Ethan D. Bloch

Proofs and Fundamentals

A First Course in Abstract Mathematics

Second Edition

Undergraduate Texts in Mathematics

Ethan D. Bloch

Proofs and Fundamentals

A First Course in Abstract Mathematics

Second Edition

Springer

Ethan D. Bloch
Mathematics Department
Bard College
Annandale-on-Hudson, NY 12504
USA
bloch@bard.edu

Printed on acid-free paper

Dedicated to my wife Nancy, in appreciation of her love and support

Contents

Part III   EXTRAS

Preface to the Second Edition

The changes from the first edition to the second have two sources: the many helpful suggestions the author has received from colleagues, reviewers, students and others who took the time and effort to contact me, and the author's experience teaching with this text in the years since the first edition was published.

Though the bulk of the text has remained unchanged from the first edition, there are a number of changes, large and small, that will hopefully improve the text. As always, any remaining problems are solely the fault of the author.

Changes from the First Edition to the Second Edition

(1) A new section about the foundations of set theory has been added at the end of Chapter 3, about sets. This section includes a very informal discussion of the Zermelo–Fraenkel Axioms for set theory. We do not make use of these axioms subsequently in the text, but it is valuable for any mathematician to be aware that an axiomatic basis for set theory exists. Also included in this new section is a slightly expanded discussion of the Axiom of Choice, and new discussion of Zorn's Lemma.

(2) Chapter 6, about the cardinality of sets, has been rearranged and expanded. There is a new section at the start of the chapter that summarizes various properties of the set of natural numbers; these properties play important roles subsequently in the chapter. The sections on induction and recursion have been slightly expanded, and have been relocated to an earlier place in the chapter (following the new section), both because they are more concrete than the material found in the other sections of the chapter, and because ideas from the sections on induction and recursion are used in the other sections. Next comes the section on the cardinality of sets (which was originally the first section of the chapter); this section gained proofs of the Schroeder–Bernstein theorem and the Trichotomy Law for Sets, and lost most of the material about finite and countable sets, which has now been moved to a new section devoted

to those two types of sets. The chapter concludes with the section on the cardinality of the number systems.

(3) The chapter on the construction of the natural numbers, integers and rational numbers from the Peano Postulates was removed entirely. That material was originally included to provide the needed background about the number systems, particularly for the discussion of the cardinality of sets in Chapter 6, but it was always somewhat out of place given the level and scope of this text. The background material needed for Chapter 6 has now been summarized in a new section at the start of that chapter, making the chapter both self-contained and more accessible than it previously was. The construction of the number systems from the Peano Postulates more properly belongs to a course in real analysis or in the foundations of mathematics; the curious reader may find this material in a variety of sources, for example [Blo11, Chapter 1].

(4) Section 3.4 on families of sets has been thoroughly revised, with the focus being on families of sets in general, not necessarily thought of as indexed.

(5) A new section about the convergence of sequences has been added to Chapter 7. This new section, which treats a topic from real analysis, adds some diversity to Chapter 7, which had hitherto contained selected topics of only an algebraic or combinatorial nature.

(6) A new section called "You Are the Professor" has been added to Chapter 8. This new section, which includes a number of attempted proofs taken from actual homework exercises submitted by students, offers the reader the opportunity to solidify her facility for writing proofs by critiquing these submissions as if she were the instructor for the course.

(7) The notation for images and inverse images of sets under a function, defined in Section 4.2, has been changed from the non-standard notation $f_*(P)$ and $f^*(Q)$ used in the first edition to the standard notation $f(P)$ and $f^{-1}(Q)$, respectively. Whereas the author still finds the notation used in the first edition superior in terms of avoiding confusion with inverse functions, he has deferred to requests from colleagues and reviewers to switch to the standard notation, with the hope that any confusion due to the standard notation will be outweighed by the benefit for students in preparing to read mathematical texts that use the standard notation.

(8) All known errors have been corrected.

(9) Many minor adjustments of wording have been made throughout the text, with the hope of improving the exposition.

Errors

Although all known errors from the first edition have been corrected, there are likely to be some remaining undetected errors, and, in spite of the author's best effort, there are likely to be some errors in the new sections and revisions of older material that were written for the second edition. If the reader finds any such errors—which will hopefully be few in number—it would be very helpful if you would send them to the author at bloch@bard.edu. An updated list of errors is available at http://math.bard.edu/bloch/proofs2_errata.pdf.

Acknowledgments

I would like to thank the following individuals for their extremely helpful comments and eagle-eyed spotting of errors: Joe Antao, Tilman Bauer, Jeff Boersema, Ryan Burt, Allen Butler, Peter de Keijzer, David Doster, Mark Halsey, Sam Hsiao, Greg Landweber, Robert McGrail, Mackay Merrill, Ethan Pribble, Lauren Rose, Rebecca Thomas, Oleg Yerokhin and Bard students Paulos Ashebir, Matthias Bahlke, Jordan Berkowitz, Anne Buchwald, Monica Elkinton, Emily Grumbling, Nabil Hossain, Mahmud Hussain, Scott McMillen, Nicholas Michaud, Supriya Munshaw, Dan Neville, Jacob Pooler, Serena Randolph, Benjamin Rin, Evan Sangaline, Evan Seitchik, Emily Shapiro, Georgi Smilyanov and Ezra Winston.

My appreciation goes to Ann Kostant, now retired Executive Editor of Mathematics/Physics at Birkhäuser, for her unceasing support of this book, and to Elizabeth Loew, Senior Editor of Mathematics at Springer-Verlag, for stepping in upon Ann's retirement and providing me with very helpful guidance. I would like to thank Sheldon Axler and Kenneth Ribet, the editors of Undergraduate Texts in Mathematics, for their many useful suggestions for improving the book. Thanks also go to Nathan Brothers and the copyediting and production staff at Springer-Verlag for their terrific work on the book; to Martin Stock for help with LaTeX; and to Pedro Quaresma for assistance with his very nice LaTeX commutative diagrams package DCpic, with which the commutative diagrams in this edition were composed.

I would very much like to thank the Einstein Institute of Mathematics at the Hebrew University of Jerusalem, and especially Professor Emanuel Farjoun, for their very kind hospitality during a sabbatical when this edition was drafted.

Lastly, I would like to thank my wonderful wife Nancy and my two amazing children Gil and Ada for their support during my work on this edition.

Ethan Bloch
Annandale-on-Hudson, NY
August 2010

Preface to the First Edition

In an effort to make advanced mathematics accessible to a wide variety of students, and to give even the most mathematically inclined students a solid basis upon which to build their continuing study of mathematics, there has been a tendency in recent years to introduce students to the formulation and writing of rigorous mathematical proofs, and to teach topics such as sets, functions, relations and countability, in a "transition" course, rather than in traditional courses such as linear algebra. A transition course functions as a bridge between computational courses such as calculus, and more theoretical courses such as linear algebra and abstract algebra.

This text contains core topics that the author believes any transition course should cover, as well as some optional material intended to give the instructor some flexibility in designing a course. The presentation is straightforward and focuses on the essentials, without being too elementary, too excessively pedagogical, and too full of distractions.

Some of the features of this text are the following:

(1) Symbolic logic and the use of logical notation are kept to a minimum. We discuss only what is absolutely necessary—as is the case in most advanced mathematics courses that are not focused on logic per se.

(2) We distinguish between truly general techniques (for example, direct proof and proof by contradiction) and specialized techniques, such as mathematical induction, which are particular mathematical tools rather than general proof techniques.

(3) We avoid an overemphasis on "fun" topics such as number theory, combinatorics or computer science-related topics, because they are not as central as a thorough treatment of sets, functions and relations for core mathematics courses such as linear algebra, abstract algebra and real analysis. Even the two sections on combinatorics in Chapter 7 were written with a focus on reinforcing the use of sets, functions and relations, rather than emphasizing clever counting arguments.

(4) The material is presented in the way that mathematicians actually use it rather than in the most axiomatically direct way. For example, a function is a special type of a relation, and from a strictly axiomatic point of view, it would make sense to treat relations first, and then develop functions as a special case of relations. Most mathematicians do not think of functions in this way (except perhaps for some combinatorialists), and we cover functions before relations, offering clearer treatments of each topic.

(5) A section devoted to the proper writing of mathematics has been included, to help remind students and instructors of the importance of good writing.

Outline of the text

The book is divided into three parts: Proofs, Fundamentals and Extras. At the end of the book is a brief Appendix summarizing a few basic properties of the real numbers, an index and a bibliography. The core material in this text, which should be included in any course, consists of Parts I and II (Chapters 1–6). A one-semester course can comfortably include all the core material, together with a small amount of material from Part III, chosen according to the taste of the instructor.

Part I, Proofs, consists of Chapters 1 and 2, covering informal logic and proof techniques, respectively. These two chapters discuss the "how" of modern mathematics, that is, the methodology of rigorous proofs as is currently practiced by mathematicians. Chapter 1 is a precursor to rigorous proofs, and is not about mathematical proofs per se. The exercises in this chapter are all informal, in contrast to the rest of the book. Chapter 2, while including some real proofs, also has a good bit of informal discussion.

Part II, Fundamentals, consists of Chapters 3–6, covering sets, functions, relations and cardinality, respectively. This material is basic to all of modern mathematics. In contrast to Part I, this material is written in a more straightforward definition/theorem/proof style, as is found in most contemporary advanced mathematics texts.

Part III, Extras, consists of Chapters 7 and 8, and has brief treatments of a variety of topics, including groups, homomorphisms, partially ordered sets, lattices, combinatorics and sequences, and concludes with additional topics for exploration by the reader, as well as a collection of attempted proofs (actually submitted by students) which the reader should critique as if she were the professor.

Some instructors might choose to skip Section 4.5 and Section 6.4, the former because it is very abstract, and the latter because it is viewed as not necessary. Though skipping either or both of these two sections is certainly plausible, instructors are urged to consider not to do so. Section 4.5 is intended to help students prepare for dealing with sets of linear maps in linear algebra, and comparable constructions in other branches of mathematics. Section 6.4 is a topic that is often skipped over in the mathematical education of many undergraduates, and that is unfortunate, because

it prevents the all too common (though incorrect) attempt to define sequences "by induction."

Acknowledgments

As with many texts in mathematics, this book developed out of lecture notes, first used at Bard College in the spring of 1997. The first draft of this text made partial use of class notes taken by Bard students Todd Krause, Eloise Michael and Jesse Ross in Math 231 in the spring of 1995.

Thanks go to the following individuals for their valuable assistance, and extremely helpful comments on various drafts: Robert Cutler, Peter Dolan, Richard Goldstone, Mark Halsey, Leon Harkleroad, Robert Martin, Robert McGrail and Lauren Rose. Bard students Leah Bielski, AmyCara Brosnan, Sean Callanan, Emilie Courage, Urska Dolinsek, Lisa Downward, Brian Duran, Jocelyn Fouré, Jane Gilvin, Shankar Gopalakrishnan, Maren Holmen, Baseeruddin Khan, Emmanuel Kypraios, Jurvis LaSalle, Dareth McKenna, Daniel Newsome, Luke Nickerson, Brianna Norton, Sarah Shapiro, Jaren Smith, Matthew Turgeon, D. Zach Watkinson and Xiaoyu Zhang found many errors in various drafts, and provided useful suggestions for improvements.

My appreciation goes to Ann Kostant, Executive Editor of Mathematics/Physics at Birkhäuser, for her unflagging support and continual good advice, for the second time around; thanks also to Elizabeth Loew, Tom Grasso, Amy Hendrickson and Martin Stock, and to the unnamed reviewers, who read through the manuscript with eagle eyes. Thanks to the Mathematics Department at the University of Pennsylvania, for hosting me during a sabbatical when parts of this book were written. The commutative diagrams in this text were composed using Paul Taylor's commutative diagrams package.

It is impossible to acknowledge every source for every idea, theorem or exercise in this text. Most of the results, and many of the exercises, are standard; some of these I first encountered as a student, others I learned from a variety of sources. The following are texts that I consulted regularly. Texts that are similar to this one: [Ave90], [FR90], [FP92], [Ger96], [Mor87]; texts on logic: [Cop68], [KMM80]; texts on set theory: [Dev93], [Vau95]; texts on combinatorics: [Bog90], [Epp90], [GKP94], [Rob84]; texts on abstract algebra: [Blo87], [Dea66], [Fra03], [GG88]; texts on posets and lattices: [Bir48], [Bog90], [CD73], [LP98]; text on writing mathematics: [KLR89].

Like many mathematicians, I am the product of my education. I would like to express my appreciation for my mathematics professors at Reed College 1974–1978: Burrowes Hunt, John Leadley, Ray Mayer, Rao Potluri, Joe Roberts and Thomas Weiting. It was they who first instilled in me many of the ideas and attitudes seen throughout this book. In particular, I have been decidedly influenced by the lecture notes of John Leadley for Math 113 (The Real Numbers) and Math 331 (Linear Algebra).

Finally, I wish to thank my mother-in-law Edith Messer, for many visits during which she took our newborn son Gil for hours at a stretch, allowing me bits of time for writing between diaper changes; and, especially, my wife Nancy Messer for her support and encouragement during the time when this book was written.

To the Student

This book is designed to bridge the large conceptual gap between computational courses such as calculus, usually taken by first- and second-year college students, and more theoretical courses such as linear algebra, abstract algebra and real analysis, which feature rigorous definitions and proofs of a type not usually found in calculus and lower-level courses. The material in this text was chosen because it is, in the author's experience, what students need to be ready for advanced mathematics courses. The material is also worth studying in its own right, by anyone who wishes to get a feel for how contemporary mathematicians do mathematics.

Though we emphasize proofs in this book, serious mathematics is—contrary to a popular misconception—not "about" proofs and logic any more than serious literature is "about" grammar, or music is "about" notes. Mathematics is the study of some fascinating ideas and insights concerning such topics as numbers, geometry, counting and the like. Ultimately, intuition and imagination are as valuable in mathematics as rigor. Both mathematical intuition and facility with writing proofs can be developed with practice, just as artists and musicians develop their creative skills through training and practice.

Mathematicians construct valid proofs to verify that their intuitive ideas are correct. How can you be sure, for example, that the famous Pythagorean Theorem is true? There are infinitely many possible triangles, so no one can check whether the Pythagorean Theorem holds for all triangles by checking each possible triangle directly. As you learn more abstract mathematical subjects, it will be even harder to be sure whether certain ideas that seem right intuitively are indeed correct. Hence we need to adhere to accepted standards of rigor.

There are two foci in this text: proofs and fundamentals. Just as writing a novel ultimately relies upon the imagination, but needs a good command of grammar, as well as an understanding of the basics of fiction such as plot and character, so too for mathematics. Our "grammar" is logic and proof techniques; our "basics" are sets, functions, relations and so on. You will have to add your own imagination to the mix.

Prerequisites

A course that uses this text would generally have as a prerequisite a standard calculus sequence, or at least one solid semester of calculus. In fact, the calculus prerequisite is used only to insure a certain level of "mathematical maturity," which means sufficient experience—and comfort — with mathematics and mathematical thinking. Calculus per se is not used in this text (other than an occasional reference to it in the exercises); neither is there much of pre-calculus. We do use standard facts about numbers (the natural numbers, the integers, the rational numbers and the real numbers) with which the reader is certainly familiar. See the Appendix for a brief list of some of the standard properties of real numbers that we use. On a few occasions we will give an example with matrices, though such examples can easily be skipped.

Exercises

Similarly to music and art, mathematics is learned by doing, not just by reading texts and listening to lectures. Doing the exercises in this text is the best way to get a feel for the material, to see what you understand, and to identify what needs further study. Exercises range from routine examples to rather tricky proofs. The exercises have been arranged in order so that in the course of working on an exercise, you may use any previous theorem or exercise (whether or not you did it), but not any subsequent result (unless stated otherwise). Some exercises are used in the text, and are so labeled.

Writing Mathematics

It is impossible to separate rigor in mathematics from the proper writing of proofs. Proper writing is necessary to maintain the logical flow of an argument, to keep quantifiers straight, and more. The reader would surely not turn in a literature paper written without proper grammar, punctuation and literary usage, and no such paper would be accepted by a serious instructor of literature. Please approach mathematics with the same attitude. (Proper writing of mathematics may not have been emphasized in your previous mathematics courses, but as you now start learning advanced mathematics, you may have to adjust your approach to doing mathematics.)

In particular, mathematicians write formal proofs in proper English (or whatever language they speak), with complete sentences and correct grammar. Even mathematical symbols are included in sentences. Two-column proofs, of the type used in some high school geometry classes, are not used in advanced mathematics (except for certain aspects of logic). So, beginning with Chapter 2, you should forget two-column proofs, and stick to proper English. In Chapter 1 we will be doing preparatory work, so we will be less concerned with proper writing there.

Mathematical Notation and Terminology

Just as mathematics is not "about" proofs and logic (as mentioned above), so too mathematics is not "about" obscure terminology and symbols. Mathematical terminology and symbols (such as Greek letters) are simply shorthand for otherwise cumbersome expressions. For example, it is much easier to solve the equation $3x + 5 = 7 - 6x$ written in symbols than it is to solve the equation given by the phrase "the sum of three times an unknown number and the number five equals the difference between the number seven and six times the unknown number." If we wrote out all of mathematics without symbols or specialized terminology, we would drown in a sea of words, and we would be distracted from the essential mathematical ideas. On the other hand, whereas the use of mathematical symbols is of great convenience, it is important to keep in mind at all times that mathematics is not the mere manipulation of symbols—every symbol means something, and it is that meaning in which we are ultimately interested.

There is no central authority that determines mathematical notation, and variations exist in the literature for the notation for some fundamental mathematical concepts; in this text we have adopted the most commonly used notation as much as possible. It should be noted that mathematical notation has evolved over time, and care is needed when studying older books and papers.

To help with readability, we have added a few symbols that are analogs of the very useful (and widely used) end-of-proof symbol, which is □. This symbol lets the reader know when a proof is done, signaling that the end is in sight, and allowing a proof to be skipped upon first reading. Mathematics texts are rarely read straight from beginning to end, but are gone over back and forth in whatever path the reader finds most helpful. In this book we decided to take a good thing and make it better, adding the symbol △ for the end of a definition, the symbol ◇ for the end of an example, and the symbol /// for the end of scratch work or other non-proofs. The point of all these symbols is to separate formal mathematical writing, namely, proofs, definitions and the like, from the informal discussion between the formal writing.

An important point to note concerning mathematical terminology is that whereas some names are invented specifically for mathematical use (for example the word "injective"), other mathematical terms are borrowed from colloquial English. For example, the words "group," "orbit" and "relation" all have technical meanings in mathematics. It is important to keep in mind, however, that the mathematical usage of these words is not the same as their colloquial usage. Even the seemingly simple word "or" has a different mathematical meaning than it does colloquially.

What This Text Is Not

Mathematics as an intellectual endeavor has an interesting history, starting in such ancient civilizations such as Egypt, Greece, Babylonia, India and China, progressing through the Middle Ages (especially in the non-Western world), and accelerating up until the present time. The greatest mathematicians of all time, such as Archimedes,

Newton and Gauss, have had no less of an impact on human civilization than their non-mathematical counterparts such as Plato, Buddha, Shakespeare and Beethoven. Unbeknownst to many non-mathematicians, mathematical research is thriving today, with more active mathematicians and more published papers than in any previous era. For lack of space, we will not be discussing the fascinating history of mathematics in this text. See [Boy91], [Str87] or [Ang94] for a treatment of the history of mathematics.

The study of mathematics raises some very important philosophical questions. Do mathematical objects exist? Do we discover mathematics or invent it? Is mathematics universal, or a product of specific cultures? What assumptions about logic (for example, the Law of the Excluded Middle) should we make? Should set theory form the basis of mathematics, as is standard at present? We will not be discussing these, and other, philosophical questions in this text, not because they are not important, but because it would be a diversion from our goal of treating certain fundamental mathematical topics. Mathematicians tend, with some exceptions, to be only minimally reflective about the philosophical underpinnings of their mathematical activity; for better or worse, this book shares that approach. There is so much interesting mathematics to do that most mathematicians—who do mathematics for the joy of it—would rather spend their time doing mathematics than worrying about philosophical questions.

The majority of mathematicians are fundamentally closet Platonists, who view mathematical objects as existing in some idealized sense, similar to Platonic forms. Our job, as we view it, is to discover what we can about these mathematical objects, and we are happy to use whatever valid tools we can, including philosophically controversial notions such as the Law of the Excluded Middle (see Section 1.2 for further discussion). Philosophers of mathematics, and those mathematicians prone to philosophizing, can be somewhat frustrated by the unwillingness of most mathematicians to deviate from the standard ways in which mathematics is done; most mathematicians, seeing how well mathematics works, and how many interesting things can be proved, see no reason to abandon a ship that appears (perhaps deceptively) to be very sturdy. In this text we take the mainstream approach, and we do mathematics as it is commonly practiced today (though we mention a few places where other approaches might be taken). For further discussion of philosophical issues related to mathematics, a good place to start is [DHM95] or [Her97]; see also [GG94, Section 5.9]. For a succinct and entertaining critique of the standard approach to doing mathematics as described in texts such as the present one, see [Pou99].

To the Instructor

There is an opposing set of pedagogical imperatives when teaching a transition course of the kind for which this text is designed: On the one hand, students often need assistance making the transition from computational mathematics to abstract mathematics, and as such it is important not to jump straight into water that is too deep. On the other hand, the only way to learn to write rigorous proofs is to write rigorous proofs; shielding students from rigor of the type mathematicians use will only ensure that they will not learn how to do mathematics properly.

To resolve this tension, a transition course should simultaneously maintain high standards in content, rigor and in writing, both by the instructor and by the students, while also giving the students a lot of individual attention and feedback. Watering down the core content of a transition course, choosing "fun" topics instead of central ones, making the material easier than it really is, or spending too much time on clever pedagogical devices instead of core mathematics, will allow students to have an easier time passing the course, but will result in students who are not ready to take more advanced mathematics courses—which is the whole point of the transition course.

When teaching students to write proofs, there is no substitute for regularly assigned homework problems, and for regular, and detailed, feedback on the homework assignments. Students can learn from their mistakes only if the mistakes are pointed out, and if better approaches are suggested. Having students present their proofs to the class is an additional forum for helpful feedback.

Most mathematicians of the author's generation never had a transition course, and simply picked up the techniques of writing proofs, and the basics of such fundamental topics as sets and functions, while they were taking courses such as linear algebra and abstract algebra. However, what worked for those who went on to become professors of mathematics does not always work for all students, and extra effort is needed to guide students until the basic idea of what constitutes a proof has sunk in. Hence, a dedicated focus on the formulation and writing of proofs, attention to the details of student work, and supportive guidance during this learning process are all very helpful to students as they make the transition to advanced mathematics.

One place where too much indulgence is given, however, even in more advanced mathematics courses, and where such indulgence is, the author believes, quite misguided, involves the proper and careful *writing* of proofs. Seasoned mathematicians make honest mathematical errors all the time (as we should point out to our students), and we should certainly understand such errors by our students. By contrast, there is simply no excuse for sloppiness in writing proofs, whether the sloppiness is physical (hastily written first drafts of proofs handed in rather than neatly written final drafts) or in the writing style (incorrect grammar, undefined symbols, etc.). Physical sloppiness is often a sign of either laziness or disrespect, and sloppiness in writing style is often a mask for sloppy thinking.

The elements of writing mathematics are discussed in detail in Section 2.6. It is suggested that these notions be used in any course taught with this book (though of course it is possible to teach the material in this text without paying attention to proper writing). The author has heard the argument that students in an introductory course are simply not ready for an emphasis on the proper writing of mathematics, but his experience teaching says otherwise: not only are students ready and able to write carefully no matter what their mathematical sophistication, but they gain much from the experience because careful writing helps enforce careful thinking. Of course, students will only learn to write carefully if their instructor stresses the importance of writing by word and example, and if their homework assignments and tests include comments on writing as well as mathematical substance.

Part I
PROOFS

Mathematics, like other human endeavors, has both a "what" and a "how." The "what" is the subject matter of mathematics, ranging from numbers to geometry to calculus and beyond. The "how" depends upon who is doing the mathematics. At the elementary school level, we deal with everything very concretely. At the high school level, when we learn algebra and geometry, things get more abstract. We prove some things, for example in geometry, and do others computationally, for example algebra. To a mathematician, by contrast, there is no split between how we do algebra and how we do geometry: everything is developed axiomatically, and all facts are proved rigorously. The methodology of rigorous proofs done the contemporary way—quite different from the two-column proofs sometimes used in high school geometry—is the "how" of mathematics, and is the subject of this part of the text. In Chapter 1 we give a brief treatment of informal logic, the minimum needed to construct sound proofs. This chapter is much more informal than the rest of the book, and should not be taken as a sign of things to come. In Chapter 2 we discuss mathematical proofs, and the various approaches to constructing them. Both of these chapters have a good bit of informal discussion, in contrast to some later parts of the book.

1

Informal Logic

Logic is the hygiene the mathematician practices to keep his ideas healthy and strong.

– Hermann Weyl (1885–1955)

1.1 Introduction

Logic is the framework upon which rigorous proofs are built. Without some basic logical concepts, which we will study in this chapter, it would not be possible to structure proofs properly. It will suffice for our purposes to approach these logical concepts informally (and briefly). Though logic is the foundation of mathematical reasoning, it is important not to overemphasize the use of formal logic in mathematics. Outside of the field of mathematical logic, proofs in mathematics almost never involve formal logic, nor do they generally involve logical symbols (although we will need such symbols in the present chapter).

Logic is an ancient subject, going back in the West to thinkers such as Aristotle, as well as to ancient non-Western thinkers. Having originated as an analysis of valid argumentation, logic is strongly linked to philosophy. Mathematicians have developed a mathematical approach to logic, although there is no rigid boundary between the study of logic by mathematicians and by philosophers; indeed, some logicians have excelled in both fields. Some aspects of logic have taken on new importance in recent years with the advent of computers, because logical ideas are at the basis of some aspects of computer science. For more about traditional logic, see [Cop68], which is very readable, and [KMM80], which is more formal. For mathematical logic, see [End72], [Mal79] or [EFT94]. See the introduction to Chapter 1 of the last of these books for a discussion of the relation of mathematical logic to traditional logic. For an interesting discussion of logic, see [EC89, Chapters 19 and 20]. For a treatment of logic in the context of computer science, see [DSW94, Part 3].

Although the informal logic we discuss in this chapter provides the underpinning for rigorous proofs, informal logic is not in itself rigorous. Hence the present chapter is substantially different from the rest of the book in that it is entirely informal.

Because we start discussing mathematical proofs only in the next chapter, for now our discussion is not written in the style appropriate for rigorous proofs. The same goes for the homework exercises in this chapter.

In this chapter, and throughout this text, we will use the basic properties of the integers, rational numbers and real numbers in some of our examples. We will assume that the reader is informally familiar with these numbers. The basic properties of the natural numbers will be discussed briefly in Section 6.2. See the Appendix for a brief list of some of the standard properties of real numbers; see [Blo11, Chapters 1 and 2] for a detailed treatment of the standard number systems.

The aspect of mathematics we are learning about in this text is to state results, such as theorems, and then prove them. Of course, a great deal of intuition, informal exploration, calculation and grunt work goes into figuring out what to try to prove, but that is another matter. Logic, at its most basic, is concerned with the construction of well-formed statements and valid arguments; these two notions will form the logical framework for the proper stating and proving of theorems. The actual mathematics of doing proofs will have to wait until Chapter 2.

1.2 Statements

When we prove theorems in mathematics, we are demonstrating the truth of certain statements. We therefore need to start our discussion of logic with a look at statements, and at how we recognize certain statements as true or false. A **statement** is anything we can say, write or otherwise express that is either true or false. For example, the expression "Fred Smith is twenty years old" is a statement, because it is either true or false. We might not know whether this statement is actually true or not, because to know that would require that we know some information about Fred Smith, for example his date of birth, and that information might not be available to us. For something to be a statement, it has to be either true or false in principle; it does not matter whether we personally can verify its truth or falsity. By contrast, the expression "Eat a pineapple" is not a statement, because it cannot be said to be either true or false.

It is important to distinguish between English expressions that we might say, and the statements they make. For example, when we wrote "Fred Smith is twenty years old," we could just as well have written "Fred Smith's age is twenty." These two English expressions are not identical because they do not have the exact same words, but they certainly make the same statement. For the sake of convenience, we will refer to expressions such as "'Fred Smith is twenty years old" as statements, though we should realize that we are really referring to the statement that the expression is making. In practice, there should not be any confusion on this point.

We will be making two assumptions when dealing with statements: every statement is either true or false, and no statement is both true and false. The first of these assumptions, often referred to as the Law of the Excluded Middle (and known formally as bivalence), may seem innocuous enough, but in fact some mathematicians have chosen to work without this powerful axiom. The majority of mathematicians

do use the Law of the Excluded Middle (the author of this book among them), and we will not hesitate to use it implicitly throughout this book. One of the consequences of this law is that if a statement is not false, then it must be true. Hence, to prove that something is true, it would suffice to prove that it is not false; this strategy is very useful in some proofs. Mathematicians who do not accept the Law of the Excluded Middle would not consider as valid any proof that uses the law (though the incorrectness of a proof does not necessitate the falsity of the statement being proved, only that another proof has to be sought). See [Wil65, Chapter 10] or [Cop68, Section 8.7] for more discussion of these issues.

If the only thing we could do with statements is to decide whether something is a statement or not, the whole concept would be fairly uninteresting. What makes statements more valuable for our purposes is that there are a number of useful ways of forming new statements out of old ones. An analog to this would be the ways we have of combining numbers to get new ones, such as addition and multiplication; if we did not have these operations, then numbers would not be very interesting. In this section we will discuss five ways of forming new statements out of old ones, corresponding to the English expressions: and; or; not; if, then; if and only if. The statements out of which we form a new one will at times be referred to as the component statements of the new statement.

For our definitions of these five constructions, we let P and Q be statements.

Our first construction, the **conjunction** of P and Q, which is denoted $P \wedge Q$, is the statement that, intuitively, is true if both P and Q are true, and is false otherwise. We read $P \wedge Q$ as "P and Q." The precise definition of $P \wedge Q$ is given by the "truth table"

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

This truth table, and all others like it, shows whether the new statement (in this case $P \wedge Q$) is true or false for each possible combination of the truth or falsity of each of P and Q.

As an example of conjunction, let $P =$ "it is raining today," and let $Q =$ "it is cold today." The statement $P \wedge Q$ would formally be "it is raining today and it is cold today." Of course, we could express the same idea more succinctly in English by saying "it is raining and cold today." In general, we will try to use statements that read well in English, as well as being logically correct.

The colloquial use of the word "and" differs from the mathematical usage stated above. The mathematical usage means the above truth table, and nothing else, while colloquially there are other meanings in addition to this one. One source of confusion involving the word "and" that is well worth avoiding is the colloquial use of this word in the sense of "therefore." For example, it is not uncommon to find a sentence such as "From the previous equation we see that $3x < 6$, and $x < 2$." What is really meant by this sentence is "From the previous equation we see that $3x < 6$, which implies that $x < 2$." Such a use of "and" to mean "therefore" is virtually never necessary, and

because it can lead to possible confusion, it is best avoided. It would be fine to say
"From the previous equation we see that $3x < 6$, and $x < 2$," because in that case the
"and" is functioning only as the conjunction between the two parts of the sentence,
and is not a substitute for the word "therefore."

Another colloquial use of "and" that differs from mathematical usage, though
one that is less likely to cause us problems here, is seen in the statement "Fred and
Susan are married." Interpreted in the strict mathematical sense, we could only con-
clude from this statement that each of Fred and Susan is married, possibly to different
people. In colloquial usage, by contrast, this statement would almost always be inter-
preted as meaning that Fred and Susan are married to each other. In literary writing,
some measure of ambiguity, or some implied meaning that is not stated explicitly, is
often valuable. In mathematics, on the other hand, precision is key, and ambiguity is
to be avoided at all costs. When using a mathematical term, always stick to the pre-
cise mathematical definition, regardless of any other colloquial usage. For example,
in mathematical writing, if we wanted to indicate that Fred and Susan are married
to each other, we should state explicitly "Fred and Susan are married to each other,"
and if we want to state only that each of Fred and Susan is married, we should say
"Fred is married and Susan is married."

Our second construction, the **disjunction** of P and Q, which is denoted $P \vee Q$, is
the statement that, intuitively, is true if either P is true or Q is true or both are true,
and is false otherwise. We read $P \vee Q$ as "P or Q." The precise definition of $P \vee Q$ is
given by the truth table

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

.

The truth of the statement $P \vee Q$ means that at least one of P or Q is true. Though
we write $P \vee Q$ in English as "P or Q," it is very important to distinguish the mathe-
matical use of the word "or" from the colloquial use of the word. The mathematical
use of the word "or" always means an inclusive "or," so that if "P or Q" is true, then
either P is true, or Q is true, or both P and Q are true. By contrast, the colloquial
use of the word "or" often means an exclusive "or," which does not allow for both P
and Q to be true. In this text, as in all mathematical works, we will always mean an
inclusive "or," as given in the truth table above.

A simple example of a disjunction is the statement "my car is red or it will rain
today." This statement has the form $P \vee Q$, where $P =$ "my car is red," and $Q =$ "it
will rain today." The truth of this statement implies that at least one of the statements
"my car is red" or "it will rain today" is true. The only thing not allowed is that both
"my car is red" and "it will rain today" are false.

Now consider the statement "tonight I will see a play or I will see a movie." In
colloquial usage it would be common to interpret this statement as an exclusive or,
meaning that either I will see a play, or I will see a movie, but not both. In colloquial
usage, if I wanted to include the possibility that I might see both a play and a movie, I

would likely say "tonight I will see a play, or I will see a movie, or both." By contrast, in mathematical usage the statement "tonight I will see a play or I will see a movie" would always be interpreted as meaning that either I will see a play, or I will see a movie, or both. In mathematical usage, if I wanted to exclude the possibility that I might see both a play and a movie, I would say "tonight I will see a play or I will see a movie, but not both."

One other source of confusion involving the word "or" that is well worth avoiding is the colloquial use of this word in the sense of "that is." Consider the colloquial sentence "when I was in France I enjoyed eating the local fromage, or, cheese." What is really meant is "when I was in France, I enjoyed eating the local fromage, that is, cheese." Such a use of "or" is best avoided in mathematical writing, because it is virtually never necessary, and can lead to confusion.

Our third construction, the **negation** of P, which is denoted $\neg P$, is the statement that, intuitively, is true if P is false, and is false if P is true. We read $\neg P$ as "not P." The precise definition of $\neg P$ is given in the truth table

$$\begin{array}{c|c} P & \neg P \\ \hline T & F \\ F & T \end{array}$$.

Let $P =$ "Susan likes mushy bananas." It would not work in English to write $\neg P$ as "Not Susan likes mushy bananas," both because that is not proper English, and because it appears as if the subject of the sentence is someone named "Not Susan." The most straightforward way of negating P is to write $\neg P =$ "it is not the case that Susan likes mushy bananas." While formally correct, this last statement is quite awkward to read, and it is preferable to replace it with an easier-to-read expression, for example "Susan does not like mushy bananas."

