f([0, 1])$ (which works just like (a)) and call that set A . Then find $f^{-1}(A)$ (which works just like (d)).

Exercise 17.3. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^2$. Find:

- (a) $f([-1, 1])$;
- (b) $f(\mathbb{Z})$;
- (c) $f^{-1}(\mathbb{N})$;
- (d) $f^{-1}([-1, 0])$;
- (e) $f^{-1}(f([0, 1]))$;
- (f) $f(f^{-1}([-1, 0]))$;
- (g) $f^{-1}([0, 1] \cup [2, 4])$;
- (h) $f([0, 1] \cap [-1, 0])$;

- (i) $f([0, 1]) \cap f([-1, 0])$. ○

Your experience with concrete sets will help you work with abstract sets.

Exercise 17.4. Looking back at the examples in the exercises above, decide which of the following you think are true for all functions $f : X \rightarrow Y$, all subsets A and B of X , and all subsets C and D of Y :

- (a) $f(f^{-1}(C)) = C$;
 (b) $f^{-1}(f(A)) = A$;
 (c) $f(A \cap B) = f(A) \cap f(B)$;
 (d) $f(A) = f(B)$ implies that $A = B$;
 (e) $f^{-1}(C) = f^{-1}(D)$ implies that $C = D$. ○

All of the statements above may look reasonable, yet they are all false. Nevertheless, there are many similar statements that are true. You can prove them all with the tools you have developed at this point. To emphasize the accepted writing techniques, we provide an example below.

Theorem 17.5. Let $f : X \rightarrow Y$ and let A_1 and A_2 be subsets of X . Then

$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2).$$

“Understanding the problem.” Remember that you won’t get anywhere if you don’t know the definitions. So we need to figure out what the sets in the statement are. We begin by making sure we know what $f(A_1 \cap A_2)$, $f(A_1)$, and $f(A_2)$ are. First, $f(A) = \{f(x) : x \in A\}$. So that should make it pretty clear. Things in $f(A_1 \cap A_2)$ look like $f(x)$ where $x \in A_1 \cap A_2$. Now it should occur to you that you must write out what it means to be in $f(A_1) \cap f(A_2)$. Once you have done that, you have done the preliminaries.

“Devising a plan.” When we worked with sets with a special form (like the Cartesian product of two sets) we emphasized that if we never used the special form of the elements, we would most likely never prove the desired result. The same is true here—if we never use the fact that the elements have the form $f(x)$ where $x \in A_1 \cap A_2$ we shouldn’t expect to be able to prove the result. The next step is to note that what we want to do is to show that one set is contained in another set. We know how to do that, too. So our plan is to start with an element in the set on the left side, use the special form of this set, and show the element is in the set on the right. As we *“carry out our plan,”* note how quickly we move to the special form of the element.

Proof. If $y \in f(A_1 \cap A_2)$, then $y = f(x)$ for some $x \in A_1 \cap A_2$. Since $x \in A_1 \cap A_2$, we have $x \in A_1$ and $x \in A_2$. Since $x \in A_1$ and $y = f(x)$, we see that $y \in f(A_1)$. Similarly, since $x \in A_2$ and $y = f(x)$, we see that $y \in f(A_2)$. Therefore $y \in f(A_1) \cap f(A_2)$. Thus $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. □

Exercise 17.6. We already have an example to show that, with the notation from the theorem above, we need not have $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$. But what is wrong with the following “proof” of this “nonfact”?

Not a proof. It follows from Theorem 17.5 that $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. To show the reverse set inclusion, we let $y \in f(A_1) \cap f(A_2)$. By definition of intersection, $y \in f(A_1)$ and $y \in f(A_2)$. Therefore, $y = f(x)$ for some x in A_1 and $y = f(x)$ for some $x \in A_2$. Since $x \in A_1$ and $x \in A_2$, we see that $x \in A_1 \cap A_2$. Thus $y = f(x)$ where $x \in A_1 \cap A_2$, so $y \in f(A_1 \cap A_2)$. This proves that $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$, and the nonfact is established! \square

We know there’s something wrong above since the assertion isn’t always true. But it isn’t always false either. Find the error and see if you can think of another hypothesis we might place on f that would help us to determine the functions for which the assertion is true. \circ

The next theorem is one you will use repeatedly. You really can do all the proofs yourself.

Theorem 17.7. *Let $f : X \rightarrow Y$. Let A, A_1 , and A_2 be subsets of X and B, B_1 , and B_2 subsets of Y . Then*

1. *if $A_1 \subseteq A_2$, then $f(A_1) \subseteq f(A_2)$;*
2. *$f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$;*
3. *$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$;*
4. *in general, $f(X \setminus A) \neq Y \setminus f(A)$;*
5. *if $B_1 \subseteq B_2$, then $f^{-1}(B_1) \subseteq f^{-1}(B_2)$;*
6. *$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$;*
7. *$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$;*
8. *$f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$;*
9. *$A \subseteq f^{-1}(f(A))$;*
10. *$f(f^{-1}(B)) \subseteq B$.*

We have already presented a proof of (3) in Theorem 17.5, and we will provide a proof of (9) in Example 17.8. The other parts of the theorem are left to the reader (that’s you) in the problems. Remember that before beginning the proof of each part you must make sure you know what the left-hand side is, and what the right-hand side is. We suggest that you write out the element definition of both sides carefully (as we do in Example 17.8 below), and then show that appropriate relations hold using acceptable mathematical and writing techniques.

If additional conditions are placed on the function f , then some of the conclusions in Theorem 17.7 can be strengthened. We look at such a case in the following example. Some of the problems will ask you to consider similar restrictions.

Example 17.8. We will prove part 9 of Theorem 17.7. Then we will show that the inclusion is, in general, proper. We conclude this example by showing that if f is required to be one-to-one, then the two sets are actually equal.

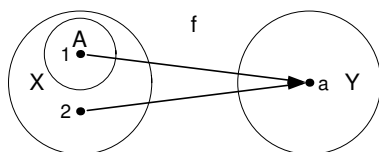


Fig. 17.1 $f : \{1, 2\} \rightarrow \{a\}$

- (a) First we prove that if $f : X \rightarrow Y$ and $A \subseteq X$, then $A \subseteq f^{-1}(f(A))$. Before we begin, we note that the right side is a bit complicated. Let's make sure we understand it: Since $f^{-1}(B) = \{x \in X : f(x) \in B\}$ replacing B by $f(A)$, we see that $f^{-1}(f(A)) = \{x \in X : f(x) \in f(A)\}$. So we must show that if $z \in A$, then $z \in \{x \in X : f(x) \in f(A)\}$; in other words, we must show that $z \in X$ and $f(z) \in f(A)$.

Proof. If $z \in A$, then since $A \subseteq X$, we know that $z \in X$. By the definition of $f(A)$, we have $f(z) \in f(A)$. Thus, $z \in f^{-1}(f(A))$, and $A \subseteq f^{-1}(f(A))$. \square

- (b) **Figure 17.1** indicates why, for an arbitrary function and an arbitrary set A , we cannot expect that the two sets A and $f^{-1}(f(A))$ are equal. From the diagram we see that if we let $A = \{1\}$ and define $f : \{1, 2\} \rightarrow \{a\}$ by $f(1) = f(2) = a$, then $A = \{1\}$ while $f^{-1}(f(A)) = f^{-1}(f(\{1\})) = f^{-1}(\{a\}) = \{1, 2\}$. Thus $A \neq f^{-1}(f(A))$.
- (c) However, if the function $f : X \rightarrow Y$ is one-to-one and $A \subseteq X$, then we can conclude that $A = f^{-1}(f(A))$.

Proof. The inclusion $A \subseteq f^{-1}(f(A))$ is proven in (a) above. For the reverse inclusion, suppose $z \in f^{-1}(f(A))$. Then $z \in X$ and $f(z) \in f(A)$. Thus, there exists $x \in A$ such that $f(z) = f(x)$. Now f is one-to-one and so $z = x$. But $x \in A$, so $z \in A$. Hence $f^{-1}(f(A)) \subseteq A$, and we conclude that the two sets are equal. \square

Definitions

Definition 17.1. Let $f : X \rightarrow Y$ be a function and let $A \subseteq X$. Then the **image** of A under f is the set

$$f(A) = \{f(a) : a \in A\}.$$

Definition 17.2. Let $f : X \rightarrow Y$ be a function and let $B \subseteq Y$. Then the **inverse image** of B under f is the set

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

Solutions to Exercises

Solution (17.1). You should be able to check that:

- (b) $f(B) = \{1, 4, 9\}$;
- (c) $f(A \cap B) = \{1\}$;
- (d) $f(A) \cap f(B) = \{1, 4\}$.

Solution (17.2). You should be able to check that:

- (b) $f^{-1}(\{1, 2, 4\}) = \{-1, 1, -\sqrt{2}, \sqrt{2}, -2, 2\}$;
- (c) $f^{-1}(f(A)) = f^{-1}(\{1, 4\}) = \{-1, 1, -2, 2\}$.

Solution (17.3). We give complete solutions to (a), (d), (f), and (h) followed by answers to (b), (c), (e), (g), and (i).

- (a) We claim that $f([-1, 1]) = [0, 1]$. To see this, let $y \in f([-1, 1])$. By definition of the image,

$$f([-1, 1]) = \{f(x) : x \in [-1, 1]\} = \{x^2 : x \in [-1, 1]\}.$$

So there exists $x \in [-1, 1]$ such that $y = x^2$. Since $x \in [-1, 1]$, we know that $0 \leq x^2 \leq 1$. Therefore, $y \in [0, 1]$, and $f([-1, 1]) \subseteq [0, 1]$.

Conversely, if $y \in [0, 1]$, then we let $x = \sqrt{y}$. Thus $x \in [0, 1] \subset [-1, 1]$, and $f(x) = x^2 = (\sqrt{y})^2 = y$. Therefore, there exists $x \in [-1, 1]$ such that $y = f(x)$ and $y \in f([-1, 1])$. So $[0, 1] \subseteq f([-1, 1])$, and we conclude that the two sets are equal.

- (d) We claim that $f^{-1}([-1, 0]) = \{0\}$. To see this, let $x \in f^{-1}([-1, 0])$. By definition,

$$f^{-1}([-1, 0]) = \{x \in \mathbb{R} : f(x) \in [-1, 0]\} = \{x \in \mathbb{R} : x^2 \in [-1, 0]\}.$$

Thus $x \in f^{-1}([-1, 0])$ implies that $x^2 \in [-1, 0]$. This is only possible if $x = 0$. Therefore $f^{-1}([-1, 0]) \subseteq \{0\}$. Now suppose that $x \in \{0\}$. Then $f(x) = f(0) = 0$. Therefore, $f(x) \in [-1, 0]$, and $x \in f^{-1}([-1, 0])$. Consequently, $\{0\} \subseteq f^{-1}([-1, 0])$, and we conclude that $f^{-1}([-1, 0]) = \{0\}$.

- (f) We claim that $f(f^{-1}([-1, 0])) = \{0\}$. By (d), we know $f^{-1}([-1, 0]) = \{0\}$. Therefore, we need to find

$$f(f^{-1}([-1, 0])) = f(\{0\}).$$

Thus

$$f(f^{-1}([-1, 0])) = f(\{0\}) = \{f(0)\} = \{0\},$$

as desired.

- (h) We work from the inside out. Thus,

$$f([0, 1] \cap [-1, 0]) = f(\{0\}) = \{f(0)\} = \{0\}.$$

The answer to (b) is $\{z^2 : z \in \mathbb{N}\}$; to (c) is $\{\sqrt{n} : n \in \mathbb{N}\} \cup \{-\sqrt{n} : n \in \mathbb{N}\}$; to (e) is $[-1, 1]$; to (g) is $[-1, 1] \cup [-2, -\sqrt{2}] \cup [\sqrt{2}, 2]$; and to (i) is $[0, 1]$.

There are many possible ways to solve these problems. Though each problem seems to be different, what remains the same in every problem is that you need to understand the notation and the definitions.

Solution (17.4). None of the five statements holds for all functions and sets. Thus we will give a counterexample for each case. In all cases we will use the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$.

- (a) Exercise 17.3 (f) provides a counterexample.
- (b) Exercise 17.3 (e) provides a counterexample.
- (c) Exercise 17.3 (h) and (i) provide a counterexample.
- (d) Using f as defined above, $f(\{-1, 1\}) = \{1\} = f(\{1\})$ but $\{-1, 1\} \neq \{1\}$.
- (e) Again using the function defined above, $f^{-1}(\{-1, 0\}) = \{0\} = f^{-1}(\{0\})$ but $\{-1, 0\} \neq \{0\}$.

Solution (17.6). In “not a proof” we correctly establish that “ $y = f(x)$ for some $x \in A_1$ and $y = f(x)$ for some $x \in A_2$.” From this statement we incorrectly conclude that “ $x \in A_1$ and $x \in A_2$.” We may only conclude that there exists an $x_1 \in A_1$ such that $y = f(x_1)$, and there exists an $x_2 \in A_2$ such that $y = f(x_2)$. We may not conclude that $x_1 = x_2$. Indeed, Exercise 17.1 shows that there are cases where neither of the two elements is in the intersection.

However, the following is true. Let $f : X \rightarrow Y$ be an injective function, and let A_1 and A_2 be subsets of X . Then $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$. Why? Well, we know that $f(x_1) = y = f(x_2)$ and we now know that f is injective. Thus, $x_1 = x_2$, so $x_1 \in A_1 \cap A_2$. The rest of the “not a proof” is valid.

Spotlight: Minimum or Infimum?

If you’ve ever forgotten to show that the infimum of a set was the minimum, this historical example should show you that it can happen to the best of us.

Suppose you know the temperature on the surface of the earth (because people on the surface measured it) and you want the temperature on the inside (but no one can get to the place to measure it). How do you get the temperature? This kind of question interested several famous mathematicians. In fact, there’s plenty of mathematical research done today that is related to this problem.

This problem is known as the Dirichlet problem. It can be studied in more generality, but we’ll stick to looking at functions defined on a sphere. To understand the statement, you need to have studied several variable calculus. At the end of this spotlight, we will state the problem on the sphere, along with the references, for those of you who have the background.

The solution to this problem used something called the “Dirichlet principle.” The idea of the principle was to look at a collection of certain integrals with the region

of integration fixed, but with different integrands. It was first argued that the values of the integrals were bounded below (and therefore, as we have learned, there was an infimum). From there, the mathematicians assumed that for one of the functions, the integral was the minimum. This principle was used by many excellent mathematicians: by George Green, Georg Friedrich Bernhard Riemann, Sir William Thomson (also known as Lord Kelvin), and others. In 1870, Karl Theodor Wilhelm Weierstrass presented an important paper about the validity of this argument. Even the title of his article “Über das sogenannte Dirichlet’sche Princip” (On the so-called Dirichlet principle) is enough to show what Weierstrass thought of the principle [107]. He began his paper by reconstructing Dirichlet’s argument. He then explained that though an expression may have a lower bound that we can get arbitrarily close to, we may never actually reach it. Weierstrass concluded his paper with an example showing how this might happen. Almost thirty years later, David Hilbert supplied a proof of the principle for certain cases when he presented what he called the “resuscitation” of the Dirichlet principle [86, p. 67].

It may seem odd that mathematicians of this calibre would use an unproven principle. There are two things to remember. First, the principle was supported on physical grounds. Second, rigor was still being introduced to mathematics. In spite of its unusual history, the Dirichlet principle served an important purpose. In Kline’s words [59, p. 704] “Had the progress made with the use of the principle awaited Hilbert’s work, a large segment of nineteenth-century work on potential theory and function theory would have been lost.”

More information on this is available in [35], [59], [32], and [71]. Another criticism of the Dirichlet principle, from a different point of view, was published by Friedrich Prym. More information about this can be found in [87]. The statement of the problem in \mathbb{R}^3 is the following: Let f be a continuous real-valued function on the sphere of radius one (the unit sphere). A real-valued function g is called harmonic on the open unit ball ($\{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 < 1\}$) if g has continuous second partial derivatives satisfying

$$g_{xx} + g_{yy} + g_{zz} = 0$$

throughout the ball. The question is: Does there exist a function F that is continuous on the closed ball of radius one, equal to f on the unit sphere, and harmonic on the open unit ball?

Problems

Problem 17.1. Recall that $[a, b]$ denotes the closed interval from a to b , while (a, b) denotes the open interval. For the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = 3x - 1$, find:

- (a) $f((0, 1))$;
- (b) $f((a, b))$, where $a, b \in \mathbb{R}$ and $a < b$;
- (c) $f^{-1}((-2, -1))$;

(d) $f^{-1}((a, b))$, where $a, b \in \mathbb{R}$ and $a < b$.

Problem 17.2. For the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = 2x^2$, find:

- (a) $f((0, 1))$;
- (b) $f((-1, 3))$;
- (c) and (in general) $f((a, b))$, where $a, b \in \mathbb{R}$ and $a < b$;
- (d) $f^{-1}((-2, -1))$;
- (e) $f^{-1}((0, 2))$;
- (f) and (in general) $f^{-1}((a, b))$, where $a, b \in \mathbb{R}$ and $a < b$.

Actually, we are really only interested in your answers to (c) and (f). So why did you have to work all the other parts?

Problem 17.3. For the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = |x|$, find:

- (a) $f((-1, 1))$;
- (b) $f(\{-1, 1\})$;
- (c) $f^{-1}(\{1\})$;
- (d) $f^{-1}([-1, 0])$;
- (e) $f^{-1}(f([0, 1]))$.

Problem 17.4. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = 9 - x^2$. Find the two sets $f((-3, 1])$ and $f^{-1}((-1, 4))$.

Problem 17.5. Consider the function $\chi_{(0,1)} : \mathbb{R} \rightarrow \mathbb{R}$ (this is the characteristic of Definition 14.4). Find:

- (a) $\chi_{(0,1)}((0, 1))$;
- (b) $\chi_{(0,1)}((-1, 3))$;
- (c) and (in general) $\chi_{(0,1)}((a, b))$, where $a, b \in \mathbb{R}$ and $a < b$; prove that the set you found is correct;
- (d) $\chi_{(0,1)}^{-1}((-2, -1))$;
- (e) $\chi_{(0,1)}^{-1}((0, 2))$;
- (f) and (in general) $\chi_{(0,1)}^{-1}((a, b))$, where $a, b \in \mathbb{R}$ and $a < b$; prove that the set you found is correct,

Actually, we are really only interested in your answers to (c) and (f). So why did you have to work all the other parts?

Problem 17.6. We denote the characteristic function of \mathbb{Z} in \mathbb{R} by $\chi_{\mathbb{Z}} : \mathbb{R} \rightarrow \mathbb{R}$ (see Definition 14.4). In each case below, start by writing out the definition for the particular set and function. Then write the solution to each of the following in as simple a form as possible:

- (a) $\chi_{\mathbb{Z}}(\mathbb{Z}^+)$;
- (b) $\chi_{\mathbb{Z}}^{-1}(\mathbb{Z}^+)$;
- (c) $\chi_{\mathbb{Z}}(\chi_{\mathbb{Z}}^{-1}(\mathbb{Z}^+))$;
- (d) $\chi_{\mathbb{Z}}^{-1}(\chi_{\mathbb{Z}}(\mathbb{Z}^+))$.

Problem 17.7. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = x^4 + 1$.

- Make a careful graph of f .
- Using your graph, show how you can guess $f([0, 2])$.
- Prove that your guess for $f([0, 2])$ is correct.
- Use your graph to find $f^{-1}([2, 17])$.
- Prove that your guess for $f^{-1}([2, 17])$ is correct.

Problem 17.8. Let p and q be two polynomials of degree two with real coefficients. (See Problem 10.13 for definitions.) Suppose $p^{-1}(\{0\}) = q^{-1}(\{0\})$.

- Give an example of such p and q , with $p \neq q$.
- Suppose that $p^{-1}(\{0\}) = \{0, 1\} = q^{-1}(\{0\})$. Must $p = q$? Either prove this or give a counterexample.

Problem 17.9. Let $f : \mathbb{Z} \rightarrow \mathbb{N}$ be defined by

$$f(n) = \begin{cases} -2n & \text{if } n \leq 0 \\ 2n - 1 & \text{if } n > 0 \end{cases}.$$

Find $f(2\mathbb{Z})$ and prove that your answer is correct.

Problem 17.10. Prove Theorem 17.7 part 1.

Problem 17.11. Using Theorem 17.7 part 1, rather than element-chasing, prove Theorem 17.7 part 3.

Problem 17.12. Prove Theorem 17.7 part 2.

Problem 17.13. (a) Establish part 4 of Theorem 17.7. We suggest the following strategy: Try to prove that the two sets are equal. If you do this carefully, you may start to wish for restrictions on f that you don't have. This should help you think of examples to show that the two sets need not be equal.

- If f is onto, does the statement in Theorem 17.7 part 4 become an equality? What if f is one-to-one?
- Show that if f is bijective, then equality holds.

Problem 17.14. (a) Prove Theorem 17.7 part 5.

- In the same context, what can you conclude if $B_1 = B_2$? State your result and prove it.

Problem 17.15. Prove Theorem 17.7 part 6.

Problem 17.16. Prove Theorem 17.7 part 7.

Problem 17.17. Prove Theorem 17.7 part 8.

Problem 17.18. (a) Prove Theorem 17.7 part 10.

- Give an example to show that the two sets may not be equal.
- If f is onto, must the two sets be equal?

- (d) If f is one-to-one, must the two sets be equal?

Problem 17.19. Let X and Y be nonempty sets and $f : X \rightarrow Y$ a function.

- (a) Prove or give a counterexample to the statement: If A and B are subsets of X , then $f(A \setminus B) = f(A) \setminus f(B)$.
- (b) Find necessary and sufficient conditions on the function f such that for all subsets A and B of X , we have $f(A \setminus B) = f(A) \setminus f(B)$.

Problem 17.20. Let $f : X \rightarrow Y$ be a function satisfying $f(A) \cap f(B) = \emptyset$ whenever A and B are sets with $A \cap B = \emptyset$.

- (a) Give an example of such a function. Prove that your example satisfies the condition above.
- (b) Prove that such a function must be one-to-one.

Problem 17.21. Let $f : A \rightarrow B$ be a function. Prove that if f is onto, then the collection $\{f^{-1}(\{b\}) : b \in B\}$ partitions the set A .

Problem 17.22. Suppose that $f : X \rightarrow Y$ is a function, and let A_1 and A_2 be subsets of X .

- (a) If $f(A_1) = f(A_2)$, must $A_1 = A_2$?
- (b) Let f be a bijective function. Show that if $f(A_1) = f(A_2)$, then $A_1 = A_2$. Indicate clearly where you use one-to-one or onto. Did you use both?

Problem 17.23. Suppose that $f : X \rightarrow Y$ is a function, and let B_1 and B_2 be subsets of Y .

- (a) If $f^{-1}(B_1) = f^{-1}(B_2)$, must $B_1 = B_2$?
- (b) Let f be a bijective function. Show that if $f^{-1}(B_1) = f^{-1}(B_2)$, then $B_1 = B_2$. Indicate clearly where you use one-to-one or onto. Did you use both?

Problem 17.24. Let X be a nonempty set and let A_1 and A_2 be subsets of X . Recall the characteristic function of A in X of Definition 14.4.

- (a) If $\chi_{A_1} = \chi_{A_2}$, must $A_1 = A_2$?
- (b) We define the product $\chi_{A_1} \cdot \chi_{A_2}$ pointwise by $(\chi_{A_1} \cdot \chi_{A_2})(x) = \chi_{A_1}(x) \cdot \chi_{A_2}(x)$ for all $x \in X$. Prove that $\chi_{A_1} \cdot \chi_{A_2} = \chi_{A_1 \cap A_2}$.
- (c) Show that $\chi_{A_1} + \chi_{A_2} - \chi_{A_1 \cap A_2} = \chi_{A_1 \cup A_2}$. (In other words, for each $x \in X$, we have $\chi_{A_1}(x) + \chi_{A_2}(x) - \chi_{A_1 \cap A_2}(x) = \chi_{A_1 \cup A_2}(x)$.)
- (d) Can you find a similar result for $\chi_{X \setminus A_1}$?

Problem 17.25. (For students with a background in calculus.) For real numbers c, d with $c < d$ we denote the open interval in \mathbb{R} by $(c, d) = \{x \in \mathbb{R} : c < x < d\}$. Recall that a function $f : \mathbb{R} \rightarrow \mathbb{R}$ is strictly increasing if for all $x, y \in \text{dom}(f)$ whenever $x < y$, then $f(x) < f(y)$.

- (a) Show that there are continuous functions $f : \mathbb{R} \rightarrow \mathbb{R}$ and real numbers a, b with $a < b$ such that $f((a, b)) \neq (f(a), f(b))$.
- (b) Prove that a continuous function $f : \mathbb{R} \rightarrow \mathbb{R}$ is strictly increasing if and only if $f((a, b)) = (f(a), f(b))$ for all $a, b \in \mathbb{R}$ with $a < b$.

Chapter 18

Mathematical Induction

Suppose that you want to show something is true for all positive integers. You could start by checking that the statement is true for $n = 1$, $n = 2$, and so on, but you would have to stop somewhere. Even if you check lots and lots of integers, you can run into problems. Consider the following:

Let us suppose that you are asked to prove that $n^2 + n + 41$ is prime for every positive integer n . You might think the following is good enough to convince someone: if $f(n) = n^2 + n + 41$, then $f(1) = 43$ (which is prime), $f(2) = 47$ (which is prime), $f(3) = 53$ (prime too), and so on. In fact, checking the first 39 integers reveals that $f(n)$ is indeed prime for $n = 1, \dots, 39$. Is this enough evidence to prove that it is true for all positive integers n ? Check $n = 40$: $f(40) = 1681$, which is divisible by 41. What's the moral of this story? That examples, even many, many examples, are not a method of proof. It can help us find counterexamples or it can motivate us to formulate a conjecture, but unless we can check every single case, it will never prove anything.

One mathematical technique to prove that a statement holds for all positive integers is to show that the statement is true for $n = 1$ and that whenever it is true for a positive integer n , it is true for the next positive integer $n + 1$. Then, since you have shown it is true for $n = 1$, it must be true for $n = 2$ (because it's always true for a successor). Now that the statement is true for $n = 2$, it has to be true for $n = 3$, because 3 is the integer after 2, and so on. This is called mathematical induction, and a more precise description of this method of proof is given below.

This method is sometimes compared to lining up dominoes and making them fall down (see H. Steinhaus [102]). What has to happen? The first one has to fall, and every time one falls the one after it must fall. Once this happens, all the dominoes do fall down.

Theorem 18.1 (Principle of mathematical induction). *For an integer n , let $P(n)$ denote an assertion. Suppose that*

- (i) *(The base step) $P(1)$ is true, and*
- (ii) *(The induction step) for all positive integers n , if $P(n)$ is true, then $P(n + 1)$ is true.*

Then $P(n)$ holds for all positive integers n .

The principle of mathematical induction is a direct consequence of the well-ordering principle of \mathbb{N} we came across in Chapter 12. The proof of Theorem 18.1 will be by contradiction: were the induction principle false, then we could construct a nonempty subset of the natural numbers that would not have a minimum—a contradiction to the well-ordering principle. This is the main idea in the proof that follows.

Proof. Suppose the induction principle were false. Then there would exist an assertion P that would satisfy conditions (i) and (ii) of the theorem, but $P(n)$ would be false for some $n \in \mathbb{Z}^+$. So let $A = \{k \in \mathbb{Z}^+ : P(k) \text{ is false}\}$. Our supposition implies that A is nonempty. By the well-ordering principle [p. 125], the set A has a minimum. Let m denote this minimum. By condition (i), $m \neq 1$. Since $m \in \mathbb{Z}^+$, it follows that $m \geq 2$. Consider the integer $n = m - 1 \geq 1$. Since $n < m$ and m is the minimum of A , we know that $n \notin A$. Thus $P(n)$ is true. By condition (ii), $P(n+1)$ is true too. But $P(n+1) = P(m)$, so $P(m)$ must also be true, a contradiction. \square

Students often mistakenly believe condition (ii) says that $P(n)$ is true, and ask why we would state it again as a conclusion. Look carefully at condition (ii). Note that it is an implication. We are *not* saying that $P(n)$ is true. We *are* saying that if $P(n)$ is true, then $P(n+1)$ is true. The antecedent in this implication is called the induction hypothesis.

The next example is one that is associated with Carl Friedrich Gauss. As one version of the story goes, when Gauss was 10 years old, his teacher, Herr Büttner, asked the students to sum the integers from 1 to 100. Gauss did it almost instantly. It is believed that he did it by the following method.

Write the sum horizontally forwards and backwards as:

$$\begin{array}{r} 1 + 2 + 3 + \cdots + 99 + 100 \\ 100 + 99 + 98 + \cdots + 2 + 1 \end{array}$$

Now add vertically. When you do this, you will get 101 one hundred times; in other words, you get $(101)(100)$. This is twice the sum that you needed, so the answer must be $(101)(100)/2$. There is nothing special about the integer 100. If you try this with a general positive integer n , you will see that $1 + 2 + 3 + \cdots + n = n(n+1)/2$ for every positive integer n . What a nice formula! You will give it a rigorous proof using mathematical induction when you work Problem 18.1. Is something like this formula true for the sums of squares of the first n integers? Indeed it is.

Example 18.2. Using mathematical induction, show that

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

for every positive integer n .

Proof. Let $P(n)$ be the assertion that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

First we check the base step: $P(1)$ is the statement that $1 = (1(1+1)(2+1))/6$, and this is certainly true.

Now we verify the induction step. Let $n \in \mathbb{Z}^+$ and suppose $P(n)$ holds. Thus we suppose that for an $n \in \mathbb{Z}^+$ we have

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}. \quad (18.1)$$

We wish to show that $P(n+1)$ holds; that is, that

$$1^2 + 2^2 + \cdots + (n+1)^2 = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.$$

We start by grouping the left side of $P(n+1)$ and then simplify as follows:

$$\begin{aligned} & 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 \\ &= (1^2 + 2^2 + \cdots + n^2) + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \quad (\text{by our induction hypothesis (18.1)}) \\ &= (n+1) \left(\frac{n(2n+1)}{6} + (n+1) \right) \quad (\text{factor out } n+1) \\ &= (n+1) \left(\frac{2n^2 + 7n + 6}{6} \right) \\ &= (n+1) \frac{(n+2)(2n+3)}{6} \\ &= \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}. \end{aligned}$$

By mathematical induction we conclude that the assertion holds for all positive integers. \square

Induction proofs must contain certain steps. Look at the proof above and see if you can find each of the steps described below.

(1) You should indicate clearly what you are trying to prove. (2) There is always the base step, in which we check the first assertion. (This need not always begin with $n = 1$; it can begin with $n = 3$, $n = 0$, or even at a negative integer! In fact, as long as what you say is true, it can begin at any integer you want it to begin at.) (3) Then we have the induction step, in which we show that for each $n \in \mathbb{Z}$ that is at least as big as the integer used in the base step, if $P(n)$ is true, then $P(n+1)$ is true.

Of course, you still need to write using complete sentences, and you still need to introduce every variable to the reader when the reader meets it (not after the reader

has met it for the first time!). Finally, do tell the reader what the base step is (“First we show the assertion holds for $n = 1$ ”), what the induction step is (“We suppose that $P(n)$ holds for an $n \in \mathbb{Z}^+$; that is ... holds”), and what you will prove (“We will show that $P(n+1)$ holds; that is ... holds”). This is as much for your benefit as it is for the reader’s. This step shows you where you will begin and where you will have to end. Then show what you said you will show and indicate clearly where you use the induction hypothesis. End your proof with a concluding sentence.

Many statements proved by induction involve sums or products. We remind you of the standard notation for this. In the following, $k \in \mathbb{Z}$ and $a_k \in \mathbb{R}$. The notation for sum is

$$a_1 + a_2 + a_3 + \cdots + a_n = \sum_{k=1}^n a_k,$$

and the notation for product is

$$a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n = \prod_{k=1}^n a_k.$$

This notation often saves space and makes a statement look neater. For instance, the result we proved in Example 18.2 is

$$\text{For } n \in \mathbb{Z}^+, \text{ we have } \sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}.$$

If you are ever unsure about what such a statement says, you will almost certainly find it helpful to rewrite the expression the long way.

Exercise 18.3. Let x_1, x_2, \dots, x_n be real numbers. Prove that for $n \in \mathbb{Z}^+$, both of the following hold:

- (a) $|\prod_{k=1}^n x_k| = \prod_{k=1}^n |x_k|$ and
- (b) $|\sum_{k=1}^n x_k| \leq \sum_{k=1}^n |x_k|.$

○

The following exercise illustrates how induction can go awry. It’s cute, but not very mathematical. A similar example, but a more mathematical one, appears in the problems. See if you can spot the error in that one.

Exercise 18.4. All people at Bucknell University have the same color hair.

Not a proof. Let $P(n)$ be the assertion that every group of n people has the same color hair (as each other). Then $P(1)$ is the statement that one person has the same color hair as herself. This is certainly true. So let $n \in \mathbb{Z}^+$ and suppose that $P(n)$ is true; that is, when we have n people, they all have the same color hair. We need to show that this implies that $n+1$ people in a group have the same color hair. So consider a group of $n+1$ people. If we look at the first n of them (people 1 through n in the group), by the induction hypothesis they all have the same color hair, which we may as well assume is black for right now. So the first n people all have black

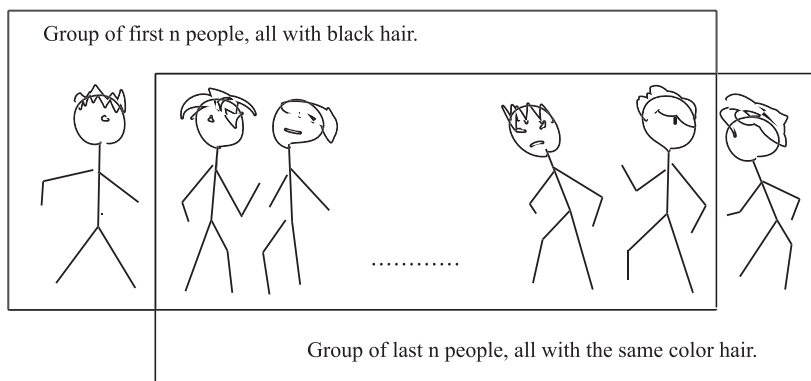


Fig. 18.1 They must all have black hair

hair. Now consider the last n people in this group (people 2 through $n + 1$ in the group). Again, by our induction hypothesis, they all have the same color hair. Those who are in both groups are also in the first group, and therefore have black hair. (See [Figure 18.1](#).) Thus, since all people in the second group have the same color hair, everyone has black hair. By mathematical induction we conclude that all people at Bucknell have the same color hair. \square

There must be an error! Exactly where is it? ○

Exercise 18.5. Use induction to prove that for all natural numbers n , the expression $4^n - 1$ is a multiple of 3.

“Understanding the problem.” Well, once again, it’s probably a good idea to make sure that we know what everything means here. We need to show that $4^n - 1$ is a multiple of 3 for every natural number n . That means we need to show that there exists an integer k such that $4^n - 1 = 3k$.

“Devising a plan.” The outline is presented to you below and the complete solution appears at the end of the chapter.

1. Say clearly what the assertion $P(n)$ is. (Most mathematicians write this out without labeling the assertion with $P(n)$ explicitly.)
2. Check the base step ($n = 0$).
3. Write out the induction step in the principle of mathematical induction clearly. Make sure you replace $P(n)$ by what it says, and replace $P(n + 1)$ by what it says. This will help you figure out what you are supposing (you are supposing $P(n)$) and what you need to end with (you need to end with $P(n + 1)$).
4. Write out the induction hypothesis; that is, write out what you are assuming to be true.
5. Having done all of the above, look at $4^{n+1} - 1$ and show that it is divisible by 3. Indicate clearly where you use the induction hypothesis.
6. State your conclusion clearly. ○

Induction can also be used to define functions. Perhaps the best known example of this technique is the definition of factorial: For $n \in \mathbb{N}$, we define n **factorial**, written as $n!$, as follows:

$$\begin{aligned} 0! &= 1 \\ (n+1)! &= (n+1) \cdot n! \text{ for } n \geq 0. \end{aligned}$$

What have we done? We defined a function $g: \mathbb{N} \rightarrow \mathbb{N}$, denoted $g(n) = n!$, by telling you that $g(0) = 1$, $g(1) = 1 \cdot g(0) = 1$, $g(2) = 2 \cdot g(1) = 2$, $g(3) = 3 \cdot g(2) = 6$, etc.

You might be thinking, “They say they’ve defined a function. Is it really well-defined?” If this is what you are, in fact, thinking, that’s great. To prove that g is a function, we’ll actually need a theorem. This theorem is often called the recursion theorem.

Theorem 18.6 (Recursion theorem). *Let X be a nonempty set, $f: X \rightarrow X$ a function, and $a \in X$. Then there is a unique function $g: \mathbb{N} \rightarrow X$ such that $g(0) = a$ and $g(n+1) = f(g(n))$ for all $n \in \mathbb{N}$.*

We usually begin by understanding the problem. In this case, understanding the theorem might also require some effort. What does it say? To define g , we say how to get started (that’s what we are doing when we tell you $g(0) = a$). But that’s only how you get started. To proceed from your starting point, we tell you how to compute $g(n+1)$. You have a rule (that’s f) and the previous values of g (that’s where $g(n)$ comes into play) and you compose them (that’s $g(n+1) = f(g(n))$). And what we are saying is that this g that you get is a well-defined function.

“*Understanding the problem*” There are two parts to this proof. We will need to show that a function g exists and that at most one function g exists. If we can figure out how to show the function exists, we will try to show that uniqueness follows the way it often does. So, how can you show that something you don’t have exists? Any function we define has to be a relation satisfying the conditions stated. But, on top of the conditions, we also want to obtain uniqueness. We will fall back on the definition of function as a relation and we’ll try to find the smallest relation that does what we need. Being the smallest should make it unique, if we are lucky. Whatever object we end up constructing will also need to satisfy conditions (i) and (ii) of the definition of function. It might, at this point, be advisable to review our original function definition, Definition 14.1.

“*Devising a plan.*” For the existence, we’ve decided that the smallest relation has a chance at satisfying the conditions. So we want a “small set” that “does certain things.” Getting a small set suggests intersecting things that do what we want. So we will look at all relations from \mathbb{N} to X ; that is, all subsets A of $\mathbb{N} \times X$, with the property that $(0, a) \in A$ and whenever $(n, x) \in A$, then $(n+1, f(x)) \in A$. If we can show that there is at least one such relation, then we’ll take the intersection of all of them and show that this is our function g .

To show uniqueness we will suppose that there is a second function h satisfying our needs and we will try to contradict something, most likely the minimal nature of g . Let us see whether we can turn this plan into a successful proof.

As you read this proof, you'll notice that the set \mathcal{C} that we define comes up a lot. So you should write down, in some very handy place, what you have to do to get into the set \mathcal{C} .

Proof. We will first show that there exists a function $g : \mathbb{N} \rightarrow X$ satisfying the stated conditions. We let \mathcal{C} be the set of all subsets A of $\mathbb{N} \times X$ with the condition that $(0, a) \in A$ and whenever $(n, x) \in A$, then $(n + 1, f(x)) \in A$. Since $\mathbb{N} \times X \in \mathcal{C}$ we see that $\mathcal{C} \neq \emptyset$. Consequently, we can form the intersection of all elements of \mathcal{C} , which we call g . So $g = \bigcap_{A \in \mathcal{C}} A$. Obviously $g \subseteq \mathbb{N} \times X$. Since $(0, a) \in A$ for all $A \in \mathcal{C}$ we also have $(0, a) \in g$. If $(n, x) \in g$, then $(n, x) \in A$ for all $A \in \mathcal{C}$. This implies that $(n + 1, f(x)) \in A$ for all $A \in \mathcal{C}$. Hence $(n + 1, f(x)) \in g$. This shows that $g \in \mathcal{C}$ and g is a relation from \mathbb{N} to X . We claim that, in fact, $g : \mathbb{N} \rightarrow X$ is a function. Since the domain and codomain are specified, we need only show that the two conditions of the function definition hold.

For condition (i) of the function definition we need to show that for each $n \in \mathbb{N}$ there exists $x \in X$ such that $(n, x) \in g$. We will prove this by induction on n . First the base step: Because $g \in \mathcal{C}$, we know that $(0, a) \in g$ where $a \in X$.

For the induction step, let $n \in \mathbb{N}$ and suppose that $(n, x) \in g$. Since $x \in X$, we know that $f(x) \in X$. Thus, since $g \in \mathcal{C}$ we conclude that $(n + 1, f(x)) \in g$. So for $n + 1$, the element $f(x)$ is the element of X that we were looking for; that is, by induction, we know that for each $n \in \mathbb{N}$ there exists $x \in X$ such that $(n, x) \in g$ and we conclude that condition (i) of the function definition holds.

For condition (ii), we need to show that for each $n \in \mathbb{N}$ if (n, x) and (n, y) are elements of g , then $x = y$. We will show this, again, by induction on n . For the base step, we have $(0, a) \in g$. Suppose that $(0, y) \in g$ with $y \neq a$. Define $h_1 = g \setminus \{(0, y)\}$. Then $h_1 \subset g$. Clearly, $(0, a) \in h_1$ since we haven't removed it from g . If for some $n \in \mathbb{N}$ we have $(n, x) \in h_1$, then the fact that $h_1 \subset g$ implies that $(n, x) \in g$. Therefore, $(n + 1, f(x)) \in g$. Since $(n + 1, f(x)) \neq (0, y)$ we conclude that $(n + 1, f(x)) \in h_1$. Thus $h_1 \in \mathcal{C}$ and $h_1 \subset g$. This contradicts the construction of g and ensures that $y = a$. Thus we have handled the base case of the induction.

We now show the induction step. So, let $n \in \mathbb{N}$ and suppose that whenever (n, x) and (n, y) are elements of g , then $x = y$. We must show that whenever $(n + 1, u)$ and $(n + 1, v)$ are elements of g , then $u = v$.

By condition (i) above there exists $z \in X$ with $(n, z) \in g$ and, since $g \in \mathcal{C}$, we know that $(n + 1, f(z)) \in g$. Suppose that there exists $w \in X$ with $f(z) \neq w$ and $(n + 1, w) \in g$. As before, we define $h_2 = g \setminus \{(n + 1, w)\}$ and we claim that $h_2 \in \mathcal{C}$. To this end, note that $(0, a) \neq (n + 1, w)$ and $(0, a) \in g$. Hence $(0, a) \in h_2$, so the first condition for admittance to \mathcal{C} is satisfied. Furthermore, if $m \in \mathbb{N}$ and $(m, x) \in h_2$, we claim $(m + 1, f(x)) \in h_2$.

To this end, note that $(m, x) \in h_2$ implies that $(m, x) \in g$. Because $g \in \mathcal{C}$ we have $(m + 1, f(x)) \in g$. If $m \neq n$, then $(m + 1, f(x)) \neq (n + 1, w)$ and $(m + 1, f(x)) \in h_2$. If $m = n$, then we have $(m, x) = (n, x) \in g$ and we chose z so that $(n, z) \in g$. Thus, by our induction hypothesis, $x = z$. Since $f(x) = f(z) \neq w$, we conclude that $(m + 1, f(x)) \neq (n + 1, w)$. This shows that $(m + 1, f(x)) \in h_2$ and completes the proof that $h_2 \in \mathcal{C}$. So, we have constructed an element, h_2 , of \mathcal{C} that is strictly contained in g . This contradicts the minimality of g and shows that $w = f(z)$.

By induction, condition (ii) of the function definition also holds. Thus the intersection g is a well-defined function $g : \mathbb{N} \rightarrow X$.

To show the uniqueness of $g : \mathbb{N} \rightarrow X$ satisfying $g(0) = a$ and $g(n+1) = f(g(n))$ for all $n \in \mathbb{N}$, we suppose to the contrary that there is a different function $k : \mathbb{N} \rightarrow X$ that also satisfies $k(0) = a$ and $k(n+1) = f(k(n))$ for all $n \in \mathbb{N}$. We define the set $S = \{x \in \mathbb{N} : g(x) \neq k(x)\}$. Now we suppose that k and g are different functions, so $S \neq \emptyset$. By the well-ordering principle of \mathbb{N} this set has a minimum, which we call $m = \min S$. So $g(m) \neq k(m)$. Since $g(0) = a = k(0)$ we know that $m > 0$. Therefore $m-1 \in \mathbb{N}$ and $m-1 \notin S$. Hence $g(m-1) = k(m-1)$. This implies that $g(m) = f(g(m-1)) = f(k(m-1)) = k(m)$. This is a contradiction and shows that our supposition is wrong. We conclude that $g = k$ and our function is unique. \square

We now have a way of defining a function on the natural numbers: 1) We give the value of the function at the initial point (this may be at $n = 0, n = 1$, or it may be any other natural number) and 2) we give a rule about how to find the value of a natural number in terms of the function value of the previous number. A function defined in this manner is said to be defined recursively or defined by induction.

Exercise 18.7. We define $g : \mathbb{N} \rightarrow \mathbb{N}$ recursively by

$$g(0) = 1 \text{ and } g(n+1) = 5g(n).$$

- (a) Find $g(1)$ and $g(8)$.
- (b) For this example describe the value a , the set X , and the function f in the recursion theorem. Why is the recursion theorem needed here? \circ

We return to our motivating example, the factorial function. It's a function you've known for years, most likely, and yet it is more complicated than it appears—more complicated than most of the other examples in this section. For example, the recursion theorem uses $g(n+1) = f(g(n))$. But we need $g(n+1) = (n+1)g(n)$ and it's difficult to imagine how to express this as $g(f(n))$. It feels more like a rule combining two functions, $(n+1)$ and $g(n)$. We exploit this observation below.

Example 18.8. We defined the factorial function above. Explain how the recursion theorem can be used to show that this definition describes a unique function.

For this example, let $a = (0, 1)$, $X = \mathbb{N} \times \mathbb{N}$, and let $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ be defined by $f(x, y) = (x+1, (x+1)y)$. The recursion theorem tells us that there is a unique function $g : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ with $g(0) = (0, 1)$ and $g(n+1) = f(g(n))$.¹ Well, we aren't interested in the first coordinate; only the second one (why?). So we compose g with the well-defined function $\pi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ where $\pi(x, y) = y$. If each function is well-defined and unique, then their composition $\pi \circ g : \mathbb{N} \rightarrow \mathbb{N}$ is too. Before going

¹ At this point, you probably know that you should write out $g(0), g(1), g(2)$, etc., until you understand what's happening.

on, check that the first coordinate of $g(n)$ is n , and note that the second coordinate of $g(n)$ is $\pi(g(n))$. Now we get

$$\begin{aligned}
 (\pi \circ g)(0) &= \pi(0, 1) = 1 \text{ and} \\
 (\pi \circ g)(n+1) &= \pi(f(g(n))) = \pi(n+1, (n+1)\pi(g(n))) = (n+1)(\pi \circ g)(n).
 \end{aligned}$$

If we write $(\pi \circ g)(n) = n!$, then we have the familiar definition. ○

Definitions

Definition 18.1. For $n \in \mathbb{N}$, we define n **factorial**, written as $n!$, as follows:

$$\begin{aligned}
 0! &= 1 \\
 (n+1)! &= (n+1) \cdot n! \text{ for } n \geq 0.
 \end{aligned}$$

Definition 18.2 (for Problem 18.22). A subset S of \mathbb{R}^2 is **convex** if for every two points $x, y \in S$, the line segment joining x and y again lies in S .

Definition 18.3 (for Problem 18.24). A **triangular number**, T_n , is the number of equally spaced points that can be used to form an equilateral triangle with sides built of n equally spaced points (see [Figure 18.2](#)).

Definition 18.4 (for Problem 18.25). For $k, n \in \mathbb{N}$ with $k \leq n$ we define the **binomial coefficient** as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Solutions to Exercises

Solution (18.3).

Proof. [Proof of (a)] The base step $n = 1$ is trivial.

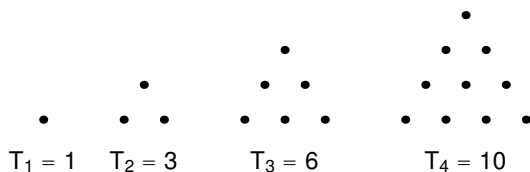


Fig. 18.2 Triangular numbers

For the induction step, let $n \in \mathbb{Z}^+$ and suppose that $|\prod_{k=1}^n x_k| = \prod_{k=1}^n |x_k|$. Then

$$\begin{aligned} \left| \prod_{k=1}^{n+1} x_k \right| &= \left| \left(\prod_{k=1}^n x_k \right) x_{n+1} \right| \\ &= \left| \prod_{k=1}^n x_k \right| |x_{n+1}| \quad (\text{by Theorem 5.3}) \\ &= \left(\prod_{k=1}^n |x_k| \right) |x_{n+1}| \quad (\text{by induction hypothesis}) \\ &= \prod_{k=1}^{n+1} |x_k|. \end{aligned}$$

The result follows from the principle of mathematical induction. □

Proof. [Proof of (b)] We will use the triangle inequality (Theorem 5.8), which has been proven (by you) in Problem 5.14. Our proof will be by induction on n . For $n \in \mathbb{Z}^+$, let $P(n)$ denote the assertion that $|\sum_{k=1}^n x_k| \leq \sum_{k=1}^n |x_k|$.

The validity of the base step, $n = 1$, is clear.

Now let n be a positive integer and suppose that $P(n)$ holds; that is, we let $n \in \mathbb{Z}^+$ and suppose that $|\sum_{k=1}^n x_k| \leq \sum_{k=1}^n |x_k|$. We must show that $P(n+1)$ holds; in other words, we must show that $|\sum_{k=1}^{n+1} x_k| \leq \sum_{k=1}^{n+1} |x_k|$. But

$$\begin{aligned} \left| \sum_{k=1}^{n+1} x_k \right| &= |(x_1 + \cdots + x_n) + x_{n+1}| \\ &\leq |x_1 + \cdots + x_n| + |x_{n+1}| \quad (\text{by the triangle inequality}) \\ &= \left| \sum_{k=1}^n x_k \right| + |x_{n+1}| \\ &\leq \sum_{k=1}^n |x_k| + |x_{n+1}| \quad (\text{by the induction hypothesis}) \\ &= \sum_{k=1}^{n+1} |x_k|, \end{aligned}$$

and the result now follows from the principle of mathematical induction. □

Solution (18.4). If the base step is for $n = 1$, then the induction step, $P(n)$ implies $P(n+1)$, needs to be valid for all $n \geq 1$. We made the following argument: “Those who are in both groups are also in the first group and therefore they have black hair.” This argument is not valid if $n = 1$. In that case, the group of the first n people is disjoint from the group of the last n people. However, our argument requires that some person be in both groups. Hence the reasoning falls apart right where it should: If a second person joins a black-haired person, there is no guarantee that he or she will also have black hair.

Solution (18.5).

Proof. For $n \in \mathbb{N}$, let $P(n)$ denote the assertion that $4^n - 1$ is a multiple of 3; that is, there is $k \in \mathbb{Z}$ such that $4^n - 1 = 3k$. We will prove this by induction on n .

We check the *base step*. For $n = 0$ the statement becomes $4^0 - 1 = 0$ is divisible by 3. This is obviously true.

Now we check the *induction step*. Let $n \in \mathbb{N}$ and suppose that there exists $k \in \mathbb{Z}$ such that $4^n - 1 = 3k$. We need to show that there exists $l \in \mathbb{Z}$ such that $4^{n+1} - 1 = 3l$. Consider the following calculation:

$$4^{n+1} - 1 = 4 \cdot 4^n - 1 = 3 \cdot 4^n + (4^n - 1) = 3 \cdot 4^n + 3k = 3(4^n + k),$$

where the second-to-last equality is justified by the induction hypothesis. Now set $l = 4^n + k$. Then $l \in \mathbb{Z}$ and $4^{n+1} - 1 = 3l$. Hence the induction step is established.

By the principle of mathematical induction, $4^n - 1$ is divisible by 3 for all $n \in \mathbb{N}$. \square

Solution (18.7).

(a) $g(1) = 5g(0) = 5 \cdot 1 = 5$.

$$g(8) = 5g(7) = 5^2g(6) = 5^3g(5) = 5^4g(4) = 5^5g(3) = 5^6g(2) = 5^7g(1) = 5^8.$$

(b) In the theorem, we set $a = 1$, $X = \mathbb{N}$, and $f : \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x) = 5x$. We can now verify that $g(0) = 1$ and $g(n+1) = f(g(n)) = 5g(n)$. The theorem tells us that the function g is well-defined and unique. Without this theorem, we wouldn't be able to conclude that this is true!

Problems

Problem 18.1. Prove that $1 + 2 + \cdots + n = n(n+1)/2$ for every positive integer n , using the principle of mathematical induction.

Problem 18.2. Prove that $1 + 3 + 5 + \cdots + (2n-1) = n^2$ for every positive integer n , using the principle of mathematical induction.

Problem 18.3. Prove that $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$ for every positive integer n , using the principle of mathematical induction.

Problem 18.4. Prove that if $n \in \mathbb{Z}^+$ and r is a real number such that $r \neq 1$, then

$$\sum_{k=0}^{n-1} r^k = \frac{1 - r^n}{1 - r}.$$

Problem 18.5. Show that $2^n \leq n!$ for all integers with $n \geq 5$.

Problem 18.6. Use induction to prove Bernoulli's inequality: For $x \in \mathbb{R}$, if $1 + x > 0$, then $(1 + x)^n \geq 1 + nx$ for all $n \in \mathbb{N}$.

Problem 18.7. Show that for every positive integer n ,

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n} \geq 1 + \frac{n}{2}.$$

(This can be used to show that the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \cdots$ diverges.)

Problem 18.8. Show that $2^n > n^2$ for all integers n with $n \geq 5$.

Problem 18.9. Prove that 8 divides $5^{2n} - 1$ for all $n \in \mathbb{N}$.

Problem 18.10. Suppose that $g : \mathbb{N} \rightarrow \mathbb{N}$ satisfies $g(n+1) = g(n) + g(1)$ for all $n \in \mathbb{N}$.

- Find $g(0)$.
- Show that $g(n+m) = g(n) + g(m)$ for all $n, m \in \mathbb{N}$.

Problem 18.11. Let $g : \mathbb{N} \rightarrow \mathbb{R}^+$ and let a be a positive real number. Suppose that g has the properties that $g(1) = a$ and $g(m+n) = g(m)g(n)$ for all natural numbers n and m .

- Find $g(0)$. Justify your answer.
- Define g recursively.
- Prove that $g(n) = a^n$ for all $n \in \mathbb{N}$.

Problem 18.12. Let a_1, a_2, \dots, a_n be real numbers that satisfy $|a_j| \leq 1$ for all $j = 1, 2, \dots, n$. Prove that for all $n \in \mathbb{Z}^+$ the following holds:

$$\left| \left(\prod_{j=1}^n a_j \right) - 1 \right| \leq \sum_{j=1}^n |a_j - 1|.$$

Problem 18.13. Show that for all positive integers n ,

$$2(\sqrt{n+1} - 1) < 1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n}.$$

Problem 18.14. Show that for all integers $n \geq 2$,

$$\prod_{k=2}^n \left(1 - \frac{1}{\sqrt{k}} \right) < \frac{2}{n^2}.$$

Problem 18.15. Find the error in the *Not a proof* below. (See Problem 10.13 for the definition of the degree of a polynomial.)

Nontheorem. Let p be a polynomial of positive degree n such that p is a product of degree-one polynomials and $p(0) = 0$. If $c \in \mathbb{R}$ satisfies $p(c) = 0$, then $c = 0$.

In other words, our claim is that if $p(x) = ax(a_1x + b_1) \cdots (a_{n-1}x + b_{n-1})$, where $a, a_1, \dots, a_{n-1}, b_1, \dots, b_{n-1} \in \mathbb{R}$ and $a, a_1, \dots, a_{n-1} \neq 0$, then the only root of p is 0.

Not a proof. We will prove this statement by induction on the degree n of the polynomial p .

For the base step, we let $n = 1$. Since $p(0) = 0$, we can write $p(x) = ax$ for some $a \in \mathbb{R}$ and $a \neq 0$. If $p(c) = 0$, then $p(c) = ac = 0$. Since $a \neq 0$, we conclude that $c = 0$.