Our final two ways of combining statements, both of which are connected to the idea of logical implication, are slightly more subtle than what we have seen so far. Consider the statement "If Fred goes on vacation, he will read a book." What would it mean to say that this statement is true? It would not mean that Fred is going on vacation, nor would it mean that Fred will read a book. The truth of this statement means only that if one thing happens (namely, Fred goes on vacation), then another thing will happen (namely, Fred reads a book). In other words, the one way in which this statement would be false would be if Fred goes on vacation, but does not read a book. The truth of this statement would not say anything about whether Fred will or will not go on vacation, nor would it say anything about what will happen if Fred does not go on vacation. In particular, if Fred did not go on vacation, then it would not contradict this statement if Fred read a book nonetheless.

Now consider the statement "If grass is green, then Paris is in France." Is this statement true? In colloquial usage, this statement would seem strange, because there does not seem any inherent connection, not to mention causality, between the first part of the sentence and the second. In mathematical usage, however, we want to be able to decide whether a statement of any form is true simply by knowing the truth or falsity of each of its component statements, without having to assess something more vague such as causality. For example, the statement "Cows make milk and cars make

noise" is certainly true, even though the two parts of the sentence are not inherently connected. Similarly, the statement "If grass is green, then Paris is in France" also ought to be decidable as true or false depending only upon whether "grass is green" and "Paris is in France" are each true or false. As in the previous paragraph, we take the approach that a statement of the form "if P then Q" should be true if it is not the case that P is true and Q is false. Therefore, because grass is indeed green and Paris is indeed in France, the statement "If grass is green, then Paris is in France" is true. This approach to the notion of "if … then …" is somewhat different from the colloquial use of the term, just as our uses of "and" and "or" were not the same as their colloquial uses. We formalize this approach as follows.

Our fourth construction, the **conditional** from P to Q, which is denoted $P \to Q$, is the statement that, intuitively, is true if it is never the case that P is true and Q is false. We read $P \to Q$ as "if P then Q." The precise definition of $P \to Q$ is given in the truth table

$$
\begin{array}{cc|c}
P & Q & P \to Q \\
\hline
T & T & T \\
T & F & F \\
F & T & T \\
F & F & T
\end{array}
$$
.

The first two rows of the truth table are fairly reasonable intuitively. If P is true and Q is true, then certainly $P \to Q$ should be true; if P is true and Q is false, then $P \to Q$ should be false. The third and fourth rows of the truth table, which say that the statement $P \to Q$ is true whenever P is false, regardless of the value of Q, are less intuitively obvious. There is, however, no other plausible way to fill in these rows, given that we want the entries in the truth table to depend only on the truth or falsity of P and Q, and that the one situation with which we are primarily concerned is that we do not want P to be true and Q to be false. Moreover, if we were to make the value of $P \to Q$ false in the third and fourth rows, we would obtain a truth table that is identical to the truth table for $P \wedge Q$, which would make $P \to Q$ redundant. The above truth table for $P \wedge Q$, which is universally accepted by mathematicians and logicians, may seem strange at first glance, and perhaps even contrary to intuition, but it is important to get used to it, because we will always use $P \to Q$ as we have defined it.

A simple example of a conditional statement is "if it rains today, then I will see a movie this evening." This statement has the form $P \to Q$, where $P =$ "it rains today," and $Q =$ "I will see a movie this evening." The truth of this statement does not say that it is raining today, nor that I will see a movie this evening. It only says what will happen if it rains today, which is that I will see a movie this evening. If it does not rain, I still might see a movie this evening, or I might not; both of these possibilities would be consistent with the truth of the original statement "if it rains today, then I will see a movie this evening."

Although it is standard to write $P \to Q$, it is not the order of writing that counts, but the logical relationship. It would be identical to write $Q \leftarrow P$ instead of $P \to Q$. Either way, each of P and Q has a specified—and distinct—role. By contrast, if we

write $Q \rightarrow P$, then we have switched the roles of Q and P, resulting in a statement that is not equivalent to $P \rightarrow Q$ (as will be discussed in Section 1.3).

There are a number of variations as to how to write the statement $P \rightarrow Q$ in English. In addition to writing "if P then Q," we could just as well write any of the following:

If P, Q;
Q if P;
P only if Q;
Q provided that P;
Assuming that P, then Q;
Q given that P;
P is sufficient for Q;
Q is necessary for P.

These variants are each useful in particular situations. For example, the statement "if it rains today, then I will see a movie this evening" could just as well be written "I will see a movie this evening if it rains today." It would also be formally correct to say "it is raining today is sufficient for me to see a movie this evening," though such a sentence would, of course, be rather awkward.

Our fifth construction, the **biconditional** from P to Q, which is denoted $P \leftrightarrow Q$, is the statement that, intuitively, is true if P and Q are both true or both false, and is false otherwise. We read $P \leftrightarrow Q$ as "P if and only if Q." The phrase "if and only if" is often abbreviated as "iff." The precise definition of $P \leftrightarrow Q$ is given in the truth table

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

An example of a biconditional statement is "I will go for a walk if and only if Fred will join me." This statement has the form $P \leftrightarrow Q$, where $P =$ "I will go for a walk," and $Q =$ "Fred will join me." The truth of this statement does not say that I will go for a walk, or that Fred will join me. It says that either Fred will join me and I will go for a walk, or that neither of these things will happen. In other words, it could not be the case that Fred joins me and yet I do not go for a walk, and it also could not be the case that I go for a walk, and yet Fred has not joined me.

There are some variations as to how to write the statement $P \leftrightarrow Q$ in English. In addition to writing "P if and only if Q," it is common to write "P is necessary and sufficient for Q."

In Section 1.3 we will clarify further the meaning of biconditional statements. Among other things, we will see that the order of writing a biconditional statement makes no difference, that is, it makes no difference whether we write $P \leftrightarrow Q$ or $Q \leftrightarrow P$.

Now that we have defined our five basic ways of combining statements, we can form more complicated compound statements by using combinations of the basic

operations. For example, we can form $P \vee (Q \to \neg R)$ out of statements P, Q and R. We need to use parentheses in this compound statement, to make sure it is unambiguous. We use the standard convention that $\neg$ takes precedence over the other four operations, but none of these four takes precedence over the others. Hence, writing "$P \vee Q \to \neg R$" would be ambiguous, and we would never write such an expression.

We can form the truth table for the statement $P \vee (Q \to \neg R)$, doing one operation at a time, as follows:

P	Q	R	$\neg R$	$Q \to \neg R$	$P \vee (Q \to \neg R)$
T	T	T	F	F	T
T	T	F	T	T	T
T	F	T	F	T	T
T	F	F	T	T	T
F	T	T	F	F	F
F	T	F	T	T	T
F	F	T	F	T	T
F	F	F	T	T	T

To save time and effort, it is possible to write a smaller truth table with the same information as the truth table above, by writing one column at a time, and labeling the columns in the order of how we write them. In the truth table shown below, we first write columns 1 and 2, which are just copies of the P and Q columns; we then write column 3, which is the negation of the R column; column 4 is formed from columns 2 and 3, and column 5 is formed from columns 1 and 4. We put the label "5" in a box, to highlight that its column is the final result of the truth table, and refers to the compound statement in which we are interested. It is, of course, the same result as in the previous truth table.

P	Q	R	P	$\vee$	$(Q$	$\to$	$\neg$	$R)$
T	T	T	T	T	T	F		F
T	T	F	T	T	T	T		T
T	F	T	T	T	F	T		F
T	F	F	T	T	F	T		T
F	T	T	F	F	T	F		F
F	T	F	F	T	T	T		T
F	F	T	F	T	F	T		F
F	F	F	F	T	F	T		T
			1	5	2	4		3

Just as we can form compound statements written with symbols, we can also form such statements written in English. The role that parentheses play in avoiding ambiguity in statements written with symbols is often played in English sentences by punctuation. For example, the sentence "I like to eat apples or pears, and I like to eat peaches" is unambiguous. If we let $A =$ "I like to eat apples," let $B =$ "I like to eat pears" and let $C =$ "I like to eat peaches," then the sentence can be written in symbols as $(A \vee B) \wedge C$. On the other hand, suppose that we were given the statement

$(A \vee B) \wedge C$, and were told to translate it into English, knowing that $A =$ "I like to eat apples," etc., but without knowing that the statement had originally been formulated in English. A careful translation into English might result in the original statement, or in some equally valid variant, such as "I like to eat apples or I like to eat pears, and I like to eat peaches." Unfortunately, imprecise translations such as "I like to eat apples or pears and peaches," or "I like to eat apples, or I like to eat pears, and I like to eat peaches," are often made. These two statements are ambiguous; the ambiguity in the first statement results from the lack of necessary punctuation, and the ambiguity in the second statement results from incorrect punctuation. In both these statements the problem with the punctuation is not a matter of grammar, but rather of capturing accurately and unambiguously the meaning of the statement $(A \vee B) \wedge C$.

We end this section with a brief mention of two important concepts. A **tautology** is a statement that is always true by logical necessity, regardless of whether the component statements are true or false, and regardless of what we happen to observe in the real world. A **contradiction** is a statement that is always false by logical necessity. Most statements we encounter will be neither of these types. For example, the statement "Irene has red hair" is neither a tautology nor a contradiction, because it is not necessarily either true or false—it is logically plausible that Irene does have red hair, and it is just as plausible that she does not. Even the statement "$1 \neq 2$" is not a tautology. It is certainly true in our standard mathematical system, as far as we know, but the truth of this statement is an observation about the way human beings have constructed their number system, not a logical necessity.

An example of a tautology is the statement "Irene has red hair or she does not have red hair." It seems intuitively clear that this statement is a tautology, and we can verify this fact formally by using truth tables. Let $P =$ "Irene has red hair." Then our purported tautology is the statement $P \vee \neg P$. The truth table for this statement is

$$
\begin{array}{c|ccc}
P & P & \vee & \neg P \\
\hline
T & T & T & F \\
F & F & T & T \\
& 1 & \boxed{3} & 2
\end{array}.
$$

We see in column 3 that the statement $P \vee \neg P$ is always true, regardless of whether P is true or false. This fact tells us that $P \vee \neg P$ is a tautology. In general, a statement is a tautology if, as verified using a truth table, it is always true, regardless of whether its component statements are true or false.

The statement "Irene has red hair and she does not have red hair" is a contradiction. In symbols this statement is $P \wedge \neg P$, and it has truth table

$$
\begin{array}{c|ccc}
P & P & \wedge & \neg P \\
\hline
T & T & F & F \\
F & F & F & T \\
& 1 & \boxed{3} & 2
\end{array}.
$$

The statement $P \wedge \neg P$ is always false, regardless of whether P is true or false. In general, a statement is a contradiction if, as verified using a truth table, it is always false, regardless of whether its component statements are true or false.

That $P \vee \neg P$ is a tautology, and that $P \wedge \neg P$ is a contradiction, seems quite intuitively reasonable. It is possible, however, to have more complicated (and not so intuitive) tautologies and contradictions. For example, the truth table of the statement $[(P \wedge Q) \rightarrow R] \rightarrow [P \rightarrow (Q \rightarrow R)$ is

P	Q	R	[(P	∧	Q)	→	R]	→	[P	→	(Q	→	R)]
T	T	T	T	T	T	T	T	**T**	T	T	T	T	T
T	T	F	T	T	T	F	F	**T**	T	F	T	F	F
T	F	T	T	F	F	T	T	**T**	T	T	F	T	T
T	F	F	T	F	F	T	F	**T**	T	T	F	T	F
F	T	T	F	F	T	T	T	**T**	F	T	T	T	T
F	T	F	F	F	T	T	F	**T**	F	T	T	F	F
F	F	T	F	F	F	T	T	**T**	F	T	F	T	T
F	F	F	F	F	F	T	F	**T**	F	T	F	T	F
			1	3	2	5	4	**11**	9	10	6	8	7

We see in column 11 that the statement $[(P \wedge Q) \rightarrow R] \rightarrow [P \rightarrow (Q \rightarrow R)$ is always true, regardless of whether each of P, Q and R is true or false. Hence the statement is a tautology. Suppose that $P =$ "Sam is sad," let $Q =$ "Warren is sad" and $R =$ "Sam and Warren eat pasta." Then the statement becomes "If it is true that if Sam and Warren are both sad then they eat pasta, then it is true that if Sam is sad, then if Warren is sad they eat pasta."

As an example of a contradiction, the reader can verify with a truth table that the statement $[Q \rightarrow (P \wedge \neg Q)] \wedge Q$ is always false.

Exercises

Exercise 1.2.1. Which of the following expressions are statements?

(**1**) Today is a nice day.
(**2**) Go to sleep.
(**3**) Is it going to snow tomorrow?
(**4**) The U.S. has 49 states.
(**5**) I like to eat fruit, and you often think about traveling to Spain.
(**6**) If we go out tonight, the babysitter will be unhappy.
(**7**) Call me on Thursday if you are home.

Exercise 1.2.2. Which of the following expressions are statements?

(**1**) $4 < 3$.
(**2**) If $x \geq 2$ then $x^3 \geq 1$.
(**3**) $y < 7$.
(**4**) $x + y = z$.
(**5**) $(a+b)^2 = a^2 + 2ab + b^2$.
(**6**) $a^2 + b^2 = c^2$.
(**7**) If $w = 3$ then $z^w \neq 0$.

Exercise 1.2.3. Let $P =$ "I like fruit," let $Q =$ "I do not like cereal" and $R =$ "I know how to cook an omelette." Translate the following statements into words.

(1) $P \wedge Q$.

(2) $Q \vee R$.

(3) $\neg R$.

(4) $\neg(P \vee Q)$.

(5) $\neg P \vee \neg Q$.

(6) $\neg P \vee Q$.

(7) $(R \wedge P) \vee Q$.

(8) $R \wedge (P \vee Q)$.

Exercise 1.2.4. Let $X =$ "I am happy," let $Y =$ "I am watching a movie" and $Z =$ "I am eating spaghetti." Translate the following statements into words.

(1) $Z \to X$.

(2) $X \leftrightarrow Y$.

(3) $(Y \vee Z) \to X$.

(4) $Y \vee (Z \to X)$.

(5) $(Y \to \neg X) \wedge (Z \to \neg X)$.

(6) $(X \wedge \neg Y) \leftrightarrow (Y \vee Z)$.

Exercise 1.2.5. Let $X =$ "Fred has red hair," let $Y =$ "Fred has a big nose" and $R =$ "Fred likes to eat figs." Translate the following statements into symbols.

(1) Fred does not like to eat figs.

(2) Fred has red hair, and does not have a big nose.

(3) Fred has red hair or he likes to eat figs.

(4) Fred likes to eat figs, and he has red hair or he has a big nose.

(5) Fred likes to eat figs and he has red hair, or he has a big nose.

(6) It is not the case that Fred has a big nose or he has red hair.

(7) It is not the case that Fred has a big nose, or he has red hair.

(8) Fred has a big nose and red hair, or he has a big nose and likes to eat figs.

Exercise 1.2.6. Let $E =$ "The house is blue," let $F =$ "The house is 30 years old" and $G =$ "The house is ugly." Translate the following statements into symbols.

(1) If the house is 30 years old, then it is ugly.

(2) If the house is blue, then it is ugly or it is 30 years old.

(3) If the house is blue then it is ugly, or it is 30 years old.

(4) The house is not ugly if and only if it is 30 years old.

(5) The house is 30 years old if it is blue, and it is not ugly if it is 30 years old.

(6) For the house to be ugly, it is necessary and sufficient that it be ugly and 30 years old.

Exercise 1.2.7. Suppose that A is a true statement, that B is a false statement, that C is a false statement and that D is a true statement. Which of the following statements are true, and which are false?

(1) $A \vee C$.

(2) $(C \wedge D) \vee B$.

(3) $\neg(A \wedge B)$.

(4) $\neg D \vee \neg C$.

(5) $(D \wedge A) \vee (B \wedge C)$.

(6) $C \vee [D \vee (A \wedge B)]$.

Exercise 1.2.8. Suppose that X is a false statement, that Y is a true statement, that Z is a false statement and that W is a true statement. Which of the following statements are true, and which are false?

(1) $Z \rightarrow Y$.

(2) $X \leftrightarrow Z$.

(3) $(Y \leftrightarrow W) \wedge X$.

(4) $W \rightarrow (X \rightarrow \neg W)$.

(5) $[(Y \rightarrow W) \leftrightarrow W] \wedge \neg X$.

(6) $(W \rightarrow X) \leftrightarrow \neg(Z \vee Y)$.

Exercise 1.2.9. Suppose that Flora likes fruit, does not like carrots, likes nuts and does not like rutabagas. Which of the following statements are true, and which are false?

(1) Flora likes fruit and carrots.

(2) Flora likes nuts or rutabagas, and she does not like carrots.

(3) Flora likes carrots, or she likes fruit and nuts.

(4) Flora likes fruit or nuts, and she likes carrots or rutabagas.

(5) Flora likes rutabagas, or she likes fruit and either carrots or rutabagas.

Exercise 1.2.10. Suppose that Hector likes beans, does not like peas, does not like lentils and likes sunflower seeds. Which of the following statements are true, and which are false?

(1) If Hector likes beans, then he likes lentils.

(2) Hector likes lentils if and only if he likes peas.

(3) Hector likes sunflower seeds, and if he likes lentils then he likes beans.

(4) Hector likes peas and sunflower seeds if he likes beans.

(5) If Hector likes lentils then he likes sunflower seeds, or Hector likes lentils if and only if he likes peas.

(6) For Hector to like beans and lentils it is necessary and sufficient for him to like peas or sunflower seeds.

Exercise 1.2.11. Make a truth table for each of the following statements.

(1) $P \wedge \neg Q$.

(2) $(R \vee S) \wedge \neg R$.

(3) $X \vee (\neg Y \vee Z)$.

(4) $(A \vee B) \wedge (A \vee C)$.

(5) $(P \wedge R) \vee \neg(Q \wedge S)$.

Exercise 1.2.12. Make a truth table for each of the following statements.

(1) $X \rightarrow \neg Y$.

(2) $(R \rightarrow S) \leftrightarrow R$.

(3) $\neg M \rightarrow (N \wedge L)$.

(4) $(E \leftrightarrow F) \rightarrow (E \leftrightarrow G)$.

(5) $(P \rightarrow R) \vee \neg(Q \leftrightarrow S)$.

Exercise 1.2.13. Which of the following statements are tautologies, which are contradictions and which are neither?

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

(2) $(X \vee Y) \leftrightarrow (\neg X \rightarrow Y)$.

(3) $(A \wedge \neg B) \wedge (\neg A \vee B)$.

(4) $[Z \vee (\neg Z \vee W)] \wedge \neg(W \wedge U)$.

(5) $[L \rightarrow (M \rightarrow N)] \rightarrow [M \rightarrow (L \rightarrow N)]$.

(6) $[(X \leftrightarrow Z) \wedge (X \leftrightarrow Y)] \wedge X$.

(7) $[(P \leftrightarrow \neg Q) \wedge P] \wedge Q$.

Exercise 1.2.14. Which of the following statements are tautologies, which are contradictions and which are neither?

(1) If John eats a blueberry pizza, then he either eats a blueberry pizza or he does not.
(2) If John either eats a blueberry pizza or he does not, then he eats a blueberry pizza.
(3) If pigs have wings and pigs do not have wings, then the sun sets in the east.
(4) If Ethel goes to the movies then Agnes will eat a cake, and Agnes does not eat cake, and Ethel goes to the movies.
(5) Rabbits eat cake or pie, and if rabbits eat pie then they eat cake.
(6) The cow is green or the cow is not green, if and only if the goat is blue and the goat is not blue.

Exercise 1.2.15. Let P be a statement, let T be a tautology and let C be a contradiction.

(1) Show that $P \vee T$ is a tautology.
(2) Show that $P \wedge C$ is a contradiction.

1.3 Relations Between Statements

Up until now we have constructed statements; now we want to discuss relations between them. Relations between statements are not formal statements in themselves, but are "meta-statements" that we make about statements. An example of a meta-statement is the observation that "if the statement 'Ethel is tall and Agnes is short' is true, then the statement 'Ethel is tall' is true." Another example is "the statement 'Irving has brown hair or Mel has red hair' being true is equivalent to the statement 'Mel has red hair or Irving has brown hair' being true." Of course, we will need to clarify what it means for one statement to imply another, or be equivalent to another, but whatever the formal approach to these concepts is, intuitively the above two meta-statements seem correct.

It might be objected to that the above examples of meta-statements are in fact statements in themselves, which is true enough informally, though in a formal setting, which we are not presenting here, there is indeed a difference between a well-formed statement in a given formal language and a meta-statement that we might make about such formal statements. In practice, the distinction between statements and meta-statements is straightforward enough for us to make use of it here.

The two examples of relations between statements given above represent the two types of such relations we will study, namely, implication and equivalence, which are the meta-statement analogs of conditionals and biconditionals. We start with implication.

The intuitive idea of logical implication is that statement P implies statement Q if necessarily Q is true whenever P is true. In other words, it can never be the case that

P is true and Q is false. Necessity is the key here, because one statement implying another should not simply be a matter of coincidentally appropriate truth values. Consider the statements $P =$ "the sky is blue" and $Q =$ "grass is green." Given what we know about sky and grass, the statement "if the sky is blue then grass is green" is certainly true (that is, the statement $P \to Q$ is true), because both P and Q are true. However, and this is the key point, we would not want to say that "the sky is blue" logically implies "grass is green," because logical implication should not depend upon the particular truth values of the particular statements. What would happen if, due to some environmental disaster, all the grass in the world suddenly turned black, although the sky still stayed blue. Then the statement "if the sky is blue then grass is green" would be false. Because this possibility could in principle happen, we do not say that "the sky is blue" implies "grass is green." In general, even though $P \to Q$ happens to be true now, given that it might be false under other circumstances, we cannot say that P implies Q. To have P imply Q, we need $P \to Q$ to be true under all possible circumstances.

Now consider the two statements "it is not the case that, if Susan thinks Lisa is cute then she likes Lisa" and "Susan thinks Lisa is cute or she likes Lisa." Whether or not each of these statements is actually true or false depends upon knowing whether or not Susan thinks Lisa is cute, and whether or not Susan likes Lisa. What will always be the case, as we will soon see, is that the statement "it is not the case that, if Susan thinks Lisa is cute then she likes Lisa" implies the statement "Susan thinks Lisa is cute or she likes Lisa," regardless of whether each component statement is true or false.

Let $P =$ "Susan thinks Lisa is cute" and $Q =$ "Susan likes Lisa." Then we want to show that $\neg(P \to Q)$ implies $P \vee Q$. We show this implication in two ways. First, we check the truth tables for each of $\neg(P \to Q)$ and $P \vee Q$, which are

P	Q	$\neg$	$(P$	$\to$	$Q)$
T	T	F	T	T	T
T	F	T	T	F	F
F	T	F	F	T	T
F	F	F	F	T	F
		$\boxed{4}$	1	3	2

P	Q	P	$\vee$	Q
T	T	T	T	T
T	F	T	T	F
F	T	F	T	T
F	F	F	F	F
		1	$\boxed{3}$	2

The column numbered 4 in the first truth table has the truth values for $\neg(P \to Q)$, and the column numbered 3 in the second truth table has the truth values for $P \vee Q$. We observe that in any row that has a T as the truth value for $\neg(P \to Q)$, there is also a T for the truth value of $P \vee Q$ (there is only one such row in this case, but that is immaterial). It makes no difference what happens in the rows in which $\neg(P \to Q)$ has truth value F. Hence $\neg(P \to Q)$ logically implies $P \vee Q$.

Alternatively, rather than having two truth tables to compare, we can use the conditional (defined in Section 1.2) to recognize that our observations about the above two truth tables is the same as saying that the single statement $[\neg(P \to Q)] \to (P \vee Q)$ will always be true, regardless of the truth or falsity of P and Q. In other words, the statement $[\neg(P \to Q)] \to (P \vee Q)$ will be a tautology (also in Section 1.2), as can be

seen in the truth table

$$
\begin{array}{cc|ccccccccc}
P & Q & [\neg & (P & \to & Q)] & \to & (P & \vee & Q) \\
\hline
T & T & F & T & T & T & T & T & T & T \\
T & F & T & T & F & F & T & T & T & F \\
F & T & F & F & T & T & T & T & F & T & T \\
F & F & F & F & T & F & T & F & F & F \\
& & 4 & 1 & 3 & 2 & \boxed{8} & 5 & 7 & 6
\end{array}
$$

We see in Column 8 that the statement $[\neg(P \to Q)] \to (P \vee Q)$ is always true, and hence it is indeed a tautology.

   This last consideration leads to the precise notion of implication. Let P and Q be statements. We say that P **implies** Q if the statement $P \to Q$ is a tautology. We abbreviate the English expression "P implies Q" with the notation "$P \Rightarrow Q$."

   It is important to note the difference between the notations "$P \Rightarrow Q$" and "$P \to Q$." The notation "$P \to Q$" is a statement; it is a compound statement built up out of the statements P and Q. The notation "$P \Rightarrow Q$" is a meta-statement, which is simply a shorthand way of writing the English expression "P implies Q," and it means that $P \to Q$ is not just true in some particular instances, but is a tautology.

   It might appear at first glance as if we are not introducing anything new here, given that we are defining implication in terms of conditional statements, but there is a significant new idea in the present discussion, which is that we single out those situations where $P \to Q$ is not just a statement (which is always the case), but where $P \to Q$ is a tautology. Moreover, we will see in Section 1.4 that implications of statements will be extremely useful in constructing valid arguments. In particular, the following implications will be used extensively.

Fact 1.3.1. *Let P, Q, R and S be statements.*

   1. $(P \to Q) \wedge P \Rightarrow Q$ *(Modus Ponens).*
   2. $(P \to Q) \wedge \neg Q \Rightarrow \neg P$ *(Modus Tollens).*
   3. $P \wedge Q \Rightarrow P$ *(Simplification).*
   4. $P \wedge Q \Rightarrow Q$ *(Simplification).*
   5. $P \Rightarrow P \vee Q$ *(Addition).*
   6. $Q \Rightarrow P \vee Q$ *(Addition).*
   7. $(P \vee Q) \wedge \neg P \Rightarrow Q$ *(Modus Tollendo Ponens).*
   8. $(P \vee Q) \wedge \neg Q \Rightarrow P$ *(Modus Tollendo Ponens).*
   9. $P \leftrightarrow Q \Rightarrow P \to Q$ *(Biconditional-Conditional).*
   10. $P \leftrightarrow Q \Rightarrow Q \to P$ *(Biconditional-Conditional).*
   11. $(P \to Q) \wedge (Q \to P) \Rightarrow P \leftrightarrow Q$ *(Conditional-Biconditional).*
   12. $(P \to Q) \wedge (Q \to R) \Rightarrow P \to R$ *(Hypothetical Syllogism).*
   13. $(P \to Q) \wedge (R \to S) \wedge (P \vee R) \Rightarrow Q \vee S$ *(Constructive Dilemma).*

Demonstration. We will show that Part (1) holds, leaving the rest to the reader in Exercise 1.3.6.

   (1). To demonstrate that $(P \to Q) \wedge P \Rightarrow Q$, we need to show that the statement $[(P \to Q) \wedge P] \to Q$ is a tautology, which we do with the truth table

$$
\begin{array}{cc|ccccccc}
P & Q & [(P & \to & Q) & \wedge & P] & \to & Q \\
\hline
T & T & T & T & T & T & T & T & T \\
T & F & T & F & F & F & T & T & F \\
F & T & F & T & T & F & F & T & T \\
F & F & F & T & F & F & F & T & F \\
& & 1 & 3 & 2 & 5 & 4 & \boxed{7} & 6
\end{array}.
$$

We see in Column 7 that the statement $[(P \to Q) \wedge P] \to Q$ is always true, and hence it is a tautology.   ///

The implications stated in Fact 1.3.1 were chosen because they are symbolic statements of various rules of valid argumentation. Consider, for example, Part (7). Suppose that $P =$ "the cow has a big nose" and $Q =$ "the cow has a small head." Translating our statement yields "the cow has a big nose or a small head, and the cow does not have a big nose" implies "the cow has a small head." This implication is indeed intuitively reasonable. The implications stated in Fact 1.3.1 will be used in Section 1.4, and so we will not discuss them in detail here.

Logical implication is not always reversible. For example, we saw that "it is not the case that, if Susan thinks Lisa is cute then she likes Lisa" implies "Susan thinks Lisa is cute or she likes Lisa." Written in symbols, we saw that $\neg(P \to Q) \Rightarrow P \vee Q$. On the other hand, the same truth tables used to establish this implication also show that $P \vee Q$ does not imply $\neg(P \to Q)$. For example, when P and Q are both true, then $P \vee Q$ is true, but $\neg(P \to Q)$ is false. Alternatively, it can be seen by a truth table that $(P \vee Q) \to [\neg(P \to Q)]$ is not a tautology. Hence "Susan thinks Lisa is cute or she likes Lisa" does not imply "it is not the case that, if Susan thinks Lisa is cute then she likes Lisa."

Some logical implications, however, are reversible. Such implications are very convenient, and they convey the idea of logical equivalence, to which we now turn. Certainly, two different English sentences can convey equivalent statements, for example "if it rains I will stay home" and "I will stay home if it rains." These two statements are both English variants of $P \to Q$, where $P =$ "it rains," and $Q =$ "I will stay home." The difference between these two statements is an issue only of the flexibility of the English language; symbolically, these two statements are identical, not just equivalent.

What interests us are logically equivalent statements that are not simply English variants of the same symbolic statement, but rather are truly different statements. For example, the statement "it is not that case that I do not own a bicycle" will be seen to be equivalent to "I own a bicycle." If we let $P =$ "I own a bicycle," then the statement "it is not that case that I do not own a bicycle" is $\neg(\neg P)$. This statement is not identical to P. It will be very important to us to be able to recognize that some non-identical statements, for example $\neg(\neg P)$ and P, are in fact logically equivalent. Such equivalences will allow us to find alternative forms of the statements of some theorems, and these alternative forms are sometimes easier to prove than the originals.

The intuitive idea of equivalence of statements is that to claim that statements P and Q are equivalent means that necessarily P is true if and only if Q is true. Necessity is once again the key here, as can be seen once more using the statements

"the sky is blue" and "grass is green," which are not equivalent, even though both are true. By contrast, consider the two statements "if Fred has good taste in food, then he likes to eat liver" and "if Fred does not like to eat liver, then he does not have good taste in food." We will show that these statements are equivalent, as follows. Let $P =$ "Fred has good taste in food" and $Q =$ "Fred likes to eat liver." Then we want to show the equivalence of $P \to Q$ and $\neg Q \to \neg P$. We need to see that each of these two statements is true when the other is true, and each is false when the other is false. Once again we can use truth tables. If we use separate truth tables, we see that

P	Q	P	$\to$	Q
T	T	T	T	T
T	F	T	F	F
F	T	F	T	T
F	F	F	T	F
			1 \boxed{3} 2	

P	Q	$\neg Q$	$\to$	$\neg P$
T	T	F	T	F
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T
		1	\boxed{3}	2

The columns numbered 3 in the truth tables have the truth values for $P \to Q$ and $\neg Q \to \neg P$ respectively. These columns are identical, which says that $P \to Q$ is true if and only if $\neg Q \to \neg P$ is true. We can avoid having to compare two truth tables, this time by using the biconditional (defined in Section 1.2). The equality of the truth values of our two statements in the two truth tables above is the same as saying that the single statement $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$ is a tautology, as can be seen in the truth table

P	Q	$(P$	$\to$	$Q)$	$\leftrightarrow$	$(\neg Q$	$\to$	$\neg P)$
T	T	T	T	T	T	F	T	F
T	F	T	F	F	T	T	F	F
F	T	F	T	T	T	F	T	T
F	F	F	T	F	T	T	T	T
		1	3	2	\boxed{7}	4	6	5

We see in Column 7 that the statement $(P \to Q) \leftrightarrow (\neg Q \to \neg P)$ is always true, and hence it is a tautology.

In general, let P and Q be statements. We say that P and Q are **equivalent** if the statement $P \leftrightarrow Q$ is a tautology. We abbreviate the English expression "P and Q are equivalent" with the notation "$P \Leftrightarrow Q$."

It is important to note the difference between the notations "$P \Leftrightarrow Q$" and "$P \leftrightarrow Q$." The latter is a statement, whereas the former is a meta-statement, which is simply a shorthand way of writing the English expression "P is equivalent to Q."

Listed below are some equivalences of statements that will be particularly useful. We will discuss some of these equivalences after stating them.

Fact 1.3.2. *Let P, Q and R be statements.*

1. $\neg(\neg P) \Leftrightarrow P$ *(Double Negation).*
2. $P \vee Q \Leftrightarrow Q \vee P$ *(Commutative Law).*
3. $P \wedge Q \Leftrightarrow Q \wedge P$ *(Commutative Law).*
4. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ *(Associative Law).*

5. $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ *(Associative Law)*.

6. $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ *(Distributive Law)*.

7. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ *(Distributive Law)*.

8. $P \rightarrow Q \Leftrightarrow \neg P \vee Q$.

9. $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$ *(Contrapositive)*.

10. $P \leftrightarrow Q \Leftrightarrow Q \leftrightarrow P$.

11. $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$.

12. $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$ *(De Morgan's Law)*.

13. $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ *(De Morgan's Law)*.

14. $\neg(P \rightarrow Q) \Leftrightarrow P \wedge \neg Q$.

15. $\neg(P \leftrightarrow Q) \Leftrightarrow (P \wedge \neg Q) \vee (\neg P \wedge Q)$.

Demonstration. Part (9) was discussed previously. We will show here that Part (7) holds, leaving the rest to the reader in Exercise 1.3.7. The demonstration here is very similar to the demonstration of Fact 1.3.1 (1).

(7). We need to demonstrate that $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$, which we do by showing that the statement $[P \vee (Q \wedge R)] \leftrightarrow [(P \vee Q) \wedge (P \vee R)]$ is a tautology, which in turn we do with the truth table

P	Q	R	[P	∨	(Q	∧	R)]	↔	[(P	∨	Q)	∧	(P	∨	R)]
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	F	T	T	T	T	T	T	T	F
T	F	T	T	T	F	F	T	T	T	T	F	T	T	T	T
T	F	F	T	T	F	F	F	T	T	T	F	T	T	T	F
F	T	T	F	T	T	T	T	T	F	T	T	T	F	T	T
F	T	F	F	F	T	F	F	T	F	T	T	F	F	F	F
F	F	T	F	F	F	F	T	T	F	F	F	F	F	T	T
F	F	F	F	F	F	F	F	T	F	F	F	F	F	F	F
			4	5	1	3	2	13	6	8	7	12	9	11	10	·

We see in Column 13 that the statement $[P \vee (Q \wedge R)] \leftrightarrow [(P \vee Q) \wedge (P \vee R)]$, and hence it is a tautology.   ///

Part (1) of Fact 1.3.2 might appear innocuous, but this equivalence plays a very important role in standard mathematical proofs. In informal terms, the equivalence of $\neg(\neg P)$ and P means that "two negatives cancel each other out." From the point of view of constructing mathematical proofs, suppose that we want to show that a statement P is true. One method to prove this statement would be to hypothesize that $\neg P$ is true, and derive a contradiction. It would then follow that $\neg P$ is false, which implies that $\neg(\neg P)$ is true. Because $\neg(\neg P)$ and P are equivalent, it would follow that P is true. This methodology of proof might sound rather convoluted, but it is often quite useful, and is called proof by contradiction. A detailed discussion of this method of proof is in Section 2.3.

Part (11) of Fact 1.3.2 gives a reformulation of the biconditional in terms of conditionals. For example, the statement "I will play the flute today if and only if I listen to the radio" is equivalent to the statement "if I play the flute today I will listen

to the radio, and if I listen to the radio I will play the flute today." The equivalence of $P \leftrightarrow Q$ and $(P \rightarrow Q) \wedge (Q \rightarrow P)$ says that to prove a statement of the form $P \leftrightarrow Q$, it is sufficient to prove $(P \rightarrow Q) \wedge (Q \rightarrow P)$; it therefore suffices to prove each of $(P \rightarrow Q)$ and $(Q \rightarrow P)$. As we will see in Chapter 2, the most basic type of statement that is proved in mathematics is a conditional statement. Hence, when we want to prove a theorem with a statement that is a biconditional, we will often prove the two corresponding conditional statements instead. See Section 2.4 for more discussion.

Part (9) of Fact 1.3.2 allows us to reformulate one conditional statement in terms of another. For example, the statement "if it snows today, Yolanda will wash her clothes" is equivalent to "if Yolanda did not wash her clothes, it did not snow today." Suppose that we know that the statement "if it snows today, Yolanda will wash her clothes" is true. Suppose further that in fact Yolanda did not wash her clothes. Then it could not have snowed, because if it had snowed, then surely Yolanda would have washed her clothes. On the other hand, if Yolanda did wash her clothes, we could not automatically conclude that it snowed, because Yolanda might choose to wash her clothes even when it does not snow. Therefore "if Yolanda did not wash her clothes, it did not snow today" must be true whenever "if it snows today, Yolanda will wash her clothes" is true. Similar reasoning shows that if the latter statement is true, then so is the former.

Because the equivalence of the statements $P \rightarrow Q$ and $\neg Q \rightarrow \neg P$ will be so important for constructing mathematical proofs, as seen in Section 2.3, relevant terminology is merited. Given a conditional statement of the form $P \rightarrow Q$, we call $\neg Q \rightarrow \neg P$ the **contrapositive** of the original statement. For example, the contrapositive of "if I eat too much I will feel sick" is "if I do not feel sick I did not eat too much." Fact 1.3.2 (9) says that a statement and its contrapositive are always equivalent.

We also give names to two other variants of statements of the form $P \rightarrow Q$. We call $Q \rightarrow P$ the **converse** of the original statement, and we call $\neg P \rightarrow \neg Q$ the **inverse** of the original statement. Continuing the example of the previous paragraph, the converse of "if I eat too much I will feel sick" is "if I feel sick then I ate too much"; the inverse of the original statement is "if I did not eat too much then I will not feel sick." It is important to recognize that neither the converse nor the inverse is equivalent to the original statement, as the reader can verify by constructing the appropriate truth tables. If we look at the statements "if I feel sick then I ate too much" and "if I did not eat too much then I will not feel sick," we observe that both of them mean that there is no other possible cause of feeling sick than eating too much, whereas the original statement "if I eat too much I will feel sick" says nothing of the sort. Although the converse and inverse of a statement are not equivalent to the original statement, we note that, however, that the converse and the inverse are equivalent to each another, as can be seen by applying Fact 1.3.2 (9) to the statement $Q \rightarrow P$.

One important use of equivalences of statements is to find convenient formulas for the negations of statements. Such formulas are found in Parts (12)–(15) of Fact 1.3.2, which show how to negate conjunctions, disjunctions, conditionals and biconditionals. For example, what is the negation of the statement "it is raining and I am happy"? We could write "it is not the case that it is raining and I am happy," but that is cumbersome, and slightly ambiguous (does the phrase "it is not the case that"

apply only to "it is raining," or also to "I am happy"?) A common error would be to say "it is not raining and I am unhappy." Observe that the original statement "it is raining and I am happy" is true if and only if both "it is raining" is true and if "I am happy" is true. If either of these two component statements is false, then the whole original statement is false. Hence, to negate "it is raining and I am happy," it is not necessary to negate both component statements, but only to know that at least one of them is false. Hence the correct negation of "it is raining and I am happy" is "it is not raining or I am unhappy." A similar phenomenon occurs when negating a statement with "or" in it. The precise formulation of these ideas, known as De Morgan's Laws, are Fact 1.3.2 (12) (13).

What is the negation of the statement "if it snows, I will go outside"? As before, we could write "it is not the case that if it snows, I will go outside," and again that would be cumbersome. A common error would be to say "if it snows, I will not go outside." To see that this latter statement is not the negation of the original statement, suppose that "it snows" is false, and "I will go outside" is true. Then both "if it snows, I will go outside" and "if it snows, I will not go outside" are true, so the latter is not the negation of the former. The original statement "if it snows, I will go outside" is true if and only if "I will go outside" is true whenever "it snows" is true. The negation of the original statement therefore holds whenever "it snows" is true and "I will go outside" is false; that is, whenever the statement "it snows and I will not go outside" is true. The precise formulation of this observation is Fact 1.3.2 (14).

<div align="center">

Exercises

</div>

Exercise 1.3.1. Let P, Q, R and S be statements. Show that the following are true.

   (1) $\neg(P \to Q) \Rightarrow P$.
   (2) $(P \to Q) \wedge (P \to \neg Q) \Rightarrow \neg P$.
   (3) $P \to Q \Rightarrow (P \wedge R) \to (Q \wedge R)$.
   (4) $P \wedge (Q \leftrightarrow R) \Rightarrow (P \wedge Q) \leftrightarrow R$.
   (5) $P \to (Q \wedge R) \Rightarrow (P \wedge Q) \leftrightarrow (P \wedge R)$.
   (6) $(P \leftrightarrow R) \wedge (Q \leftrightarrow S) \Rightarrow (P \vee Q) \leftrightarrow (R \vee S)$.

Exercise 1.3.2. [Used in Exercise 1.3.12 and Section 2.4.] Let P, Q, A and B be statements. Show that the following are true.

   (1) $P \Leftrightarrow P \vee (P \wedge Q)$.
   (2) $P \Leftrightarrow P \wedge (P \vee Q)$.
   (3) $P \leftrightarrow Q \Leftrightarrow (P \to Q) \wedge (\neg P \to \neg Q)$.
   (4) $P \to (A \wedge B) \Leftrightarrow (P \to A) \wedge (P \to B)$.
   (5) $P \to (A \vee B) \Leftrightarrow (P \wedge \neg A) \to B$.
   (6) $(A \vee B) \to Q \Leftrightarrow (A \to Q) \wedge (B \to Q)$.
   (7) $(A \wedge B) \to Q \Leftrightarrow (A \to Q) \vee (B \to Q)$.
   (8) $(A \wedge B) \to Q \Leftrightarrow A \to (B \to Q)$.

Exercise 1.3.3. Let P be a statement, let T be a tautology and let C be a contradiction.

   (1) Show that $P \wedge T \Leftrightarrow P$.
   (2) Show that $P \vee C \Leftrightarrow P$.

Exercise 1.3.4. For each pair of statements, determine whether or not the first implies the second.

   (1) "If you will kiss me I will dance a jig, and I will dance a jig"; and "you will kiss me."
   (2) "Yolanda has a cat and a dog, and Yolanda has a python"; and "Yolanda has a dog."
   (3) "If cars pollute then we are in trouble, and cars pollute"; and "we are in trouble."
   (4) "Our time is short or the end is near, and doom is impending"; and "the end is near."
   (5) "Vermeer was a musician or a painter, and he was not a musician"; and "Vermeer was a painter."
   (6) "If I eat frogs' legs I will get sick, or if I eat snails I will get sick"; and "if I eat frogs' legs or snails I will get sick."

Exercise 1.3.5. For each pair of statements, determine whether or not the two statements are equivalent.

   (1) "If it rains, then I will see a movie"; and "it is not raining or I will see a movie."
   (2) "This shirt has stripes, and it has short sleeves or a band collar"; and "this shirt has stripes and it has short sleeves, or it has a band collar."
   (3) "It is not true that I like apples and oranges"; and "I do not like apples and I do not like oranges."
   (4) "The cat is gray, or it has stripes and speckles"; and "the cat is gray or it has stripes, and the cat is gray or it has speckles."
   (5) "It is not the case that: melons are ripe if and only if they are soft to the touch"; and "melons are ripe and soft to the touch, or they are not ripe or not soft to the touch."

Exercise 1.3.6. [Used in Fact 1.3.1.] Prove Fact 1.3.1 (2) (3) (4) (5) (6) (7) (8) (9) (10) (11) (12) (13).

Exercise 1.3.7. [Used in Fact 1.3.2.] Prove Fact 1.3.2 (1) (2) (3) (4) (5) (6) (8) (10) (11) (12) (13) (14) (15).

Exercise 1.3.8. State the inverse, converse and contrapositive of each of the following statements.

   (1) If it's Tuesday, it must be Belgium.
   (2) I will go home if it is after midnight.
   (3) Good fences make good neighbors.
   (4) Lousy food is sufficient for a quick meal.
   (5) If you like him, you should give him a hug.

Exercise 1.3.9. For each of the following pair of statements, determine whether the second statement is the inverse, converse or contrapositive of the first statements, or none of these.

(1) "If I buy a new book, I will be happy"; and "If I do not buy a new book, I will be unhappy."

(2) "I will be cold if I do not wear a jacket"; and "I will not be cold if I do not wear a jacket."

(3) "If you smile a lot, your mouth will hurt"; and "If your mouth hurts, you will smile a lot."

(4) "A warm house implies a warm bathroom"; and "A cold bathroom implies a cold house."

(5) "Eating corn implies that I will have to floss my teeth"; and "Not having to floss my teeth implies that I will eat corn."

(6) "Going to the beach is sufficient for me to have fun"; and "Not going to the beach is sufficient for me not to have fun."

Exercise 1.3.10. Negate each of the following statements.

(1) $e^5 > 0$.

(2) $3 < 5$ or $7 \geq 8$.

(3) $\sin\left(\frac{\pi}{2}\right) < 0$ and $\tan(0) \geq 0$.

(4) If $y = 3$ then $y^2 = 7$.

(5) $w - 3 > 0$ implies $w^2 + 9 > 6w$.

(6) $a - b = c$ if and only if $a = b + c$.

Exercise 1.3.11. Negate each of the following statements.

(1) It is Monday and it is snowing.

(2) This book is red or it was written in 1997.

(3) Susan likes to eat figs and drink prune juice.

(4) If I tell you a joke, you will smile.

(5) The play will end on time if and only if the actors are in good spirits.

(6) The room will get painted if you buy the paint.

Exercise 1.3.12. Simplify the following statements. You can make use of the equivalences in Exercise 1.3.2 in addition to the equivalences discussed in the text.

(1) $\neg(P \to \neg Q)$.

(2) $A \to (A \wedge B)$.

(3) $(X \wedge Y) \to X$.

(4) $\neg(M \vee L) \wedge L$.

(5) $(P \to Q) \vee Q$.

(6) $\neg(X \to Y) \vee Y$.

Exercise 1.3.13. [Used in Example 6.3.5.] This exercise is related to switching circuits, which are the basis for computer technology. See Example 6.3.5 for further discussion and references.

(1) The operations $\wedge$ and $\vee$ are examples of binary logical operations, in that they take two inputs and give one output; the operation $\neg$ is an example of a unary logical operation, in that it takes one input and gives one output. How many possible unary and binary logical operations are there? List all of them using truth tables, and give the familiar names to those that we have already seen.

(2) Show that all the operations you found in Part (1) can be obtained by combinations of $\wedge$ and $\neg$ operations.

(3) Let $\overline{\wedge}$ be the binary logical operation, often referred to as **nand**, defined by the truth table

P	Q	$P\,\overline{\wedge}\,Q$
T	T	F
T	F	T
F	T	T
F	F	T

.

It is straightforward to verify that $P\,\overline{\wedge}\,Q \Leftrightarrow \neg(P\wedge Q)$. Show that all the operations you found in Part (1) can be obtained by combinations of $\overline{\wedge}$ operations.

1.4 Valid Arguments

In the previous sections of this chapter we looked at statements from the point of view of truth and falsity. We verified the truth or falsity of statements via truth tables, which allowed us to consider all possible ways in which various component statements might be true or false. This approach, while the most basic way to treat the truth or falsity of statements, does not appear to resemble the way mathematicians prove theorems, which is by starting with the hypotheses, and then writing one new statement at a time, each of which is implied by the previous statements, until the conclusion is reached. In this section we look at the analogous construction in logic, that is, the rules of logical argumentation, and we will see the relation of this approach to what was discussed in the previous sections of this chapter.

When we turn to the formulation of mathematical proofs in Chapter 2, we will be focusing on the mathematical content of our proofs, and we will not explicitly refer to the rules of logical argumentation discussed in the present section—doing so would be a distraction from the mathematical issues involved. We will also not be using the logical notation of the present section in future chapters. Nonetheless, we will be using the rules of logical argumentation implicitly all the time. For a mathematician these rules of logic are somewhat similar to a body builder's relation to the skeleton of the human body—you do not always think about it explicitly as you do your work, but it is the framework upon which all is built.

Consider the following collection of statements, which has a number of premises together with a conclusion.

> If the poodle-o-matic is cheap or is energy efficient, then it will not make money for the manufacturer. If the poodle-o-matic is painted red, then it will make money for the manufacturer. The poodle-o-matic is cheap. Therefore the poodle-o-matic is not painted red.

This collection of statements is an example of a **logical argument**, which in general is a collection of statements, the last of which is the conclusion of the argument, and the rest of which are the premises of the argument. Clearly, the use of the word "argument" in logic is different from the colloquial use of the word, where it could

mean the reasons given for thinking that something is true, or it could mean a heated (and not necessarily logical) discussion.

An argument is a collection of statements that are broken up into premises and a conclusion. Of course, a random collection of statements, in which there is no inherent connection between those designated as premises and the one designated as conclusion, will not be of much use. An argument is **valid** if the conclusion necessarily follows from the premises. Thinking about the notion of logical implication used in Section 1.3, we can say that an argument is valid if we cannot assign truth values to the component statements used in the argument in such a way that the premises are all true but the conclusion is false. To a mathematician, what logicians call an argument would simply correspond to the statement of a theorem; the justification that an argument is valid would correspond to what mathematicians call the proof of the theorem.

How can we show that our sample argument given above is valid? We start by converting the argument to symbols. Let $C =$ "the poodle-o-matic is cheap," let $E =$ "the poodle-o-matic is energy efficient," let $M =$ "the poodle-o-matic makes money for the manufacturer" and let $R =$ "the poodle-o-matic is painted red." The argument then becomes

$$(C \vee E) \to \neg M$$
$$R \to M$$
$$\underline{C}$$
$$\neg R,$$

where the horizontal line separates the premises from the conclusion. Alternatively, in keeping with our notation from Section 1.3, we could write this argument as $[(C \vee E) \to \neg M] \wedge (R \to M) \wedge C \Rightarrow \neg R$.

Considering the last way we wrote our argument, we could attempt to show that it is valid just as we showed that certain logical implications were true in Section 1.3, that is, by showing that the statement $\{[(C \vee E) \to \neg M] \wedge (R \to M) \wedge C\} \to \neg R$ is a tautology, which we could accomplish by using a truth table. This method would indeed work, but it would be neither pleasant nor helpful. First, given that there are four statements involved, the needed truth table would have 16 rows, which would be somewhat tedious. For even more complicated arguments, the truth tables would have to be even larger. Second, using a truth table gives no intuitive insight into why the argument is valid. Finally, when proving mathematical statements, we often use quantifiers (as described in Section 1.5), which make truth tables virtually impossible to use. Mathematical proofs (except perhaps in the field of logic) are never done with truth tables.

Instead of using truth tables, we will try to justify the validity of arguments by making use of what we learned in Section 1.3 about logical implication. If we want to show that a complicated logical implication holds, perhaps we could do so by breaking it down into a collection of simpler implications, taken one at a time. If the simpler implications are already known, then they could be building blocks for the more complicated implication. Some of the standard simple implications that we use, known as **rules of inference**, are listed below. Most of these simple implications

should be familiar—they were proved in Fact 1.3.1, although we are stating them in a different format here, to conform to the notation used for logical arguments.

Modus Ponens	$P \to Q$ P Q	Modus Tollendo Ponens	$P \lor Q$ $\neg P$ Q
Modus Tollens	$P \to Q$ $\neg Q$ $\neg P$	Modus Tollendo Ponens	$P \lor Q$ $\neg Q$ P
Double Negation	$\neg\neg P$ P	Biconditional-Conditional	$P \leftrightarrow Q$ $P \to Q$
Double Negation	P $\neg\neg P$	Biconditional-Conditional	$P \leftrightarrow Q$ $Q \to P$
Repetition	P P	Conditional-Biconditional	$P \to Q$ $Q \to P$ $P \leftrightarrow Q$
Simplification	$P \land Q$ P		
Simplification	$P \land Q$ Q	Hypothetical Syllogism	$P \to Q$ $Q \to R$ $P \to R$
Adjunction	P Q $P \land Q$	Constructive Dilemma	$P \to Q$ $R \to S$ $P \lor R$ $Q \lor S$
Addition	P $P \lor Q$		
Addition	Q $P \lor Q$		

The names for some of the above rules of inference, such as modus ponens, are quite standard; a few of the rules of inference have slightly different names in different texts. There are more rules of inference, but the ones listed above suffice for our purposes. See [KMM80] for a thorough discussion of rules of inference.

A few of the rules of inference listed above were not treated in Fact 1.3.1, although they are easily seen to be true. Double Negation is proved in Fact 1.3.2, although here we state it as two implications, rather than one equivalence. Repetition is evidently true (because $P \to P$ is a tautology), but is still useful as a rule of inference. Adjunction is just a glorified version of repetition, because if we stated it in the format of Fact 1.3.1, it would look like $P \land Q \Rightarrow P \land Q$.

We now return to our argument concerning the poodle-o-matic. Using the rules of inference listed above, we can construct a justification for the argument. We use here the two-column format that may be familiar from high school geometry proofs,

in which each line is labeled by a number, and is given a justification for why it is true in terms of previous lines and rules of inference; no justification is needed for the premises. (We will not, it is worth noting, use this two-column format in mathematical proofs, starting in Chapter 2.) Our justification for the argument is

$$(1)\ (C \vee E) \rightarrow \neg M$$
$$(2)\ R \rightarrow M$$
$$(3)\ C$$
$$\overline{\hspace{3cm}}$$

$(4)\ C \vee E$	(3), Addition
$(5)\ \neg M$	(1), (4), Modus Ponens
$(6)\ \neg R$	(2), (5), Modus Tollens.

This sort of justification, often referred to by logicians as a **derivation**, is a chain of statements connected by meta-statements (namely, the justifications for each line). If an argument has a derivation, we say that the argument is **derivable**. Observe that the derivability of an argument is one thing, and the truth of the component statements involved is another. We can have a derivable argument with component statements that happen to be true, or happen to be false, and we can have a non-derivable argument with component statements that happen to be true, or happen to be false. The derivability of an argument is only a question of the relation of the conclusion of the argument with the premises, not whether the conclusion or premises are actually true.

For a given argument, there is often more than one possible derivation. The following is another derivation for the poodle-o-matic argument, this time making use of the equivalences of statements given in Fact 1.3.2, in addition to our rules of inference. In general, it is acceptable in a derivation to replace one statement with another that is equivalent to it. The alternative derivation is

$$(1)\ (C \vee E) \rightarrow \neg M$$
$$(2)\ R \rightarrow M$$
$$(3)\ C$$
$$\overline{\hspace{3cm}}$$

$(4)\ C \vee E$	(3), Addition
$(5)\ \neg M \rightarrow \neg R$	(2), Contrapositive
$(6)\ (C \vee E) \rightarrow \neg R$	(1), (5), Hypothetical Syllogism
$(7)\ \neg R$	(4), (6), Modus Ponens.

This alternative derivation happens to be longer than the previous one, but our purpose here is only to show that alternatives exist, not to find the most efficient derivation.

We now face an important question: given an argument, we have two notions of whether the argument works, which are that it is or is not valid, and that it is or is not derivable. The former notion involves checking truth values (which is done with truth tables), the latter constructing a chain of statements linked by rules of inference. What is the relation between these two approaches? Though it is not at all obvious, nor easy to prove, it turns out quite remarkably that these two approaches, while different in nature, always yield the same result. That is, an argument is valid

if and only if it is derivable. Hence, if we want to show that a given argument is valid, it will suffice to show that it is derivable, and vice versa. The equivalence of these two approaches is a major result in logic. That validity implies derivability is often referred to as the "Completeness Theorem," and that derivability implies validity is often referred to as the "Soundness Theorem" or "Correctness Theorem." See [End72, Section 25] and [EFT94, Chapters 4 and 5] for details. (Different treatments of this subject might use different collections of rules of inference, but the basic ideas are the same.)

From the above considerations we see that to show that a given argument is valid, we simply need to find a derivation, which is often a much more pleasant prospect than showing validity directly. To show that a given argument is invalid, however, derivations are not much help, because we would need to show that no derivation could possibly be found. It would not suffice to say that you tried your best to find a derivation but could not find one, because you cannot be sure that you have not simply overlooked a derivation that works. Rather, to show that an argument is invalid, we use the definition of validity directly, and we find some truth values for the component statements of the argument that make the premises all true but the conclusion false.

Consider the following argument.

> If aliens land on planet Earth, then all people will buy flowers. If Earth receives signals from outer space, then all people will grow long hair. Aliens land on Earth, and all people are growing long hair. Therefore all people buy flowers, and the Earth receives signals from outer space.

This argument is invalid, which we can see as follows. Let $A =$ "aliens land on planet Earth," let $R =$ "all people buy flowers," let $S =$ "Earth receives signals from outer space" and let $H =$ "all people grow long hair." The argument then becomes

$$A \rightarrow R$$
$$S \rightarrow H$$
$$\underline{A \wedge H}$$
$$R \wedge S.$$

Suppose that A is true, that R is true, that S is false and that H is true. Then $A \rightarrow R$ and $S \rightarrow H$ and $A \wedge H$ are all true, but $R \wedge S$ is false. Therefore the premises are all true but the conclusion is false, which means that the argument is invalid. For some other combinations of A, R, S and H being true or false, it works out that the premises are all true and the conclusion is true, and for some combinations of A, R, S and H being true or false, it works out that the premises are not all true (in which case it does not matter whether the conclusion is true or false for the conclusion to be implied by the premises). Nonetheless, the existence of at least one set of truth values for A, R, S and H for which the premises are all true but the conclusion is false is sufficient to cause the argument to be invalid.

We now look at a particular type of argument for which special care is needed. Before reading further, try to figure out what is strange about this argument.

Jethro does not play the guitar, or Susan plays the flute. If Leslie does not play the xylophone, then Susan does not play the flute. Jethro plays the guitar, and Leslie does not play the xylophone. Therefore Ferdinand plays the accordion.

The strange thing about this argument is that there is no apparent connection between the conclusion and the premises. However, try as you might, you will not be able to find truth values for the component statements used in the argument for which the premises are all true but the conclusion is false. The argument is in fact valid, as odd as that might appear. Let $J =$ "Jethro plays the guitar," let $S =$ "Susan plays the flute," let $L =$ "Leslie plays the xylophone" and let $F =$ "Ferdinand plays the accordion." A derivation for this argument is

(1) $\neg J \vee S$
(2) $\neg L \rightarrow \neg S$
(3) $J \wedge \neg L$
(4) J (3), Simplification
(5) $J \vee F$ (4), Addition
(6) $\neg L$ (3), Simplification
(7) $\neg S$ (2), (6), Modus Ponens
(8) $\neg J$ (1), (7), Modus Tollendo Ponens
(9) F (5), (8), Modus Tollendo Ponens.

This derivation has no flaws, though there is still something suspicious about it. To see what is going on, consider the following derivation, which is also completely correct.

(1) $\neg J \vee S$
(2) $\neg L \rightarrow \neg S$
(3) $J \wedge \neg L$
(4) J (3), Simplification
(5) $J \vee \neg F$ (4), Addition
(6) $\neg L$ (3), Simplification
(7) $\neg S$ (2), (6), Modus Ponens
(8) $\neg J$ (1), (7), Modus Tollendo Ponens
(9) $\neg F$ (5), (8), Modus Tollendo Ponens.

In other words, the same premises can be used to imply the negation of the conclusion in the original argument.

How can it be that the same premises can imply a conclusion and its negation? The answer is that the premises themselves are no good, in that they form a contradiction (as defined in Section 1.2). In symbols, the premises are $(\neg J \vee S) \wedge (\neg L \rightarrow \neg S) \wedge (J \wedge \neg L)$, and, as is left to the reader to check with a truth table, this statement is a contradiction. We leave it to the reader to supply the details. The key to this strange state of affairs is the definition of the conditional. Recall that a statement of the form $P \rightarrow Q$ is always true whenever P is false, regardless of whether Q is true or false. So, if we have premises that form a contradiction, that is, they are always false, then we can logically derive any desired conclusion from these premises.

The moral of this story is that we should avoid arguments that have premises that form contradictions. Such premises are often called **inconsistent**. Premises that are not inconsistent are called **consistent**. It is not that there is anything logically wrong with inconsistent premises, they are simply of no use to mathematicians, because we can derive anything from them. For example, when non-Euclidean geometry was first discovered in the early nineteenth century, it was important to determine whether the proposed axiom system for such geometry was consistent or not. In many mathematical situations, for example geometry, it is not possible to demonstrate consistency directly via truth tables and the like, but it was eventually shown that non-Euclidean is no less consistent than Euclidean geometry. Because Euclidean geometry is so well studied and so widely used, and its consistency is not generally doubted, it followed that non-Euclidean geometry was no less worthwhile mathematically than Euclidean geometry. See [Tru87, Chapter 7] for details.

Whereas arguments with inconsistent premises are not logically flawed, but rather do not allow for any useful conclusions, we often do encounter logical errors in both formal and informal argumentation. We conclude this section with a brief mention of a few common logical errors, often referred to as fallacies, that are regularly found in attempted mathematical proofs (and elsewhere).

The first two errors we mention involve applications of commonly used non-existent "rules of inference." For example, consider the following argument.

> If Fred eats a good dinner, then he will drink a beer. Fred drank a beer.
> Therefore Fred ate a good dinner.

This argument is definitely invalid. The first premise states that Fred will drink a beer if something happens, namely, if he eats a good dinner. It does not say that he would not drink a beer otherwise. Hence, just because we assume that Fred drank a beer, we cannot conclude anything about Fred's dinner. In symbols, the argument is $(P \rightarrow Q) \wedge Q \Rightarrow P$. There is no such implication, as can be seen by checking the truth table for $[(P \rightarrow Q) \wedge Q] \rightarrow P$, which is not a tautology. This fallacy is known as the fallacy of the converse (and is also known as the fallacy of affirming the consequent).

Our next type of fallacy is seen in the following argument.

> If Senator Bullnose votes himself a raise, then he is a sleazebucket. Senator Bullnose did not vote himself a raise. Therefore the senator is not a sleaze-bucket.

Again this argument is invalid. The first premise says what we could conclude if the senator does a certain thing, namely, votes himself a raise. It does not say anything if that certain thing does not happen. Therefore, just because the senator did not vote himself a raise, we cannot conclude anything about his character—there could be many other things that might raise questions about him. In symbols, the argument here is $(P \rightarrow Q) \wedge \neg P \Rightarrow \neg Q$. Again, there is no such implication, as can be seen by checking the appropriate truth table. This fallacy is known as the fallacy of the inverse (and is also known as the fallacy of denying the antecedent).

The third type of error we mention is of a slightly different nature. Consider the following argument.

If Deirdre has hay fever, then she sneezes a lot. Therefore Deirdre sneezes a lot.

The problem with this argument, which again is invalid, is not the use of an incorrect "rule of inference," but rather the making of an unjustified assumption. If we were also to assume that in fact Deirdre has hay fever, then we could use Modus Ponens to conclude that she sneezes a lot. Without that assumption, however, no such conclusion can be drawn. This fallacy is known as the fallacy of unwarranted assumptions.

The examples we just gave of fallacious arguments might seem so trivial that they are hardly worth dwelling on, not to mention give names to. They are ubiquitous, however, both in everyday usage (in political discussions, for example) and in mathematics classes, and are especially hard to spot when embedded in lengthier and more convoluted argumentation. Hence we alert you to them here. For further discussion of fallacies in formal and informal argumentation, see [KMM80, Section 1.5]. For errors in argumentation involving not only logical mistakes but also rhetorical devices such as appeals to authority, irrelevant circumstances and abusive statements, see [Cop68, Chapter 3].

Exercises

Exercise 1.4.1. For each of the following arguments, if it is valid, give a derivation, and if it is not valid, show why.

(1) $P \wedge Q$
$\dfrac{(P \vee Q) \to R}{R}$

(2) $\neg X \to Y$
$\dfrac{\neg X \to Z}{\neg Z \to \neg Y}$

(3) $E \to F$
$\neg G \to \neg F$
$H \to I$
$\dfrac{E \vee H}{G \vee I}$

(4) $L \to M$
$(M \vee N) \to (L \to K)$
$\dfrac{\neg P \wedge L}{K}$

(5) $P \to Q$
$\neg R \to (S \to T)$
$R \vee (P \vee T)$
$\dfrac{\neg R}{Q \vee S}$

(6) $\neg A \to (B \to \neg C)$
$C \to \neg A$
$(\neg D \vee A) \to \neg \neg C$
$\dfrac{\neg D}{\neg B}$

Exercise 1.4.2. For each of the following arguments, if it is valid, give a derivation, and if it is not valid, show why.

(1) If Fishville is boring, then it is hard to find. If Fishville is not small, then it is not hard to find. Fishville is boring. Therefore Fishville is small.

(2) If the new CD by The Geeks is loud or tedious, then it is not long and not cacophonous. The new CD by The Geeks is tedious. Therefore the CD is not long.

(3) If the food is green, then it is undercooked. If the food is smelly, then it is stale. The food is green or it is stale. Therefore the food is undercooked or it is smelly.

(4) If Susan likes fish, then she likes onions. If Susan does not like garlic, then she does not like onions. If she likes garlic, then she likes guavas. She likes fish or she likes cilantro. She does not like guavas. Therefore, Susan likes cilantro.

(5) It is not the case that Fred plays both guitar and flute. If Fred does not play guitar and he does not play flute, then he plays both organ and harp. If he plays harp, then he plays organ. Therefore Fred plays organ.

(6) If you rob a bank, you go to jail. If you go to jail, you do not have fun. If you have a vacation, you have fun. You rob a bank or you have a vacation. Therefore you go to jail or you have fun.

Exercise 1.4.3. Write a derivation for each of the following arguments, all of which are valid. State whether the premises are consistent or inconsistent

(1) If amoebas can dance, then they are friendly. If amoebas make people sick, then they are not friendly. Amoebas can dance and they make people sick. Therefore people are friendly.

(2) If warthogs are smart, then they are interesting. Warthogs are not interesting or they are sneaky. It is not the case that warthogs are pleasant or not smart. Therefore warthogs are sneaky.

(3) It is not the case that clothes are annoying or not cheap. Clothes are not cheap or they are unfashionable. If clothes are unfashionable they are silly. Therefore clothes are silly.

(4) If music soothes the soul then souls have ears. Music soothes the soul or musicians are calm. It is not the case that souls have ears or musicians are calm. Therefore musicians have souls.

(5) Computers are useful and fun, and computers are time consuming. If computers are hard to use, then they are not fun. If computers are not well designed, then they are hard to use. Therefore computers are well designed.

(6) If Marcus likes pizza then he likes beer. If Marcus likes beer then he does not like herring. If Marcus likes pizza then he likes herring. Marcus likes pizza. Therefore he likes herring pizza.

Exercise 1.4.4. Find the fallacy, or fallacies, in each of the following arguments.

(1) Good fences make good neighbors. Therefore we have good neighbors.

(2) If Fred eats a frog then Susan will eat a snake. Fred does not eat a frog. Therefore Susan does not eat a snake.

(3) The cow moos whenever the pig oinks. The cow moos. Therefore the pig oinks.

(4) A nice day is sufficient for frolicking children or napping adults. Adults are napping. Therefore it is a nice day.

(5) If my rabbit eats a hamburger, then she gets sick. If my rabbit gets sick, then she is unhappy. Therefore my rabbit gets sick.

(6) If Snoozetown elects a mayor, then it will raise taxes. If Snoozetown does not raise taxes, then it will not build a new stadium. Snoozetown does not elect a mayor. Therefore it will not build a new stadium.

1.5 Quantifiers

Our discussion of logic so far has been missing one crucial ingredient used in the formulation of theorems and proofs. We often encounter in mathematics expressions such as "$x^3 \geq 8$," which we might wish to prove. This expression as written is not precise, however, because it does not state which possible values of x are under consideration. Indeed, the expression is not a statement. A more useful expression, which is a statement, would be "$x^3 \geq 8$, for all real numbers $x \geq 2$." The phrase "for all real numbers $x \geq 2$" is an example of a quantifier. The other type of quantifier commonly used is the first part of the statement "there exists a real number x such that $x^2 = 9$." What is common to both these phrases is that they tell us about the variables under consideration; they tell us what the possible values of the variable are, and whether the statement involving the variable necessarily holds for all possible values of the variable or only for some values (that is, one or more value).

The use of quantifiers vastly expands the range of possible statements that can be formed in comparison with the statements that were made in previous sections of this chapter. Quantifiers are so important that the type of logic that involves quantifiers has its own name, which is "first-order" (and is also known as "predicate") logic; the type of logic we looked at previously is called "sentential" (and is also known as "propositional") logic.

Many statements of theorem in mathematics have quantifiers in them, sometimes multiple quantifiers. The importance of quantifiers in rigorous proofs cannot be overestimated. From the author's experience teaching undergraduate mathematics courses, confusion arising out of either the misunderstanding of quantifiers in complicated definitions and theorems, or the ignoring of quantifiers when writing proofs, is the single largest cause of problems for students who are learning to construct proofs. A solid understanding of how to use quantifiers is therefore well worth acquiring.

Quantifiers can arise in a variety of statements. Consider the statement "some people in this room have red hair." Though it might not appear so at first, this statement does inherently have a quantifier, because it could be rephrased as "there exists a person in this room who has red hair." The statement "all cats like to eat all mice" has two quantifiers. We could rephrase this statement as "for each cat x, and each mouse y, cat x likes to eat mouse y." The statement "every person has a mother" combines two different types of quantifiers, because it could be rephrased as "for each person A, there is a woman B such that B is the mother of A." Of course, as with any other type of statement, a statement involving quantifiers is either true or false. The statement "every person has a mother" is true, whereas "every person has a sister" is false.