For the induction step, let $n \in \mathbb{Z}^+$ and suppose that if p is a polynomial of degree n that is a product of degree-one polynomials and satisfies $p(0) = 0$, then $p(c) = 0$ implies that $c = 0$. Let p be a polynomial of degree $n + 1$ that factors into $n + 1$ degree-one polynomials and satisfies $p(0) = 0$. We need to show that $p(c) = 0$ implies that $c = 0$. Write $p(x) = ax(a_1x + b_1) \cdots (a_nx + b_n)$, where a, a_1, \dots, a_n are nonzero real numbers and $b_1, \dots, b_n \in \mathbb{R}$. Suppose that $p(c) = 0$. Then

$$0 = p(c) = ac(a_1c + b_1) \cdots (a_nc + b_n).$$

One of the factors, $ac, a_1c + b_1, \dots, a_nc + b_n$, must vanish. Rearranging terms if necessary, we may assume that the factor ac or the factor $a_1c + b_1$ vanishes. Now,

$$q(x) = ax(a_1x + b_1) \cdots (a_{n-1}x + b_{n-1})$$

is a polynomial of degree n that is a product of degree-one polynomials and satisfies $q(0) = 0$. Since $ac(a_1c + b_1) = 0$, we have $q(c) = 0$. Since our induction hypothesis applies to q , we conclude that $c = 0$. Therefore, $p(c) = 0$ implies that $c = 0$, and the nontheorem follows from mathematical induction. \square

Problem 18.16. We define the function $g : \mathbb{N} \rightarrow \mathbb{R}^+$ recursively by $g(0) = 1$ and $g(n + 1) = \frac{g(n)^2 + 5}{g(n)}$ for $n \in \mathbb{N}$.

- Calculate $g(3)$.
- Find the value of a , the set X , and the function f used in the recursion theorem to justify the recursive definition of this particular function g .

Problem 18.17. Let $X = \{(x, y) \in \mathbb{R}^2 : x \geq 0, y \geq 0, \text{ and } x + y \leq 1\}$. We define the function $g : \mathbb{N} \rightarrow \mathcal{P}(X)$ recursively as follows:

$$g(0) = X \text{ and for } n \in \mathbb{N},$$

$$\begin{aligned} g(n + 1) = & \\ & \{(x/2, y/2) : (x, y) \in g(n)\} \cup \{(x + 1)/2, y/2) : (x, y) \in g(n)\} \\ & \cup \{(x/2, (y + 1)/2) : (x, y) \in g(n)\}. \end{aligned}$$

Sketch $g(0), g(1), g(2)$, and $g(3)$. What kind of object is this function building?

Problem 18.18. Let $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ be defined by $f(x, y) = (x + 1, y^2/x)$ and choose $(1, 5) \in \mathbb{N} \times \mathbb{N}$. According to the recursion theorem, there is a unique function $g : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ such that $g(0) = (1, 5)$ and $g(n + 1) = f(g(n))$ for $n \in \mathbb{N}$. Let $\pi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ be defined by $\pi(x, y) = y$ and let $h = \pi \circ g : \mathbb{N} \rightarrow \mathbb{N}$.

- Calculate $h(2)$.

- (b) Define h recursively by giving $h(0)$ and $h(n+1)$ in terms of $h(n)$ and n .

Problem 18.19. Write recursive functions for the following, identifying the point a , the set X , and the functions f and g in the recursion theorem. Prove that your answers are correct.

- (a) Given a real number $r > 0$, write a recursive function that computes r^n to every $n \in \mathbb{N}$;
 (b) Write a recursive function that computes the sum of the first n positive integers.

There is an equivalent form of the principle of mathematical induction, namely:

Theorem 18.9 (Second principle of mathematical induction). For an integer n , let $Q(n)$ denote an assertion. Suppose that

- (i) $Q(1)$ is true and
 (ii) for all positive integers n , if $Q(1), \dots, Q(n)$ are true, then $Q(n+1)$ is true.

Then $Q(n)$ holds for all positive integers n .

Problem 18.20. Prove that the first principle of mathematical induction (Theorem 18.1) implies the second one (Theorem 18.9). To do so, let $P(n)$ be the assertion “ $Q(1), \dots, Q(n)$ are true.”

Problem 18.21. Prove that every integer n , where $n \geq 2$, is a prime or the product of prime numbers. (We have used this before; this shows that every integer $n \geq 2$ can be factored as a product of primes. If you also prove the uniqueness of this factorization, you will have proved the fundamental theorem of arithmetic.)

Problem 18.22. A subset S of \mathbb{R}^2 is **convex** if for every two points $x, y \in S$, the line segment joining x and y again lies in S . Recall that an interior angle at a vertex of a convex polygon is the smaller of the two angles formed by the edges at that vertex.

Prove that for an integer n , where $n \geq 3$, the sum of all the interior angles of a convex polygon with n vertices is $(n-2)180$ degrees. (See [Figure 18.3](#).)

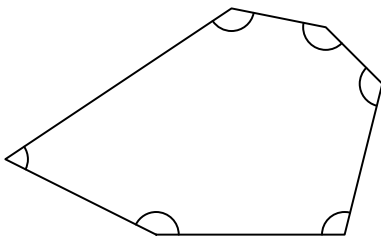


Fig. 18.3 The sum of all the interior angles in this convex polygon is $4 \cdot 180^\circ$

Problem 18.23. Let p_n be a polynomial with real coefficients and of positive degree n . (See Problem 10.13 for the definitions.)

- Suppose $p_n(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. For a real number a , what is the largest the degree of q_n , defined by $q_n(x) = p_n(x) - (x-a)a_n x^{n-1}$, can be?
- Let $a \in \mathbb{R}$ and $n \in \mathbb{Z}^+$. Prove that $p_n(a) = 0$ if and only if $(x-a)$ is a factor of $p_n(x)$.

Problem 18.24. A **triangular number**, T_n , is the number of equally spaced points that can be used to form an equilateral triangle with sides built of n equally spaced points (see [Figure 18.2](#) on page 201).

- Find a formula for the n^{th} triangular number, and prove that your formula is correct.
- Can you think of a (familiar) game that uses T_4 ? T_5 ?

For $k, n \in \mathbb{N}$ with $k \leq n$ we define the **binomial coefficient** as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Because the binomial coefficient is the number of ways that we can choose k different elements from a set of n elements, we read $\binom{n}{k}$ as “ n choose k .”

Theorem 18.10 (Binomial theorem). Let $a, b \in \mathbb{R} \setminus \{0\}$ and $n \in \mathbb{Z}^+$. Then

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

Problem 18.25. This problem refers to the notation and theorem above.

- Compute each of the following:

$$5!, \quad \binom{8}{3}, \quad \binom{8}{5}, \quad \binom{5}{2}, \quad \binom{5}{3}, \quad \binom{7}{0}, \quad \text{and} \quad \binom{7}{7}.$$

- Consider the special case of Theorem 18.10 in which $(m+1)^2 = m^2 + 2m + 1$, where $m \in \mathbb{N}$. A “picture proof” is presented in [Figure 18.4](#). Explain the picture proof.
- Prove that for all $k, n \in \mathbb{N}$ with $1 \leq k \leq n$, we get

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

(If you write out what it means, life will be a lot easier.)

- Use part (c) to prove Theorem 18.10. (See Project 29.8, on Pascal’s triangle.)

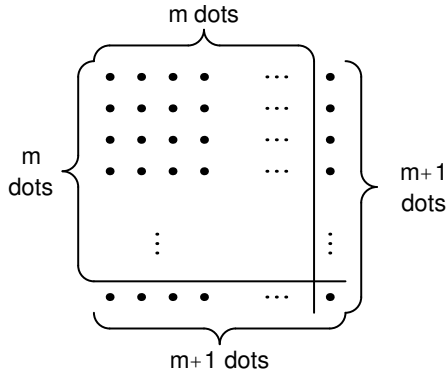


Fig. 18.4 “Proof” of $(m+1)^2 = m^2 + 2m + 1$

(e) Prove that

$$\sum_{k=0}^n \binom{n}{k} (-1)^k = 0 \text{ for all } n \in \mathbb{Z}^+.$$

Problem 18.26. Deduce the well-ordering principle of \mathbb{N} , stated in Chapter 12, from Theorem 18.9 stated on page 206.

Recall that we used the well-ordering principle of \mathbb{N} to prove Theorem 18.1 and that Theorem 18.1 implies Theorem 18.9 (as shown in Problem 18.20). So this problem shows that the principle of mathematical induction, the second principle of mathematical induction, and the well-ordering principle of \mathbb{N} are all equivalent.

Chapter 19

Sequences

We have all seen lists of numbers. For example, we've all worked with a list of positive even integers presented in increasing order, $(2, 4, 6, 8, \dots, 2n, \dots)$, where $n = 1, 2, 3, 4, \dots$. The positive odd numbers $(1, 3, 5, 7, \dots, 2n - 1, \dots)$ can also be presented in such a list, where $n = 1, 2, 3, 4, \dots$. What we are interested in here is a precise definition of "infinite list."

Here's an example from your childhood of a problem that yields such a list. Let n be a positive integer with $n \geq 2$. Suppose that we have n children arranged in a circle, and that rather than use their names, we number them $\{1, 2, \dots, n\}$. Say these children want to see who goes first in a game. They begin by eliminating the second child, and then proceed around the circle, eliminating every other child until there is only one child left. That happy child goes first. The question is, where should you stand in order to be the winning child? Let's start small: if there are two children, you should stand in the first spot. If there are three, you should stand in the third spot. If there are four, you should stand in the first spot. Where should you stand if there are n children? (This challenging problem is known as the Josephus problem. The answer appears at the end of the chapter. Of course, the children can count off by three or four, giving us a new problem to solve.) In this problem, for each group of n children, we have an answer. Thus we again have a list of numbers. We now turn to the definition of "list."

A **sequence** is a function f from the natural numbers \mathbb{N} to a set X . In this chapter, we will concentrate on the case $X = \mathbb{R}$. It is standard to write $x_n = f(n)$, and to refer to x_n as a **term** in the sequence. The sequence will be denoted $(x_n)_{n=0}^{\infty}$, or just (x_n) when it is clear which n we are referring to or when it doesn't matter where the sequence starts. We can begin a sequence at an integer other than $n = 0$ when convenient, and we will often begin the sequence at $n = 1$ without much fanfare. We'll tell you where we are starting when it really matters.

Since sequences are functions, we can graph them as functions defined on the nonnegative (or positive) integers and then we can see what they are doing.

Example 19.1. The sequence (x_n) is defined by $x_n = 1 + 1/n$ for $n \in \mathbb{Z}^+$. We will write out the first few terms and graph the beginning of the sequence in [Figure 19.1](#).

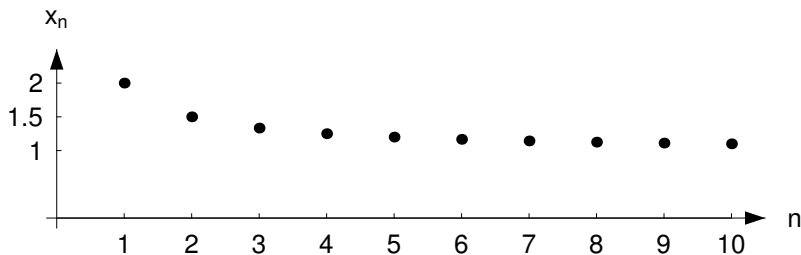


Fig. 19.1 Graph of (x_n) , where $x_n = 1 + 1/n$ for $n \geq 1$

The first four terms are

$$x_1 = 2, \quad x_2 = \frac{3}{2}, \quad x_3 = \frac{4}{3}, \quad x_4 = \frac{5}{4}.$$

Exercise 19.2. For each of the sequences given below, write out the first four terms and graph the beginning of the sequence.

- (a) Let $x_n = 1 - (-1)^n$, for $n = 0, 1, 2, \dots$
- (b) Let $x_n = n/(n+1)$, for $n = 0, 1, 2, \dots$
- (c) Let $x_n = (n^2 + 1)/(1 - n)$, for $n = 2, 3, \dots$

○

When we look at sequences, we notice that different sequences behave in different ways. This is illustrated by our examples in Exercise 19.2. Some sequences approach some horizontal line as $n \rightarrow \infty$. Some seem to be shooting off to infinity, others jump around a lot. We need to understand how these sequences differ from each other, and the following definitions will help us do that.

You'll notice that a lot of terms that we introduced when we studied sets reappear here. What is really happening is that each sequence (x_n) (where order counts) gives rise to a nonempty set $S = \{x_n : n \in \mathbb{N}\}$ (where order doesn't count). For example, the sequence (z_n) where $z_n = (-1)^n$ gives rise to the set $S = \{-1, 1\}$, while the sequence $(y_n)_{n=1}^{\infty}$ where $y_n = n$ gives rise to the set $T = \{n : n \in \mathbb{Z}^+\} = \mathbb{Z}^+$. The set S that is associated with the sequence (x_n) is precisely the range of the sequence. Furthermore, once we understand this connection, we can ask the same questions about sequences that we have asked about sets: For example, we can ask when a sequence is bounded above, bounded below, bounded, has an infimum or supremum—and we can use everything we learned about sets to find an answer.

How important are sequences? Very important. In fact, we believe that these are so important to your future mathematical development that we will restate all the definitions in the specific setting of sequences. For example, a sequence of real numbers (x_n) is bounded if the set $S = \{x_n : n \in \mathbb{N}\}$ is bounded. Thus, according to our definition of bounded set, a sequence of real numbers (x_n) is **bounded above**, if there is a real number M such that $x_n \leq M$ for all n , and **bounded below**, if there

exists a real number m such that $x_n \geq m$ for all n . A sequence is **bounded** if it is bounded above and below. That's how we defined it. But you may find that the following provides a more useful way to think about boundedness in \mathbb{R} .

Exercise 19.3. Let (x_n) be a sequence. Prove that (x_n) is bounded if and only if there exists a real number N such that $|x_n| \leq N$ for all n . \circ

Just as before, a real number U satisfying $x_n \leq U$ for all n is called an **upper bound** of the sequence (x_n) , and a real number L satisfying $L \leq x_n$ for all n is a **lower bound** of the sequence (x_n) . In our illustration above, we considered the sequence (z_n) , where $z_n = (-1)^n$. We see that this sequence is bounded above (1 is an upper bound) and bounded below (-1 is a lower bound), and therefore it is bounded. Alternatively, $|z_n| \leq 1$ for all n , and by the previous exercise we may conclude that the sequence (z_n) is bounded.

Exercise 19.4. (a) Give an example of a real number that is not an upper bound of the sequence given by $x_n = n/(n+1)$.
 (b) Complete the following sentence: The real number U is not an upper bound of the sequence (x_n) , if ... \circ

If (x_n) is a sequence that is bounded below, the set $S = \{x_n : n \in \mathbb{N}\}$ is bounded below. Since S is a nonempty set of real numbers that is bounded below, the infimum version of the completeness axiom (see Exercise 12.9) implies that S has an infimum, and we call this the **infimum** of the sequence (x_n) (or **greatest lower bound** of (x_n)). We denote it by $\inf(x_n)$. Recall that you showed (Problem 12.17) that the infimum is unique. The definition of the infimum of a sequence, without reference to the set associated with the sequence, is given in the example below.

Example 19.5. Let (x_n) be a sequence that is bounded below. State the two properties that the infimum of (x_n) must satisfy.

The infimum of the sequence (x_n) is the real number m satisfying

- (i) $m \leq x_n$ for all n , and
- (ii) if p is a real number satisfying $p \leq x_n$ for all n , then $p \leq m$.

Each of the statements (i) and (ii) can be stated in the vernacular, and you should do so now. \circ

Exercise 19.6. Guess the infimum for each of the cases below:

- (a) $x_n = 1/n$, for $n = 1, 2, 3, \dots$;
- (b) $x_n = n^2$, for $n \in \mathbb{N}$;
- (c) $x_n = n/(n+1)$, for $n \in \mathbb{N}$;
- (d) $x_n = (-1)^n/(n^2+1)$, for $n \in \mathbb{N}$. \circ

When you look for the infimum, remember that it may or may not appear in the sequence. Everything we do for the infimum can be done for the supremum. So the **supremum** of the sequence (x_n) (or **least upper bound** of (x_n)) is the supremum of the set $S = \{x_n : n \in \mathbb{N}\}$. We denote it by $\sup(x_n)$. The rest is left to you in the next exercise.

Exercise 19.7. Let (x_n) be a sequence that is bounded above. State the two properties that the supremum of (x_n) must satisfy, and say why it exists. \circ

That takes care of how high and how low a sequence can go. Now we turn to how it gets where it is going.

A sequence (x_n) is **increasing** if $x_n \leq x_{n+1}$ for all n , and **decreasing** if $x_n \geq x_{n+1}$ for all n . We say the sequence (x_n) is **strictly increasing** if $x_n < x_{n+1}$ for all n . Likewise, a sequence (x_n) is **strictly decreasing** if $x_n > x_{n+1}$ for all n .

Exercise 19.8. The object of this exercise is to make sure you understand the definitions above. Either explain why you cannot give an example of the following, or give an example of

- (a) a bounded sequence. Find an upper bound and a lower bound.
- (b) a sequence that is bounded below, but not bounded above. Find a lower bound. Must the sequence be increasing?
- (c) a sequence that is bounded above, but not bounded below. Find an upper bound.
- (d) an increasing sequence that is neither bounded above nor below.
- (e) a strictly increasing bounded sequence.
- (f) a strictly decreasing sequence that is bounded above, but not below.
- (g) a sequence that is neither strictly increasing nor strictly decreasing. \circ

Exercise 19.9. What is your best guess for the supremum of the sequence

$$x_n = \underbrace{0.999\dots9}_{n \text{ 9's}}?$$

In Problem 20.18 of the next chapter you will give a rigorous proof of this fact. \circ

Since sequences are functions, we can manipulate them algebraically. For example, to add two sequences together, we define the sum $(x_n) + (y_n)$ to be the sequence $(x_n + y_n)$. In the same way, we may subtract sequences.

Example 19.10. Suppose (x_n) and (y_n) are two bounded sequences. If $\sup(x_n) = l$ and $\sup(y_n) = m$, is $\sup(x_n + y_n) = l + m$?

We'll first show that $l + m$ is an upper bound of $(x_n + y_n)$. (Thus it makes sense to talk about the supremum of $(x_n + y_n)$.) Then we will try to show the second thing:

that $l+m$ is the least of all the upper bounds, in the sense defined above. Remember that since we don't know the answer here, our attempt might fail.

So let $l = \sup(x_n)$ and $m = \sup(y_n)$. Then $x_n \leq l$ for all n and $y_n \leq m$ for all n . Thus $x_n + y_n \leq l + m$ for all n . So far so good; we know that $l + m$ is an upper bound (and we know that the sequence $(x_n + y_n)$ is bounded above). But we still have to see whether or not $l + m$ is the least upper bound. So suppose that p is another upper bound. We are supposed to show that $p \geq l + m$. Well, $p \geq x_n + y_n$ for every n , but that doesn't seem to help since that doesn't (in general) imply anything about the relation between p and x_n or p and y_n . In fact, closer inspection reveals that if one of the sequences is negative, we can't say anything at all. So we abandon our attempt at a proof and search for a counterexample, using what we learned above.

Let (x_n) be a bounded nonconstant sequence, say $x_1 = 1$ and $x_n = 2$ for all other n . Thus $l = 2$. Now let $y_n = -x_n$. Then $m = -1$. So $x_n + y_n = 0$, and the supremum of $(x_n + y_n)$ is clearly 0, while $l + m = 1$. Hence the supremum of $(x_n + y_n)$ need not be $l + m$. \circ

The lesson here is that in trying to prove something, we came up with an example that showed it wasn't true. This is a perfectly reasonable way to approach the problem as long as we are always on the lookout for what can go wrong with a proof.

Exercise 19.11. Let (x_n) be a sequence that is bounded below. Let $l = \inf(x_n)$. Show that $(-x_n)$ is bounded above and find the supremum of the sequence. \circ

Recall that we introduced recursively defined functions in the last chapter: The recursively defined function had domain \mathbb{N} and codomain X . Now X was allowed to be any nonempty set, but the domain had to be \mathbb{N} (or a set of the form $\{x \in \mathbb{N} : x \geq m\}$ for some $m \in \mathbb{Z}$). So, these functions, our motivating example, $n!$, and every other function to which we applied the recursion theorem are all sequences. Many sequences are defined recursively, including several famous sequences, as we will see below. If a sequence is defined by giving a formula for x_n in terms of n , then we say that the sequence is defined explicitly. It is possible for a sequence to have both a recursive definition as well as an explicit one, as we will see below.

Exercise 19.12. Reconsider the function of Exercise 18.7, $g : \mathbb{N} \rightarrow \mathbb{R}$, defined recursively by $g(0) = 1$ and $g(n+1) = 5g(n)$ for every $n \in \mathbb{N}$. Then g is a familiar function. What is it? \circ

One of the most famous examples of a sequence defined recursively is the Fibonacci sequence. Fibonacci, whose real name is Leonardo Pisano, was born in 1170 in Pisa. (One source you might consult for more information about Leonardo Pisano is L. Sigler's book [98].) The Fibonacci sequence is often presented with pictures of rabbits. So here is a version of Fibonacci's original rabbit problem: Suppose that rabbits live forever. Starting at the age of two months, each pair produces (exactly) one baby pair, and continues to do so every month thereafter. If we start

with one brand new pair, how many pairs of rabbits will we have in the n th month? Now here's the sequence. See if you can figure out the reference to these rabbits.

Define $F_0 = 0, F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. This sequence is called the **Fibonacci sequence** and the terms of the sequence are called the **Fibonacci numbers**. In this example, the recursion uses two preceding terms of the sequence. This complicates the application of the recursion theorem. In Problem 19.17 we will ask you to provide the details of this application of the recursion theorem.

Example 19.13. Find the first seven terms of the Fibonacci sequence.

The first seven Fibonacci numbers are: $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8$. \circ

The Fibonacci sequence is extremely appealing to mathematicians and nonmathematicians. In fact, there are many web sites and books with information and problems about Fibonacci sequences, as well as the journal *The Fibonacci Quarterly*.

We present one of the many interesting patterns found in Fibonacci numbers below. Others can be found in the problems, as well as some of the references given in this chapter.

Exercise 19.14. Let (F_n) denote the Fibonacci sequence. Show that for every positive integer n the equation $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ holds.

Check the equation for the first few values of n to see if this is reasonable (but, of course, this is not a proof). The proof of Exercise 19.14 will use mathematical induction, and you can read our solution below when you are ready. \circ

We now return to the solution of the Josephus problem mentioned at the beginning of the chapter. For each integer $n \geq 2$, we let $f(n)$ denote the number of the winning child. Then $f(2) = 1, f(3) = 3, f(2n) = 2f(n) - 1$, and $f(2n + 1) = 2f(n) + 1$. Note that a variation on our "recursion theorem theme" made this solution possible! For more information on the Josephus problem, we recommend the article [97].

Definitions

Definition 19.1. A **sequence** is a function f from the natural numbers \mathbb{N} to a set X . It is standard to write $x_n = f(n)$, and to refer to x_n as a **term** in the sequence. The sequence will be denoted (x_n) .

Definition 19.2. A sequence of real numbers (x_n) is **bounded above**, if there is a real number M such that $x_n \leq M$ for all n , and **bounded below**, if there exists a real number m such that $x_n \geq m$ for all n . A sequence is **bounded** if it is bounded above and below.

Definition 19.3. A real number U satisfying $x_n \leq U$ for all n is called an **upper bound** of the sequence (x_n) , and a real number L satisfying $L \leq x_n$ for all n is a **lower bound** of the sequence (x_n) .

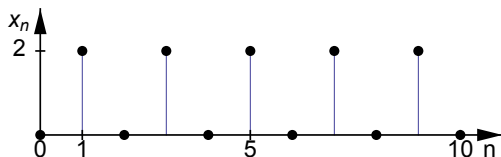


Fig. 19.2 Graph of (x_n) , where $x_n = 1 - (-1)^n$ for $n \geq 0$

Definition 19.4. The **infimum** (or **greatest lower bound**) of the sequence of real numbers (x_n) that is bounded below is the real number $\inf(x_n)$ satisfying

- (i) $\inf(x_n) \leq x_m$ for all m , and
- (ii) if p is a real number satisfying $p \leq x_m$ for all m , then $p \leq \inf(x_n)$.

Definition 19.5. The **supremum** (or **least upper bound**) of the sequence of real numbers (x_n) that is bounded above is the real number $\sup(x_n)$ satisfying

- (i) $\sup(x_n) \geq x_m$ for all m , and
- (ii) if p is a real number satisfying $p \geq x_m$ for all m , then $p \geq \sup(x_n)$.

Definition 19.6. A sequence (x_n) is **increasing** if $x_n \leq x_{n+1}$ for all n . It is **strictly increasing** if $x_n < x_{n+1}$ for all n .

Definition 19.7. A sequence (x_n) is **decreasing** if $x_n \geq x_{n+1}$ for all n . It is **strictly decreasing** if $x_n > x_{n+1}$ for all n .

Definition 19.8. Define $F_0 = 0, F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. This sequence is called the **Fibonacci sequence** and the terms of the sequence are called the **Fibonacci numbers**.

Solutions to Exercises

Solution (19.2).

- (a) $x_0 = 0, x_1 = 2, x_2 = 0$, and $x_3 = 2$. The first eleven terms are graphed in [Figure 19.2](#).
- (b) $x_0 = 0, x_1 = 1/2, x_2 = 2/3$, and $x_3 = 3/4$. The first eleven terms are graphed in [Figure 19.3](#).

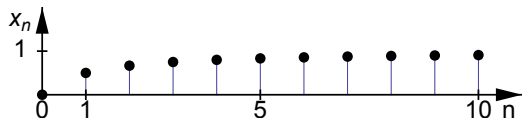


Fig. 19.3 Graph of (x_n) , where $x_n = n/(n+1)$ for $n \geq 0$

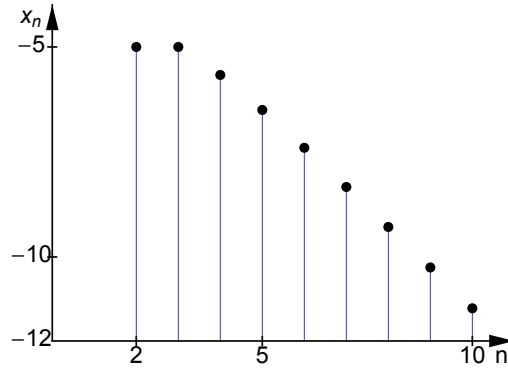


Fig. 19.4 Graph of (x_n) , where $x_n = (n^2 + 1)/(1 - n)$ for $n \geq 2$

- (c) $x_2 = -5$, $x_3 = -5$, $x_4 = -17/3 \approx -5.67$, and $x_5 = -13/2 = -6.5$. The first nine terms are graphed in [Figure 19.4](#).

Solution (19.3). If you have solved Problem 12.8, then you have solved this exercise as well. If not, here is a solution.

First we'll prove that if (x_n) is bounded, then there exists a real number N such that $|x_n| \leq N$ for all n . By the definition of bounded sequence, there exist real numbers m and M such that $m \leq x_n \leq M$, for all n . Hence $-|m| \leq m \leq x_n \leq M \leq |M|$ for all n . Letting $N = \max\{|m|, |M|\}$, we have $-N \leq x_n \leq N$. Thus $|x_n| \leq N$ for all n .

Finally, we prove that if there exists a real number N such that $|x_n| \leq N$ for all n , then (x_n) is bounded. Since $|x_n| \leq N$ for all n , we have $-N \leq x_n \leq N$ for all n . This shows that (x_n) is bounded below and bounded above. Hence the sequence (x_n) is bounded.

Solution (19.4). Many answers are possible for (a).

- (a) Consider the number $m = -1$. Then m is not an upper bound of the sequence since $x_1 > m$.
- (b) The real number U is not an upper bound of the sequence $(x_n)_{n \in \mathbb{N}}$ if there exists $n \in \mathbb{N}$ such that $x_n > U$.

Solution (19.6). The answers are: (a) 0, (b) 0, (c) 0, (d) $-1/2$.

Solution (19.7). A real number U is the supremum of a sequence (x_n) if (i) $x_n \leq U$ for all n , and (ii) if V is another upper bound of (x_n) , then $U \leq V$.

The set $\{x_n\}$ is bounded above and thus, by the completeness axiom of \mathbb{R} , this set has a supremum. The supremum of this set is the supremum of the sequence (x_n) .

Solution (19.8). You should be able to find examples for all parts of this problem, except part (d). An increasing sequence will always be bounded below, and its first term will serve as a lower bound. For parts (a) and (g), the sequence $((-1)^n)$ yields such an example. An upper bound for this sequence is 10 and a lower bound is

–10 (of course many other choices are possible). For (c) and (f), you can use the sequence $(-n)$, which is bounded above by 0 but is not bounded below. For (b), the sequence defined by $x_n = n + 2(-1)^n$ for $n \in \mathbb{N}$ is bounded below (by, for example, –100) and this sequence is not increasing (since $x_0 = 2$ and $x_1 = -1$). Finally, for (e) the sequence $(1 - 1/n)$ for $n \in \mathbb{Z}^+$ serves as an example.

Solution (19.9). Your guess was surely 1. Right?

Solution (19.11). Since $l = \inf(x_n)$, we know that $x_n \geq l$ for all n . Multiplying both sides by -1 we obtain $-x_n \leq -l$ for all n , and consequently $(-x_n)$ is bounded above and $-l$ is an upper bound. We claim that $-l$ is the supremum, too. Suppose that m is also an upper bound. Then $-x_n \leq m$ for all n . Multiplying by -1 , we see that $x_n \geq -m$ for all n . But this implies that $-m$ is a lower bound for (x_n) . Since $l = \inf(x_n)$, we know that $-m \leq l$. Thus $m \geq -l$, and $-l$ is the least of all the upper bounds. So $-l = \sup(-x_n)$.

Solution (19.12). We note that $g(0) = 1, g(1) = 5, g(2) = 5^2$, and $g(3) = 5^3$. We guess that $g(n) = 5^n$ for all $n \in \mathbb{N}$. We prove this guess using induction.

For the base step of $n = 0$ we have $g(0) = 1 = 5^0$.

Now for the induction step, we let $n \in \mathbb{N}$ and we suppose that $g(n) = 5^n$. Then $g(n+1) = 5g(n)$ by the recursive definition. Using the induction hypothesis we get $5(g(n)) = 5(5^n)$. We conclude that $g(n+1) = 5^{n+1}$, completing the induction step.

By mathematical induction the function is $g(n) = 5^n$, as we guessed above.

Solution (19.14). We will prove the validity of this equation using induction. We will consider two base steps here. For $n = 1$, we easily check that $F_2F_0 - F_1^2 = -1$. Similarly, for $n = 2$, we can check that $F_3F_1 - F_2^2 = 1$. For the induction step, let $n \in \mathbb{N}$ with $n \geq 2$ and suppose that $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. In other words, we assume that $F_n^2 = F_{n+1}F_{n-1} - (-1)^n$. We will show that $F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$. To see this, note that $F_{n+2} = F_{n+1} + F_n$ for all n . Thus (you should fill in reasons for each of the equalities):

$$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= (F_{n+1} + F_n)F_n - F_{n+1}^2 \\ &= F_{n+1}F_n + F_n^2 - F_{n+1}^2. \end{aligned}$$

Use the induction hypothesis to replace the middle term, F_n^2 , in the summand above to conclude that

$$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= F_{n+1}F_n + F_{n+1}F_{n-1} - (-1)^n - F_{n+1}^2 \\ &= F_{n+1}(F_n + F_{n-1}) - F_{n+1}^2 + (-1)^{n+1} \\ &= (-1)^{n+1}, \end{aligned}$$

and the result now follows from the principle of mathematical induction.

The first 100 Fibonacci numbers can be found on the Web [60]. From there you can get to a very cute picture of little rabbits, as well as a set of puzzles based on these numbers. Fibonacci numbers also make an appearance in the popular children's book *The Number Devil* by Hans Magnus Enzensberger [25].

Problems

Problem 19.1. Graph the following sequences and briefly describe each of the graphs:

- (a) $x_n = (-1)^n$, where $n \in \mathbb{N}$;
- (b) $x_n = 1/2^n$, where $n \in \mathbb{N}$;
- (c) $x_n = n/(n-1)$, where $n \in \mathbb{N}$ and $n \geq 2$;
- (d) $x_n = (-1)^n/2^n$, where $n \in \mathbb{N}$;
- (e) $x_n = (-1)^n(n^2/(n+1))$, where $n \in \mathbb{N}$.

Problem 19.2. Prove that the sequence (x_n) , defined by $x_n = \frac{n}{n+1}$, is strictly increasing.

Problem 19.3. In what follows, no rigorous proofs are required. However, you should provide a brief explanation of your answers.

- (a) Give an example of a sequence of rational numbers that is bounded above.
- (b) Give an example of a sequence of rational numbers that has no upper bound, but does have a lower bound.
- (c) Give an example of a strictly increasing sequence of numbers that has a supremum, but such that the supremum is not a term in the sequence. Can you find a strictly increasing sequence (x_n) such that the supremum is equal to x_n for some n ? Why or why not?

Problem 19.4. The game of chess seems to have some of its roots in India. As the story goes, the emperor of India was smitten with the new game, and he asked the inventor of chess how he could reward him for this marvelous invention. The (apparently modest) reply was to ask for one grain of rice for the first square of the chess board, double that for the second, double that for the third, and so on. Thus, for each square after the first, the inventor receives double the number of grains he received on the previous square.

Let $x_n =$ number of rice grains for the n th square of the chessboard. Then (x_n) is a sequence.

- (a) Find the first four terms of (x_n) .
- (b) Find an explicit formula for x_n .

Consider the new sequence (a_n) , where $a_n =$ total number of rice grains for the first n squares. You will need to use the formula for a geometric sum: For a real number $a \neq 1$ and positive integer n we have $1 + a + \cdots + a^n = (1 - a^{n+1})/(1 - a)$. (If this formula is unfamiliar to you, prove it!)

- (c) Find the first four terms of (a_n) .
- (d) Find an explicit formula for a_n .
- (e) What is the mass of the rice the inventor asked for? (Use the fact that the mass of one grain of rice is approximately 25 mg.)
- (f) The rice production of the whole world in 2004 was approximately 600 million metric tons of rice. How does this compare with the inventor's request?

Problem 19.5. Phenytoin is a medication designed to control seizures. It is administered twice daily at 8:00 a.m. and at 8:00 p.m. The dosage at each administration is 75 mg. The retention rate after 12 hours is 65% (that is, 12 hours after intake, 65% of the drug remains in the body). Let S_n denote the amount of phenytoin in the patient's body shortly after the n th administration of the drug.

- (a) Calculate the first four terms of the sequence $(S_n)_{n=1}^{\infty}$.
- (b) Give a recursive definition of this sequence.
- (c) Prove that (S_n) is strictly increasing, bounded, and that $\sup(S_n)$ exists.

We let s_n denote the amount of phenytoin in the patient's body shortly *before* the n th administration of the drug.

- (d) Express s_n in terms of S_n .
- (e) Indicate why (s_n) is also increasing, bounded, and $\sup(s_n)$ exists.
- (f) Find the minimum and maximum amount of phenytoin in the patient's blood following the 8 a.m. dose on day 3 and prior to the 8 a.m. dose on day 4.

Problem 19.6. Give an example of a sequence of rational numbers that has an irrational number as supremum. Prove your claim!

Problem 19.7. We define a sequence (a_n) by $a_1 = 1$ and $a_{n+1} = 3 - 1/a_n$ for all $n \geq 1$.

- (a) Show that (a_n) is bounded.
- (b) Prove that (a_n) is strictly increasing.

Problem 19.8. We define the sequence (x_n) by $x_n = \frac{n^3+n^2-1}{n^3+1}$ for $n \in \mathbb{N}$.

- (a) Prove that (x_n) is bounded.
- (b) Is (x_n) increasing? Prove it or give a counterexample.
- (c) Find $\inf(x_n)$.

Problem 19.9. If $l = \sup(x_n)$, what is $\inf(-x_n)$? (You should know by now that the first thing to do is to try examples. Make up at least three different examples.) State your conjecture. Prove it.

Problem 19.10. If $l = \sup(x_n)$, what is $\sup(kx_n)$ where $k \in \mathbb{R}^+$? Prove your conjecture.

Problem 19.11. Let (x_n) be a bounded sequence such that $x_n \leq -2$ for all $n \in \mathbb{N}$.

- (a) Prove that (x_n^2) is bounded.

- (b) Let $l = \inf(x_n)$ and $m = \sup(x_n)$. Find $\inf(x_n^2)$ in terms of l or m , or both. Prove that your result is correct.

Problem 19.12. Suppose that (x_n) and (y_n) are bounded below.

- (a) Show that $\inf(x_n + y_n) \geq \inf(x_n) + \inf(y_n)$.
 (b) Is it always true that $\inf(x_n + y_n) = \inf(x_n) + \inf(y_n)$? Prove this or give a counterexample.

Problem 19.13. Suppose that (x_n) and (y_n) are bounded below. Is it always true that $\inf(x_n y_n) = \inf(x_n) \inf(y_n)$? Prove this or give a counterexample.

Problem 19.14. Let (x_n) and (y_n) be two sequences of real numbers. Assume that (y_n) is bounded above and that $x_n < y_n$ for all $n \in \mathbb{N}$.

- (a) Prove that (x_n) is also bounded above.
 (b) Prove that $\sup(x_n) \leq \sup(y_n)$.
 (c) Do the assumptions imply that $\sup(x_n) < \sup(y_n)$? If yes, prove it; if no, find a counterexample.

Problem 19.15. Let (x_n) and (y_n) be two sequences of real numbers. Assume that (x_n) is bounded above and that $x_n < y_n < x_{n+1}$ for all $n \in \mathbb{N}$.

- (a) What can you say about $\sup(x_n)$ and $\sup(y_n)$? Must they exist? If so, how do they compare?
 (b) What can you say about $\inf(x_n)$ and $\inf(y_n)$? Must they exist? If so, how do they compare?

Problem 19.16. We define a sequence (x_n) recursively by letting $x_0 = 1000$ and $x_n = (.05)x_{n-1}$ for $n \geq 1$. Find another representation for this sequence. Have you seen this anywhere else before? If so, where?

Problem 19.17. With the help of the recursion theorem, prove that the Fibonacci sequence (see Definition 19.8) is well-defined; that is, specify a , X , and f appearing in the recursion theorem. (You can use Example 18.8 to suggest an approach to this problem.)

Problem 19.18. (a) Prove that the Fibonacci sequence is increasing.
 (b) Prove that the Fibonacci sequence is unbounded.

Problem[#] 19.19. Let (F_n) be the Fibonacci sequence and $x_n = F_{n+1}/F_n$, for $n \geq 1$. Show that $x_n = 1 + 1/x_{n-1}$, for $n \geq 2$.

Problem 19.20. Prove the following explicit formula for the n th Fibonacci number:

$$F_n = \frac{a^n - b^n}{a - b}, \text{ where } a = \frac{1 + \sqrt{5}}{2} \text{ and } b = \frac{1 - \sqrt{5}}{2}.$$

Problem 19.21. Let $f(0) = 2$, $f(1) = 2$, and define $f(n+1) = f(n)f(n-1)$. Find an explicit formula for $f(n)$.

Problem 19.22. Let (F_n) denote the Fibonacci sequence. Define the Lucas sequence by $L_0 = 2$, $L_1 = 1$, and for $n \geq 1$ define $L_{n+1} = L_n + L_{n-1}$. (For some proofs you may want to use the second principle of induction stated in the problem section of Chapter 18 as Theorem 18.9.)

- (a) Calculate L_1, \dots, L_{10} .
- (b) Calculate $L_n - F_{n-1}$, for $n \geq 1$. Find a remarkable pattern in this list of numbers. State it clearly and prove it by induction.
- (c) Calculate $F_n + L_n$. Find a remarkable pattern in this list of numbers. State it clearly and prove it using part (b).

Chapter 20

Convergence of Sequences of Real Numbers

As we saw in the last chapter, when we graph several terms of a sequence, certain behavior may appear. We may become convinced, for whatever reason, that the sequence is unbounded. Or, we may believe that the sequence is bounded and we may even notice the sequence moving toward a particular horizontal line. But how do we check that what we believe is happening really is happening?

Our efforts to explain this require that you fully understand how to measure distance. So we remind you that distance is usually measured using the absolute value function, or $|x|$, and the absolute value of a real number x measures the distance from x to 0. If we want to measure the distance between two real numbers x and a , we would need to look at $|x - a|$.

For an arbitrary positive real number ε , we know what it means to say $|x| = \varepsilon$. What does it mean to say $|x| < \varepsilon$? The answer is, as you can check, that $|x| < \varepsilon$ if and only if $-\varepsilon < x < \varepsilon$. So how do we determine when a sequence of real numbers approaches a real number L ? We will use the absolute value function to measure the distance from terms in the sequence to L . We make this precise in the following definition.

We say that a sequence (x_n) **converges** if there exists a real number L such that for all $\varepsilon > 0$ there exists a real number N such that $|x_n - L| < \varepsilon$ for all $n \geq N$. If such an L exists, we call L the **limit** of the sequence (x_n) , we say that (x_n) **converges to L** , and we write $x_n \rightarrow L$ or $\lim_{n \rightarrow \infty} x_n = L$. If no such L exists, we say that the sequence **diverges**. While we allow N to be a real number, we caution you to remember that the indices on the terms of a sequence, x_n , are natural numbers. To really understand this definition, we must understand it visually, and we must also know how to use it to show that a sequence converges. We first turn to the visual aspect of convergence.

Let's think about the definition. If we believe the sequence (x_n) converges, then we need to find a real number L such that the sequence gets really really close to the line $y = L$. Mathematically, we say that we need the sequence arbitrarily close to the horizontal line. This, in turn, implies that the distance from the sequence to the line $y = L$ should be less than every positive real number ε that we can think of; that is what arbitrarily close means. But it may not happen right away; it may only happen eventually (for each ε , there will exist N such that x_n may not satisfy what we want

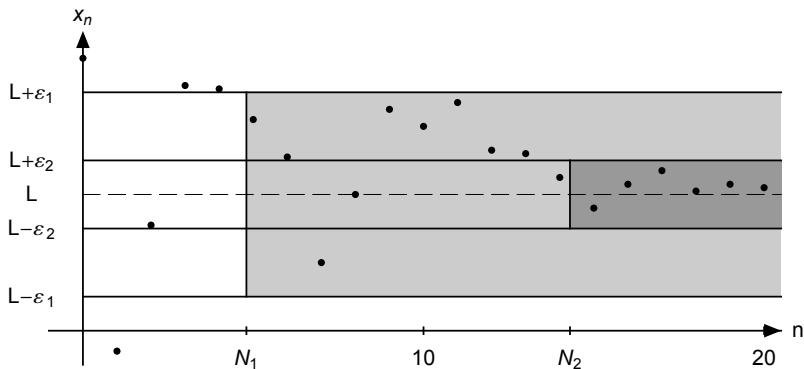


Fig. 20.1 Definition of a convergent sequence; two-dimensional illustration

for $n < N$, but it will satisfy it for $n \geq N$). That’s why we defined convergence the way we did.

We illustrate this definition in Figure 20.1. In this picture, we first pick a value $\epsilon = \epsilon_1 > 0$. Then we indicate a corresponding real number $N = N_1$ such that for all $n \geq N_1$ we have $|x_n - L| < \epsilon_1$. Looking at the figure, we see that the strip from $y = L - \epsilon_1$ to $y = L + \epsilon_1$ contains all the terms of the sequence from x_5 on. Generally, the smaller the value of ϵ , the larger the value of N . Let’s think about why this is true: Returning to Figure 20.1, we see that $\epsilon = \epsilon_2$ is smaller than ϵ_1 , and this, in turn, forces the sequence to be closer to the horizontal line. So we go farther out in the sequence to get closer to the line $y = L$. You also probably noticed that once we find a value of N that works, anything larger than N will work, too.

Figure 20.2 below is yet another way to illustrate the same situation. Explain this sketch to yourself.

Now let’s turn to how we show a sequence converges. First we make a conjecture as to the value of the limit, call it L . The important thing to notice, when we make our conjecture, is that we are interested in the behavior as $n \rightarrow \infty$. We don’t really care what happens for small n , for example. So if we ask what a sequence converges to, you can guess by ignoring terms that don’t really matter in the long run. For example, if we ask you to guess what

$$\left(\frac{2n^2 + 3n + 4}{4n^2 - 3n - 5} \right)$$

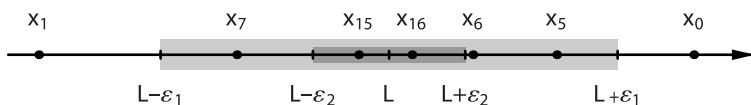


Fig. 20.2 Definition of a convergent sequence; one-dimensional illustration

converges to, you would remember that only behavior near infinity matters, so you would probably guess that $2n^2$ really dominates the quantity in the numerator, while $4n^2$ really dominates the quantity in the denominator. Thus, when you guess this limit, you'll probably guess that it's the same as the limit of the sequence with terms $x_n = 2n^2/(4n^2)$ —which it is. You probably also would guess that this limit is $1/2$, and you'd be right again. Before we move to our second step, try practicing your guessing on some of the examples below.

Exercise 20.1. Guess the limits of each of the following sequences:

(a) $\left(\frac{3n^2 + n + 4}{3 + n + 5n^2}\right)$;

(b) $\left(\frac{2n^3 + n^2 + 5}{n^4 + 6}\right)$;

(c) $\left(\frac{\sqrt{n} + n}{\sqrt{n} - n}\right)$. ○

Now, once you have guessed your limit, you must prove that it is correct. To do this, assume that we are given an arbitrarily small number, which we denote by ϵ . We then try to find a real number N (depending on ϵ) so that for the remaining terms of the sequence, that is, for $n \geq N$, we have $|x_n - L| < \epsilon$. This is where things get tricky.

Let's see how we would use this definition, starting with a fairly simple example.

Example 20.2. Show that the sequence (x_n) defined by $x_n = 1/n$ converges to 0.

We'll find this easier if we follow Pólya's list.

“Understanding the problem.” We need to show that for every $\epsilon > 0$ there exists a real number N such that $n \geq N$ implies that $|x_n - 0| < \epsilon$. We fill in what we can, remembering that ϵ is arbitrary; that is, it is chosen for us and we have no control over its value. So once someone gives us ϵ , we are supposed to come up with N so that $|1/n - 0| < \epsilon$ for $n \geq N$.

“Devising a plan.” Now we'll work backwards to see what N has to be. We need $|1/n| < \epsilon$. So we need $n > 1/\epsilon$. It appears that if we take $N > 1/\epsilon$, say $N = 2/\epsilon$, we'll get exactly what we need when $n \geq N$. Since N depends on ϵ (there's an ϵ in our definition of N), many authors write $N = N(\epsilon)$.

Before we carry out the plan, note that if we knew ϵ , then this would tell us exactly how big N has to be. If $\epsilon = 0.1$, then N needs to be bigger than $1/0.1 = 10$; if $\epsilon = 0.01$, then N needs to be bigger than $1/0.01 = 100$; and if ϵ just happens to be itself, then N needs to be greater than $1/\epsilon$. We're now ready to carry out the plan. We have to write this up, so that a reader who has not seen our work will know what we are doing.

Proof. If $\epsilon > 0$ and we choose $N = 2/\epsilon$, then for $n \geq N$, we have $|x_n - 0| = |1/n - 0| = 1/n \leq 1/N = \epsilon/2 < \epsilon$. Therefore, if $n \geq N$, then $|x_n - 0| < \epsilon$ as desired. □

Our second example is a bit more challenging, and requires slightly different techniques. You'll see more problems of this type and more challenging limit problems when you take your first analysis course.

Example 20.3. Show that $\lim_{n \rightarrow \infty} n/(n+2) = 1$.

As above, we'll first understand our problem, and then devise a plan.

“Understanding the problem.” We start by writing out the definition: For all $\varepsilon > 0$ there exists N such that $n \geq N$ implies that $|x_n - L| < \varepsilon$.

Next we'll fill in x_n and L : For all $\varepsilon > 0$ there exists N such that $n \geq N$ implies that $|n/(n+2) - 1| < \varepsilon$.

Now simplify the expression $|n/(n+2) - 1| < \varepsilon$ to find out how big n must be in terms of ε : We need to find N so that $n \geq N$ implies that $2/(n+2) < \varepsilon$.

“Devising a plan.” You can solve for n , as above, if you wish, but that method only works well in simple cases. So we are going to try to change this problem from the one we have to a simpler problem. How will we do that? Well, we want to make $2/(n+2)$ small. If we can find something bigger and simpler than $2/(n+2)$, and if we can make that less than ε , then we will also know that $2/(n+2)$ is less than ε . What's bigger and simpler? The previous example wasn't too bad. So if we just had a simple fraction, we would be in good shape. A general strategy that often works is this: If the numerator is complicated, we'll try to find something simpler and larger than the numerator. If the denominator is complicated, we'll try to find something simpler and smaller than the denominator. Our simpler expression must still “act the same in the long run” as the original.

For this exercise, the numerator is simple, so we'll leave it alone. For the denominator, we'll try to somehow use the thing that dominates: n . We need $n+2$ greater than or equal to something simple involving n . It's pretty clear that $n+2 \geq n$, so we'll use n . Putting this together, we have found that

$$\frac{2}{n+2} \leq \frac{2}{n}.$$

Thus, if we make $2/n < \varepsilon$, we will also make $2/(n+2) < \varepsilon$. But making $2/n < \varepsilon$ is easy, since $2/n < \varepsilon$ if and only if $n > 2/\varepsilon$. Therefore, it appears that if $N > 2/\varepsilon$, then $2/n < \varepsilon$ and thus $2/(n+2) < \varepsilon$, which is what we need.

“Carrying out the plan.” Write out the proof, beginning with “If $\varepsilon > 0$ and . . .” The very next phrase should identify N , unless there are things you need to tell the reader in order for the reader to understand your definition of the real number N . Remember that the reader will only see your proof, not your plan.

Proof. If $\varepsilon > 0$ and we choose $N = 3/\varepsilon$, then for $n \geq N$, we have

$$\left| \frac{n}{n+2} - 1 \right| = \left| \frac{2}{n+2} \right| \leq \frac{2}{n} \leq \frac{2}{N} = \frac{2\varepsilon}{3} < \varepsilon.$$

Thus, $\lim_{n \rightarrow \infty} n/(n+2) = 1$. □

Here's one more exercise on limits.

Exercise 20.4. The sequence $((2n+4)/(n^2+n+1))$ converges. Guess the limit and prove that your guess is correct, using the definition of convergence. \circ

It's time to think about negating the definition of convergence.

Exercise 20.5. By negating the definition of convergence, explicitly state what it means for a sequence (x_n) to diverge. \circ

Exercise 20.6. Using Exercise 20.5, show that the sequence $((-1)^n)$ diverges. \circ

We state the most basic properties of limits and convergent sequences here. The first theorem says that there can be one and only one choice for the limit of a convergent sequence.

Theorem 20.7. *If a sequence converges, then the limit is unique.*

We've done uniqueness proofs before and we'll do this one the same way: We suppose to the contrary that there are two different limits L and M , and then we will show that they must be the same. So, we need to show that $L - M = 0$. We also use a standard trick: *we add and subtract the same quantity to an object*. Why? Well, since all we know is that L and M get close to the terms of the sequence (x_n) , we have to somehow use these terms. But there is no x_n in the equation $L - M = 0$. So we will have to insert an x_n where none appears.

Proof. Let (x_n) be a convergent sequence. Suppose to the contrary that $x_n \rightarrow L$ and $x_n \rightarrow M$, where $L \neq M$. Let $\varepsilon = (1/4)|L - M|$. Then $\varepsilon > 0$. By the definition of convergence, since $\varepsilon > 0$, there exists N_1 such that $|x_n - L| < \varepsilon$ for $n \geq N_1$ and there exists N_2 such that $|x_n - M| < \varepsilon$ for $n \geq N_2$. Let $N = \max\{N_1, N_2\}$. Then for $n \geq N$ we have

$$\begin{aligned} |L - M| &= |L - x_n + x_n - M| \\ &\leq |L - x_n| + |x_n - M| \quad (\text{by the triangle inequality}) \\ &< \varepsilon + \varepsilon \quad (\text{since } n \geq N_1 \text{ and } n \geq N_2) \\ &= \frac{1}{2}|L - M|. \end{aligned}$$

But this is silly, since no positive real number is smaller than half of itself. This contradiction establishes the result that limits of sequences are unique. \square

Here's another important theorem. It uses Exercise 19.3, which says that a sequence (x_n) is bounded if and only if there exists a real number M such that $|x_n| \leq M$ for all n .

Theorem 20.8. *Every convergent sequence is bounded.*

Proof. Suppose that the sequence $(x_n)_{n=1}^{\infty}$ converges to the real number L . Let $\varepsilon = 1$. Then there exists N such that $|x_n - L| < 1$ for all $n \geq N$. Let K be the smallest integer satisfying $K \geq N$. Thus $|x_n| = |x_n - L + L| \leq |x_n - L| + |L| < 1 + |L|$

for all $n \geq K$. Consider the real numbers $|x_1|, |x_2|, \dots, |x_{K-1}|$ and $1 + |L|$. Since there are finitely many such numbers, we may choose the maximum of these. Let $M = \max\{|x_1|, |x_2|, \dots, |x_{K-1}|, 1 + |L|\}$. Then $|x_n| \leq M$ for all n , and we conclude that the sequence (x_n) is bounded. \square

Part (i) of the next theorem says that if we sum two convergent sequences, the new sequence converges, too. It also says “the limit of the sum is the sum of the limits.” What do the other parts say?

Theorem 20.9. *Let (x_n) and (y_n) be two sequences that converge. Let L and M be real numbers such that $x_n \rightarrow L$ and $y_n \rightarrow M$. Then*

- (i) $x_n + y_n \rightarrow L + M$,
- (ii) $\alpha x_n \rightarrow \alpha L$, for every real number α ,
- (iii) $x_n y_n \rightarrow LM$, and
- (iv) if $M \neq 0$ and $y_n \neq 0$ for all n , then $1/y_n \rightarrow 1/M$.

We prove part (i) here. All the proofs are similar, and this part will illustrate the most important idea, which is that we need to choose things carefully to make everything work out. Here’s what we mean: For every $\varepsilon > 0$, we need to find N such that for $n \geq N$ we have $|(x_n + y_n) - (L + M)| < \varepsilon$. We can make $|x_n - L| < \varepsilon$ for n large enough, and we can make $|y_n - M| < \varepsilon$ for n large enough, but if we add these together we get 2ε . You’ll now see how we handle this problem.

Proof. [Proof of (i)] Let $\varepsilon > 0$. Since $\varepsilon/2 > 0$ and $x_n \rightarrow L$, there exists N_1 such that $|x_n - L| < \varepsilon/2$ for $n \geq N_1$. Again, since $\varepsilon/2 > 0$ and $y_n \rightarrow M$, there exists N_2 such that $|y_n - M| < \varepsilon/2$ for $n \geq N_2$. Let $N = \max\{N_1, N_2\}$. Then for $n \geq N$, we know that $n \geq N_1$ and $n \geq N_2$, so

$$\begin{aligned} |(x_n + y_n) - (L + M)| &= |(x_n - L) + (y_n - M)| \\ &\leq |x_n - L| + |y_n - M| \quad (\text{by the triangle inequality}) \\ &< \varepsilon/2 + \varepsilon/2 \quad (\text{since } n \geq N_1 \text{ and } n \geq N_2). \end{aligned}$$

We conclude that for all $\varepsilon > 0$ there exists N such that for all $n \geq N$ we have $|(x_n + y_n) - (L + M)| < \varepsilon$, as desired. \square

This theorem can be used to find the limit of a recursively defined function rather easily, if we know that the sequence converges.

Exercise 20.10. Define the sequence (x_n) by $x_1 = 1$ and $x_{n+1} = 0.02x_n^2 + 8$ for all $n \in \mathbb{Z}^+$. You may assume that the sequence (x_n) converges and is bounded above by 20. Find $\lim_{n \rightarrow \infty} x_n$. \circ

Definitions

Definition 20.1. We say that a sequence (x_n) **converges** if there exists a real number L such that for all $\varepsilon > 0$ there exists a real number N such that $|x_n - L| < \varepsilon$ for all $n \geq N$. If such an L exists, we call L the **limit** of the sequence (x_n) , we say that (x_n) **converges to** L , and we write $x_n \rightarrow L$ or $\lim_{n \rightarrow \infty} x_n = L$.

Definition 20.2. A sequence **diverges** if it does not converge.

Definition 20.3 (for Problem 20.20). Let (x_n) be a bounded sequence. For each positive integer n , let $s_n = \sup\{x_m : m \geq n\}$. Then (s_n) converges and its limit is called the **limit superior** of (x_n) , written $\limsup(x_n)$.

Definition 20.4 (for Problem 20.20). Let (x_n) be a bounded sequence. For each positive integer n , let $t_n = \inf\{x_m : m \geq n\}$. Then (t_n) converges and its limit is called the **limit inferior** of (x_n) , written $\liminf(x_n)$.

Definition 20.5 (for Problem 20.21). A sequence (x_n) of real numbers **diverges to infinity** (written $x_n \rightarrow \infty$) if for every $M \in \mathbb{R}$ there exists a real number N such that $n \geq N$ implies $x_n > M$.

Definition 20.6 (for Problem 20.21). A sequence is **monotone** if it is an increasing sequence or a decreasing sequence.

Definition 20.7 (for Problem 20.21). A sequence (x_n) is a **Cauchy sequence** if for all $\varepsilon > 0$ there exists a real number N such that $n, m \geq N$ implies that $|x_n - x_m| < \varepsilon$.

Definition 20.8 (for Problem 20.22). Let $(x_n)_{n=1}^{\infty}$ be a sequence of real numbers and let (n_k) be a strictly increasing sequence of positive integers. The sequence (x_{n_k}) is called a **subsequence** of (x_n) .

Solutions to Exercises

Solution (20.1). The answers are (in this order): $3/5$, 0 , and -1 .

Solution (20.4). Normally when we write up our solution we will include the proof and not our work on devising a plan. But one more careful example here will certainly be useful. So here's our plan: We guess that this converges to 0 , so we need to show that for all $\varepsilon > 0$, there exists N such that $|(2n+4)/(n^2+n+1)| < \varepsilon$ for all $n \geq N$. Now both numerator and denominator are a bit complicated. For the denominator, we need to find something smaller and simpler than n^2+n+1 involving the highest-order term n^2 . So for this part, we note that $n^2+n+1 > n^2$. Now for the numerator, we need to find something larger and simpler than $2n+4$ involving the highest-order term n . For $n \geq 1$, since $4 \leq 4n$, we see that $2n+4 \leq 2n+4n = 6n$. Putting this together, for $n \geq 1$, we have

$$\left| \frac{2n+4}{n^2+n+1} \right| \leq \frac{6n}{n^2} = \frac{6}{n}.$$

So, if we make $6/n < \varepsilon$, we should be able to complete the proof. Thus, we'll choose $N = 7/\varepsilon$.

Proof. If $\varepsilon > 0$, we choose $N = 7/\varepsilon$. Then for $n \geq N$, we have

$$\left| \frac{2n+4}{n^2+n+1} - 0 \right| \leq \frac{6n}{n^2} = \frac{6}{n} \leq \frac{6}{N} = \frac{6\varepsilon}{7} < \varepsilon,$$

where the first inequality follows since $n \geq 1$ and, consequently, $2n+4 \leq 6n$. Thus $((2n+4)/(n^2+n+1))$ converges to 0. \square

Solution (20.5). A sequence (x_n) diverges if for every real number L there exists $\varepsilon > 0$ such that for all $N \in \mathbb{R}$ there exists $n \geq N$ with $|x_n - L| \geq \varepsilon$.

Solution (20.6).

Proof. Let L be a real number, and let $\varepsilon = 1/2$. We break this into two cases. First suppose that $L < 0$. Let $N \in \mathbb{R}$ and choose n to be an even integer satisfying $n \geq N$. Then $|x_n - L| = |1 - L| > 1 > \varepsilon$. Now if $L \geq 0$, then for $N \in \mathbb{R}$ choose an odd integer with $n \geq N$. It follows that $|x_n - L| = |-1 - L| = |1 + L| \geq 1 > \varepsilon$. Therefore (x_n) diverges. \square

Solution (20.10). First note that $\lim_{n \rightarrow \infty} x_{n+1} = \lim_{n \rightarrow \infty} x_n$. This is, as you should check, an immediate consequence of the definition of the limit of a sequence. Since $L = \lim_{n \rightarrow \infty} x_n$ exists, Theorem 20.9 implies that $\lim_{n \rightarrow \infty} (x_n)^2$ exists and is L^2 . Further, and again using Theorem 20.9, we get

$$L = \lim_{n \rightarrow \infty} x_{n+1} = \lim_{n \rightarrow \infty} (0.02x_n^2 + 8) = 0.02L^2 + 8.$$

We solve this quadratic equation and get $L = 10$ or $L = 40$. Since (x_n) is bounded above by 20, we conclude that $\lim_{n \rightarrow \infty} x_n = 10$.

Using induction, you can prove that (x_n) is strictly increasing and bounded above by 20. Prove it! Once you've done this, Theorem 20.11 of Problem 20.17 below implies that (x_n) converges. This justifies the hypothesis that we told you to assume.

Problems

Problem 20.1. For each of the following, give an example that satisfies all requirements or prove that no such example exists:

- a divergent sequence that is bounded;
- an increasing sequence (x_n) with $\lim_{n \rightarrow \infty} x_n = 9$ and $\lim_{n \rightarrow \infty} (-2x_n) = -8$;

- (c) a bounded increasing sequence (x_n) such that $x_n \neq 0$ for all n and such that $(1/x_n)$ diverges.

Problem# 20.2. We used the following several times in this chapter: Let $x, y, z \in \mathbb{R}$. Then $|x - y| \leq |x - z| + |y - z|$. Prove this statement.

Problem 20.3. Let a and δ be real numbers with $\delta > 0$. Show that for all real numbers x , we have $|x - a| < \delta$ if and only if $a - \delta < x < a + \delta$.

Problem 20.4. For each of the following, guess the limit and then prove (using the definition of convergence) that your guess is correct:

- (a) $\lim_{n \rightarrow \infty} \frac{1}{3n}$;
- (b) $\lim_{n \rightarrow \infty} \frac{1}{\sqrt{n}}$;
- (c) $\lim_{n \rightarrow \infty} \frac{1}{\sqrt{n+7}}$;
- (d) $\lim_{n \rightarrow \infty} \frac{n^2 + 4}{n^2}$;
- (e) $\lim_{n \rightarrow \infty} \frac{2n + 1}{n + 2}$;
- (f) $\lim_{n \rightarrow \infty} \frac{3}{n!}$;
- (g) $\lim_{n \rightarrow \infty} \frac{1}{(n+7)!}$;
- (h) $\lim_{n \rightarrow \infty} \frac{3n^2 + 1}{4n^2 + n + 2}$.

Problem 20.5. Let (x_n) and (y_n) be convergent sequences. Use the definition of convergence (no limit theorems!) to prove that the sequence $(3x_n - 2y_n)$ converges.

Problem 20.6. This is a continuation of Problem 19.5. We will use all the notation that was introduced there.

- (a) Find an explicit formula for the terms S_n of the sequence (S_n) . (You may need the formula for a geometric sum, see Problem 19.4.)
- (b) Guess $\lim_{n \rightarrow \infty} S_n$ and then prove that your guess is correct.
- (c) Find $\lim_{n \rightarrow \infty} s_n$.
- (d) Find the minimum and maximum amount of phenytoin in the patient's blood after one week and after one month (60 administrations of the drug).
- (e) Find the minimum and maximum amount of phenytoin in the patient's blood in the long run (that is, as $n \rightarrow \infty$).

Problem 20.7. Prove Theorem 20.9 part (ii).

Problem 20.8. (a) Suppose that (x_n) and (y_n) are sequences and $0 \leq x_n \leq y_n$ for all positive integers n . Show that if $y_n \rightarrow 0$, then $x_n \rightarrow 0$.

- (b) Suppose that (x_n) and (y_n) are sequences and $-y_n \leq x_n \leq y_n$ for all positive integers n . Show that if $y_n \rightarrow 0$, then $x_n \rightarrow 0$.
- (c) Find $\lim_{n \rightarrow \infty} \frac{\sin^2 n}{n}$ and $\lim_{n \rightarrow \infty} \frac{(-1)^n}{n^2 + 1}$, and prove that your answers are correct.

Problem 20.9. Redo Problem 20.4, parts (a), (c), (d), (e), (g), and (h) using theorems in this chapter or Problem 20.8.

Problem 20.10. Let (x_n) be a convergent sequence defined recursively by $x_1 = 50$ and $x_{n+1} = \frac{1}{2}x_n + 5$ for $n \geq 1$. Without finding an explicit form of x_n , calculate $\lim_{n \rightarrow \infty} x_n$. Justify all steps in your calculation.

Problem 20.11. Claim: Let (y_n) be a sequence defined recursively by $y_1 = 5$ and $y_{n+1} = 3y_n - 6$ for $n \geq 1$. Then $\lim_{n \rightarrow \infty} y_n = 3$.

Proof? Applying Theorem 20.9,

$$\lim_{n \rightarrow \infty} y_{n+1} = 3 \lim_{n \rightarrow \infty} y_n - 6.$$

Hence $2 \lim_{n \rightarrow \infty} y_n = 6$. This implies that $\lim_{n \rightarrow \infty} y_n = 3$. □

If this proof is correct, fill in the details, citing the theorems that are applied. If this proof is incorrect, show exactly where an incorrect conclusion is drawn. Is the claim correct? Explain.

Problem 20.12. (a) Show that for every sequence (x_n) we have

$$0 \leq |x_n| + x_n \leq 2|x_n|.$$

- (b) Prove that if $|x_n| \rightarrow 0$, then $x_n \rightarrow 0$. (See Problem 20.8.)
- (c) If (x_n) is a sequence such that $|x_n| \rightarrow 1$, must $x_n \rightarrow 1$?

Problem 20.13. Prove Theorem 20.9 part (iii). (Hint: You may want to use Theorem 20.8.)

Problem 20.14. The proof of Theorem 20.9 part (iv) is outlined below.

- (a) Prove that for real numbers y and M , if $|y - M| \leq |M|/2$, then $|y| \geq |M|/2$. (You might wish to use the lower triangle inequality to establish this implication.)
- (b) Let (y_n) be a sequence of nonzero real numbers, and suppose that $y_n \rightarrow M$, where $M \neq 0$. Prove that if $0 < \varepsilon < |M|/2$, then there exists N such that for $n \geq N$ if $|y_n - M| < \varepsilon$, then $|(M - y_n)/(My_n)| \leq (2/M^2)|M - y_n|$.
- (c) Prove Theorem 20.9 part (iv).

Problem 20.15. Let a be a real number satisfying $0 < a < 1$.

- (a) Show that there exists a real number x such that $x > 0$ and $a = 1/(1+x)$.
- (b) Show that $a^n \leq 1/(1+nx)$ for all $n \in \mathbb{N}$. (You will need to do Problem 18.6 if you have not already done it.)

- (c) Show carefully that $1/(1+nx) \rightarrow 0$.
- (d) Show that $a^n \rightarrow 0$. (You will want to do Problem 20.8 if you have not already done it.)
- (e) Show that if $x_n = \underbrace{0.999\dots 9}_{n \text{ 9's}}$, then $x_n \rightarrow 1$.

Problem 20.16. Let $x_n = F_{n+1}/F_n$, where F_n denotes the n th Fibonacci number. In Problem 19.19 we showed that $x_n = 1 + 1/x_{n-1}$. Assume further that there exists a nonzero real number L such that $x_n \rightarrow L$. Explain why $1/x_n \rightarrow 1/L$ and use these facts to compute L .

The number L is the golden ratio, which appears frequently in architecture and in nature. The Greeks, and others, felt (and still feel) that rectangles with sides in golden ratio are the most beautiful.

Problem 20.17. (An exercise in reading and writing.) The combination of the two theorems in this problem is usually called the **monotone convergence theorem for sequences**.

- (a) Read the proof below until you understand it. Mathematicians often read proofs many times, and you may have to do so with this one.

Theorem 20.11. *Every increasing bounded sequence converges to its supremum.*

Proof. Let $l = \sup(x_n)$, and let $\varepsilon > 0$. Since $l - \varepsilon$ is not an upper bound, there exists N such that $x_N > l - \varepsilon$. We have assumed that (x_n) is an increasing sequence. Therefore, if $n \geq N$, we know that $x_n \geq x_N > l - \varepsilon$. Since $x_n \leq l$ for all n , for $n \geq N$ we have $l - \varepsilon < x_n < l + \varepsilon$, and thus $|x_n - l| < \varepsilon$. Therefore, the sequence (x_n) converges to l . \square

- (b) Use the ideas in the proof above to prove Theorem 20.12.

Theorem 20.12. *Every decreasing bounded sequence converges to its infimum.*

- (c) Can you find another proof of Theorem 20.12, this time using the statement of Theorem 20.11 rather than its proof?

Problem 20.18. Use Problems 20.15 and 20.17 to prove your guess of Exercise 19.9, namely, that if $x_n = \underbrace{0.999\dots 9}_{n \text{ 9's}}$, then $\sup(x_n) = 1$.

Problem 20.19. This problem takes up the situation and notation of Problem 19.5.

- (a) Use your work of parts (b), (c), and (d) of Problem 19.5 and the theorems of Problem 20.17 to find $\sup(S_n)$ and $\sup(s_n)$.
- (b) Use part (a) to find the range of the amount of phenytoin in the patient's blood in the long run (that is, as $n \rightarrow \infty$). (Note that though this is the same question as in Problem 20.6 part (e), the solution does not require the explicit form of the sequence (S_n) !)

Problem 20.20. Use the theorems of Problem 20.17 for the following.

- Show that $(n!/n^n)$ converges.
- Let (x_n) be a bounded sequence. For $n \in \mathbb{Z}^+$, let $s_n = \sup\{x_m : m \geq n\}$. Prove that (s_n) converges. The limit of (s_n) is called the **limit superior** of (x_n) , and is usually denoted by $\limsup(x_n)$. What is the $\limsup((-1)^n)$?
- Let (x_n) be a bounded sequence. For $n \in \mathbb{Z}^+$, let $t_n = \inf\{x_m : m \geq n\}$. Prove that (t_n) converges. The limit of (t_n) is called the **limit inferior** of (x_n) , and is usually denoted by $\liminf(x_n)$.

Problem 20.21. Sequences afford an excellent opportunity to practice everything you have learned. That's what you'll do in this problem: For each of the definitions below, do the following.

- Read the definition.
- Try to find an example of something that illustrates the definition.
- Try to find an example of something that does not satisfy the defining conditions.
- Write the definition in symbols.
- Negate the definition.
 - A sequence (x_n) of real numbers **diverges to infinity** (written $x_n \rightarrow \infty$) if for every $M \in \mathbb{R}$ there exists a real number N such that $n \geq N$ implies $x_n > M$.
 - A sequence is **monotone** if it is an increasing sequence or a decreasing sequence.
 - A sequence (x_n) is a **Cauchy sequence** if for all $\varepsilon > 0$ there exists a real number N such that $n, m \geq N$ implies that $|x_n - x_m| < \varepsilon$.
In addition, for this one, pretend you were talking to a high school student who loves mathematics and just *has* to know what a Cauchy sequence is but has never heard of ε and N . What would you tell him or her?

Problem 20.22. Consider the following definition.

Let $(x_n)_{n=1}^\infty$ be a sequence of real numbers and let (n_k) be a strictly increasing sequence of positive integers. The sequence (x_{n_k}) is called a **subsequence** of (x_n) . For this problem, do all the things you did in Problem 20.21, plus (a), (b), and (c) below.

- This definition says that when you choose a subsequence, you must do two things: you need to list all the x_n in order of appearance, and then you obtain the x_{n_k} by choosing one element after the other from your list, making sure that the term you choose comes after the one you just chose. How does the definition tell you that you must choose from this list? How does it tell you that you must choose in order of increasing appearance?
- Let $x_n = 1/n$. Is (x_n) a subsequence of itself? If $y_n = x_{2n}$, give a formula for y_n in terms of n . If $z_n = x_{n+4}$, give a formula for z_n in terms of n .
- How can you tell that the sequence (w_n) given by $w_n = (-1)^n/n$ is not a subsequence of (x_n) as defined in (b)?

Problem 20.23. In Problem 20.21 part (c) we defined a Cauchy sequence. Show that every convergent sequence is a Cauchy sequence.

Chapter 21

Equivalent Sets

If you were asked how many people are in your class, you would do the natural thing and count them. Thinking about this carefully, we see that what you are doing is assigning each person in the room one and only one number. If we asked whether or not there are more people in this class than were in your high school geometry class, you could certainly answer that question by comparing the two numbers.

Now suppose we look at the positive integers and the natural numbers. Which set has more elements? What should that even mean? This is a more difficult question to answer correctly than you might think. The following mathematical folktale (often attributed to Hilbert) illustrates the problem and a solution.

Suppose there is a hotel with infinitely many rooms. The hotel is completely booked when the coach of a Davis Cup team arrives. The clever manager accommodates her by moving all of the other guests to the room numbered one higher than the room they previously occupied, which clears the first room for the coach. Then the four members of the team arrive. Each must have his own room, of course. The very clever manager moves everyone up four rooms, making enough room for the four athletes. Finally, the team's infinitely many fans arrive (this happens all the time at really good hotels). The very, very clever manager accommodates all guests by moving the residents of room number n to the room with number $2n$. Now all the new people can go in the odd-numbered rooms.

An interesting commentary of this problem was given by Smilla in the book *Smilla's Sense of Snow*. She says, "What delights me about this story is that everyone involved, the guests and the owner, accept it as perfectly natural to carry out an infinite number of operations so that one guest can have peace and quiet in a room of his own. That is a great tribute to solitude."¹ [53, p. 11].

What does "Hotel Infinity" really show us? It is our aim in the next few sections to discuss and answer these questions.

To make precise what it means for two sets (even two infinite sets) to have the same number of elements, we need a definition. We say that a set A is **equivalent** to

¹ Excerpt from *Smilla's Sense of Snow* by Peter Høeg, translated by Tiina Nunnally. Translation copyright ©1993 by Farrar, Straus and Giroux, LLC. Reprinted by permission of Farrar, Straus and Giroux, LLC.

a set B if there exists a bijection $f : A \rightarrow B$. We write $A \approx B$ for A is equivalent to B . (Other authors use the words equipotent or equinumerous.)

You actually know a lot about this concept from previous chapters (particularly Chapter 15). The next result summarizes information we already have.

Theorem 21.1. *Let \mathcal{A} be a nonempty collection of sets. Equivalence between elements A and B of \mathcal{A} , as defined by $A \approx B$ above, is an equivalence relation on \mathcal{A} .*

You will be asked to prove this theorem in Problem 21.5.

Example 21.2. Show that the open interval $(0, 1)$ is equivalent to the open interval $(0, 3)$.

Proof. Define a function $f : (0, 1) \rightarrow (0, 3)$ by $f(x) = 3x$. We leave it to you to show that this function is bijective. Thus $(0, 1) \approx (0, 3)$. \square

Since the relation \approx is symmetric, we will usually say that A and B are equivalent, rather than A is equivalent to B . This concept allows us to give a precise definition of a finite set. We say that a set S is **finite** either if $S = \emptyset$ or if S is equivalent to the set $\{1, 2, 3, \dots, n\}$ for some positive integer n . Thus, to prove that a nonempty set is finite, we need to find a bijection between S and a set $\{1, 2, 3, \dots, n\}$ for some $n \in \mathbb{Z}^+$. Since the relation is symmetric, either set can serve as the domain. The bijection is the mathematical analog of what we usually describe as counting. A set is said to be **infinite** if it is not finite.

Example 21.3. By negating the definition of finite, say what it means for a set to be infinite.

A set S is infinite if it is nonempty and for every positive integer n there does not exist a bijection from S to the subset $\{1, 2, 3, \dots, n\}$. \circ

What are some examples of finite sets? By our definition, every set of the form $\{1, 2, 3, \dots, n\}$ is a finite set. What about a set like $\{2, 4, 6\}$? It certainly feels finite, but to prove that it is finite we would have to construct a bijective function. It is easy here; the function $f : \{1, 2, 3\} \rightarrow \{2, 4, 6\}$ defined by $f(n) = 2n$ certainly works. You could also define a function g on $\{1, 2, 3\}$ by $g(1) = 4, g(2) = 6$, and $g(3) = 2$. In fact, if our set has more than one element, then there is more than one choice for the bijection.

Exercise 21.4. Show that the set $\{6, 8, 10, 14\}$ is finite. \circ

The rest of this chapter is a paraphrasing of much of the work we did in Chapters 14 through 17. We isolate the important ideas below and we guide you through the proofs, but you have all the techniques to prove everything yourself.

Theorem 21.5. *The sets \mathbb{Z} and \mathbb{N} are equivalent.*

This theorem is really the essence of the story behind “Hotel Infinity.” An infinite set, \mathbb{Z} , can have a proper subset, \mathbb{N} , that has the “same number of elements” in it!

Proof. Define $f : \mathbb{Z} \rightarrow \mathbb{N}$ explicitly as follows:

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -(1+2x) & \text{otherwise} \end{cases} .$$

In Example 15.7, we showed that this function is bijective. From this we conclude that $\mathbb{Z} \approx \mathbb{N}$. □

The same techniques that were used to prove Theorem 21.5 can be used to prove the next theorem.

Theorem 21.6. *Let A, B, C , and D be nonempty sets. If $A \cap B = \emptyset$, $C \cap D = \emptyset$, $A \approx C$, and $B \approx D$, then $A \cup B \approx C \cup D$.*

Proof. [Outline of proof] Since $A \approx C$, there exists a bijective function $f : A \rightarrow C$. Similarly, since $B \approx D$, there exists a bijective function $g : B \rightarrow D$. We define a function $H : A \cup B \rightarrow C \cup D$ in cases by

$$H(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in B \end{cases} .$$

We leave it to you to show that H is well-defined and bijective. □

Exercise 21.7. What happens to our proof if $A \cap B \neq \emptyset$? If we do not assume that $A \cap B = \emptyset$, is the theorem still true? ○

For finite sets, Theorem 21.6 has an interesting consequence.

Corollary 21.8. *Let A and B be disjoint sets. If A and B are finite, then $A \cup B$ is finite.*

The proof of Corollary 21.8 is left to you in Problem 21.9.

Since the definition of equivalent sets uses bijective functions, many of the theorems you have had will come in quite handy. If you have forgotten the definition of the restriction of a function (see Definition 15.4), you will want to review it before proceeding. We’ll use restrictions in many of the proofs about finite and infinite sets.

Theorem 21.9. *Let n be a positive integer. Then every subset of $\{1, 2, 3, \dots, n\}$ is finite.*

Proof. The proof will be by induction on n .

If $n = 1$, then our set is $\{1\}$, and there are only two subsets; $\{1\}$ and \emptyset . Therefore, the result holds if $n = 1$.

We now turn to the induction step. So let $n \in \mathbb{Z}^+$ and suppose that every subset of $\{1, 2, \dots, n\}$ is finite. We must show that every subset of $\{1, 2, \dots, n+1\}$ is finite.

So consider the set $\{1, 2, \dots, n, n+1\}$, and a subset S of this set. If $S \subseteq \{1, 2, \dots, n\}$, then S is finite by our induction hypothesis. Otherwise, $n+1 \in S$. In this case, notice that $\{n+1\}$ is a finite set. Since $S \setminus \{n+1\} \subseteq \{1, \dots, n\}$ we also know from the induction hypothesis that $S \setminus \{n+1\}$ is finite. Applying Corollary 21.8 we may conclude that $S = (S \setminus \{n+1\}) \cup \{n+1\}$ is finite, completing the proof. \square

Corollary 21.10. *Let S be a finite set. Then every subset of S is finite.*

Proof. If S is empty, the result is clear. So suppose that S is nonempty, and let T denote a subset of S . Again, we may assume that T is nonempty.

By our assumption there exists $n \in \mathbb{Z}^+$ and a bijection $f: S \rightarrow \{1, 2, \dots, n\}$. By Problem 15.19, the restriction function, $f|_T$, is a bijective mapping from T onto a nonempty subset B of $\{1, 2, \dots, n\}$. From Theorem 21.9, the set B is finite, and therefore there exists a positive integer m and a bijection $g: B \rightarrow \{1, 2, \dots, m\}$. By Theorem 16.6, the composition $h = g \circ (f|_T)$ of the two bijective functions g and $f|_T$ is a bijection of T onto $\{1, 2, \dots, m\}$. Thus T is finite, completing the proof. \square

We assumed in Corollary 21.8 that the finite sets A and B were disjoint, but our intuition tells us that the union of two finite sets should be finite. How do we prove this? The idea is that the union of two sets can be expressed as the union of two disjoint sets: the intersection appears in the union twice, so to speak, so if we remove it once (from one of the sets), we haven't changed the union. That is the key to the next result.

Theorem 21.11. *The union of two finite sets is finite.*

Proof. Let A and B denote the two finite sets. Now you have already shown (in Problem 7.14) that

$$A \cup B = (A \setminus B) \cup B,$$

and it should be clear that these two sets are disjoint. By Corollary 21.10, the set $A \setminus B$ is finite. The set B is finite by assumption. Since these are two disjoint sets, we have written $A \cup B$ as the disjoint union of two finite sets and Corollary 21.8 now implies that $A \cup B$ is finite. \square

Note that in the theorem above, we showed that a set is finite without exhibiting a specific bijection. We'll be building up many results that are useful, and we will not always go back to the definition to see how to prove things. This is a great plus—proofs become shorter, and sometimes prettier and more interesting. Of course, to use the theorems, you also have to know what they are!

We conclude this chapter with a useful exercise.

Exercise 21.12. Use induction to prove the following. Let $m \in \mathbb{Z}^+$. If A_1, A_2, \dots, A_m are finite sets, then the union $\bigcup_{j=1}^m A_j$ is finite.

Definitions

Definition 21.1. A set A is **equivalent** to a set B if there exists a bijection $f : A \rightarrow B$. We write $A \approx B$ for A is equivalent to B .

Definition 21.2. A set S is **finite** if either $S = \emptyset$ or if S is equivalent to the set $\{1, 2, 3, \dots, n\}$ for some positive integer n .

Definition 21.3. A set is **infinite** if it is not finite.

Solutions to Exercises

Solution (21.4). We define $f : \{6, 8, 10, 14\} \rightarrow \{1, 2, 3, 4\}$ by $f(6) = 1$, $f(8) = 2$, $f(10) = 3$, and $f(14) = 4$. It is clear that f is a bijective function, hence $\{6, 8, 10, 14\}$ is finite.

Solution (21.7). If A and B are not disjoint, the function H may not be well-defined. In addition, if A and B are not disjoint, the conclusion of the theorem may not hold. To see this, take finite sets with $A = B = \{1\}$, $C = \{2\}$, and $D = \{3\}$.

Solution (21.12). We will prove this statement by induction on m . For the base step ($m = 1$), we get $\bigcup_{j=1}^1 A_j = A_1$, which is finite by assumption.

Now we proceed to the induction step. Let $m \in \mathbb{Z}^+$ and suppose that $\bigcup_{j=1}^m A_j$ is finite. We need to show that $\bigcup_{j=1}^{m+1} A_j$ is finite. But $\bigcup_{j=1}^{m+1} A_j = (\bigcup_{j=1}^m A_j) \cup A_{m+1}$. By the induction hypothesis, $\bigcup_{j=1}^m A_j$ is finite, and A_{m+1} is assumed to be finite. By Theorem 21.11, the union of two finite sets is finite. Thus $\bigcup_{j=1}^{m+1} A_j$ is finite. The result now follows from the principle of mathematical induction.

Problems

Problem 21.1. Show that the following intervals of real numbers are equivalent:

- (a) $[0, 1]$ and $[0, 2]$;
- (b) $[0, 1]$ and $[2, 5]$.

Problem 21.2. Prove that $\{1, \dots, 10\} \times \{1, \dots, 15\}$ is finite using only the definition of a finite set; that is, write down the relevant bijection explicitly.

Problem 21.3. Explain, in words, the difference between a “finite union of sets” and a “union of finite sets.” Give examples of each that show these really are different.

Problem# 21.4. (a) Show that the set \mathbb{Q}^+ of positive rationals and the set \mathbb{Q}^- of negative rationals are equivalent.

- (b) Show that the set of even integers and set of odd integers are equivalent.

Problem 21.5. Prove Theorem 21.1.

Problem 21.6. (a) Prove that $(0, 1) \approx \mathbb{R}$. (If you choose to use Problem 15.13, make sure you solve that problem too!)

- (b) Prove that $\mathbb{R} \approx \mathbb{R}^+$.

Problem 21.7. (a) Show that $\mathbb{Z} \approx 2\mathbb{Z}$.

- (b) Using theorems from this chapter (don't define functions!) show that $2\mathbb{Z} \approx \mathbb{N}$.

Problem 21.8. Prove Theorem 21.6 working with the outline given in the text.

Problem 21.9. (a) Suppose that A and B are nonempty finite sets and $A \cap B = \emptyset$. Show that there exist positive integers n and m such that $A \approx \{1, 2, \dots, n\}$ and $B \approx \{n + 1, \dots, n + m\}$.

- (b) Prove Corollary 21.8.

Problem 21.10. Prove Theorem 21.13 below. We suggest that you start by working Problem 16.17 if you have not already done so.

Theorem 21.13. Let A, B, C , and D be nonempty sets with $A \approx C$ and $B \approx D$. Then $A \times B \approx C \times D$.

Problem 21.11. Prove the following corollary of Theorem 21.13 above.

Corollary 21.14. Let A and B be finite sets. Then $A \times B$ is a finite set.

Problem 21.12. Let $\mathcal{A} = \{[a, b) : a, b \in \mathbb{R} \text{ and } a < b\}$ be the collection of bounded half-open intervals of real numbers.

- (a) Prove that $\mathcal{A} \approx \mathbb{R} \times \mathbb{R}^+$.
 (b) Prove that $\mathcal{A} \approx \mathbb{R} \times \mathbb{R}$.

Problem 21.13. For $j \in \mathbb{Z}^+$, let $A_j \subseteq \{1, \dots, j\}$. Suppose that for some $n \in \mathbb{Z}^+$, we have $B \subseteq \bigcup_{j=1}^n A_j$. Is B necessarily finite? Prove it or give a counterexample.

Problem 21.14. Let A be a subset of the set of all functions $f : \mathbb{R} \rightarrow \mathbb{R}$ and let $g : \mathbb{R} \rightarrow \mathbb{R}$ be a bijective function. We use the notation $gAg^{-1} = \{g \circ f \circ g^{-1} : f \in A\}$. Prove that $A \approx gAg^{-1}$.

Problem 21.15. Prove that $((\mathbb{Z}^+ \times \mathbb{N}) \cup (\mathbb{Z}^- \times \mathbb{N})) \approx \mathbb{Z} \times \mathbb{Z}$.

Problem 21.16. By Theorem 21.5, $\mathbb{Z} \approx \mathbb{N}$ and hence there is a bijection $g : \mathbb{Z} \rightarrow \mathbb{N}$.

- (a) We define $G : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{N} \times \mathbb{N}$ by $G(n, m) = (g(n), g(m))$. Prove that G is a bijection from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{N} \times \mathbb{N}$.
 (b) Explain why part (a) shows that $\mathbb{Z} \times \mathbb{Z} \approx \mathbb{N} \times \mathbb{N}$.
 (c) Show that $\mathbb{Z} \times \mathbb{Z} \approx \mathbb{N} \times \mathbb{N}$ using theorems from this chapter and without constructing a bijective function.

Problem 21.17. Let A be a nonempty finite set of integers and let \mathcal{L} be the set of all linear polynomials with coefficients in A ; that is, $\mathcal{L} = \{ax + b : a \in A \text{ and } b \in A\}$. Prove that \mathcal{L} is finite.

Problem 21.18. Let $A = \{(a_1, a_2, a_3, a_4, a_5) : a_j \in \{0, 1\} \text{ for } j \in \mathbb{Z} \text{ and } 1 \leq j \leq 5\}$. Prove that $\mathcal{P}(\{1, 2, 3, 4, 5\}) \approx A$.

Problem 21.19. Let $n \in \mathbb{Z}^+$ and define $A_n = \{(a_1, \dots, a_n) : a_j \in \{0, 1\} \text{ for } j \in \mathbb{Z} \text{ and } 1 \leq j \leq n\}$. Prove that for all $n \in \mathbb{Z}^+$ we have $\mathcal{P}(\{1, \dots, n\}) \approx A_n$. (See Problem 21.18.)

Problem 21.20. Prove that $(0, \infty) \approx [0, \infty)$.

Problem 21.21. Prove that $(0, 1) \approx [0, 1]$.

Chapter 22

Finite Sets and an Infinite Set

We have proved that sets are finite, but we have not yet shown rigorously that a set is infinite. It is not as easy as you might think to do so, nor do we have an exact notion of what it means for a finite set “to have n elements.” Our proof of the former and the definition of the latter will depend on a principle known as the *pigeonhole principle*. The pigeonhole principle is something that is familiar to all of us. As a very simple example of this, recall a childhood birthday party in which you played musical chairs. In case you weren’t invited to any parties, we’ll remind you of the rules behind the game. Let’s say there were 10 children at the party. Someone, say the child’s father, would set up 9 chairs in a row. Someone else, say the child’s mother, would play a song on the piano stopping unexpectedly at some point. When the music ended, the 10 children would scramble for the 9 seats. If everyone sat down, two people would sit in the same chair. This game is our first example of the pigeonhole principle. Now we turn to a more elaborate one.

Theorem 22.1. *Suppose that n people ($n \geq 2$) are at a party. Then there exist at least two people at the party who know the same number of people present.*

First you need to know the rules. We will assume that no one knows him- or herself. We will also assume that if x claims to know y , then y also knows x .

The idea behind the proof is this, and you can try it out at your next party. You will put n boxes on the board numbered 0 through $n - 1$. Each person counts up the number of people he or she knows at the party. You ask them that number and write their name in the box with the same number. Note that each person’s answer corresponds to exactly one of the boxes 0 through $n - 1$. The theorem claims that at least two people’s names will end up in the same box.

Proof. We imagine n boxes that are numbered 0 through $n - 1$. For an integer m with $0 \leq m \leq n - 1$, box m contains the names of the people who know m people at the party.

We break this proof into two cases. First, suppose that there is someone at the party who doesn’t know anyone. We’ll call this party crasher Ms. X . Now if we pick some other party attendee, he doesn’t know himself and, since Ms. X doesn’t know

him, he doesn't know Ms. X either. This implies that he knows at most $n - 2$ people at the party. The point is this: No one's name can be in the box labeled $n - 1$. This means that the names of the n people are in the $n - 1$ boxes labeled 0 through $n - 2$. Obviously then, there is a box with at least two names in it, indicating that two of those people know the same number of people and we are done in this case.

Now suppose that everyone knows at least one person at the party. Then no one's name can be in the box marked 0; everyone's name will be in one of the $n - 1$ boxes marked $1, \dots, n - 1$. Once again we have n names in $n - 1$ boxes, and thus at least two must be in the same box. \square

This theorem and its proof illustrate the idea behind the pigeonhole principle. In its popular form, the principle says that *if there are more pigeons than holes, then at least one hole is the home of more than one pigeon*. There are many wonderful applications of the pigeonhole principle (and many can be found at the website [13] under algebra).

We now turn to the more precise statement of the pigeonhole principle and its proof. The principle is attributed to Peter Gustav Lejeune Dirichlet and is also known as the Dirichlet principle or the Dirichlet drawer principle. (There are other Dirichlet principles; see Spotlight: Minimum or Infimum? in Chapter 17.) Curiously, this intuitively obvious principle has a rather intricate proof.

Theorem 22.2 (Pigeonhole principle). *Let m and n be positive integers with $m > n$, and let f be a map satisfying $f : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$. Then f is not one-to-one.*

Proof. We will prove this theorem by induction on n . The assertion that we will prove is: For every integer m such that $m > n$, if $f : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$, then f is not one-to-one.

For the base case, $n = 1$. Our assumption that $m > n$ implies that $m > 1$. For every map $f : \{1, \dots, m\} \rightarrow \{1\}$, it is clear that $f(1) = 1 = f(m)$. Since $1 \neq m$, we may conclude that f is not one-to-one, completing the base step.

For the induction step, let $n \in \mathbb{Z}^+$ and suppose that if m is an integer greater than n and f is a function $f : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$, then f is not one-to-one. We will show that if $m > n + 1$ and $f : \{1, \dots, m\} \rightarrow \{1, \dots, n + 1\}$, then f is not one-to-one.

So let us suppose that $m > n + 1$ and we have a map

$$f : \{1, \dots, m\} \rightarrow \{1, \dots, n + 1\}.$$

There are three cases to consider: Either f maps nothing to $n + 1$, more than one element to $n + 1$, or exactly one element to $n + 1$.

For the first case, $n + 1$ is not in the range of f , so f actually defines a map $f : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$. Since $m > n + 1 > n$, our induction hypothesis tells us that f is not one-to-one, and we are done in this case.

In case two, there exist $j, k \in \{1, \dots, m\}$ with $j \neq k$, and $f(j) = n + 1 = f(k)$. Then f is not one-to-one, and we are done in this case, too.

For the last case, we may assume that $j \in \{1, \dots, m\}$ is the only integer for which $f(j) = n + 1$. We now define the function $g : \{1, \dots, m\} \rightarrow \{1, \dots, m\}$ that interchanges m with j and leaves all other elements of $\{1, \dots, m\}$ fixed:

$$g(k) = \begin{cases} k & \text{if } k \neq j, m \\ j & \text{if } k = m \\ m & \text{if } k = j \end{cases} .$$

Then g is one-to-one. Furthermore, since j is the only integer that f maps to $n + 1$ we know that $(f \circ g)(k) = f(g(k)) = n + 1$ if and only if $g(k) = j$. Since g is one-to-one, this happens if and only if $k = m$. Thus $(f \circ g)|_{\{1, \dots, m-1\}}$ maps $\{1, \dots, m-1\}$ to $\{1, \dots, n\}$. Since we assume that $m > n + 1$, we know that $m - 1 > n$. Our induction hypothesis now applies, and we conclude that $(f \circ g)|_{\{1, \dots, m-1\}}$ is not one-to-one. By Problem 15.19 $f \circ g$ is not one-to-one. Since g is one-to-one, by Theorem 16.7 f is not one-to-one in this case either.

By the principle of mathematical induction, if $m, n \in \mathbb{Z}^+$ and $m > n$, then no function $f : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ is one-to-one. □

The proof of the pigeonhole principle summarizes much of what you learned: mathematical induction, proof in cases, and one-to-one functions.

We are now in a position to prove that a set is infinite.

Theorem 22.3. *The set \mathbb{N} is infinite.*

Proof. Suppose to the contrary that \mathbb{N} is finite. Since $\mathbb{N} \neq \emptyset$ there exists an integer m and a one-to-one mapping, g , of \mathbb{N} onto $\{1, 2, \dots, m\}$. Now $\{1, 2, \dots, m + 1\} \subseteq \mathbb{N}$, so we may consider the restriction $g|_{\{1, 2, \dots, m+1\}} : \{1, 2, \dots, m + 1\} \rightarrow \{1, 2, \dots, m\}$. The pigeonhole principle (Theorem 22.2) implies that $g|_{\{1, 2, \dots, m+1\}}$ is not one-to-one. This, in turn, implies (as you surely showed in Problem 15.19) that g is not one-to-one, contradicting our choice of g . Therefore, it must be the case that \mathbb{N} is infinite. □

Exercise 22.4. Prove that \mathbb{Z} is infinite. ○

The next exercise is similar to the one above, but requires more work.

Exercise 22.5. Prove that if X is an infinite set, then the power set of X is infinite. ○

We carefully defined what it means for a set to be finite, but so far we have not described what it means for a set to “have n elements.” After the following theorem, we will be ready to do that.

Theorem 22.6. *Let A be a nonempty finite set. There is a unique positive integer n such that $A \approx \{1, \dots, n\}$.*

Before we begin, note that there are two things to show: there exists a positive integer n with certain properties and that there is only one such integer. One of these should be easy. Which one?

Proof. The existence of some $n \in \mathbb{Z}^+$ such that there is a bijection $f : A \rightarrow \{1, \dots, n\}$ is guaranteed by the definition of a nonempty finite set. So all we have to do is show that there is no other $m \in \mathbb{Z}^+$ with an associated bijection $g : A \rightarrow \{1, \dots, m\}$.

Suppose to the contrary that there does exist such a positive integer m with $m \neq n$, and bijective function g . Since $m \neq n$, one of these integers must be larger than the other, so we assume that $m > n$. Since g is a bijection, it has an inverse. Composing the two bijective functions f and g^{-1} , we obtain a bijective function $f \circ g^{-1} : \{1, \dots, m\} \rightarrow \{1, \dots, n\}$. But this contradicts the pigeonhole principle, and we conclude that n is unique. \square

The integer n in the above theorem is exactly what we mean by the “size of A ” or “number of elements in A .” We will say that the **cardinality** of a finite set A is 0 if A is empty and n if $A \approx \{1, \dots, n\}$. In symbols, we write $|A| = n$, where $n \in \mathbb{N}$. (Why couldn’t we define the cardinality of a set before we proved the theorem?) While it is possible to define cardinality in more generality, we have only defined it in the case that A is finite.

Definition

Definition 22.1. The **cardinality** of a finite set A is 0 if A is empty and n if $A \approx \{1, \dots, n\}$. In symbols, we write $|A| = n$, where $n \in \mathbb{N}$.

Solutions to Exercises

Solution (22.4).

Proof. We know that $\mathbb{N} \subset \mathbb{Z}$, and Theorem 22.3 tells us that \mathbb{N} is infinite. Since Corollary 21.10 says that every subset of a finite set is finite, our set \mathbb{Z} must be infinite. \square

Solution (22.5).

Proof. Define a map $f : X \rightarrow \mathcal{P}(X)$ by $f(x) = \{x\}$ for all $x \in X$. It is clear that f is well-defined and one-to-one. Therefore, f maps X onto a subset, \mathcal{A} , of $\mathcal{P}(X)$. Since X is infinite and f is a bijection of X onto \mathcal{A} , we know that \mathcal{A} must be infinite as well. Thus, \mathcal{A} is an infinite subset of $\mathcal{P}(X)$, and we may use Corollary 21.10 to conclude that $\mathcal{P}(X)$ is infinite. \square

Problems

Problem 22.1. Consider the story of n people at a party in Theorem 22.1. Suppose someone else has a rival party the same evening, and no one can attend both. Some-

one takes a picture of the people at the rival party and shows it to everyone at your party. Your party isn't that much fun, so you each look at the picture and say how many people you know at the other party. No one says the same number. What can you conclude about the number of people attending the other party?

Problem 22.2. (a) Suppose there are 15 people in a class. Show that two people must be born in the same month.

(b) A conductor has just taken on a new job in a small town where he has five trumpet players in his orchestra. He has a concert every other evening for his first year. Traditionally the players are seated from left to right in order of decreasing musical ability. The conductor does not want to offend the players, so he has decided to seat them differently at each performance. Can he do it? Why or why not?

Problem 22.3. Suppose 21 numbers are chosen from the set $\{1, \dots, 40\}$. Show that among the chosen numbers there are (at least) two of them, n and m , such that $n - m = 1$.

Problem 22.4. Let S be a region in the plane bounded by a square with sides of length two. Prove that if we put five points in S , there exist (at least) two of these points that are at most a distance of $\sqrt{2}$ apart.

Problem 22.5. Let $n \in \mathbb{N}$ and let $f : \{1, 2, \dots, 2n + 1\} \rightarrow \{1, 2, \dots, 2n + 1\}$ be a bijective function. Prove that for some odd integer $k \in \{1, 2, \dots, 2n + 1\}$, the integer $f(k)$ is also odd.

Problem 22.6. Let $f : \{1, 2, \dots, 99\} \rightarrow \{1, 2, \dots, 99\}$ be an injective function. Define $g : \{1, 2, \dots, 99\} \rightarrow \mathbb{N}$ by $g(n) = n + f(n)$. Prove that there exists an integer n such that $g(n)$ is even.

Problem 22.7. Prove the following alternate form of the pigeonhole principle.

Let A and B be nonempty finite sets, and suppose that $|A| > |B|$. If $f : A \rightarrow B$ is a function, then f is not one-to-one.

Problem[#] 22.8. Show that \mathbb{Q} is infinite.

Problem 22.9. Using only the definition of finite and the pigeonhole principle, prove that \mathbb{R} is infinite.

Problem 22.10. Let A be a set, and suppose that B is an infinite subset of A . Show that A must be infinite.

Problem 22.11. Suppose that A is an infinite set, B is a finite set, and $f : A \rightarrow B$ is a function. Show that there exists $b \in B$ such that $f^{-1}(\{b\})$ is infinite.

Problem 22.12. Let X be an infinite set, and A and B be finite subsets of X . Answer each of the following, giving reasons for your answers:

(a) Is $A \cap B$ finite or infinite?

- (b) Is $A \setminus B$ finite or infinite?
- (c) Is $X \setminus A$ finite or infinite?
- (d) Is $A \cup B$ finite or infinite?
- (e) If $f : A \rightarrow X$ is a one-to-one function, is $f(A)$ finite or infinite?

Problem 22.13. Let A, B , and C be finite sets.

- (a) Recall that we showed that if A and B are disjoint, then $A \cup B$ is finite. Look over the proof outlined in Problem 21.9 and determine $|A \cup B|$ in terms of $|A|$ and $|B|$, assuming that A and B are disjoint.
- (b) Suppose that A and B are not disjoint. Show that $|A \cup B| = |A| + |B| - |A \cap B|$.
- (c) Find a formula that works for three sets A, B , and C . (You don't need to prove that your formula works.)

Problem 22.14. (a) Suppose that A and B are finite sets with $|A| = m$ and $|B| = n$. In Problem 21.11 you showed that if A and B are finite, then $A \times B$ is finite. Look over the proof and determine $|A \times B|$ in terms of m and n .

- (b) Suppose that A_1, A_2, \dots, A_k are finite sets. Guess a formula for the cardinality of $A_1 \times A_2 \times \dots \times A_k$ (in terms of $|A_1|, |A_2|, \dots$, and $|A_k|$). Prove that your formula is correct.

Problem 22.15. Prove that if X is a finite set with $|X| = n \in \mathbb{N}$, then $|\mathcal{P}(X)| = 2^n$.

Problem 22.16. Each of the problems below is an application of one of the counting principles given in Problems 22.13 and 22.14. Decide which part of that problem applies, and use it to answer the problem.

- (a) Thirty second-graders, twenty-five third-graders, and fifteen fourth-graders entered an art contest. Three prizes were awarded, one for each grade. In how many ways can the prizes be awarded to three of the children? (Don't forget to say which formula from Problem 22.13 or 22.14 applies.)
- (b) Suppose that there are 100 people in a room. Of these 55 are men, 33 are Swiss, 10 are Swiss males. How many are Swiss or male (or both)? (Don't forget to say which formula from Problem 22.13 or 22.14 applies.)

The rest of the problems are interrelated. If you can't see how to do the problem you are working on, look at the results from the previous problems and Problem 22.13.

Problem 22.17. Let A be a nonempty finite set with $|A| = n$ and let $a \in A$. Prove that $A \setminus \{a\}$ is finite and $|A \setminus \{a\}| = n - 1$.

Problem 22.18. (a) Suppose that A is a finite set and $B \subseteq A$. We showed that B is finite. Show that $|B| \leq |A|$.

- (b) Suppose that A is a finite set and $B \subseteq A$. Show that if $B \neq A$, then $|B| < |A|$.
- (c) Show that if two finite sets A and B satisfy $B \subseteq A$ and $|A| \leq |B|$, then $A = B$.

Problem 22.19. Suppose that A and B are finite sets and $f : A \rightarrow B$ is one-to-one. Show that $|A| \leq |B|$.

Problem 22.20. Let A and B be sets with A finite. Let $f : A \rightarrow B$. Prove that $|\text{ran}(f)| \leq |A|$.

Problem 22.21. Let A be a finite set. Show that a function $f : A \rightarrow A$ is one-to-one if and only if it is onto. Is this still true if A is infinite?

Chapter 23

Countable and Uncountable Sets

I see it but I do not believe it.—Georg Cantor [59, p. 997]

Having mastered finite sets, we now turn to understanding the infinite. We know that \mathbb{N} is infinite, and we know that \mathbb{Q} is infinite (see Problem 22.8). Are they equivalent? In some sense, we can count \mathbb{N} and it may feel as though we cannot count \mathbb{Q} —that is, as though we cannot list a first element, second element, third element, and so on. However, we shall see that \mathbb{Q} and \mathbb{N} are, in fact, equivalent.

An infinite set A is said to be **countably infinite** if $A \approx \mathbb{N}$. In Chapter 21 we showed that $\mathbb{Z} \approx \mathbb{N}$ and $2\mathbb{Z} \approx \mathbb{N}$, so these also are countably infinite. It is also easy to show that $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\} \approx \mathbb{N}$. A set is **countable** if it is either finite or countably infinite. A set is said to be **uncountable** if it is not countable. Note that if we only know that a set is countable, we don't necessarily know if it is finite or infinite. If we have an infinite countable set, it automatically is equivalent to \mathbb{N} .

Exercise 23.1. Let A and B be two countably infinite sets. Prove that there is a bijection of A onto B .

Theorem 23.2. *Every subset of \mathbb{N} is countable.*

The proof of this theorem will be presented as an exercise in reading mathematics.

Exercise 23.3. This is an exercise in reading a proof. We ask that as you read you pretend that the set T (appearing in the proof) is the set of prime numbers. Of course, you are not allowed to pick a particular subset, call it T , and conclude that you have proved the theorem. However, for the purpose of understanding someone else's proof, this might be quite helpful. We will call this set the demo, and denote it by T . Whenever you see (?) you should figure out what happens for this set. If at the end you remain largely unsatisfied, pick another set for T and try again. No matter what, you'll understand more of the proof than if you hadn't tried anything at all. So read the proof, think about the question marks, and then answer the set of questions provided below.

- (a) In the statement of Theorem 18.6 a function f appears. What is this function in the proof (when the demo set T is used)?
- (b) Find $g(0), g(1), \dots, g(5)$ in the demo. What is the subset of T that is used to define $g(6)$ in our demo? What is $g(6)$ (when you use the demo set T to define $g(6)$)?
- (c) For one-to-one, we thought we had to show that if $g(j) = g(\ell)$, then $j = \ell$. What's going on in this proof?
- (d) Say $t = 19$. What element is mapped to t when the demo set is used? \circ

Before proceeding with our proof, we give a sense of the idea behind it: If T is an infinite subset of \mathbb{N} , we will construct a function $g : \mathbb{N} \rightarrow T$ recursively, listing the elements of T in increasing order. Since the list is strictly increasing, g will be one-to-one. And, since the list is constructed to look at what has been chosen and then move on to the next largest number in T , the function g will also be onto. This part of the proof will require some work, however, and we will proceed as follows: We will suppose that g is not onto. The well-ordering principle will allow us to conclude that there is a smallest element in T that is not in the range of g . However, g will be constructed in a way that will not allow us to “skip over” elements of T and so we will obtain a contradiction. We now make these ideas precise.

Note that the (?)’s in this proof refer to Exercise 23.3. Once you have worked through the exercise, you should be able to read through the proof, ignoring the symbol (?) as you read.

Proof. Let T denote a subset of \mathbb{N} . If T is finite, it is countable and we are done. (?) We suppose, then, that T is infinite and show that it is countably infinite. To this end we construct a bijection $g : \mathbb{N} \rightarrow T$ recursively.

Since T is a nonempty subset of \mathbb{N} , the well-ordering principle implies that T has a least element. We set $g(0) = \min T$. (?) Note that for any $t \in T$ we can write $T = \{x \in T : x \leq t\} \cup \{x \in T : x > t\}$. (?) Since $\{x \in T : x \leq t\} \subseteq \{0, \dots, t\}$, we may use Theorem 21.9 to conclude that $\{x \in T : x \leq t\}$ is finite. Since T is infinite, Theorem 21.11 implies that $\{x \in T : x > t\}$ is infinite for every $t \in T$. (?) In particular, the set $\{x \in T : x > t\}$ is nonempty for every $t \in T$ and contains a minimum by the well-ordering principle. Thus, we can define $g(n+1) = \min\{x \in T : x > g(n)\}$. (?) By the recursion theorem, Theorem 18.6, the function $g : \mathbb{N} \rightarrow T$ is well-defined.

In order to prove that our function g is one-to-one we first show that if $k \in \mathbb{N}$ and $n \in \mathbb{Z}^+$, then $g(k+n) > g(k)$. To show this we use induction on n . By definition, $g(k+1) = \min\{x \in T : x > g(k)\} > g(k)$. (?) This concludes the base step. For the induction step, we let $n \in \mathbb{Z}^+$ and suppose that $g(k+n) > g(k)$. Then $g(k+n+1) = \min\{x \in T : x > g(k+n)\} > g(k+n)$. (?) By the induction hypothesis we get $g(k+n+1) > g(k)$. The result follows by induction. It is now immediate that if $j \neq \ell$, then $g(j) \neq g(\ell)$ (in Exercise 23.3 part (c) you are asked to provide the details for this claim). Hence g is one-to-one.

Finally, we show that the function g is onto. Suppose to the contrary that it is not. Then the set $S = \{x \in T : x \notin \text{ran}(g)\}$ is nonempty. By the well-ordering principle,

since S is a subset of \mathbb{N} it contains a least element. Call this element $a(?)$, and note that a is simply the smallest element in T that is not in the range of g , and therefore everything strictly smaller than a (and in T) is in the range of g . If $a = \min T$, then $a = g(0)$, which is not possible. Hence the set $\{x \in T : x < a\} \neq \emptyset$. This set is also bounded above (by a), and by Problem 12.18 it has a maximum, which we call $b.(?)$ Since $b = \max\{x \in T : x < a\}$, we know that b is strictly smaller than a and so b is in the range of g . Therefore, there exists $n \in \mathbb{N}$ with $g(n) = b$. Now there can be nothing in T between a and b , so $\{x \in T : x > b\} = \{x \in T : x \geq a\}$, and we have

$$\begin{aligned} g(n+1) &= \min\{x \in T : x > g(n)\} \\ &= \min\{x \in T : x > b\} = \min\{x \in T : x \geq a\}.(?) \end{aligned}$$

Therefore $g(n+1) = a$, contradicting our choice of $a \in S$, so g is onto.

Since g is a bijection, T is also countable if it is infinite. □

As you read the theorems and corollaries below, think about whether or not you know a corresponding result for finite sets. If so, what was the proof? Do the ideas from those proofs help you here? Why or why not? We leave the corollaries for you to prove in Problems 23.9 and 23.10.

Corollary 23.4. *Every subset of a countable set is countable.*

Remember that when we say that a set is countable, we mean that it is finite or countably infinite. The next exercise will often allow you to handle both cases at once.

Exercise 23.5. Prove that a nonempty set A is countable if and only if there exists a one-to-one function $f : A \rightarrow \mathbb{N}$. ○

Theorem 23.6. *Suppose that A and B are countable. Then $A \cup B$ is countable.*

Our proof begins with something we have used several times before.

Proof. If $A \subseteq B$ or $B \subseteq A$, the result is clear. So suppose that $A \setminus B$ and $B \setminus A$ are both nonempty. Now note that $A \cup B = A \cup (B \setminus A)$ and $A \cap (B \setminus A) = \emptyset$. Since $B \setminus A \subseteq B$, Corollary 23.4 implies that $B \setminus A$ is countable. Further, A and $B \setminus A$ are countable, so by Exercise 23.5 there exist one-to-one functions f and g such that $f : A \rightarrow \mathbb{N}$ and $g : B \setminus A \rightarrow \mathbb{N}$. Define $H : A \cup B \rightarrow \mathbb{N}$ by

$$H(x) = \begin{cases} 2f(x) & \text{if } x \in A \\ 2g(x) + 1 & \text{if } x \in B \setminus A \end{cases} .$$

You can check (as you have many times before) that H is well-defined and one-to-one. Using Exercise 23.5 once again, we conclude that $A \cup B$ is countable. □

Corollary 23.7. *The union of finitely many countable sets is countable.*

In the next theorem, we want to show that $\mathbb{N} \times \mathbb{N}$ is equivalent to \mathbb{N} . It is oh, so tempting to go to the definition and try to define a function that is a bijection from our set onto \mathbb{N} ; after all, that is the definition of equivalence. But if we do everything using definitions, we will not be taking advantage of the useful body of mathematics we have proved thus far, and we will have to re-prove everything we have done. Some of it was quite difficult to prove! Life will be much easier if we think about the theorems we have proved already and see when and how we can use them.