Quantifiers often occur in both colloquial and mathematical statements, even when they are not mentioned explicitly. Non-explicit quantifiers in colloquial English can occasionally lead to some odd confusions. What does the sentence "someone is hit by a car every hour" mean? Does the same person keep getting hit every hour? In mathematics there is no room for ambiguous statements, and so when we attempt to prove a complicated mathematical statement, it is often useful to start by rephrasing it so as to make the quantifiers explicit.

As a preliminary to our discussion of quantifiers, consider the expression $P =$ "$x + y > 0$." Observe that x and y have the same roles in P. Using P we can form a new expression $Q =$ "for all positive real numbers x, the inequality $x + y > 0$ holds." In contrast to P, there is a substantial difference between the roles of x and y in Q. The symbol x is called a **bound variable** in Q, in that we have no ability to choose which values of x we want to consider. By contrast, the symbol y is called a **free variable** in Q, because its possible values are not limited. Because y is a free variable in Q, it is often useful to write $Q(y)$ instead of Q to indicate that y is free. In P both x and y are free variables, and we would denote that by writing $P(x, y)$.

The difference between a bound variable and a free one can be seen by changing the variables in Q. If we change every occurrence of x to w in Q, we obtain $\hat{Q} =$ "for all positive real numbers w, the inequality $w + y > 0$ holds." For each possible value of y, we observe that $\hat{Q}$ and Q have precisely the same meaning. In other words, if Q were part of a larger expression, then the larger expression would be entirely unchanged by replacing Q with $\hat{Q}$. By contrast, suppose that we change every occurrence of y to z in Q, obtaining $\tilde{Q} =$ "for all positive real numbers x, the inequality $x + z > 0$ holds." Then $\tilde{Q}$ does not have the same meaning as Q, because y and z (over which we have no control in Q and $\tilde{Q}$ respectively) might be assigned different values, for example if Q were part of a larger expression that had both y and z appearing outside Q. In other words, changing the y to z made a difference precisely because y is a free variable in Q.

Observe that an expression with a free variable is not a statement. Our expression Q in the previous paragraph is not a statement because we cannot determine its truth or falsity without knowing something about the possible values of y under consideration. By contrast, the expression "for all positive real numbers x, and all real numbers y, the inequality $x + y > 0$ holds," has no free variables, and it is indeed a statement (which happens to be false).

We are now ready for a closer look at the two types of quantifiers that we will use. Let $P(x)$ be an expression with free variable x. Let U denote a collection of possible values of x. A **universal quantifier** applied to $P(x)$ is the statement, denoted $(\forall x \text{ in } U)P(x)$, which is true if $P(x)$ is true for all possible values of x in U. If the collection U is understood from the context, then we will write $(\forall x)P(x)$.

One way to think of the statement $(\forall x \text{ in } U)P(x)$ is to view it as the conditional statement "if x is in U, then $P(x)$ is true." As we saw in our discussion of conditional statements in Section 1.2, the truth of the statement "if x is in U, then $P(x)$ is true" does not say anything about what happens if x is not in U. That is, if the statement $(\forall x \text{ in } U)P(x)$ is true, it tells us only about $P(x)$ when x is in U; it might or might not

be the case that $P(x)$ is true for some values of x that are not in U, but we cannot tell that from the statement as written.

There are a variety of ways to write $(\forall x \text{ in } U)P(x)$ in English, for example:

For all values of x in U, the statement $P(x)$ is true;
For each x in U, the statement $P(x)$ is true;
The statement $P(x)$ is true for all x in U;
All values of x in U satisfy the $P(x)$.

For example, let $P(\alpha) = $ "person α has red hair," and let W be the collection of all people in the world. The statement $(\forall \alpha \text{ in } W)P(\alpha)$ would mean that "all people in the world have red hair" (which is certainly not a true statement). Let $S(n) = $ "n is a perfect square greater than 1," and $C(n) = $ "n is a composite number" (a composite number is an integer that is not a prime number), where the collection of possible values of n is the integers. The statement $(\forall n)[S(n) \rightarrow C(n)]$ can be written in English as "for all integers n, if n is a perfect square greater than 1, then n is a composite number" (this statement happens to be true). We could rephrase this statement by saying "for all perfect squares n greater than 1, the number n is a composite number," or even more concisely as "all perfect squares greater than 1 are composite," where it is taken as implicitly known that the terms "perfect square" and "composite" apply only to integers (and not other types of numbers).

Changing the collection U in a statement of the form $(\forall x \text{ in } U)P(x)$ can change the truth or falsity of the statement, so that the choice of U is crucial. For example, let $R(x) = $ "the number x has a square root." If we let U be the collection of positive real numbers, then the statement $(\forall x \text{ in } U)R(x)$ is true. On the other hand, if we let W be the collection of all real numbers, then the statement $(\forall x \text{ in } W)R(x)$ is certainly false.

For the sake of completeness, we need to allow the case where the collection U has nothing in it. In that case, the statement $(\forall x \text{ in } U)P(x)$ is always true, no matter what $P(x)$ is, for the following reason. The statement "$(\forall x \text{ in } U)P(x)$" is equivalent to the statement "if x is in U, then $P(x)$ is true." When the collection U has nothing in it, then the statement "x is in U" is false, and hence the conditional statement "if x is in U, then $P(x)$ is true" is true.

For the other type of quantifier we are interested in, once again let $P(x)$ be a statement with free variable x, and let U denote a collection of possible values of x. An **existential quantifier** applied to $P(x)$ is the statement, denoted $(\exists x \text{ in } U)P(x)$, which is true if $P(x)$ is true for at least one value of x in U. If the collection U is understood from the context, then we will write $(\exists x)P(x)$. Observe that if the collection U has nothing in it, then the statement $(\exists x)P(x)$ is false.

It is important to note that the phrase "at least one value of x in U" means one or more, possibly many, or even all x in U. In particular, if $(\forall x \text{ in } U)P(x)$ is true, then $(\exists x \text{ in } U)P(x)$ is true, except in the special case that U has nothing in it. Of course, the statement $(\exists x \text{ in } U)P(x)$ does not imply that $(\forall x \text{ in } U)P(x)$ is true, except in the case that U has either one thing or nothing in it.

There are a variety of ways to write $(\exists x \text{ in } U)P(x)$ in English, for example:

There exists some x in U such that $P(x)$ holds;

There is x in U such that $P(x)$ holds;

There exists at least one x in U such that $P(x)$ holds;

For some value of x in U, the condition $P(x)$ holds;

It is the case that $P(x)$ is true for some x in U.

Let $Q(r) =$ "person r has brown hair," and let W be the collection of all people in the world. Then the statement $(\exists r$ in $W)Q(r)$ would mean that "there is someone with brown hair," or equivalently "some people have brown hair" (which is a true statement). Let $E(m) =$ "m is an even number" and let $M(m) =$ "m is a prime number," where the collection of possible values of m is the integers. The statement "some integers are even and prime" can be expressed symbolically by first rephrasing it as "there exists x such that x is even and x is prime," which is $(\exists x)[E(x) \wedge M(x)]$ (this statement is true, because 2 is both even and prime).

The reader might wonder why we use only the above two types of quantifiers, and whether other quantifiers are needed. For example, the statement "no dog likes cats" clearly has a quantifier, but which quantifier is it? If we let U be the collection of all dogs, and if we let $P(x) =$ "dog x likes cats," then our statement is "there is no x in U such that $P(x)$." However, the expression "there is no x in U," though certainly a quantifier of some sort, is neither a universal quantifier nor an existential quantifier. Fortunately, rather than needing to define a third type of quantifier to be able to handle the present statement, we can rewrite our statement in English as "every dog does not like cats," and in symbols that becomes $(\forall x$ in $U)(\neg P(x))$. In general, all the quantification that we need in mathematics can be expressed in terms of universal quantifiers and existential quantifiers.

We can form statements with more than one quantifier, as long as different quantifiers involve different variables. Suppose that $P(x,y) =$ "$x + y^2 = 3$," where x and y are real numbers. The statement $(\forall y)(\exists x)P(x,y)$ can then be written in English as "for all y there exists some x such that $x + y^2 = 3$," or equivalently "for each y there is some x such that $x + y^2 = 3$." This statement is true, because for any real number y we can always solve for x in terms of y, yielding $x = 3 - y^2$. If we reverse the order of the quantifiers, we obtain the statement $(\exists x)(\forall y)P(x,y)$, which can be written in English as "there exists some x such that for all y, the equation $x + y^2 = 3$ holds." This statement is clearly false, because for any given x, there can be at most two values of y such that $x + y^2 = 3$. The order of the quantifiers therefore matters.

When attempting to prove a theorem, the statement of which involves multiple quantifiers, it is sometimes useful to translate the statement of the theorem into symbols, to help keep track of the meaning of the quantifiers. Suppose that we are given the statement "if x is a non-negative real number, then x is a perfect square." This statement can be interpreted as a doubly quantified statement by rephrasing it as "for each non-negative real number x, there is some real number y such that $x = y^2$." Written symbolically, the statement is

$$(\forall x \text{ in the non-negative real numbers})(\exists y \text{ in the real numbers})(x = y^2).$$

Once again, it can be seen that reversing the order of the quantifiers in this statement would change its meaning. A lack of attention to the order of quantifiers can easily

lead to mistakes in proving theorems that have statements with multiple quantifiers. A very important occurrence of the importance of the order of multiple quantifiers is in the "ε-δ" proofs treated in real analysis courses; see Section 7.8 for a similar type of proof from real analysis, and see any introductory real analysis text for a detailed discussion of ε-δ proofs.

A non-mathematical example of a statement that can be clarified by writing it symbolically in terms of quantifiers is the statement "someone is hit by a car every hour," which we encountered previously. Suppose that the possible values of x are all people, that the possible values of t are all hour-long time intervals that start precisely on the hour and that $C(x,t) = $ "person x is hit by a car at time t." The statement "someone is hit by a car every hour" can then be written symbolically as $(\forall t)(\exists x)C(x,t)$. Once again, the order of the quantifiers matters. The statement $(\exists x)(\forall t)C(x,t)$ would mean that there is a single person who gets hit by a car every hour, which is not what the original statement intended to say.

There are eight possible generic ways of writing two quantifiers in a statement that has variables. Most of the eight possibilities have different meanings from one another. Suppose, for example, that the possible values of x are all people, the possible values of y are all types of , and that $L(x,y) = $ "person x likes to eat fruit y." The eight ways of applying two quantifiers to $L(x,y)$ are as follows.

(1) $(\forall x)(\forall y)L(x,y)$. This statement can be written in English as "for each person x, for each type of fruit y, person x likes to eat y," and more simply as "every person likes every type of fruit." To verify whether this statement is true, we would have to ask each person in the world if she likes every type of fruit; if even one person does not like one type of fruit, then the statement would be false.

(2) $(\forall y)(\forall x)L(x,y)$. This statement can be written as "for each type of fruit y, for each person x, we know x likes to eat y," and more simply as "every type of fruit is liked by every person." This statement is equivalent to Statement 1.

(3) $(\forall x)(\exists y)L(x,y)$. This statement can be written as "for each person x, there is a type of fruit y such that x likes to eat y," and more simply as "every person likes at least one type of fruit." To verify whether this statement is true, we would have to ask each person in the world if she likes some type of fruit; if at least one person does not like any type of fruit, then the statement would be false.

(4) $(\exists x)(\forall y)L(x,y)$. This statement can be written as "there is a person x such that for all types of fruit y, person x likes to eat y," and more simply as "there is a person who likes every type of fruit." To verify whether this statement is true, we would start asking one person at a time if she likes every type of fruit; as soon as we found one person who answers yes, we would know that the statement is true, and we could stop asking more people. If no such person is found, then the statement would be false.

(5) $(\forall y)(\exists x)L(x,y)$. This statement can be written as "for each type of fruit y, there is a person x such that x likes to eat y," and more simply as "every type

of fruit is liked by at least one person." To verify whether this statement is true, we would have to list all the types of fruit, and then for each type of fruit, ask one person at a time whether she likes the fruit; once we found someone who liked that fruit, we could move onto the next fruit, and again ask one person at a time about it. For the statement to be true, we would have to find at least one person per fruit, though the same person could be selected for more than one fruit.
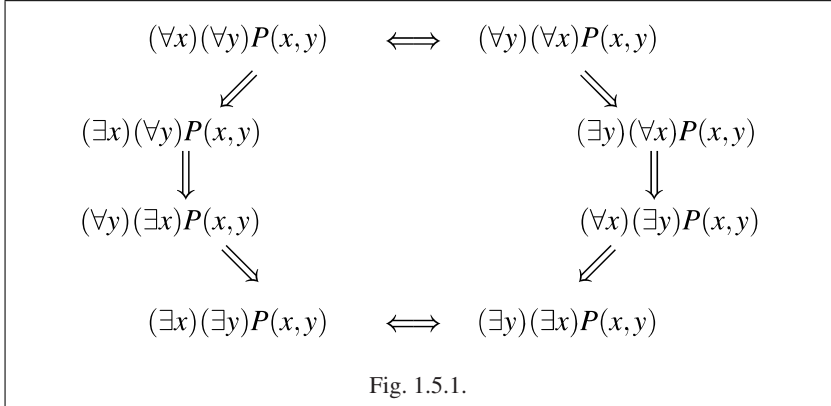
(6) $(\exists y)(\forall x)L(x,y)$. This statement can be written as "there is a type of fruit y such that for all persons x, we know that x likes to eat y," and more simply as "there is a type of fruit that all people like." To verify whether this statement is true, we would have to list all the types of fruit, and then for one type of fruit at a time, ask each person in the world if she likes that type of fruit; as soon as we found one type of fruit that everyone likes, we would know that the statement is true, and we could stop asking about more types of fruit.

(7) $(\exists x)(\exists y)L(x,y)$. This statement can be written as "there is a person x such that there is a type of fruit y such that x likes to eat y," and more simply as "there is a person who likes at least one type of fruit." To verify whether this statement is true, we would have to start asking one person at a time if she likes some type of fruit; as soon as we found one person who answers yes, we would know that the statement is true, and we could stop asking more people.

(8) $(\exists y)(\exists x)L(x,y)$. This statement can be written as "there is a type of fruit y such that there is a person x such that x likes to eat y," and more simply as "there is a type of fruit that is liked by at least one person." This statement is equivalent to Statement 7.

In the above example we had eight cases, because there were two variables. When there are more variables, then the number of cases will be even larger. Also, we observe that whereas most of the cases in the above example are different from one another, there exist some examples of statements where some of the distinct cases above happen to coincide (for example, where the roles of x and y in $P(x,y)$ are equal).

Some statements with quantifiers imply others. For the sake of avoiding special cases, we will assume that the collection U, which is often not written explicitly but is implicitly assumed, always has something it it. With one variable, we saw that $(\forall x)P(x)$ implies $(\exists x)P(x)$. With two variables, the various implications are shown in Figure 1.5.1.

We now look at the negation of statements with quantifiers. For example, let Q = "all people have red hair." The negation of this statement can, most directly, be written as $\neg Q$ = "it is not the case that all people have red hair." For this last statement to be true, it would have to be the case that at least one person does not have red hair. Hence, we could rewrite $\neg Q$ as "there are people who do not have red hair." We can rewrite Q and $\neg Q$ using symbols as follows. Let $P(x)$ = "person x has red hair." Then $Q = (\forall x)P(x)$, and $\neg Q = (\exists x)(\neg P(x))$. It is very important

to recognize that $\neg Q$ is not the same as the statement "all people do not have red hair," which in symbols would be written $(\forall x)(\neg P(x))$. This last statement is much stronger than is needed to say that Q is false. The effect of the negation of Q is to change the quantifier, as well as to negate the statement being quantified.

$$(\forall x)(\forall y)P(x,y) \quad\Longleftrightarrow\quad (\forall y)(\forall x)P(x,y)$$

$$(\exists x)(\forall y)P(x,y) \qquad\qquad\qquad (\exists y)(\forall x)P(x,y)$$

$$(\forall y)(\exists x)P(x,y) \qquad\qquad\qquad (\forall x)(\exists y)P(x,y)$$

$$(\exists x)(\exists y)P(x,y) \quad\Longleftrightarrow\quad (\exists y)(\exists x)P(x,y)$$

Fig. 1.5.1.

Similar reasoning holds for the negation of a statement with an existential quantifier. Let $R =$ "there is a pig with wings." The negation of this statement can be written most directly as $\neg R =$ "it is not the case that there is a pig with wings," and more simply as $\neg R =$ "all pigs have no wings." (It would be more natural in English to say "no pigs have wings," but that phrasing is not useful to us here, because we do not have a quantifier that corresponds directly to "no pigs.") Let $W(x) =$ "pig x has wings." Then $R = (\exists x)W(x)$, and $\neg R = (\forall x)(\neg W(x))$. Observe that $\neg R$ is not the same as the statement "there is a pig with no wings," which in symbols would be written $(\exists x)(\neg W(x))$. This last statement is much weaker than is needed to say that R is false. Again, the effect of the negation of R is to change the quantifier, as well as to negate the statement being quantified.

The two cases examined above are completely typical, as we now see.

Fact 1.5.1. *Let $P(x)$ be a statement with free variable x, which takes values in some collection U.*

1. $\neg[(\forall x \text{ in } U)P(x)] \Leftrightarrow (\exists x \text{ in } U)(\neg P(x))$.
2. $\neg[(\exists x \text{ in } U)P(x)] \Leftrightarrow (\forall x \text{ in } U)(\neg P(x))$.

Unlike the equivalences discussed in Section 1.3, we cannot use truth tables to verify the equivalences in Fact 1.5.1, though they are true nonetheless, based on the meanings of the quantifiers.

We can use the above equivalences to negate statements with more than one quantifier. For example, suppose that f is a function that takes real numbers to real numbers (for example $f(x) = x^2$ for all real numbers x). Let $Q =$ "for each real number w, there is some real number y such that $f(y) = w$." We would like to find $\neg Q$. We start

by writing Q symbolically. Let $P(w, y) =$ "$f(y) = w$." Then $Q = (\forall w)(\exists y)P(w, y)$. Using our equivalences we have

$$\neg Q \Leftrightarrow \neg[(\forall w)(\exists y)P(w, y)] \Leftrightarrow (\exists w)\neg[(\exists y)P(w, y)]$$
$$\Leftrightarrow (\exists w)(\forall y)(\neg P(w, y)).$$

Rephrasing this last expression in English yields $\neg Q =$ "there exists a real number w such that for all real numbers y, the relation $f(y) \neq w$ holds." It is often easier to negate statements with multiple quantifiers by first translating them into symbolic form, negating them symbolically and then translating back into English. With a bit of practice it is possible to negate such statements directly in English as well, as long as the statements are not too complicated.

Finally, we turn to rules of inference with quantifiers. There are four such rules of inference, and while their use requires a bit more care than the rules of inference in Section 1.4, they are used for the same purpose, which is to show the validity of logical arguments.

Universal Instantiation $\qquad \dfrac{(\forall x \text{ in } U)P(x)}{P(a)}$

where a is anything in U.

Existential Instantiation $\qquad \dfrac{(\exists x \text{ in } U)P(x)}{P(b)}$

where b is something of U, and where the symbol "b" does not already have any other meaning in the given argument.

Universal Generalization $\qquad \dfrac{P(c)}{(\forall x \text{ in } U)P(x)}$

where c is an arbitrary thing in U.

Existential Generalization $\qquad \dfrac{P(d)}{(\exists x \text{ in } U)P(x)}$

where d is something in U.

Observe the restrictions on the variables used in each rule. For example, in Existential Instantiation, it is important that when we deduce from $(\exists x \text{ in } U)P(x)$ that $P(b)$ holds for some b in U, we cannot assume that the letter "b" refers to any other symbol already being used in the argument. Hence we need to choose a new letter, rather than one already used for something else. In Universal Generalization, when we deduce from $P(c)$ that $(\forall x \text{ in } U)P(x)$, it is crucial that c be an arbitrarily chosen member of U. Otherwise, we could not conclude that $P(x)$ is true for all x in U. This last observation is crucial when we attempt to prove mathematical statements involving universal quantifiers, as we will see in Section 2.5, and throughout this book. Though we will not necessarily be referring to them by name, these four rules

of inference will be used regularly in our mathematical proofs. See [Cop68, Chapter 10] for further discussion of these rules of inference.

An example of a simple logical argument involving quantifiers is the following.

Every cat that is nice and smart likes chopped liver. Every Siamese cat is nice. There is a Siamese cat that does not like chopped liver. Therefore there is a stupid cat.

(We are assuming here that "stupid" is the negation of "smart.") To translate this argument into symbols, let U be the collection of all cats, let $N(x) =$ "cat x is nice," let $S(x) =$ "cat x is smart," let $C(x) =$ "cat x likes chopped liver" and let $T(x) =$ "cat x is Siamese." The argument then becomes

$$(\forall x \text{ in } U)[(N(x) \wedge S(x)) \rightarrow C(x)]$$
$$(\forall x \text{ in } U)[T(x) \rightarrow N(x)]$$
$$\underline{(\exists x \text{ in } U)[T(x) \wedge \neg C(x)]}$$
$$(\exists x \text{ in } U)[\neg S(x)].$$

A derivation for this argument, using rules of inference from Section 1.4 as well as from this section, is

(1)	$(\forall x \text{ in } U)[(N(x) \wedge S(x)) \rightarrow C(x)]$	
(2)	$(\forall x \text{ in } U)[T(x) \rightarrow N(x)]$	
(3)	$\underline{(\exists x \text{ in } U)[T(x) \wedge \neg C(x)]}$	
(4)	$T(a) \wedge \neg C(a)$	(3), Existential Instantiation
(5)	$\neg C(a)$	(4), Simplification
(6)	$T(a)$	(4), Simplification
(7)	$T(a) \rightarrow N(a)$	(2), Universal Instantiation
(8)	$N(a)$	(7), (6), Modus Ponens
(9)	$\neg\neg N(a)$	(8), Double Negation
(10)	$(N(a) \wedge S(a)) \rightarrow C(a)$	(1), Universal Instantiation
(11)	$\neg(N(a) \wedge S(a))$	(10), (5), Modus Tollens
(12)	$\neg N(a) \vee \neg S(a)$	(11), De Morgan's Law
(13)	$\neg S(a)$	(12), (9), Modus Tollendo Ponens
(14)	$(\exists x \text{ in } U)[\neg S(x)]$	(13), Existential Generalization.

Observe that in line (4) we chose some letter "a" that was not in use prior to that line, because we are using Existential Instantiation. We needed to use that rule of inference at that point in the derivation in order to remove the quantifier in line (3) of the premises, which then allows us to use the rules of inference given in Section 1.4 (which did not involve quantifiers). In lines (7) and (10) we were free to use the same letter "a" as in line (4), because Universal Instantiation allows us to choose anything in U that we want.

<div align="center">

Exercises

</div>

Exercise 1.5.1. Suppose that the possible values of x are all people. Let $Y(x) =$ "x has green hair," let $Z(x) =$ "x likes pickles" and let $W(x) =$ "x has a pet frog." Translate the following statements into words.

(1) $(\forall x)Y(x).$
(2) $(\exists x)Z(x).$
(3) $(\forall x)[W(x) \wedge Z(x)].$

(4) $(\exists x)[Y(x) \rightarrow W(x)].$
(5) $(\forall x)[W(x) \leftrightarrow \neg Z(x)].$

Exercise 1.5.2. Suppose that the possible values of x and y are all cars. Let $L(x,y) =$ "x is as fast as y," let $M(x,y) =$ "x is as expensive as y" and let $N(x,y) =$ "x is as old as y." Translate the following statements into words.

(1) $(\exists x)(\forall y)L(x,y).$
(2) $(\forall x)(\exists y)M(x,y).$

(3) $(\exists y)(\forall x)[L(x,y) \vee N(x,y)].$
(4) $(\forall y)(\exists x)[\neg M(x,y) \rightarrow L(x,y)].$

Exercise 1.5.3. Suppose that the possible values of y are all cows. Let $P(y) =$ "y is brown," let $Q(y) =$ "y is four years old" and let $R(y) =$ "y has white spots." Translate the following statements into symbols.

(1) There is a brown cow.
(2) All cows are four years old.
(3) There is a brown cow with white spots.
(4) All four-year-old cows have white spots.
(5) There exists a cow such that if it is four years old, then it has no white spots.
(6) All cows are brown if and only if they are not four years old.
(7) There are no brown cows.

Exercise 1.5.4. Suppose that the possible values of p and q are all fruit. Let $A(p,q) =$ "p tastes better than q," let $B(p,q) =$ "p is riper than q" and let $C(p,q) =$ "p is the same species as q." Translate the following statements into symbols.

(1) There is a fruit such that all fruit taste better than it.
(2) For every fruit, there is a fruit that is riper than it.
(3) There is a fruit such that all fruit taste better than it and is not riper than it.
(4) For every fruit, there is a fruit of the same species that does not taste better than it.

Exercise 1.5.5. Convert the following statements, which do not have their quantifiers explicitly given, into statements with explicit quantifiers, both in symbols and in English.

(1) People are nice.
(2) Someone gave me a present.
(3) Cats like eating fish and taking naps.
(4) I liked one of the books I read last summer.
(5) No one likes ice cream and pickles together.

Exercise 1.5.6. Write a negation of each statement. Do not write the word "not" applied to any of the objects being quantified (for example, do not write "Not all boys are good" for Part (1) of this exercise).

(1) All boys are good.

(2) There are bats that weigh 50 lbs or more.

(3) The equation $x^2 - 2x > 0$ holds for all real numbers x.

(4) Every parent has to change diapers.

(5) Every flying saucer is aiming to conquer some galaxy.

(6) There is an integer n such that n^2 is a perfect number.

(7) There is a house in Kansas such that everyone who enters the house goes blind.

(8) Every house has a door that is white.

(9) At least one person in New York City owns every book published in 1990.

Exercise 1.5.7. Negate the following statement: There exists an integer Q such that for all real numbers $x > 0$, there exists a positive integer k such that $\ln(Q - x) > 5$ and that if $x \leq k$ then Q is cacophonous. (The last term used in this exercise is meaningless.)

Exercise 1.5.8. Negate the following statement: For every real number $\varepsilon > 0$ there exists a positive integer k such that for all positive integers n, it is the case that $|a_n - k^2| < \varepsilon$.

Exercise 1.5.9. Let x be a real number. The number x is **gelatinous** if it is both phlegmatic, and if for every integer n there is some real number y such that y^2 upper-encapsulates x or $y + n$ lower-encapsulates x. How would you characterize a non-gelatinous real number x? (The terms used in this exercise are meaningless.)

Exercise 1.5.10. Someone claims that the argument

$$\frac{\begin{array}{l}(\exists x \text{ in } U)[P(x) \wedge Q(x)] \\ (\exists x \text{ in } U)[M(x)]\end{array}}{(\exists x \text{ in } U)[M(x) \wedge Q(x)]}$$

is valid, using the alleged derivation

(1) $(\exists x \text{ in } U)[P(x) \wedge Q(x)]$	
(2) $(\exists x \text{ in } U)[M(x)]$	
(3) $P(a) \wedge Q(a)$	(1), Existential Instantiation
(4) $Q(a)$	(3), Simplification
(5) $M(a)$	(2), Existential Instantiation
(6) $M(a) \wedge Q(a)$	(5), (4), Adjunction
(7) $(\exists x \text{ in } U)[M(x) \wedge Q(x)]$	(6), Existential Generalization.

Find the flaw(s) in the derivation.

Exercise 1.5.11. Write a derivation for each of the following arguments.

(1) $$\frac{\begin{array}{l}(\forall x \text{ in } U)[R(x) \rightarrow C(x)] \\ (\forall x \text{ in } U)[T(x) \rightarrow R(x)]\end{array}}{(\forall x \text{ in } U)[\neg C(x) \rightarrow \neg T(x)].}$$

(2) $(\forall a$ in $V)[N(a) \rightarrow B(a)]$
$\underline{(\exists b$ in $V)[N(b) \wedge D(b)]}$
$(\exists c$ in $V)[B(c) \wedge D(c)]$.

(3) $(\forall x$ in $Z)[(A(x) \rightarrow R(x)) \vee T(x)]$
$(\exists x$ in $Z)[T(x) \rightarrow P(x)]$
$\underline{(\forall x$ in $Z)[A(x) \wedge \neg P(x)]}$
$(\exists x$ in $Z)[R(x)]$.

(4) $(\forall x$ in $W)(\exists y$ in $W)[E(x) \rightarrow (M(x) \vee N(y))]$
$\neg(\forall x$ in $W)[M(x)]$
$\underline{(\forall x$ in $W)[E(x)]}$
$(\exists x$ in $W)[N(x)]$.

Exercise 1.5.12. Write a derivation for each of the following arguments.

(1) Every fish that is bony is not pleasant to eat. Every fish that is not bony is slimy. Therefore every fish that is pleasant to eat is slimy.

(2) Each high school student in Slumpville who takes an honors class is cool. There is a high school student in Slumpville who is smart and not cool. Therefore there is a high school student in Slumpville who is smart and not taking an honors class.

(3) Every baby who eats will make a mess and drool. Every baby who drools will smile. There is a baby who eats and screams. Therefore there is a baby who smiles.

(4) Every cockroach that is clever eats garbage. There is a cockroach that likes dirt or does not like dust. For each cockroach, it is not the case that it likes dirt or eats garbage. Therefore there is a cockroach such that it is not the case that if it is not clever then it likes dust.

2

Strategies for Proofs

Rigour is to the mathematician what morality is to men.

– André Weil (1906–1998)

2.1 Mathematical Proofs—What They Are and Why We Need Them

Not all mathematics involves proofs. We learn a good bit of arithmetic in grade school long before we learn how to prove that the rules of arithmetic are correct. Mathematics originated in the ancient world, in various cultures, prior to the notion of proof. It was the contribution of the ancient Greeks (who, contrary to popular misconception, did not invent mathematics, nor even geometry) to bring the notion of proof into mathematics. The first use of proof is generally attributed to Thales of Miletus, who lived in the sixth century B.C.E. Euclid, who lived in Alexandria in the third century B.C.E., brought the notion of proofs based on axioms to its first peak of success. See [Hea21] for a discussion of ancient Greek mathematics.

Euclid used an axiomatic system—which is needed for proofs—in the field of geometry. Today, virtually all branches of pure mathematics are based on axiomatic systems, and work in pure mathematics involves the construction of rigorous proofs for new theorems. Much of the great mathematics of the past has been recast with a precision missing from its original treatment. Abstract algebra, for example, which received its modern form only in the last one hundred years, reconstructs the elementary algebra studied in high school in a rigorous, axiomatic fashion. A lot of applied mathematics today also has rigorous foundations (though the work of applied mathematicians, while no less challenging than pure mathematics, is not always oriented toward proofs).

Be the above as it may, the importance of proofs should be put in the proper perspective. Intuition, experimentation and even play are no less important in today's mathematical climate than rigor, because it is only by our intuition that we decide what new results to try to prove. The relation between intuition and formal rigor is not a trivial matter. Formal proofs and intuitive ideas essentially occupy different realms,

and we cannot "prove" that an intuitive idea is true. Instead, there is essentially a dialectical relationship between intuition and rigor. We set up formal systems that mirror our intuition as closely as possible; we then use what we prove rigorously to further our intuitive understanding, which in turn points to new theorems requiring rigorous proofs, and so forth.

Mathematics has moved over time in the direction of ever greater rigor, though why that has happened is a question we leave to historians of mathematics to explain. We can, nonetheless, articulate a number of reasons why mathematicians today use proofs. The main reason, of course, is to be sure that something is true. Contrary to popular misconception, mathematics is not a formal game in which we derive theorems from arbitrarily chosen axioms. Rather, we discuss various types of mathematical objects, some geometric (for example, circles), some algebraic (for example, polynomials), some analytic (for example, derivatives) and the like. To understand these objects fully, we need to use both intuition and rigor. Our intuition tells us what is important, what we think might be true, what to try next and so forth. Unfortunately, mathematical objects are often so complicated or abstract that our intuition at times fails, even for the most experienced mathematicians. We use rigorous proofs to verify that a given statement that appears intuitively true is indeed true.

Another use of mathematical proofs is to explain why things are true, though not every proof does that. Some proofs tell us that certain statements are true, but shed no intuitive light on their subjects. Other proofs might help explain the ideas that underpin the result being proved; such proofs are preferable, though any proof, even if non-intuitive, is better than no proof at all. A third reason for having proofs in mathematics is pedagogical. A student (or experienced mathematician for that matter) might feel that she understands a new concept, but it is often only when attempting to construct a proof using the concept that a more thorough understanding emerges. Finally, a mathematical proof is a way of communicating to another person an idea that one person believes intuitively, but the other does not.

What does a rigorous proof consist of? The word "proof" has a different meaning in different intellectual pursuits. A "proof" in biology might consist of experimental data confirming a certain hypothesis; a "proof" in sociology or psychology might consist of the results of a survey. What is common to all forms of proof is that they are arguments that convince experienced practitioners of the given field. So too for mathematical proofs. Such proofs are, ultimately, convincing arguments that show that the desired conclusions follow logically from the given hypotheses.

There is no formal definition of proof that mathematicians use (except for mathematical logicians, when they develop formal theories of proofs, but these theories are distinct from the way mathematicians go about their daily business). Although we briefly discussed rules of inference and logical derivations in Section 1.4, what we are really interested in for the rest of this book is the way contemporary mathematicians do proofs, in order to prepare you for the kinds of proofs and basic mathematical concepts you will encounter in advanced mathematics courses.

Mathematicians who are not logicians virtually never write proofs as strings of logical symbols and rules of inference, for a number of reasons. First, and foremost, mathematical proofs are often much too long and complicated to be conve-

niently broken down into the two-column (statement-justification) format. Second, the mathematical ideas of the proof, not its logical underpinnings, are the main issue on which we want to focus, and so we do not even mention the rules of logical inference used, but rather mention only the mathematical justification of each step. Second, mathematicians who are not logicians, which means most mathematicians, find long strings of logical symbols not only unpleasant to look at, but in most cases rather difficult to follow. See [EFT94, pp. 70–71] for a fully worked out example of putting a standard mathematical proof in group theory into a two-column format using formal logic. The mathematical result proved in that example is given in Exercise 7.2.8; see Sections 7.2 and 7.3 for a brief introduction to groups. One look at the difference between the mathematicians' version of the proof and the logicians' version, in terms of both length and complexity, should suffice to convince the reader why mathematicians do things as they do.

To some extent mathematicians relate to proofs the way the general public often reacts to art—they know it when they see it. But a proof is not like a work of modern art, where self-expression and creativity are key, and all rules are to be broken, but rather like classical art that followed formal rules. (This analogy is not meant as an endorsement of the public's often negative reaction to serious modern art—classical art simply provides the analog we need here.) Also similarly to art, learning to recognize and construct rigorous mathematical proofs is accomplished not by discussing the philosophy of what constitutes a proof, but by learning the basic techniques, studying correct proofs, and, most importantly, doing lots of them. Just as art criticism is one thing and creating art is another, philosophizing about mathematics and doing mathematics are distinct activities (though of course it helps for the practitioner of each to know something about the other). For further discussion about the conceptual nature of proofs, see [Die92, Section 3.2] or [EC89, Chapter 5], and for more general discussion about mathematical activity see [Wil65] or [DHM95].