Theorem 23.8. *The set $\mathbb{N} \times \mathbb{N}$ is countable.*

Proof. We show that $\mathbb{N} \times \mathbb{N}$ is countable by defining a function $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ explicitly. So, let $f(n, m) = 2^n 3^m$ for all $(n, m) \in \mathbb{N} \times \mathbb{N}$. This is clearly a well-defined function. (Note that this function is not onto, since a number like 7 is not in the range. Therefore, we will not try to show that f is a bijection between $\mathbb{N} \times \mathbb{N}$ and \mathbb{N} .) Since the prime factorization of a natural number is unique, the function is one-to-one. Thus we have a one-to-one mapping $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$. By Exercise 23.5, we conclude that $\mathbb{N} \times \mathbb{N}$ is countable. \square

Though we did not say so explicitly, $\mathbb{N} \times \mathbb{N}$ is infinite. Therefore, what we have shown is that $\mathbb{N} \times \mathbb{N}$ is equivalent to \mathbb{N} .

Exercise 23.9. Let A be a finite set and let B be a countable set. Prove that $A \times B$ is countable. \circ

Corollary 23.10. *If A and B are countable sets, then $A \times B$ is countable.*

Assuming you were paying attention to all the previous results, this will not be hard to prove (see Problem 23.11).

We are now ready for the two main theorems of this chapter. After all this work, we can finally show that the set of rational numbers is countably infinite.

Theorem 23.11. *The set of rational numbers, \mathbb{Q} , is countably infinite.*

What follows is a natural way to attempt to prove this. It is, unfortunately, incorrect. But it's worthwhile to present it, see what goes wrong, and fix it.

Not a proof. The rationals can be thought of as p/q where p and q are integers with $q \neq 0$. Thus, we can define a map from \mathbb{Q} to $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by $f(p/q) = (p, q)$. Then f is bijective, so $\mathbb{Q} \approx \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. By Corollary 23.10, the latter set is countable. Thus we conclude that \mathbb{Q} is countable. \square

As we mentioned (though not quite this dramatically) there's a *HUGE* error in this proof. Find it, fix it, and then read on and see if you really figured it out.

The problem above was that the function was not well-defined. So let's try again. In the proof below, we begin by considering the positive rationals so that we don't have to worry about whether to put the minus sign in the numerator or denominator.

Proof. [Proof; the real thing] We will begin by showing that \mathbb{Q}^+ is countable. We define $f: \mathbb{Q}^+ \rightarrow \mathbb{N} \times \mathbb{N}$ as follows. Write each member of \mathbb{Q}^+ as p/q where $p, q > 0$ and p/q is in reduced form; that is, p and q have no positive common factor other than 1. Now define $f(p/q) = (p, q)$. Because p/q is in reduced form, f is well-defined and one-to-one. Since $\mathbb{N} \times \mathbb{N}$ is countable (Theorem 23.8), and $f(\mathbb{Q}^+)$ is a subset of it, we know from Corollary 23.4 that $f(\mathbb{Q}^+)$ is countable. We conclude that \mathbb{Q}^+ is countable. Now the set of negative rationals, \mathbb{Q}^- , is equivalent to \mathbb{Q}^+ . Since $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$, and we have a finite union of countable sets, we use Corollary 23.7 to conclude that \mathbb{Q} is countable. Since \mathbb{Q} is infinite we know that it is countably infinite. \square

Looks like we live in a countable world! Not quite—it's time to give an example of an uncountable set. The next theorem will show that the set of real numbers is uncountable.

There's one sticky point in our proof that the reals are uncountable. We will use the decimal representation of real numbers in $(0, 1)$. Thus, a word about decimal expansions is in order here. Each element of $(0, 1)$ has a decimal representation; that is, for $x \in (0, 1)$, there exist integers $a_1, a_2, \dots, a_n, \dots$ with $0 \leq a_n \leq 9$ such that $x = 0.a_1a_2\dots a_n\dots$. In Problem 20.15, we showed that $0.999\dots = 1.000\dots$. This means that the number 1 has two representations. In fact, many numbers in $(0, 1)$ have two decimal representations. It can be shown, however, that the only time this can happen is when the representations are of the form $0.a_1a_2a_3\dots a_n999\dots$ for some $n \in \mathbb{Z}^+$, or $0.a_1a_2a_3\dots a_m1000\dots$ for some $m \in \mathbb{Z}^+$. When given a choice, we will always choose the representation ending with repeated 9's. (See also Problem 20.18.)

Theorem 23.12. *The set of real numbers, \mathbb{R} , is uncountable.*

The idea of this proof is due to Georg Cantor and is called Cantor's diagonal argument.

Proof. We will suppose, to the contrary, that \mathbb{R} is countable and see what happens. Since every subset of a countable set is countable, the open interval $(0, 1)$ must be countable, too. Since $(0, 1)$ is clearly infinite, and we have shown that \mathbb{Z}^+ is countably infinite, there exists a bijective function $f: \mathbb{Z}^+ \rightarrow (0, 1)$. We will list the values of f using the decimal expansion of each element of $(0, 1)$. So,

$$\begin{aligned} f(1) &= 0.a_{11}a_{12}a_{13}\dots \\ f(2) &= 0.a_{21}a_{22}a_{23}\dots \\ f(3) &= 0.a_{31}a_{32}a_{33}\dots \\ &\vdots \end{aligned}$$

where each a_{ij} represents an integer between 0 and 9. Since f is onto, each number in $(0, 1)$ appears in this list.

The odd thing is this: we can construct a number $b = 0.b_1b_2\dots \in (0, 1)$ not in this list (hence showing that our function cannot possibly be onto) by describing its

decimal representation as follows. Look at $f(1)$. If $a_{11} = 2$, let $b_1 = 3$. If, on the other hand, $a_{11} \neq 2$, define $b_1 = 2$. Then the first digits of $f(1)$ and b are different, so b is not $f(1)$. For b_2 , if $a_{22} = 2$, let $b_2 = 3$. If, on the other hand, $a_{22} \neq 2$, define $b_2 = 2$. Then the second digits of b and $f(2)$ are different. So b is not $f(2)$. Now compare the element b we have constructed with the list below:

$$\begin{aligned} f(1) &= 0.\mathbf{a}_{11}a_{12}a_{13}\dots \\ f(2) &= 0.a_{21}\mathbf{a}_{22}a_{23}\dots \\ f(3) &= 0.a_{31}a_{32}\mathbf{a}_{33}\dots \\ &\vdots \\ f(n) &= 0.a_{n1}a_{n2}a_{n3}\dots\mathbf{a}_{nn}\dots \\ \\ b &= 0.\mathbf{b}_1\mathbf{b}_2\mathbf{b}_3\dots \end{aligned}$$

We constructed b so that $b_n \neq a_{nn}$, and therefore $b \neq f(n)$ for every n . Then b can't be in our list, which is a bit bizarre since we claim to have numbered all the elements in $(0, 1)$, and b is certainly one of the things we numbered. This contradiction must mean that we have assumed falsely that \mathbb{R} is countable. \square

A word of caution: students often forget that some of the theorems proved in previous chapters and some of the definitions only apply to finite sets. Since the notion of finite and infinite is often counterintuitive, you really must make sure that you check the hypotheses of the theorems you wish to apply *before* you apply the theorems.

Reactions to Cantor's work in set theory were mixed (see, for example, [59, p. 1003]). Leopold Kronecker opposed Cantor's theory and so did Henri Poincaré (see Spotlight: The Continuum Hypothesis on page 270). In a discussion of Cantor's work, Poincaré [83] said, "For my part, and I am not alone, I think that the important thing is never to introduce objects other than those that can be completely defined in a finite number of words."¹ Hilbert and Russell praised Cantor's work. In his memorial speech for Hermann Minkowski, Hilbert points out that Minkowski was the first mathematician of their time who understood the importance of Cantor's work. He quotes Minkowski as saying, "History will call Cantor one of the most profound mathematicians of our time; it is truly regretful that a very prominent mathematician [here Hilbert tells us that this mathematician is Kronecker] led an opposition not based entirely upon factual grounds, which spoiled Cantor's pleasure in his scientific investigations."¹

Definitions

Definition 23.1. An infinite set A is said to be **countably infinite** if $A \approx \mathbb{N}$.

¹ The translation is ours.

Definition 23.2. A set is **countable** if it is either finite or countably infinite. A set is said to be **uncountable** if it is not countable.

Solutions to Exercises

Solution (23.1).

Proof. Since A and B are countably infinite, we know that $A \approx \mathbb{N}$ and $B \approx \mathbb{N}$. By the transitivity (and symmetry) of the relation \approx , we may conclude that $A \approx B$. By the definition of this equivalence relation, there exists a bijective function f mapping A onto B . \square

Solution (23.3).

- (a) For the demo, $f : T \rightarrow T$ is defined by $f(t) = \min\{x \in T : x > t\}$.
- (b) $g(0) = 2, g(1) = 3, g(2) = 5, g(3) = 7, g(4) = 11, g(5) = 13$. The subset of T used is $\{x \in T : x > g(5)\} = \{x \in T : x > 13\} = \{17, 19, 23, \dots\}$. Thus $g(6) = \min\{17, 19, 23, \dots\} = 17$.
- (c) Suppose that $j \neq \ell$. We may assume that $j < \ell$. We showed that this implies that $g(j) < g(\ell)$. Hence $g(j) \neq g(\ell)$. This is the contrapositive of the statement in the question, and therefore the statement “if $g(j) = g(\ell)$, then $j = \ell$ ” is true as well.
- (d) From the list in part (b) we deduce that $19 = g(7)$.

Solution (23.5). First suppose that A is countable. If A is finite, then since $A \neq \emptyset$ there exists an integer n and a bijection $f : A \rightarrow \{1, 2, \dots, n\}$. In particular, f is a one-to-one mapping of A into \mathbb{N} . So we have found our f , if A is finite. If A is infinite, then A is countably infinite. Therefore, there is a bijection $f : A \rightarrow \mathbb{N}$. Thus, in both cases, we have a one-to-one mapping $f : A \rightarrow \mathbb{N}$.

Now suppose that we have a one-to-one mapping f of A into \mathbb{N} . Then f maps A onto its range. Therefore $A \approx \text{ran}(f)$. But $\text{ran}(f)$ is a subset of \mathbb{N} , and by Theorem 23.2 we know that it must be countable. Thus A is countable, as desired.

Solution (23.9). Here’s one way to prove this:

Proof. If $A = \emptyset$, then $A \times B$ is empty and we are done. Otherwise there exists a positive integer n and a bijective function $f : \{1, 2, \dots, n\} \rightarrow A$. Thus we may write $A \times B$ as a union: $A \times B = \bigcup_{j=1}^n (\{f(j)\} \times B)$. It is easy to check that for each j the function $g_j : B \rightarrow \{f(j)\} \times B$ defined by $g_j(b) = (f(j), b)$ is a bijection. Therefore, $\{f(j)\} \times B$ is countable for each j . Thus, we have written $A \times B$ as a finite union of countable sets, and by Corollary 23.7 we know that a finite union of countable sets is countable. Thus $A \times B$ is countable. \square

Problems

Problem 23.1. Give an example, if possible, of each of the following:

- (a) a countably infinite collection of pairwise disjoint finite sets whose union is countably infinite (see Problem 8.18 for the definition of pairwise disjoint);
- (b) a countably infinite collection of nonempty sets whose union is finite;
- (c) a countably infinite collection of pairwise disjoint nonempty sets whose union is finite.

Problem 23.2. Which of the following sets are finite? countably infinite? uncountable? (Be careful—don't apply theorems for finite sets to infinite sets and don't apply theorems for countable sets to uncountable sets!) Give reasons for your answers for each of the following:

- (a) $\{1/n : n \in \mathbb{Z} \setminus \{0\}\}$;
- (b) $\mathbb{R} \setminus \mathbb{N}$;
- (c) $\{x \in \mathbb{N} : |x - 7| > |x|\}$;
- (d) $2\mathbb{Z} \times 3\mathbb{Z}$.

Problem 23.3. For each of the following sets decide whether it is countable or uncountable and justify your answer:

- (a) The set of all lines with rational slopes;
- (b) $\mathbb{Q} \setminus \{0\}$;
- (c) $\mathbb{N} \setminus \{1, 3\}$;
- (d) $\{(x, y) \in \mathbb{R} \times \mathbb{R} : x + y = 1\}$;
- (e) $[0, \infty)$.

Problem 23.4. Is the set of all infinite sequences of 0's and 1's finite, countably infinite, or uncountable? Guess and then prove, please.

Problem 23.5. Suppose that $A \subseteq B \subseteq C$, that the sets A and C are equivalent, and that C is countable. Is $A \approx B$? Prove or give a counterexample.

Problem 23.6. (a) Give an example of two sets A and B , such that $B \subseteq A$ and $B \approx A$, but $B \neq A$.

- (b) Prove that if A is a countably infinite set, then there is always a subset B of A such that $B \subset A$ and $B \approx A$.
- (c) Prove that if A is an uncountable set, then there is always a subset B of A such that $B \subset A$ and B is also uncountable.
- (d) Prove that if A is a finite set, $B \subseteq A$, and $B \approx A$, then $B = A$.

Problem 23.7. Prove that a set A is uncountable if there is an injective function $f : (0, 1) \rightarrow A$.

Problem 23.8. (a) Let $X, Y \subseteq \mathbb{R}$. Suppose that $f : X \rightarrow Y$ is a function with the property that for all $x, y \in X$, if $x < y$, then $f(x) < f(y)$. Prove that f is one-to-one.

(b) Suppose that $g : \mathcal{P}(\{1, 2\}) \rightarrow \mathcal{P}(\{1, 2, 3\})$ is a function with the property that for all $A, B \in \mathcal{P}(\{1, 2\})$, if $A \subset B$, then $g(A) \subset g(B)$. Is g necessarily one-to-one? Prove it or give an example of g that is not one-to-one.

Problem 23.9. Prove Corollary 23.4.

Problem 23.10. Prove Corollary 23.7. To do this, note that the corollary can be restated a bit more formally as follows. If for some positive integer n , we have n sets A_1, \dots, A_n , and each one is countable, then $\bigcup_{i=1}^n A_i$ is countable.

Problem 23.11. Prove Corollary 23.10.

Problem 23.12. There is another way to show that \mathbb{Q} is countable. Turn the outline below into a proof by describing the counting process. (Don't try to find a formula for the function.)

Proof. [Outline of proof] The proof is simplest if we show that the set of positive rationals, \mathbb{Q}^+ , is countably infinite. You showed in the exercises (and it is easy to see) that $\mathbb{Q}^- \approx \mathbb{Q}^+$. Then $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^- \cup \{0\}$ is infinite and countable, so $\mathbb{Q} \approx \mathbb{N}$. So we will restrict our attention to \mathbb{Q}^+ . To see that \mathbb{Q}^+ is countable, we will make a chart of all the fractions of the form m/n where m and n are positive integers; that is, we consider the following array of numbers:

$$\begin{array}{ccccccc}
 1 & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \dots & & \\
 & \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \dots & \\
 & & \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \dots \\
 & & & \frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \dots \\
 & & & & \dots & \dots & \dots & \dots
 \end{array}$$

Try counting the elements in the array in an orderly fashion. Make sure you don't count numbers twice! □

Problem 23.13. The set $\mathbb{Z}[\sqrt{-5}]$ is a subset of the complex numbers defined by $\mathbb{Z}[\sqrt{-5}] = \{a + \sqrt{5}bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, and it is called a quadratic integer ring. Is $\mathbb{Z}[\sqrt{-5}]$ countable or uncountable? Prove your answer.

Problem 23.14. Let $n \in \mathbb{Z}^+$ and denote by $\mathbb{N}^n = \mathbb{N} \times \mathbb{N} \times \dots \times \mathbb{N}$ (n times). Prove that \mathbb{N}^n is countable for all $n \in \mathbb{Z}^+$.

Problem 23.15. We denote by $\mathbb{N}^\infty = \{(a_1, a_2, a_3, \dots) : a_j \in \mathbb{N} \text{ for all } j \in \mathbb{Z}^+\}$. Prove that \mathbb{N}^∞ is uncountable.

Problem 23.16. Let X and Y be two nonempty finite sets and denote by $\mathcal{F}(X, Y)$ the set of all functions $f : X \rightarrow Y$. Is $\mathcal{F}(X, Y)$ finite, countably infinite, or uncountable? Prove your answer.

Problem 23.17. Prove that the set $A = \{m^2 : m \in \mathbb{Z}\}$ is countably infinite.

Problem 23.18. Prove that if $A \cap B = \emptyset$, then $\mathcal{P}(A \cup B) \approx \mathcal{P}(A) \times \mathcal{P}(B)$.

Problem 23.19. Prove the following equivalences:

- (a) $(0, 1) \approx [0, 1)$ and
- (b) $(0, 1) \approx (0, 1/2) \cup [1, 2)$.

Problem 23.20. Prove the following generalization of Exercise 21.12.

Theorem 23.13. *If A_j is finite for all $j \in \mathbb{Z}^+$, then $\bigcup_{j \in \mathbb{Z}^+} A_j$ is countable.*

Note that induction will not work here. We suggest that you adapt the ideas of the alternate proof of Theorem 23.11 outlined in Problem 23.12. As a second note, we mention that this theorem could be generalized to allow the sets A_j to be countable. However, a proof of this has a subtlety and requires something we have not yet discussed—something known as the axiom of choice. See Project 29.12.

Problem 23.21. Prove that the set of all decreasing functions from \mathbb{N} to \mathbb{N} is countable.

Chapter 24

The Cantor–Schröder–Bernstein Theorem

No one shall be able to chase us out of the paradise that Cantor created for us.¹—David Hilbert [52, p. 170]

Suppose we have two finite sets. We have developed enough machinery to tell when one set has more elements than another. But what about infinite sets? For example, we might consider \mathbb{N} and \mathbb{Z}^+ , and we may ask which one has more elements. Well, we have already developed mathematical concepts that convince us that these two sets have the same number of elements. In this chapter, we investigate the situation for general infinite sets.

The next few definitions will seem natural, but there's more to them than meets the eye! Given two sets A and B , we say that they are of **equal cardinality**, written $|A| = |B|$, if the sets are equivalent. Recall that this means that there is a bijective function $f : A \rightarrow B$. For two sets, A and B we say that the **cardinality of A is less than or equal to the cardinality of B** , written $|A| \leq |B|$, if there is an injection $f : A \rightarrow B$. If our two given sets A and B satisfy $|A| \leq |B|$ and $|A| \neq |B|$, then we say that the **cardinality of A is less than the cardinality of B** and we will write $|A| < |B|$.

As we mentioned above, we have already said what it means for two finite sets A and B to satisfy $|A| = |B|$ or $|A| \leq |B|$, because according to Definition 22.1 the cardinality of a finite set is a natural number and we understand when one natural number is smaller than or equal to another. Does our notion of \leq , defined above for general sets A and B , agree with our definition of \leq for the cardinality of two finite sets? Of course it does! You will have the opportunity to show this in Problem 24.6.

Exercise 24.1. Explore the definitions above for \mathbb{Z} and \mathbb{R} : Is $|\mathbb{Z}| \leq |\mathbb{R}|$? Is $|\mathbb{Z}| < |\mathbb{R}|$? ○

Exercise 24.2. Explore the definitions above for \mathbb{Z} and $\mathcal{P}(\mathbb{Z})$: Is $|\mathbb{Z}| \leq |\mathcal{P}(\mathbb{Z})|$? ○

¹ The translation is ours.

In the exercise above, we didn't ask you whether $|\mathbb{Z}| < |\mathcal{P}(\mathbb{Z})|$. Before you read on, think about it. The longer you think about this question, the easier it will be to follow the proofs below.

We would like our cardinality relation to have the usual nice properties of a partial order. The relation is a partial order, but it's going to require some work on our part to prove this. (In fact, it is a total order, but you will need to work Project 29.12 in order to see this!)

We have many examples of finite sets and many examples of countably infinite sets. We don't, however, have a long list of uncountable sets that are intrinsically different from \mathbb{R} . We'll fix that by proving the theorem below.

Theorem 24.3 (Cantor). *For any set X , we have $|X| < |\mathcal{P}(X)|$.*

The main part of the proof will be to show that there is no bijection between X and $\mathcal{P}(X)$. Before we turn to this, let's think about whether or not we've seen something like this before. Have we seen a proof in which we showed that there is no bijection between two infinite sets? Absolutely: When we showed that \mathbb{R} is uncountable, we used *Cantor's diagonal argument*. Take a moment to look back at the proof of Theorem 23.11 and try to adapt that proof to the theorem below. This is exactly what Cantor did.

Proof. The function $f : X \rightarrow \mathcal{P}(X)$ defined by $f(x) = \{x\}$ is clearly an injection, so we have $|X| \leq |\mathcal{P}(X)|$.

Suppose, to the contrary, that $|X| = |\mathcal{P}(X)|$. By definition, there is a bijection $g : X \rightarrow \mathcal{P}(X)$. In particular, g is surjective. (Note that g maps elements in X to sets, so $g(x)$ will be a set.) Consider the set $A = \{x \in X : x \notin g(x)\}$. Since $A \in \mathcal{P}(X)$ and we suppose g to be onto, there exists $a \in X$ with $g(a) = A$. Is $a \in A$? If it is, then $a \in A = g(a)$. So $a \in g(a)$ and if we look back at the definition of A , we see that $a \notin A$, a contradiction. The only other possibility is that $a \notin A = g(a)$. But let's return to the definition of A : Since $a \notin g(a)$, we see that $a \in A$! This is again a contradiction, and we conclude that there is no such bijection g . \square

Choosing various infinite sets for X , we obtain different examples of uncountable sets.

Corollary 24.4. *The set $\mathcal{P}(\mathbb{N})$ is uncountable.*

The cardinality of $\mathcal{P}(X)$ depends only on the cardinality of X (and you'll explain why this is the case in the next exercise). In particular, this implies that $|\mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{Z})| = |\mathcal{P}(\mathbb{Q})|$, to compare just a few of our favorite sets.

Exercise 24.5. Show that if for two sets X and Y we have $|X| = |Y|$, then $|\mathcal{P}(X)| = |\mathcal{P}(Y)|$. \circ

How do the two uncountable sets \mathbb{R} and $\mathcal{P}(\mathbb{N})$ compare? We will be able to show that, in fact, $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$, and $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$. Now this notation certainly suggests that we can conclude that the two cardinalities are the same, but we need to be very

careful here—we are not comparing natural numbers. We are saying that we have an injection from $\mathcal{P}(\mathbb{N})$ to \mathbb{R} and an injection from \mathbb{R} to $\mathcal{P}(\mathbb{N})$. To conclude that the two cardinalities are equal, we'll need to construct a bijection out of the two injections. This is the content of the following very important theorem.

Theorem 24.6 (Cantor–Schröder–Bernstein). *If A and B are two sets such that $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.*

Our basic proof strategy will be as follows: Our assumption implies that we can start with two injections, $f : A \rightarrow B$ and $g : B \rightarrow A$. Now we partition each of the sets A and B into the same (finite) number of sets (it will be three in our case). Then we will pair up the sets in the partitions in such a way that the restriction of the appropriate injection is actually a bijection. Finding just the right kind of partition of each set is, in fact, ingenious and it is the reason why the names of three major mathematicians are associated with this theorem. Two different proofs are outlined in Problems 24.13 and 24.14. The first of these proofs is shorter than the one we give here. We have chosen the proof below, because we find it particularly clear and enlightening. We hope you feel the same way about it. It is adapted from Halmos [41].

Proof. Since $|A| \leq |B|$, there is an injection $f : A \rightarrow B$ and since $|B| \leq |A|$, there is an injection $g : B \rightarrow A$.

We will define three subsets A_a, A_b , and A_∞ of A . An element of A will belong to exactly one of these subsets depending on something we will call its length, a notion we now define.

First note that since g is injective we have that for any $z \in A$, the set $g^{-1}(\{z\})$ is either empty or a set with exactly one element. Likewise, for any $z \in B$ the set $f^{-1}(\{z\})$ is either empty or contains exactly one element. This allows us to define for each $x \in A$ a sequence (x_n) with terms from $A \cup B$ as follows. We take

$$x_0 = x.$$

If, in the following, the set on the right is not empty, then we define x_n as indicated below:

$$\begin{aligned} x_1 &\in g^{-1}(\{x_0\}) \\ x_2 &\in f^{-1}(\{x_1\}) \\ x_3 &\in g^{-1}(\{x_2\}) \\ &\dots \end{aligned}$$

If, at some point, the set on the right-hand side is empty, then the sequence stops. In order to visualize this, consider the diagram below beginning on the right:

$$\dots x_3 \xrightarrow{g} x_2 \xrightarrow{f} x_1 \xrightarrow{g} x_0 = x.$$

If k is the first positive integer for which the inverse image of $\{x_{k-1}\}$ is empty, then the sequence is finite (the diagram above stops) with k terms. Note that for every $x \in A$, the sequence (x_n) is of length at least one, though it may be finite or infinite.

We now define the three promised sets, A_a, A_b , and A_∞ :

$$\begin{aligned} A_a &= \{x \in A : (x_n) \text{ has an odd number of terms}\}, \\ A_b &= \{x \in A : (x_n) \text{ has an even number of terms}\}, \\ A_\infty &= \{x \in A : (x_n) \text{ is an infinite sequence}\}. \end{aligned}$$

Evidently, $A = A_a \cup A_b \cup A_\infty$ and the three sets are pairwise disjoint.

For each $y \in B$, we define a sequence (y_n) with terms in $A \cup B$ analogously. We take

$$y_0 = y.$$

If, in the following, the set on the right is not empty, then we define y_n as indicated below:

$$\begin{aligned} y_1 &\in f^{-1}(\{y_0\}) \\ y_2 &\in g^{-1}(\{y_1\}) \\ y_3 &\in f^{-1}(\{y_2\}) \\ &\dots \end{aligned}$$

If, at some point, the set on the right-hand side is empty, then the sequence stops. In order to visualize this, consider the diagram below beginning on the right:

$$\dots y_3 \xrightarrow{f} y_2 \xrightarrow{g} y_1 \xrightarrow{f} y_0 = y.$$

If k is the first positive integer for which the inverse image of $\{y_{k-1}\}$ is empty, then the sequence is finite with k terms. Note that for any $y \in B$, the sequence (y_n) is of length at least one, though it may be finite or infinite. We then define

$$\begin{aligned} B_b &= \{y \in B : (y_n) \text{ has an odd number of terms}\}, \\ B_a &= \{y \in B : (y_n) \text{ has an even number of terms}\}, \\ B_\infty &= \{y \in B : (y_n) \text{ is an infinite sequence}\}. \end{aligned}$$

Evidently, $B = B_b \cup B_a \cup B_\infty$ and the three sets are pairwise disjoint. (Our notation suggests that we will pair A_a and B_b , A_b and B_a , and A_∞ and B_∞ .)

Note that the sequences corresponding to $x \in A$ and $y \in B$ are defined according to the same rule and in such a way that every term depends only on the term before. Thus, if two sequences, one corresponding to $x \in A$ and the other to $y \in B$, take on the same value at a term with an even index for (x_n) and a term with an odd index for (y_n) or vice versa, then the tails of the two sequences are the same from there

on. (If at this point you are confused about the definition of these two sequences, we recommend taking a short break from the proof and working Exercises 24.7 and 24.8 immediately following the proof. After working the exercises, you should find the proof easier to read.)

We will now compare A_a with B_a , A_b with B_b , and A_∞ with B_∞ . We will need to handle the case in which $A_a = \emptyset$ separately from the case in which it is nonempty.

Claim 1. If $A_a \neq \emptyset$, then $f|_{A_a} : A_a \rightarrow B_a$ is a bijection.

Let $x \in A$. Then $y = f(x) \in B$. Let’s compare the two sequences, (x_n) and (y_n) : The sequence corresponding to y is $(y_n) = (y, x, y_2, \dots)$, while the sequence corresponding to x is (x, x_1, \dots) . Once x appears, the subsequent terms will all be the same. In other words, and this will be crucial in what follows, $x_k = y_{k+1}$ for $k \geq 0$. Furthermore, it will be helpful to keep in mind that (x_n) has even, odd, or infinite length if and only if (y_n) has odd, even, or infinite length, respectively.

First we check that $f|_{A_a}$ maps A_a onto B_a . To this end, we recall that if $x \in A_a$, then the sequence (x_n) is of odd length. From the discussion in the last paragraph, the sequence (y_n) is of even length; that is, $y \in B_a$. This implies that $\text{ran}(f|_{A_a}) \subseteq B_a$. For the reverse inclusion, if $y \in B_a$, then the sequence (y_n) is of even length and has at least two terms (y, y_1, \dots) . We set $x = y_1$ and note that $y = f(x)$. As above, the sequence of x satisfies $x_k = y_{k+1}$ for $k \geq 0$. Since (y_n) is of even length, (x_n) is of odd length and thus $x \in A_a$. This shows that $B_a \subseteq \text{ran}(f|_{A_a})$.

Thus, we now know that $f|_{A_a} : A_a \rightarrow B_a$ is well-defined and surjective. Since $f|_{A_a}$ is the restriction of an injection, it is also one-to-one, establishing the first claim.

Claim 2. If $A_a = \emptyset$, then $B_a = \emptyset$.

Suppose, to the contrary, that $B_a \neq \emptyset$. Then there is $y \in B$ such that the sequence (y_n) is of even length and, in particular, of length at least two. Then $x = y_1 \in A$ and the sequence (x_n) satisfies $x_k = y_{k+1}$ for all $k \geq 0$. In particular, (x_n) is of odd length and thus $A_a \neq \emptyset$. This contradiction establishes the second claim.

These results imply that $A_a \approx B_a$. In entirely analogous ways we can show that $g|_{B_b} : B_b \rightarrow A_b$ and $f|_{A_\infty} : A_\infty \rightarrow B_\infty$ are bijections. Hence we also have $A_b \approx B_b$ and $A_\infty \approx B_\infty$.

By Theorem 21.6, we have $A = A_a \cup A_b \cup A_\infty \approx B_b \cup B_a \cup B_\infty = B$. Thus $|A| = |B|$. □

Exercise 24.7. Since $|\mathbb{N}| \leq |\mathbb{Z}|$ and $|\mathbb{Z}| \leq |\mathbb{N}|$, there exist two injective functions $f : \mathbb{N} \rightarrow \mathbb{Z}$ and $g : \mathbb{Z} \rightarrow \mathbb{N}$. We will make the following choices for f and g :

$$f(x) = 2x \quad \text{and} \quad g(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x - 1 & \text{if } x < 0 \end{cases}.$$

In what follows, we refer to the notation from the proof of Theorem 24.6.

- (a) Find the three sequences defined for 0, 3, and 8 in \mathbb{N} .

- (b) Find the three sequences defined for 0, -5 , and 10 in \mathbb{Z} . ○

Exercise 24.8. Continuing the exercise above and using the notation from the proof of Theorem 24.6, describe the set \mathbb{N}_b . ○

Exercise 24.9. Using the notation of the proof above, show that $A_\infty \approx B_\infty$. ○

It's now possible to show, as we ask you to in Problem 24.4, that the relation \leq , as defined in this chapter, “almost” satisfies the conditions of a partial order; that is, it is reflexive, transitive, and “almost” antisymmetric. Choosing the proper set on which to define the relation, we can make it a true partial order and, in fact, a total order. More on that appears in Project 29.12.

We will ask you to show, in the exercise below, that there are infinitely many uncountable sets all of different cardinality. So there are not merely two different infinities—there are at least countably infinitely many of them. At the time of Cantor's construction this theory was not easy for people to accept. To learn more about this, see the spotlight on the continuum hypothesis.

Exercise 24.10. Using Theorems 24.3 and 24.6, show that there are infinitely many uncountable and (mutually) nonequivalent sets. ○

We finish the chapter by following through on our vow to compare the sizes of our “original” uncountable sets, \mathbb{R} and $\mathcal{P}(\mathbb{N})$.

Theorem 24.11. *The sets \mathbb{R} and $\mathcal{P}(\mathbb{N})$ have the same cardinality.*

Proof. We define a function $f : \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$ by $f(x) = \{y \in \mathbb{Q} : y \leq x\}$. For each $x \in \mathbb{R}$, the set $f(x)$ is uniquely determined and $f(x) \subseteq \mathbb{Q}$. Thus f is a well-defined function.

We will show that f is one-to-one. Let $x, y \in \mathbb{R}$ with $x \neq y$. Without loss of generality, we may assume that $x < y$. By Theorem 12.12, there is a rational number c with $x < c < y$. But $c \notin f(x)$ while $c \in f(y)$, so $f(x) \neq f(y)$. This shows that f is injective.

Using the result of Exercise 24.5 we conclude that $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$.

For the other direction we define a function $g : \mathcal{P}(\mathbb{N}) \rightarrow \mathbb{R}$ by

$$g(A) = \sum_{j=0}^{\infty} \frac{a_j}{3^j} \text{ where } a_j = \begin{cases} 1 & \text{if } j \in A \\ 0 & \text{if } j \notin A \end{cases}.$$

For each $A \in \mathcal{P}(\mathbb{N})$, we have a unique series. Using the comparison test (comparing to the convergent geometric series $\sum_{j=0}^{\infty} \frac{1}{3^j}$) we see that $\sum_{j=0}^{\infty} \frac{a_j}{3^j}$ converges. Consequently, $g(A) \in \mathbb{R}$ and is unique. Hence the function g is well-defined.

To show that g is one-to-one, consider $A, B \in \mathcal{P}(\mathbb{N})$ with $A \neq B$. By the well-ordering principle of \mathbb{N} , there is a smallest integer k that belongs to one of the two

sets but not the other. Without loss of generality we may assume that $k \in A$ and $k \notin B$. Using the notation $g(A) = \sum_{j=0}^{\infty} \frac{a_j}{3^j}$ and $g(B) = \sum_{j=0}^{\infty} \frac{b_j}{3^j}$, we note that since k is the smallest integer in $A \setminus B$, we have $a_j = b_j$ for $j = 0, 1, \dots, k-1$. Now we use this and properties of geometric series to calculate:

$$\begin{aligned} g(A) - g(B) &= \sum_{j=0}^{\infty} \frac{a_j - b_j}{3^j} \\ &= \frac{1}{3^k} + \sum_{j=k+1}^{\infty} \frac{a_j - b_j}{3^j} \\ &\geq \frac{1}{3^k} - \sum_{j=k+1}^{\infty} \frac{1}{3^j} \\ &= \frac{1}{3^k} - \frac{1}{2(3^k)} > 0. \end{aligned}$$

Thus $g(A) \neq g(B)$ and g is an injection. This implies that $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$.

We apply Theorem 24.6 to finish the proof. □

In this text, we have defined what it means for the cardinality of two infinite sets, A and B , to be *less than or equal to* and *equal to*. It is also possible (with significantly more effort) to define the cardinal number of an arbitrary set. When this is done, it is common to introduce special symbols for the cardinality of \mathbb{R} and \mathbb{N} . The cardinal number $|\mathbb{R}|$ is denoted by \mathfrak{c} and is called the continuum, while $|\mathbb{N}|$ is denoted by \aleph_0 (where \aleph is the Hebrew letter aleph). The symbol \aleph_0 is read “aleph-nought.” If $|X| = \alpha$, we write $|\mathcal{P}(X)| = 2^\alpha$. In Problem 22.15 you showed that this notation agrees with the usual one for finite sets (see Definition 22.1 for that definition of cardinal number). Problem 24.18 provides the motivation for this power notation. Using this notation, we see that another way to state Theorem 24.11 is that $\mathfrak{c} = 2^{\aleph_0}$. The sets \mathbb{R} and $\mathcal{P}(\mathbb{N})$ are the smallest uncountable sets that we introduced in this text. Are they the smallest ones? Some people believe that Cantor drove himself into madness by his repeated attempts to prove that this is indeed the case (see [67], for example). His conjecture, that there is no uncountable set of cardinality strictly less than \mathfrak{c} , is called the continuum hypothesis. A discussion of this topic is in Spotlight: The Continuum Hypothesis.

Definitions

Definition 24.1. For two sets A and B the **cardinality of A is equal to the cardinality of B** , written $|A| = |B|$, if there is a bijective function $f : A \rightarrow B$.

Definition 24.2. For two sets A and B the **cardinality of A is less than or equal to the cardinality of B** , written $|A| \leq |B|$, if there is an injective function $f : A \rightarrow B$.

If, in addition, $|A| \neq |B|$, then we say the cardinality of A is less than the cardinality of B and we write $|A| < |B|$.

Solutions to Exercises

Solution (24.1). Let $f : \mathbb{Z} \rightarrow \mathbb{R}$ be defined by $f(n) = n$. Then f is obviously an injection, so $|\mathbb{Z}| \leq |\mathbb{R}|$. We know from Theorem 23.11 that $|\mathbb{Z}| \neq |\mathbb{R}|$, therefore $|\mathbb{Z}| < |\mathbb{R}|$.

Solution (24.2). We claim that $|\mathbb{Z}| \leq |\mathcal{P}(\mathbb{Z})|$. To see this, define $f : \mathbb{Z} \rightarrow \mathcal{P}(\mathbb{Z})$ by $f(n) = \{n\}$. Then f is an injection and therefore $|\mathbb{Z}| \leq |\mathcal{P}(\mathbb{Z})|$.

Solution (24.5). Since $|X| = |Y|$, there is a bijection $f : X \rightarrow Y$. We define a function $F : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$, by $F(A) = \{f(a) : a \in A\}$ for $A \in \mathcal{P}(X)$.

Since $f(a) \in Y$ for all $a \in X$, we have for each $A \subseteq X$ a unique $F(A) \subseteq Y$ and the function F is well-defined.

Suppose that for $A, B \in \mathcal{P}(X)$ we have $F(A) = F(B)$. If $z \in A$, then $f(z) \in F(A)$ and thus $f(z) \in F(B)$. That is, $f(z) = f(w)$ for some $w \in B$. Since f is one-to-one, $z = w$ and $z \in B$. Thus $A \subseteq B$. Entirely analogously one shows that $B \subseteq A$. Hence $A = B$ and the function F is one-to-one.

Let $B \in \mathcal{P}(Y)$. We define $A = \{f^{-1}(x) : x \in B\}$. Note that $f^{-1} : Y \rightarrow X$ exists since f is a bijection. We claim that $F(A) = B$. If $x \in B$, then $f^{-1}(x) \in A$ and thus $x = f(f^{-1}(x)) \in F(A)$. For the converse, if $x \in F(A)$, then $x = f(y)$ for some $y \in A$. Then $y = f^{-1}(z)$ for some $z \in B$. Thus $x = f(y) = z$ and $x \in B$. This establishes the claim and shows that the function F is onto.

We conclude that our function $F : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$ is a bijection and hence $|\mathcal{P}(X)| = |\mathcal{P}(Y)|$.

Solution (24.7).

- (a) We have $(0_n) = (0, 0, 0, \dots)$, $(3_n) = (3, -2)$, and $(8_n) = (8, 4, 2, 1)$. A brief explanation of some of these might help: For 0, we start with 0. Then we ask what was mapped to 0 under g (the answer is 0). Then we ask what was mapped to 0 under f . Again, the answer is zero. For 3, we start with 3 and ask what g mapped to 3. The answer is -2 . Then we ask what f mapped to -2 . The answer is that nothing was mapped to -2 , and that is why this sequence ends.

- (b) We have $(0_n) = (0, 0, 0, \dots)$, $(-5_n) = (-5)$, and $(10_m) = (10, 5, -3)$.

Solution (24.8). We claim that $\mathbb{N}_b = \mathbb{Z}^+$. In Exercise 24.7, we saw that (0_n) is infinite. Hence $0 \notin \mathbb{N}_b$ and therefore $\mathbb{N}_b \subseteq \mathbb{Z}^+$.

Conversely, suppose that $x \in \mathbb{Z}^+$. We first consider the case when x is odd. Then $(x_n) = (x, -(x+1)/2)$ and $x \in \mathbb{N}_b$. Now we break the case in which x is even into

two subcases. Note first that every even $z \in \mathbb{Z}^+$ can be written as $2^k w$, where w is odd and k is a positive integer. Let $x \in \mathbb{Z}^+$.

If $x = 2^k y$, where $k > 0$ is even and y is odd, then

$$(x_n) = (x, 2^{k-1}y, \dots, 2y, y, -\frac{y+1}{2}).$$

Thus, (x_n) is of even length and $x \in \mathbb{N}_b$.

If $x = 2^k y$, where $k > 0$ is odd and y is odd, then

$$(x_n) = (x, 2^{k-1}y, \dots, 2y, y).$$

This sequence is again of even length and hence $x \in \mathbb{N}_b$. Thus $\mathbb{Z}^+ \subseteq \mathbb{N}_b$ and the claim is established.

Solution (24.9). Claim 1. If $A_\infty \neq \emptyset$, then $f|_{A_\infty} : A_\infty \rightarrow B_\infty$ is a bijection.

Let $x \in A$. Then $y = f(x) \in B$ with corresponding sequence $(y_n) = (y, x, y_2, \dots)$ while the sequence of x is (x, x_1, \dots) and thus $x_k = y_{k+1}$ for $k \geq 0$. Therefore, if $x \in A_\infty$, then the sequence (x_n) is infinite and hence (y_n) is also, that is, $y \in B_\infty$. This implies that $\text{ran}(f|_{A_\infty}) \subseteq B_\infty$. If $y \in B_\infty$, then the sequence (y_n) is infinite: (y, y_1, \dots) . We set $x = y_1$ and note that $y = f(x)$. As above the sequence of x satisfies $x_k = y_{k+1}$ for $k \geq 0$. Since (y_n) is an infinite sequence, (x_n) is also and thus $x \in A_\infty$. This shows that $B_\infty \subseteq \text{ran}(f|_{A_\infty})$.

We have now shown that $f|_{A_\infty} : A_\infty \rightarrow B_\infty$ is well-defined and surjective. Since $f|_{A_\infty}$ is the restriction of an injection, it is also one-to-one. This establishes the first claim.

Claim 2. If $A_\infty = \emptyset$, then $B_\infty = \emptyset$.

If $B_\infty \neq \emptyset$, then there exists $y \in B$ such that the sequence (y_n) is infinite. Then $x = y_1 \in A$ and the sequence (x_n) satisfies $x_k = y_{k+1}$ for all $k \geq 0$. In particular, (x_n) is infinite and thus $A_\infty \neq \emptyset$. This establishes the second claim.

The two claims together show that $A_\infty \approx B_\infty$.

Solution (24.10). We will define recursively a sequence of sets as follows:

$$X_0 = \mathbb{N} \quad \text{and} \quad X_{n+1} = \mathcal{P}(X_n) \text{ for } n \geq 0.$$

It is clear that all sets are infinite, but suppose that not all of them have different cardinality. Then there are natural numbers j and k with $j < k$ such that $|X_j| = |X_k|$. In Problem 24.4 you will show that for all sets A, B, C with $|A| \leq |B|$ and $|B| \leq |C|$, you can conclude that $|A| \leq |C|$. Using this fact repeatedly together with Theorem 24.3 we get $|X_{j+1}| \leq |X_k| = |X_j|$. Theorem 24.3 also implies that $|X_j| \leq |\mathcal{P}(X_j)| = |X_{j+1}|$. By Theorem 24.6 we conclude that $|X_j| = |X_{j+1}|$. This contradicts Theorem 24.3 and shows that no two sets have the same cardinality and all but X_0 are uncountable.

Spotlight: The Continuum Hypothesis

The origin of set theory is generally attributed to Georg Cantor and Richard Dedekind. In 1872, the two men met while on vacation in Interlaken, Switzerland. The result of the meeting was a long-lasting correspondence in which many of the new ideas were discussed. Cantor was somewhat isolated at the University of Halle (his place of employment) and this long-distance collaboration was a great help to him. In an attempt to understand the infinite as a workable concept, Cantor arrived at a hierarchy of infinities. His work was understood by few and, in fact, it was opposed by many of the leading mathematicians at the time. In particular, a bitter antagonism between Cantor and his former teacher, Leopold Kronecker, developed. In addition, in philosophy of religion some people understood Cantor’s construction of many infinities as a threat to monotheism: one god—the infinite was jeopardized and the path to polytheism opened.

The concept of many infinities led to questions within the mathematical theory of cardinality of sets. Cantor wondered whether the set of real numbers was of smallest possible size of uncountable infinity; that is, is there an uncountable set that has “smaller size” than the real numbers? Cantor’s conjecture is known as the *Continuum Hypothesis*:

There is no set X such that $|\mathbb{N}| < |X| < |\mathbb{R}|$.

Cantor’s attempts to prove or disprove this hypothesis coincided with his first recorded attack of depression. He suffered from a bipolar disease that resulted in manic depression, periods of stays in an insane asylum, and the inability to work on mathematics. In between he worked on the continuum hypothesis, fearful that he would never be able to answer the question posed. He announced a proof, only to retract it a few months later. Then he announced a refutation, but had to concede the incompleteness of his arguments for that as well.

The continuum hypothesis survived the nineteenth century unresolved. David Hilbert, in his famous address to the International Congress of Mathematicians in Paris in 1900, gave a list of mathematical problems [50] that were of foremost interest to the discipline. (See also Spotlight: Hilbert’s Seventh Problem on page 359.) The very first problem he stated was the continuum hypothesis. This undoubtedly magnified the number of mathematicians attempting to conquer the hypothesis. And what happened to Cantor during this time? Though Cantor would live for 17 more years, teach courses, and give a few lectures on the paradoxes that his theory created, he also spent the rest of his life fighting his mental illness. Sadly, Hilbert’s quote (stated on page 261), showing the mathematical community’s acceptance and even admiration of Cantor’s work, did not appear until eight years after his death.

And what about the continuum hypothesis (or CH as it is often called)? Before proving or rejecting CH, a clear statement of what is allowed in such a proof or refutation had to be established. By 1930, the framework that was quite universally accepted was the axiomatic system of Ernst Zermelo and Abraham Fraenkel (ZF) together with the axiom of choice (AC) (see the Appendix for the exact statements). We’ll refer to this system as ZFC for short. A resolution of the CH question came in

two stages and in a surprising way: In 1940 Kurt Gödel proved that if ZFC does not contain a contradiction—that is, it is consistent—then so are ZFC and CH. Twenty years later Paul Cohen showed that if ZFC is consistent, so are ZFC and \neg CH. These two major mathematical results of the twentieth century ended efforts to decide about the continuum hypothesis; the question of whether CH is true or false cannot be answered within ZFC.

For an enjoyable dramatization of the heroic battles of Cantor and Gödel (together with Boltzman and Turing) we recommend the BBC documentary *Dangerous Knowledge* [67].

The Clay Institute’s millennium questions, a centennial update of Hilbert’s problems, no longer contain the continuum hypothesis. So is the subject dead? Not at all. Both proofs about the consistency of CH and \neg CH with ZFC brought with them completely new techniques. In the first case, “Gödel numbering” was introduced. In the second case, the technique of “forcing” was developed. This technique can be thought of as a way to introduce additional sets without losing control over the axioms. This has turned out to be a major tool for proving consistency and independence results. With this as well as other techniques, set theory has developed tremendously in the last century. The demands of other fields of mathematics led set theorists like W. Hugh Woodin, Jan Mycielski, and many others to look for more axioms. Many of the ZFC axioms postulate ways to create new sets. These axioms can be extended with *large cardinal axioms*, or ways to produce bigger sets. Another strategy is to bring the following idea into the picture: Let $A \subseteq \mathbb{R}$. In a countably infinite game, two players take turns in choosing decimals of a real number. If at the end the number is in A , player I wins, otherwise player II wins. If, for either player, a winning strategy exists, then the set A is called *determined*. The axiom of determinacy declares all subsets of \mathbb{R} to be determined. However, this axiom contradicts AC and therefore cannot be used together with ZFC in order to decide on the validity of CH.

Perhaps the most promising attempts to expand ZFC are due to Saharon Shelah. He worked with a new axiom, called the proper forcing axiom (due to Jim Baumgartner). Stevo Todorčević showed that ZFC together with the proper forcing axiom imply that the CH fails and, in fact, that there is exactly one cardinal number strictly between \aleph_0 and the continuum \mathfrak{c} .

However, the good thing about ZFC is that all mathematicians understand the axioms and most mathematicians accept them, even the axiom of choice. The newer axioms are neither widely understood nor universally accepted. Finally, there is *Gödel’s First Incompleteness Theorem*, which implies that set theorists cannot make every sentence provable. But much remains to be understood: Reverse mathematics, for example, is a program that takes mathematical results and tries to understand the axioms necessary to prove them. Thus, we can expect many interesting discoveries in the future. (A summary of the history of set theory through the present for the advanced reader is in [31, pp. 1–92].)

Problems

Problem 24.1. Let A and B be subsets of a set X .

- (a) Prove that $|A \times B| = |B \times A|$.
- (b) Prove that if $B \neq \emptyset$, then $|A| \leq |A \times B|$.

Problem 24.2. Prove each of the following, by defining an appropriate function between the two given sets:

- (a) $|2\mathbb{Z}| = |4\mathbb{Z}|$;
- (b) $|\mathbb{N}| \leq |\mathbb{Z}|$;
- (c) $|\mathbb{Z}| \leq |\mathbb{N}|$;
- (d) $|\mathbb{N}| < |\mathbb{R}|$.

Problem 24.3. Using the notation of the proof of Theorem 24.6, prove that $A_b \approx B_b$.

Problem# 24.4. Let \mathcal{A} be a nonempty collection of sets. We define the following relation on \mathcal{A} . For $A, B \in \mathcal{A}$,

$$A \preceq B \text{ if } |A| \leq |B|.$$

- (a) Show that \preceq is reflexive and transitive on \mathcal{A} .
- (b) Show that for $A, B \in \mathcal{A}$, if $A \preceq B$ and $B \preceq A$, then $A \approx B$.
- (c) Is \preceq a partial order of \mathcal{A} ? If it is, prove it; if it isn't, give a counterexample.

Problem 24.5. Assign the appropriate integer or symbol to each of the following cardinal numbers, put them in increasing order, and give a brief explanation for your answer:

$$|\mathcal{P}(\mathbb{Q})|, |\mathcal{P}(\emptyset)|, |\mathcal{P}(\mathcal{P}((0, 1)))|, |\{0\}|, |\mathbb{R} \setminus \mathbb{Q}|, |\mathcal{P}(\mathcal{P}(\emptyset))|,$$

$$|\{0, 1\}|, |\mathbb{Q}|, |\emptyset|, |(0, 1)|, |[0, 1]|, |\mathcal{P}((0, 1))|, |\mathcal{P}(\mathcal{P}(\mathbb{N}))|, |\mathcal{P}(\{0, 1\})|.$$

Problem# 24.6. Let X and Y be finite sets with $|X| = m$, $|Y| = n$, and $m \leq n$. Show that according to Definition 24.2 we have $|X| \leq |Y|$.

Problem 24.7. Prove the following: If X and Y are sets with $X \subseteq Y$, then $|X| \leq |Y|$. If we know that $X \subset Y$, can we conclude that $|X| < |Y|$? Prove it or give a counterexample.

Problem 24.8. Prove the following: If X and Y are sets with $|X| \leq |Y|$, then $|\mathcal{P}(X)| \leq |\mathcal{P}(Y)|$.

Problem 24.9. In each of the following parts, give an example of such functions or explain why it is not possible to do so:

- (a) Functions f and g such that $f : \mathbb{Q} \rightarrow \mathbb{N}$, $g : \mathbb{N} \rightarrow \mathbb{Q}$, both are one-to-one but neither of them is onto;

- (b) Functions f and g such that $f : \mathbb{Q} \rightarrow \mathbb{N}$, $g : \mathbb{N} \rightarrow \mathbb{Q}$, both are onto but neither of them is one-to-one;
- (c) A function $f : \mathbb{R} \rightarrow \mathbb{Q}$ that is one-to-one;
- (d) A function $f : \mathcal{P}(\mathbb{R}) \rightarrow \mathbb{R}$ that is one-to-one.

Problem 24.10. Let $A = \{1, 2, 3, 4, \dots\}$ and $B = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$. We define the injective functions

$$f : A \rightarrow B \text{ by } f(x) = \frac{1}{x+3} \quad \text{and} \quad g : B \rightarrow A \text{ by } g(x) = \frac{1}{x} + 5.$$

In the following we always refer to the notation from the proof of Theorem 24.6 and the sequences that we defined in that theorem.

- (a) Find the sequence that starts with $1/3$.
- (b) Find the sequence that starts with $1/10$.
- (c) Consider the elements 2, 10, and 15 in A . Find the corresponding elements in the set B constructed in the proof of Theorem 24.6.

Problem 24.11. Let X and Y be nonempty finite sets and suppose we have injections $f : X \rightarrow Y$ and $g : Y \rightarrow X$ as in the hypotheses of Theorem 24.6. The notation below refers to that of the proof of Theorem 24.6. For parts (a) and (b) your answer will involve f and g .

- (a) For $x \in X$, find the sequence (x_n) .
- (b) For $y \in Y$, find the sequence (y_n) .
- (c) Describe the sets X_a, X_b , and X_∞ .
- (d) Describe the sets Y_a, Y_b , and Y_∞ .

Problem 24.12. Since $|\mathbb{N}| \leq |\mathbb{Z}|$ and $|\mathbb{Z}| \leq |\mathbb{N}|$, there are two injective functions $f : \mathbb{N} \rightarrow \mathbb{Z}$ and $g : \mathbb{Z} \rightarrow \mathbb{N}$. We will make the following choices:

$$f(x) = 3x \quad \text{and} \quad g(x) = \begin{cases} 3x & \text{if } x \geq 0 \\ -3x + 1 & \text{if } x < 0 \end{cases}.$$

In the following we always refer to the notation from the proof of Theorem 24.6.

- (a) Find each of the five sequences that start with the following elements in \mathbb{N} : 0, 1, 45, $4(3^6)$, and $5(3^6)$.
- (b) Show that $\mathbb{N}_\infty = \{0\}$ and

$$\mathbb{N}_a = \{(3^{2s})k : k, s \in \mathbb{N} \text{ and } k = 1 \text{ or } k = 3m + 2, m \in \mathbb{N}\}.$$

Problem 24.13. For an alternate proof of the Cantor–Schröder–Bernstein theorem construct a sequence of subsets of A as follows, using the notation from the theorem as stated in the text:

$$C_0 = A \setminus g(B), \quad C_{j+1} = g(f(C_j)) \text{ for } j \geq 0.$$

Set $C = \bigcup_{j=0}^\infty C_j$ and define a function $h : A \rightarrow B$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in C \\ y, \text{ where } g(y) = x & \text{if } x \notin C \end{cases}.$$

Finish this proof by showing that h is well-defined and that it is a bijection.

Problem 24.14. This problem outlines yet another proof of the Cantor–Schröder–Bernstein theorem. Using the notation from the theorem as stated in the text we define $B' = f(A)$, $A' = g(B)$, $P = (g \circ f)(A)$, and $Q = A' \setminus P$.

For $X \subseteq A$ we define $X^* = (g \circ f)(X) \cup Q$. We say that a subset X of A is normal if $X^* \subseteq X$.

- Show that the collection of normal subsets of A is not empty.
- Show that the intersection of a nonempty collection of normal subsets is a normal subset.
- Show that if X is a normal subset, then so is X^* .
- We let N denote the intersection of all normal subsets of A and define $Y = P \setminus (g \circ f)(N)$. Prove that $P \cup Q = Y \cup N$.
- Prove that the last part implies that $|P \cup Q| = |P|$.
- Prove the theorem.

Note: This proof is essentially due to Peano and Zermelo who came up with the same idea independently and published it independently in 1906, see [34].

Problem 24.15. The set $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ is the open unit interval. Prove that $|(0, 1)| = |(0, 1) \times (0, 1)|$.

(Cantor proved this first and it was on this occasion that he wrote the sentence quoted on page 251.)

Problem 24.16. Prove that $|\mathbb{R}| = |\mathbb{C}|$, where $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ denotes the complex numbers. (If you worked Problem 24.15, you might want to use the result here.)

Problem 24.17. We denote by $I = [0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$ the closed interval from 0 to 1 and by $\mathcal{F}(I)$ the set of all functions $f : I \rightarrow I$.

- Find an injective function $g : \mathcal{F}(I) \rightarrow \mathcal{P}(I \times I)$. (Prove that your function is well-defined and one-to-one.)
- Find an injective function $h : \mathcal{P}(I) \rightarrow \mathcal{F}(I)$. (Consider the function h defined as follows: Given a set $X \in \mathcal{P}(I)$, define $h(X) = \chi_X$ where χ_X is the characteristic function of the set X . Be sure to prove that h is well-defined and one-to-one.)
- Use parts (a) and (b) together with the result of Problem 24.15 to prove that $|\mathcal{F}(I)| = |\mathcal{P}(\mathbb{R})|$.

Problem 24.18. Let X be a nonempty set. We denote by 2^X the set of all functions $f : X \rightarrow \{0, 1\}$. Prove that $|\mathcal{P}(X)| = |2^X|$. (You may find it helpful to use characteristic functions here.)

Problem 24.19. Using the Cantor–Schröder–Bernstein theorem, give an easy proof of $|(-1, 1)| = |[-1, 1]|$.