Ultimately, a mathematical proof is a convincing argument that starts from the premises, and logically deduces the desired conclusion. How someone may have thought of a proof is one thing, but the proof itself has to proceed logically from start to finish. The distinction between a valid mathematical proof itself and how it was thought of is something that is very important to keep in mind when you work on your own proofs. When solving a problem, you first try all sorts of approaches to find something that works, perhaps starting with the hypotheses and working forwards, or starting with the conclusion and working backwards, or some combination of the two. Whatever your explorations might be, a record of such exploration should never be mistaken for a final proof. Confusing the exploration with the proof is a very common mistake for students first learning advanced mathematics. We will see some examples of this distinction later on.

What is it that we prove in mathematics? We prove statements, which are usually called theorems, propositions, lemmas, corollaries and exercises. There is not much difference between these types of statements; all need proofs. Theorems tend to be important results; propositions are usually slightly less important than theorems; lemmas are statements that are used in the proofs of other results; corollaries are statements that follow easily from other results; exercises are statements that are

left to the reader to prove. When discussing proofs, we will generically refer to "the-orems" when we mean any of theorems, propositions and the like.

Let us examine the statement of a very famous theorem.

Theorem 2.1.1 (**Pythagorean Theorem**). *Let* $\triangle ABC$ *be a right triangle, with sides of length a, b and c, where c is the length of the hypotenuse. Then* $a^2 + b^2 = c^2$.

When asked what the Pythagorean Theorem says, students often state "$a^2 + b^2 = c^2$." This expression alone is not the statement of the theorem—indeed, it is not a statement at all. Unless we know that a, b and c are the lengths of the sides of a right triangle, with c the length of the hypotenuse, we cannot conclude that $a^2 + b^2 = c^2$. (The formula $a^2 + b^2 = c^2$ is never true for the sides of a non-right triangle.) It is crucial to state theorems with all their hypotheses if we want to be able to prove them.

We will not give a proof of the Pythagorean Theorem; see [Loo40] for a variety of proofs. Rather, we want to consider its logical form. Although the words "if ... then" do not appear in the statement of the theorem, the statement is nonetheless a conditional statement (as discussed in Section 1.2). If we let P = "a, b and c are the lengths of the sides of a right triangle, with c the length of the hypotenuse," and let Q = "$a^2 + b^2 = c^2$," then the theorem has the form $P \rightarrow Q$. Many (if not all) statements of theorems are essentially conditional statements, or combinations of them, even though the words "if ... then" do not appear explicitly. A proof of a theorem is therefore an argument that shows that one thing implies another, or a combination of such arguments. It is usually much easier to formulate proofs for theorems when we recognize that they have the form $P \rightarrow Q$, even if they are not given to us in that form.

Theorems are not proved in a vacuum. To prove one theorem, we usually need to use various relevant definitions, and theorems that have already been proved. If we do not want to keep going backwards infinitely, we need to start with some objects that we use without definition, as well as some facts about these objects that are assumed without proof. Such facts are called axioms, and a body of knowledge that can be derived from a set of axioms is called an axiomatic system. In modern abstract mathematics, we take set theory as our basis for all arguments. In each branch of mathematics, we then give specific axioms for the objects being studied. For example, in abstract algebra, we study constructs such as groups, rings and fields, each of which is defined by a list of axioms; the axioms for groups are given in Section 7.2.

In Chapters 3–6 we will discuss sets, and various basic constructs using sets such as functions and relations, which together form the basis for much of modern mathematics. Our concern in the present chapter, by contrast, is not with the basis upon which we rely when we construct proofs, but rather the construction of proofs themselves. It may appear as if we are doing things backwards, in that we are not starting with what we say is the basis for modern mathematics, but we want to be able to give proofs about sets in Chapter 3, so we need to know how to write proofs before discussing set theory. As a basis for our work in the present chapter, we will make use of standard definitions and properties of the familiar number systems such as the integers, rational numbers and real numbers. We will assume that the reader is

informally familiar with these numbers. See the Appendix for a brief list of some of the standard properties of the real numbers.

We conclude this section with our first example of a proof. You are probably familiar with the statement "the sum of even numbers is even." This statement can be viewed in the form $P \rightarrow Q$ if we look at it properly, because it actually says "if n and m are even numbers, then $n + m$ is an even number." To construct a rigorous proof of our statement (as well as the corresponding result for odd numbers), we first need precise definitions of the terms involved.

Our theorem is concerned with the integers, that is, the numbers

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots,$$

and so we need to assume that we know what the integers are, that we have the operations addition, subtraction, multiplication and division, and that these operations satisfy standard properties, for example the Distributive Law. Using only those standard facts about the integers, we can make the following definition, which is the basis for our theorem and its proof.

Definition 2.1.2. Let n be an integer. The number n is **even** if there is some integer k such that $n = 2k$. The number n is **odd** if there is some integer j such that $n = 2j + 1$. $\triangle$

As the reader knows intuitively, and as we will prove in Corollary 5.2.6, every integer is either even or odd, but not both.

We are now ready to state and prove our theorem. This result may seem rather trivial, but our point here is to see a properly done proof, not to learn an exciting new result about numbers.

Theorem 2.1.3. *Let n and m be integers.*

1. *If n and m are both even, then $n + m$ is even.*
2. *If n and m are both odd, then $n + m$ is even.*
3. *If n is even and m is odd, then $n + m$ is odd.*

Proof.

(1). Suppose that n and m are both even. Then there exist integers k and j such that $n = 2k$ and $m = 2j$. Then

$$n + m = 2k + 2j = 2(k + j).$$

Because k and j are integers, so is $k + j$. Hence $m + n$ is even.

(2) & (3). These two parts are proved similarly to Part (1), and the details are left to the reader. $\square$

There is a fourth possible case we did not state in Theorem 2.1.3, namely, the case when n is odd and m is even, because that case is really no different from Part (3) of the theorem, and hence it would not tell us anything new; it makes no difference whether we call the even number n and the odd number m, or vice versa.

The proof of Part (1) of Theorem 2.1.3 is quite simple, but there are a few features worth mentioning, because they are typical of what is found in virtually all our subsequent proofs (and in the proofs you will need to write). First, the proof relies completely on the definition of what it means to be an even or an odd integer. In a large number of proofs, going back to the formal definitions involved is the key step; forgetting to do so is a major source of error by students who are first learning about proofs.

Second, observe that the proof is written in grammatically correct English. Complete sentences are used, with proper punctuation. Each sentence begins with a capital letter, and ends with a period, even if the end of the sentence is in a displayed equation. Mathematical formulas and symbols are parts of sentences, and are treated no differently from other words. We will be writing all our proofs in this style; scratch work, by contrast, can be as careless as desired. The two-column method of writing proofs, which we used in our discussion of valid logical arguments in Section 1.4, and is often used in high school geometry, should be left behind at this point. Mathematics texts and research papers are all written in the style of Theorem 2.1.3. See Section 2.6 for more about writing mathematics.

An important consideration when writing a proof is recognizing what needs to be proved and what doesn't. There is no precise formula for such a determination, but the main factor is the context of the proof. In an advanced book on number theory, it would be unnecessary to prove the fact that the sum of two even integers is even; it would be safe to assume that the reader of such a book would either have seen the proof of this fact, or could prove it herself. For us, however, because we are just learning how to do such proofs, it is necessary to write out the proof of this fact in detail, even though we know from experience that the result is true. The reasons to prove facts that we already know are twofold: first, in order to gain practice writing proofs, we start with simple results, so that we can focus on the writing, and not on mathematical difficulties; second, there are cases where "facts" that seem obviously true turn out to be false, and the only way to be sure is to construct valid proofs.

Though mathematical proofs are logical arguments, observe that in the proof of Theorem 2.1.3 we did not use the logical symbols we discussed in Chapter 1. In general, it is not proper to use logical symbols in the writing of mathematical proofs. Logical symbols were used in Chapter 1 to help us become familiar with informal logic. When writing mathematical proofs, we make use of that informal logic, but we write using standard English (or whatever language is being used).

For the record, in the proof of Theorem 2.1.3 we did make use of some of the rules of inference discussed in Section 1.4, though as will always be the case, these rules are not mentioned explicitly in proofs to avoid unnecessary length and clutter. For instance, the hypothesis in Part (1) has the form $P \wedge Q$, where $P = $ "n is even" and $Q = $ "m is even." The proofs starts by assuming that $P \wedge Q$ is true. We then used Simplification to deduce that each of P and Q is true, so that we could apply

the definition of even numbers to each, to deduce that each of the statements "there exists an integer k such that $n = 2k$" and "there exists an integer j such that $m = 2j$" holds. We then applied Adjunction to deduce that the statement "$n = 2k$ and $m = 2j$" holds, so that we could do the calculation involving $n + m$. Finally, we made repeated use of Hypothetical Syllogism to put all the pieces of the proof together. Of course, even though mathematicians do not generally mention the rules of logical inference used in their proofs, care must be taken to ensure that the rules of inference are used correctly, even when not stated explicitly.

One final comment on writing proofs: neither thinking up proofs nor writing them properly is easy, especially as the material under consideration becomes more and more abstract. Mathematics is not a speed activity, and you should not expect to construct proofs rapidly. You will often need to do scratch work first, before writing up the actual proof. As part of the scratch work, it is very important to figure out the overall strategy for the problem being solved, prior to looking at the details. What type of proof is to be used? What definitions are involved? Not every choice of strategy ultimately works, of course, and so any approach needs to be understood as only one possible way to attempt to prove the theorem. If one approach fails, try another. Every mathematician has, in some situations, had to try many approaches to proving a theorem before finding one that works; the same is true for students of mathematics.

<div style="text-align:center">

Exercises

</div>

Exercise 2.1.1. Reformulate each of the following theorems in the form $P \rightarrow Q$. (The statements of the theorems as given below are commonly used in mathematics courses; they are not necessarily the best possible ways to state these theorems.)

(1) The area of the region inside a circle of radius r is πr^2.
(2) Given a line l and a point P not on l, there is exactly one line m containing P that is parallel to l.
(3) Let $\triangle ABC$ be a triangle, with sides of length a, b and c. Then

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}.$$

(4) $e^{x+y} = e^x e^y$.
(5) (Fundamental Theorem of Calculus) Let f be a continuous function on $[a, b]$, and let F be any function for which $F'(x) = f(x)$. Then

$$\int_a^b f(x)\,dx = F(b) - F(a).$$

2.2 Direct Proofs

As mentioned in the previous section, the statement of virtually every theorem, when viewed appropriately, is of the form $P \rightarrow Q$, or some combination of such statements.

For example, each of the three parts of Theorem 2.1.3 is of the form $P \rightarrow Q$. To prove theorems, we therefore need to know how to prove statements of the form $P \rightarrow Q$.

The simplest form of proof, which we treat in this section, is the most obvious one: assume that P is true, and produce a series of steps, each one following from the previous ones, which eventually lead to Q. This type of proof is called a **direct proof**. That this sort of proof deserves a name is because there are other approaches that can be taken, as we will see in Section 2.3. An example of a direct proof is the proof of Theorem 2.1.3.

How do we construct direct proofs? There is no single answer to this question, but some useful strategies exist. To start, it is important to recognize that what is "direct" about a direct proof is the way the proof reads when you are done writing it. The completed proof starts at the beginning (the statement P) and ends at the end (the statement Q), and shows how to get logically from the former to the latter. How you think of the proof is another matter entirely. The way a proof looks when you are done constructing it often has little relation to how you went about thinking of it, especially for more difficult proofs. Similarly to writing a literature paper, for which you might take notes, make an outline, prepare a rough draft and revise it a number of times, so too with constructing a rigorous mathematical proof—the final version may be the result of a process involving a number of distinct steps, and much revision.

When constructing a proof, the first thing to do is specify what you are assuming, and what it is you are trying to prove. This comment may sound trivial, but the author has seen many students skip this important step in their rush to get to the details (which are usually more interesting). Then you pick a strategy for the proof; one such strategy is direct proof. The next stage is actually figuring out a proof, making use of your chosen strategy. If you cannot devise a proof using your chosen strategy, perhaps another strategy should be attempted. There is no fixed way of finding a proof; it requires experimentation, playing around and trying different things. Of course, with experience some standard ways of constructing proofs in certain familiar situations tend to suggest themselves.

Even when the chosen strategy is direct proof, there are a number of ways of trying to figure out the details of the proof. To find a direct proof of $P \rightarrow Q$, you might try assuming P, playing around with it, seeing where it leads. Or you might try looking at Q, determining what is needed to prove Q, and then what is needed to prove that, etc. Or you might do both of these, hoping to meet in the middle. However you go about working out the proof, once you understand it informally, you have only completed the "scratch work" stage of constructing the proof. Then comes the next stage, which is writing the proof in final form. No matter how convoluted a route you took in thinking up the proof, the final write-up should be direct and logical. In a direct proof, the write-up should start with P and go step by step until Q is reached. Therefore, this type of proof typically has the following form.

Proof. Suppose that P is true.

$\vdots$

(argumentation)

$\vdots$

Then Q is true. □

We are now ready to give two simple examples of direct proof. We will put in more details here than one might normally include, in order to make each step as explicit as possible. We start with a definition concerning the integers.

Definition 2.2.1. Let a and b be integers. The number a **divides** the number b if there is some integer q such that $aq = b$. If a divides b, we write $a|b$, and we say that a is a **factor** of b, and that b is **divisible** by a. △

Before discussing the content of Definition 2.2.1, we need to make an important remark about its logical structure. The definition says that "the number a divides the number b if …," where the … describe a certain condition involving the numbers a and b. Strictly speaking, it would have been proper to write "if and only if" instead of just "if," because it is certainly meant to be the case that if the condition does not hold, then we do not say that a divides b. However, it is customary in definitions to write "if" rather than "if and only if," because it is taken as assumed that if the condition does not hold, then the term being defined cannot be applied. We will stick with the customary formulation of definitions, but it is important to think of definitions as meaning "if and only if."

To show the truth of a statement of the form "$a|b$," it is necessary to find an integer q such that $aq = b$. Therefore, a statement of the form "$a|b$" is an existence statement.

The expression "$a|b$" should not be confused with the fraction "a/b." The latter is a number, whereas the former is a shorthand way of writing the statement "the integer a divides the integer b." For example, even though it is not sensible to write the fraction $7/0$, it is perfectly reasonable to write the expression $7|0$, because 7 does in fact divide 0, because $7 \cdot 0 = 0$. Because of this potential confusion, and also to avoid ambiguous expressions such as $1/2+3$ (is that $\frac{1}{2} + 3$ or $\frac{1}{2+3}$?), we suggest writing all fractions as $\frac{a}{b}$ rather than a/b.

We now have two simple results about divisibility. The proof of each theorem is preceded by scratch work, to show how one might go about formulating such a proof.

Theorem 2.2.2. *Let a, b and c be integers. If $a|b$ and $b|c$, then $a|c$.*

Scratch Work. Our goal is to show that $a|c$, so that we need to find some integer k such that $ak = c$. We are free to choose any k that we can think of. Because $a|b$ and $b|c$, there are integers q and r such that $aq = b$ and $br = c$. Substituting the first equation into the second equation looks like a good idea to try, and we obtain $(aq)r = c$. By rearranging the left-hand side of this equation, we see that $k = qr$ is a good guess. ///

Proof. Suppose that $a|b$ and $b|c$. Hence there are integers q and r such that $aq = b$ and $br = c$. Define the integer k by $k = qr$. Then $ak = a(qr) = (aq)r = br = c$. Because $ak = c$, it follows that $a|c$. □

Compare the proof with the scratch work. The proof might not appear substantially better than the scratch work at first glance, and it might even seem a bit mysterious to someone who had not done the scratch work. Nonetheless, the proof is better than the scratch work, though in such a simple case the advantage might not be readily apparent. Unlike the scratch work, the proof starts with the hypotheses and proceeds logically to the conclusion, using the definition of divisibility precisely as stated. Later on we will see examples where the scratch work and the proof are more strikingly different.

Theorem 2.2.3. *Any integer divides zero.*

Scratch Work. In the statement of this theorem we are not given any particular choices of "variables," in contrast to the previous theorem (which was stated in terms of a, b and c). To prove something about any possible integer, we pick an arbitrary one, say n. Then we need to show that $n|0$. It would certainly not suffice to choose one particular number, say 5, and then show that 5 divides 0. Once we have chosen an arbitrary n, the rest of the details in this proof are extremely simple.   ///

Proof. Let n be an integer. Observe that $n \cdot 0 = 0$. Hence $n|0$.   □

The first step in proving a theorem often involves reformulating it in a more useful way, such as choosing n in the above proof.

The reader might be concerned that, in comparison to the scratch work for the above two theorems, the way we wrote the proofs involves "covering up our tracks." Although it might appear that way, the purpose of the proper writing of proofs is not at all to hide anything, but rather to make sure that what seemed like a good idea intuitively is indeed logical. The only way to check whether a proof is really valid is to write it up properly, and such a write-up does not include a description of everything that went through your mind when you were figuring out the details of the proof. The final proof must stand on its own, with no reference to what was written in the scratch work. For example, not all arguments are reversible, and an argument that worked backwards during scratch work might not work when written forwards, and it is only by writing the proof properly that we find out if the idea really works. Intuitive thinking that may have been useful in formulating the proof should be replaced with logical deduction in the final written proof.

In sum, there are two main steps to the process of producing a rigorous proof: formulating it and writing it. These two activities are quite distinct, though in some very simple and straightforward proofs you might formulate as you write. In most cases, you first formulate the proof (at least in outline form) prior to writing. For a difficult proof the relation between formulating and writing is essentially dialectical. You might formulate a tentative proof, try writing it up, discover some flaws, go back to the formulating stage and so on.

<div align="center">

Exercises

</div>

Exercise 2.2.1. Outline the strategy for a direct proof of each of the following statements (do not prove them, because the terms are meaningless).

   (1) Let n be an integer. If $7|n$, then n is bulbous.
   (2) Every globular integer is even.
   (3) If an integer is divisible by 13 and is greater than 100, then it is pesky.
   (4) An integer is both tactile and filigreed whenever it is odd.

Exercise 2.2.2. Let n and m be integers.

   (1) Prove that $1|n$.
   (2) Prove that $n|n$.
   (3) Prove that if $m|n$, then $m|(-n)$.

Exercise 2.2.3. Let n be an integer.

   (1) Prove that if n is even, then $3n$ is even.
   (2) Prove that if n is odd, then $3n$ is odd.

Exercise 2.2.4. **[Used in Theorem 2.3.5 and Theorem 2.4.1.]** Let n be an integer. Prove that if n is even then n^2 is even, and if n is odd then n^2 is odd.

Exercise 2.2.5. Let n and m be integers. Suppose that n and m are divisible by 3.

   (1) Prove that $n+m$ is divisible by 3.
   (2) Prove that nm is divisible by 3.

Exercise 2.2.6. Let a, b, c, m and n be integers. Prove that if $a|b$ and $a|c$, then $a|(bm+cn)$.

Exercise 2.2.7. Let a, b, c and d be integers. Prove that if $a|b$ and $c|d$, then $ac|bd$.

Exercise 2.2.8. Let a and b be integers. Prove that if $a|b$, then $a^n|b^n$ for all positive integers n. (There is no need for mathematical induction here.)

2.3 Proofs by Contrapositive and Contradiction

In this section we discuss two strategies for proving statements of the form $P \rightarrow Q$. Both these strategies are a bit more convoluted than direct proof, but in some situations they are nonetheless easier to work with. A less than perfect analogy might be when the straightest road between two cities leads up and down a mountain and through difficult terrain, whereas a curved road might at first seem to be going in the wrong direction, but in fact it bypasses the mountain and is ultimately easier and quicker than the straight road.

   There is no foolproof method for knowing ahead of time whether a proof on which you are working should be a direct proof or a proof by one of these other methods. Experience often allows for an educated guess as to which strategy to try first. In any case, if one strategy does not appear to bear fruit, then another strategy should be attempted. It is only when the proof is completed that we know whether a given choice of strategy works.

   Both strategies discussed in this section rely on ideas from our discussion of equivalence of statements in Section 1.3. For our first method, recall that the contrapositive of $P \rightarrow Q$, the statement $\neg Q \rightarrow \neg P$, is equivalent to $P \rightarrow Q$. Hence, in order

to prove $P \to Q$, we could just as well prove $\neg Q \to \neg P$, which we would do by the method of direct proof. We construct such a proof by assuming that Q is false, and then, in the final write-up, presenting a step-by-step argument going from $\neg Q$ to $\neg P$. A proof of this sort is called **proof by contrapositive**. This type of proof typically has the following form.

Proof. Suppose that Q is false.

$$\vdots$$

(argumentation)

$$\vdots$$

Then P is false. $\square$

The following proof is a simple example of proof by contrapositive.

Theorem 2.3.1. *Let n be an integer. If n^2 is odd, then n is odd.*

Scratch Work. If we wanted to use a direct proof, we would have to start with the assumption that n^2 is odd. Then there would be some integer j such that $n^2 = 2j+1$. It is not clear, however, how to proceed from this point, so instead we try proof by contrapositive. Such a proof would involve assuming that n is not odd, which implies that it is even, and then deducing that n^2 is even, which implies that it is not odd. We start such a proof by observing that if n is even, then there is some integer k such that $n = 2k$, and we then compute n^2 in terms of k, leading to the desired result.   ///

Proof. Suppose that n is even. Then there is some integer k such that $n = 2k$. Hence $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Because $2k^2$ is an integer, it follows that n^2 is even. By contrapositive, we see that if n^2 is odd then n is odd. $\square$

In the above proof we mentioned that we used proof by contrapositive. In general, it is often helpful to the reader to have the method of proof stated explicitly.

Another method of proof for theorems with statements of the form $P \to Q$, which looks similar to proof by contrapositive but is actually distinct from it, is **proof by contradiction**.

Logicians use the term "proof by contradiction" to mean the proof of a statement A by assuming $\neg A$, then reaching a contradiction, and then deducing that A must be true. For our purposes, we are interested in proof by contradiction for the special case where the statement A has the form $P \to Q$, because that is how mathematical theorems are formulated. We now take a closer look at this particular type of proof by contradiction.

Recall from Section 1.3 that $\neg(P \to Q)$ is equivalent to $P \wedge \neg Q$. Suppose that we could prove that $P \wedge \neg Q$ is false. It would follow that $\neg(P \to Q)$ is false, and hence that $\neg(\neg(P \to Q))$ is true. Then, using Double Negation (Fact 1.3.2 (1)), we could conclude that $P \to Q$ is true.

The method of proof by contradiction is to show that $P \to Q$ is true by assuming that $P \wedge \neg Q$ is true, and then deriving a logical contradiction, by which we mean, as discussed in Section 1.2, a statement that cannot be true under any circumstances;

often such statements have the form $B \wedge \neg B$ for some statement B. Once we reach a contradiction, we conclude that $P \wedge \neg Q$ is false, and then as above we deduce that $P \rightarrow Q$ is true.

Another way to think of proof by contradiction is to observe from the truth table for $P \rightarrow Q$ that the only way for this statement to be false is if P is true and Q is false, that is, if P is true and $\neg Q$ is true. Hence, if we assume both of these, and then derive a contradiction, we would know that $P \rightarrow Q$ cannot be false; hence $P \rightarrow Q$ must be true.

A proof by contradiction typically has the following form.

Proof. We prove the result by contradiction. Suppose that P is true and that Q is false.

$$\vdots$$

(argumentation)

$$\vdots$$

We have therefore reached a contradiction. Therefore P implies Q. $\square$

We now turn to a simple example of proof by contradiction. It is a good idea to start such a proof by stating that you are using this strategy.

Theorem 2.3.2. *The only consecutive non-negative integers a, b and c that satisfy $a^2 + b^2 = c^2$ are 3, 4 and 5.*

Scratch Work. The statement of this theorem has the form $P \rightarrow Q$, because it can be restated as "if a, b and c are consecutive non-negative integers such that $a^2 + b^2 = c^2$, then a, b and c are 3, 4 and 5." It is hard to prove the result directly, because we are trying to prove that something does not exist. Rather, we will assume that consecutive integers a, b and c, other than 3, 4 and 5, exist and satisfy $a^2 + b^2 = c^2$, and we will then derive a contradiction. Also, we observe that if a, b and c are consecutive integers, then $b = a + 1$ and $c = a + 2$.   ///

Proof. We prove the result by contradiction. Suppose that a, b and c are non-negative consecutive integers other than 3, 4 and 5, and that $a^2 + b^2 = c^2$. Because a, b and c are not 3, 4 and 5, we know that $a \neq 3$, and because the three numbers are consecutive, we know that $b = a + 1$ and $c = a + 2$. From $a^2 + b^2 = c^2$ we deduce that $a^2 + (a+1)^2 = (a+2)^2$. After expanding and rearranging we obtain $a^2 - 2a - 3 = 0$. This equation factors as $(a - 3)(a + 1) = 0$. Hence $a = 3$ or $a = -1$. We have already remarked that $a \neq 3$, and we know a is non-negative. Therefore we have a contradiction, and the theorem is proved. $\square$

Our next two theorems are both famous results that have well-known proofs by contradiction. These clever proofs are much more difficult than what we have seen so far, and are more than would be expected of a student to figure out on her own at this point.

Our first result involves irrational numbers, which we will shortly define. Irrational numbers are a type of real number, and so we need to assume informal knowledge of the real numbers, just as we assumed informal knowledge of the integers

in Sections 2.1 and 2.2. The real numbers are the collection of all the numbers that are generally used in elementary mathematics (not including the complex numbers), and they have operations addition, subtraction, multiplication and division, and these operations satisfy standard properties such as the Commutative Law for addition and multiplication. See the Appendix for a brief summary of some of the standard properties of real numbers. We now turn to the matter at hand.

Definition 2.3.3. Let x be a real number. The number x is a **rational number** if there exist integers n and m such that $m \neq 0$ and $x = \frac{n}{m}$. If x is not a rational number, it is an **irrational number**. △

Observe that if x is a rational number, then there are many different fractions of the form $\frac{n}{m}$ such that $x = \frac{n}{m}$. Given any fraction $\frac{n}{m}$ such that $n \neq 0$, we can always reduce it to "lowest terms," by which we mean that the numerator and denominator have no common factors other than 1 and -1. See the Appendix for a reference, where this fact about rational numbers is stated as Theorem A.6.

Are there any irrational numbers? Though it is not at all obvious, there are in fact infinitely many of them, and in a certain sense there are more irrational numbers than rational ones, as will be made precise in Section 6.7.

At this point, however, we will have to be satisfied with verifying that irrational numbers exist. In particular, we will prove that $\sqrt{2}$ is an irrational number. To us this fact may seem rather innocuous, though when first discovered it was something of a shock. The result was discovered by someone in the Pythagorean school in ancient Greece (possibly the sixth century B.C.E.). This school, centered around the figure of Pythagoras, was dedicated to mathematics as well as various mystical beliefs. Among other things, the Pythagoreans believed in the importance of whole numbers, and held that anything meaningful in the universe could be related to whole numbers or to ratios of whole numbers. The ancient Greeks tended to think of numbers geometrically, and they probably did not think of $\sqrt{2}$ as an algebraically defined object, as we do today. However, by using the Pythagorean Theorem, we see that if a square has sides of length 1, then the diagonal of the square will have length $\sqrt{2}$. Hence $\sqrt{2}$ would be a geometrically meaningful number to the Pythagoreans, and therefore they were very disturbed to discover that this number was not expressible as a ratio of whole numbers. One legend has it that the discoverer of this fact, in despair, threw himself overboard from a ship.

Before we state and prove our theorem about $\sqrt{2}$, we need a proper definition for this number.

Definition 2.3.4. Let p be a positive real number. The **square root** of p, denoted $\sqrt{p}$, is a positive real number x such that $x^2 = p$. △

Our goal is to prove that $\sqrt{2}$ is an irrational number, but there is a more fundamental question about $\sqrt{2}$ that needs to be addressed first, which is whether it exists. Definition 2.3.4 states that if there is a number denoted $\sqrt{2}$, it would be a positive real number x such that $x^2 = 2$, but nothing in the definition guarantees that such a number x exists. Clearly, if there is no such real number x, it would make no sense to try to prove that such a number is irrational. In fact, as expected, it is indeed true

that there is a positive real number x such that $x^2 = 2$ (and there is only one such number), but unfortunately it is beyond the scope of this book to give a proof of that fact. The proof requires tools from real analysis; see [Blo11, Theorem 2.6.9] for a proof.

Assuming that $\sqrt{2}$ exists, however, we can prove here that this number is irrational. Observe that the following theorem is self-contained, and does not rely upon a proof that $\sqrt{2}$ exists; it only says that if $\sqrt{2}$ exists, then it is irrational.

Theorem 2.3.5. *There is no rational number x such that $x^2 = 2$.*

Preliminary Analysis. The statement of our theorem says that something does not exist, which is hard to prove directly. However, we can easily reformulate the statement to avoid that problem, because to say that there is no rational number with a certain property means that if a real number has that property, that number cannot be rational. That is, we can reformulate our theorem as "if x is a real number and $x^2 = 2$, then x is irrational," which has the familiar form $P \rightarrow Q$. We then use proof by contradiction, which we start by assuming that x is a real number such that $x^2 = 2$, and also that x is not irrational (and hence it is rational).   ///

Proof. Let x be a real number. Suppose that $x^2 = 2$, and that x is rational. We will derive a contradiction. Because x is rational, there are integers n and m such that $x = \frac{n}{m}$. Observe that $n \neq 0$. If $\frac{n}{m}$ is not in lowest terms, then we could cancel any common factors, bringing it to lowest terms. There is no problem assuming that this has been done already, and so we may assume that n and m have no common factors other than 1 and -1.

Because $x^2 = 2$, then $\left(\frac{n}{m}\right)^2 = 2$. It follows that $\frac{n^2}{m^2} = 2$, and hence $n^2 = 2m^2$. We now ask whether n is even or odd. If n were odd, then using Exercise 2.2.4 we would see that n^2 would be odd. This last statement is not possible, because $n^2 = 2m^2$, and $2m^2$ must be even, because it is divisible by 2. It follows that n cannot be odd; hence n must be even. Therefore there is some integer k such that $n = 2k$. Then $(2k)^2 = 2m^2$, so that $4k^2 = 2m^2$, and therefore $2k^2 = m^2$. By an argument similar to the one used above, we see that m is even. We therefore conclude that both n and m are even. We have therefore reached a contradiction, because any two even numbers have 2 as a common factor, and yet we assumed that n and m have no common factors other than 1 and -1. Hence x is not rational.   □

The proof of Theorem 2.3.5 is mentioned (without details) in Aristotle's "Prior Analytics" (I.23), and is presumed to be of earlier origin; perhaps it is the proof used by the Pythagoreans (though they would not have formulated it as we do).

Our second famous result involves prime numbers, and has a proof by contradiction for a subpart of a proof by contradiction. We will make use of the definition of divisibility given in Section 2.2.

Definition 2.3.6. Let p be an integer greater than 1. The number p is a **prime number** if the only positive integers that divide p are 1 and p. The number p is a **composite number** if it is not a prime number.   △

The first few prime numbers are $2, 3, 5, 7, 11, \ldots$. The study of prime numbers is quite old and very extensive; see any book on elementary number theory, for example [Ros05], for details.

The number 1 is not considered to be either prime or composite. On the one hand, the only positive integers that divide 1 are 1 and itself, which would make it seem as if 1 were a prime number. However, the prime numbers are always defined as being 2 or larger to avoid special cases and awkward statements of theorems. For example, if 1 were a prime number, then the factorization of integers into prime numbers would not be unique, and uniqueness would hold only for "factorization into prime numbers other than 1," which is cumbersome to state. On the other hand, the number 1 is not considered composite, because there are no positive integers other than 1 and itself that divide it.

Whereas we restrict our attention to the integers greater than 1 when we discuss prime numbers and composite numbers, some authors consider negative numbers such as $-2, -3, -5, \ldots$ to be prime numbers, and similarly for composite numbers. Moreover, the term "prime" is used in the more general context of rings, a structure that is studied in abstract algebra, and that includes the integers as a special case; see any introductory abstract algebra text, for example [Fra03], for details.

Observe that a composite number n can always be written as $n = ab$ for some positive integers a and b such that $1 < a < n$ and $1 < b < n$.

How many prime numbers are there? In particular, are there only finitely many prime numbers, or infinitely many? The following theorem answers this question. The proof we give is very commonly used, and goes back to Euclid; see [Rib96, Chapter 1] for further discussion, as well as some other nice proofs of this theorem.

Theorem 2.3.7. *There are infinitely many prime numbers.*

Preliminary Analysis. We have not yet seen a rigorous treatment of what it means for there to be infinitely many of something, and so for now we need to use this concept in an intuitive fashion. A thorough discussion of finite vs. infinite is found in Chapter 6. The essential idea discussed in that chapter is that if a collection of objects can be listed in the form $a_1, a_2, \ldots, a_n$ for some positive integer n, then the collection of objects is finite; if the collection of objects cannot be described by any such list, then it is infinite. In Chapter 6 we will see a rigorous formulation of this idea in terms of sets and functions, but this intuitive explanation of finite vs. infinite completely captures the rigorous definition.

To say that there are infinitely many prime numbers means that there is no list of the form $P_1, P_2, \ldots, P_n$, for any positive integer n, that contains all prime numbers. It is easier to prove this statement if we reformulate it as "if n is a positive integer, and $P_1, P_2, \ldots, P_n$ are prime numbers, then $P_1, P_2, \ldots, P_n$ does not include all prime numbers." The proof of this last statement is by contradiction.   ///

Proof. Let n be a positive integer, and let $P_1, P_2, \ldots, P_n$ be a collection of prime numbers. Suppose that $P_1, P_2, \ldots, P_n$ contains all prime numbers.

Let $Q = (P_1 \times P_2 \times \cdots \times P_n) + 1$. We will show that Q is a prime number. Because Q is clearly larger than any of the numbers $P_1, P_2, \ldots, P_n$, it will follow that Q is a prime number that is not in the collection $P_1, P_2, \ldots, P_n$, and we will therefore know that the collection $P_1, P_2, \ldots, P_n$ does not contain all prime numbers, which is a contradiction. It will then follow that if n is a positive integer, and $P_1, P_2, \ldots, P_n$ are prime numbers, then $P_1, P_2, \ldots, P_n$ does not include all prime numbers, and we will conclude that there are infinitely many prime numbers.