Problem 24.20. A generalization of the continuum hypothesis says that for any infinite set X , there is no set Y such that $|X| < |Y| < |\mathcal{P}(X)|$. Under the assumption of this generalized continuum hypothesis, prove that a set X with at least two elements is infinite if and only if there is no set Y with $|X| < |Y| < |\mathcal{P}(X)|$.

Problem 24.21. See Problem 24.20 above for a statement of the generalized continuum hypothesis. Let X and Y be sets such that Y is countable and $|\mathcal{P}(X)| \leq |\mathcal{P}(Y)|$. Assuming the generalized continuum hypothesis, prove that $|Y| \not< |X|$.

Chapter 25

Metric Spaces

There are many ways to measure distance in the spaces in which we live and work. For example, if you want the shortest distance between two geographical places (the distance “as the crow flies”), you follow the line segment joining them. But in real life this isn’t always possible. If you are driving your car through a city or across your campus, you need to go around solid objects and not through them. So how do we calculate distance in those cases? Measuring distance in a set X is a very small (but interesting) part of a branch of mathematics known as “point set topology,” and we will look at it in detail in this chapter. We will now often refer to the elements of X as points.

So let’s go back to the first time you measured distance. It was probably in \mathbb{R} , on a number line, and you learned that the distance between two points x and y was the absolute value of the difference of the two numbers. If we write $d(x, y) = |x - y|$, then d is a function and $d : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$. That’s straightforward enough, but now we want to generalize our concept of distance. So let’s turn to the essential properties of a distance function.

First, distance shouldn’t be negative, so $d(x, y) \geq 0$ for two points x and y , and if the distance satisfies $d(x, y) = 0$, then you didn’t move anywhere, so $x = y$. You also surely believe that distance from x to y should be the distance from y to x . And finally, in Theorem 5.8 (Problem 5.14) you learned the triangle inequality, which said that “if x and y are two real numbers, then $|x + y| \leq |x| + |y|$.” In Problem 20.2, you showed how to switch the triangle inequality into a statement about distances. We recall the result of that problem here: For real numbers x, y , and z ,

$$|x - y| \leq |x - z| + |z - y|.$$

In English, this means that our path will be shorter if we go directly from x to y as opposed to taking a detour through z , which is as it should be. So we would want our general distance function to satisfy something like this too; that is, in our new “ d ” notation we want $d(x, y) \leq d(x, z) + d(z, y)$ for arbitrary points x, y , and z . So now we will define something that acts like a distance on an arbitrary set X and does all the important things that a distance should do.

Let X be a nonempty set. Then a **metric** on X is a function $d : X \times X \rightarrow \mathbb{R}$ satisfying (i)–(iv) below.

- (i) (Nonnegativity) For all $x, y \in X$, the function d satisfies $d(x, y) \geq 0$.
- (ii) (Definiteness) For all $x, y \in X$, the function d satisfies $d(x, y) = 0$ if and only if $x = y$.
- (iii) (Symmetry) For all $x, y \in X$, the function d satisfies $d(x, y) = d(y, x)$.
- (iv) (Triangle inequality) For all $x, y, z \in X$, the function d satisfies

$$d(x, y) \leq d(x, z) + d(z, y).$$

A metric is also called a distance function. A nonempty set X together with the metric d is called a **metric space** and is denoted by (X, d) , or just X when it is clear which distance function we are using.

When you learn the definition, don't forget to say "Let X be a nonempty set. Then a metric on X is a function $d : X \times X \rightarrow \mathbb{R} \dots$." These sentences tell us something about d , and cannot be omitted.

In the introduction, we showed that a metric can be defined on \mathbb{R} by $d_u(x, y) = |x - y|$. Though we outlined how to show that d_u is a metric, you should write out the details to complete the proof. This metric is often called the **usual metric** (hence the subscript u) or the **Euclidean metric** on \mathbb{R} , and it is the one upon which your intuition is almost certainly based. A set can have lots of metrics. The next example is a metric on \mathbb{R} that is not the same as the metric given by the absolute value.

Example 25.1. Define a metric $d_d : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ by

$$d_d(x, y) = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{if } x \neq y \end{cases}.$$

We will show that d_d is a metric on \mathbb{R} . This metric is called the **discrete metric**, and it can really challenge your intuition.

Proof. It is clear that d_d is a function from $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$. Now let x and y be points of \mathbb{R} . We begin with nonnegativity: $d_d(x, y) = 0$ or $d_d(x, y) = 1$, so clearly $d_d(x, y) \geq 0$. Thus, the nonnegativity condition holds. Furthermore, since $d_d(x, y) = 0$ if and only if $x = y$, the definiteness condition holds. For symmetry, note that if $x \neq y$, then $y \neq x$ and consequently $d_d(x, y) = 1 = d_d(y, x)$. If $x = y$, then $d_d(x, y) = 0 = d_d(y, x)$, establishing symmetry. Finally, we establish the triangle inequality. To this end, note that if z is a point of \mathbb{R} , then we have two cases to consider. In the first case, if $x = y$, then $d_d(x, y) = 0$ and the nonnegativity condition implies that $d_d(x, y) = 0 \leq d_d(x, z) + d_d(z, y)$. In the second case, $x \neq y$, which implies that $z \neq x$ or $z \neq y$ (or both). Therefore, either $d_d(x, z) = 1$ or $d_d(z, y) = 1$ (or both). Thus, $d_d(x, y) = 1 \leq d_d(x, z) + d_d(z, y)$, completing the proof of the triangle inequality. \square

The discrete metric can be defined on every space: the distance between two distinct points is one, and the distance from a point to itself is necessarily zero. The

proof that this is a metric on a set X is indistinguishable from the one above. Thus we have an example of a metric on \mathbb{R}^2 . Example 25.2 and Exercise 25.3 provide us with some other metrics on \mathbb{R}^2 .

Example 25.2. On \mathbb{R}^2 define a metric by

$$d_u((x_1, x_2), (y_1, y_2)) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}.$$

Using Project 29.10, it can be shown that this is actually a metric on \mathbb{R}^2 . For now, you may accept this fact. This metric is referred to as the **usual metric** or the **Euclidean metric** on \mathbb{R}^2 . In fact, one may also define the **usual metric on \mathbb{R}^n** by

$$d_u((x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n)) = \sqrt{\sum_{j=1}^n (x_j - y_j)^2}. \quad \circ$$

Exercise 25.3. We now have two examples of metrics on \mathbb{R} and two on \mathbb{R}^2 . Here are two more metrics on \mathbb{R}^2 . Before you begin the exercise, familiarize yourself with the metrics by computing various distances. For example, try to find the distance from the point $(1, 3)$ to the points $(-3, 4)$ using the various metrics below.

- (a) Show that $d_{tc}((x_1, x_2), (y_1, y_2)) = |x_1 - y_1| + |x_2 - y_2|$ is a metric on \mathbb{R}^2 . This metric, d_{tc} , is called the **taxicab metric**. Why would it be called that?
- (b) Show that $d_m((x_1, x_2), (y_1, y_2)) = \max\{|x_1 - y_1|, |x_2 - y_2|\}$ is also a metric on \mathbb{R}^2 . The metric d_m is sometimes called the **max metric**. ○

The two examples introduced in Exercise 25.3 will appear again in the near future.

A metric tells us when points are close. We studied the notion of “closeness” in Chapter 20 when we studied convergent sequences. You can picture convergence of a sequence to the number L in the following way: a sequence converges to L if for every $\varepsilon > 0$, the sequence eventually lies in the open interval $(L - \varepsilon, L + \varepsilon)$; more precisely, the definition of convergence said, “There exists a real number L such that for every $\varepsilon > 0$, there exists a real number N such that $|x_n - L| < \varepsilon$ for all $n \geq N$.” We return to the idea of finding the limit of a sequence, but this time in a metric space. So given a sequence (x_n) of points in a metric space (X, d) , then (as we did before) we say that (x_n) **converges** in X if there exists a point $x \in X$ such that for every $\varepsilon > 0$, there exists a real number N such that $d(x_n, x) < \varepsilon$ for all $n \geq N$. As before, in the event that such an x exists, it is also unique. (See Theorem 25.8 below.) The value x is called the **limit** of the sequence, we say that the sequence **converges to x** , and, as before, we write $x_n \rightarrow x$ or $\lim_{n \rightarrow \infty} x_n = x$. If the sequence does not converge, we say that it **diverges**. If we consider $X = \mathbb{R}$ with the usual metric, this is exactly the same definition that we had in Chapter 20. Since we allow all sorts of choices for X now, we would like to take this opportunity to point out that the

point x must be in the space X —not in some larger space that happens to contain X . If it is clear that x belongs to X , we will often say that the sequence converges, rather than “the sequence converges in X .” Also, note that as the metric d changes, the distance between pairs of points changes as well. Therefore, it is conceivable that some sequences will converge in one metric, but not in another.

Exercise 25.4. Complete the sentences.

- (a) Let (x_n) be a sequence in a metric space X with metric d . Let $x \in X$. Then (x_n) does not converge to x if
- (b) Let (x_n) be a sequence in a metric space (X, d) . Then (x_n) does not converge if

We’ll break tradition and give you the answer to part (a) of the above exercise here, because we need it: A sequence (x_n) does not converge to x if there exists an $\varepsilon > 0$ such that for every real number N , there exists $m \in \mathbb{N}$ such that $m \geq N$ and $d(x_m, x) \geq \varepsilon$. While an answer to (b) might read “a sequence (x_n) does not converge if for every $x \in X$, the sequence does not converge to x ,” this will probably not be the most useful formulation of the answer. We leave the more useful version to you.

○

Example 25.5. We know that $1/n \rightarrow 0$ in \mathbb{R} with the usual metric. Show that $(1/n, 1/n) \rightarrow (0, 0)$ in \mathbb{R}^2 with the usual metric.

Proof. Let $\varepsilon > 0$, and let N be a real number with $N > \sqrt{2}/\varepsilon$. If n is an integer with $n \geq N$, then

$$\begin{aligned} d_u((1/n, 1/n), (0, 0)) &= \sqrt{(1/n - 0)^2 + (1/n - 0)^2} \\ &= \sqrt{2}/n \\ &\leq \sqrt{2}/N && \text{(since } n \geq N) \\ &< \sqrt{2}(\varepsilon/\sqrt{2}) && \text{(as } N > \sqrt{2}/\varepsilon) \\ &= \varepsilon. \end{aligned}$$

See [Figure 25.1](#) for a graphical illustration of this convergent sequence. □

You may wonder where we came up with $\sqrt{2}/\varepsilon$. We did it by understanding the problem and devising a plan by working backwards. So what you see here is what happened after we went to a separate sheet of paper, and started with the inequality $\sqrt{2}/n < \varepsilon$.

Example 25.6. In Chapter 20, we showed that the sequence $(1/n)$ converges to 0 in \mathbb{R} with the usual metric. Does $(1/n)$ converge to 0 in the discrete metric?

We claim that the sequence (in \mathbb{R} with the discrete metric) does not converge to 0. To see this, let $\varepsilon = 1/2$. For every $N \in \mathbb{R}$, there exists an integer $n \geq N$. Since $1/n \neq 0$, we know that $d_d(1/n, 0) = 1$. Hence for $\varepsilon = 1/2$, and for every $N \in \mathbb{R}$, there exists an integer $n \geq N$ such that $x_n = 1/n$ satisfies $d_d(x_n, 0) = d_d(1/n, 0) = 1 \geq 1/2$. Thus $(1/n)$ does not converge to 0. □

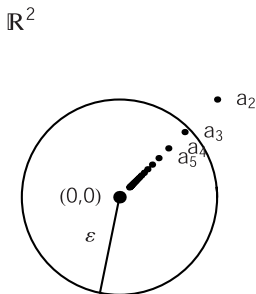


Fig. 25.1 $(1/n, 1/n) \rightarrow (0, 0)$

In the discrete metric, every point is “far” from every other point. This makes it very hard to converge.

Exercise 25.7. Consider \mathbb{R} with the discrete metric. Describe the convergent sequences in this metric space. ○

Sequences have many important properties, some of which we discuss in the problems. The proofs are often quite similar to the proofs we did in Chapter 20. At this point, we give one example of a theorem with such a proof.

Theorem 25.8. *If a sequence (x_n) in a metric space (X, d) converges, then the limit is unique.*

The proof of this is, with an appropriate change in notation, the same as the proof of Theorem 20.7.

Definitions

Definition 25.1. Let X be a nonempty set. Then a **metric** on X is a function $d : X \times X \rightarrow \mathbb{R}$ satisfying (i)–(iv) below.

- (i) (Nonnegativity) For all $x, y \in X$, the function d satisfies $d(x, y) \geq 0$.
- (ii) (Definiteness) For all $x, y \in X$, the function d satisfies $d(x, y) = 0$ if and only if $x = y$.
- (iii) (Symmetry) For all $x, y \in X$, the function d satisfies $d(x, y) = d(y, x)$.
- (iv) (Triangle inequality) For all $x, y, z \in X$, the function d satisfies

$$d(x, y) \leq d(x, z) + d(z, y).$$

Definition 25.2. A nonempty set X together with a metric d is called a **metric space** and is denoted by (X, d) or, when it is clear which distance function we are using, we will simply refer to the space X .

Definition 25.3. The **usual metric** or **Euclidean metric** on the reals is defined by $d_u(x, y) = |x - y|$ for $x, y \in \mathbb{R}$.

Definition 25.4. The **discrete metric** on \mathbb{R} is defined by

$$d_d(x, y) = \begin{cases} 0 & \text{if } x = y \\ 1 & \text{if } x \neq y \end{cases} \text{ for } x, y \in \mathbb{R}.$$

Definition 25.5. The **usual metric** or **Euclidean metric** on \mathbb{R}^n for $n \in \mathbb{Z}^+$ is defined by

$$d_u((x_1, \dots, x_n), (y_1, \dots, y_n)) = \sqrt{\sum_{j=1}^n (x_j - y_j)^2},$$

for $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathbb{R}^n$.

Definition 25.6. The **taxicab metric** on \mathbb{R}^2 is defined by

$$d_{tc}((x_1, x_2), (y_1, y_2)) = |x_1 - y_1| + |x_2 - y_2| \text{ for } (x_1, x_2), (y_1, y_2) \in \mathbb{R}^2.$$

Definition 25.7. The **max metric** on \mathbb{R}^2 is defined by

$$d_m((x_1, x_2), (y_1, y_2)) = \max\{|x_1 - y_1|, |x_2 - y_2|\} \text{ for } (x_1, x_2), (y_1, y_2) \in \mathbb{R}^2.$$

Definition 25.8. A sequence (x_n) of points in a metric space (X, d) **converges** in X if there exists a point $x \in X$ such that for every $\varepsilon > 0$, there exists a real number N such that $d(x_n, x) < \varepsilon$ for all $n \geq N$. The value x is called the **limit** of the sequence (x_n) , we say that the sequence **converges to** x , and we write $x_n \rightarrow x$ or $\lim_{n \rightarrow \infty} x_n = x$.

Definition 25.9. A sequence (x_n) **diverges** in a metric space (X, d) if it does not converge in (X, d) .

Definition 25.10 (for Problem 25.7). A set F in a metric space (X, d) is **bounded** if there exists a positive real number M such that $d(x, y) \leq M$ for all $x, y \in F$.

Definition 25.11 (for Problem 25.8). Let (X, d) be a metric space. The metric $d_b : X \times X \rightarrow \mathbb{R}$ defined by

$$d_b(x, y) = \min\{d(x, y), 1\}$$

is called the **bounded metric associated with** d on X .

Solutions to Exercises

Solution (25.3). Parts (a) and (b) are very similar, so we will work part (a) only.

By definition, d_{tc} is a function from $\mathbb{R} \times \mathbb{R}$ to \mathbb{R} . Now let (x_1, x_2) and (y_1, y_2) be elements of \mathbb{R}^2 . We will first show the nonnegativity. Because $|a| \geq 0$ for all real numbers a , we know that $d_{tc}((x_1, x_2), (y_1, y_2)) = |x_1 - y_1| + |x_2 - y_2| \geq 0$, showing that nonnegativity of d_{tc} holds. For definiteness, note that $d_{tc}((x_1, x_2), (y_1, y_2)) = 0$ if and only if $|x_1 - y_1| + |x_2 - y_2| = 0$. This last equality holds if and only if $|x_1 - y_1| = 0$ and $|x_2 - y_2| = 0$. This, in turn, holds if and only if $x_1 = y_1$ and $x_2 = y_2$; in other words, $(x_1, x_2) = (y_1, y_2)$. This string of equivalences establishes the definiteness of d_{tc} . Symmetry is shown as follows:

$$\begin{aligned} d_{tc}((x_1, x_2), (y_1, y_2)) &= |x_1 - y_1| + |x_2 - y_2| \\ &= |y_1 - x_1| + |y_2 - x_2| \\ &= d_{tc}((y_1, y_2), (x_1, x_2)). \end{aligned}$$

To prove that the triangle inequality holds for d_{tc} , let $(z_1, z_2) \in \mathbb{R}^2$. Then

$$\begin{aligned} d_{tc}((x_1, x_2), (y_1, y_2)) &= |x_1 - y_1| + |x_2 - y_2| \\ &\leq |x_1 - z_1| + |z_1 - y_1| + |x_2 - z_2| + |z_2 - y_2| \\ &\quad \text{(by the triangle inequality in } \mathbb{R} \text{)} \\ &= (|x_1 - z_1| + |x_2 - z_2|) + (|z_1 - y_1| + |z_2 - y_2|) \\ &= d_{tc}((x_1, x_2), (z_1, z_2)) + d_{tc}((z_1, z_2), (y_1, y_2)). \end{aligned}$$

This shows that d_{tc} is a metric on \mathbb{R}^2 . The taxicab metric between two points measures the distance you have to travel from one point to the next in a city built with rectangular blocks, assuming you stay on the streets, do not take detours, and do not have to worry about one-way streets.

Solution (25.4). The solution to part (a) was given earlier following the exercise, so here is the solution to part (b).

The sequence (x_n) does not converge in the metric space (X, d) if for every $x \in X$ there exists a real number $\varepsilon > 0$ such that for every real number N , there exists m such that $m \geq N$ and $d(x_m, x) \geq \varepsilon$.

Solution (25.7). We claim that a sequence (x_n) in (\mathbb{R}, d_d) converges if and only if there exist real numbers x and M such that $x_n = x$ for all $n \geq M$. (Such a sequence is called an eventually constant sequence.)

First assume that (x_n) is a sequence for which there exist real numbers x and M satisfying $x_n = x$ for all $n \geq M$. We will show that $x_n \rightarrow x$. Let $\varepsilon > 0$ and let $N = M$. Then for $n \geq N$ we know that $d_d(x_n, x) = d_d(x, x) = 0 < \varepsilon$, which shows that (x_n) converges.

For the converse, assume that (x_n) converges. Consider $\varepsilon = 1/2$. Then there exists N such that $d_d(x_n, x) < 1/2$ for $n \geq N$. By the definition of d_d , the only way that this can happen is if $x_n = x$ for $n \geq N$. Taking $M = N$, we have shown that there exist x and M such that $x_n = x$ for all $n \geq M$, as desired.

Problems

Unless otherwise specified, assume that you are working in a general metric space (X, d) .

Problem 25.1. (a) Suppose a student writes the following: A metric is a function satisfying (i)–(iv) below.

- (i) (Nonnegativity) $d(x, y) \geq 0$,
- (ii) (Definiteness) $d(x, y) = 0$, if and only if $x = y$,
- (iii) (Symmetry) $d(x, y) = d(y, x)$, and
- (iv) (Triangle inequality) if z is a point in X , then

$$d(x, y) \leq d(x, z) + d(z, y).$$

Write this student a letter indicating what was omitted from the definition, what must be inserted, and what else (if anything) needs to be changed to make it a correct definition.

- (b) Suppose the student had exactly the same definition as in the text, except for the triangle inequality, where the student has “ $d(x, y) \leq d(x, z) + d(z, y)$ for some $z \in X$.”

Write a correct, careful, and complete response to this student.

Problem 25.2. (a) In \mathbb{R} , find the distance of the number 1 to the number 3 in the usual metric and in the discrete metric.

- (b) In \mathbb{R}^2 , find the distance of the point $(1, 3)$ to the point $(2, 5)$ in the usual metric, the taxicab metric, the max metric, and the discrete metric.

Problem 25.3. (a) Sketch the set $\{(x, y) \in \mathbb{R}^2 : d_u((x, y), (0, 0)) < 1\}$, where d_u is the usual metric.

- (b) Sketch the set $\{(x, y) \in \mathbb{R}^2 : d_{tc}((x, y), (0, 0)) < 1\}$, where d_{tc} is the taxicab metric.
- (c) Sketch the set $\{(x, y) \in \mathbb{R}^2 : d_m((x, y), (0, 0)) < 1\}$, where d_m is the max metric.
- (d) Sketch the set $\{(x, y) \in \mathbb{R}^2 : d_d((x, y), (0, 0)) < 1\}$, where d_d is the discrete metric.
- (e) Sketch the set $\{(x, y, z) \in \mathbb{R}^3 : d_u((x, y, z), (0, 0, 0)) < 1\}$, where d_u is the usual metric.

Problem 25.4. (a) We defined the max metric on \mathbb{R}^2 . Define the max metric on \mathbb{R}^n and prove that it is a metric.

- (b) We defined the taxicab metric on \mathbb{R}^2 . Define the taxicab metric on \mathbb{R}^n and prove that it is a metric.

Problem 25.5. (a) Show that $d : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ defined by

$$d((x_1, x_2), (y_1, y_2)) = |x_1 - y_1|$$

is not a metric on \mathbb{R}^2 .

(b) Is $d : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ defined by

$$d((x_1, x_2), (y_1, y_2)) = (x_1 - y_1)^2 + (x_2 - y_2)^2$$

a metric on \mathbb{R}^2 ? If you think it is a metric, prove it. If you think it is not a metric, find points in \mathbb{R}^2 for which one of the conditions is violated.

Problem 25.6. Let (X, d) be a metric space. Let α be a real number and define a new function d_α on $X \times X$ by $d_\alpha(x, y) = \alpha d(x, y)$. Is d_α a metric on X ? If not, what assumptions must be placed on α to assure that d_α is a metric? Prove your answer.

Problem 25.7. A set F in a metric space (X, d) is **bounded** if there exists a positive real number M such that $d(x, y) \leq M$ for all $x, y \in F$.

- (a) Consider the following “not a definition” of a bounded set.
 “A set is bounded if for each $x, y \in F$ there exists a positive real number M such that $d(x, y) \leq M$.”
 Give a complete, clear, concise explanation of the problems with this definition.
- (b) Give an example of a metric space and an infinite set that is bounded in that metric. Prove that it is bounded.
- (c) Complete the following definition: Let X be a metric space with metric d and let F be a subset of X . Then F is not bounded if . . .
- (d) Give an example of a metric space and a set that is not bounded in that metric. Prove that it is not bounded.

Problem 25.8. Let X be a set with a metric d . Define a function $d_b : X \times X \rightarrow \mathbb{R}$ by

$$d_b(x, y) = \min\{d(x, y), 1\}.$$

- (a) Show that d_b is a metric on X . This metric is called the **bounded metric associated with d** on X .
- (b) (This part uses Problem 25.7.) Consider the metric space (X, d_b) . Show that in this space, every subset of X is bounded.

Problem 25.9. Let (X, d) be a metric space and let A be a finite subset of X . Must A be bounded? A complete answer to this question will either be a proof that the set A must be bounded, or an explicit example of a metric space X and a finite unbounded subset A . Justify all assertions!

Problem 25.10. Show that in a metric space (X, d) the metric satisfies

$$|d(x, z) - d(y, z)| \leq d(x, y),$$

for all $x, y, z \in X$.

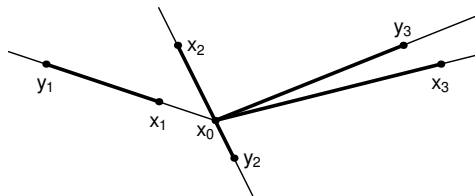


Fig. 25.2 The metric: $d(x_i, y_i)$ for $i = 1, 2, 3$

Problem 25.11. Let X be the space of polynomials with real coefficients. Define a function d from $X \times X \rightarrow \mathbb{R}$ by $d(p, q) = |p(0) - q(0)|$. Is d a metric? If so, prove it. If not, why not?

Problem 25.12. *The following problem is appropriate only if you have had integration in calculus.*

Let X be the space of real-valued continuous functions defined on the interval $[0, 1]$. Define a function $d : X \times X \rightarrow \mathbb{R}$ by

$$d(f, g) = \int_0^1 |f(t) - g(t)| dt,$$

for all $f, g \in X$.

- (a) Show that d is a metric.
- (b) Find the distance between e^x and $\sin(\pi x/2)$.

Problem 25.13. *This problem is appropriate only if you have had integration in calculus.*

Here (X, d) denotes the space of real-valued continuous functions defined on the interval $[0, 1]$ with the metric introduced in Problem 25.12. For each $n \in \mathbb{Z}^+$, we define a function $f_n : [0, 1] \rightarrow \mathbb{R}$ by $f_n(x) = x^n$. Prove that the sequence (f_n) converges in X and find $\lim_{n \rightarrow \infty} f_n$.

Problem 25.14. Choose a fixed point x_0 in \mathbb{R}^2 . If d_u denotes the usual (or Euclidean) metric on \mathbb{R}^2 , then we define $d : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ by

$$d(x, y) = \begin{cases} d_u(x, y) & \text{if } x \text{ and } y \text{ are on a straight} \\ & \text{line through } x_0 \\ d_u(x, x_0) + d_u(x_0, y) & \text{otherwise} \end{cases}.$$

Figure 25.2 illustrates this function for three pairs of points in the plane. Prove that d is a metric on \mathbb{R}^2 .

This metric is sometimes called the “French railway system metric” or the “SNCF metric” (Société Nationale des Chemins de fer Français, see [49, p. 56]). The reason for this is the following: Think of x_0 as Paris, and you’ll note that all trains pass through Paris, whether they need to or not.

Problem 25.15. Let d denote the “SNCF metric” on \mathbb{R}^2 as introduced in Problem 25.14. For $x_1 \in \mathbb{R}^2$ and a positive real number r , sketch the circle $C = \{x \in \mathbb{R}^2 : d(x, x_1) = r\}$. You may find it helpful to consider the three cases, $d(x_0, x_1) = 0$, $0 < d(x_0, x_1) < r$, and $d(x_0, x_1) \geq r$, separately.

Problem 25.16. Prove each of the following.

- Consider \mathbb{R}^2 with the max metric. Prove that $(1/n, 2/n) \rightarrow (0, 0)$.
- Consider \mathbb{R} with the usual metric. Prove that $(-1)^n n / (3n + 1) \not\rightarrow 0$.
- Consider \mathbb{R}^2 with the max metric. Does $((-1)^n, 2/n)$ converge in this space?

Problem 25.17. Consider \mathbb{Z} with the usual metric.

- Show that a sequence that is eventually constant converges; that is, if there exist integers m and k such that $x_n = k$ for all $n \geq m$, then the sequence converges.
- Can you give other examples of convergent sequences in (\mathbb{Z}, d_u) ? Explain your answer.

Problem 25.18. Let (X, d) be a metric space, and let (x_n) be a convergent sequence in X .

- Prove that there exists $x \in X$ and a natural number K such that

$$d(x_n, x) \leq K \text{ for all } n \in \mathbb{N}.$$

(You should know a similar problem.)

- Prove that the set $\{x_n : n \in \mathbb{N}\}$ is bounded; that is, prove that there exists a positive number M such that $d(x_n, x_m) \leq M$ for all $n, m \in \mathbb{N}$.

Problem 25.19. In Problem 20.21 part (c), we defined the term Cauchy sequence and proved some facts about such sequences. This problem asks you to do the same in a general metric space.

- Define a Cauchy sequence in a metric space (X, d) .
- Prove that if (x_n) converges in (X, d) , then (x_n) is Cauchy.

Problem 25.20. (This problem uses Problem 25.19.) Let $X = \mathbb{R} \setminus \mathbb{Q}$ with the usual metric d_u . Prove that the sequence (x_n) , where $x_n = \sqrt{2}/n$, is a Cauchy sequence in X , but (x_n) does not converge in X .

Problem 25.21. Let (X, d) be a metric space. Define a new function $d_e : X \times X \rightarrow \mathbb{R}$ by

$$d_e(x, y) = \frac{d(x, y)}{1 + d(x, y)}.$$

Show that d_e is also a metric on X .

Chapter 26

Getting to Know Open and Closed Sets

When we work in \mathbb{R} with the usual metric, we think of distance as measured by absolute value. Points are close when the absolute value of the difference is small. We might reasonably argue that points x and y are close when they satisfy $|y-x| < r$, where r is a small positive number; that is to say, y is in the open interval $(x-r, x+r)$. This interpretation allows us to visualize the distance between the points. As it turns out, all metrics have this visual interpretation.

Let x be a point in a metric space (X, d) and let r be a real number with $r > 0$. Then the **open ball of radius r about x** is denoted $B_d(x, r)$ and is defined by $B_d(x, r) = \{y \in X : d(y, x) < r\}$. We will call $B_d(x, 1)$ the **open unit ball about x** . Note that the radius of the open ball $B_d(x, r)$ is always positive, and $B_d(x, r)$ is centered at x . This is quite an important definition, and we will be able to do a lot with it. But remember, before you work an example, state a theorem, or write a proof, make sure that you and your intended reader are clear on the space you are working on, the metric you are using, and what you want to show.

Example 26.1. Consider the set \mathbb{R} with the usual metric. What does $B_{d_u}(1, 1/2)$ mean? Describe $B_{d_u}(x, r)$, for an arbitrary $x \in X$ and $r > 0$ as follows: Describe the set in terms of open intervals and sketch the set on a number line.

By definition, $B_{d_u}(1, 1/2) = \{y \in \mathbb{R} : d_u(y, 1) < 1/2\}$. The notation is preventing us from seeing something we all know pretty well, so let's get rid of it. Rewriting,



Fig. 26.1 $B_{d_u}(1, 1/2)$

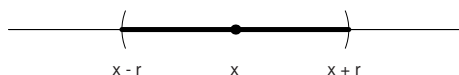


Fig. 26.2 $B_{d_u}(x, r)$

$$\begin{aligned}
 B_{d_u}(1, 1/2) &= \{y \in \mathbb{R} : |y - 1| < 1/2\} \\
 &= \{y \in \mathbb{R} : -1/2 < y - 1 < 1/2\} \\
 &= \{y \in \mathbb{R} : 1/2 < y < 3/2\} \\
 &= (1/2, 3/2).
 \end{aligned}$$

Figure 26.1 shows $B_{d_u}(1, 1/2)$ graphically.

The solution of the general case is the same (see also Figure 26.2): By definition, $B_{d_u}(x, r) = \{y \in \mathbb{R} : d_u(y, x) < r\} = \{y \in \mathbb{R} : |y - x| < r\} = \{y \in \mathbb{R} : -r < y - x < r\} = \{y \in \mathbb{R} : x - r < y < x + r\} = (x - r, x + r)$. Therefore, $B_{d_u}(x, r) = (x - r, x + r)$. \circ

The next example shows that the open balls depend on the underlying set X .

Example 26.2. Consider the set $X = [0, 1)$ with the usual metric. Find the open ball $B_{d_u}(1/4, 2/3)$.

Since the center is $x = 1/4$ and the radius is $r = 2/3$, we find

$$\begin{aligned}
 B_{d_u}(1/4, 2/3) &= \{x \in [0, 1) : |x - 1/4| < 2/3\} \\
 &= \{x \in [0, 1) : -2/3 < x - 1/4 < 2/3\} \\
 &= \{x \in [0, 1) : -5/12 < x < 11/12\} \\
 &= [0, 11/12).
 \end{aligned}$$

\circ

Now it's your turn.

Exercise 26.3. Consider the set \mathbb{R}^2 with the usual metric (defined in Example 25.2). What is the set $B_{d_u}((0, 1), 4)$? Describe the set using precise set notation and sketch it. \circ

These balls can be used to describe the basic structure of metric spaces. For example, for two distinct points x and y in a metric space, we can always find two disjoint open balls, B_x and B_y , such that $x \in B_x$ and $y \in B_y$. This probably agrees with your intuition. On the other hand, as we shall see, there exist metric spaces in which sets consisting of a single point are open balls! In the remainder of this chapter, we will see how these balls can be used to determine which sequences converge. But before we can develop the connection between balls and convergence, we need to

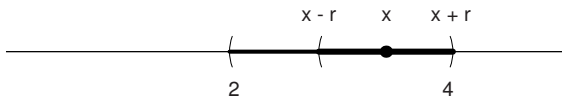


Fig. 26.3 $B_{d_u}(x, r) \subseteq (2, 4)$

look at some of the important sets we can make using these balls together with the set operations we studied earlier.

In a metric space (X, d) , a subset U of X is **open** if for every point $x \in U$, there exists an open ball $B_d(x, r)$ satisfying $B_d(x, r) \subseteq U$. Note that r depends on x , so that as x changes, r will too. This definition is very visual, so pictures will help you. A word of caution is in order before we begin our examples: Throw away any preconceived notions you have about what an open ball should look like.

Example 26.4. Show that the interval $(2, 4)$ is open in \mathbb{R} with the usual metric.

You may be thinking that there’s nothing to show; after all, it’s an open interval. But we still need to use the definition to check that this interval is open in the sense we have defined here, so let’s briefly review exactly what we have to show.

We will show that *for every* $x \in (2, 4)$, there is an open ball $B_{d_u}(x, r) \subseteq (2, 4)$. We know our metric is the usual one, so by Example 26.1, we know we need to show that there exists a positive number r with $(x - r, x + r) \subseteq (2, 4)$. To find r , you should draw pictures whenever you can. Before you read our solution, find your own following this outline: first, draw and label an appropriate picture, which you will then use as you continue on in this proof. Next, pick an *arbitrary* point $x \in (2, 4)$. Now, we need to find a positive number r with $B_{d_u}(x, r) = (x - r, x + r) \subseteq (2, 4)$. Look at your picture to find a possible value of r . Then show that it works.

Proof. We will prove that $(2, 4)$ is open. Let $x \in (2, 4)$. Then $2 < x < 4$, so both $x - 2$ and $4 - x$ are positive. Let $r = \min\{x - 2, 4 - x\}$. (See [Figure 26.3](#).) Then $r > 0$. Now we’ll check that $B_{d_u}(x, r) \subseteq (2, 4)$. So let $y \in B_{d_u}(x, r)$. Then, by definition, $|y - x| < r$. Thus, $-r < y - x < r$. From the upper inequality we obtain $y - x < 4 - x$, and hence $y < 4$. From the lower inequality we obtain $-(x - 2) < y - x$, and hence $2 < y$. Thus, $y \in (2, 4)$, and we conclude that $B_{d_u}(x, r) \subseteq (2, 4)$. □

A few questions and comments are in order. First, don’t forget to check that $r > 0$. An open ball of 0 radius, or (worse yet) negative radius, is no ball at all. Choosing r as the minimum of finitely many real numbers is a pretty standard thing to do, so it’s a good idea to get used to it now. And finally, there are lots of choices for r . We picked one value that worked. Every smaller positive value would work too.

Exercise 26.5. Let (X, d) be a metric space and let $U \subseteq X$. Complete the sentence: The set U is not open in (X, d) if . . .

This is one of those exercises where you will want to check your solution against ours before you go on. So here’s ours: The set U is not open in (X, d) if there exists

a point $x \in U$ such that for every open ball $B_d(x, r)$ about x , there exists a point $y \in B_d(x, r) \cap U^c$. ○

Exercise 26.6. Show that the interval $[2, 4]$ is not open in \mathbb{R} with the usual metric. ○

Exercise 26.7. The setting: \mathbb{R}^2 with the usual metric. Your mission: to show that the open unit ball, $B_{d_u}((0, 0), 1)$, about $(0, 0)$ is open.

Let the following steps guide you:

- (a) Sketch the open ball of radius 1 about the point $(0, 0)$.
- (b) Without thinking too much about it, choose a point in the open ball (make sure you don't choose $(0, 0)$). Make a dot at the point, and label it (a, b) .
- (c) Draw as large an open ball as you can that is still contained in $B_{d_u}((0, 0), 1)$ and centered at your dot (a, b) . What's the radius of that open ball? (Here's a potentially helpful suggestion: draw the radius of the open ball $B_{d_u}((0, 0), 1)$ that passes through the point (a, b) .)
- (d) Now you are ready to start the exercise. Find a positive real number r such that $B_{d_u}((a, b), r)$ appears to be contained in $B_{d_u}((0, 0), 1)$.
- (e) Show that $B_{d_u}((a, b), r) \subseteq B_{d_u}((0, 0), 1)$. Write out the whole proof carefully. Include your picture; it's very helpful for the writer and the reader. ○

There are lots of interesting sets in a metric space, all building on the notion of open ball. We have already introduced open sets. We come now to closed sets. A set E in a metric space X is **closed** if and only if the complement, E^c , is open. So, since the complement of an arbitrary open set is a closed set, we can immediately write down several closed sets. For example, in \mathbb{R} with the usual metric, the set $(-\infty, 2] \cup [4, \infty)$ must be closed, since its complement is the open set $(2, 4)$. (See Example 26.4).

It's important to know many ways to show that sets are open, closed, or neither. Here's a useful result that should have a one-line proof.

Theorem 26.8. *Let (X, d) be a metric space. A subset U of X is open if and only if its complement is closed.*

Exercise 26.9. Find the one- (or two-) line proof of Theorem 26.8. ○

We now have examples of open sets and closed sets. But, as you will see as you work the next two exercises, things often get a bit complicated.

Exercise 26.10. Give an example of a set that is neither open nor closed in \mathbb{R}^2 with the usual metric. ○

Exercise 26.11. Let (X, d) be a metric space. Is the empty set open? closed? both? neither? ○

You might have found yourself concluding that if a set is not open, then it is closed. This is normal, because in ordinary English if a door is not open, then it is closed. Unfortunately, in mathematics, that’s false! In the two exercises above, we have seen examples of sets that are neither open nor closed, and examples of sets that are both open and closed. Don’t assume anything when you work the problems: if we didn’t prove it, state it, or use it, then it may not be true.

We defined an open ball and an open set. You will show (in Problem 26.13) that every open ball is an open set, but since this is so important, we’ll state it as a theorem. It’s interesting to note that the proof is very much like the proof of Exercise 26.7.

Theorem 26.12. *Let (X, d) be a metric space. For every point $x \in X$, and every positive real number r , the set $B_d(x, r)$ is open.*

Now we will get to see some ways that we can use open sets and some more odd properties of metric spaces. The first theorem tightens the relationship between open sets and open balls.

Theorem 26.13. *Let (X, d) be a metric space. A set U is open if and only if there is a subset I of X and a set of radii $\{r_y \in \mathbb{R}^+ : y \in I\}$ such that $U = \bigcup_{y \in I} B_d(y, r_y)$.*

There are some things that might be confusing to you in this statement, but it’s much easier to see what it means to be an open set if you understand Theorem 26.13. The index set is a way of saying that we don’t know how many y we have; there could be finitely many or not, countably many or not, and this way we don’t have to deal with that issue. Next, the r_y might confuse you. Each ball has a (positive) radius, and if we wrote $B_d(y, r)$ for all y , we would be saying that all the balls have the same radius, r . That’s not what the theorem says, so we shouldn’t say that either. By using the notation r_y , we allow each y in I to have its own radius, r_y . Having said all this, we now begin the proof.

Proof. Suppose first that there is a subset I of X such that

$$U = \bigcup_{y \in I} B_d(y, r_y).$$

By the definition of open set, we need to show that for an arbitrary $x \in U$, there exists an open ball $B_d(x, r_x)$ contained in U . Now if $x \in U$, then there exists an element $z \in I$ such that $x \in B_d(z, r_z)$. By Theorem 26.12, the ball $B_d(z, r_z)$ is an open set, and therefore there exists a positive real number s_x such that $B_d(x, s_x) \subseteq B_d(z, r_z)$. Since $B_d(z, r_z) \subseteq U$, we know that $B_d(x, s_x) \subseteq U$. Hence the set U is open.

Now suppose that U is open. We have to find a collection of open balls such that U is the union of those open balls. By the definition of open set, if $x \in U$, there exists an open ball $B_d(x, r_x)$ with $B_d(x, r_x) \subseteq U$. Now we claim that $U = \bigcup_{x \in U} B_d(x, r_x)$. If

we establish this claim, our proof will be complete. To see that U is contained in the union, note that if $y \in U$, then $y \in B_d(y, r_y)$, and therefore $y \in \bigcup_{x \in U} B_d(x, r_x)$. Thus, $U \subseteq \bigcup_{x \in U} B_d(x, r_x)$. To show that U contains the union, note that $B_d(x, r_x) \subseteq U$ for each x . From this it is easy to see¹ that $\bigcup_{x \in U} B_d(x, r_x) \subseteq U$, completing the proof. \square

Theorem 26.13 can be restated as follows: A set U in a metric space X is open if and only if U is a union of open balls.

The proofs of many of the theorems in this chapter provide an excellent opportunity for you to apply all the techniques that you have learned in this course. For this reason, we have left many as problems. Here's another useful theorem.

Theorem 26.14. *An arbitrary union of open sets is open.*

The proof of this is left as a problem (Problem 26.11) for you, the reader. By "arbitrary union" we mean that we don't know how many sets we have. So make sure that you don't accidentally assume that there are finitely many sets, or even countably many.

Theorem 26.15. *An arbitrary intersection of closed sets is closed.*

The proof of this is left for you to do (Problem 26.12). If you have been paying close attention to the theorems and definitions presented thus far, this should follow from Theorem 26.14. What about an intersection of open sets? a union of closed sets? The results are given below and the proofs are outlined in the problems.

Theorem 26.16. *Let U_1, \dots, U_n be open sets. Then $\bigcap_{j=1}^n U_j$ is an open set.*

Theorem 26.17. *Let F_1, \dots, F_n be closed sets. Then $\bigcup_{j=1}^n F_j$ is a closed set.*

We'll conclude this chapter with the metric we promised would challenge your intuition.

Example 26.18. Consider \mathbb{R} with the discrete metric, d_d . Prove the following.

- For each point $x \in \mathbb{R}$, the set $\{x\}$ is an open ball.
- Every set in (\mathbb{R}, d_d) is open.
- Every set in (\mathbb{R}, d_d) is closed.

For part (a), note that for $x \in \mathbb{R}$, the set $\{x\} = B_{d_d}(x, 1/2)$. By Theorem 26.12, the set $B_{d_d}(x, r)$ is an open set and, consequently, $\{x\}$ is open.

For part (b), let S be a subset of \mathbb{R} . Since $S = \bigcup_{s \in S} \{s\}$, from part (a) we see that S is a union of open sets. By Theorem 26.14, S is open.

For part (c), let T be a subset of \mathbb{R} . Then T^c is also a subset of \mathbb{R} , and it follows from part (b) that T^c is open. But a set is closed if and only if its complement is open, and therefore T is closed. \circ

There's lots more that we can do here, and we will do it in the problems.

¹ If this isn't easy to see, show it using an element-chasing argument. In fact, when you worked Exercise 8.10, you already showed it.

Definitions

Definition 26.1. Let x be a point in a metric space (X, d) and let r be a real number with $r > 0$. Then the **open ball of radius r about x** is denoted $B_d(x, r)$ and is defined by $B_d(x, r) = \{y \in X : d(y, x) < r\}$.

Definition 26.2. The **open unit ball about x** in a metric space (X, d) is the open ball $B_d(x, 1)$.

Definition 26.3. In a metric space (X, d) , a subset U of X is **open** if for every point $x \in U$, there exists an open ball $B_d(x, r)$ satisfying $B_d(x, r) \subseteq U$.

Definition 26.4. A set E in a metric space X is **closed** if the complement, E^c , is open.

Definition 26.5 (for Problem 26.18). Let (X, d_X) and (Y, d_Y) be metric spaces. A function $f : (X, d_X) \rightarrow (Y, d_Y)$ **preserves distances** if

$$d_Y(f(x), f(x')) = d_X(x, x')$$

for all x, x' in X .

Definition 26.6 (for Problems 26.19 and 26.20). Let E be a subset of a set X with metric d . A point x is said to be an **interior point** of E if there exists an open ball $B_d(x, r)$ with $B_d(x, r) \subseteq E$. The set of all interior points is called **the interior** of E and is denoted by E° .

Definition 26.7 (for Problems 26.21 through 26.24). Let (X, d) be a metric space. Let $E \subseteq X$. A point $x \in X$ is a **limit point** of E if every open set containing x contains a point $y \in E$ with $y \neq x$. We denote the set of all limit points of the set E by E_l .

Definition 26.8 (for Problem 26.24). Let E be a subset of a metric space X . The **closure** of E is denoted by \bar{E} and is defined by $\bar{E} = E \cup E_l$.

Solutions to Exercises

Solution (26.3). We first calculate $B_{d_u}((0, 1), 4)$. The graphical representation is shown in [Figure 26.4](#).

$$\begin{aligned} B_{d_u}((0, 1), 4) &= \{(x, y) \in \mathbb{R}^2 : d_u((x, y), (0, 1)) < 4\} \\ &= \{(x, y) \in \mathbb{R}^2 : \sqrt{x^2 + (y-1)^2} < 4\} \\ &= \{(x, y) \in \mathbb{R}^2 : x^2 + (y-1)^2 < 16\}. \end{aligned}$$

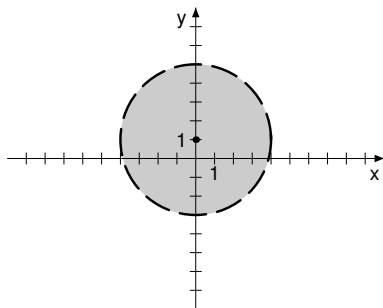


Fig. 26.4 $B_{d_u}((0,1),4)$

Solution (26.6). We will use the solution to Exercise 26.5: Choose $x = 2$ and note that $2 \in [2,4]$. Let $B_{d_u}(2,r)$ be an arbitrary open ball about 2. Then r is a positive real number. We claim that $2 - r/2 \in B_{d_u}(2,r) \cap [2,4]^c$. Since $d_u(2 - r/2, 2) = |(2 - r/2) - 2| = r/2 < r$, we conclude that $2 - r/2 \in B_{d_u}(2,r)$. Also, since $2 - r/2 < 2$ we know that $2 - r/2 \notin [2,4]$. This establishes the claim and we have shown that $[2,4]$ is not open in \mathbb{R} with the usual metric.

Solution (26.7). We follow the outline provided beginning with the illustration in Figure 26.5.

For $(a,b) \in B_{d_u}((0,0),1)$, let $r = 1 - \sqrt{a^2 + b^2}$. Now we claim that $B_{d_u}((a,b),r)$ is an open ball about (a,b) satisfying $B_{d_u}((a,b),r) \subseteq B_{d_u}((0,0),1)$.

For the first part of this claim, note that since $(a,b) \in B_{d_u}((0,0),1)$, we have $d_u((a,b),(0,0)) = \sqrt{a^2 + b^2} < 1$. Hence $r = 1 - \sqrt{a^2 + b^2} > 0$ and $B_{d_u}((a,b),r)$ is an open ball about (a,b) .

To prove the set inclusion, let $(x,y) \in B_{d_u}((a,b),r)$. Then

$$\begin{aligned} d_u((x,y),(0,0)) &\leq d_u((x,y),(a,b)) + d_u((a,b),(0,0)) \\ &\quad \text{(by the triangle inequality for the metric } d_u) \\ &< r + \sqrt{a^2 + b^2} \quad \text{(since } (x,y) \in B_{d_u}((a,b),r)) \\ &= 1 - \sqrt{a^2 + b^2} + \sqrt{a^2 + b^2} = 1. \end{aligned}$$

Hence $(x,y) \in B_{d_u}((0,0),1)$. This establishes the second part of the claim.

The definition of an open set implies that $B_{d_u}((0,0),1)$ is open.

Solution (26.9). By the definition of closed set, the set U^c is closed in a metric space (X,d) if and only if $(U^c)^c = U$ is open in X .

Solution (26.10). The set $A = \{(x,y) : 0 < x \leq 1\}$ is neither open nor closed in \mathbb{R}^2 .

To show that A is not open, consider $(1,0) \in A$. Let $r \in \mathbb{R}$ with $r > 0$. Then $(1 + r/2, 0) \in B_{d_u}((1,0),r)$ and $(1 + r/2, 0) \notin A$. Since r was an arbitrary positive real number we conclude that for each $r \in \mathbb{R}^+$ we have $B_{d_u}((1,0),r) \not\subseteq A$. Hence A is not open.

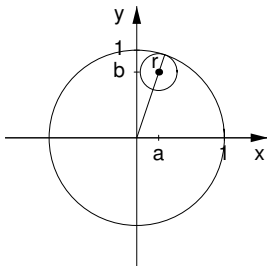


Fig. 26.5 Sketch to find r , the radius of the open ball centered at (a, b)

To show that A is not closed, we will show that A^c is not open. To this end, consider $(0, 0) \in A^c = \{(x, y) \in \mathbb{R}^2 : x \leq 0 \text{ or } x > 1\}$. We may assume that $r < 2$. For every $r \in \mathbb{R}^+$ with $r < 2$ we have $(r/2, 0) \in B_{d_u}((0, 0), r)$ and $(r/2, 0) \notin A^c$. Thus A^c is not open and hence A is not closed.

Solution (26.11). The empty set is open in every metric space (X, d) . The reason is that the antecedent “ $x \in \emptyset$ ” is always false. This means that the defining implication is always true for \emptyset .

The whole space X is also always open: For all $x \in X$, we know that $B_d(x, r) \subseteq X$ for every positive real r . Since $\emptyset^c = X$ and X is open, the definition of closed implies that \emptyset is closed.

Thus we have two examples of sets that are both open and closed: X and \emptyset .

Problems

We continue to assume that X is a metric space with metric d unless otherwise stated.

Problem 26.1. Show that the set $(1, 3) \cup (4, 5)$ is open in \mathbb{R} with the usual metric.

Problem 26.2. Consider \mathbb{R} with the usual metric. In each case, give an example of a nonempty closed set C and a nonempty open set U such that

- (a) $U \cap C$ is open.
- (b) $U \cup C$ is closed.
- (c) $U \cap C$ is neither open nor closed.
- (d) $U \cup C$ is neither open nor closed.

Problem 26.3. Consider the set $A = \{(x, y) \in \mathbb{R}^2 : -1 < x < 0, -1 < y < 1\}$. Prove that A is open in \mathbb{R}^2 with respect to the max metric, d_m . Include a sketch with your proof.

Problem 26.4. Decide whether the statements below are true or false. If the statement is true, give a brief reason why. If the statement is false, give a counterexample.

- (a) In \mathbb{R} with the usual metric, the interval $[0, \infty)$ is a closed set.
- (b) In \mathbb{R} with the discrete metric, the interval $[0, \infty)$ is an open set.
- (c) A finite union of open sets is an open set.
- (d) An arbitrary union of closed sets is a closed set.

Problem 26.5. Consider the set \mathbb{R}^+ with the usual metric.

- (a) Show that the set $(1, \infty)$ is an open set in (\mathbb{R}^+, d_u) .
- (b) Show that the set $(0, 1]$ is a closed set in (\mathbb{R}^+, d_u) .

Problem 26.6. Let (X, d) be a metric space.

- (a) Prove that for all x and y in X , if $y \neq x$, then there exists an open ball centered at y , say $B_d(y, r)$, such that $x \notin B_d(y, r)$.
- (b) Prove that if $x \in X$, then $\{x\}$ is a closed set.

Problem 26.7. Let (X, d) be a metric space. Let $(U_j)_{j=1}^\infty$ be a sequence of open sets.

- (a) Give an example to show that $\bigcap_{j=1}^\infty U_j$ may not be open.
- (b) Is it ever true that $\bigcap_{j=1}^\infty U_j$ is open?

Problem 26.8. Let $E = \{(x, y) \in \mathbb{R}^2 : 1 < x^2 + y^2 < 4\}$. Prove that E is open in \mathbb{R}^2 with respect to the usual metric.

Problem 26.9. Complete the following definition. Let X be a metric space with metric d and let F be a subset of X . Then F is not closed if

- Problem 26.10.**
- (a) Give three examples of sets that are both open and closed in \mathbb{R} with the discrete metric.
 - (b) Give two examples of sets that are both open and closed in \mathbb{R} with the usual metric.
 - (c) Give an example of a set that is neither open nor closed in \mathbb{R}^2 with the max metric. Prove that it is neither open nor closed!
 - (d) Give an example of a set that is closed and not open in \mathbb{R}^2 with the usual metric. Prove that it is closed and not open!

Problem 26.11. Prove Theorem 26.14. (In other words, show that if $\{O_\alpha : \alpha \in I\}$ is a collection of open sets, then $\bigcup_{\alpha \in I} O_\alpha$ is open.)

Problem 26.12. Prove Theorem 26.15.

Problem 26.13. Prove Theorem 26.12.

Problem 26.14. Let (X, d) be a metric space, $x, y \in X$, and let r_1 and r_2 be positive real numbers with $r_1 < r_2$. In what follows, do not use Theorem 26.16.

- (a) Show that $B_d(x, r_1) \subseteq B_d(x, r_2)$.
- (b) From the previous problem we know that every open ball is open. Show that if $B_d(x, r_1)$ and $B_d(y, r_2)$ are open balls, then $B_d(x, r_1) \cap B_d(y, r_2)$ is an open set. Is it an open ball? (Justify your answer to this last question, please.)

Problem 26.15. Prove Theorem 26.16 by completing both steps below. You may find it very helpful to work Problem 26.14 first.

- (a) Show that the intersection of two open sets is an open set.
- (b) Show that the intersection of finitely many open sets is an open set.

Problem 26.16. Prove Theorem 26.17. If you did Problem 26.15, you might consider using that result here.

Problem 26.17. (a) Let x and y be two distinct points in X and let $r = d(x,y)/2$. Show that $B_d(x,r)$ and $B_d(y,r)$ are disjoint sets.

- (b) Show that for two distinct points x and y in a metric space, there exist disjoint open sets \mathcal{O}_x and \mathcal{O}_y with $x \in \mathcal{O}_x$ and $y \in \mathcal{O}_y$.

Problem 26.18. Let (X, d_X) and (Y, d_Y) be metric spaces. We say that a function $f : (X, d_X) \rightarrow (Y, d_Y)$ **preserves distances** if $d_Y(f(x), f(x')) = d_X(x, x')$ for all x, x' in X .

- (a) In \mathbb{R} with the usual metric, the function $f : (\mathbb{R}, d_u) \rightarrow (\mathbb{R}, d_u)$ defined by $f(x) = x$ obviously preserves distances. Give an example of another function that preserves distances.
- (b) Is every function that preserves distances one-to-one? Either prove this statement or give a counterexample.

Problem 26.19. Let E be a subset of a set X with metric d . A point x is said to be an **interior point** of E if there exists an open ball $B_d(x,r)$ with $B_d(x,r) \subseteq E$. The set of all interior points is called **the interior** of E and is denoted by E^o .

- (a) In \mathbb{R} with the usual metric, and $E = (2, 4]$, show that $4 \notin E^o$. Then show that $(2, 4) = E^o$.
- (b) In \mathbb{R}^2 with the max metric, find E^o if $E = \{(x,y) : |x| \leq 1\}$.

Problem 26.20. This problem is only appropriate if you completed Problem 26.19. Let (X, d) be a metric space, and E be a subset of X .

- (a) By the definition of interior point, if $x \in E^o$, then there exists an open ball $B_d(x,r)$ centered at x such that $B_d(x,r) \subseteq E$. Show that, in fact, for each point $x \in E^o$, there exists an open ball $B_d(x, r_x) \subseteq E^o$. Use this to prove that E^o is an open set.
- (b) Prove that a set E is open if and only if every point of E is an interior point. Conclude that a set E is open if and only if $E = E^o$.

Problem 26.21. Let (X, d) be a metric space. Let $E \subseteq X$. A point $x \in X$ is a **limit point** of E if every open set containing x contains a point $y \in E$ with $y \neq x$. Let E_l denote the set of all limit points of the set E .

- (a) Complete the following definition. A point $x \in X$ is not a limit point of E if

- (b) What are the limit points of the interval $(2, 4]$ in \mathbb{R} with the usual metric? the discrete metric?
- (c) What are the limit points of $B_{d_u}((0, 0), 1)$ in \mathbb{R}^2 with the usual metric? the discrete metric?
- (d) What are the limit points of $\{1/n : n \in \mathbb{Z}^+\}$ in \mathbb{R} with the usual metric? the discrete metric?