To show that Q is a prime number, we use proof by contradiction. Suppose that Q is not a prime number. Therefore Q is a composite number. By Theorem 6.3.10 we deduce that Q has a factor that is a prime number. (Though this theorem comes later in the text, because it needs some tools we have not yet developed, it does not use the result we are now proving, and so it is safe to use.) The only prime numbers are $P_1, P_2, \ldots, P_n$, and therefore one of these numbers must be a factor of Q. Suppose that P_k is a factor of Q, for some integer k such that $1 \leq k \leq n$. Therefore there is some integer R such that $P_k R = Q$. Hence

$$P_k R = (P_1 \times P_2 \times \cdots \times P_n) + 1,$$

and therefore

$$P_k[R - (P_1 \times \cdots \times P_{k-1} \times P_{k+1} \times \cdots \times P_n)] = 1.$$

It follows that P_k divides 1. However, the only integers that divide 1 are 1 and -1. (We will not provide a proof of this last fact; it is stated as Theorem A.4 in the Appendix.) Because P_k is a prime number it cannot possibly equal 1 or -1, which is a contradiction. We deduce that Q is not a composite number, and hence it is a prime number. □

The proof of Theorem 2.3.7 actually yields more than just what the statement of the theorem says; it in fact gives an explicit procedure for producing arbitrarily many prime numbers. We start by letting $P_1 = 2$, which is the smallest prime number. We then let $P_2 = P_1 + 1 = 3$, and then $P_3 = (P_1 \times P_2) + 1 = 7$, and then $P_4 = (P_1 \times P_2 \times P_3) + 1 = 43$, and so on. We could continue this process indefinitely, producing as many prime numbers as we liked. This process is not entirely satisfying, however, both because it does not yield a simple explicit formula for P_n as a function of n, and also because this process skips over many prime numbers. In fact, no one has yet found a simple procedure to produce all prime numbers.

We conclude this section with the observation that proof by contradiction implicitly uses Double Negation, which ultimately relies upon the Law of the Excluded Middle, which says that any statement is either true or false. (See Section 1.2 for more discussion of this issue.) Any mathematician who does not believe in the Law of the Excluded Middle would therefore object to proof by contradiction. There are such mathematicians, though the majority of mathematicians, including the author of this book, are quite comfortable with the Law of the Excluded Middle, and hence with proof by contradiction.

<div align="center">

Exercises

</div>

Exercise 2.3.1. For each of the statements in Exercise 2.2.1, outline the strategy for a proof by contrapositive, and the strategy for a proof by contradiction (do not prove the statements, because the terms are meaningless).

Exercise 2.3.2. Let n be an integer. Prove that if n^2 is even, then n is even.

Exercise 2.3.3. Let a, b and c be integers. Prove that if a does not divide bc, then a does not divide b.

Exercise 2.3.4. [Used in Theorem 6.7.4.] Prove that the product of a non-zero rational number and an irrational number is irrational.

Exercise 2.3.5. Let a, b and c be integers. Suppose that there is an integer d such that $d|a$ and $d|b$, but that d does not divide c. Prove that the equation $ax+by = c$ has no solution such that x and y are integers.

Exercise 2.3.6. Let c be an integer. Suppose that $c \geq 2$, and that c is not a prime number. Prove that there is an integer b such that $b \geq 2$, that $b|c$ and that $b \leq \sqrt{c}$.

Exercise 2.3.7. Let q be an integer. Suppose that $q \geq 2$, and that for any integers a and b, if $q|ab$ then $q|a$ or $q|b$. Prove that $\sqrt{q}$ is irrational.

Exercise 2.3.8. Let q be an integer. Suppose that $q \geq 2$, and that for any integers a and b, if $q|ab$ then $q|a$ or $q|b$. Prove that q is a prime number. (The converse to this statement is also true, though it is harder to prove; see [Dea66, Section 3.6] for details, though note that his use of the term "prime," while keeping with the standard usage in ring theory, is not the same as ours.)

2.4 Cases, and If and Only If

The notion of equivalence of statements, as discussed in Section 1.3, has already been seen to be useful in proving theorems, for example in proof by contrapositive. In this section we will make use of some other equivalences of statements to prove certain types of theorems.

One commonly used method for proving a statement of the form $P \rightarrow Q$ is by breaking up the proof into a number of cases (and possibly subcases, subsubcases and so on). Formally, we use proof by cases when the premise P can be written in the form $A \vee B$. We then use Exercise 1.3.2 (6) to see that $(A \vee B) \rightarrow Q$ is equivalent to $(A \rightarrow Q) \wedge (B \rightarrow Q)$. Hence, in order to prove that a statement of the form $(A \vee B) \rightarrow Q$ is true, it is sufficient to prove that each of the statements $A \rightarrow Q$ and $B \rightarrow Q$ is true. The use of this strategy often occurs when proving a statement involving a quantifier of the form "for all x in U," and where no single proof can be found for all such x, but where U can be divided up into two or more parts, and where a proof can be found for each part.

For the following simple example of proof by cases, recall the definition of even and odd integers in Section 2.1.

Theorem 2.4.1. *Let n be an integer. Then $n^2 + n$ is even.*

Preliminary Analysis. Because we know about sums and products of even numbers and odd numbers, it seems like a good idea to try breaking up the proof into two cases, one case where n is even and one case where n is odd. Formally, let $A =$ "n is an even integer," let $B =$ "n is an odd integer" and let $Q =$ "$n^2 + n$ is even." Then the theorem has the form $(A \lor B) \to Q$. We will prove the theorem by proving that $(A \to Q)$ and $(B \to Q)$ are both true; each of these statements will be proved as a separate case. The proof of this theorem could be done either by making use of Theorem 2.1.3 and Exercise 2.2.4, or from scratch; because the latter is simple enough, we will do that.   ///

Proof. Case 1: Suppose that n is even. By definition we know that there is some integer k such that $n = 2k$. Hence

$$n^2 + n = (2k)^2 + 2k = 4k^2 + 2k = 2(2k^2 + k).$$

Because k is an integer, so is $2k^2 + k$. Therefore $n^2 + n$ is even.

Case 2: Suppose that n is odd. By definition we know that there is some integer j such that $n = 2j + 1$. Hence

$$n^2 + n = (2j + 1)^2 + (2j + 1) = (4j^2 + 4j + 1) + (2j + 1)$$
$$= 4j^2 + 6j + 2 = 2(2j^2 + 3j + 1).$$

Because j is an integer so is $2j^2 + 3j + 1$. Therefore $n^2 + n$ is even.   □

It is not really necessary to define A and B explicitly as we did in the scratch work for Theorem 2.4.1, and we will not do so in the future, but it was worthwhile doing it once, just to see how the equivalence of statements is being used.

In the proof of Theorem 2.4.1 we had two cases, which together covered all possibilities, and which were exclusive of each other. It is certainly possible to have more than two cases, and it is also possible to have non-exclusive cases; all that is needed is that all the cases combined cover all possibilities. The proof of Theorem 2.4.4 below has two non-exclusive cases.

We now turn to theorems that have statements of the form $P \to (A \lor B)$. Such theorems are less common than the previously discussed type, but do occur, and it is worth being familiar with the standard proof strategies for such theorems. There are two commonly used strategies, each one being advantageous in certain situations. One approach would be to use the contrapositive together with De Morgan's Law (Fact 1.3.2 (13)), which together imply that $P \to (A \lor B)$ is equivalent to $(\neg A \land \neg B) \to \neg P$. The other would be to use Exercise 1.3.2 (5), which says that $P \to (A \lor B)$ is equivalent to $(P \land \neg A) \to B$. The roles of A and B could also be interchanged in this last statement. The second approach is more commonly used, and so we use it in the following proof, although in this particular case the first approach would work quite easily, as the reader should verify.

Theorem 2.4.2. *Let x and y be real numbers. If xy is irrational, then x or y is irrational.*

Preliminary Analysis. The statement of this theorem has the form $P \rightarrow (A \lor B)$. We will prove $(P \land \neg A) \rightarrow B$, which we do by assuming that xy is irrational and that x is rational, and deducing that y is irrational. ///

Proof. Suppose that xy is irrational and that x is rational. Hence $x = \frac{a}{b}$ for some integers a and b such that $b \neq 0$. We will show that y is irrational, by using proof by contradiction. Suppose that y is rational. It follows that $y = \frac{m}{n}$ for some integers m and n such that $n \neq 0$. Hence $xy = \frac{am}{bn}$, and $bn \neq 0$, contradicting the fact that xy is irrational. Hence y is irrational. □

   Having discussed the appearance of $\lor$ in the statements of theorems, we could also consider the appearance of $\land$, though these occurrences are more straightforward. As expected, a theorem with statement of the form $(A \land B) \rightarrow Q$ is proved by assuming A and B, and using both of these statements to derive Q. To prove a theorem with statement of the form $P \rightarrow (A \land B)$, we can use Exercise 1.3.2 (4), which states that $P \rightarrow (A \land B)$ is equivalent to $(P \rightarrow A) \land (P \rightarrow B)$. Hence, to prove a theorem with statement of the form $P \rightarrow (A \land B)$, we simply prove each of $P \rightarrow A$ and $P \rightarrow B$, again as expected.

   Not only are there a variety of ways to structure proofs, but there are also variants in the logical form of the statements of theorems. Whereas the most common logical form of the statement of a theorem is $P \rightarrow Q$, as we have discussed so far, another common form is $P \leftrightarrow Q$. We refer to such theorems as "if and only if" theorems (often abbreviated "iff" theorems). To prove such a theorem, we make use of the fact that $P \leftrightarrow Q$ is equivalent to $(P \rightarrow Q) \land (Q \rightarrow P)$, as was shown in Fact 1.3.2 (11). Hence, to prove a single statement of the form $P \leftrightarrow Q$, it is sufficient to prove the two statements $P \rightarrow Q$ and $Q \rightarrow P$, each of which can be proved using any of the methods we have seen so far. We now give a typical example of such a proof; it is sufficiently straightforward so that we dispense with the scratch work. Recall the definition of divisibility of integers in Section 2.2.

Theorem 2.4.3. *Let a and b be non-zero integers. Then a|b and b|a if and only if a = b or a = −b.*

Proof.

   ⇒. Suppose that $a|b$ and $b|a$. Because $a|b$, there is some integer m such that $am = b$, and because $b|a$, there is some integer k such that $bk = a$. Substituting this last equation into the previous one, we obtain $(bk)m = b$, and hence $b(km) = b$. Because $b \neq 0$, it follows that $km = 1$. Because k and m are integers, then either $k = 1$ and $m = 1$, or $k = -1$ and $m = -1$. (We will not provide a proof of this last fact; it is stated as Theorem A.4 in the Appendix.) In the former case $a = b$, and in the latter case $a = -b$.

   ⇐. Suppose that $a = b$ or $a = -b$. First, suppose that $a = b$. Then $a \cdot 1 = b$, so $a|b$, and $b \cdot 1 = a$, so $b|a$. Similarly, suppose that $a = -b$. Then $a \cdot (-1) = b$, so $a|b$, and $b \cdot (-1) = a$, so $b|a$. □

Our next example of an if and only if theorem combines a number of the methods we have discussed so far.

Theorem 2.4.4. *Let m and n be integers. Then mn is odd if and only if both m and n are odd.*

Scratch Work. The "$\Leftarrow$" part of this theorem, which is the "if" part, says that if m and n are both odd, then mn is odd. This implication will be straightforward to prove, using the definition of odd integers.

The "$\Rightarrow$" part of this theorem, which is the "only if" part, says that if mn is odd, then both m and n are odd. A direct proof of this part of the theorem would start with the assumption that mn is odd, which would mean that $mn = 2p+1$ for some integer p, but it is not clear how to go from there to the desired conclusion. It is easier to make assumptions about m and n and proceed from there, so we will prove this part of the theorem by contrapositive, in which case we assume that m and n are not both odd, and deduce that mn is not odd. When we assume that m and n are not both odd, we will have two (overlapping) cases to consider, namely, when m is even or when n is even. Alternatively, it would be possible to make use of three non-overlapping cases, which are when m is even and n is odd, when m is odd and n is even, and when m and n are both even; however, the proof is no simpler as a result of the non-overlapping cases, and in fact the proof would be longer with these three cases rather than the two overlapping ones as originally proposed, and so we will stick with the latter.   ///

Proof.

$\Leftarrow$. Suppose that m and n are both odd. Hence there is an integer j such that $m = 2j+1$, and there is an integer k such that $n = 2k+1$. Therefore

$$mn = (2j+1)(2k+1) = 4jk+2j+2k+1 = 2(2jk+j+k)+1.$$

Because k and j are integers, so is $2jk+j+k$. Therefore mn is odd.

$\Rightarrow$. Suppose that m and n are not both odd. We will deduce that mn is not odd, and the desired result will follow by contrapositive. If m and n are not both odd, then at least one of them is even. Suppose first that m is even. Then there is an integer p such that $m = 2p$. Hence $mn = (2p)n = 2(pn)$. Because p and n are integers, so is pn. Therefore mn is even. Next assume that n is even. The proof in this case is similar to the previous case, and we omit the details.   □

A slightly more built-up version of an if and only if theorem is a theorem that states that three or more statements are all mutually equivalent. Such theorems often include the phrase "the following are equivalent," sometimes abbreviated "TFAE." The following theorem, which involves 2×2 matrices, is an example of this type of result. For the reader who is not familiar with matrices, we summarize the relevant notation. A 2×2 matrix is a square array of numbers of the form $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, for some real numbers a, b, c and d. The determinant of such a matrix is defined by $\det M = ad - bc$, and the trace of the matrix is defined by $\operatorname{tr} M = a + d$. An upper

triangular 2×2 matrix has the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, for some real numbers a, b and d. See any introductory text on linear algebra, for example [AR05, Chapters 1 and 2], for the relevant information about matrices.

Theorem 2.4.5. *Let $M = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ be an upper triangular 2×2 matrix. Suppose that a, b and d are integers. The following are equivalent.*

    a. $\det M = 1$.
    b. $a = d = \pm 1$.
    c. $\operatorname{tr} M = \pm 2$ *and* $a = d$.

What Theorem 2.4.5 says is that (a) if and only if (b), that (a) if and only if (c), and that (b) if and only if (c). Hence, to prove these three if and only if statements we would in principle need to prove that (a) $\Rightarrow$ (b), that (b) $\Rightarrow$ (a), that (a) $\Rightarrow$ (c), that (c) $\Rightarrow$ (a), that (b) $\Rightarrow$ (c), and that (c) $\Rightarrow$ (b). In practice we do not always need to prove six separate statements. The idea is to use the transitivity of logical implication, which follows from Fact 1.3.1 (12). For example, suppose that we could prove that (a) $\Rightarrow$ (b), that (b) $\Rightarrow$ (c), and that (c) $\Rightarrow$ (a); the other three implications would then hold automatically. We could just as well prove that (a) $\Rightarrow$ (c), that (c) $\Rightarrow$ (b), and that (b) $\Rightarrow$ (a), if that were easier. Another way to prove the theorem would be to prove that (a) $\Rightarrow$ (b), that (b) $\Rightarrow$ (a), that (a) $\Rightarrow$ (c), and that (c) $\Rightarrow$ (a). It is sufficient to prove any collection of logical implications from which the remaining logical implications can be deduced using transitivity; the choice of what to prove and what to deduce depends upon the particular theorem being proved. Similar reasoning holds when more than three statements are being proved equivalent.

Proof of Theorem 2.4.5. We will prove that (a) $\Rightarrow$ (b), that (b) $\Rightarrow$ (c), and that (c) $\Rightarrow$ (a).

(a) $\Rightarrow$ (b). Suppose that $\det M = 1$. Hence $ad - b \cdot 0 = 1$, and therefore $ad = 1$. Because both a and d are integers, it must be the case that either $a = 1$ and $d = 1$, or $a = -1$ and $d = -1$, using Theorem A.4.

(b) $\Rightarrow$ (c). Suppose that $a = d = \pm 1$. First, suppose that $a = d = 1$. Then $\operatorname{tr} M = a + d = 2$. Second, suppose that $a = d = -1$. Then $\operatorname{tr} M = a + d = -2$. Hence $\operatorname{tr} M = \pm 2$ and $a = d$.

(c) $\Rightarrow$ (a). Suppose that $\operatorname{tr} M = \pm 2$ and $a = d$. We can rewrite $\operatorname{tr} M = \pm 2$ as $a + d = \pm 2$. Hence $4 = (a + d)^2 = a^2 + 2ad + d^2$. Because $a = d$, then $a^2 = ad = d^2$, and therefore $4 = 4ad$. It follows that $ad = 1$. Because $\det M = ad - b \cdot 0 = ad$, we deduce that $\det M = 1$. $\qquad\square$

<div align="center">

Exercises

</div>

Exercise 2.4.1. Outline the strategy for a proof of each of the following statements (do not prove them, because the terms are meaningless).

    (1) If an integer is combustible then it is even or prime.
    (2) A 2×2 matrix is collapsible if and only if its determinant is greater than 3.

(3) For an integer to be putrid, it is necessary and sufficient that it is both odd and divisible by 50.

(4) Let n be an integer. The following are equivalent: (a) the integer n is composite and greater than 8; (b) the integer n is suggestive; (c) the integer n is indifferent or fragile.

Exercise 2.4.2. Let a, b and c be integers. Suppose that $c \neq 0$. Prove that $a|b$ if and only if $ac|bc$.

Exercise 2.4.3. **[Used in Exercise 4.4.8, Exercise 6.7.9 and Section 8.8.]** Let a and b be integers. The numbers a and b are **relatively prime** if the following condition holds: if n is an integer such that $n|a$ and $n|b$, then $n = \pm 1$. See Section 8.2 for further discussion and references.

(1) Find two integers p and q that are relatively prime. Find two integers c and d that are not relatively prime.

(2) Prove that the following are equivalent.

    a. a and b are relatively prime.

    b. a and $-b$ are relatively prime.

    c. $a+b$ and b are relatively prime.

    d. $a-b$ and b are relatively prime.

Exercise 2.4.4. Let n be an integer. Prove that one of the two numbers n and $n+1$ is even, and the other is odd. (You may use the fact that every integer is even or odd.)

Exercise 2.4.5. It follows from Corollary 5.2.5, using $n = 3$, that if a is an integer, then precisely one of the following holds: either $a = 3k$ for some integer k, or $a = 3k+1$ for some integer k, or $a = 3k+2$ for some integer k.

Let n and m be integers.

(1) Suppose that 3 divides n, and that 3 does not divide m. Prove that 3 does not divide $n+m$.

(2) Prove that 3 divides mn if and only if 3 divides m or 3 divides n.

Exercise 2.4.6. Are there any integers p such that $p > 1$, and such that all three numbers p, $p+2$ and $p+4$ are prime numbers? If there are such triples, prove that you have all of them; if there are no such triples, prove why not. Use the discussion at the start of Exercise 2.4.5.

Exercise 2.4.7. Let n be an integer. Using only the fact that every integer is even or odd, and without using Corollary 5.2.5, prove that precisely one of the following holds: either $n = 4k$ for some integer k, or $n = 4k+1$ for some integer k, or $n = 4k+2$ for some integer k, or $n = 4k+3$ for some integer k.

Exercise 2.4.8. Let n be an integer. Suppose that n is odd. Prove that there is an integer k such that $n^2 = 8k+1$.

Exercise 2.4.9. Let x be a real number. Define the **absolute value** of x, denoted $|x|$, by

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

Let a and b be real numbers. Prove the following statements.

(1) $|-a| = |a|$.

(2) $|a|^2 = a^2$.

(3) $|a - b| = |b - a|$.

(4) $|ab| = |a||b|$.

Exercise 2.4.10. Let x and y be real numbers. Let $x \frown y$ and $x \smile y$ be defined by

$$x \frown y = \begin{cases} x, & \text{if } x \ge y \\ y, & \text{if } x \le y, \end{cases} \quad \text{and} \quad x \smile y = \begin{cases} y, & \text{if } x \ge y \\ x, & \text{if } x \le y. \end{cases}$$

(Observe that $x \frown y$ is simply the maximum of x and y, and $x \smile y$ is the minimum, though our notation is more convenient for the present exercise than writing $\max\{x, y\}$ and similarly for the minimum.)

Let a, b and c be real numbers. Prove the following statements. The definition of absolute value is given in Exercise 2.4.9.

(1) $(a \frown b) + (a \smile b) = a + b$.

(2) $(a \smile b) + c = (a + c) \smile (b + c)$ and $(a \frown b) + c = (a + c) \frown (b + c)$.

(3) $(a \frown b) \frown c = a \frown (b \frown c)$ and $(a \smile b) \smile c = a \smile (b \smile c)$.

(4) $(a \frown b) - (a \smile b) = |a - b|$.

(5) $a \frown b = \frac{1}{2}(a + b + |a - b|)$ and $a \smile b = \frac{1}{2}(a + b - |a - b|)$.

2.5 Quantifiers in Theorems

A close look at the theorems we have already seen, and those we will be seeing, shows that quantifiers (as discussed in Section 1.5) appear in the statements of many theorems—implicitly if not explicitly. The presence of quantifiers, and especially multiple quantifiers, in the statements of theorems is a major source of error in the construction of valid proofs by beginners. So, extra care should be taken with the material in this section; mastering it now will save much difficulty later on. Before proceeding, it is worth reviewing the material in Section 1.5. Though we will not usually invoke them by name, to avoid distraction, the rules of inference for quantifiers discussed in Section 1.5 are at the heart of much of what we do with quantifiers in theorems.

We start by considering statements with a single universal quantifier, that is, statements of the form "$(\forall x \text{ in } U)P(x)$." Many of the theorems we have already seen have this form, even though the expression "for all" might not appear in their statements. For example, Theorem 2.3.1 says "Let n be an integer. If n^2 is odd, then n is odd." This statement implicitly involves a universal quantifier, and it can be rephrased as "For all integers n, if n^2 is odd, then n is odd." In order to prove that something is true for all integers, we picked an arbitrary integer that we labeled n (any other symbol would do), and proved the result for this arbitrarily chosen integer n. It was crucial

that we picked an arbitrary integer n, rather than a specific integer, for example 7. It is true that $7^2 = 49$ is odd, and that 7 is odd, but checking this one particular case does not tell us anything about what happens in all the other cases where n is an integer with n^2 odd.

More generally, suppose that we want to prove a theorem with statement of the form $(\forall x \text{ in } U)P(x)$. The key observation is that the statement "$(\forall x \text{ in } U)P(x)$" is equivalent to "if x is in U, then $P(x)$ is true." This latter statement has the form $A \rightarrow B$, and it can be proved by any of the methods discussed previously. A direct proof for $(\forall x \text{ in } U)P(x)$ would therefore proceed by choosing some arbitrary x_0 in U, and then deducing that $P(x_0)$ holds. Phrases such as "let x_0 be in U" are often used at the start of an argument to indicate an arbitrary choice of x_0. This type of proof typically has the following form.

Proof. Let x_0 be in U.

$$\vdots$$

(argumentation)

$$\vdots$$

Then $P(x_0)$ is true.   □

Again, we stress that it is crucial in this type of proof that an arbitrary x_0 in U is picked, not some particularly convenient value. It is not possible to prove that something is true for all values in U by looking at only one (or more) particular cases. In terms of rules of inference, look closely at the discussion of the variable in the Universal Generalization rule of inference in Section 1.5.

For example, a well-known function due to Leonhard Euler is defined by the formula $f(n) = n^2 + n + 41$ for all integers n. If you substitute the numbers $n = 0, 1, 2, \ldots, 39$ into this function, you obtain the numbers 41, 43, 47, ..., 1601, all of which are prime numbers. It therefore might appear that substituting in every positive integer into this function would result in a prime number (which would be a very nice property), but it turns out that $f(40) = 1681 = 41^2$, which is not prime. See [Rib96, p. 199] for more discussion of this, and related, functions. The point is that if you want to prove that a statement is true for all x in U, it does not suffice to try only some of the possible values of x.

Statements of the form $(\forall x \text{ in } U)P(x)$ can be proved by strategies other than direct proof. For example, the proof of such a statement using proof by contradiction typically has the following form.

Proof. We use proof by contradiction. Let y_0 be in U. Suppose that $P(y_0)$ is false.

$$\vdots$$

(argumentation)

$$\vdots$$

Then we arrive at a contradiction.   □

We will not show here any examples of proofs of statements of the form $(\forall x \text{ in } U)P(x)$, because we have already seen a number of such proofs in the previous sections of this chapter.

We now consider statements with a single existential quantifier, that is, statements of the form "$(\exists x \text{ in } U)P(x)$." Using the Existential Generalization rule of inference in Section 1.5, we see that to prove a theorem of the form $(\exists x)P(x)$ means that we need to find some z_0 in U such that $P(z_0)$ holds. It does not matter if there are actually many x in U such that $P(x)$ holds; we need to produce only one of them to prove existence. A proof of "$(\exists x \text{ in } U)P(x)$" can also be viewed as involving a statement of the form $A \rightarrow B$. After we produce the desired object z_0 in U, we then prove the statement "if $x = z_0$, then $P(x)$ is true." Such a proof typically has the following form.

Proof. Let $z_0 = \ldots$.

$\vdots$

(argumentation)

$\vdots$

Then z_0 is in U.

$\vdots$

(argumentation)

$\vdots$

Then $P(z_0)$ is true. $\square$

How we find the element z_0 in the above type of proof is often of great interest, and sometimes is the bulk of the effort we spend in figuring out the proof, but it is not part of the actual proof itself. We do not need to explain how we found z_0 in the final write-up of the proof. The proof consists only of defining z_0, and showing that z_0 is in U, and that $P(z_0)$ is true. It is often the case that we find z_0 by going backwards, that is, assuming that $P(z_0)$ is true, and seeing what z_0 has to be. However, this backwards work is not the same as the actual proof, because, as we shall see, not all mathematical arguments can be reversed—what works backwards does not necessarily work forwards.

We now turn to a simple example of a proof involving an existential quantifier. Recall the definitions concerning 2×2 matrices prior to Theorem 2.4.5. We say that a 2×2 matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has integer entries if a, b, c and d are integers.

Proposition 2.5.1. *There exists a 2×2 matrix A with integer entries such that* $\det A = 4$ *and* $\operatorname{tr} A = 7$.

Scratch Work. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. The condition $\det A = 4$ means that $ad - bc = 4$; the condition $\operatorname{tr} A = 7$ means that $a + d = 7$. We have two equations with four unknowns. Substituting $d = 7 - a$ into the first equation and rearranging, we obtain $a^2 - 7a + (bc + 4) = 0$. Applying the quadratic equation yields

$$a = \frac{7 \pm \sqrt{33 - 4bc}}{2}.$$

Because we want a, b, c and d to be integers, we need to find integer values of b and c such that $33 - 4bc$ is the square of an odd integer. Trial and error shows that $b = 2$ and $c = 3$ yield either $a = 5$ and $d = 2$, or $a = 2$ and $d = 5$. (There are other possible solutions, for example $b = -2$ and $c = 2$, but we do not need them).   ///

Proof. Let $A = \left(\begin{smallmatrix} 5 & 2 \\ 3 & 2 \end{smallmatrix}\right)$. Then $\det A = 5 \cdot 2 - 2 \cdot 3 = 4$, and $\operatorname{tr} A = 5 + 2 = 7$.   □

The difference between the scratch work and the actual proof for the above proposition is quite striking, as often occurs in proofs of theorems involving existential quantifiers. In the scratch work we went backwards, by which we mean that we started with the desired conclusion, in this case the assumption that there is some matrix A as desired, and proceeded to find out what criteria would then be imposed on a, b, c, d. We then found a, b, c, d that satisfy these criteria. Such a procedure was helpful, but it could not be our final proof, because we needed to show that the matrix A existed; we were not asked to show what could be said about A if it existed, which is what we did in the scratch work. To show that the desired matrix A existed, we simply had to produce it, and then show that it satisfied the requisite properties regarding its determinant and trace. This is what we did in the proof. How we produced A is irrelevant to the final proof (though not to our understanding of matrices). It is important that the actual proof reads "forwards," not backwards. Moreover, because we were asked to show only that A existed, and not describe how many possible matrices A there were, we needed to exhibit only one value of A in the actual proof, even though we knew that there was more than one possibility from our scratch work. Not everything we learn in the scratch work is necessarily needed in the final proof.

Backwards proofs are so common, especially in elementary mathematics, that unfortunately they are often unnoticed by students, and rarely criticized by instructors. Whereas backwards proofs might not produce any real harm in elementary mathematics, it is crucial to avoid them in advanced mathematics, where questions of logical implication are often much trickier.

Let us examine two simple examples of backwards proofs. First, suppose that we are asked to solve the equation $7x + 6 = 21 + 4x$. A typical solution submitted by a high school student might look like

$$
\begin{aligned}
7x + 6 &= 21 + 4x \\
3x - 15 &= 0 \\
3x &= 15 \\
x &= 5.
\end{aligned}
\tag{2.5.1}
$$

There is nothing wrong with the algebra here, and indeed $x = 5$ is the correct solution. For computational purposes such a write-up is fine, but logically it is backwards. We were asked to find the solutions to the original equation. A solution to an equation is a number that can be plugged into the equation to obtain a true statement. To solve an equation in the variable x, we simply have to produce a collection of numbers, which we then plug into the equation one at a time, verifying that each one makes the equation a true statement when plugged in. How these solutions are found is

logically irrelevant (though, of course, of great pedagogical interest). A logically correct "forwards" write-up of the solution to $7x + 6 = 21 + 4x$ would be as follows.

"Let $x = 5$. Plugging $x = 5$ into the left-hand side of the equation yields $7x + 6 = 7 \cdot 5 + 6 = 41$, and plugging it into the right-hand side of the equation yields $21 + 4x = 21 + 4 \cdot 5 = 41$. Therefore $x = 5$ is a solution. Because the equation is linear, it has at most one solution. Hence $x = 5$ is the only solution."

Such a write-up seems ridiculously long and overly pedantic, given the simplicity of the original equation, and in practice no one would (or should) write such a solution. Logically, however, it is the correct form for the solution to the problem as stated. The backwards approach in Equation 2.5.1 did happen to produce the correct solution to our problem, because all steps in this particular case are reversible. Not all computations are reversible, however, as we now see.

Suppose that we are asked to solve the equation

$$\sqrt{x^2 - 5} = \sqrt{x + 1},$$

where, as is common in high school, we consider only real number solutions. A typical (and backwards) write-up might look like

$$\sqrt{x^2 - 5} = \sqrt{x + 1}$$
$$x^2 - 5 = x + 1$$
$$x^2 - x - 6 = 0$$
$$(x - 3)(x + 2) = 0$$
$$x = 3 \quad \text{or} \quad x = -2.$$

The above write-up is definitely not correct, because $x = -2$ is not a solution to the original equation. In fact, it is not even possible to substitute $x = -2$ into either side of the original equation, because we cannot take the square root of negative numbers. The source of the error in the write-up is that not every step in it is reversible; it is left to the reader to figure out which step cannot be reversed. In an elementary course such as high school algebra or calculus, it would suffice to write up the above computation, and then observe that $x = -2$ should be dropped. In more rigorous proofs, however, it is best to stick to logically correct writing, in order to avoid errors that might otherwise be hard to spot. In your scratch work you can go forwards, backwards, sideways or any combination of these; in the final write-up, however, a proof should always go forwards, starting with the hypothesis and ending up with the desired conclusion.

Returning to our discussion of existence results, one variant on such results concerns theorems that involve existence and uniqueness, of which the following theorem is an example. This theorem concerns 2×2 matrices, as discussed prior to Theorem 2.4.5. This time we need some additional aspects of matrices, namely, the 2×2 identity matrix $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and matrix multiplication. It would take us too far afield to define matrix multiplication here; we assume that the reader is familiar

with such multiplication. See any introductory text on linear algebra, for example [AR05, Chapter 1], for information about matrix multiplication. It is easy to verify that $AI = A = IA$ for any 2×2 matrix A. It can also be verified (by a slightly tedious computation) that $(AB)C = A(BC)$ for any three 2×2 matrices A, B and C.

The following theorem concerns inverse matrices. Given a 2×2 matrix A, an inverse matrix for A is a 2×2 matrix B such that $AB = I = BA$. Does every 2×2 matrix have an inverse matrix? The answer is no. For example, the matrix $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ has no inverse matrix, as the reader may verify (by supposing it has an inverse matrix, and seeing what happens). The following theorem gives a very useful criterion for the existence of inverse matrices. In fact, the criterion is both necessary and sufficient for the existence of inverse matrices, and its analog holds for square matrices of any size, but we will not prove these stronger results.

Theorem 2.5.2. *Let A be a 2×2 matrix such that $\det A \neq 0$. Then A has a unique inverse matrix.*

The phrase "A has a unique inverse matrix" means that an inverse matrix for A exists, and that only one such inverse matrix exists. The logical notation for such a statement is $(\exists ! x)P(x)$, where "$\exists ! x$" means "there exists unique x." To prove such a statement, we need to prove two things, namely, existence and uniqueness, and it is usually best to prove each of these two things separately. It makes no difference which part is proved first. To prove existence, we proceed as before, and produce an example of the desired object. To prove uniqueness, the standard strategy is to assume that there are two objects of the sort we are looking for, and then show that they are the same. (It is also possible to assume that there are two different objects of the sort we are looking for, and then arrive at a contradiction by showing that the two object are actually the same, but there is rarely any advantage to using this alternative strategy.)

Scratch Work for Theorem 2.5.2. We start with the uniqueness part of the proof, to show that it really is independent of the existence part of the proof. To prove uniqueness, we assume that A has two inverse matrices, say B and C, and then use the properties of matrices cited above, together with the definition of inverse matrices, to show that $B = C$. The proof of existence is rather different. A backwards calculation to try to find an inverse matrix for A would be as follows. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Suppose that $B = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ is an inverse matrix of A. Then $BA = I$ and $AB = I$. The latter equality says

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

which yields

$$\begin{pmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This matrix equation yields the four equations

$$ax+bz = 1$$
$$ay+bw = 0$$

$$cx + dz = 0$$
$$cy + dw = 1,$$

where x, y, z and w are to be thought of as the variables and a, b, c and d are to be thought of as constants. We then solve for x, y, z and w in terms of a, b, c and d. The solution to these four equations turns out to be $x = \frac{d}{ad-bc}$, and $y = \frac{-b}{ad-bc}$, and $z = \frac{-c}{ad-bc}$ and $w = \frac{a}{ad-bc}$. Because $\det A = ad - bc$, we see why the hypothesis that $\det A \neq 0$ is necessary.   ///

Proof of Theorem 2.5.2. Uniqueness: Suppose that A has two inverse matrices, say B and C. Then $AB = I = BA$ and $AC = I = CA$. Using standard properties of matrix multiplication, we then compute

$$B = BI = B(AC) = (BA)C = IC = C.$$

Because $B = C$, we deduce that A has a unique inverse.

Existence: Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The condition $\det A \neq 0$ means that $ad - bc \neq 0$. Let B be the 2×2 matrix defined by

$$B = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}.$$

Then

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} \frac{ad}{ad-bc} + \frac{-bc}{ad-bc} & \frac{-ab}{ad-bc} + \frac{ab}{ad-bc} \\ \frac{cd}{ad-bc} + \frac{-cd}{ad-bc} & \frac{-bc}{ad-bc} + \frac{ad}{ad-bc} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

A similar calculation shows that $BA = I$. Hence B is an inverse matrix of A.   □

An understanding of quantifiers is also useful when we want to prove that a given statement is false. Suppose that we want to prove that a statement of the form "$(\forall x \text{ in } U)P(x)$" is false. We saw in Section 1.5 that $\neg[(\forall x \text{ in } U)Q(x)]$ is equivalent to $(\exists x \text{ in } U)(\neg Q(x))$. To prove that the original statement is false, it is sufficient to prove that $(\exists x \text{ in } U)(\neg Q(x))$ is true. Such a proof would work exactly the same as any other proof of a statement with an existential quantifier, that is, by finding some x_0 in U such that $\neg Q(x_0)$ is true, which means that $Q(x_0)$ is false. The element x_0 is called a "counterexample" to the original statement $(\forall x \text{ in } U)P(x)$.

For example, suppose that we want to prove that the statement "all prime numbers are odd" is false. The statement has the form $(\forall x)Q(x)$, where x has values in the integers, and where $Q(x) = $ "if x is prime, then it is odd." Using the reasoning above, it is sufficient to prove that $(\exists x)(\neg Q(x))$ is true. Using Fact 1.3.2 (14), we see that $\neg Q(x)$ is equivalent to "x is prime, and it is not odd." Hence, we need to find some integer x_0 such that x_0 is prime, and it is not odd, which would be a counterexample to the original statement. The number $x_0 = 2$ is just such a number (and in fact it is the only even prime number, though we do not need that fact). This example is so

simple that it may seem unnecessary to go through a lengthy discussion of it, but our point is to illustrate the general approach.

Similar considerations can be used to prove that a statement of the form $(\exists y)R(y)$ is false. It is often very hard to show directly that something does not exist, because one would have to examine all possible cases, and show that none of them have the desired property. Rather, we use the fact that $\neg[(\exists y)R(y)]$ is equivalent to $(\forall y)(\neg R(y))$, and we prove this last statement by our usual methods.

Finally, we look at theorems with statements that involve more than one quantifier. Such theorems might typically have the form $(\forall y)(\exists x)P(x,y)$ or $(\exists a)(\forall b)Q(a,b)$. We saw in Section 1.5 that there are eight possible ways of forming statements with two quantifiers, and clearly with more than two quantifiers there are many more possibilities. There is no point in giving detailed instructions on how to proceed for each different combination of quantifiers, both because there would be too many cases to consider, and because one single strategy works in all cases: take one quantifier at a time, from the outside in. The following two simple results are typical examples of this strategy.

Proposition 2.5.3. *For every real number a, there exists a real number b such that* $a^2 - b^2 + 4 = 0$.

Scratch Work. This proposition has the form $(\forall a)(\exists b)(a^2 - b^2 + 4 = 0)$, where a and b are real numbers. To prove this proposition, we start with the outside quantifier, which is $\forall a$. We can rewrite the statement to be proved as $(\forall a)Q(a)$, where $Q(a) =$ "$(\exists b)(a^2 - b^2 + 4 = 0)$." To prove the statement $(\forall a)Q(a)$, which is a statement with a single universal quantifier, we proceed as before, namely, by picking an arbitrary real number a_0, and then showing that $Q(a_0)$ holds. Therefore we need to show that $(\exists b)((a_0)^2 - b^2 + 4 = 0)$ is true for the given a_0. Again, we have a statement with one quantifier, this time an existential quantifier, and we do a backwards computation to solve for b, which yields $b = \pm\sqrt{(a_0)^2 + 4}$, though we need only one of these solutions. As always, we now write the proof forwards, to make sure that everything is correct.   ///

Proof. Let a_0 be a real number. Let $b_0 = \sqrt{(a_0)^2 + 4}$. Then

$$(a_0)^2 - (b_0)^2 + 4 = (a_0)^2 - (\sqrt{(a_0)^2 + 4})^2 + 4 = 0.$$

Hence, for each real number a_0, we found a real number b_0 such that $(a_0)^2 - (b_0)^2 + 4 = 0$.   □

Proposition 2.5.4. *There exists a real number x such that* $(3 - x)(y^2 + 1) > 0$ *for all real numbers y.*

Scratch Work. This proposition has the form $(\exists x)(\forall y)((3 - x)(y^2 + 1) > 0)$, where x and y are real numbers. Again, we start with the outside quantifier, which is $\exists x$. We rewrite the statement to be proved as $(\exists x)R(x)$, where $R(x) =$ "$(\forall y)((3 - x)(y^2 + 1) > 0)$." We prove the statement $(\exists x)R(x)$ by producing a single real number x_0 for which $R(x_0)$ holds. That is, we need to find a real number x_0 such that $(\forall y)((3 - x_0)(y^2 + $

$1) > 0$) is true, and hence we need to find a real number x_0, such that if we pick an arbitrary real number y_0, then $(3 - x_0)((y_0)^2 + 1) > 0$ will hold. Again we do our scratch work backwards. Observe that $(y_0)^2 + 1 > 0$ for all real numbers y_0, and that $3 - x_0 > 0$ for all $x_0 < 3$. We need to pick a single value of x_0 that works, and we randomly pick $x_0 = 2$. ///

Proof. Let $x_0 = 2$. Let y_0 be a real number. Observe that $(y_0)^2 + 1 > 0$. Then

$$(3 - x_0)((y_0)^2 + 1) = (3 - 2)((y_0)^2 + 1) > 0.$$

Hence, we have found a real number x_0 such that $(3 - x_0)((y_0)^2 + 1) > 0$ for all real numbers y_0. □

As discussed in Section 1.5, the order of the quantifiers in the statement of a theorem often matters. The statement of Proposition 2.5.3 is "For every real number a, there exists a real number b such that $a^2 - b^2 + 4 = 0$," which is $(\forall a)(\exists b)(a^2 - b^2 + 4 = 0)$. If we were to reverse the quantifiers, we would obtain $(\exists b)(\forall a)(a^2 - b^2 + 4 = 0)$, which in English would read "there is a real number b such that $a^2 - b^2 + 4 = 0$ for all real numbers a." This last statement is not true, which we can demonstrate by showing that its negation is true. Using Fact 1.5.1 (2), it follows that $\neg[(\exists b)(\forall a)(a^2 - b^2 + 4 = 0)]$ is equivalent to $(\forall b)(\exists a)(a^2 - b^2 + 4 \neq 0)$. To prove this latter statement, let b_0 be an arbitrary real number. We then choose $a_0 = b_0$, in which case $(a_0)^2 - (b_0)^2 + 4 = 4 \neq 0$. Hence the negation of the statement is true, so the statement is false. We therefore see that the order of the quantifiers in Proposition 2.5.3 does matter. On the other hand, changing the order of the quantifiers in the statement of Proposition 2.5.4, while changing the meaning of the statement, does not make it become false, as the reader may verify.

Exercises

Exercise 2.5.1. Convert the following statements, which do not have their quantifiers explicitly written, into statements with explicit quantifiers (do not prove them, because the terms are meaningless).

(1) If a 5×5 matrix has positive determinant then it is bouncy.
(2) There is a crusty integer that is greater than 7.
(3) For each integer k, there is an opulent integer w such that $k|w$.
(4) There is a fibrous 2×2 matrix P such that $\det P > m$, for each ribbed integer m.
(5) Some 2×2 matrix M has the property that every subtle integer divides $\mathrm{tr}\, M$.

Exercise 2.5.2. A problem that might be given in a high school mathematics class is "Prove that the equation $e^x = 5$ has a unique solution." We could rewrite the problem as "Prove that there exists a unique real number x such that $e^x = 5$." First, write up a solution to the problem as would be typically found in a high school class. Second, write up a proper solution to the problem, using the ideas discussed in this section. Write up the uniqueness first, without making use of the existence part of

the proof; avoid a backwards proof when showing existence. Do not use a calculator (the number x does not have to be given explicitly in decimal expansion).

Exercise 2.5.3. Prove or give a counterexample to each of the following statements.

(1) For each non-negative number s, there exists a non-negative number t such that $s \geq t$.

(2) There exists a non-negative number t such that for all non-negative numbers s, the inequality $s \geq t$ holds.

(3) For each non-negative number t, there exists a non-negative number s such that $s \geq t$.

(4) There exists a non-negative number s such that for all non-negative numbers t, the inequality $s \geq t$ holds.

Exercise 2.5.4. Prove or give a counterexample to each of the following statements.

(1) For each integer a, there exists an integer b such that $a|b$.

(2) There exists an integer b such that for all integers a, the relation $a|b$ holds.

(3) For each integer b, there exists an integer a such that $a|b$.

(4) There exists an integer a such that for all integers b, the relation $a|b$ holds.

Exercise 2.5.5. Prove or give a counterexample to each of the following statements.

(1) For each real number x, there exists a real number y such that $e^x - y > 0$.

(2) There exists a real number y such that for all real numbers x, the inequality $e^x - y > 0$ holds.

(3) For each real number y, there exists a real number x such that $e^x - y > 0$.

(4) There exists a real number x such that for all real numbers y, the inequality $e^x - y > 0$ holds.

Exercise 2.5.6. Prove or give a counterexample to the following statement. For each positive integer a, there exists a positive integer b such that

$$\frac{1}{2b^2 + b} < \frac{1}{ab^2}.$$

Exercise 2.5.7. Prove or give a counterexample to the following statement. For every real number y, there is a real number x such that $e^{3x} + y = y^2 - 1$.

Exercise 2.5.8. Prove or give a counterexample to the following statement. For each real number p, there exist real numbers q and r such that $q \sin \left(\frac{r}{5} \right) = p$.

Exercise 2.5.9. Prove or give a counterexample to the following statement. For each integer x, and for each integer y, there exists an integer z such that $z^2 + 2xz - y^2 = 0$.

Exercise 2.5.10. Let $P(x,y)$ be a statement with free variables x and y that are real numbers. Let a and b be real numbers. The real number u is called the least P-number for a and b if two conditions hold: (1) the statements $P(a,u)$ and $P(b,u)$ are both true; and (2) if w is a real number such that $P(a,w)$ and $P(b,w)$ are both true, then $u \leq w$. Suppose that c and d are real numbers, and that there is a least P-number for c and d. Prove that this least P-number is unique.

Exercise 2.5.11. A student is asked to show that the equation $x(x-1) = 2(x+2)$ has a solution. In the context of writing rigorous proofs, what is wrong with the following solution she handed in?

"Proof:

$$x(x-1) = 2(x+2)$$
$$x^2 - x = 2x + 4$$
$$x^2 - 3x - 4 = 0$$
$$(x-4)(x+1) = 0$$
$$x = 4 \quad \text{or} \quad x = -1.$$

Therefore there are two solutions."

Exercise 2.5.12. Look through mathematics textbooks that you have previously used (in either high school or college), and find an example of a backwards proof.

2.6 Writing Mathematics

In mathematics—as in any other field—careful writing is of great importance for both the writer and the reader. Careful writing is clearly necessary if the writer's proofs are to be understood by the reader. For the writer's own benefit, putting a mathematical idea into written form forces her to pay attention to all the details of an argument. Often an idea that seemed to make sense in one's head is found to be insufficient when put on paper. Any experienced mathematician knows that until an idea has been written up carefully, its correctness cannot be assumed, no matter how good the idea seemed at first.

Mathematical correctness is certainly the ultimate test of the validity of a proof, but to allow us to judge mathematical correctness, however, a number of important factors in the proper writing of mathematics are needed. Some of these ideas are described below. See [Gil87], [Hig98], [KLR89] and [SHSD73] for further discussion of writing mathematics.

1. A Written Proof Should Stand on Its Own

The first rule of writing proofs actually applies to all forms of writing, not just mathematical writing: The written text should stand on its own, without any need for clarification by the writer. Unlike writing of a more personal nature such as poetry and fiction, a written proof is not an expression of the writer's feelings, but rather a document that should work according to objective standards. When writing a proof, state everything you are doing as explicitly and clearly as possible. DO NOT ASSUME THE READER IS A MIND READER. Err on the side of too much explanation.

2. Write Precisely and Carefully

There is no room in mathematics for ambiguity. The most minute matters of phraseology in mathematics may make a difference. For example, compare the statement "If the given integer n is prime then it is not less than 2, and it is a perfect number" with "If the given integer n is prime, then it is not less than 2 and it is a perfect number." Something as seemingly insignificant as the change of the location of a comma can change the meaning of a statement. MAKE SURE WHAT YOU WRITE IS WHAT YOU MEAN.

As in non-mathematical writing, revision is often the key to achieving precision and clarity. Do not confuse the rough drafts of a proof with the final written version. You should revise your proofs just as you should revise all writing, which is by trying to read what you wrote as if someone else (whose thoughts you do not know) had written it.

Write mathematics in simple, straightforward, plodding prose. Leave your imagination to the mathematical content of your writing, but keep it out of your writing style, so that your writing does not get in the way of communicating your mathematical ideas. Serious mathematics is hard enough as it is, without having unnecessary verbiage or convoluted sentences making it even less clear.

Particular care should be taken with the use of mathematical terminology, where common words are sometimes given technical meanings different from their colloquial meanings (for example, the word "or"). Precision should not be overlooked in the statement of what is being proved. Mathematics is often read by skipping back and forth, and so it is important that the statements of theorems, lemmas, propositions and the like contain all their hypotheses, rather than having the hypotheses in some earlier paragraphs. Better a bit of redundancy than a confused reader.

3. Prove What Is Appropriate

A good proof should have just the right amount of detail—neither too little nor too much. The question of what needs to be included in a proof, and what can be taken as known by the reader, is often a matter of judgment. A good guideline is to assume that the reader is at the exact same level of knowledge as you are, but does not know the proof you are writing. It is certainly safe to assume that the reader knows elementary mathematics at the high school level (for example, the quadratic formula). In general, do not assume that the reader knows anything beyond what has been covered in your mathematics courses. When in doubt—prove.

4. Be Careful with Saying Things Are "Obvious"

It is very tempting to skip over some details in a proof by saying that they are "obvious" or are "similar to what has already been shown." Such statements are legitimate if true, but are often used as a cover for uncertainty or laziness. "Obvious" is in the eye of the beholder; what may seem obvious to the writer after spending hours (or

days) on a problem might not be so obvious to the reader. That something is obvious should mean that another person at your level of mathematical knowledge could figure it out in very little time and with little effort. If it does not conform to this criterion, it is not "obvious." As an insightful colleague once pointed out, if something is truly obvious, then there is probably no need to remind the reader of that fact.

The words "trivial" and "obvious" mean different things when used by mathematicians. Something is trivial if, after some amount of thought, a logically very simple proof is found. Something is obvious if, relative to a given amount of mathematical knowledge, a proof can be thought of very quickly by anyone at the given level. According to an old joke, a professor tells students during a lecture that a certain theorem is trivial; when challenged by one student, the professor thinks and thinks, steps out of the room to think some more, comes back an hour later, and announces to the class that the student was right, and that the result really is trivial. The joke hinges on the fact that something can be trivial without being obvious.

5. Use Full Sentences and Correct Grammar

The use of correct grammar (such as complete sentences and correct punctuation) is crucial if the reader is to follow what is written. Mathematical writing should be no less grammatically correct than literary prose. Mathematics is not written in a language different from the language we use for general speech. In this text all mathematics is written in English.

A distinguishing feature of mathematical writing is the use of symbols. It is very important to understand that mathematical symbols are nothing but shorthand for expressions that could just as well be written out in words. For example, the phrase "$x = z^2$" could be written as "the variable x equals the square of the variable z." Mathematical symbols are therefore subject to the rules of grammar just as words are. Mathematical symbols floating freely on a page are neither understandable nor acceptable. All symbols, even those displayed between lines, should be embedded in sentences and paragraphs.

A proof is an explanation of why something is true. A well-written proof is an explanation that someone else can understand. Proper grammar helps the reader follow the logical flow of the proof. Connective words such as "therefore," "hence" and "it follows that" help guide the logical flow, and should be used liberally. Look through this entire book, and you will see that we always use complete sentences and paragraphs, as well as correct grammar and the frequent use of connective words (except, of course, for some instances of typographical errors). Though it may at times seem cumbersome when you are writing a proof, and would like to get it done as quickly as possible, sticking with correct grammar and a readable style will pay off in the long run.

The following two examples of poor writing, both of which contain all the mathematical ideas of the proof of Theorem 2.3.5, are written without regard to proper grammar and style, and are modeled on homework assignments the author has received from students. Compare these versions of the proof with the proof as originally given in Section 2.3.

The first version is genuinely awful, though for reasons the author does not understand, some students seem to be given the impression in high school that this sort of writing is acceptable.

$x^2 = 2$ and x rational

$\therefore x = \frac{n}{m}$

n and m have no common factors

$\left(\frac{n}{m}\right)^2 = 2 \Rightarrow \frac{n^2}{m^2} = 2 \Rightarrow n^2 = 2m^2$ which is even

if n odd, n^2 odd (Exercise 2.2.4) contradiction

$\therefore n$ even

$n = 2k \Rightarrow (2k)^2 = 2m^2 \Rightarrow 4k^2 = 2m^2 \Rightarrow 2k^2 = m^2$

m even (as before)

$\therefore n$ and m both even—impossible (no common factors)

$\therefore x$ is not rational.

This second version is slightly better, being in paragraph form and with a few more words, but it is still far from desirable.

$x^2 = 2$, x is rational. so $x = \frac{n}{m}$; n and m have no common factors. $\left(\frac{n}{m}\right)^2 = 2$, $\frac{n^2}{m^2} = 2$, $n^2 = 2m^2$. If n were odd, then n^2 would be odd by Exercise 2.2.4 a contradiction because $2m^2$ is even because it is divisible by 2. n not odd and hence is even. $n = 2k$ $(2k)^2 = 2m^2$, $4k^2 = 2m^2$, $2k^2 = m^2$. m is even as before   both n and m even—impossible because any two even numbers have 2 as a factor, but n and m have no common factors. x is not rational.

Mathematicians do not write papers and books this way; please do not write this way yourself!

6. Use "=" Signs Properly

One of the hallmarks of poor mathematical writing is the improper use of "=" signs. It is common for beginners in mathematics to write "=" when it is not appropriate, and to drop "=" signs when they are needed. Both these mistakes should be studiously avoided. For example, suppose that a student is asked to take the derivative of the function defined by $f(x) = x^2$ for all real numbers x. The first type of mistake occurs when someone writes something such as "$f(x) = x^2 = 2x = f'(x)$." What is meant is correct, but what is actually written is false (because this function does not equal its derivative), and it is therefore extremely confusing to anyone other than the writer of the statement. THE READER SHOULD NOT HAVE TO GUESS WHAT THE WRITER INTENDED.

The second type of mistake occurs when someone writes "$f(x) = x^2$, and so $2x$." Here again the reader has to guess what is meant by $2x$. If it is meant that $f'(x) = 2x$, then why not write that?

Both of these examples of the improper use of "=" signs may seem far-fetched, but the author has seen these and similar mistakes quite regularly on homework assignments and tests in calculus courses. A proper write-up could be either "$f(x) = x^2$ for all real numbers x, so $f'(x) = 2x$ for all x," or simply "$(x^2)' = 2x$."

Another common type of error involving "=" signs involves lengthier calcula-
tions. Suppose that a student is asked to show that

$$(x^2+2x)(x^2-4)(x^2-2x)=(x^3-4x)^2.$$

An incorrect way of writing the calculation, which the author has seen very regularly
on homework assignments, would be

$$(x^2+2x)(x^2-4)(x^2-2x)=(x^3-4x)^2$$
$$x(x+2)(x-2)(x+2)x(x-2)=(x^3-4x)^2$$
$$x^2(x+2)^2(x-2)^2=(x^3-4x)^2$$
$$[x(x-2)(x+2)]^2=(x^3-4x)^2$$
$$(x^3-4x)^2=(x^3-4x)^2.$$

The problem here is that this calculation as written is a backwards proof, as discussed
in Section 2.5. The calculation starts by stating the equation that we are trying to
prove, and deducing from it an equation that is clearly true. A correct proof should
start from what we know to be true, and deduce that which we are trying to prove.
In principle, if the writer of such a backwards proof were to verify that every step is
reversible, and indicate this fact after the above write-up, then the calculation would
be correct. However, no one ever does that, and doing so would be more complicated
than doing the proof correctly to begin with.

Another incorrect way of writing this same calculation, and also one that the
author has seen regularly, is

$$(x^2+2x)(x^2-4)(x^2-2x)$$
$$x(x+2)(x-2)(x+2)x(x-2)$$
$$x^2(x+2)^2(x-2)^2$$
$$[x(x-2)(x+2)]^2$$
$$(x^3-4x)^2.$$

The problem here is with what is not written, namely, the "=" signs. What is written
is a collections of formulas, without any explicit indication of what equals what.
The reader can often deduce what the writer of such a collection of formulas meant,
but why risk confusion? Written mathematics should strive for clarity, and should
therefore state exactly what the writer means.

A helpful way to think about this second type of error is via the need for correct
grammar. The statement "$(x^2+2x)(x^2-4)(x^2-2x)=(x^3-4x)^2$" is a complete
sentence, with subject "$(x^2+2x)(x^2-4)(x^2-2x)$," with verb "=" and with object
"$(x^3-4x)^2$." To drop the = sign is to drop the verb in this sentence. Few students
would ever turn in a literature paper with missing verbs. And yet, unfortunately, many
students do the equivalent in mathematics homework assignments—not because of
any ill intention, but because, sadly, improper ways of writing lengthy calculations
are actually taught to many students in high school. These errors should be discarded.

There are a number of correct ways of writing the above calculation, for example

$$(x^2 + 2x)(x^2 - 4)(x^2 - 2x) = x(x+2)(x-2)(x+2)x(x-2)$$
$$= x^2(x+2)^2(x-2)^2$$
$$= [x(x-2)(x+2)]^2$$
$$= (x^3 - 4x)^2,$$

and

$$(x^2 + 2x)(x^2 - 4)(x^2 - 2x) = x(x+2)(x-2)(x+2)x(x-2)$$
$$= x^2(x+2)^2(x-2)^2 = [x(x-2)(x+2)]^2 = (x^3 - 4x)^2.$$

The differences between these correctly written calculations and the incorrect ones may seem extremely minor and overly picky, but mathematics is a difficult subject, and every little detail that makes something easier to follow (not to mention logically correct) is worthwhile. A lack of attention to fundamentals such as writing "=" signs correctly can often be a symptom of a general lack of attention to logical thoroughness. A good place to start building logical thinking is with the basics.

7. Define All Symbols and Terms You Make Up

Any mathematical symbols used as variables, even simple ones such as x or n, need to be defined before they are used. Such a definition might be as simple as "let x be a real number." (If you are familiar with programming languages such as C++ or Java, think of having to declare all variables before they are used.) For example, it is not acceptable to write "$x + y$" without somewhere stating that x and y are real numbers (or whatever else they might be); the symbol $+$ needs no definition, because it is not a variable, and its meaning is well-known. The same need for definition holds when the variable is a set, function, relation or anything else. Just because a letter such as n is often used to denote an integer, or the letter f is often used to denote a function, one cannot rely upon such conventions, because these same letters can be used to mean other things as well. If you want to use n to denote an integer, you must say so explicitly, and similarly for f denoting a function.

The need to define variables can get a bit tricky when quantifiers are involved. It is important to understand the scope of any quantifier being used. Suppose that somewhere in a proof you have the statement "for each positive integer n, there is an integer p such that …." The variables n and p are bound variables, and are defined only inside that statement. They cannot be used subsequently, unless they are redefined. If you subsequently want to use a positive integer, you cannot assume that the symbol n has already been defined as such. You would need to define it for the current use, by saying, as usual, something such as "let n be a positive integer."

Finally, it is tempting in the course of a complicated proof to make up new words and symbols, and to use all sorts of exotic alphabets. For the sake of readability, avoid

this temptation as much as possible. Do not use more symbols than absolutely necessary, and avoid exotic letters and complications (such as subscripts of subscripts) where feasible. Try to stick to standard notation. If you do make up some notation, make sure you define it explicitly.

8. Break Up a Long Proof into Steps

If a proof is long and difficult to follow, it is often wise to break it up into steps, or to isolate preliminary parts of the proof as lemmas (which are simply smaller theorems used to prove bigger theorems). If you use lemmas, be sure to state them precisely. Prior to going into the details of a long proof, it is often useful to give a sentence or two outlining the strategy of the proof. All lemmas and their proofs should be placed before they are used in the main theorem. Do not put a lemma inside the proof of the main theorem—doing so can be very confusing to the reader.

9. Distinguish Formal vs. Informal Writing

Writing mathematics involves both formal and informal writing. Formal writing is used for definitions, statements of theorems, proofs and examples; informal writing is for motivation, intuitive explanations, descriptions of the mathematical literature, etc. When writing up the solution to an exercise for a mathematics course, the writing should be a formal proof. A lengthier exposition (such as a thesis or a book) will make use of both kinds of writing—formal writing to make sure that mathematical rigor is maintained, and informal writing to make the text understandable and interesting. Do not confuse the two types of writing, or each will fail to do what it is supposed to do. Intuitive aids such as drawings, graphs, Venn diagrams and the like are extremely helpful when writing up a proof, though such aids should be in addition to the proof, not instead of it.

10. Miscellaneous Writing Tips

Most of the following items are from [KLR89] and [OZ96, pp. 109–118], which have many other valuable suggestions not included here for the sake of brevity. All the examples of poor writing given below are based on what the author has seen in homework assignments and tests.

(A) Do not put a mathematical symbol directly following punctuation. As a corollary, do not start a sentence with a symbol. The only exception to this rule is when the punctuation is part of the mathematical notation, for example (x, y). It is important to avoid ambiguities that might arise from using punctuation without proper care. For example, does the expression "$0 < x, y < 1$" mean that both x and y are between 0 and 1, or does it mean that $0 < x$ and $y < 1$?

    Bad: For all $x > 3$, $x^2 > 9$. $y \leq 0$, so $xy < 0$.

    Good: For all $x > 3$, it follows that $x^2 > 9$. Moreover, because $y \leq 0$, then $xy < 0$.

(B) In the final write-up of a proof, do not use logical symbols, such as $\wedge$, $\vee$, $\exists$, $\forall$ and $\Rightarrow$, as abbreviations for words. Unless you are writing about logic, where logical symbols are necessary, the use of logical symbols makes proofs harder for others to read. Of course, you may use any symbols you want in your scratch work.

Bad: $\forall$ distinct real numbers $x \wedge y$, if $x < y \Rightarrow \exists$ rational q such that $x < q < y$.

Good: For all distinct real numbers x and y, if $x < y$ then there exists a rational number q such that $x < q < y$.

(C) Use equal signs only in equations (and only then when the two sides are equal!). Do not use equal signs when you mean "implies," "the next step is" or "denotes." Do not use equal signs instead of punctuation, or as a substitute for something properly expressed in words.

Bad: $n = $ odd $= 2k + 1$.

Good: Let n be an odd number. Then $n = 2k + 1$ for some integer k.

Bad: For the next step, let $i = i + 1$.

Good: For the next step, replace i with $i + 1$.

Bad: Let $P = $ the # of people in the room.

Good: Let P denote the number of people in the room.

(D) Use consistent notation throughout a proof. For example, if you start a proof using uppercase letters for matrices and lowercase letters for numbers, stick with that notation for the duration of the proof. Do not use the same notation to mean two different things, except when it is unavoidable due to standard mathematical usage—for example, the multiple uses of the notation "(a, b)."

(E) Display long formulas, as well as short ones that are important, on their own lines. Recall, however, that such displayed formulas are still parts of sentences, and require normal punctuation. In particular, if a sentence ends with a displayed formula, do not forget the period at the end of the formula. Also, do not put an unnecessary colon in front of a displayed formula that does not require it.

Bad: From our previous calculations, we see that:

$$x^5 - r\cos\theta = \sqrt{y^2 + 3}$$

Good: From our previous calculations, we see that

$$x^5 - r\cos\theta = \sqrt{y^2 + 3}.$$

(F) Colons are very rarely needed. They are usually either unnecessary, as in the bad example in Item (E), or meant as substitutes for words in situations where words would be much more clear. In mathematical writing, colons should normally be used only in headings or at the starts of lists, and in certain mathematical symbols. Do not use a colon in mathematical writing in a place where you would not use one in non-mathematical writing.

Bad: $x^2 + 10x + 3 = 0$ has two real solutions: $10^2 - 4 \cdot 1 \cdot 3 > 0$.

Good: The equation $x^2 + 10x + 3 = 0$ has two real solutions because $10^2 - 4 \cdot 1 \cdot 3 > 0$.

(G) Capitalize names such as "Theorem 2.3" and "Lemma 17." No capitalization is needed in phrases such as "by the previous theorem."

Exercises

Exercise 2.6.1. State what is wrong with each of the following write-ups; some have more than one error.

(1) We make use of the fact about the real numbers that if $x > 0$, $x^2 > 0$.

(2) To solve $x^2 + 6x = 16$:

$$x^2 + 3 = 8$$

$$x^2 + 6x = 16$$

$$x^2 + 6x - 16 = 0$$

$$(x - 2)(x + 8) = 0$$

and $x = 2$, $x = -8$.

(3) In order to solve $x^2 + 6x = 16$, then $x^2 + 6x - 16 = 0$, $(x - 2)(x + 8) = 0$, and therefore $x = 2$, $x = -8$.

(4) We want to solve the equation $x^2 - 2x = x + 10$. then $x^2 - 3x - 10$, so $(x - 5)(x + 2)$, so 5 and -2.

(5) We want to multiply the two polynomials $(7 + 2y)$ and $(y^2 + 5y - 6)$, which we do by computing

$$(7 + 2y)(y^2 + 5y - 6)$$

$$7y^2 + 35y - 42 + 2y^3 + 10y^2 - 12y$$

$$2y^3 + 17y^2 + 23y - 42$$

the answer is $2y^3 + 17y^2 + 23y - 42$.

(6) A real number x is gloppy if there is some integer n such that $x^2 - n$ is sloppy. Suppose that x is gloppy. Because n is an integer, then its square is an integer, ... (The terms here are meaningless.)

(7) Let x be a real number. Then $x^2 \geq 0$ for all real numbers x, ...

(8) It is known that $\sqrt{a} < a$ for all $a > 1$. Hence $\sqrt{a} + 3 < a + 3$. Hence $(\sqrt{a} + 3)^2 < (a + 3)^2$.

Part II
FUNDAMENTALS

We turn now from the "how" of mathematics, which is the methodology of proofs, to the "what," which is the content of mathematics. In such a vastly broad subject as mathematics, it might be hard to imagine that there is anything common to all aspects of it, but in fact most of modern pure mathematics is based upon a few shared fundamental ideas such as sets, functions and relations. We now discuss the basic features of these ideas. The tone and style of writing in the text now changes correspondingly to the change in our subject matter. We will have less informal discussion, and will write in the more straightforward definition/theorem/proof style used in most advanced mathematics texts (though we will not drop all intuitive explanation). This change in style occurs for several reasons: the need to cover a fairly large amount of material in a reasonable amount of space; the intention of familiarizing the reader with the standard way in which mathematics is written; the fact that with practice (which comes from doing exercises), the reader will not need to be led through the proofs so slowly any more.

3

Sets

No one shall expel us from the paradise that Cantor created for us.

– David Hilbert (1862–1943)

3.1 Introduction

A completely rigorous treatment of mathematics, it might seem, would require us to define every term and prove every statement we encounter. However, unless we want to engage in circular reasoning, or have an argument that goes backwards infinitely far, we have to choose some place as a logical starting point, and then do everything else on the basis of this starting point. This approach is precisely what Euclid attempted to do for geometry in "The Elements," where certain axioms were formulated, and everything else was deduced from them. (We say "attempted" because there are some logical gaps in "The Elements," starting with the proof of the very first proposition in Book I. Fortunately, these gaps can be fixed by using a more complete collection of axioms, such as the one proposed by Hilbert in 1899, which made Euclidean geometry into the rigorous system that most people believed it was all along. The discovery of non-Euclidean geometry is a separate matter. See [WW98] for details on both these issues. This critique of Euclid, it should be stressed, is in no way intended to deny the overwhelming importance of his work.)

What Euclid did not seem to realize was that what holds for theorems also holds for definitions. Consider, for example, Euclid's definition of a straight line, found at the start of "The Elements": "A line is breadthless length. A straight line is a line which lies evenly with itself." By modern standards this definition is rather worthless. What is a "length," breadthless or not, and what is "breadth"? What does it mean for something to "lie evenly with itself"? This last phrase does correspond to our intuitive understanding of straight lines, but if we want to give a rigorous definition such vague language will definitely not do.

The problem with Euclid's definitions is not just their details, but rather the attempt to define every term used. Just as we cannot prove every theorem, and have to start with some unproved results, we cannot define every object, and need to

start with some undefined terms. Even analytic geometry (invented long after Euclid), which appears to do geometry without the use of axioms about geometry, ultimately relies upon some axioms and undefined terms regarding the real numbers. Axioms and undefined terms are unavoidable for rigorous mathematics. The modern approach in mathematics accepts the existence of undefined terms, as long as they are used properly. Ultimately, undefined objects do not bother us because such objects do not so much exist in themselves as they are determined by the axiomatic properties hypothesized for them, and it is these properties that we use in proofs.

A common misconception is that mathematicians spend their time writing down arbitrary collections of axioms, and then playing with them to see what they can deduce from each collection. Mathematics (at least of the pure variety) is then thought to be a kind of formal, abstract game with no purpose other than the fun of playing it (others might phrase it less kindly). In fact, nothing could be further from the truth. Not only would arbitrarily chosen axioms quite likely be contradictory, but, no less important, they would not describe anything of interest. The various axiomatic schemes used in modern mathematics, in such areas as group theory, linear algebra and topology, were arrived at only after long periods of study, involving many concrete examples and much trial and error. You will see these various collections of axioms in subsequent mathematics courses. The point of axiomatic systems is to rigorize various parts of mathematics that are otherwise of interest, for either historical or applied reasons. Of course, mathematicians do find real pleasure in doing mathematics—that is why most of us do it—but it is the pleasure of thinking about subtle and fascinating ideas, not the pleasure of playing games.

In this text we will not focus on developing mathematics in an axiomatic fashion, though a few systems of axioms will be given in Chapter 7. In the present chapter we will discuss the common basis for all systems of axioms used in contemporary mathematics, which is set theory. Though of surprisingly recent vintage, having been developed by Georg Cantor in the late nineteenth century, set theory has become widely accepted among mathematicians as the starting place for rigorous mathematics. We will take an intuitive approach to set theory (often referred to as "naive set theory"), but then build on it rigorously. Set theory itself can be done axiomatically, though doing so is non-trivial, and there are a number of different approaches that are used. In Section 3.5 we will informally discuss the most common axiomatic approach to set theory, the Zermelo–Fraenkel Axioms, but other than in that section we maintain the standard approach of taking an intuitive approach to the foundations of set theory, but then proving everything else rigorously on the basis of sets.

For additional information about naive set theory see the classic reference [Hal60]; see [EFT94, Section 7.4] for a discussion of the role of set theory as a basis for mathematics; and see [Sup60], [Ham82], [Dev93] and [Vau95] for more about axiomatic set theory.

3.2 Sets—Basic Definitions

The basic undefined term we will use is that of a **set**, which we take to be any collection of objects, not necessarily mathematical ones. For example, we can take the set of all people born in San Francisco in 1963. The objects contained in the set are called the **elements** or **members** of the set. If A is a set and a is an element of A, we write

$$a \in A.$$

If a is not in the set A, we write

$$a \notin A.$$

Given any set A and any object a, we assume that precisely one of $a \in A$ or $a \notin A$ holds.