Problem 26.22. (This problem assumes that you have completed Problem 26.21.) Let (X, d) be a metric space. Let E be a subset of X . Show that x is a limit point of a set E if and only if every open ball $B_d(x, r)$ about x contains a point $y \in E$ with $y \neq x$.

Problem 26.23. (This problem assumes that you have completed Problem 26.21.) Let (X, d) be a metric space. Let E be a subset of X .

- (a) Prove that x is a limit point of a set E if and only if every open set about x contains infinitely many points different from x .
- (b) Prove that a finite set has no limit points.

Problem 26.24. (This problem assumes that you have completed Problem 26.21.) Let (X, d) be a metric space. Let E be a subset of X .

- (a) Show that E is closed if and only if E contains all its limit points. In other words, prove that E is closed if and only if $E_l \subseteq E$.
- (b) Let E be a set. The **closure** of E is denoted by \overline{E} and is defined by $\overline{E} = E \cup E_l$. Show that if x is a limit point of \overline{E} , then x is a limit point of E .
- (c) Show that if x is a limit point of \overline{E} , then $x \in \overline{E}$ (note that you did the hard part in (b) above). Conclude that \overline{E} is closed.

Chapter 27

Modular Arithmetic

You began your mathematical education adding, subtracting, multiplying, and dividing integers. From there you moved on to rational numbers, then to real numbers, and, perhaps, to complex numbers. But this is not the only kind of arithmetic mathematicians study. In fact, there's a very different kind of arithmetic that you use every single day. The popular name for these calculations is *clock arithmetic*, and it is indeed based upon the clock.

Consider the following scenario: Suppose it is now 3:00 P.M., and you start on a 28-hour trip. What time will it be when you return? A quick calculation yields an answer of 7:00 P.M. How did you arrive at this answer? You did something we all find natural—you did clock arithmetic. We will build carefully upon this idea, and we will apply many of the concepts we have already covered to help us understand it.

Clock arithmetic isn't done on numbers, but rather on equivalence classes of numbers. So we need to find the right equivalence relation. Recall that for two integers a and b with $a \neq 0$, we say that a divides b , written $a \mid b$, if there is an integer k such that $b = ak$. Now we are ready for the equivalence relation. Let $n \in \mathbb{Z}$ be such that $n > 1$. Two integers x and y will be related if $n \mid (y - x)$. In this case we say x is **congruent to y modulo n** , and we will write $x \equiv y \pmod{n}$.

Exercise 27.1. Find five different solutions to each of the problems below, and then find five integers that are not solutions.

- (a) Find $x \in \mathbb{Z}$ such that $5 \equiv x \pmod{12}$.
- (b) Find $x \in \mathbb{Z}$ such that $x > 1$ and $-3 \equiv 39 \pmod{x}$. ○

Theorem 27.2. Let $n > 1$ be an integer. The relation congruence modulo n is an equivalence relation on \mathbb{Z} .

The proof of this theorem is left as Problem 27.3.

For an integer $n > 1$, the set of all equivalence classes with respect to the relation congruence modulo n is called the **integers modulo n** and denoted by \mathbb{Z}_n . It follows from Theorem 11.4 that \mathbb{Z}_n is a partition of \mathbb{Z} . There will be times when we will

need to refer to the elements of \mathbb{Z}_n , and since these are equivalence classes and not just integers, the notation must be chosen carefully. So we introduce the following: for $m \in \mathbb{Z}$, we write $[m]_n = \{x \in \mathbb{Z} : n \mid (x - m)\}$.

Note that we now have two ways of denoting exactly the same thing. For integers a, b , and n with $n > 1$, the two statements “ $a \equiv b \pmod{n}$ ” and “ $[a]_n = [b]_n$ ” are equivalent.

Let us stop and think about what this all means in the context of time. Suppose we are told that, “in this camp, breakfast is served at 7:00 A.M.” What does this mean? Is there exactly one instant on a certain day and time at which breakfast is served? This can hardly be the case, since we eat breakfast every day. What it must mean is that breakfast is served at 7:00 A.M. today, tomorrow, yesterday, and in a week. So 7:00 A.M. actually represents many different times, as long as the difference between that time and 7:00 A.M. is a multiple of 24 hours. Mathematically, this idea is expressed by an equivalence class. The class of 7 modulo 24 is the set of all integers that differ from 7 by a multiple of 24. Thus,

$$[7]_{24} = [31]_{24} = [-41]_{24} = \cdots = \{\dots, -41, -17, 7, 31, 55, \dots\}.$$

The “numbers” in modular arithmetic are sets of numbers.

Before exploring some of the properties of the integers modulo n , we need to learn a bit more about the integers themselves. You are no doubt familiar with these properties of the integers, but you may not know the rigorous definitions or the exact statements of the theorems. The first statement, which was introduced in Problem 13.22, is simply about division of one integer by another.

Theorem 27.3 (Division algorithm). *Let m and n be integers with $n \neq 0$. Then there exist unique integers q and r such that $m = nq + r$ and $0 \leq r < |n|$.*

In plain English, the division algorithm says that for two integers, m and n , we can write m as a multiple of n plus what’s left over. Of course, that’s just the statement that q is the quotient and r the remainder when we divide m by n . You might not understand why we need to prove this—after all, you have been using it for a long time. But did you ever stop to think about what it really means and why it is true? In fact, if you worked Problem 13.22, then you already proved this theorem following the outline that was provided. (The statement of the result was presented in Theorem 13.6.) If you have not already done so, this would be the right moment to return to that problem and the outline and produce a proof of the division algorithm. We’ll need this result very soon.

Let’s move on to another old friend from the past. Given two numbers, say 28 and 42, what is the gcd (or greatest common divisor) of the two numbers? You can probably figure out, without too much trouble, that the answer is 14. But now that you have much more mathematical experience, we are able to ask (and answer) the more complicated questions of “how can we give a precise definition of gcd?” and “is there an algorithm to find its value?”

Define the **greatest common divisor** d (which we’ll soon see is unique) of two integers m and n , where m and n are not both zero, to be the positive integer d that satisfies

- (i) $d|m$ and $d|n$, and
- (ii) if s is a positive integer such that $s|m$ and $s|n$, then $s|d$.

We denote the greatest common divisor of m and n by $\gcd(m, n)$. We say m and n are **relatively prime** if $\gcd(m, n) = 1$.

- Exercise 27.4.** (a) What does condition (i) of the definition of the greatest common divisor really say?
 (b) What does condition (ii) really say?
 (c) We mentioned that the gcd of two numbers is unique. How would you try to prove this? ○

Exercise 27.5. Find $\gcd(-16, 40)$, $\gcd(0, 45)$, and $\gcd(-30, -27)$. ○

The next theorem tells us that the gcd always exists and is, as we promised, unique.

Theorem 27.6. *Let m and n be integers, not both zero. Then their greatest common divisor exists, is unique, and there are integers k and l such that $\gcd(m, n) = km + ln$.*

This theorem actually tells us more than the existence and uniqueness of the greatest common divisor. It tells us that the gcd can be expressed as the sum of multiples of the two numbers m and n . This fact is certainly not obvious, and it will turn out to be very useful. A sum of the form $km + ln$ where k and l are integers is called a linear combination of m and n . Theorem 27.6 is usually proved by first showing that $\gcd(m, n) = km + ln$. The proof looks at the set A of all the linear combinations of m and n that yield a positive integer. Since A will be a nonempty set of positive integers, the well-ordering principle tells us that this set has a smallest element. It turns out that this element will satisfy both (i) and (ii) in the definition of greatest common divisor. Once we have shown this, we will still need to present an argument that there is no other integer that is also the gcd of m and n .

Proof. For $m, n \in \mathbb{Z}$ not both zero, define $A = \{xm + yn : x, y \in \mathbb{Z} \text{ and } xm + yn > 0\}$. First we'll show that $A \neq \emptyset$. We know that $m, n \in \mathbb{Z}$, and so we may set $x = m$ and $y = n$. Since $m \neq 0$ or $n \neq 0$, we conclude that $xm + yn = m^2 + n^2 > 0$, and hence $m^2 + n^2 \in A$. Thus $A \neq \emptyset$. By the well-ordering principle, every nonempty set of positive integers has a smallest element, and we call this element d . Since $d \in A$, there exist $x_0, y_0 \in \mathbb{Z}$ such that $d = x_0m + y_0n$. We will show that $d = \gcd(m, n)$, proving two parts of the theorem, namely, that a greatest common divisor exists, and that this divisor can be written in the form $km + ln$ for some $k, l \in \mathbb{Z}$.

Since $d \in A$, we know that $d > 0$. By the division algorithm (Theorem 27.3), we can write $m = qd + r$, where q and r are two integers with $0 \leq r < d$. Therefore $r = m - dq = m - (x_0m + y_0n)q = (1 - x_0q)m + (-y_0q)n$, where $1 - x_0q$ and $-y_0q$ are integers. Now if $r > 0$, then r would be an element of A . But $r < d$ and d is the smallest element of A . This means that $r \notin A$. Hence it must be the case that $r = 0$;

in other words, $d|m$. Exactly the same argument shows that $d|n$. Thus $d|m$ and $d|n$, and (i) in the definition of gcd holds.

Suppose that s is a positive integer such that $s|m$ and $s|n$. Since $d = x_0m + y_0n$, we conclude that $s|d$. (You are asked to write out the details of this last step in Problem 27.1.) Hence (ii) also holds for d . We now know that a greatest common divisor exists and has the right form. It remains to show that it is unique.

So suppose that d and t are both greatest common divisors of m and n . Then, since d is a gcd, property (ii) of the definition says that $t|d$. On the other hand, t is a gcd, so $d|t$. We conclude that $t|d$ and $d|t$. Since both t and d are positive integers it follows (see Problem 27.2) that $t = d$, completing the proof of uniqueness. \square

Incidentally, while the greatest common divisor d is unique, the integers x_0 and y_0 , as defined in the proof, are not. Here is a simple example: Consider the integers $m = 6$ and $n = 9$. Then

$$\gcd(6, 9) = 3 = 2 \cdot 6 + (-1) \cdot 9 = (-1) \cdot 6 + 1 \cdot 9.$$

Unfortunately, the proof of Theorem 27.6 was not constructive; that is, it's a nice enough proof, but it doesn't really tell us how to find $\gcd(m, n)$. However, there is an algorithm to do just that—one that appeared in Euclid's *Elements* over 2,300 years ago. The algorithm is appropriately called the *Euclidean algorithm* and you will learn to apply it in Problem 27.20 to calculate the gcd of two integers.

We now return to modular arithmetic. To get you back into the proper state of mind, we suggest that you reread (in the beginning of this chapter) what it means for two integers to be equivalent modulo n , where $n > 1$. Then work the following exercise:

Exercise 27.7. Show that for integers m and n with $n > 1$, there exists an integer r satisfying $0 \leq r < n$ such that $m \equiv r \pmod{n}$. \circ

One good thing about the integers is that we can perform basic algebraic manipulations on them, like adding, subtracting, and multiplying. Can we do this on \mathbb{Z}_n also? The answer is yes, but we must first carefully define how these operations work on the equivalence classes that make up the set \mathbb{Z}_n . That's what we will do right after we work an example to remind you what it means for two equivalence classes modulo n to be the same.

Example 27.8. For integers r, s , and n with $n > 1$, prove that $[r]_n = [s]_n$ if and only if there exists $k \in \mathbb{Z}$ such that $r - s = kn$.

Proof. By Problem 10.10, $[r]_n = [s]_n$ if and only if $r \sim s$. Thus $[r]_n = [s]_n$ if and only if $r \equiv s \pmod{n}$. Hence $[r]_n = [s]_n$ if and only if there exists an integer k such that $r - s = kn$. \square

Be sure to keep this fact in mind as you read on in the text, and especially as you work your way through Example 27.9, in which we will show that multiplication on \mathbb{Z}_n , as introduced below, is well-defined.

Fix an integer $n > 1$. Now \mathbb{Z}_n is closely related to \mathbb{Z} , so we will try to modify the operations of \mathbb{Z} so that they apply to \mathbb{Z}_n . For $r, s \in \mathbb{Z}$, define

$$[r]_n + [s]_n = [r + s]_n, [r]_n - [s]_n = [r - s]_n, \text{ and } [r]_n \cdot [s]_n = [rs]_n.$$

Before going on, convince yourself that

$$[12]_5 + [7]_5 = [4]_5, [12]_5 - [7]_5 = [0]_5, \text{ and } [12]_5 \cdot [7]_5 = [4]_5.$$

These definitions amount to defining three functions from $\mathbb{Z}_n \times \mathbb{Z}_n$ to \mathbb{Z}_n , and we need to show that they are well-defined. We will provide a complete proof for the operation of multiplication, and we will leave addition and subtraction to you in Problem 27.11.

Example 27.9. Define $f : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, by $f([r]_n, [s]_n) = [rs]_n$. Then f is a well-defined function that yields a multiplication on \mathbb{Z}_n .

“Understanding the problem.” To show that a function is well-defined, we need to prove two things. (i) We must show that f maps $\mathbb{Z}_n \times \mathbb{Z}_n$ into \mathbb{Z}_n . In other words, we must show that for every element x in $\mathbb{Z}_n \times \mathbb{Z}_n$, there exists an element y in \mathbb{Z}_n such that $f(x) = y$. It is important to recall that when an element of a set can be written in a special form, as is the case with x in $\mathbb{Z}_n \times \mathbb{Z}_n$, we should take advantage of it. So if x is in $\mathbb{Z}_n \times \mathbb{Z}_n$, then there exist integers r and s such that $x = ([r]_n, [s]_n)$.

(ii) We must also show that, for x in $\mathbb{Z}_n \times \mathbb{Z}_n$, if $f(x) = y$ and $f(x) = z$, then $y = z$. Again, we will expect to use the special form of x, y , and z . Now x can be written as $([r]_n, [s]_n)$ for some integers r and s . Our function f is supposed to look at the pair of equivalence classes, choose an integer from each (they could be r and s , but don't have to be), multiply these together, and produce the resulting equivalence class.

What could possibly go wrong? Let us look at an example. We know that $[7]_6 = [19]_6$, because $6 \mid (19 - 7)$. By the definition of multiplication in \mathbb{Z}_6 , we write $[7]_6 \cdot [4]_6 = [28]_6$ and $[19]_6 \cdot [4]_6 = [76]_6$. The left sides of both equations are the same, so the right sides had better be the same as well, or we have a fatal problem on our hands. Are they the same? Our proof will need to show that the result of the multiplication operation is independent of the particular integers we used to represent the equivalence classes.

“Devising a plan.” To prove part (i), we have to show that f is defined for every element of $\mathbb{Z}_n \times \mathbb{Z}_n$, and yields an element in \mathbb{Z}_n . For part (ii), we let $x \in \mathbb{Z}_n \times \mathbb{Z}_n$ and suppose that $f(x) = y$ and $f(x) = z$. We must show that $y = z$. Now, we can assume that there exist integers r, s, u , and v such that $x = ([r]_n, [s]_n) = ([u]_n, [v]_n)$ and $y = f([r]_n, [s]_n) = [rs]_n$, while $z = f([u]_n, [v]_n) = [uv]_n$. Therefore we must show that $[rs]_n = [uv]_n$. By Example 27.8, we know that this means that we must show that there exists an integer m such that $rs - uv = mn$. How can we show that such an integer m exists? By using what we know, namely, that $([r]_n, [s]_n) = ([u]_n, [v]_n)$. Looks like we are now ready to carry out our plan.

Proof. Let $x \in \mathbb{Z}_n \times \mathbb{Z}_n$. Then $x = ([r]_n, [s]_n)$ for some $r, s \in \mathbb{Z}$. Hence, $rs \in \mathbb{Z}$, and therefore $[rs]_n \in \mathbb{Z}_n$. By the definition of f , we have $f(x) = [rs]_n$. Thus, f maps $\mathbb{Z}_n \times \mathbb{Z}_n$ to \mathbb{Z}_n .

Again let $x \in \mathbb{Z}_n \times \mathbb{Z}_n$. We consider two arbitrary representations of x , say $x = ([r]_n, [s]_n)$ and $x = ([u]_n, [v]_n)$. Then $f(x) = [rs]_n$ and $f(x) = [uv]_n$. We need to show that $[rs]_n = [uv]_n$. Since $([r]_n, [s]_n) = ([u]_n, [v]_n)$, the definition of ordered pair implies that $[r]_n = [u]_n$ and $[s]_n = [v]_n$. Thus

$$u - r = kn, \quad \text{for some } k \in \mathbb{Z}, \text{ and} \quad (27.1)$$

$$v - s = ln, \quad \text{for some } l \in \mathbb{Z}. \quad (27.2)$$

To show that $[rs]_n = [uv]_n$, we calculate

$$\begin{aligned} uv - rs &= uv - rv + rv - rs \\ &= (u - r)v + r(v - s) \\ &= knv + rln \quad (\text{using equations (27.1) and (27.2)}) \\ &= (kv + rl)n. \end{aligned}$$

Now $kv + rl \in \mathbb{Z}$ and, by Example 27.8, $[rs]_n = [uv]_n$. Thus f is well-defined, as desired. \square

Exercise 27.10. Define “modular exponentiation” as follows: For an integer $n > 1$ and $a, b \in \mathbb{Z}$, define $[a]_n^{[b]_n} = [a^b]_n$. Either prove that this operation is well-defined, or give an example to show that modular exponentiation is not well-defined. \circ

In \mathbb{Z}_n , the operations of multiplication and addition are commutative and associative. The set \mathbb{Z}_n has an additive identity; that is, there is an element $\theta \in \mathbb{Z}_n$ such that $x + \theta = x$ for all $x \in \mathbb{Z}_n$ (namely, $\theta = [0]_n$). Similarly, \mathbb{Z}_n has a multiplicative identity; that is, there is an element $e \in \mathbb{Z}_n$ such that $x \cdot e = x$ for all $x \in \mathbb{Z}_n$ (namely, $e = [1]_n$). Further, every element of \mathbb{Z}_n has an additive inverse; that is, for every $x \in \mathbb{Z}_n$ there is $y_x \in \mathbb{Z}_n$ such that $x + y_x = [0]_n$ (if $x = [r]_n$, then $-x = [-r]_n$). Multiplication is also distributive over addition. (See Problem 27.14.) Thus, they satisfy everything you might reasonably hope an operation would satisfy except for one thing: not every nonzero element has a multiplicative inverse. The following immediate consequence of Theorem 27.6 tells us something about reciprocals in \mathbb{Z}_n .

Corollary 27.11. *Let n be a positive integer with $n > 1$. Then for every integer a with $\gcd(a, n) = 1$, there exists an integer b such that $ab \equiv 1 \pmod{n}$.*

Before proceeding to the proof of the corollary, write out what it means to say that $ab \equiv 1 \pmod{n}$.

Proof. Since $\gcd(a, n) = 1$, Theorem 27.6 tells us that there exist $b, c \in \mathbb{Z}$ such that $ba + cn = 1$. Then $ba - 1 = (-c)n$ and $-c \in \mathbb{Z}$. Thus, $ab \equiv 1 \pmod{n}$. \square

For an integer a to satisfy the hypothesis of this corollary, a needs to be relatively prime to the modulus n . Is it possible that we have two integers, a and b with $a \equiv b \pmod{n}$, such that one of the integers, say a , satisfies the hypothesis and the other one, b , does not? The answer to this query is no, as we see from the following lemma:

Lemma 27.12. *Let a, c , and n be integers with $n > 1$ and such that $a \equiv c \pmod{n}$. Then $\gcd(a, n) = 1$ if and only if $\gcd(c, n) = 1$. Further, if b and d are integers such that $ab \equiv 1 \pmod{n}$ and $cd \equiv 1 \pmod{n}$, then $b \equiv d \pmod{n}$.*

The proof of this lemma requires the multiplication defined on \mathbb{Z}_n earlier in this chapter, and the (easily checked) algebraic properties of this multiplication. (See Problem 27.14.)

Proof. For the first part of the proof, we prove the contrapositive; that is, we prove that if $\gcd(c, n) \neq 1$, then $\gcd(a, n) \neq 1$. So assume that $\gcd(c, n) = k > 1$. Since $a \equiv c \pmod{n}$, we conclude that $a - c = ln$ for some $l \in \mathbb{Z}$. Hence $a = c + ln$. But $k|c$ and $k|n$, so $k|a$. By (ii) in the definition of \gcd , we conclude that $k|\gcd(a, n)$. Thus $\gcd(a, n) > 1$. The converse is obtained by interchanging the roles of a and c .

For the second part of the proof, we use our assumptions: $[a]_n[b]_n = [ab]_n = [1]_n$, $[c]_n[d]_n = [cd]_n = [1]_n$, and $[a]_n = [c]_n$. Thus, we calculate

$$[b]_n = [bcd]_n = [bad]_n = [abd]_n = [d]_n,$$

and we conclude that $b \equiv d \pmod{n}$. □

Taken together, the corollary and the lemma tell us that if an integer a is relatively prime to n , then there exists an integer b such that the equivalence classes satisfy $[a]_n \cdot [b]_n = 1$. So, for a relatively prime to n , the equivalence class has something that should remind you of a reciprocal. This leads to the following definition: For a, b , and $n \in \mathbb{Z}$ with $n > 1$, we call b a **reciprocal modulo n** of a if $ab \equiv 1 \pmod{n}$. The notation is $b \equiv a^{-1} \pmod{n}$.

Exercise 27.13. (a) Find the reciprocals modulo 7 of 3, 5, and 6.

(b) Which elements of \mathbb{Z}_6 have reciprocals modulo 6 and which do not? ○

The use of modular arithmetic is widespread. Every time you are on the Web, your browser is likely to make your transactions secure using an encryption that is based on modular arithmetic. (Work Project 29.13 on codes to see one such use.) We motivated the ideas in the chapter using time and calculations modulo 24. If you schedule tasks by days of the week you probably want to calculate with modulus 7; if you are interested in a monthly schedule, the modulus is 12. In fact, now that we've mentioned it, you can surely think of many other times when you have used modular arithmetic.

Definitions

Definition 27.1. Let $n \in \mathbb{Z}$ with $n > 1$. Integers x and y will be related if $n|(y - x)$. In this case, we say that x is **congruent to y modulo n** , and we write $x \equiv y \pmod{n}$.

Definition 27.2. For an integer $n > 1$, the set of all equivalence classes with respect to the relation congruence modulo n is called the **integers modulo n** and denoted by \mathbb{Z}_n .

Definition 27.3. The **greatest common divisor** of two integers m and n , where m and n are not both zero, is the positive integer d that satisfies

- (i) $d|m$ and $d|n$, and
- (ii) if s is a positive integer such that $s|m$ and $s|n$, then $s|d$.

It is denoted by $\gcd(m, n)$.

Definition 27.4. Two integers m and n are **relatively prime** if $\gcd(m, n) = 1$.

Definition 27.5. For a, b , and $n \in \mathbb{Z}$ with $n > 1$, we call b a **reciprocal modulo n** of a if $ab \equiv 1 \pmod{n}$. The notation is $b \equiv a^{-1} \pmod{n}$.

Solutions to Exercises

Solution (27.1).

- (a) We defined $5 \equiv x \pmod{12}$ by $12 \mid (x - 5)$. Some possible values for x are: 5, 17, 125, -7 , -115 . Some values that do not work are: 0, 7, 1200, -5 , -12 .
- (b) The equivalence $-3 \equiv 39 \pmod{x}$ is defined by $x|42$ where x is an integer greater than 1. The set of all positive factors greater than 1 of 42 is the set $A = \{2, 3, 6, 7, 14, 21, 42\}$. Any five integers from A will work. The five non-solutions must be chosen from the integers greater than 1 that are not in A .

Solution (27.4).

- (a) Condition (i) says that the greatest common divisor divides both integers. In other words, it is a statement about being a common divisor.
- (b) Condition (ii) says that every other positive integer that divides both m and n also divides the $\gcd(m, n)$, and therefore is a factor of it. In other words, the second condition explains the choice of the word “greatest.”
- (c) We will need to prove the uniqueness of the greatest common divisor. To do so, we will prove that if there are integers d_1 and d_2 , both satisfying the definition of greatest common divisor, then $d_1 = d_2$.

Solution (27.5). We list the answers here: $\gcd(-16, 40) = 8$, $\gcd(0, 45) = 45$, and $\gcd(-30, -27) = 3$.

Solution (27.7). The integers m and n are given and $n > 1$. By Theorem 27.3, there are $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r < n$. Hence $m - r = nq$ for some $q \in \mathbb{Z}$. Thus $m \equiv r \pmod{n}$ and $0 \leq r < n$.

Solution (27.10). This is not well-defined. Let $n = 5$. Then $2 \equiv 7 \pmod{5}$. Now $[3]_5^{[2]_5} = [4]_5$ and $[3]_5^{[7]_5} = [2]_5$, but $4 \not\equiv 2 \pmod{5}$.

Solution (27.13).

- (a) Check that $3^{-1} \equiv 5 \pmod{7}$, $5^{-1} \equiv 3 \pmod{7}$, and $6^{-1} \equiv 6 \pmod{7}$.
 (b) By Corollary 27.11, the integers 1 and 5 have reciprocals modulo 6; it is easy to check that none of the others does.

Problems

Problem 27.1. Let a, b, c, x , and $y \in \mathbb{Z}$. Prove that if $a|b$ and $a|c$, then $a|(bx + cy)$.

Problem 27.2. Let a and b be positive integers such that $a|b$ and $b|a$. Prove that $a = b$.

Problem 27.3. Prove Theorem 27.2. (Note that this generalizes part (c) of Problem 10.2.)

Problem 27.4. Carefully read the definition of greatest common divisor. What should the least common multiple of two integers be? Make up a definition for it. The least common multiple of two integers m and n is denoted by $\text{lcm}(m, n)$.

Problem 27.5. Using your definition from Problem 27.4 and the notation defined above, prove that if m and n are positive integers, then

$$\gcd(m, n) \cdot \text{lcm}(m, n) = mn.$$

Problem 27.6. Let $m, n \in \mathbb{Z}$, not both zero. Suppose that a is an integer that divides both m and n and whenever s is an integer dividing both m and n , then $s \leq a$. Prove that $a = \gcd(m, n)$.

Problem 27.7. Let $m, n \in \mathbb{Z}$ and assume that $m \neq 0$. Prove the following statements.

- (a) For all positive integers k , we have $\gcd(mk, nk) = k \gcd(m, n)$.
 (b) If $d = \gcd(m, n)$ and $k, l \in \mathbb{Z}$, then $\gcd(m, n) | \gcd(m + kd, n + ld)$.

Problem 27.8. Let p be a prime number and $a, b \in \mathbb{Z}$. Prove that if $p|ab$, then $p|a$ or $p|b$. (You may use Theorem 27.6 to solve this problem.)

Problem 27.9. Here is another theorem that you have been using for a long time.

Theorem 27.14 (Fundamental theorem of arithmetic). *Every integer n , where $n \geq 2$, is the product of prime numbers. This factorization is unique, up to the order of the factors.*

If you worked Problem 18.21, then you already proved that such a factorization exists. You will still need to prove uniqueness of the factorization. (You may use induction and the result of Problem 27.8 to do so.)

Problem 27.10. Let $p > 1$ be an integer with the property that for all integers a and b , if $p|ab$, then $p|a$ or $p|b$. Prove that p is prime.

(In your future mathematics courses you will see that this is a more useful definition of prime than the one to which you have become accustomed.)

Problem 27.11. Let $n > 1$ be an integer.

- (a) Define $g : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ by $g([r]_n, [s]_n) = [r + s]_n$. Prove that g is well-defined.
- (b) Define $h : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ by $h([r]_n, [s]_n) = [r - s]_n$. Prove that h is well-defined.

Problem 27.12. Define $f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{24}$ by $f([x]_{12}) = [3x]_{24}$. Is f well-defined? Prove your claim.

Problem 27.13. Let p be an odd prime and define $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ by $f([x]_p) = [2x]_p$. Prove that f is well-defined and that f is a bijection.

Problem[#] 27.14. Let $n > 1$ be an integer. Using the addition and multiplication defined on \mathbb{Z}_n in this chapter, prove the following statements:

- (a) $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$ for all $a, b, c \in \mathbb{Z}$;
- (b) there is an integer $\theta \in \mathbb{Z}$ such that
 - (i) $[a]_n + [\theta]_n = [\theta]_n + [a]_n = [a]_n$ for all $a \in \mathbb{Z}$, and
 - (ii) for every $a \in \mathbb{Z}$, there is $b \in \mathbb{Z}$ such that $[a]_n + [b]_n = [b]_n + [a]_n = [\theta]_n$;
- (c) $[a]_n + [b]_n = [b]_n + [a]_n$ for all $a, b \in \mathbb{Z}$;
- (d) $([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$ for all $a, b, c \in \mathbb{Z}$;
- (e) $[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$ and $([a]_n + [b]_n) \cdot [c]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n$ for all $a, b, c \in \mathbb{Z}$;
- (f) there is an element $e \in \mathbb{Z}$ such that $[a]_n \cdot [e]_n = [e]_n \cdot [a]_n = [a]_n$ for all $a \in \mathbb{Z}$;
- (g) $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$ for all $a, b \in \mathbb{Z}$.

(A set with two well-defined operations satisfying (a)–(g) is called a “commutative ring with identity.”)

Problem 27.15. You may know the following criterion for divisibility by nine: A positive integer is divisible by nine if and only if the sum of its digits is divisible by nine.

- (a) Prove this criterion.
- (b) Is 47832973 divisible by 9?

A variation of the divisibility criterion is the calculation check called “casting out nines.” We may use this to check an addition, subtraction, multiplication, or division (turning the division into a multiplication before checking) of integers by replacing each integer by the sum of its digits (repeating the summation until the integer is a single digit). If our computation does not pass this check, it was incorrect. (However, it may pass the check and still be an incorrect computation!) For instance: To check that

$$56782351912/25785 = 2202146 \text{ plus a remainder of } 17302,$$

we first write this as

$$56782351912 = 25785 \cdot 2202146 + 17302.$$

Now we “cast out nines”:

$$4 = 0 \cdot 8 + 4,$$

and we see that our “check” is consistent with the process of casting out nines. However, if we had

$$56782341912 = 25785 \cdot 2202146 + 17202,$$

our “check” would yield

$$4 = 0 \cdot 8 + 3,$$

and we would be alerted to an error.

- (c) Explain “casting out nines” (use your work from part (a)).
- (d) Find an example that shows that it is possible to have a situation in which the check works, but the original computation is incorrect.

Problem 27.16. Let n be an integer with $n > 1$. Prove that the following are equivalent.

1. For all m , if $m \not\equiv 0 \pmod{n}$, then m has a reciprocal modulo n .
2. The integer n is prime.

(This makes \mathbb{Z}_p , where p is prime, as good a set to do arithmetic in as \mathbb{Q} . As far as multiplication is concerned, \mathbb{Z}_p is better than \mathbb{Z} , because very few numbers (two, to be exact) in \mathbb{Z} have reciprocals that also lie in \mathbb{Z} . The set, \mathbb{Z}_p , for p a prime, is what is called a “field” in mathematics. Other examples include \mathbb{Q} , \mathbb{R} , and \mathbb{C} . The set \mathbb{Z} is not a field.)

Problem 27.17. (This problem is appropriate only if you studied Chapter 22.) Use the result of Exercise 27.7 to show that $|\mathbb{Z}_n| = n$.

Problem 27.18. Find *all* solutions in \mathbb{Z}_n for the following equivalences:

- (a) $3x \equiv 0 \pmod{12}$;
- (b) $3x \equiv 0 \pmod{17}$;
- (c) $3x \equiv 0 \pmod{10}$.

Problem 27.19. Find *all* solutions in \mathbb{Z}_n for the following equivalences:

- (a) $4x \equiv 1 \pmod{11}$;
- (b) $4x \equiv 1 \pmod{9}$;
- (c) $3x \equiv 1 \pmod{11}$;
- (d) $3x \equiv 1 \pmod{9}$.

Problem[#] 27.20. Here's a brief explanation of the Euclidean algorithm, which is an effective way to find the greatest common divisor of two integers m and n , not both zero. This algorithm is in the seventh book of Euclid's *Elements*, but was likely known earlier.

There are two trivial cases that must be considered before moving to the interesting one. If $m = n$, then the greatest common divisor is obviously $|m|$. If one of the integers is zero (remember that both can't be zero), then the greatest common divisor is the absolute value of the nonzero integer. Now for the main case, note that the positive divisors of an integer m are the same as the ones of $-m$. For this reason, we may assume that both m and n are positive. After possible relabeling of the two numbers, we may further assume that $m > n > 0$.

The Euclidean algorithm is a repeated application of the division algorithm, Theorem 27.3. Each line is obtained from the previous one by shifting the divisor to the spot previously occupied by the dividend, and the remainder to the spot previously occupied by the divisor. It's easier to see than to say. Here is the way to see it:

$$\begin{aligned} m &= q_1n + r_1, \\ n &= q_2r_1 + r_2, \\ r_1 &= q_3r_2 + r_3, \\ &\dots \\ r_{k-3} &= q_{k-1}r_{k-2} + r_{k-1}, \\ r_{k-2} &= q_k r_{k-1} + r_k, \\ r_{k-1} &= q_{k+1}r_k. \end{aligned}$$

By the division algorithm, the remainders satisfy the inequalities

$$n > r_1 > \dots > r_i > r_{i+1} > \dots > 0.$$

This guarantees that the algorithm comes to a halt after finitely many steps. We label the last nonzero remainder r_k and solve for r_k as follows:

$$\begin{aligned} r_k &= r_{k-2} - q_k r_{k-1} \\ &= r_{k-2} - q_k(r_{k-3} - q_{k-1}r_{k-2}) = -q_k r_{k-3} + (1 + q_k q_{k-1})r_{k-2} \\ &\dots \\ &= x_0 m + y_0 n. \end{aligned}$$

It can be shown (but we won't ask you to do it) that $r_k = \gcd(m, n)$.

We'll work out one example for you, so you can see how this is done. We will find the greatest common divisor of 8 and 27 and express it as a linear combination of the given integers. Now we need $m > n$, so $m = 27$ and $n = 8$. We now proceed with the algorithm. The remainders are underlined, and will be replaced with what we obtained in the column on the left.

$$\begin{array}{l|l}
 27 = 3 \cdot 8 + \underline{3} & \text{so } \underline{1} = 3 - 1 \cdot \underline{2} \\
 8 = 2 \cdot 3 + \underline{2} & = 3 - 1 \cdot (8 - 2 \cdot 3) = -8 + 3 \cdot \underline{3} \\
 3 = 1 \cdot 2 + \underline{1} & = -8 + 3(27 - 3 \cdot 8) = 3 \cdot 27 - 10 \cdot 8 \\
 2 = 2 \cdot 1 &
 \end{array}$$

So our algorithm tells us that $1 = 3 \cdot 27 - 10 \cdot 8$, and you can now check that this answer is correct.

You'll understand the algorithm better if you use it to calculate the gcd of two numbers. Do so for the following pairs of integers (m, n) and find the corresponding integers x_0 and y_0 :

- (a) (2745, 135);
- (b) (528, 627);
- (c) (4746, 894).

Problem 27.21. Use the Euclidean algorithm of Problem 27.20 to show that 2542 and 4095 are relatively prime.

Problem 27.22. On a calculator or a computer, program the Euclidean algorithm as outlined in Problem 27.20. Check your program by trying it out on parts (a) through (c) in that problem.

Problem 27.23. In the text we defined what it means for an integer p to be prime. We also defined what it means for two integers a and b to be relatively prime. Give an alternate definition for an integer p to be prime by requiring a and p to be relatively prime for certain integers a . Prove that the original and the alternate definition of prime are equivalent.

Problem 27.24. It is possible to define a function f that tells you the day of the week your birthday will fall on each year. To construct such a function, you need to find out what day of the week you were born. (Encode the weekdays as: 0—Sunday, 1—Monday, and so on.) Letting s denote the encoded week day of your birth, a the year you were born, and b the year in which you want to know the weekday of your birthday, you will need to define f in terms of s , a , and b . Thus, the required function f will be a map from $\mathbb{Z}_7 \times \mathbb{Z} \times \mathbb{Z}$ into \mathbb{Z}_7 . (The formula will depend on whether your birthday is before, after, or on February 29 of your birth year.)

Use modular arithmetic, but keep in mind that there are leap years. (The year 2000 was a leap year. The formula becomes considerably more complicated if you want to extend it past 2100, because that year will not be a leap year.)

To find out the day of your birth and to check your formula, access one of the perpetual calendars on the Web such as [38].

Chapter 28

Fermat's Little Theorem

We begin this chapter with a fundamental result of number theory, discovered by Pierre de Fermat. Fermat lived from 1601 to 1665. Many of his contemporaries were “number-lovers” rather than number theorists, [108, p. 51], and one thing that interested them was perfect numbers (a number is perfect if it is the sum of all its proper divisors). Bernard Frénicle de Bessy, who was also a mathematician and physicist, first raised the question of whether there was a perfect number of 20 digits and, if not, what the next largest perfect number was. (See [29] and [30].) The answer to the question required determining whether certain large numbers were prime. As a consequence, the men began corresponding. In a letter to Frénicle, dated October 18, 1640, Fermat stated what is now known as Fermat's theorem or Fermat's little theorem (to distinguish it from Fermat's last theorem), but he did not include a proof. In 1736, almost a century later, Leonhard Euler gave the first rigorous proof of the little theorem. Though this theorem is clearly theoretical in nature, it plays an important role in primality testing; that is, in deciding whether or not a certain number is prime. Fermat's little theorem (in the form due to Euler) is also the mathematical heart of the widely used RSA code that we will describe later in this chapter. In fact, Fermat's little theorem is not little at all.

Theorem 28.1 (Fermat's Little Theorem). *Let p be a prime and let a be an integer satisfying $\gcd(a, p) = 1$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Exercise 28.2. Verify Theorem 28.1 for a few values of p and a . ○

We will state and prove Euler's generalization of this theorem below. Fermat's little theorem will then follow as a special case.

In order to state the form of the theorem that we will prove, we will introduce a new function: **Euler's ϕ -function** is the function $\phi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ where $\phi(n)$ denotes the number of integers k , with $0 \leq k < n$, that are relatively prime to n .

Exercise 28.3. Calculate $\phi(1), \phi(12), \phi(7), \phi(13)$, and $\phi(7 \cdot 13)$. ○

Exercise 28.4. Show that if p is prime, then $\phi(p) = p - 1$. ○

The following lemmas will assist us in our proof of Theorem 28.7 below. The first lemma requires the multiplication in \mathbb{Z}_n that we defined in Chapter 27.

Lemma 28.5. *Let n and a be integers satisfying $n > 1$ and $\gcd(a, n) = 1$. If r and s are integers satisfying $ar \equiv as \pmod{n}$, then $r \equiv s \pmod{n}$.*

Proof. Since $\gcd(a, n) = 1$, we may apply Corollary 27.11 to obtain an integer b such that $ab \equiv 1 \pmod{n}$. We now multiply the equivalence $ar \equiv as \pmod{n}$ by b to get $arb \equiv asb \pmod{n}$. Using commutativity of the multiplication (see Problem 27.14) and simplifying, we obtain $r \equiv s \pmod{n}$, as desired. □

We summarize much of what we have learned below.

Lemma 28.6. *Let a and n be integers with $n > 1$ and $\gcd(a, n) = 1$. Then there exist exactly $\phi(n)$ distinct integers, $m_1, m_2, \dots, m_{\phi(n)}$ such that*

- (i) $0 \leq m_i < n$ and $\gcd(m_i, n) = 1$ for $i = 1, \dots, \phi(n)$,
- (ii) there exists $c \in \mathbb{Z}$ such that

$$\left(\prod_{i=1}^{\phi(n)} m_i \right) c \equiv 1 \pmod{n}, \text{ and}$$

- (iii) $am_i \not\equiv am_j \pmod{n}$ for $i \neq j$.

Proof. By the definition of Euler's ϕ -function, there exist exactly $\phi(n)$ distinct integers satisfying (i).

Using Problem 28.1, it follows from property (i) that $\gcd(\prod_{i=1}^{\phi(n)} m_i, n) = 1$. Thus we may apply Corollary 27.11 to obtain an integer c such that

$$\left(\prod_{i=1}^{\phi(n)} m_i \right) c \equiv 1 \pmod{n},$$

completing the proof of (ii).

For part (iii) recall that $\gcd(a, n) = 1$. Now $m_1, \dots, m_{\phi(n)}$ are distinct integers with $0 \leq m_k < n$ for each k . So, if $i \neq j$, then $m_i \not\equiv m_j \pmod{n}$. Thus (the contrapositive of) Lemma 28.5 implies that $am_i \not\equiv am_j \pmod{n}$ for $i \neq j$. □

Now we are ready for Euler's generalization of Fermat's little theorem.

Theorem 28.7 (Euler's Theorem). *Let $a, n \in \mathbb{Z}$ with $n > 1$. If $\gcd(a, n) = 1$, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $m_1, m_2, \dots, m_{\phi(n)}$ be as in Lemma 28.6. Then $am_1, am_2, \dots, am_{\phi(n)}$ are distinct integers $(\text{mod } n)$, and $\gcd(m_i, n) = 1$. Note that since there are $\phi(n)$ integers, we have

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i = \prod_{i=1}^{\phi(n)} (am_i). \quad (28.1)$$

Thus, if we can find $\prod_{i=1}^{\phi(n)} (am_i)$ as well as the reciprocal of $\prod_{i=1}^{\phi(n)} m_i \pmod{n}$, we can also compute $a^{\phi(n)} \pmod{n}$.

To compute the product in equation (28.1), use Exercise 27.7 to obtain $\phi(n)$ integers, $s_1, s_2, \dots, s_{\phi(n)}$ such that $s_i \equiv am_i \pmod{n}$ and $0 \leq s_i < n$. Now, $\gcd(a, n) = 1$ and $\gcd(m_i, n) = 1$, so by Problem 28.1, $\gcd(am_i, n) = 1$. Thus, Lemma 27.12 implies that $\gcd(s_i, n) = 1$. We have found $\phi(n)$ different integers, $s_1, s_2, \dots, s_{\phi(n)}$, all relatively prime to n . So $s_1, s_2, \dots, s_{\phi(n)}$ is simply a (possible) reordering of $m_1, m_2, \dots, m_{\phi(n)}$. Consequently

$$\prod_{i=1}^{\phi(n)} (am_i) \equiv \prod_{i=1}^{\phi(n)} s_i \equiv \prod_{i=1}^{\phi(n)} m_i \pmod{n}. \quad (28.2)$$

Combining (28.1) and (28.2) we get

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i \equiv \prod_{i=1}^{\phi(n)} m_i \pmod{n}. \quad (28.3)$$

By Lemma 28.6, there is an integer c such that $(\prod_{i=1}^{\phi(n)} m_i)c \equiv 1 \pmod{n}$. So, multiplying both sides of (28.3) by c , we obtain

$$\left(a^{\phi(n)} \prod_{i=1}^{\phi(n)} m_i \right) c \equiv \left(\prod_{i=1}^{\phi(n)} m_i \right) c \pmod{n}.$$

Using associativity and simplifying, we obtain $a^{\phi(n)} \equiv 1 \pmod{n}$, as desired. \square

Since Fermat's little theorem is a special case of Euler's theorem, with $n = p$ for a prime p and $\phi(p) = p - 1$, we now have a proof of Theorem 28.1 as well.

One interesting application of Euler's theorem is in an area of mathematics known as coding theory. Here's the idea: Suppose you want to transmit a message to a receiver, whom we shall refer to as Henry, in such a way that no one else can read it. This is done all the time. (Just think how often you have sent your credit card number over the Internet!) The idea is to use a code that is difficult to decode. But of course, if it's too difficult, Henry won't be able to decode it either. Applying the code to our secret message is like applying a function. Henry needs to undo the code, or mathematically speaking, apply the inverse function. So we need something like a function that has an inverse, but whose inverse is very difficult to find. Such functions are called trapdoor functions. (Anyone can get in, but only Henry can get out.) Since it is virtually impossible to find the inverse function, the original func-

tion used to hide the message can be made public. This is achieved using a method called a public key encryption, which includes a public key and a private key.

One particular trapdoor function leads to the following method. Henry, the receiver of the messages, decides on a function that is determined by the two integers, n and e , called the key of the code. Anybody who is interested can learn about these two numbers (this is why it is a *public key encryption*). If you want to send a message to Henry, then you first turn the English text into a positive integer m , called the plaintext. There are standard ways to do this, but the number produced does not yet hide the message. (If the translation leads to a number m that is greater than n , the message must be divided into several smaller messages.) The plaintext, m , must now be scrambled so that its meaning cannot be deciphered by anyone except Henry. Or, mathematically speaking, we have to apply the trapdoor function to it. A simple but very safe way to do this, is to change m to $m^e \pmod{n}$. It's interesting to note that though it appears that everyone has all the information Henry has, it turns out that Henry knows something no one else knows. We'll explain this once we tell you how Henry will unscramble the message. So the question is: How can Henry recover m from $m^e \pmod{n}$? It turns out that he will use Euler's theorem. Here's how:

Example 28.8. Let m, n , and e be positive integers satisfying $n > 1$, $\gcd(m, n) = 1$, and $\gcd(e, \phi(n)) = 1$. Find a positive integer d such that $(m^e)^d \equiv m \pmod{n}$.

Why is this example relevant? Well, once you have d , you have m^e, n, e , and d . You can then calculate $(m^e)^d$, which (as we learned in this example) is equivalent to m modulo n .

In order for the solution to this problem to be useful, we need a constructive way to find d . We claim that (i) we can find an integer d such that $e \cdot d \equiv 1 \pmod{\phi(n)}$ and that (ii) any such integer will fulfill the requirement $(m^e)^d \equiv m \pmod{n}$.

Now since e is a positive integer relatively prime to $\phi(n)$, Theorem 27.6 guarantees the existence of integers k and l such that $1 = ke + l\phi(n)$. Let d be the smallest positive integer such that $d \equiv k \pmod{\phi(n)}$. Then $1 \equiv de \pmod{\phi(n)}$, which is what we needed to show.

For part (ii), calculate $(m^e)^d = m^{ed}$, and recall that $m^{\phi(n)} \equiv 1 \pmod{n}$, by Euler's theorem. We just showed that $1 = ed + j\phi(n)$ for some $j \in \mathbb{Z}$, so

$$m^{ed} = m^{1-j\phi(n)} = m \cdot (m^{\phi(n)})^{-j} \equiv m \cdot 1 \equiv m \pmod{n}.$$

Note that in Problem 27.20 we gave a constructive method to find the integers k and l used above, and in Exercise 27.7, you showed how to get the integer d from k . ○

Now back to Henry. Remember that he has determined, rather carefully, his n and e and has given out these two integers. He also calculated the very important integer d from Example 28.8, but kept it a secret. Now you may well be asking the question, "Why can't everyone with access to n and e calculate d themselves, and then read the messages meant for Henry?" The reason is that in order to find d , a person needs to know the modulus that determines d , namely, $\phi(n)$. Henry knows (as you will

once you work Problem 28.12) that if he chooses n such that it is the product of two primes p_1 and p_2 , then $\phi(n) = (p_1 - 1)(p_2 - 1)$. So he lets p_1 and p_2 be two primes, each about 300 digits long, following current recommendations. (He must be a little careful choosing p_1 and p_2 , but we will not go into that here.) Now he and everyone else knows the product n , but not p_1 and p_2 . This is the trapdoor. Henry knows n , p_1 , and p_2 . So he can find $\phi(n)$. But everyone else only knows n , so they would have to find p_1 and p_2 . It takes no time at all to multiply two 300-digit numbers, but you cannot factor the product in a million years, not even with supercomputers! There is a second reason that Henry had to know $\phi(n)$: he needed e to be relatively prime to $\phi(n)$.

There is one more thing that we should mention. In Example 28.8 we have the additional condition $\gcd(m, n) = 1$ (see also Problem 28.19). Thus, it appears from our solution above that we also need $\gcd(m, n) = 1$. Fortunately our decoding method still works if we have $n = p_1 p_2$ for two different primes p_1 and p_2 and $\gcd(m, n) = p_1$. If you work Project 29.13, you will prove this in Lemma 29.16.

Henry's method to get secure messages is called the RSA public key encryption, and Example 28.8 is the mathematical content of it. To learn more about this ingenious and widely used method, work Project 29.13 on the RSA Code.

Definition

Definition 28.1. Euler's ϕ -function is the function $\phi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ where $\phi(n)$ denotes the number of integers k , with $0 \leq k < n$, that are relatively prime to n .

Solutions to Exercises

Solution (28.2). We calculate two examples.

1. Let $p = 5$ and $a = 7$. Then $7^4 = 2401 \equiv 1 \pmod{5}$.
2. Let $p = 13$ and $a = 8$. Then $8^{12} = 68719476736$. Now $8^{12} - 1 = 68719476735 = 13 \cdot 5286113595$. Hence $8^{12} \equiv 1 \pmod{13}$.

Solution (28.3). $\phi(1) = 1$.

The nonnegative integers smaller than 12 are all listed. We cross out the ones that are not relatively prime to 12: $\emptyset, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, 10, 11$. Hence $\phi(12) = 4$.

Similarly, $\phi(7) = 6$, $\phi(13) = 12$, and $\phi(7 \cdot 13) = \phi(91) = 72$.

Notice that, in these examples, for p and q different primes $\phi(p) = p - 1$ and $\phi(p \cdot q) = \phi(p) \cdot \phi(q)$. Are these coincidences?

Solution (28.4). Note that for p prime and a an integer with $0 \leq a < p$, we have $\gcd(a, p) = 1$ if and only if $a \neq 0$. Thus $\phi(p) = p - 1$ for every prime p .

Spotlight: Public and Secret Research

Research in mathematics today is often done by professors who work at universities or colleges. People frequently work collaboratively, though they also sometimes work alone. They might communicate via e-mail, get together when they can, work together at institutes, or they may never even meet each other. Once their work is done, they write it up and send it to a journal. The editor of the journal sends it to carefully selected referees who read the paper. The author is responsible for the correctness of the mathematics in the paper, but the referee (whose identity is generally hidden from the author) determines the value of the work, the appropriateness of its placement in the journal, the originality of the mathematics, and often the correctness of the results. Once the paper appears, everyone has access to the results and proofs in the paper.

There are also other places where mathematical research is done. In the United States, the *National Security Agency* (NSA) refers to itself as the “leading employer” of nonacademic mathematicians. In Great Britain, there is the *Government Communications Headquarters* (GCHQ), the successor to the famous Bletchley Park where British code breakers were so successful in intercepting and reading Nazi attack plans. The mathematics done in a place like this might become the government's secret, and therefore may never be published. Public key encryption is an example of how such secrecy may hamper mathematical progress.

In 1976, Whitfield Diffie, Martin Hellman, and Ralph Merkle developed the idea of the public key. In 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman gave us the RSA code. A couple of decades later, it became known that British mathematicians at GCHQ had worked out the encryption idea a few years earlier. James Ellis, Clifford Cocks, and Malcolm Williamson, all employed at GCHQ, had discovered public key encryption, but neither they nor their supervisors realized the power and widespread applicability of the method. Their results were considered top secret and were only circulated within the agency. A few years later, the world admired the “new” cryptosystem and celebrated the “originators” in the United States, [99, Chapter 6].

Some private companies also restrict their employees' publications. There are instances of researchers circumventing this restriction by publishing under a pen-name. In 1908, William S. Gosset, who worked for the Guinness Brewing Company in Dublin, published a paper under the name “Student” to avoid repercussions. The distribution Gosset introduced is now known as *Student's t-distribution* (or the Student *t*-distribution) and it has had a profound impact on statistical theory and practice.

To learn more about the interesting history of public key encryption we recommend [99, Chapter 6] or [61].

An in-depth treatment of Fermat's little theorem, Euler's theorem, and Euler's ϕ -function, as well as historical notes can be found in the text [15, pp. 91–96 and 123–150]. In [57, pp. 418–420 and 556–558] Fermat's theorem and Euler's theorem are put in context. For short biographies of Pierre de Fermat and Leonhard Euler, see the Web at [79]. For a biographical sketch of Euler and a delightful description

of Euler's mathematics in the various fields, see [22]. A good source to learn more about Fermat's life and his mathematics is [66].

Problems

Problem# 28.1. (a) Let $a, b, s \in \mathbb{Z}$ such that $\gcd(a, s) = 1$ and $\gcd(b, s) = 1$. Show that $\gcd(ab, s) = 1$.

(b) Let $n \in \mathbb{Z}^+$ and a_1, \dots, a_n , and s be integers such that $\gcd(a_k, s) = 1$ for all integers k with $1 \leq k \leq n$. Show that $\gcd(\prod_{k=1}^n a_k, s) = 1$.

Problem 28.2. Show that the conclusion of Fermat's little theorem (Theorem 28.1) may not hold if p is not prime.

Problem 28.3. Use Fermat's little theorem to show that for p a prime, every integer a with $a \not\equiv 0 \pmod{p}$ has a reciprocal modulo p .

Problem 28.4. In Problem 28.3 above you proved that if p is a prime, then every integer that is not equivalent to zero modulo p has a reciprocal modulo p .

- Find the reciprocals of $1, 2, \dots, 6$ modulo 7 .
- Given a prime p , find all integers x with $1 \leq x < p$ that are the reciprocals of themselves.
- Prove the following theorem:

Theorem 28.9 (Wilson's theorem). *If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.*

Problem 28.5. Prove the converse of Wilson's theorem, namely: For an integer $n > 1$, if $(n-1)! \equiv -1 \pmod{n}$, then n is prime. (Hint: The case $n = 2^2$ needs to be considered separately.)

Problem 28.6. (a) Let p and q be primes with $p \neq q$, and let a and b be two integers. Prove that if $a \equiv b \pmod{p}$ and $a \equiv b \pmod{q}$, then $a \equiv b \pmod{pq}$.

(b) Use part (a) to show that if p and q are prime numbers with $p \neq q$, and a is an integer satisfying $\gcd(a, pq) = 1$, $a^p \equiv a \pmod{q}$, and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

Problem 28.7. In this problem, we show that the following converse of Fermat's little theorem is false: If a is a prime and $a^{m-1} \equiv 1 \pmod{m}$, then m is necessarily a prime.

Let $a = 2, p = 11, q = 31$, and $m = pq$. Use Problem 28.6 part (b) to show that the statement above is false. (Note: You can verify this counterexample directly with a calculator or computer. If you use Problem 28.6 part (b) and do the modular exponentiation efficiently, the verification can be done easily by hand. The example is from [46].)

Problem 28.8. Let a and n be integers with $n > 1$ and $\gcd(a, n) = 1$. Prove that there exists a smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ and $m \mid \phi(n)$.

Problem 28.9. (a) Calculate $\phi(5^2)$, $\phi(5^3)$, and $\phi(5^4)$.

(b) For p a prime and n a positive integer, show that $\phi(p^n) = p^n(1 - 1/p)$.

(c) Calculate $\phi(128)$.

Problem 28.10. Is Euler's ϕ -function additive; that is, for all $m, n \in \mathbb{Z}^+$ is it the case that $\phi(m+n) = \phi(m) + \phi(n)$? Prove it or give a counterexample.

Problem 28.11. This problem guides you through the proof of the fact that Euler's ϕ -function is in some sense multiplicative. More precisely, you will prove

Theorem 28.10. *Let m and n be integers such that $m > 1$ and $n > 1$. If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

(a) Let k_1, k_2, l_1 , and l_2 be integers satisfying $0 \leq k_1, k_2 < n$ and $0 \leq l_1, l_2 < m$.

Show that if $k_1m + l_1n \equiv k_2m + l_2n \pmod{mn}$, then $k_1 = k_2$ and $l_1 = l_2$.

(b) Use the result of (a) to show that for each $a \in \mathbb{Z}$ there is exactly one element $(k, l) \in \mathbb{Z} \times \mathbb{Z}$ such that $0 \leq k < n$, $0 \leq l < m$, and $a \equiv km + ln \pmod{mn}$.

(c) For positive integers m and n , use (b) to conclude that

$$|\{(k, l) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq k < n, 0 \leq l < m, \text{ and } \gcd(km + ln, mn) = 1\}| = \phi(mn).$$

(d) For $k, l \in \mathbb{Z}$ with $0 \leq k < n$ and $0 \leq l < m$, show that $\gcd(km + ln, mn) = 1$ if and only if $\gcd(k, n) = 1$ and $\gcd(l, m) = 1$.

(e) Use (c) and (d) to obtain the conclusion of Theorem 28.10.

Problem 28.12. Use the results of Problems 28.9 and 28.11 to answer the following.

(a) Let $m \in \mathbb{Z}$ and suppose $m = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$, where p_1, p_2, \dots, p_k are distinct primes and a_1, a_2, \dots, a_k are positive integers. Prove that

$$\phi(m) = m \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

(b) Calculate $\phi(5712200)$.

Problem 28.13. Prove that for $n \in \mathbb{Z}^+$, the Euler ϕ -function satisfies

$$\phi(2n) = \begin{cases} \phi(n) & \text{if } n \text{ is odd} \\ 2\phi(n) & \text{if } n \text{ is even} \end{cases}.$$

Problem 28.14. Use the formula from Problem 28.12 to show that for p prime and r a positive integer, $\sum_{d|p^r} \phi(d) = p^r$.

Problem 28.15. Let a, b , and c be integers such that $\gcd(a, b) = 1$ and $a|bc$. Prove that this implies that $a|c$.

Problem 28.16. Prove Theorem 28.1 directly by adapting the proof of Theorem 28.7 to this simpler situation.

Problem 28.17. In each of the two cases below, use the method of Example 28.8 to find an integer m with $0 \leq m < 33$ satisfying

- (a) $m^3 \equiv 8 \pmod{33}$ and $\gcd(m, 33) = 1$;
- (b) $m^{77} \equiv 15 \pmod{143}$ and $\gcd(m, 143) = 1$.

Problem 28.18. Show that the conclusion of Euler's theorem may not hold if $\gcd(a, n) > 1$.

Problem 28.19. Show that if x and y are integers and p is a prime, then

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

(You may find the binomial theorem useful here. If so, you may use, without proof, the fact that the binomial coefficient $\binom{n}{k}$ is an integer for $k, n \in \mathbb{N}$ with $k \leq n$.)

Problem 28.20. The RSA code relies on being able to calculate $m^e \pmod{n}$ quickly. Fortunately, this is possible with an intelligent plan and with the help of a computer.

- (a) Devise a plan to calculate m^{100} with the smallest number of multiplications by multiplying two (and only two) integers at a time. How many multiplications and divisions did you need? (You don't need to prove that the number of multiplications you require is the smallest.)
- (b) To multiply or divide two integers of n digits each we need to do roughly n^2 operations. If m and n have 600 digits, how many operations are needed to calculate $m^{100} \pmod{n}$?
- (c) Your computer is, most likely, capable of performing $2 \cdot 10^{10}$ operations per second. How long will it take to calculate your $m^{100} \pmod{n}$?

Problem 28.21. The RSA code can also be used as a signature. In doing so, the sender sends out n and d and keeps e for himself. You receive two messages, one is a plain message and the other is an encrypted message. You can check whether the two messages are the same, because you have n and d . So, if the encrypted message unscrambles to the plain one, then it must come from the sender—the only person who knows e .

In this problem, we'll look at a specific example: The public signature key is $n = 77$ and $d = 13$. The message you get is 8 with the encrypted form 50. Decide whether the message came from the sender. If it didn't, calculate the true pair of messages.

Of course the numbers here are much too small, and you would be able to calculate e easily. If n were a 600-digit number, then you would no longer be able to do so, but you could still decode the encrypted message with the given information in a reasonable amount of time. In fact, you can decode the message very quickly if you have a computer—basically instantaneously, if your computer is programmed to do so. Sending the plain text can usually be omitted, because the probability that a randomly generated text makes sense is zero. Thus, if the decoded text makes sense, the signature is (for all practical purposes) correct.

Chapter 29

Projects

Tips on Talking about Mathematics

It's not easy to talk about mathematics to other people. In this section, we present some tips that we find helpful when we present a talk to undergraduates.

Let's say someone has just asked you to give a talk about mathematics to undergraduates. Here's what you need to do:

- Thank them, and say you'd love to. Then do the rest of the things below.
- Find out who the audience is and what they know.
- Pick an interesting topic. Find out about the history of the topic, the main players in the field, and the main results.
- Now that you have your topic, you need to write the talk. Start with something everyone is interested in. This could be the history of what you plan to talk about, or it could be an interesting related result. Then motivate the question you are interested in looking at, build up the talk, and remember to find a good conclusion for it.
- As you write your talk, keep the level of the audience in mind. Do not use terms that your audience will not understand. If they haven't heard certain words you will have to define them, which brings us to our next point: the more terms you have to define, the more people you will lose. Pick a topic that doesn't require a lot of introduction.
- You need to decide whether you will use transparencies, the computer, or the blackboard. Each has its advantages and disadvantages. We'll run through each below.

1. *Blackboard.* If you use the blackboard, you'll most likely move at the right speed for the audience. It's also livelier than the other methods. On the other hand, you should absolutely not rely on your notes. Therefore, if you give a talk using the blackboard, you'll need to know what you are going to say and when you are going to say it. You'll need to watch where you write things, and you shouldn't erase something you want the audience to look at. Make

sure that you move away from the board so that everyone can see what you wrote. If your handwriting is illegible, think about using transparencies or the computer.

2. *Transparencies.* Unless you are very careful, you will probably move too quickly for the audience. You'll probably also stand in front of the transparency from time to time, blocking the audience's view. If you are aware of these potential problems, you can correct them. For example, you can use two overheads. You should not write too much on one transparency, and you should always be aware of where you are standing. Find out how big the room is, and make sure that someone in the back of the room will be able to see what you have written. The advantage of transparencies or the computer is that you'll have all your diagrams and pictures in place, and you'll have an outline of your talk with you. So the main disadvantages are that your talk may become monotonous and that it's possible to move so quickly that your audience won't be listening. These are pretty big disadvantages.
3. *Computer.* In many ways, using the computer to give your talk is similar to using transparencies. Many of the advantages and disadvantages are the same. Still, there are a few things that we should mention. For mathematics, many people use Beamer from LaTeX. (A tutorial can be found at [9].) As we mentioned, some things are the same as for transparencies. The basic rule is: Don't overdo it. Don't use too many fonts, too many pictures, too many colors, and don't put too much on one screen. However, the computer presents new challenges: If you use a computer, you cannot correct things in front of an audience. You'll need to proofread your slides very very carefully. It's also possible to use a tool that allows you to stand in exactly one position, moving only your thumb. If you do this for your entire talk, it's fairly likely that your talk—no matter how well you prepare it—will be dull. Move! Even if you don't have to, it's important to move around. If you must use a laser pointer, use it sparingly. It's distracting to see a red beam moving rapidly around as you try to read a slide. You can liven up the talk by adding relevant photographs of places, manuscripts, or people. You might even add a video clip. Just make sure that these "attention getters" are relevant and well incorporated.
4. *Blackboard, Transparencies, and Computer.* One thing you can do is combine two or three of these methods of presentation. In a talk for undergraduates, it's nice for them to have something to look at from time to time, other than the speaker.

Pick the method you are most comfortable with and that you like the best. Then work around the disadvantages.

- So now you have your topic, your talk, and a method of presentation. You're done, right? Um . . . no. You still have to present the talk. Surprisingly, the hardest part of the talk is timing. We've alluded to this already in our discussion on transparencies, but there's more to be said.

- Find out how long the talk is. If it's twenty minutes, talk for twenty minutes. (No one will complain if it's eighteen minutes, and everyone will complain if it's thirty.) There is only one way to know how long your talk is: practice it.
- The best way to practice a talk is to give it to yourself once. Fix the things you realize need fixing. Then try to find an audience of two people, one who knows what you are talking about and one who does not. Ask them if you can present the talk to them. Listen to their comments and use them to improve your talk.
- Write an interesting, but truthful abstract. The abstract should indicate the level of the talk.
- Before you give your talk, ask if you can see the room that you will speak in. Check that everything you need is there.
- Make sure that everyone in the room can hear you when you speak. When you give the talk, look at the audience. They'll let you know how you are doing.

There are other articles on how to talk about mathematics ([68], [43]), but these are primarily aimed at graduate students or professional mathematicians. Of course, many of the tips are the same, because many of the mistakes people make—whether talking to undergraduates, graduate students, or professors—are the same.

29.1 Picture Proofs

Introduction

You have probably heard the saying “a picture is worth a thousand words.” The same is true in mathematics: a good picture can help a reader visualize what is happening, it can aid a mathematician in finding a solution, and it can shed light on other potential results. A bad picture, on the other hand, can be deceiving. Relying too much on what we see might lead us to incorrect proofs, which in turn can lead to false results. This project should help convince you of that.

One of the most influential theorems in mathematics is Pythagoras' theorem. It states that in a right triangle the lengths of the sides of the triangle satisfy $a^2 + b^2 = c^2$, where c denotes the length of the hypotenuse, and a and b denote the lengths of the other two sides of the triangle. There are many known proofs of this theorem, some of them based on clever figures. You will see two such proofs below.

Prerequisites

Basic geometry skills plus an understanding of what constitutes a rigorous argument are the necessary prerequisites for this project. We suggest that you read through Chapter 5 before attempting this project.

Guided Project

1. The diagram in [Figure 29.1](#) suggests a proof of Pythagoras' theorem. To make this proof rigorous, however, you will need to do two things; you need to prove something about the diagram and you need to do an algebraic calculation. Do both.
2. Give a second proof of Pythagoras' theorem based on [Figure 29.2](#). This one does not need algebraic calculations. It is all in the picture—or is it?
3. If you accepted the picture of [Figure 29.2](#) as a complete proof of Pythagoras' theorem, then you are probably willing to believe that [Figure 29.3](#) provides a proof that $168 = 169$. After all, both proofs require that we shift the pieces around to form another familiar object. What is wrong with this proof?
4. Find a picture to illustrate the statement

$$\sum_{k=1}^{\infty} \frac{1}{2^k} = 1.$$

Does your picture amount to a rigorous proof? What are its strengths and what are its weaknesses?

5. Use the picture of [Figure 29.4](#) to prove that

$$\int_0^1 \frac{dx}{1+x^2} = \frac{\pi}{4}.$$

(This problem was proposed by Michael Vowe in [105]. [Figure 29.4](#) is part of the solution given by Gerhard Wanner in [106].)

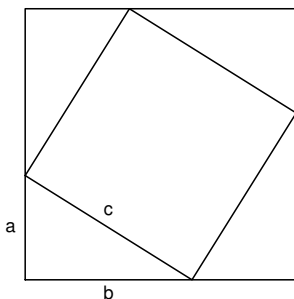


Fig. 29.1 $a^2 + b^2 = c^2$

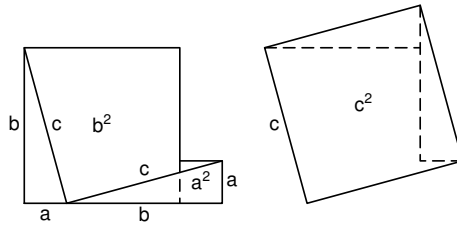


Fig. 29.2 $a^2 + b^2 = c^2$

Open-Ended Project

Try to find some other picture proofs. (We suggest you think back to your geometry course.) Can you also come up with a (somewhat) convincing picture proof of a false statement?

Notes and Sources

We first learned of the false proof presented in part 3 from our colleague, G. Adams. For a connection between this problem and Fibonacci sequences see the article [54], where the author indicates that this “not a picture proof” can be traced back to the year 1868. There are two excellent books on picture proofs by R. B. Nelsen, [75] and [76]. The website by A. Bogomolny [13] contains 84 proofs of Pythagoras’ theorem, many of them with pictures, and some of them with applets.

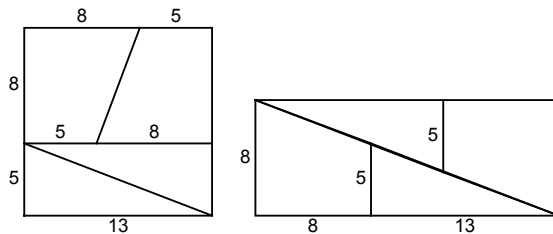


Fig. 29.3 $169 = 13^2 = (8 + 13) \cdot 8 = 168$

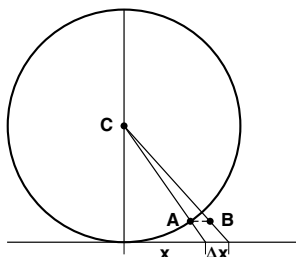


Fig. 29.4 $\int_0^1 \frac{dx}{1+x^2} = \frac{\pi}{4}$

29.2 The Best Number of All (and Some Other Pretty Good Ones)

Introduction

We know that positive integers can be even or odd, they can be prime or composite, and they can be triangular or square. (Each of these terms, with the exception of “square,” appears either below or in the index of this book, if you have forgotten the definition.) In this project we’ll look at some more things that they may be: the sum of their proper divisors, the product of their proper divisors, or both.

Prerequisites

This exercise requires an understanding of proof techniques (Chapter 5).

Guided Project

Recall that an integer greater than 1 is prime if its only positive divisors are 1 and itself. A positive integer greater than 1 that is not prime is called composite. By a proper divisor, we mean a positive divisor that is not equal to the integer itself. A positive integer is said to be **perfect** if it is the sum of its proper divisors.

1. Show that 6 is a perfect number.
2. Show that 6 is the only perfect number less than 10.
3. Find another perfect number that is less than 30.

By now you should have found the first two perfect numbers. The next is 496.

4. Check that 496 is a perfect number.

5. Find five positive integers, each one being the product of all of its proper divisors.
6. Characterize all positive integers that are the product of their proper divisors.

Now you are almost ready to prove the main theorem in this project. Steps 7–9 below will lead you through the proof.

Theorem 29.1. *There is only one positive integer that is both the product and sum of all its proper positive divisors, and that number is 6.*

7. Let p be a prime. Prove that p^3 is not perfect.
8. Prove as many of the following as you need to, until you see the proof of the theorem.
 - (a) Prove that the only even number that is both the product and sum of all its proper positive divisors is 6.
 - (b) Prove that the only multiple of 3 that is both the product and sum of all its proper positive divisors is 6.
 - (c) Prove that there is no multiple of 5 with this property.
 - (d) Prove that there is no multiple of 7 with this property.
9. Prove the theorem.

The goal of the next part of this project is to solve the following:

Problem. Let n be an odd positive integer. Find all perfect numbers of the form $n^n + 1$.

It is also possible to find all perfect numbers of the form $n^n + 1$ when n is an even integer—but this is more difficult. The case n odd is already quite difficult, so we will help you by outlining steps you may follow to solve the problem. We also suggest that you use the following theorem, which is due to Euler. (See, for example, [22, pp. 10–11] for a proof of this theorem.)

Theorem 29.2 (Euler). *If N is an even perfect number, then $N = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime.*

10. Find an integer a such that $n^n + 1 = (n + 1)a$. (The integer a will be a sum and an expression that involves n .)
11. Prove that $n + 1$ and a have no positive common divisor other than 1. (We say that $n + 1$ and a are relatively prime.)
12. Assuming that n is odd and $n^n + 1$ is perfect, use Euler's theorem to show that $n + 1 = 2^{k-1}$ for some integer k .
13. Solve the problem.

This was posed as a problem in the *American Mathematical Monthly* [72].

Open-Ended Project

Let p be a polynomial over \mathbb{Z} or \mathbb{R} (see Problem 10.13). What might it mean to say that a polynomial is prime? composite? perfect? square? triangular? While some of these might make sense, others may not. Once you have defined the terms that make sense, are there some interesting theorems you can prove about them?

Notes and Sources

Euclid, in his *Elements*, IX.36, gave the result that if $p = 2^k - 1$ is a prime, then $2^{k-1}p$ is perfect. For $k = 2, 3, 5,$ and 7 we note that $2^k - 1$ is prime. Thus we get four perfect numbers, 6, 28, 496, and 8128. The eighth perfect number is already quite large: 2,305,843,008,139,952,128. A good source to begin learning more about numbers is the book [20]. The problem we discussed in the guided portion of this project appears in [15], which we recommend to those wanting to know more about number theory.

29.3 Set Constructions

Introduction

It is amazing how much one is able to build out of almost nothing—and by almost nothing here we mean the empty set. The guided project will lead you through a construction of the natural numbers.

Prerequisites

While the set theory introduced in Chapters 6–9 is sufficient, you may find it helpful to have an understanding of mathematical induction (Chapter 18), which is also introduced in this project.

Guided Project

Let x be a set. Define the successor of x to be the set $x^+ = x \cup \{x\}$.

1. Determine the successors and the successors of the successors of the sets \emptyset , $\{\emptyset\}$, and $\{a, b, c\}$.

We now introduce the following notation. Let $0 = \emptyset$, $1 = 0^+$, $2 = 1^+$, and so on.

2. Write down 0, 1, 2, 3, and 4 as sets in two different ways; first using the definitions made above, and then using only the symbol \emptyset , set brackets, and appropriate set notation.

It may seem intuitively obvious that if we “do this forever,” then we will have defined the natural numbers. However, as simple and as attractive as this approach may be, it is not what we call mathematically rigorous. What we need is a statement that explains that we can do this forever. We will take this statement as an axiom, and thus it will not be proved.

Axiom 29.3 (Axiom of infinity). There exists a set containing 0 and containing the successor of each of its elements.

3. Let I be a nonempty set and $\{A_k : k \in I\}$ be an indexed collection of sets. Suppose that for each $k \in I$, the set A_k has the two properties (i) $0 \in A_k$ and (ii) if $x \in A_k$, then $x^+ \in A_k$. Show that the set $\bigcap_{k \in I} A_k$ also has these two properties. We will call a set with these two properties a successor set.
4. The axiom of infinity guarantees the existence of a successor set. So, let A be an arbitrary successor set. Define the set ω_A to be the intersection of all subsets of A that are also successor sets. In symbols we might write

$$\omega_A = \bigcap_{B \in I} B,$$

where $I = \{B : B \subseteq A, \text{ and } B \text{ is a successor set}\}$.

By part 3, ω_A is a successor set. Show that $\omega_A = \omega_B$ for all successor sets A and B . Perhaps surprisingly, our definition does not depend on our initial choice of successor set, and therefore we will write ω rather than ω_A .

We call ω the set of natural numbers. Thus far we know that ω is a successor set, and it is the only successor set that is contained in every other successor set.

5. Prove the following statement. Suppose $S \subseteq \omega$ satisfies the two properties
 - (i) $0 \in S$, and
 - (ii) if $x \in S$, then $x^+ \in S$.

Show that $S = \omega$. (This is called the principle of mathematical induction and is discussed in Chapter 18.)

6. Prove that $x^+ \neq 0$ for all $x \in \omega$.
7. Consider the set $S = \{x \in \omega : \forall y \in \omega, \text{ if } y \in x, \text{ then } y \subseteq x\}$. Use part 5 to show that $S = \omega$. Conclude that for all u and v in ω , if $u \in v$, then $u \subseteq v$.
8. Use part 7 to prove that if x and y are in ω and $x^+ = y^+$, then $x = y$.

The two defining properties ((i) and (ii)) of a successor set, the principle of mathematical induction, and parts 6 and 8 of this project are known as the five Peano axioms. They are the pillars of the construction of the natural numbers.

Open-Ended Project

We have created new sets from old ones using element relations, union, intersection, power sets, and Cartesian products. Use some (or all) of these to create new sets from the empty set. Do your new sets have some interesting properties?

Notes and Sources

This project is guided by Chapters 11 and 12 of P. Halmos' *Naive Set Theory* [41]. For a brief presentation of the Peano axioms and some other attempts to give the natural numbers a solid foundation see [59, pp. 987–989].

29.4 Rational and Irrational Numbers

Introduction

We know that when we add two rational numbers, the result is a rational number. For this reason, we say that the rationals are *closed under addition*. Similarly, when we multiply two rational numbers, the result is rational. Thus, the rationals are also *closed under multiplication*. In this project, you will investigate the behavior of the rationals and irrationals under other operations.

Prerequisites

This project relies on proofs in cases (Chapter 5), as well as familiarity with rational and irrational numbers. In particular, you will need to use the fact that $\sqrt{2}$ is irrational.

Guided Project

Let a and b be two irrational numbers.

1. Give an example of two irrational numbers a and b such that $a + b$ is irrational.
2. Give an example of two irrational numbers a and b such that $a + b$ is rational.

So the irrational numbers are not closed under addition and certainly are less well behaved than the rational numbers. Now consider two real numbers, a and b .

3. Give an example of two rational numbers a and b such that a^b is rational.
4. Give an example of two rational numbers a and b such that a^b is irrational.

Here's a charming little proof, based entirely upon things that you have proved in this course, that an irrational number raised to an irrational power can be rational.

5. Consider the following.

Theorem 29.4. *There exist irrational numbers a and b such that a^b is rational.*

Complete the proof of this theorem, using appropriate choices for a and b and the two cases below:

Case 1. $\sqrt{2}^{\sqrt{2}}$ is a rational number;

Case 2. $\sqrt{2}^{\sqrt{2}}$ is an irrational number.

The interesting thing about your proof of Theorem 29.4 is that you don't need to know whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational!

6. There are many other examples of irrational powers of irrational numbers that are rationals, assuming you know lots of different ways to express irrational numbers. See if you can come up with another example based on the fact that the natural logarithm of 2, denoted $\ln 2$, is irrational. Can you find other examples?

Knowing that an irrational number to an irrational power may be rational raises the question of whether an irrational to an irrational can be irrational. Again, we are looking for a proof that does not use anything more than what we stated in the prerequisites. There are some nonelementary proofs of this, but an elementary proof exists as well [56].

7. Prove the following theorem.

Theorem 29.5. *There exist irrational numbers a and b such that a^b is irrational.*

We suggest that you consider using a proof in cases, with $\sqrt{2}^{\sqrt{2}}$ for one of your cases.

Open-Ended Project

Study the behavior of the rationals and irrationals under different operations. Your investigations might deal with specific numbers, or with the rationals and irrationals in general. For example, is $\sqrt{2} + \sqrt{3}$ irrational? In another direction, can you define an operation, \odot , such that $a \odot b$ is irrational for all irrational a and b ? Think of other questions along these lines and try to answer them.

Notes and Sources

The connection of this problem to Hilbert's seventh problem is discussed in the Spotlight: Hilbert's Seventh Problem at the end of this chapter. The proof that an irrational number to an irrational power can be irrational appears in [56]. These authors attribute the proof of Theorem 29.4 to D. Jarden, [55]. This problem appears as a "fun fact" on the Web at [104].

29.5 Irrationality of e and π

Introduction

The problems in this project require knowledge of calculus. More specifically, you need to know what the number e is, what a geometric series is, and what the series expansion for e is. If you have seen all this, then you probably have also been told that e is an irrational number. The first task of this project is to work through Ivan Niven's proof of this fact. If you have never seen the proof, it's a nice application of series. Everything you need to prove that e is irrational is provided in this project.

The proof that π is irrational, outlined in this project, is also due to I. Niven. In his words, "In the June 1947 issue of the *Bulletin of the A. M. S.*, I gave a one page proof that π is irrational. I had worked on this problem for a specific reason: in the first edition (1938) of what is now a great classic, *Introduction to the Theory of Numbers*, by G. H. Hardy and E. M. Wright, the authors made the observation that 'There is no simple proof of the irrationality of π .' I wondered why this should be so." (See [3] for the full text of Niven's conversation.)

We have provided you with all the steps you need to re-create Niven's one-page proof.

Prerequisites

Since the proofs are by contradiction, you will need to have covered Chapter 5. This project also assumes that you have a basic understanding of infinite series.

For the proof that these numbers are irrational, you will need to recall three results from your calculus course. The first is that, for $-1 < r < 1$, the geometric series satisfies

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}.$$

The second fact is that the series expansion for e^x is

$$e^x = 1 + x/1! + x^2/2! + x^3/3! + \cdots + x^k/k! + \cdots.$$

The last result that you will need is the product rule for differentiation.

Guided Project

1. Prove the following theorem, using the steps outlined below.

Theorem 29.6. *The number e is irrational.*

Step 1. Let $k \in \mathbb{Z}^+$. Show that

$$\begin{aligned} \frac{1}{(k+1)} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + \cdots \\ \leq \frac{1}{(k+1)} + \frac{1}{(k+1)^2} + \frac{1}{(k+1)^3} + \cdots. \end{aligned}$$

Step 2. Prove that if k is an integer with $k \geq 2$, then

$$\frac{1}{(k+1)} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + \cdots < 1.$$

Step 3. Suppose to the contrary that e is rational. Prove that this implies there exists an integer k such that $k!e$ is an integer.

Step 4. Using the series expansion for e , show that $k!e$ is never an integer. This step should complete the contradiction.

2. Prove the following theorem by contradiction, using the steps below.

Theorem 29.7. *The number π is irrational.*

Suppose to the contrary that there are positive integers a and b such that $\pi = a/b$. We will write $f^{(m)}$ for the m th derivative of f .

For $n \in \mathbb{Z}^+$, define the two polynomials f_n and F_n by

$$f_n(x) = \frac{x^n(a - bx)^n}{n!} \quad \text{and}$$

$$F_n(x) = f_n(x) - f_n^{(2)}(x) + f_n^{(4)}(x) - \cdots + (-1)^n f_n^{(2n)}(x).$$

We will determine a value for n in the fifth step below. Until then, assume that n is a positive integer.

Step 1. Show that for every positive integer j , all of the following are integers:

$$f_n(0), f_n(\pi) = f_n(a/b), f_n^{(j)}(0), \text{ and } f_n^{(j)}(\pi) = f_n^{(j)}(a/b).$$

Step 2. Prove that $f_n(x) \sin x = \frac{d}{dx}(F_n'(x) \sin x - F_n(x) \cos x)$.

Step 3. Prove that $\int_0^\pi f_n(x) \sin x dx = F_n(\pi) + F_n(0)$.

Step 4. Find the maximum of the function f_n on the interval $[0, \pi]$. (Note that the maximum depends on n .)

Step 5. Prove that for n sufficiently large, $\int_0^\pi f_n(x) \sin x dx$ is not an integer. This step should complete the contradiction.

Open-Ended Project

Can you prove that e^2 is irrational? What else can you prove is irrational?

Notes and Sources

In 1737, Euler showed that e is irrational. Johann Heinrich Lambert showed, in 1761, that π is irrational. The number π has a very interesting history. For a brief history of π , see [26, p. 100]. For a fuller account, up to about 1971, see [11]. For more recent developments, see [7].

The one-page proof in the *Bulletin of the A.M.S.* that Niven refers to in the quote above can be found in [77]. The reference for Hardy and Wright's text is given in [46]. The conversation with Niven appears in [3].

29.6 A Complex Project

Introduction

In this project, we investigate the complex numbers. In order to say something interesting, we will need to assume several facts—some elementary and some not.

Prerequisites

You will need to use the material on relations in Chapter 10 and order in Chapters 12 and 13. In particular, you must be familiar with the order definitions: Definitions 13.1 and 13.2. We will introduce complex numbers here, and we will not assume that you have already seen them. This project also assumes a basic familiarity with series. If you have taken a calculus course that covered infinite series of functions including e^x , $\sin x$, and $\cos x$, you will have the necessary background in series.

Guided Project

Let's begin by recalling the complex numbers,

$$\mathbb{C} = \{z : z = a + bi, \text{ where } a, b \in \mathbb{R} \text{ and } i^2 = -1\}.$$

Complex numbers can be thought of in several ways. When considered as above, it's easy to see how to multiply and add them: For $z, w \in \mathbb{C}$ write $z = a + bi$ and $w = c + di$, where $a, b, c, d \in \mathbb{R}$. Then

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i$$

and

$$z \cdot w = (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Using these definitions and the properties stated in the Appendix on page 363 (Algebraic Properties of \mathbb{R}), answer the following questions:

1. Which of the properties A1–A4, M1–M4, and D1 in the Appendix on page 363 apply to the complex numbers with multiplication and division defined as above?

There is another way to think about complex numbers that is quite helpful for computations. For this notation, you should think in polar coordinates. For $z = 0$, for example, we can write

$$0 = 0 + 0i = 0(\cos \theta + i \sin \theta),$$

for any choice of a real number θ . For $z \neq 0$, we may write

$$z = a + bi = r(\cos \theta + i \sin \theta) \tag{29.1}$$

where, as you learned when you discussed polar coordinates, $\theta \in \mathbb{R}$ is the measure of the angle from the polar axis to the line joining the origin to the point (a, b) . When $\theta > 0$, the measure is taken in the counterclockwise direction (as in [Figure 29.5](#)) and when $\theta < 0$ it is taken in the clockwise direction. The nonnegative real number $r = (a^2 + b^2)^{1/2}$ represents the distance of z to the origin. Of course, there are infinitely many choices for θ , for once one choice works $\theta + 2n\pi$ will work for every integer n .

If you haven't done this before, you should practice writing several numbers in both notations. You can check that you have the correct answer using a calculator or computer.

Euler's formula provides another way to write complex numbers. Euler's formula says that for any real number t ,

$$e^{it} = \cos t + i \sin t. \tag{29.2}$$

As a consequence of equations 29.1 and 29.2, we can write every complex number in the form $re^{i\theta}$, where θ and r are real numbers and $r \geq 0$.

We'll ask you to provide a justification for Euler's formula in a moment. Before proceeding, we provide two exercises to convince you that multiplication and raising complex numbers to high powers is much more pleasant if you use Euler's formula. What we mean is the following: Consider $z = re^{i\alpha}$ and $w = se^{i\beta}$. Then

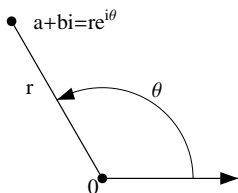


Fig. 29.5 The complex number $a + bi = re^{i\theta}$ with $\theta > 0$

$$zw = (re^{i\alpha})(se^{i\beta}) = rse^{i(\alpha+\beta)}. \quad (29.3)$$

- Multiply $e^{i\pi/4}$ and $2e^{i\pi/3}$ by writing the first as $a + bi$, the second as $c + di$, and then performing the multiplication. Then multiply the two numbers using equation (29.3). Finally, show that the two answers are equal. (For the final part of this problem, you may want to use the formulas for $\sin(x + y)$ and $\cos(x + y)$.)
- Compute $(1 + i)^{10000}$ without a calculator. You should write the answer in the form $s^n(a + bi)$, where $s > 0$.

We are not interested in a rigorous proof of Euler's formula here, but we hope to convince you of its validity using facts about series from your calculus classes. So recall that for all real x the following series converge as indicated:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}, \quad \cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}, \quad \text{and} \quad \sin x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}.$$

- Ignoring issues of convergence in the proofs below, assuming that you may replace x by it in the equations above, and rearranging terms in the series if need be, show that you can obtain Euler's formula: $e^{it} = \cos t + i \sin t$. In particular, when $t = \pi$ we have

$$e^{i\pi} = \cos \pi + i \sin \pi,$$

or

$$e^{i\pi} + 1 = 0,$$

which is sometimes called Euler's equation.

- Show that $e^{i\pi/2} = i$. Using this fact and assuming that exponentiation works as usual, show that i^i is real. Once you have completed this part of the project, please read the notes (under Notes and Sources) provided below.
- Complex numbers are, actually, more complex than real numbers. Our brief discussion of exponentiation has already pointed out one potential problem. There are some very famous "false proofs" involving complex numbers. Here is a proof that $1 = -1$. See if you can figure out where the error is.

Not a proof. Since $(-1)/1 = 1/(-1)$ we may take square roots to obtain the equation $\sqrt{-1/1} = \sqrt{1/-1}$. Thus $\sqrt{-1}/\sqrt{1} = \sqrt{1}/\sqrt{-1}$. So $i = 1/i$ and multiplying the equation by i , we get $-1 = 1$. \square

We probably all can agree that something is wrong. Find the mistake and write a concise explanation of what the error is.

In the final part of this guided project, we discuss order on the complex numbers. In Chapter 12 we studied some properties of the ordered sets \mathbb{R} and \mathbb{N} . For example, we introduced the well-ordering principle of \mathbb{N} . Sets, including \mathbb{N} and \mathbb{R} , may be ordered in many ways. In this project, we will discuss a specific order on the complex numbers. At this point, you will need to recall Definitions 13.1 and 13.2.

We can define an order on the complex numbers as follows: If $z = a + bi$ and $w = c + di$, we will say that

$$z \preceq w \text{ if } a < c \text{ or we have } a = c \text{ and } b \leq d.$$

Note that if the numbers z and w are real, then $z = a + 0i$ and $w = c + 0i$ and this order reduces to the usual one (\leq) on \mathbb{R} . This order is called the lexicographical order on \mathbb{C} because the order is the same as the one used to order the words in a dictionary.

7. Show that the lexicographical order on \mathbb{C} is a partial order.
8. Show that the lexicographical order on \mathbb{C} is a total order.
9. One important property of \mathbb{R} is the following: If a, b , and c are real numbers with $a \leq b$ and $0 < c$, then $ac \leq bc$. We now investigate this property in \mathbb{C} .

We have seen that the lexicographical order on \mathbb{C} reduces to the usual less than or equal to relation on \mathbb{R} . Writing $u \prec v$ for $u \preceq v$ and $u \neq v$, does the lexicographical order preserve the property above? That is, if $z \preceq w$ and $0 \prec u$, is it always the case that $zu \preceq wu$? Either prove this or give a counterexample.

Open-Ended Project

This part of the project is an exercise in searching journals and/or the Web. There are at least two other “proofs” of Euler’s formula. Do a search until you find the one you feel is simplest. You should have at least three proofs (including the one given here). Explain the one you have decided is simplest, providing as much detail as you can. Summarize the other two and explain why you believe the proof you chose is the “best.”

Notes and Sources

In your proof that i^i is real, we told you to use the fact that $e^{i\pi/2} = i$. It is also true that $e^{i5\pi/2} = i$ and had we suggested you use $e^{i5\pi/2}$ instead, you would have obtained a different value of i^i . That's because exponentiation of complex numbers is more complicated than that of real numbers and it involves a discussion of “multivalued functions” that we will not address here. Instead, we recommend [95] and [74]. We do note, however, that this is like a complex version of Theorem 29.4, which showed that there exist irrational numbers a and b such that a^b is rational.

The equation $e^{i\pi} + 1 = 0$ is considered one of the most beautiful equations of all time. One reason for this is that it provides a relationship between e , i , π , 1 , and 0 , which are considered five of the most important constants in mathematics. In fact, readers of *Physics World* were asked in 2004 to vote for their favorite equation and this one came in first, beating out other obvious contenders such as $E = mc^2$. (Admittedly, it tied with Maxwell's equations of electromagnetism.) Nahin, [73], wrote a whole book about what he called “Dr. Euler's Fabulous Formula.”

You might wish to conduct a survey of your mathematical friends and teachers to see what they think is the most beautiful equation. It will almost certainly be Euler's equation!

29.7 When Does $f^{-1} = 1/f$?

Introduction

Students often confuse the inverse of f , denoted f^{-1} , with the multiplicative inverse of f , denoted $1/f$. When are these two equal? Surprisingly, although the mistake of assuming $f^{-1} = 1/f$ is common, functions that have this seemingly intuitive property are not common at all.

Prerequisites

This project requires an understanding of functions and their inverses, presented in Chapters 14–16.

Guided Project

In what follows, $f : X \rightarrow Y$ will always denote a bijective function between two subsets, X and Y , of \mathbb{R} satisfying $f^{-1} = 1/f$.

1. What can you say about the domain and range of such a function?
2. Find an example of such a function, where the domain of f consists of a single point.
3. Find an example of such a function on a domain consisting of two points.
4. Can such a function f exist on the integers? Why or why not?
5. Show that $(f \circ f)(x) = 1/x$ and $f(1/f(x)) = x$ for all $x \in X$.
6. Show that $f(1/x) = 1/f(x)$ for all $x \in X$.
7. Define a function $g : (\mathbb{R} \setminus \{0\}) \rightarrow (\mathbb{R} \setminus \{0\})$ by

$$g(x) = \begin{cases} -x^3, & \text{if } x > 0 \\ -1/(x^{1/3}), & \text{if } x < 0. \end{cases}$$

Show that g satisfies $g^{-1} = 1/g$ on its domain $\mathbb{R} \setminus \{0\}$.

8. Can you find other examples of such functions?

Open-Ended Project

We mention here some other common errors that occur with functions $f : X \rightarrow \mathbb{R}$, where $X \subseteq \mathbb{R}$. Students often confuse the composition $f \circ f$ with the product $f \cdot f$, where $(f \cdot f)(x) = f(x) \cdot f(x)$ for all $x \in X$. What can you say about a function f that satisfies $f \circ f = f \cdot f$?

Yet another problem arises with powers. Which functions $f : X \rightarrow \mathbb{R}$ have the property that $f(x^2) = (f(x))^2$ for all $x \in X$?

Notes and Sources

This project is based upon two interesting articles. The first article, [6], has several other interesting questions and problems for students. Some of them require knowledge of continuous functions. The second article, [18], is rather advanced, and it presents much more than we have here. It includes a look at complex-valued functions.

29.8 Pascal's Triangle

Introduction

In this project you will explore an arithmetical triangle that was the object of study by Blaise Pascal in a treatise he wrote in 1654 (though it was known to mathemati-

cians before him). He used this triangle to solve a question posed to him about gambling. You can find out more about the history of this problem from the references at the end of the project.

Prerequisites

This project is appropriate after Chapter 18 on induction has been covered. You should read over Problem 18.25 before you begin.

Guided Project

Pascal's triangle is presented below. Each line has one more entry than the previous line. All entries along the left and right edges of the triangle are one. Every other entry in a line is the sum of the two numbers on the line above that lie to the immediate left and right. The triangle is unbounded below.

$$\begin{array}{ccccccc}
 & & & & 1 & & & & \\
 & & & & & 1 & & 1 & \\
 & & & & & & 1 & & 2 & & 1 \\
 & & & & & & & 1 & & 3 & & 3 & & 1 \\
 & & & & & & & & 1 & & 4 & & 6 & & 4 & & 1 \\
 & & & & & & & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & & & & & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot \\
 & & & & & & & & & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot
 \end{array}$$

Recall that we defined n factorial and the binomial coefficient $\binom{n}{k}$ in the problems in Chapter 18.

The first few exercises should help familiarize you with Pascal's triangle.

1. Compute each of the following:

$$\binom{6}{0}, \binom{6}{1}, \binom{6}{2}, \binom{6}{3}, \binom{6}{4}, \binom{6}{5}, \text{ and } \binom{6}{6}.$$

2. Solve Problem 18.25 (c) if you haven't already. In other words, prove that for all $k, n \in \mathbb{N}$ with $1 \leq k \leq n$, we get

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

3. Use the definition of Pascal's triangle given above to show that all entries in Pascal's triangle are binomial coefficients and find a familiar mathematical expression for the k th entry from the left in the n th row. (The first entry from

the left is entry 0 and the first row is row 0.) Use induction to prove that your familiar expression is correct.

4. For each $n \in \mathbb{N}$, consider the statement

$$\sum_{k=0}^n \binom{n}{k} = 2^n.$$

- (a) Check this formula for a few small values of n .
 (b) Prove the statement. (You may use Theorem 18.10.)
 (c) Show how you can obtain this sum using Pascal's triangle.
5. For each $n \in \mathbb{Z}^+$, consider the statement

$$\sum_{k=1}^n \binom{k}{k-1} = \binom{n+1}{n-1}.$$

- (a) Do something clever for a few n (as you did in 4 (a)).
 (b) Prove the statement.
 (c) Show how you can obtain this sum using Pascal's triangle.
6. How does Pascal's triangle relate to the Binomial Theorem (Theorem 18.10)?

Now you are ready for the main task of this project. Work it carefully. Be as creative, imaginative, clever, and resourceful as possible.

Open-Ended Project

Find a pattern that appears in Pascal's triangle, but that does not already appear in the text. State your formula carefully, and then prove the result. There are many different patterns!

Notes and Sources

Pascal's original article, in Latin with a French translation, appears in [81]. A very readable comprehensive history of Pascal's triangle can be found in [23].



Fig. 29.6 First stage: E_1



Fig. 29.7 Second stage: E_2

29.9 The Cantor Set

Introduction

In this project, you'll learn about the Cantor set—a set that is in some ways very small, and in other ways very big.

Prerequisites

Proofs in this section are by induction. You will need the background provided by Chapter 18, and Chapters 21–23.

Guided Project

1. **(The Cantor Set)** To construct the Cantor set, let $I = [0, 1]$.
 - (a) (First stage.) We will remove the middle third of this set; that is, we remove the open interval $(1/3, 2/3)$ from $[0, 1]$. So two intervals remain. (See [Figure 29.6](#).) Let $E_1 = I \setminus (1/3, 2/3) = [0, 1/3] \cup [2/3, 1]$. If you were to assign a length to E_1 , what length would you assign?
 - (b) (Second stage.) Remove the middle open third from each of the two remaining intervals; that is, let $E_2 = E_1 \setminus ((1/9, 2/9) \cup (7/9, 8/9))$. So E_2 is a union of four closed intervals. (See [Figure 29.7](#).) Write E_2 as this union of four closed intervals. If you were to assign a length to E_2 , what length would you assign?
 - (c) (Third stage.) Remove the middle open third from each of the remaining four intervals. Thus E_3 is a union of eight intervals. (See [Figure 29.8](#).) Write E_3 as a union of these eight closed intervals. If you were to assign a length to E_3 , what length would you assign?
 - (d) (n th stage.) Now consider E_n , obtained from E_{n-1} by removing the open middle thirds of each of the intervals that compose E_{n-1} . If you



Fig. 29.8 Third stage: E_3

were to assign a length to E_n , what length would you assign? State your guess for the length of E_n in a complete, coherent sentence. Prove that your guess is correct.

The **Cantor set** is the set E defined by $E = \bigcap_{n=1}^{\infty} E_n$.

2. If you were to assign a length to E , what length would you assign? Why?
3. Give examples of numbers that you know are in the Cantor set; that is, give examples of numbers that are in E_n for every n .
4. *Another view of the Cantor set.* There are far more points in the Cantor set than you might think. To see this, it is best to revisit the Cantor set.

Each point x in the interval $[0, 1]$ has something called a ternary expansion. The first digit in the ternary expansion for x , denoted x_1 , is found as follows: We divide the interval $[0, 1]$ into thirds. If x lies in the first third, $[0, 1/3]$, we assign x_1 the value 0. If x lies in the middle third, $[1/3, 2/3]$, we assign x_1 the value 1, and if it lies in the last third, $[2/3, 1]$, we assign x_1 the value 2. (We note that there is some ambiguity about what happens at the endpoints. When working with the Cantor set (as we discuss below), whenever we have a choice, we will choose either 0 or 2 and not the number 1.)

We now proceed to the second digit, x_2 , in the ternary expansion, which we find as follows: If $x_1 = 0$, then x lies in the interval $[0, 1/3]$. Divide this interval into thirds. If x lies in the first third, $[0, 1/9]$, we assign x_2 the value 0. If x lies in the middle third, $[1/9, 2/9]$, we assign x_2 the value 1. And if x lies in the final third, $[2/9, 3/9]$, we assign x_2 the value 2. Similarly, if $x_1 = 1$, then x lies in the interval $[1/3, 2/3]$, and we assign x_2 a value of 0 if x lies in the interval $[3/9, 4/9]$, a value of 1 if x lies in the interval $[4/9, 5/9]$, and a value of 2 if x lies in the interval $[5/9, 6/9]$. Finally, if $x_1 = 2$, then x lies in $[2/3, 1]$, and we divide this interval into thirds, assigning x_2 the value of 0, 1, or 2.

For x_3 , we use x_1 and x_2 to tell us which interval to look at. We then divide that interval into thirds, and we assign a value of 0, 1, or 2 to x_3 . It should be clear that all endpoints will have two possible representations, while all other points will have exactly one representation. Comparing the procedure defined in part 1 of this project, with the procedure we have outlined to find the ternary expansion of x , we see that the Cantor set consists of all points for which there exists a ternary expansion consisting of 0's and 2's. (That's why we never chose the number 1.) Without going into too many details, the ternary expansion really means that

$$x = \sum_{k=1}^{\infty} \frac{x_k}{3^k}, \text{ where } x_k = 0, 1, \text{ or } 2.$$

- (a) There are two ternary representations for the number $1/3$. What are they?
 - (b) There are two ternary representations for the number $2/3$. What are they?
 - (c) Find the first six terms of the sequence associated with $1/4$.
 - (d) Find the first six terms of the sequence associated with $1/8$.
5. If you have studied series, then you recall that for $-1 < r < 1$, we have the following formula for the sum of the geometric series: $\sum_{k=1}^{\infty} r^k = r/(1-r)$. Using the first six terms of the ternary expansion for $1/4$ that you determined above, guess all the other digits in the expansion. Then sum the series $\sum_{k=1}^{\infty} x_k/3^k$ to show that you have found the representation for $1/4$. Does $1/4$ lie in the Cantor set? What about $1/8$?
 6. We have presented the outline of a proof that there is a one-to-one correspondence between points in the Cantor set and sequences of 0's and 2's. Fill in the details, and use this to prove the theorem below.

Theorem 29.8. *The Cantor set is uncountable.*

So the Cantor set has “length” zero, but is an uncountable set. You can learn more about the Cantor set (much more) and the idea of length in the reference given below.

Open-Ended Project

What happens if instead of removing the middle third of the set, you remove the middle fifth? Think about other sets you can create in this way, and say as much as you are able to about them.

Notes and Sources

This topic is discussed in many textbooks. In particular, a summary of many of the interesting properties of this set can be found in [8, pp. 352–354]. For a short article (with a card trick) relating the Cantor set to fractals, see [12, pp. 114–121].

29.10 The Cauchy–Bunyakovsky–Schwarz Inequality

Introduction

In this project you'll prove two inequalities. The second of the two is the triangle inequality in \mathbb{R}^n , and the first is used to prove the second.

Prerequisites

What you need for this project depends upon how you prove it. You may need little to no background, other than an understanding of what \mathbb{R}^n is and how you add and subtract in that space.

Guided Project

Consider two points, $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$, in \mathbb{R}^n . Recall that $x + y = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$ and $x \cdot y = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$. We'll introduce some notation that will make things neater. We'll write $x \cdot y = \sum_{j=1}^n x_j y_j$ and $\|x\| = \sqrt{x_1^2 + x_2^2 + \dots + x_n^2}$. For $\lambda \in \mathbb{R}$, we write $\lambda x = (\lambda x_1, \lambda x_2, \dots, \lambda x_n)$.

1. Get used to this notation: Let $x = (0, 1, 2)$ and $y = (-1, 2, 3)$ in \mathbb{R}^3 . What is $x \cdot y$? What is $\|x\|$? $\|y\|$? $x - y$? $x + y$? Make up some examples in \mathbb{R}^2 and \mathbb{R}^4 .
2. Keep getting used to this notation: What is the set $\{x \in \mathbb{R}^2 : \|x\| = 1\}$? What is $\{x \in \mathbb{R}^3 : \|x\| = 1\}$? If you fix $x \in \mathbb{R}^3$, what is $\{y \in \mathbb{R}^3 : \|x - y\| \leq 2\}$?
3. Let $x \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$. Prove that $\|\lambda x\| = |\lambda| \|x\|$.
4. Let $x, y \in \mathbb{R}^n$. Prove that $(x + y) \cdot (x + y) = \|x + y\|^2$.
5. Let $x, y \in \mathbb{R}^n$. Prove that $(x - y) \cdot (x - y) = \|x\|^2 - 2(x \cdot y) + \|y\|^2$.
6. Let $x, y \in \mathbb{R}^n$. Find a similar formula for $(x + y) \cdot (x + y)$.
7. Suppose x and y are two points in \mathbb{R}^n such that $\|x\| = 1$ and $\|y\| = 1$. Prove that $|x \cdot y| \leq 1$. (Problem 5 above together with the fact that $z \cdot z \geq 0$ for all $z \in \mathbb{R}^n$, should help to point you in the right direction.)
8. Let $x \in \mathbb{R}^n$. Prove that if $x \neq (0, 0, \dots, 0)$, then $\|x/\|x\|\| = 1$.
9. Let x and y be two points in \mathbb{R}^n . Prove that $|x \cdot y| \leq \|x\| \|y\|$. (Problems 7 and 8 should be helpful here.) In many textbooks, this inequality is referred to as the Cauchy–Schwarz inequality; others call it the Cauchy–Bunyakovsky–Schwarz inequality.
10. Use Problems 4 and 9 to prove that for x and y in \mathbb{R}^n , the triangle inequality holds; that is, $\|x + y\| \leq \|x\| + \|y\|$.
11. The Cauchy–Bunyakovsky–Schwarz inequality can be used to prove interesting inequalities about real numbers. Use it to prove the following: Let

a_1, a_2, \dots, a_n be real numbers. Then

$$\sum_{j=1}^n a_j^2 \geq \left(\sum_{j=1}^n a_j \right)^2 / n.$$

12. Bunyakovsky, Cauchy, and Schwarz all have their names attached to this theorem. Who proved what, and when did they prove it?

Open-Ended Project

For two points x and y in \mathbb{R}^n , the **line segment** joining x and y is defined by the set $\{z \in \mathbb{R}^n : z = \lambda x + (1 - \lambda)y, \text{ where } \lambda \in \mathbb{R} \text{ and } 0 \leq \lambda \leq 1\}$. For example, in \mathbb{R}^2 choose two points, say $(1, 2)$ and $(2, 4)$. Then the line segment joining these two points is the set

$$\{(\lambda + 2(1 - \lambda), 2\lambda + 4(1 - \lambda)), 0 \leq \lambda \leq 1\} = \{(2 - \lambda, 4 - 2\lambda) : 0 \leq \lambda \leq 1\},$$

which is indeed the line segment joining the two points $(1, 2)$ and $(2, 4)$. Try this out on other points, and in \mathbb{R}^3 , and then move on to the next definition:

A nonempty set $S \subseteq \mathbb{R}^n$ is said to be **convex** if whenever $x, y \in S$, then the line segment joining x and y is in S . Investigate this definition, considering the following in your investigation. (You'll find the triangle inequality, as well as many of the exercises above, quite handy.)

1. Show that $\{x \in \mathbb{R}^n : \|x\| \leq 1\}$ is convex.
2. Give other examples of convex sets.
3. Is the union of two convex sets convex?
4. Is the intersection of two convex sets convex?
5. Now return to part 2 and see if you can come up with other interesting examples.
6. What are some other interesting questions (and answers) about convex sets?

Notes and Sources

For more information on the Cauchy–Bunyakovsky–Schwarz inequality, see the article by P. Schreiber [96]. There are also other (more clever, less intuitive) ways of proving this inequality.

29.11 Algebraic Numbers

Introduction

A real number is **algebraic** if it is the root of a polynomial

$$p(x) = a_n x^n + \cdots + a_1 x + a_0,$$

where n is a positive integer, $a_0, a_1, \dots, a_n \in \mathbb{Z}$, and $a_n \neq 0$. A real number is **transcendental** if it is not algebraic.

It's easy to think of examples of algebraic numbers: 0 is algebraic, because it is a (the) root of the polynomial $p(x) = x$; the number $1/2$ is algebraic, because it is a root of the polynomial $q(x) = 2x^2 - x$. It's much more difficult to think of a number that is not algebraic. Why? Well, suppose you have a guess that a certain real number a is transcendental. Then to prove your guess, you must show that for every polynomial p with integer coefficients, $p(a) \neq 0$. Before reading on, try to guess whether there are more transcendental numbers or more algebraic numbers.

In an 1874 paper Georg Cantor proved:

Theorem 29.9 (Cantor). *There are countably many algebraic numbers.*

In this project, you will prove this theorem.

Prerequisites

This project requires material up to and including Chapter 23. We mention one additional theorem that you will need and that we have not covered yet, namely Theorem 29.15 stated below. If you work Project 29.12, you will also have a proof of this theorem. For this project, however, you may assume the validity of Theorem 29.15 and apply it to complete the work required here.

Theorem 29.15. *If for each $j \in \mathbb{Z}^+$ the set A_j is countable, then $\bigcup_{j \in \mathbb{Z}^+} A_j$ is countable.*

Guided Project

1. Familiarize yourself with the definition of an algebraic number by answering the next few questions. As you do so, you should also get an idea of what transcendental numbers are like, and you will begin to suspect some of your old numerical friends of being transcendentals.

Come up with examples of algebraic real numbers that have not been presented in this project. Are some rational numbers algebraic? are all rational numbers algebraic? What about the irrational numbers? How would you

prove that a particular number is algebraic or transcendental? Try to guess which of the following are transcendental numbers: $\sqrt{2}$, $5/7$, π , and e . (If you think one of these numbers is algebraic, prove it. It's beyond our capabilities, at this time, to prove that the other numbers are transcendental.)

Now you should be ready for the proof of Cantor's theorem. The proof is outlined below.

2. How might you attack the proof of Cantor's theorem? Does it remind you of anything we have done before? What?
3. Solve Problem 5.22, if you haven't already done so.
4. Solve Problem 23.10, if you haven't already done so.
5. Recall that for sets A_1, A_2, \dots, A_n , the Cartesian product of these n sets is

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \dots, x_n) : x_j \in A_j\}.$$

Prove the following generalization of Corollary 23.10.

Theorem 29.10. *Let $n \in \mathbb{Z}^+$. If A_i is countable for all $i = 1, 2, \dots, n$, then $A_1 \times A_2 \times \cdots \times A_n$ is countable.*

6. Let $n \in \mathbb{Z}^+$. Show that the set of polynomials of degree n with integer coefficients is countable.
7. Prove that the set of all polynomials with integer coefficients is countable.
8. Prove that the set of algebraic numbers is countable.
9. Show that there exist transcendental numbers. (Suggestion: Don't try to actually find such a number; just try to show that they exist.)
10. Are the transcendental numbers countable or uncountable? Prove your answer.

You have now seen how the partition of the reals into the algebraic numbers and the transcendental numbers works. It is time to try something on your own.

Open-Ended Project

Define a property \mathcal{P} of real numbers that seems to be of value to you. Let A denote the set of all reals that have property \mathcal{P} , and let B denote the set of all reals that do not have property \mathcal{P} . Then decide for each of the two sets, A and B , whether the set is countable or not. Prove all your statements. The more creative you are in defining \mathcal{P} , the harder it will be to prove the countability or uncountability of your sets. Here's a chance to really show all your mathematical prowess!

Notes and Sources

There is a difference between proving the existence of transcendental numbers, and showing that a particular number is transcendental. As we mention in the Spotlight: Hilbert's Seventh Problem, proofs that the numbers π and e are transcendental were given around the time of Cantor's proof. The original paper by G. Cantor [16] is written in German. A brief summary of Cantor's proof can be found in M. Kline's book [59, pp. 996–997].

29.12 The Axiom of Choice

Introduction

Return, for the moment, to Hilbert's Hotel Infinity discussed in Chapter 21. Suppose that in each room there is exactly one pair of boots. Can you come up with a rule that chooses one boot from each room? To be mathematically precise, we'll introduce the following notation. The set B_j will contain the two boots, and only the two boots, in room j . Then $\mathcal{B} = \{B_j : j \in \mathbb{Z}^+\}$ is the collection of all these sets of boots. Can we find a function $f : \mathcal{B} \rightarrow \bigcup_{j \in \mathbb{Z}^+} B_j$ such that $f(B_j) \in B_j$? The answer, as you probably guessed, is "sure, we can do that." For instance, we can define $f(B_j)$ to be the left boot in B_j . The sentence " y is the left boot in the set B_j " is a statement. Thus the substitution axiom on page 365 allows us to obtain the desired function.

Suppose now that the hotel guests have gone out and taken their boots, but they have forgotten their socks. Assume that their socks are identical; that is, you cannot tell the right sock from the left sock. (This is true of most, but not all, socks!) Can we come up with a rule that chooses one sock from each room? We'll let S_j denote the set containing the two socks, and only the two socks, of room j . Then $\mathcal{S} = \{S_j : j \in \mathbb{Z}^+\}$ is the collection of all these sets of socks. The question is then, can we find a function $f : \mathcal{S} \rightarrow \bigcup_{j \in \mathbb{Z}^+} S_j$ such that $f(S_j) \in S_j$? This time it's difficult to come up with a solution to this problem; in fact, we don't have a rule available along the lines of the one we had for shoes. Nevertheless, intuitively speaking, it seems as though it should be possible to pick one sock from each pair—at least, most mathematicians think this is intuitive. We'll now introduce an axiom that will allow us to do exactly this.

Axiom 29.11 (Axiom of Choice). Given a nonempty collection \mathcal{F} of nonempty sets, there is a function $f : \mathcal{F} \rightarrow \bigcup_{A \in \mathcal{F}} A$ such that $f(A) \in A$.

There are many statements that turn out to be equivalent to the axiom of choice. Some of these statements are major theorems, some are part of set theory, and some are theorems in other fields of mathematics. We'll just mention two of the most important ones in set theory. In order to understand the statements you will need to review Definitions 13.1 and 13.2.

We'll introduce a few more terms before we begin this project. You'll need a firm grasp on these definitions, so work through some examples and nonexamples of each. We start by generalizing Definition 19.3 to arbitrary partially ordered sets. Namely, if X is a set with a partial order \preceq and A is a nonempty subset of X , then we call $a \in X$ an upper bound of A if $x \preceq a$ for all $x \in A$. A chain in a partially ordered set X is a subset C that is totally ordered when the order on X is restricted to C . A least element in a partially ordered set X is an element $m \in X$ such that $m \preceq x$ for all $x \in X$. A maximal element, $M \in X$, is an element with the property that for all $x \in X$, if $M \preceq x$, then $M = x$. Finally, a partially ordered set Y is well-ordered if every nonempty subset A of Y has a least element in A .

Theorem 29.12 (Well-ordering theorem). *Every set can be well-ordered.*

This theorem surely reminds you of the well-ordering principle of \mathbb{N} in Chapter 12. In some ways it is a generalization, as the theorem above applies to any set—not just to the natural numbers. But be careful: the well-ordering theorem does not tell you about a particular order on a set; it just claims that there is an order under which the set is well-ordered. For instance, \mathbb{R} with the usual order (less than or equal to) is not well-ordered. (Why not?) The theorem claims that there is an order under which \mathbb{R} is well-ordered but, unfortunately, it does not give us any hints on how to construct such an order. Looking at it from this perspective, we see that the theorem stated above is not a generalization of the well-ordering principle of \mathbb{N} .

It turns out that the following form of the axiom of choice is particularly useful. It is due to Max Zorn, a much-loved mathematician as can be seen from testimonies of his family [114] and colleagues [40].

Lemma 29.13 (Zorn's lemma). *Let X be a partially ordered set such that every chain in X has an upper bound in X . Then X contains a maximal element.*

For a proof of the equivalence of Zorn's lemma, the axiom of choice, and the well-ordering theorem see [41]. A short proof that the axiom of choice implies Zorn's lemma is in [63]. Despite the fact that all three statements are equivalent, people have a better intuition for some of them than for others. The American mathematician Jerry Bona expressed this aptly: "The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?"

One of our goals in this project is to help you understand the axiom of choice; it will appear frequently in your future mathematics courses. But our main goal in the guided portion of this project is to show that we can find a total order that allows us to compare the cardinalities of every pair of sets from a collection of sets, \mathcal{A} .

Prerequisites

This project requires that you have a basic understanding of sets, relations, order, and functions as explained in Chapters 5 through 17. You also need to understand the theory of cardinality as developed in Chapters 22 through 24.

Guided Project

In the introduction to this project we presented you lots of definitions, some old and some new. We need to make sure that you fully understand them before proceeding to the project.

1. Solve (or re-solve) Problems 13.13–13.15.
2. Consider $\mathcal{P}(\mathbb{N})$ with the partial order \subseteq . Give an example of an interesting nonempty finite subset of $\mathcal{P}(\mathbb{N})$ that is a chain and an interesting infinite subset of $\mathcal{P}(\mathbb{N})$ that is a chain. Then give an example of a nonempty finite subset of $\mathcal{P}(\mathbb{N})$ that is not a chain and an infinite subset of $\mathcal{P}(\mathbb{N})$ that is not a chain—both sets should be interesting! (We define “interesting” in this problem to mean that the sets are nontrivial, and that the answers to part 3 below are as varied as possible.)
3. Write down the definitions of greatest element and minimal element. Explain the difference between greatest element and maximal element as well as the difference between least element and minimal element. For each of your four sets in part 2, decide whether it has a minimal, maximal, greatest, and least element.

Let \mathcal{A} be a nonempty collection of sets and denote by $E(\mathcal{A})$ the set of all equivalence classes of the relation \approx on \mathcal{A} as defined in Definition 21.1 (and shown to be an equivalence relation in Theorem 21.1). Thus if $E_A \in E(\mathcal{A})$, then two sets A_1 and A_2 in \mathcal{A} are in E_A if and only if there is a bijection between the two sets A_1 and A_2 .

For $E_A, E_B \in E(\mathcal{A})$, we will let A' denote a set in E_A and B' denote a set in E_B . We define the relation \preceq on $E(\mathcal{A})$ by $E_A \preceq E_B$ if $|A'| \leq |B'|$ (that is, there is an injective function $f : A' \rightarrow B'$).

We aim to establish the theorem below, using the terminology introduced above. This theorem tells us that we can compare the cardinality of any two sets and that this comparison obeys the usual rules of a total order.

Theorem 29.14. *For a nonempty collection \mathcal{A} of sets, the relation \preceq is a total order on $E(\mathcal{A})$.*

4. If you have not yet done so, work Problem 24.4.
5. Prove that the relation \preceq on $E(\mathcal{A})$, as defined above, is well-defined. That is, show that given $E_A, E_B \in E(\mathcal{A})$ we can always find $A' \in E_A$ and $B' \in E_B$ and that the definition of \preceq does not depend on the particular choice of A' and B' .
6. Using the result of part 4, show that \preceq is a partial order on $E(\mathcal{A})$.
7. For two sets A and B we say that f is a partial function from A to B if $f : A' \rightarrow B$ for some $A' \subseteq A$. Let \mathcal{F} be the set of all injective partial functions from A to B . We define a relation \vdash on \mathcal{F} as follows: For $f_1 : A_1 \rightarrow B$ and $f_2 : A_2 \rightarrow B$, partial functions in \mathcal{F} ,

$$f_1 \vdash f_2 \text{ if } A_1 = \text{dom}(f_1) \subseteq \text{dom}(f_2) = A_2 \text{ and} \\ f_1 \text{ is the restriction of } f_2 \text{ to } A_1.$$

Prove that \vdash is a partial order on \mathcal{F} .

8. Let A and B be two sets such that $|A| \not\leq |B|$. Prove that $|A| \leq |B|$ using the construction from part 7 of this project and Zorn's lemma.
9. Prove Theorem 29.14.

Now we turn our attention to the following theorem, which is a generalization of Corollary 23.7.

Theorem 29.15. *If for each $j \in \mathbb{Z}^+$ the set A_j is countable, then $\bigcup_{j \in \mathbb{Z}^+} A_j$ is countable.*

10. Prove Theorem 29.15. Note that induction will not work here. We suggest that you adapt the ideas of the alternate proof of Theorem 23.11 outlined in Problem 23.12.
11. Say, explicitly, where you used the axiom of choice in the above proof.

Open-Ended Project

This part is an exercise in the history of mathematics. We will ask you to find resources, summarize your findings, and present them in a coherent and interesting way: Research the history of the axiom of choice. Find variations and give an overview of equivalent forms of the axiom of choice. What does mathematical constructivism think of the axiom of choice? (To answer the last question you will need to find out what mathematical constructivism is!)

Notes and Sources

There are many books that explore the history of the axiom of choice, its implications, and its equivalent forms. Two of them are [48] and [91]. The first part of the guided project is based on [28]. Finally, we note that there are many jokes based on Zorn's lemma and the axiom of choice. Every budding mathematician should know the following, "What is yellow, sour, and equivalent to the axiom of choice?" Answer: "Zorn's lemon."

Mathematicians are funny.

29.13 The RSA Code

Introduction

Though coding theory has always been important, a giant leap forward occurred in the second half of the twentieth century, with the invention of public key cryptography. The main idea (due to W. Diffie and M. Hellman) is the concept of a trapdoor function—a function that has an inverse, but the inverse is very difficult to find. In fact, it should require so long for someone who did not invent the original function to find the inverse that, for all practical purposes, the inverse does not exist. In 1976, R. L. Rivest, A. Shamir, and L. M. Adleman succeeded in finding such a class of functions, and their idea is based upon one of the most elementary ideas in mathematics—multiplication of two numbers. (See the Spotlight: Public and Secret Research in Chapter 28.)

It turns out that if you take two very large numbers and multiply them together, a machine can quickly compute the answer. But, if you give the machine the answer and ask for two factors, the factorization will not appear in a useful amount of time. The public key system, built upon these ideas, is now known as RSA-key (after the three men who created the system). It was described in Chapter 28, but in this project you will learn the details.

Prerequisites

We assume that you worked Chapters 27 and 28 on modular arithmetic and Euler's theorem. In particular, we will refer to the description of the public code that was given at the end of Chapter 28. The notation was introduced in the chapter. You will also need a good calculator; one that is able to determine whether a number is prime, can factor an integer, and can do modular arithmetic. For some parts of this project, you will need to use Mathematica. (If you don't have access to Mathematica, you can skip the parts that require it.)

Guided Project

1. Reread the paragraphs of Chapter 28 following the proof of Euler's theorem.
2. Let's start with a small example to make sure we understand the basics of the code: We choose $p = 13$ and $q = 17$ (so that $n = pq = 13 \cdot 17 = 221$). For the encoding exponent we choose $e = 11$. Verify that $e = 11$ is a feasible choice for the encoding exponent. Use the public key (n, e) to calculate the "secret" value of d . Encode the following three plaintexts:

(a) $m = 157$;

- (b) $m = 97216$;
- (c) $m = 91$.

Decode them again to convince yourself that the method works.

3. Note that $\gcd(91, 13 \cdot 17) = 13 \neq 1$, so the hypothesis of Example 28.8 is not satisfied. It turns out that the method still works, even in this case. Let's try to see why it still works—what could go wrong? In this code, we always assume that n is the product of two primes: $n = pq$, where p and q are primes. Thus, the $\gcd(m, n)$ is p, q , or 1. If $\gcd(m, n) = 1$, then Example 28.8 applies. Prove that even if $\gcd(m, n) = p$ (or q), the decoding with exponent d still works:

Lemma 29.16. *Let $m, n \in \mathbb{Z}$ with $0 < m < n$, $\gcd(m, n) = p$, and $n = pq$ for primes p and q with $p \neq q$. Further, let $e, d \in \mathbb{Z}$ with $ed \equiv 1 \pmod{\phi(n)}$. Then $m^{ed} \equiv m \pmod{n}$.*

You will need Theorem 28.10 (appearing in the problem section) and Theorem 28.7 for this proof.

4. In practice, n must be chosen to be quite large—certainly larger than 10. Nevertheless, it may still be the case that the plaintext m may satisfy $m \geq n$. Recall that if $m \geq n$, then we have to break the integer m into parts. Here's how to do this: Choose positive integers m_1, m_2, \dots, m_k such that $m_i < n$ for $1 \leq i \leq k$ and $m = m_1|m_2|\dots|m_k$, where the last expression denotes simple lining up of the integers in the decimal notation for m . (For example, if $m = 15208$ and $n = 77$, we can take $m_1 = 15$, $m_2 = 20$, and $m_3 = 8$. Then $m = 15|20|8$.) We will then denote the (chopped up) plaintext as (m_1, m_2, \dots, m_k) and the ciphertext as $(m_1^e \pmod{n}, m_2^e \pmod{n}, \dots, m_k^e \pmod{n})$. Now you are ready for the problem: Suppose you are given the public key, $n = 2881$ and $e = 47$. The intercepted message contains the criminal's hair color. However, the message is encoded according to the rules we described in the previous paragraph. The ciphertext reads $(2574, 1120, 166, 742)$ (all integers $\pmod{2881}$). The translation from letters to integers is done by converting $a \rightarrow 01, b \rightarrow 02, \dots, z \rightarrow 26$. Crack the code to find out the criminal's hair color.
5. If you cracked the message in the previous part, then it is obvious that this encryption is not safe. That's because the function we used in that part of the problem is not really a trapdoor function. However, it will become one if we choose our primes large enough. The bigger the primes, the harder it is to factor n (a task believed to be necessary to break the code). To get a feeling for the unequal amount of time it takes to find primes and multiply versus factoring, do the following on your calculator.
 - (a) By trial and error using the calculator's prime check, find two primes of ten digits each. (Primality testing is also an interesting and important subject. Your calculator uses sophisticated algorithms to check whether an integer is prime.)
 - (b) Multiply the two integers together. (Notice how quickly your calculator can do that!)

- (c) Now use the factor command to factor the number you obtained into its two primes. How long did it take?
6. To do safe encoding with the RSA method you need huge primes. Currently the recommendation is to use primes of 300 decimal digits each. If you have access to Mathematica, download the notebook RSA-Notebook.nb from the site given below. Explore this package and use it to communicate with a classmate, creating public keys and sending messages to each other.
<http://library.wolfram.com/infocenter/MathSource/1966/>

Open-Ended Project

Either create a code of your own, or find a code from another book. Try your code out on a partner, compare it to RSA, and discuss the strengths and weaknesses of your code.

Notes and Sources

The original paper by R.L. Rivest, A. Shamir, and L.M. Adleman appears in [88]. A more detailed treatment can be found in the general number theory text book by K. H. Rosen [89, Chapter 8]. See [90] for the commercial site of RSA Security Inc., a company founded by Rivest, Shamir, and Adleman.

To learn about primality testing, you can start with the *Mathematics Magazine* article [70] that gives a historical treatment of the subject up to the use of computers. A comprehensive treatment at the undergraduate level is contained in the text by Bressoud [14]. Also, a recent breakthrough is presented in the more advanced paper [1].

Spotlight: Hilbert's Seventh Problem

In 1900, David Hilbert presented a speech in Paris entitled “Mathematische Probleme” to the International Congress of Mathematicians. His aim was to look at the future of mathematics. His speech began with a description of what makes a problem significant. This introduction is followed by the statement and discussion of 23 problems. His speech appeared in 1900 in the *Nachrichten* of the Göttingen Scientific Society (more precisely, in *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen*). It was translated into English, and published in 1902 in the *Bulletin of the American Mathematical Society*.

Information about the time leading up to and following the presentation can be found in C. Reid's biography *Hilbert* [86]. We present the English translation of the seventh problem below. Even today, it's exciting to hold a copy of this speech in your hands.

(You can find a definition of algebraic and transcendental numbers in Project 29.11.)

Hermite's arithmetical theorems on the exponential function and their extension by Lindemann are certain of the admiration of all generations of mathematicians. Thus the task at once presents itself to penetrate further along the path here entered, as A. Hurwitz has already done in two interesting papers,¹ "Ueber arithmetische Eigenschaften gewisser transzenderter Funktionen." I should like, therefore, to sketch a class of problems which, in my opinion, should be attacked as here next in order. That certain special transcendental functions, important in analysis, take algebraic values for certain algebraic arguments, seems to us particularly remarkable and worthy of thorough investigation. Indeed, we expect transcendental functions to assume, in general, transcendental values for even algebraic arguments; and, although it is well known that there exist integral transcendental functions which even have rational values for all algebraic arguments, we shall still consider it highly probable that the exponential function $e^{i\pi z}$, for example, which evidently has algebraic values for all rational arguments z , will on the other hand always take transcendental values for irrational algebraic values of the argument z . We can also give this statement a geometrical form, as follows:

If, in an isosceles triangle, the ratio of the base angle to the angle at the vertex be algebraic but not rational, the ratio between base and side is always transcendental.

In spite of the simplicity of this statement and of its similarity to the problems solved by Hermite and Lindemann, I consider the proof of this theorem very difficult; as also the proof that

The expression α^β , for an algebraic base α and an irrational algebraic exponent β , e. g., the number $2^{\sqrt{2}}$ or $e^\pi = i^{-2i}$, always represents a transcendental or at least an irrational number.

It is certain that the solution of these and similar problems must lead us to entirely new methods and to a new insight into the nature of special irrational and transcendental numbers. [51, pp. 455–456].

Hilbert mentions Charles Hermite, who proved in 1873 that e is transcendental, and Ferdinand Lindemann, who proved in 1882 that π is transcendental [26, p. 466]. The answer to Hilbert's question was published in 1934 by Aleksandr O. Gelfond, and (independently) by Theodor Schneider in 1935. It follows from the Gelfond–Schneider theorem that $\sqrt{2}^{\sqrt{2}}$ is irrational (see Project 29.4), but there's an easier example. You can find this easier solution at [104].

Hilbert's original address can be found in [50]. The full text of the English translation is available on the Web, [51]. See also [59, Chapter 25, sec. 1] and [59, p. 980]. For another view of Hilbert's problems read [36], and for a recent book on this topic see [37].

In honor of the 100-year anniversary of Hilbert's Paris address, the new century, and the new millenium, several mathematicians were asked to pose problems for the next century. Steve Smale proposed 18 problems for your century that you can

¹ *Math. Ann.*, vols. 22, 32 (1883, 1888).

find in [100]. The article [39] by Phillip Griffiths also contains a look at challenges for the future. The Clay Mathematics Institute of Cambridge, Massachusetts (CMI) selected seven problems for the new millenium. They also offer a reward of one million dollars per problem, and consequently have received a fair amount of publicity. More information about the Institute and the problems can be found on their website, [19], as well as in [21].

Appendix

Algebraic Properties of \mathbb{R}

We will assume that you are familiar with the following properties of \mathbb{R} .

If x and y are real numbers, then both $x + y$ and $x \cdot y$ are real numbers. Furthermore, addition and multiplication satisfy the following axioms:

- A1. (The commutative property for addition) $x + y = y + x$ for all real numbers x and y ;
- A2. (The associative property for addition) $(x + y) + z = x + (y + z)$ for all real numbers $x, y,$ and z ;
- A3. (Existence of additive identity) There is a unique real number 0 such that $0 + x = x$ for all $x \in \mathbb{R}$;
- A4. (Existence of additive inverse) If $x \in \mathbb{R}$, then there is a unique element $-x$ such that $x + (-x) = 0$;
- M1. (The commutative property for multiplication) $x \cdot y = y \cdot x$ for all real numbers x and y ;
- M2. (The associative property for multiplication) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all real numbers $x, y,$ and z ;
- M3. (Existence of multiplicative identity) There is a unique real number 1 , with $1 \neq 0$, such that $1 \cdot x = x$ for all real numbers x .
- M4. (Existence of multiplicative inverse) For each nonzero real number x , there exists a unique real number x^{-1} such that $x \cdot x^{-1} = 1$;
- D1. (The distributive property) $(x + y) \cdot z = x \cdot z + y \cdot z$ for all real numbers $x, y,$ and z .

We note that this list of properties is not minimal; for example, the uniqueness of the additive identity 0 follows from some of the other properties in the list.

Order Properties of \mathbb{R}

A set satisfying all of the properties above is called a **field**. Thus, \mathbb{R} is an example of a field. In addition, \mathbb{R} has an order defined on it. This means the following:

There is a subset \mathbb{R}^+ of $\mathbb{R} \setminus \{0\}$ satisfying:

- O1. If $x, y \in \mathbb{R}^+$, then $x \cdot y \in \mathbb{R}^+$;
- O2. If $x, y \in \mathbb{R}^+$, then $x + y \in \mathbb{R}^+$;
- O3. For every real number x , exactly one of the following three things happens: either $x \in \mathbb{R}^+$, $-x \in \mathbb{R}^+$, or $x = 0$.

If x and y are two real numbers and $x - y \in \mathbb{R}^+$, we write $x > y$ (or $y < x$). The set \mathbb{R}^+ is called the **positive real numbers**. Thus \mathbb{R} is a field with an order, and we call it an **ordered field**. The third property, O3, is called the **trichotomy principle**. It is not difficult to show that the results below follow from the statements A1–A4, M1–M4, D1, and O1–O3.

Theorem. *Let x, y , and z be real numbers. Then the following hold:*

1. *If $x < y$ and $y < z$, then $x < z$;*
2. *If $x < y$, then $x + z < y + z$;*
3. *If $x < y$ and $z > 0$, then $x \cdot z < y \cdot z$;*
4. *If $x < y$ and $z < 0$, then $x \cdot z > y \cdot z$;*
5. *If $x \neq 0$, then $x^2 > 0$;*
6. *$1 > 0$;*
7. *If $x > 0$, then $x^{-1} > 0$.*

Proof. We'll do the first and the sixth of these; you can prove the others.

For the proof of (1), note that $y - x \in \mathbb{R}^+$ and $z - y \in \mathbb{R}^+$. By O2 and the associative and commutative properties of addition, $(y - x) + (z - y) = z - x \in \mathbb{R}^+$. Therefore $z - x \in \mathbb{R}^+$ and $x < z$.

For the proof of (6), note that 1 is the multiplicative identity, so $1 \cdot x = x$ for all $x \in \mathbb{R}$. Taking $x = 1$, we get $1^2 = 1 \cdot 1 = 1$. Since $1 \neq 0$, the result now follows from (5). \square

Axioms of Set Theory

To give set theory and large parts of mathematics a firm foundation, axioms were developed upon which mathematicians could agree. The rest of set theory, then, needs to follow from these axioms using the rules of logic. Currently the generally accepted axiomatic system is that due to Ernst Zermelo and Abraham Fraenkel, together with the axiom of choice. The abbreviation ZFC is commonly used for this system. (This list of axioms follows that of [41], except for the axiom of choice where we preferred a different version.)

- ZFC 1 (Axiom of extension) Two sets are equal if and only if they have the same elements.
- ZFC 2 (Axiom of specification) For every set A and every condition $S(x)$, there corresponds a set B whose elements are exactly those elements x of A for which $S(x)$ holds.
- ZFC 3 (Axiom of pairing) For every two sets there exists a set to which they both belong.
- ZFC 4 (Axiom of unions) For every collection of sets there exists a set that contains all the elements that belong to at least one set of the given collection.
- ZFC 5 (Axiom of powers) For each set there exists a collection of sets that contains, among its elements, all the subsets of the given set.
- ZFC 6 (Axiom of infinity) There exists a set containing 0 and containing the successor of each of its elements.
(Recall that $0 = \emptyset$ and the successor of x is $x^+ = x \cup \{x\}$.)
- ZFC 7 (Axiom of substitution) If A is a set and $S(a, b)$ is a sentence such that for each a in A the set $\{b : S(a, b)\}$ can be formed, then there exists a function $F : A \rightarrow \{\{b : S(a, b)\} : a \in A\}$ such that $F(a) = \{b : S(a, b)\}$.
- ZFC 8 (Axiom of choice) Given a nonempty collection \mathcal{F} of nonempty sets, there is a function $f : \mathcal{F} \rightarrow \bigcup_{A \in \mathcal{F}} A$ such that $f(A) \in A$.

Pólya's List

HOW TO SOLVE IT

First.
You have to *understand* the problem.

Second.
Find the connection between the data and the unknown. You may be obliged to consider auxiliary problems if an immediate connection cannot be found. You should obtain eventually a *plan* of the solution.

Third.
Carry out your plan.

Fourth.
Examine the solution obtained.

UNDERSTANDING THE PROBLEM

- What is the *unknown*? What are the *data*? What is the *condition*?
- Is it possible to satisfy the condition? Is the condition sufficient to determine the unknown? Or is it insufficient? Or redundant? Or contradictory?
- Draw a figure. Introduce suitable notation.
- Separate the various parts of the condition. Can you write them down?

DEVISING A PLAN

- Have you seen it before? Or have you seen the same problem in a slightly different form?
- Do you know a *related problem*? Do you know a theorem that could be useful?
- Look at the *unknown*/ And try to think of a familiar problem having the same or a similar *unknown*.
- *Here is a problem related to yours and solved before. Could you use it?* Could you use its result? Could you use its method? Should you introduce some auxiliary element in order to make its use possible?
- Could you restate the problem? Could you restate it still differently? Go back to definitions.
- If you cannot solve the proposed problem try to solve first some related problem. Could you imagine a more accessible related problem? A more general problem? A more special problem? An analogous problem? Could you solve a part of the problem? Keep only a part of the condition, drop the other part; how far is the unknown then determined, how can it vary? Could you derive something useful from the data? Could you think of other data appropriate to determine the unknown? Could you change the unknown or the data, or both if necessary, so that the new unknown and the new data are nearer to each other?
- Did you use all the data? Did you use the whole condition? Have you taken into account all essential notions involved in the problem?

CARRYING OUT THE PLAN

- Carrying out your plan of the solution *check each step*. Can you see clearly that the step is correct? Can you prove that it is correct?

LOOKING BACK

- Can you check the *result*? Can you check the argument?
- Can you derive the result differently? Can you see it at a glance?
- Can you use the result, or the method, for some other problem?

⁰ From the inside cover of George Pólya, *How to Solve it* [84], Copyright ©1945, 1973 renewed by Princeton University Press. Reprinted by permission of Princeton University Press.

References

1. Agrawal, M., Kayal, N., Saxena, N.: PRIMES is in P. *Ann. of Math. (2)* **160**(2), 781–793 (2004)
2. Akopyan, A.V., Zaslavsky, A.A.: Geometry of conics, *Mathematical World*, vol. 26. American Mathematical Society, Providence, RI (2007). Translated from the 2007 Russian original by Alex Martsinkovsky
3. Albers, D.J., Alexanderson, G.L.: A conversation with Ivan Niven. *College Math. J.* **22**(5), 370–402 (1991)
4. Alexanderson, G.L.: The Random Walks of George Pólya. Mathematical Association of America, Washington, DC (2000)
5. Alley, M.: The Craft of Scientific Writing, third edn. Springer, New York (1996)
6. Anschuetz, R., Sherwood, H.: When is a function's inverse equal to its reciprocal? *College Math. J.* **27**, 388–393 (2002)
7. Bailey, D.H., Borwein, J.M., Borwein, P.B., Plouffe, S.: The quest for pi. *Math. Intelligencer* **19**(1), 50–57 (1997)
8. Bartle, R.G., Sherbert, D.R.: Introduction to Real Analysis, second edn. John Wiley and Sons, New York (1992)
9. Batts, C.T.: A beamer tutorial in beamer. Downloadable from UNC Greensboro REU site: <http://www.uncg.edu/cmp/reu/summer2010/> (2007). Cited 30 December 2010
10. BBC-TV/WGBH Boston co-production: The Proof (videorecording), Nova Adventures in Science. South Burlington, VT: WGBH Boston Video (1997). Produced and written by John Lynch; directed by Simon Singh
11. Beckmann, P.: A History of π . The Golem Press, Boulder, CO (1971)
12. Benson, D.C.: The Moment of Proof. Oxford University Press, New York (1999)
13. Bogomolny, A.: Cut-the-Knot. <http://www.cut-the-knot.org>. Cited 30 December 2010
14. Bressoud, D.M.: Factorization and Primality Testing. Undergraduate Texts in Mathematics. Springer-Verlag, New York (1989)
15. Burton, D.: Elementary Number Theory, fifth edn. McGraw-Hill, Boston, MA (2002)
16. Cantor, G.: Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen. *J. Reine Angew. Math.* **77**, 258–262 (1874)
17. Carroll, L.: Alice in Wonderland, second edn. W.W. Norton & Company, New York (1992)
18. Cheng, R., Dasgupta, A., Ebanks, B.R., Kinch, L.F., Larson, L.M., McFadden, R.B.: When does $f^{-1} = 1/f$? *Amer. Math. Monthly* **105**, 704–717 (1998)
19. Clay Mathematics Institute: Millenium Prize Problems. <http://www.claymath.org> (2000). Cited 30 December 2010
20. Conway, J.H., Guy, R.K.: The Book of Numbers. Copernicus, New York (1996)

21. Devlin, K.: *The Millennium Problems*. Basic Books, New York (2002)
22. Dunham, W.: Euler: The Master of Us All, *The Dolciani Mathematical Expositions*, vol. 22. Mathematical Association of America, Washington, DC (1999)
23. Edwards, A.W.F.: *Pascal's Arithmetical Triangle*. Oxford University Press, New York (1987)
24. Edwards, A.W.F.: *Cogwheels of the mind*. Johns Hopkins University Press, Baltimore, MD (2004). The story of Venn diagrams, With a foreword by Ian Stewart
25. Enzensberger, H.M.: *The Number Devil: A Mathematical Adventure*. Henry Holt, New York (1998)
26. Eves, H.: *An Introduction to the History of Mathematics*, fourth edn. Holt, Rinehart and Winston, New York (1976)
27. Eves, H.: Great Moments in Mathematics (after 1650), *The Dolciani Mathematical Expositions*, vol. 7. Mathematical Association of America, Washington, DC (1981)
28. Feigelstock, S.: Comparing Sets. *Math. Mag.* **71**(3), 213–216 (1998)
29. Fletcher, C.R.: Fermat's theorem. *Historia Math.* **16**(2), 149–153 (1989)
30. Fletcher, C.R.: A reconstruction of the Frenicle–Fermat correspondence of 1640. *Historia Math.* **18**(4), 344–351 (1991)
31. Foreman, M., Kanamori, A. (eds.): *Handbook of Set Theory*. Springer, New York (2010). In 3 volumes
32. Gårding, L.: The Dirichlet problem. *Math. Intelligencer* **2**, 43–53 (1979)
33. Gessen, M.: *Perfect Rigor: A Genius + The Mathematical Breakthrough of the Century*. Houghton Mifflin Harcourt, Boston, MA (2009)
34. Gillman, L.: Two classical surprises concerning the axiom of choice and the continuum hypothesis. *Amer. Math. Monthly* **109**(6), 544–553 (2002)
35. Gorkin, P., Smith, J.H.: Dirichlet: his life, his principle, and his problem. *Math. Mag.* **78**(4), 283–296 (2005)
36. Grattan-Guinness, I.: A sideways look at Hilbert's twenty-three problems of 1900. *Notices Amer. Math. Soc.* **47**(7), 752–757 (2000)
37. Gray, J.J.: *The Hilbert Challenge*. Oxford University Press, Oxford (2000)
38. Greater Online Marketing, LLC: CalendarHome.com. <http://www.calendarhome.com/tycl/>. Cited 30 December 2010
39. Griffiths, P.A.: Mathematics at the turn of the millennium. *Amer. Math. Monthly* **107**(1), 1–14 (2000)
40. Halmos, P.: Postcards from Max. *Amer. Math. Monthly* **100**(10), 942–944 (1993)
41. Halmos, P.R.: *Naive Set Theory*. D. Van Nostrand Company, Princeton, NJ (1960)
42. Halmos, P.R.: How to write mathematics. *Enseign. Math.* (2) **16**, 123–152 (1970)
43. Halmos, P.R.: How to talk mathematics. *Notices Amer. Math. Soc.* **21**, 155–158 (1974)
44. Halmos, P.R.: *I Want to Be a Mathematician: An Automathography*. Springer-Verlag, New York (1985)
45. Hardy, G.H.: *A Mathematician's Apology*, canto edn. Cambridge University Press, London (1993). First published 1940
46. Hardy, G.H., Wright, E.M.: *An Introduction to the Theory of Numbers*, first edn. Clarendon, Oxford (1938)
47. Heath, T.L.: *The Thirteen Books of Euclid's Elements*, 3 volumes, second edn. Dover, New York (1956)
48. Herrlich, H.: Axiom of choice, *Lecture Notes in Mathematics*, vol. 1876. Springer-Verlag, Berlin (2006)
49. Heuser, H.: *Funktionalanalysis*. Mathematische Leitfäden. [Mathematical Textbooks]. B. G. Teubner, Stuttgart (1992)
50. Hilbert, D.: Mathematische Probleme. *Nachr. Königl. Ges. Wiss. Göttingen* pp. 253–297 (1900). Also in: *Archiv der Mathematik und Physik*, (3) 1 (1901), pp. 44–63 and 213–237
51. Hilbert, D.: Mathematical problems. *Bull. Amer. Math. Soc.* **8**, 437–479 (1902). Translated into English by Dr. Mary Winston Newson. Full English text at: <http://babbage.clarku.edu/~djoyce/hilbert/problems.html>. Cited 30 December 2010
52. Hilbert, D.: Über das Unendliche. *Math. Ann.* **95**(1), 161–190 (1926)

53. Høeg, P.: *Smilla's Sense of Snow*. Farrar, Straus and Giroux, New York (1993)
54. Horadam, A.F.: A generalized Fibonacci sequence. *Amer. Math. Monthly* **68**, 455–459 (1961)
55. Jarden, D.: Curiosa: A simple proof that a power of an irrational number to an irrational exponent may be rational. *Scripta Math.* **19**, 229 (1953)
56. Jones, J.P., Toporowski, S.: Irrational numbers. *Amer. Math. Monthly* **80**, 423–424 (1973)
57. Katz, V.: *A History of Mathematics: An Introduction*, second edn. Addison-Wesley, Reading, MA (1998)
58. Kleiner, I.: Evolution of the function concept: A brief survey. *College Math. J.* **20**, 282–300 (1989)
59. Kline, M.: *Mathematical Thought from Ancient to Modern Times*. Oxford University Press, New York (1972)
60. Knott, R.: Fibonacci numbers and the golden section. <http://www.mcs.surrey.ac.uk/Personal/R.Knott/Fibonacci/>. Cited 30 December 2010
61. Koblitz, N.: Cryptography. In: B. Enquist, W. Schmid (eds.) *Mathematics Unlimited—2001 and Beyond*, pp. 749–769. Springer-Verlag, Berlin (2001)
62. Krantz, S.G.: *A Primer of Mathematical Writing*. American Mathematical Society, Providence, RI (1997)
63. Lewin, J.: A simple proof of Zorn's lemma. *Amer. Math. Monthly* **98**(4), 353–354 (1991)
64. Luzin, N.: Function: Part I. *Amer. Math. Monthly* **105**, 59–67 (1998). Translated by Abe Shenitzer
65. Luzin, N.: Function: Part II. *Amer. Math. Monthly* **105**, 263–270 (1998). Translated by Abe Shenitzer
66. Mahoney, M.S.: *The Mathematical Career of Pierre de Fermat, 1601–1665*, second edn. Princeton University Press, Princeton, NJ (1994)
67. Malone, D.: *Dangerous Knowledge*. BBC, 2007. On DVD from Becauseyouthink.tv and online at <http://video.google.com/videoplay?docid=-5122859998068380459#> (Cited 30 December 2010)
68. McCarthy, J.E.: How to give a good colloquium. *Canadian Mathematical Society Notes* **31**(5), 3–4 (1999)
69. Mendelson, E.: *Introduction to Mathematical Logic*. Chapman & Hall, London (1997)
70. Mollin, R.A.: A brief history of factoring and primality testing B. C. (before computers). *Math. Mag.* **75**(1), 18–29 (2002)
71. Monna, A.F.: *Dirichlet's Principle—A Mathematical Comedy of Errors and Its Influence on the Development of Analysis*. Oosthoek, Scheltema and Holkema, Utrecht, the Netherlands (1975)
72. Montgomery, P.L., Selfridge, J.L.: Problem 10230. *Amer. Math. Monthly* **99**(6), 570 (1992)
73. Nahin, P.J.: *Dr. Euler's fabulous formula*. Princeton University Press, Princeton, NJ (2006). Cures many mathematical ills
74. Needham, T.: *Visual complex analysis*. The Clarendon Press Oxford University Press, New York (1997)
75. Nelsen, R.B.: *Proofs Without Words: Exercises in Visual Thinking*. Mathematical Association of America, Washington, DC (1993)
76. Nelsen, R.B.: *Proofs Without Words II: More Exercises in Visual Thinking*. Mathematical Association of America, Washington, DC (2000)
77. Niven, I.: A simple proof that π is irrational. *Bull. Amer. Math. Soc. (N.S.)* **53**, 509 (1947)
78. North Dakota State University: The Mathematics Genealogy Project. <http://genealogy.math.ndsu.nodak.edu/>. Cited 30 December 2010
79. O'Connor, J.J., Robertson, E.F.: The mactutor history of mathematics archive. School of Mathematics and Statistics, University of St. Andrews, Scotland. <http://www-history.mcs.st-andrews.ac.uk/index.html>. Cited 30 December 2010
80. Pascal, B.: Lettre au provincial, seizième lettre 1656. In: J. Chevalier (ed.) *Oeuvres complètes*. Éditions Gallimard, Paris (1954)
81. Pascal, B.: *Traité du triangle arithmétique*. In: J. Chevalier (ed.) *Oeuvres Complètes de Blaise Pascal*, Bibliothèque de la Pléiade, no. 34. Pléiade, Paris (1954)

82. Peterson, I.: Math trek: The counterfeit coin. Wake Forest University (1998). <http://www.maa.org/mathland/mathtrek%5F2%5F16%5F98.html>. Cited 30 December 2010
83. Poincaré, H.: L'avenir des mathématiques. *Bull. Sci. Math.* **32**, 168–90 (1908)
84. Pólya, G.: How to Solve It. Princeton University Press, Princeton, NJ (1945)
85. Pólya, G.: The Pólya Picture Album: Encounters of a Mathematician. Birkhäuser, Boston, MA (1987). Edited by G. L. Alexanderson
86. Reid, C.: Hilbert. Springer-Verlag, New York (1970)
87. von Renteln, M.: Friedrich Prym (1841–1915)—and his investigations on the Dirichlet problem. *Rend. Circ. Mat. Palermo* (2) Suppl. (44), 43–55 (1996)
88. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM* **21**, 120–126 (1978)
89. Rosen, K.H.: Elementary Number Theory and Its Applications, fifth edn. Addison-Wesley, Reading, MA (2005)
90. RSA Security, Inc.: Company website. <http://www.rsasecurity.com/>. Cited 30 December 2010
91. Rubin, H., Rubin, J.E.: Equivalents of the axiom of choice. II, *Studies in Logic and the Foundations of Mathematics*, vol. 116. North-Holland, Amsterdam (1985)
92. Rudin, W.: Principles of mathematical analysis, third edn. McGraw-Hill, New York (1976). International Series in Pure and Applied Mathematics
93. Ruskey, F., Savage, C.D., Wagon, S.: The search for simple symmetric Venn diagrams. *Notices Amer. Math. Soc.* **53**(11), 1304–1312 (2006)
94. Rüthing, D.: Some definitions of the concept of function from Joh. Bernoulli to N. Bourbaki. *Math. Intelligencer* **6**(4), 72–77 (1984)
95. Saff, E.B., Snider, A.D.: Fundamentals of Complex Analysis with Applications to Engineering, Science, and Mathematics, third edn. Prentice Hall, Englewood Cliffs, NJ (2003)
96. Schreiber, P.: The Cauchy-Bunyakovsky-Schwarz inequality. In: Hermann Graßmann (Lieschow, 1994), pp. 64–70. Ernst-Moritz-Arndt-Universität, Greifswald (1995)
97. Schumer, P.: The Josephus problem: Once more around. *Math. Mag.* **75**, 12–17 (2002)
98. Sigler, L.E.: The Book of Squares by Leonardo Pisano Fibonacci; An Annotated Translation into Modern English. Academic Press, Boston, MA (1987)
99. Singh, S.: The Code Book. Doubleday, New York (1999)
100. Smale, S.: Mathematical problems for the next century. *Math. Intelligencer* **20**(2), 7–15 (1998)
101. Smullyan, R.M.: What Is the Name of This Book?: The Riddle of Dracula and Other Logical Puzzles. Prentice-Hall, Englewood Cliffs, NJ (1978)
102. Steinhaus, H.: Mathematical Snapshots. Oxford University Press, New York (1950)
103. Stewart, I.: The truth about Venn diagrams. *Math. Gaz.* **60**(411), 47–54 (1976)
104. Su, F.E., et al.: Rational irrational power. *Math Fun Facts*, <http://www.math.hmc.edu/funfacts>. Cited 30 December 2010
105. Vowe, M.: Aufgabe 1155 (Die einfache (?) dritte Aufgabe). *Elem. Math.* **55**(1), 39 (2001)
106. Wanner, G.: Nachtrag zu Aufgabe 1155. *Elem. Math.* **56**(3), 133–134 (2001)
107. Weierstrass, K.: Über das sogenannte Dirichlet'sche Princip, gelesen in der Königl. Akademie der Wissenschaften am 14. Juli 1870. In: Karl Weierstrass, *Mathematische Werke*, vol. 2, pp. 49–54. Mayer & Müller, Berlin (1895)
108. Weil, A.: Number Theory. Birkhäuser, Boston, MA (1984)
109. Weyl, H.: Philosophie der Mathematik und Naturwissenschaft, 6 edn. R. Oldenbourg Verlag, München (1990)
110. Wieschenberg, A.A.: A conversation with George Pólya. *Math. Mag.* **60**(5), 265–268 (1987)
111. Wiles, A.: Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* (2) **141**(3), 443–551 (1995)
112. Williams, J.M.: Style: Toward Clarity and Grace. The University of Chicago Press, Chicago (1990)
113. Youschkevitch, A.P.: The concept of function up to the middle of the 19th century. *Arch. History Exact Sci.* **16**(1), 37–85 (1976/77)
114. Zorn, E.: A Math Wizard, Hero to His Family. *Math. Mag.* **66**(4), 277–278 (1993)

Index

- (X, d) , 276, 279
- (a, b) , 34, 92, 97
- (x_n) , 209, 214
- (x_{n_k}) , 229, 234
- $2\mathbb{Z}$, 60
- $2\mathbb{Z} + 1$, 60
- $3\mathbb{Z}$, 60
- $=$, 65
- A^c , 64, 65
- $B_d(x, r)$, 287, 293
- E^o , 293, 297
- E_I , 293, 297
- E_x , 103
- F_n , 215
- $P \leftrightarrow Q$, 16
- $P \rightarrow Q$, 15
- $P \vee Q$, 15
- $P \wedge Q$, 15
- $X \times Y$, 90, 93, 97
- $[a, b]$, 34
- $[m]_n$, 300
- \aleph_0 , 265
- \approx , 235, 236, 238
- $\bigcap_{A \in \mathcal{A}} A$, 82
- $\bigcup_{A \in \mathcal{A}} A$, 82
- $\binom{n}{k}$, 201, 207
- \cap , 64, 65
- \mathbb{C} , 34
- $\text{cod}(f)$, 143, 149
- \cup , 64, 65
- $\text{dom}(f)$, 143, 149
- \emptyset , 59, 65
- $\equiv \pmod{n}$, 299, 305
- \exists , 35
- \forall , 35
- gcd , 301, 306
- \in , 33, 63
- inf , 124, 127, 211
- $\text{inf}(x_n)$, 215
- lcm , 307
- $\lfloor x \rfloor$, 150, 155
- $\lim_{n \rightarrow \infty} x_n$, 223, 229
- $\liminf(x_n)$, 229
- $\limsup(x_n)$, 229
- $\mathcal{P}(S)$, 92
- $\max A$, 122, 126
- $\min A$, 122, 126
- $\neg P$, 14
- \mathbb{N} , 34
- \bar{E} , 293, 298
- ϕ , 313, 317
- $\mathcal{P}(S)$, 89
- \square , viii, 48
- \mathbb{Q} , 34
- \mathbb{Q}^+ , 34
- \mathbb{Q}^- , 34
- $\text{ran}(f)$, 147, 149
- \mathbb{R} , 34
- \mathbb{R}^+ , 34
- \mathbb{R}^- , 34
- \mathbb{R}^2 , 34
- \mathbb{R}^n , 34
- \setminus , 64, 65
- \sim , 101
- \subset , 61, 65
- \subseteq , 61, 63, 65
- sup , 123, 127, 212
- $\text{sup}(x_n)$, 215
- \triangle , 77
- \mathbb{Z} , 34
- \mathbb{Z}^+ , 34
- \mathbb{Z}^- , 34
- \mathbb{Z}_n , 299, 306
- $\#$, viii

- $a \mid b$, 47, 52, 299
- d , 276, 279
- d_b , 280, 283
- d_d , 276, 280
- d_m , 277, 280
- d_{rc} , 277, 280
- d_u , 276, 277, 280
- $f|_C$, 161, 162
- $f(A)$, 181, 185
- $f : A \rightarrow B$, 143
- f^{-1} , 168, 174
- $f^{-1}(B)$, 182, 185
- $g \circ f$, 167, 174
- i_A , 171, 174
- $n!$, 198, 201
- $x_n \rightarrow L$, 223, 229
- \square ix
- $|A|$, 244
- \bigcirc , viii

- absolute value, 49, 52
 - function, 146, 223
- Adleman, L. M., 318, 355
- algebraic number, 349
- antecedent, 15
- Archimedean property, 125
- associative property, 361
 - compound statement, 25
 - sets, 76
- asymmetric, 136, 138
- axiom, 124, 269
- axiom of choice, 258, 351, 363
- axiom of infinity, 331

- ball
 - open, 287, 293
 - unit, 287, 293
- barber problem, 67
- Bernoulli's inequality, 203
- Bernoulli, Johann, 152
- bijective, 157, 162
- binomial coefficient, 201, 207
- binomial theorem, 207
- birthday calendar, 311
- bounded sequence, 211, 214
 - above, 210, 214
 - below, 210, 214
- bounded set, 121, 126
 - above, 121, 126
 - below, 121, 126

- Caesar cipher, 7
- Cantor, G., 249, 254, 268, 349
 - diagonal argument, 253, 260
 - set, 344
 - theorem, 260
- Cantor–Schröder–Bernstein theorem, 261
 - proof of, 261–263, 271, 272
- cardinality, 244
 - $=$, 259, 261, 264, 265
 - \leq , 259, 265
 - of power sets, 260, 265
- Carroll, Lewis, 13, 56
- Cartesian product, 90, 93, 97
- Cauchy sequence, 229, 234
 - metric space, 285
- Cauchy–Bunyakovsky–Schwarz inequality, 347
- chain, 352
- characteristic function, 149, 153
- cipher, 2
- Clay Mathematics Institute, 50
- clock arithmetic, 299
- closed set, 290, 293
 - closed interval, 34
 - not closed, 296
 - unbounded interval, 34
- closure, 293, 298
- Cocks, C., 318
- code, 315, 355
- codomain, 143, 149
- collection, 59
 - indexed, 84
- commutative property, 361
 - compound statements, 25
 - sets, 76
- complement, 64, 65
- completeness axiom of \mathbb{R} , 125
 - infimum version, 125, 128
- complex numbers, 34, 336
- composite function, 167, 174
- composite number, 328
- composition, 167, 174
- conclusion, 15
- congruence modulo n , 299, 305
- conjecture, 50
- conjunction, 15
- connectives, 14
- contained, 61
- continuum, 265
- continuum hypothesis, 265, 268, 269
 - generalized, 273
- contradiction, 17
- contrapositive, 26, 39
- convergent sequence, 223, 229
 - metric space, 277, 280
 - proving convergence, 225
 - theorems, 228, 233

- converse, 27, 39
- convex set, 201, 206
 - \mathbb{R}^n , 348
- countable set, 249, 255
- countably infinite set, 249, 254
- counterexample, 51
- counterfeit coin problem, 10

- decreasing sequence, 212, 215
- Dedekind, R., 152, 268
- dedication, v
- DeMorgan's laws, 18, 75, 76, 84
- diagram of a relation, 103
- Diffie, W., 318, 355
- Dirichlet, P. G. L., 151, 242
 - drawer principle, 242
 - function, 151
 - pigeonhole principle, 241
 - principle, 187, 242
 - problem, 187
- discrete metric, 276, 280
- disjoint, 64
 - pairwise, 84, 88
- disjunction, 15
- distance, 223, 275
- distributive property, 361
 - compound statements, 25
 - sets, 73, 76, 87
- divergent sequence, 223, 227, 229
 - diverges to ∞ , 229, 234
 - metric space, 277, 280
- divides, 47, 52, 299
- division algorithm, 140, 300
- domain, 143, 149
- double negation, 18

- element, 59
- Ellis, J., 318
- empty set, 63
- equivalence class, 104
- equivalence of statements, 16
- equivalence relation, 101–104, 113
 - classes, 103, 104
- equivalent
 - statement, 17
 - statement forms, 17
- equivalent sets, 235, 238
- Euclid, 53
 - Elements*, 53, 302, 310, 330
- Euclidean n -space, 34
- Euclidean algorithm, 302, 310–311
- Euclidean metric, 276, 280
- Euler, L., 51, 151, 152, 313, 336
 - ϕ -function, 313, 317
- equation, 338
- formula, 337
- theorem, 314, 355

- factorial, 198, 201
- Fermat, P. de, 51, 313
 - last theorem, 50
 - little theorem, 313
- Fibonacci, 213
 - numbers, 214, 215, 233
 - sequence, 214, 215
- field, 362
 - ordered, 362
- Fields Medal, 50
- finite set, 236, 238
- floor function, 150, 155
- Fourier, J., 152
- Frénicle de Bessy, B., 313
- function, 143, 149, 150, 152
 - characteristic, 149, 153
 - defined in cases, 145
 - equality, 146
 - floor, 150, 155
 - greatest integer, 150, 155
 - indicator, 149, 153
 - notation, 144
 - preserves distance, 293, 297
 - step, 149, 154
 - strictly increasing, 191
 - well-defined, 143
- fundamental theorem of arithmetic, 206, 307

- Gödel's first incompleteness theorem, 269
- Gauss, C. F., 194
- GCHQ, 318
- Gelfond, A. O., 358
- Gelfond–Schneider theorem, 358
- geometric series, 334, 346
- geometric sum, 218
- golden ratio, 233
- greatest common divisor, 300, 306
- greatest integer, 150, 155
- greatest lower bound, 123, 127
 - sequence, 211, 215
- Green, G., 188

- Halmos, P. R., 97, 110
- Hardy, G. H., 48, 53, 334
- harmonic series, 204
- Heine, H. E., 152
- Hellman, M., 318, 355
- Hermite, C., 358
- Hilbert, D., 188, 235, 254, 259, 268, 357
- Hotel Infinity, 235

- identity, 361
- identity function, 171, 174
- image, 181, 185
 - theorems, 184
- implication, 15, 18
 - negation of, 18
- increasing sequence, 212, 215
- index set, 82, 84
- indexed collection, 156
- indexed set, 82, 84
- indexed sets, 156
- indicator function, 149, 153
- induction, 193, 208, 331
 - second principle, 206
- induction hypothesis, 194
- infimum, 123, 127, 187
 - sequence, 211, 215
 - uniqueness, 124, 130
- infinite set, 236, 238
- injective, 157, 162
- integer
 - even, 26, 28
 - odd, 26, 28
- integers, 34
 - divisible by 3, 60
 - even, 60
 - modulo n , 299, 306
 - negative, 34
 - odd, 60
 - positive, 34
- interior point, 293, 297
- intersection, 64, 82, 84
 - collection of sets, 84
 - finitely many sets, 81
 - indexed collection of sets, 83
 - infinitely many sets, 81
- intersection of the collection, 82, 84
- inverse, 168, 174, 361
 - composition, 172
 - uniqueness, 171
- inverse image, 182, 185
 - theorems, 184
- irrational number, 42, 332–336

- Josephus problem, 209

- Kronecker, L., 254

- Lacroix, S.-F., 152
- Lambert, J. H., 336
- least common multiple, 307
- least element, 352
- least upper bound, 122, 127
 - sequence, 212, 215

- lemma, 113
- lexicographical order, 339
- limit, 223, 229
 - inferior, 229, 234
 - superior, 229, 234
 - uniqueness, 227
- limit point, 293, 297
- Lindemann, F., 358
- linear combination, 301
- lower bound
 - sequence, 211, 214
 - set, 121, 126
- lower triangle inequality, 55
- Lucas sequence, 221

- map, 143
- max metric, 277, 280
- maximum, 122, 126
- member, 59
- Merkle, R., 318
- metric, 276, 279
 - bounded associated, 280, 283
 - definiteness, 276, 279
 - discrete, 276, 280
 - Euclidean, 276, 280
 - max, 277, 280
 - nonnegativity, 276, 279
 - symmetry, 276, 279
 - taxicab, 277, 280
 - triangle inequality, 276, 279
 - usual, 276, 280
- metric space, 276, 279
- minimum, 122, 126, 187
- Minkowski, H., 254
- monotone sequence, 229, 234

- natural numbers, 34
- negation, 14, 18, 19, 36–39
- Niven, I., 334, 336
- NSA, 318

- one-to-one, 157, 162
 - not one-to-one, 162
- onto, 157, 162
 - not onto, 161
- open set, 289, 293
 - ball, 287, 293
 - unit ball, 287, 293
 - not open, 289
 - open interval, 34
 - unbounded interval, 34
- order
 - partial, 136, 138, 260, 264
 - total, 136, 138, 260

- ordered pair, 90, 92, 97
- Pólya, G., 1, 8
 - the list, 1, 8, 364
- pairwise disjoint, 84, 88
- paradox, 67
- partial function, 353
- partial order, 136, 138
- partially ordered set, 139
- partition, 111, 113, 115
- Pascal, B., 98, 341
 - triangle, 342
- Peano axioms, 331
- Perelman, G., 50
- perfect number, 328–330
- pigeonhole principle, 241, 242
- Pisano, L., 213
- plaintext, 356
- plane, 34, 70
- Poincaré conjecture, 50
- Poincaré, H., 254
- polynomial, 108
 - degree, 108
 - root, 56
- power set, 89, 92, 260
- primality testing, 357
- prime number, 27, 28, 53, 307
- product notation, 196
- proof
 - contradiction, 47–49
 - direct, 47, 48
 - if and only if, 51, 52, 75
 - iff, 52
 - in cases, 47, 49–50, 73
 - reductio ad absurdum, 48
 - top down, bottom up, 61, 74
 - uniqueness, 122–123
 - working backwards, 147, 225, 278
- proper divisor, 328
- proper subset, 61
- Prym, F., 188
- public key encryption, 316
- Pythagorean theorem, 326
- quantifier
 - existential, 35
 - negation of, 36
 - universal, 35
- range, 147, 149
- rational numbers, 34, 332–334
 - closed under addition, 332
 - closed under multiplication, 332
 - negative, 34
 - positive, 34
- real numbers, 34
 - negative, 34
 - positive, 34, 362
- reciprocal modulo n , 305, 306
- recursion theorem, 198
- reflexive, 101, 104, 136, 138
- relation, 92, 93, 101
 - diagram of, 103
 - equivalence, 101, 104
 - from X to Y , 92, 93
 - on X , 92, 93
- relatively prime, 301, 306
- restriction, 161, 162
- Riemann, G. F. B., 188
- Rivest, R., 318, 355
- RSA-key, 355
- Russell, B., 67, 254
- Schneider, T., 358
- sequence, 209, 214
 - bounded, 211, 214
 - Cauchy, 229, 234
 - convergent, 223, 229
 - convergent in a metric space, 277, 280
 - decreasing, 212, 215
 - divergent, 223, 229
 - divergent in a metric space, 277, 280
 - eventually constant, 281
 - greatest lower bound, 211, 215
 - increasing, 212, 215
 - infimum, 211, 215
 - least upper bound, 212, 215
 - limit, 277, 280
 - lower bound, 211, 214
 - monotone, 229, 234
 - strictly decreasing, 212, 215
 - strictly increasing, 212, 215
 - subsequence, 229, 234
 - sum of, 212
 - supremum, 212, 215
 - term, 209, 214
 - upper bound, 211, 214
- set, 59
 - bounded, 121, 126, 280, 283
 - closure, 293, 298
 - complement, 64, 65
 - convex, 348
 - countable, 249, 255
 - countably infinite, 249, 254
 - difference, 64, 65
 - disjoint, 65
 - empty, 59, 63, 65
 - equality, 62, 65

- greatest lower bound, 123, 127
- inclusion, 73–75
- index, 84
- indexed, 82, 84
- infimum, 127
- interior, 293, 297
- interior point, 293, 297
- intersection, 64, 65
- least upper bound, 122, 127
- limit point, 293, 297
- lower bound, 121, 126
- notation, 33, 60
- partially ordered, 139
- supremum, 122, 127
- symmetric difference, 77
- uncountable, 249, 255, 260, 264
- union, 64, 65
- upper bound, 121, 126
- useful relations, 76
- set difference, 64
- Shamir, A., 318, 355
- Smale, S., 358
- Smilla's Sense of Snow*, 235
- statement, 13–21
- statement form, 14, 16
- step function, 149, 154
- strictly decreasing sequence, 212, 215
- strictly increasing sequence, 212, 215
- subsequence, 229, 234
- subset, 61, 65
 - proper subset, 61, 65
- successor, 330
- summation notation, 196
- supremum, 122, 127
 - sequence, 212, 215
 - uniqueness, 123
- surjective, 157, 162
- symmetric, 101, 104
- tautology, 17, 25–27
- taxicab metric, 277, 280
- term, 209, 214
- ternary expansion, 345
- Thomson, W., 188
- topology, 275
- total order, 136, 138, 353
- transcendental number, 349
- transitive, 68, 101, 104, 136, 138
- triangle inequality, 55, 275
 - \mathbb{R}^n , 347
 - metric spaces, 276, 279
- triangular numbers, 201, 207
- trichotomy principle, 362
- truth table, 14
- uncountable set, 249, 255
- union, 64, 82, 84
 - collection of sets, 84
 - finitely many sets, 81
 - indexed collection of sets, 82
 - infinitely many sets, 81
- union of the collection, 82, 84
- universe, 33
- upper bound
 - sequence, 211, 214
 - set, 121, 126
- usual metric, 276, 277, 280
- variables, 35
- Venn diagram, 64, 73
- vibrating string problem, 151
- Weierstrass, K. T. W., 188
- well-ordered set, 352
- well-ordering principle of \mathbb{N} , 125, 194, 208
- well-ordering theorem, 352
- Weyl, H., 152
- Wiles, A., 50
- Williamson, M., 318
- Wright, E. M., 334
- ZFC, 363
- Zorn's lemma, 352