The simplest way of presenting a set is to list its elements, which by standard convention are written between curly brackets. For example, the set consisting of the letters a, b, c and d is written

$$\{a,b,c,d\}.$$

The order in which the elements of a set are listed is irrelevant. Hence the set $\{1,2,3\}$ is the same as the set $\{2,3,1\}$. Each element of a set is listed once and only once, so that we would never write $\{1,2,2,3\}$.

There are four sets of numbers that we will use regularly: the set of **natural numbers**

$$\{1,2,3,\ldots\},$$

denoted $\mathbb{N}$; the set of **integers**

$$\{\ldots,-2,-1,0,1,2,\ldots\},$$

denoted $\mathbb{Z}$; the set of **rational numbers**, denoted $\mathbb{Q}$, which is the set of fractions; the set of **real numbers**, denoted $\mathbb{R}$, which is the set of all the numbers that are informally thought of as forming the number line.

An extremely valuable set we will regularly encounter is the **empty set** (also called the **null set**) which is the set that does not have any elements in it. That is, the empty set is the set { }. This set is denoted $\emptyset$. It may seem strange to consider a set that doesn't have anything in it, but the role of the empty set in set theory is somewhat analogous to the role of zero in arithmetic. (The number zero was a historically late arrival, and presumably might have seemed strange to some at first, just as the empty set might seem strange at first today; zero does not seem strange to us today because we start getting used to it at a young age).

It is sometimes not convenient, or not possible, to list explicitly all the elements of a set. In such situations it is sometimes possible to present a set by describing it as the set of all elements satisfying some criteria. For example, consider the set of all integers that are perfect squares. We could write this set as

$$S = \{n \in \mathbb{Z} \mid n \text{ is a perfect square}\},$$

which is read "the set of all n in $\mathbb{Z}$ such that n is a perfect square." Some books use a colon ":" instead of a vertical line in the above set notation, though the meaning is exactly the same, namely, "such that." If we want to write the above set even more carefully we could write

$$S = \{n \in \mathbb{Z} \mid n = k^2 \text{ for some } k \in \mathbb{Z}\}.$$

If we wanted to emphasize the existential quantifier, we could write

$$S = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k^2\}. \tag{3.2.1}$$

The letters n and k used in this definition are "dummy variables." We would obtain the exact same set if we wrote

$$S = \{x \in \mathbb{Z} \mid \text{there exists } r \in \mathbb{Z} \text{ such that } x = r^2\}. \tag{3.2.2}$$

The above method of defining sets is quite straightforward, but there is one point about this method that needs to be stressed. Because the letters x and r in Equation 3.2.2 are dummy variables, we cannot use them outside the "$\{ \mid \}$" notation without redefinition. Hence, if we want to refer to some element of the set defined in Equation 3.2.1 and Equation 3.2.2, for example pointing out that such elements must be non-negative, it would not be correct to say simply "observe that $x \geq 0$." By contrast, it would be correct to say "observe that $x \geq 0$ for all $x \in S$." However, this latter formulation has the defect that if we want to continue to discuss elements in S, we would have to define x once again, because the x in "$x \geq 0$ for all $x \in S$" is bound by the quantifier. A better approach would be to write "let $x \in S$; then $x \geq 0$." Now that x has been defined as an element of S, not bound by a quantifier, we can use it as often as we wish without redefinition.

An example of the above method of defining sets is seen in the following widely used definition.

Definition 3.2.1. An **open bounded interval** is a set of the form

$$(a,b) = \{x \in \mathbb{R} \mid a < x < b\},$$

where $a, b \in \mathbb{R}$ and $a \leq b$. A **closed bounded interval** is a set of the form

$$[a,b] = \{x \in \mathbb{R} \mid a \leq x \leq b\},$$

where $a, b \in \mathbb{R}$ and $a \leq b$. A **half-open interval** is a set of the form

$$[a,b) = \{x \in \mathbb{R} \mid a \leq x < b\} \quad \text{or} \quad (a,b] = \{x \in \mathbb{R} \mid a < x \leq b\},$$

where $a, b \in \mathbb{R}$ and $a \leq b$. An **open unbounded interval** is a set of the form

$$(a,\infty) = \{x \in \mathbb{R} \mid a < x\} \quad \text{or} \quad (-\infty,b) = \{x \in \mathbb{R} \mid x < b\} \quad \text{or} \quad (-\infty,\infty) = \mathbb{R},$$

where $a, b \in \mathbb{R}$. A **closed unbounded interval** is a set of the form

$$[a,\infty) = \{x \in \mathbb{R} \mid a \leq x\} \quad \text{or} \quad (-\infty,b] = \{x \in \mathbb{R} \mid x \leq b\},$$

where $a, b \in \mathbb{R}$. $\triangle$

Observe that there are no intervals that are "closed" at ∞ or $-\infty$, for example there is no interval of the form $[a, \infty]$, because "∞" is not a real number, and therefore it cannot be included in an interval contained in the real numbers. The symbol "∞" is simply a shorthand way of saying that an interval "goes on forever."

If $a, b \in \mathbb{R}$ and $a \leq b$, then the set (a, b) is "contained in" the set $[a, b]$. This notion of a set being contained in another is formalized as follows.

Definition 3.2.2. Let A and B be sets. The set A is a **subset** of the set B, denoted $A \subseteq B$, if $x \in A$ implies $x \in B$. If A is not a subset of B, we write $A \not\subseteq B$. $\triangle$

Observe that if A and B are sets and if $A \not\subseteq B$, then it is still possible that some of the elements of A are in B, just not all. See Figure 3.2.1 for a schematic drawing of $A \subseteq B$ and $A \not\subseteq B$.

$$A \subseteq B \qquad\qquad A \not\subseteq B$$

Fig. 3.2.1.
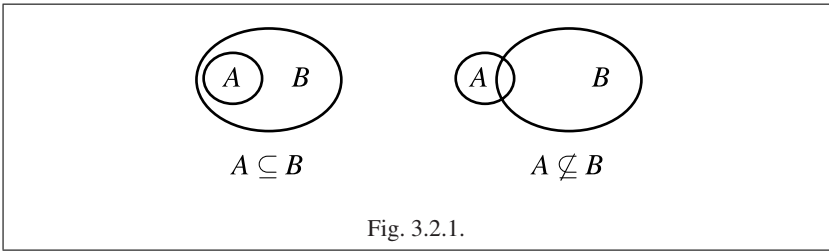
Example 3.2.3.

(1) Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 3\}$. Then $B \subseteq A$ and $A \not\subseteq B$.

(2) Let M be the set of all men, and let T be the set of all proctologists. Then $T \not\subseteq M$ because not all proctologists are men, and $M \not\subseteq T$ because not all men are proctologists. $\diamond$

There is a standard strategy for proving a statement of the form "$A \subseteq B$," which is to take an arbitrary element $a \in A$, and then to use the definitions of A and B to deduce that $a \in B$. Such a proof typically has the following form.

Proof. Let $a \in A$.

$$\vdots$$

(argumentation)

$$\vdots$$

Then $a \in B$. Hence $A \subseteq B$. $\square$

We will see a number of proofs using this strategy throughout this chapter. To prove a statement of the form "$A \not\subseteq B$," by contrast, we simply need to find some $a \in A$ such that $a \notin B$, a fact that seems intuitively clear, and that can be seen formally as follows. The statement $A \subseteq B$ can be written as $(\forall x)([x \in A] \rightarrow [x \in B])$. Then $A \not\subseteq B$

can be written as $\neg(\forall x)([x \in A] \rightarrow [x \in B])$, which is equivalent to $(\exists x)([x \in A] \wedge [x \notin B])$ by Fact 1.5.1 (1) and Fact 1.3.2 (14).

It is important to distinguish between the notion of an object being an element of a set, and the notion of a set being a subset of another set. For example, let $A = \{a,b,c\}$. Then $a \in A$ and $\{a\} \subseteq A$ are true, whereas the statements "$a \subseteq A$" and "$\{a\} \in A$" are false. Also, observe that a set can be an element of another set. Let $B = \{\{a\},b,c\}$. Observe that B is not the same as the set A. Then $\{a\} \in B$ and $\{\{a\}\} \subseteq B$ are true, but "$a \in B$" and "$\{a\} \subseteq B$" are false.

The following lemma states some basic properties of subsets. The proof of this lemma, our first proof about sets, makes repeated use of the strategy mentioned above for showing that one set is a subset of another set.

Lemma 3.2.4. *Let A, B and C be sets.*

    1. *$A \subseteq A$.*
    2. *$\emptyset \subseteq A$.*
    3. *If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Proof.

    (1). To show that $A \subseteq A$, we start by choosing an arbitrary element $a \in A$, where we think of this "A" as the one on the left-hand side of the expression "$A \subseteq A$." It then follows that $a \in A$, where we now think of this "A" as the one on the right-hand side of the expression "$A \subseteq A$." Hence $A \subseteq A$, using the definition of subsets.

    (2). We give two proofs, because both are instructive. First, we have a direct proof. To show that $\emptyset \subseteq A$, we need to show that if $a \in \emptyset$, then $a \in A$. Because $a \in \emptyset$ is always false, then the logical implication "if $a \in \emptyset$, then $a \in A$" is always true, using the precise definition of the conditional given in Section 1.2.

Next, we have a proof by contradiction. Suppose that $\emptyset \nsubseteq A$. Then there exists some $x \in \emptyset$ such that $x \notin A$. This statement cannot be true, however, because there is no x such that $x \in \emptyset$. We have therefore reached a contradiction, and hence the desired result is true.

This proof by contradiction might not appear to fit the standard outline for such proofs as described in Section 2.3, because it does not appear as if we are viewing the statement being proved as having the form $P \rightarrow Q$. In fact, there are two ways of viewing the statement being proved as having this form. For the direct proof given above, we viewed the statement being proved as $(\forall A)([a \in \emptyset] \rightarrow [a \in A])$. We then chose an arbitrary set A, and proved the statement $[a \in \emptyset] \rightarrow [a \in A]$. For the proof by contradiction, we viewed the statement being proved as "if A is a set, then $\emptyset \subseteq A$," and then indeed used our standard method of doing proof by contradiction.

    (3). This proof, having no logical tricks, is extremely typical. Let $a \in A$. Because $A \subseteq B$, it follows that $a \in B$. Because $B \subseteq C$, it follows that $a \in C$. Therefore we see that $a \in A$ implies $a \in C$, and hence $A \subseteq C$. $\square$

When are two sets equal to one another? Intuitively, two sets are equal when they have the same elements. We formally define this concept as follows.

Definition 3.2.5. Let A and B be sets. The set A **equals** the set B, denoted $A = B$, if $A \subseteq B$ and $B \subseteq A$. The set A is a **proper subset** of the set B, denoted $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$.   △

There is a bit of variation in the mathematical literature for the notation used for proper subsets. Some texts use $A \subset B$ to mean A is a proper subset of B, whereas others use the notation $A \subset B$ to mean what we write as $A \subseteq B$.

Example 3.2.6.

(1) Let A and B be the sets in Example 3.2.3 (1). Then B is a proper subset of A.

(2) Let $X = \{a, b, c\}$, and let $Y = \{c, b, a\}$. Then clearly $X \subseteq Y$ and $Y \subseteq X$, so $X = Y$.

(3) Let

$$P = \{x \in \mathbb{R} \mid x^2 - 5x + 6 < 0\},$$

and

$$Q = \{x \in \mathbb{R} \mid 2 < x < 3\}.$$

We will show that $P = Q$, putting in more detail than is really necessary for a problem at this level of difficulty, but we want to make the proof strategy as explicit as possible.

First, we show that $P \subseteq Q$. Let $y \in P$. Then $y^2 - 5y + 6 < 0$. Hence $(y-2)(y-3) < 0$. It follows that either $y - 2 < 0$ and $y - 3 > 0$, or that $y - 2 > 0$ and $y - 3 < 0$. If $y - 2 < 0$ and $y - 3 > 0$, then $y < 2$ and $3 < y$; because there is no number that satisfies both these inequalities, then this case cannot occur. If $y - 2 > 0$ and $y - 3 < 0$, then $2 < y$ and $y < 3$. Hence $2 < y < 3$. It follows that $y \in Q$. Therefore $P \subseteq Q$.

Next, we show that $Q \subseteq P$. Let $z \in Q$. Then $2 < z < 3$. Hence $2 < z$ and $z < 3$, and so $z - 2 > 0$ and $z - 3 < 0$. Therefore $(z-2)(z-3) < 0$, and therefore $z^2 - 5z + 6 < 0$. Hence $z \in P$. Therefore $Q \subseteq P$.

By combining the previous two paragraphs we deduce that $P = Q$.   ◇

Example 3.2.6 (3) may seem to be much ado about nothing, because the result proved is trivial, but the strategy used is not. Virtually every time we show that two sets A and B are equal, we go back to the definition of equality of sets. The strategy for proving a statement of the form "$A = B$" for sets A and B is therefore to prove that $A \subseteq B$ and that $B \subseteq A$. Such a proof typically has the following form.

Proof. Let $a \in A$.

$\vdots$

(argumentation)

$\vdots$

Then $a \in B$. Therefore $A \subseteq B$.

Next, Let $b \in B$.

$\vdots$

(argumentation)

$$\vdots$$

Then $b \in A$. Hence $B \subseteq A$.

We conclude that $A = B$. □

We will see a number of examples of this strategy, starting with the proof of Theorem 3.3.3 (4) in the next section.

The following lemma gives the most basic properties of equality of sets. The three parts of the lemma correspond to three properties of relations we will discuss in Sections 5.1 and 5.3.

Lemma 3.2.7. *Let A, B and C be sets.*

1. $A = A$.
2. *If $A = B$ then $B = A$.*
3. *If $A = B$ and $B = C$, then $A = C$.*

Proof. All three parts of this lemma follow straightforwardly from the definition of equality of sets together with Lemma 3.2.4. Details are left to the reader. □

In some situations we will find it useful to look at not just one subset of a given set, but at all subsets of the set. In particular, we can form a new set, the elements of which are the subsets of the given set.

Definition 3.2.8. Let A be a set. The **power set** of A, denoted $\mathcal{P}(A)$, is the set defined by

$$\mathcal{P}(A) = \{X \mid X \subseteq A\}. \qquad\qquad \triangle$$

Example 3.2.9.

(1) Because $\emptyset \subseteq \emptyset$, then $\mathcal{P}(\emptyset) = \{\emptyset\}$. In particular, we see that $\mathcal{P}(\emptyset) \neq \emptyset$.

(2) Let $A = \{a, b, c\}$. Then the subsets of A are $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a,b\}$, $\{a,c\}$, $\{b,c\}$ and $\{a,b,c\}$. The last of these subsets is not proper, but we need all subsets, not only the proper ones. Therefore

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}.$$

It can be seen intuitively that if A is a finite set with n elements, then $\mathcal{P}(A)$ is a finite set with 2^n elements; by Part (1) of this exercise we see that this formula holds even when $n = 0$. This formula is proved in Theorem 7.7.10 (1). ◇

Sets can be either finite or infinite in size. The set A in Example 3.2.9 (2) is finite, whereas sets such as $\mathbb{N}$ or $\mathbb{R}$ are infinite. For now we will use the terms "finite" and "infinite" intuitively. These concepts will be defined rigorously in Section 6.5. If a set A is finite, then we use the notation $|A|$ to denote the number of elements in A (often referred to as the "cardinality" of A). Some basic facts about the cardinalities of finite sets can be found in Sections 6.5, 7.6 and 7.7.

<div style="text-align:center">

Exercises

</div>

Exercise 3.2.1. How many elements does the set $A = \{a, b, \{a,b\}\}$ have?

Exercise 3.2.2. Which of the following are true and which are false?

(1) $3 \in (3,5]$.
(2) $10 \notin (-\infty, \pi^2]$.
(3) $7 \in \{2,3,4,\ldots,11\}$.
(4) $\pi \in (2,\infty)$.
(5) $-1.3 \in \{\ldots,-3,-2,-1\}$.

(6) $[1,2] \subseteq \{0,1,2,3\}$.
(7) $\{-1,0,1\} \subseteq [-1,1)$.
(8) $[5,7] \subseteq (4,\infty)$.
(9) $\{2,4,8,16,\ldots\} \subseteq [2,\infty)$.

Exercise 3.2.3. What are the following sets commonly called?

(1) $\{n \in \mathbb{Z} \mid n = 2m \text{ for some } m \in \mathbb{Z}\}$.
(2) $\{k \in \mathbb{N} \mid \text{there exist } p, q \in \mathbb{N} \text{ such that } k = pq, \text{ and that } 1 < p < k \text{ and } 1 < q < k\}$.
(3) $\{x \in \mathbb{R} \mid \text{there exist } a, b \in \mathbb{Z} \text{ such that } b \neq 0 \text{ and } x = \frac{a}{b}\}$.

Exercise 3.2.4. Let P be the set of all people, let M be the set of all men and let F be the set of all women. Describe each of the following sets with words.

(1) $\{x \in P \mid x \in M \text{ and } x \text{ has a child}\}$.
(2) $\{x \in P \mid \text{there exist } y, z \in P \text{ such that } y \text{ is a child of } x, \text{ and } z \text{ is a child of } y\}$.
(3) $\{x \in P \mid \text{there exist } m \in F \text{ such that } x \text{ is married to } m\}$.
(4) $\{x \in P \mid \text{there exist } q \in P \text{ such that } x \text{ and } q \text{ have the same mother}\}$.
(5) $\{x \in P \mid \text{there exist } h \in P \text{ such that } h \text{ is older than } x\}$.
(6) $\{x \in P \mid \text{there exist } n \in M \text{ such that } x \text{ is the child of } n, \text{ and } x \text{ is older than } n\}$.

Exercise 3.2.5. Describe the following sets in the style of Equation 3.2.1.

(1) The set of all positive real numbers.
(2) The set of all odd integers.
(3) The set of all rational numbers that have a factor of 5 in their denominators.
(4) The set $\{-64, -27, -8, -1, 0, 1, 8, 27, 64\}$.
(5) The set $\{1, 5, 9, 13, 17, 21, \ldots\}$.

Exercise 3.2.6. We assume for this exercise that functions are intuitively familiar to the reader (a formal definition will be given in Chapter 4). Let F denote the set of all functions from the real numbers to the real numbers; let D denote the set of all differentiable functions from the real numbers to the real numbers; let P denote the set of all polynomial functions from the real numbers to the real numbers; let C denote the set of all continuous functions from the real numbers to the real numbers; let E denote the set of all exponential functions from the real numbers to the real numbers. Which of these sets are subsets of which?

Exercise 3.2.7. Among the following sets, which is a subset of which?

M is the set of all men;

W is the set of all women;

P is the set of all parents;

O is the set of all mothers;

F is the set of all fathers;

U is the set of all uncles;

A is the set of all aunts;

C is the set of all people who are children of other people.

Exercise 3.2.8. Among the following sets, which is a subset of which?

$$C = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k^4\};$$
$$E = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = 2k\};$$
$$P = \{n \in \mathbb{Z} \mid n \text{ is a prime number}\};$$
$$N = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k^8\};$$
$$S = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = 6k\};$$
$$D = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k - 5\};$$
$$B = \{n \in \mathbb{Z} \mid n \text{ is non-negative}\}.$$

Exercise 3.2.9. Find sets A and B such that $A \in B$ and $A \subseteq B$. (It might appear as if we are contradicting what was discussed after Example 3.2.3; the solution, however, is the "exception that proves the rule.")

Exercise 3.2.10. Let A, B and C be sets. Suppose that $A \subseteq B$ and $B \subseteq C$ and $C \subseteq A$. Prove that $A = B = C$.

Exercise 3.2.11. [Used in Theorem 3.5.6.] Let A and B be sets. Prove that it is not possible that $A \subsetneq B$ and $B \subseteq A$ are both true.

Exercise 3.2.12. Let A and B be any two sets. Is it true that one of $A \subseteq B$ or $A = B$ or $A \supseteq B$ must be true? Give a proof or a counterexample.

Exercise 3.2.13. Let $A = \{x, y, z, w\}$. List all the elements in $\mathcal{P}(A)$?

Exercise 3.2.14. Let A and B be sets. Suppose that $A \subseteq B$. Prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Exercise 3.2.15. List all elements of each of the following sets.

(1) $\mathcal{P}(\mathcal{P}(\emptyset))$.   **(2)** $\mathcal{P}(\mathcal{P}(\{\emptyset\}))$.

Exercise 3.2.16. Which of the following are true and which are false?

(1) $\{\emptyset\} \subseteq G$ for all sets G.   **(6)** $\emptyset \in \mathcal{P}(G)$ for all sets G.
(2) $\emptyset \subseteq G$ for all sets G.   **(7)** $\{\{\emptyset\}\} \subseteq \mathcal{P}(\emptyset)$.
(3) $\emptyset \subseteq \mathcal{P}(G)$ for all sets G.   **(8)** $\{\emptyset\} \subseteq \{\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}\}$.
(4) $\{\emptyset\} \subseteq \mathcal{P}(G)$ for all sets G.   **(9)** $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.
(5) $\emptyset \in G$ for all sets G.

3.3 Set Operations

There are a number of ways to make new sets out of old, somewhat analogous to combining numbers via addition and multiplication. A closer analogy is the way in which we combined statements in Section 1.2. The two most basic set operations, which we now describe, correspond to the logical operations "or" and "and."

Definition 3.3.1. Let A and B be sets. The **union** of A and B, denoted $A \cup B$, is the set defined by

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}.$$

The **intersection** of A and B, denoted $A \cap B$, is the set defined by

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}. \qquad\qquad \triangle$$

If A and B are sets, the set $A \cup B$ is the set containing everything that is either in A or B or both (recall our discussion of the mathematical use of the word "or" in Section 1.2). The set $A \cap B$ is the set containing everything that is in both A and B.

Example 3.3.2. Let $A = \{x, y, z, p\}$ and $B = \{x, q\}$. Then

$$A \cup B = \{x, y, z, p, q\} \quad \text{and} \quad A \cap B = \{x\}. \qquad\qquad \Diamond$$

To help visualize unions and intersections of sets (as well as other constructions we will define), we can make use of what are known as Venn diagrams. A Venn diagram for a set is simply a region of the plane that schematically represents the set. See Figure 3.3.1 (i) for a Venn diagram representing two sets A and B, placed in the most general possible relation to each other. In Figure 3.3.1 (ii) the region representing $A \cup B$ is shaded, and in Figure 3.3.1 (iii) the region representing $A \cap B$ is shaded.

Fig. 3.3.1.
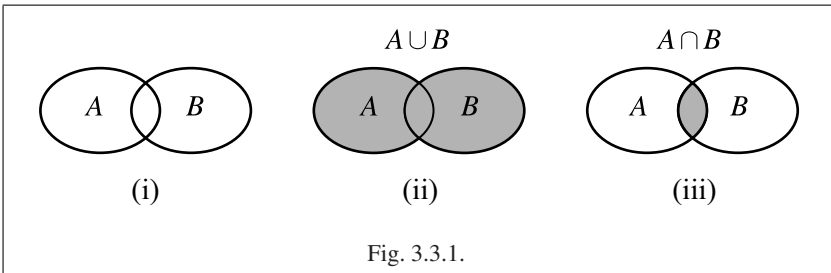
Venn diagrams can be useful for convincing ourselves of the intuitive truth of various propositions concerning sets. For instance, we will prove in Theorem 3.3.3 (5) that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ for any three sets A, B and C. To gain an intuitive feeling for this result, we can find the region in a Venn diagram for each of the two sides of the equation, and then observe that the two regions are the same, namely, the shaded region in Figure 3.3.2. Although Venn diagrams seem much easier to use

than proofs, a Venn diagram is no more than a visual aid, and is never a substitute for a real proof. Moreover, it is tricky to use Venn diagrams for more than three sets at a time, and this severely limits their use.

Fig. 3.3.2.
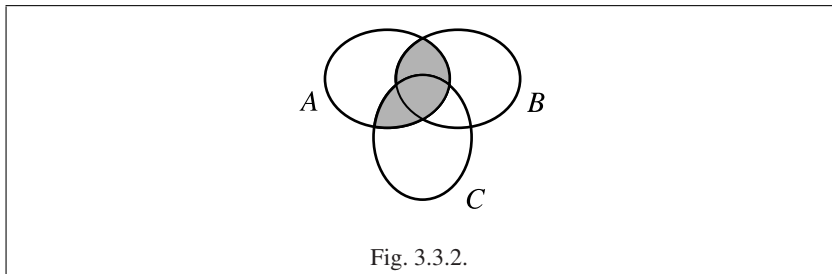
Do the familiar properties of addition and multiplication of numbers (such as commutativity and associativity) also hold for union and intersection of sets? The following theorem shows that such properties do hold, although they are not exactly the same as for addition and multiplication.

Theorem 3.3.3. *Let A, B and C be sets.*

1. *$A \cap B \subseteq A$ and $A \cap B \subseteq B$. If X is a set such that $X \subseteq A$ and $X \subseteq B$, then $X \subseteq A \cap B$.*
2. *$A \subseteq A \cup B$ and $B \subseteq A \cup B$. If Y is a set such that $A \subseteq Y$ and $B \subseteq Y$, then $A \cup B \subseteq Y$.*
3. *$A \cup B = B \cup A$ and $A \cap B = B \cap A$ (Commutative Laws).*
4. *$(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$ (Associative Laws).*
5. *$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (Distributive Laws).*
6. *$A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$ (Identity Laws).*
7. *$A \cup A = A$ and $A \cap A = A$ (Idempotent Laws).*
8. *$A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$ (Absorption Laws).*
9. *If $A \subseteq B$, then $A \cup C \subseteq B \cup C$ and $A \cap C \subseteq B \cap C$.*

Proof. We will prove Parts (4) and (5), leaving the rest to the reader in Exercise 3.3.6.

(4). We will show that $(A \cup B) \cup C = A \cup (B \cup C)$; the other equation can be proved similarly, and we omit the details. As usual, the equality of the two sets under consideration is demonstrated by showing that each is a subset of the other.

Let $x \in (A \cup B) \cup C$. Then $x \in A \cup B$ or $x \in C$. First, suppose that $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in A$ then $x \in A \cup (B \cup C)$ by Part (2) of this theorem, and if $x \in B$ then $x \in B \cup C$, and hence $x \in A \cup (B \cup C)$. Second, suppose that $x \in C$. It follows from Part (2) of this theorem that $x \in B \cup C$, and hence $x \in A \cup (B \cup C)$. Putting the two cases together, we deduce that $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

The proof that $A \cup (B \cup C) \subseteq (A \cup B) \cup C$ is similar to the above proof, simply changing the roles of A and C, and we omit the details.

We deduce that $(A \cup B) \cup C = A \cup (B \cup C)$.

(5). We prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; the other equation can be proved similarly. Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Hence $x \in B$ or $x \in C$. If $x \in B$ we deduce that $x \in A \cap B$, and if $x \in C$ we deduce that $x \in A \cap C$. In either case, we use Part (2) of this theorem to see that $x \in (A \cap B) \cup (A \cap C)$. Therefore $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Now let $y \in (A \cap B) \cup (A \cap C)$. Then $y \in A \cap B$ or $y \in A \cap C$. First, suppose that $y \in A \cap B$. Then $y \in A$ and $y \in B$. Hence $y \in B \cup C$ by Part (2) of the theorem, and therefore $y \in A \cap (B \cup C)$. Second, suppose that $y \in A \cap C$. A similar argument to the previous case shows that $y \in A \cap (B \cup C)$; we omit the details. Combining the two cases we deduce that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

We conclude that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. $\qquad\qquad$ $\square$

It is seen in Part (5) of Theorem 3.3.3 that both union and intersection distribute over each other, which is quite different from addition and multiplication of numbers, where multiplication distributes over addition, but not vice versa.

The following definition formalizes the notion of two sets having no elements in common.

Definition 3.3.4. Let A and B be sets. The sets A and B are **disjoint** if $A \cap B = \emptyset$. $\quad \triangle$

Example 3.3.5. Let E be the set of even integers, let O be the set of odd integers and let P be the set of prime numbers. Then E and O are disjoint, whereas E and P are not disjoint (because $E \cap P = \{2\}$). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\Diamond$

Another useful set operation is given in the following definition.

Definition 3.3.6. Let A and B be sets. The **difference** (also called the **set difference**) of A and B, denoted $A - B$, is the set defined by

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}. \qquad\qquad\qquad \triangle$$

Some books use the notation $A \setminus B$ instead of $A - B$. The set $A - B$ is the set containing everything that is in A but is not in B. The set $A - B$ is defined for any two sets A and B; it is not necessary to have $B \subseteq A$. See Figure 3.3.3 for a Venn diagram of the $A - B$.

$A - B$

Fig. 3.3.3.
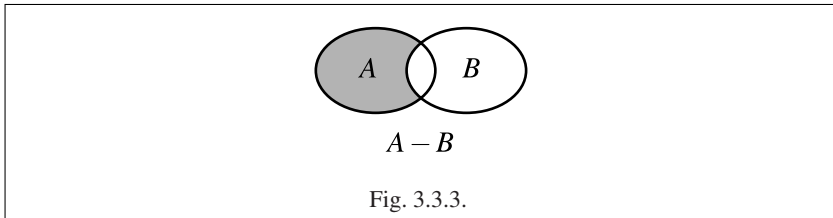
Example 3.3.7. Let A and B be the sets in Example 3.3.2. Then

$$A - B = \{y, z, p\}. \qquad \Diamond$$

The following theorem gives some standard properties of set difference.

Theorem 3.3.8. *Let A, B and C be sets.*

1. $A - B \subseteq A$.
2. $(A - B) \cap B = \emptyset$.
3. $A - B = \emptyset$ *if and only if* $A \subseteq B$.
4. $B - (B - A) = A$ *if and only if* $A \subseteq B$.
5. *If* $A \subseteq B$, *then* $A - C = A \cap (B - C)$.
6. *If* $A \subseteq B$, *then* $C - A \supseteq C - B$.
7. $C - (A \cup B) = (C - A) \cap (C - B)$ *and* $C - (A \cap B) = (C - A) \cup (C - B)$ *(De Morgan's Laws).*

Proof. We will prove Part (7), leaving the rest to the reader in Exercise 3.3.7.

(7). We will show that $C - (A \cup B) = (C - A) \cap (C - B)$; the other equation can be proved similarly, and we omit the details. Let $x \in C - (A \cup B)$. Then $x \in C$ and $x \notin A \cup B$. It follows that $x \notin A$ and $x \notin B$, because $x \in A$ or $x \in B$ would imply that $x \in A \cup B$. Because $x \in C$ and $x \notin A$, then $x \in C - A$. Because $x \in C$ and $x \notin B$, then $x \in C - B$. Hence $x \in (C - A) \cap (C - B)$. Therefore $C - (A \cup B) \subseteq (C - A) \cap (C - B)$.

Now let $y \in (C - A) \cap (C - B)$. Hence $y \in C - A$ and $y \in C - B$. Because $y \in C - A$, it follows that $y \in C$ and $y \notin A$. Because $y \in C - B$, it follows that $y \in C$ and $y \notin B$. Because $y \notin A$ and $y \notin B$, it follows that $y \notin A \cup B$. Therefore $y \in C - (A \cup B)$. Hence $(C - A) \cap (C - B) \subseteq C - (A \cup B)$.

We conclude that $C - (A \cup B) = (C - A) \cap (C - B)$. $\qquad \square$

There is one more fundamental way of forming new sets out of old that we will be using regularly. Think of how the plane is coordinatized by ordered pairs of real numbers. In the following definition we make use of the notion of an ordered pair of elements, denoted (a, b), where a and b are elements of some given sets. Unlike a set $\{a, b\}$, where the order of the elements does not matter (so that $\{a, b\} = \{b, a\}$), in an ordered pair the order of the elements does matter. We take this idea intuitively, though it can be defined rigorously in terms of sets (see [Mac96]). The idea is to represent the ordered pair (a, b) as the set $\{\{a\}, \{a, b\}\}$. Though it may seem obvious, it is important to state that the ordered pair (a, b) equals the ordered pair (c, d) if and only if $a = c$ and $b = d$. (The notation "(a, b)" used to denote an ordered pair is, unfortunately, identical to the notation "(a, b)" used to denote an open bounded interval of real numbers, as defined in Section 3.2. Both uses of this notation are very widespread, so we are stuck with them. In practice the meaning of "(a, b)" is usually clear from the context.)

Definition 3.3.9. Let A and B be sets. The **product** (also called the **Cartesian product**) of A and B, denoted $A \times B$, is the set

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

where (a,b) denotes an ordered pair.   △

Example 3.3.10.

(1) Let $A = \{a,b,c\}$ and $B = \{1,2\}$. Then

$$A \times B = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}.$$

(2) Roll a pair of dice. The possible outcomes are

$$\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6).
\end{array}$$

This table is the product of the set $\{1,\ldots,6\}$ with itself.

(3) It can be seen intuitively that if A and B are finite sets, then $A \times B$ is finite and $|A \times B| = |A| \cdot |B|$. This fact is proved in Theorem 7.6.3.   ◊

We can form the product of more than two sets, and although there is no essential problem doing so, there is one slight technicality worth mentioning. Suppose that we want to form the product of the three sets A, B and C. Keeping these sets in the given order, we could form the triple product in two ways, yielding the sets $(A \times B) \times C$ and $A \times (B \times C)$. Strictly speaking, these two triple products are not the same, because the first has elements of the form $((a,b),c)$, whereas the second has elements of the form $(a,(b,c))$. There is, however, no practical difference between the two triple products, and we will therefore gloss over this technicality, simply referring to $A \times B \times C$, and writing a typical element as (a,b,c). The precise relation between $(A \times B) \times C$ and $A \times (B \times C)$, which is given in Exercise 4.4.6, makes use of the concepts developed in Section 4.4.

Example 3.3.11. We can think of $\mathbb{R}^2$, which is defined in terms of ordered pairs of real numbers, as $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Similarly, we think of $\mathbb{R}^n$ as

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ times}}.$$ ◊

The following theorem gives some standard properties of products of sets.

Theorem 3.3.12. *Let A, B, C and D be sets.*

1. *If $A \subseteq B$ and $C \subseteq D$, then $A \times C \subseteq B \times D$.*
2. *$A \times (B \cup C) = (A \times B) \cup (A \times C)$ and $(B \cup C) \times A = (B \times A) \cup (C \times A)$*   *(Distributive Laws).*
3. *$A \times (B \cap C) = (A \times B) \cap (A \times C)$ and $(B \cap C) \times A = (B \times A) \cap (C \times A)$*   *(Distributive Laws).*

4. $A \times \emptyset = \emptyset$ and $\emptyset \times A = \emptyset$.

5. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

Proof. We will prove Part (3), leaving the rest to the reader in Exercise 3.3.8.

(3). We will prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$; the other equation can be proved similarly, and we omit the details. As usual, we will show that the sets on the two sides of the equation are subsets of each other. First, we show that $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$. This part of the proof proceeds in the standard way. Let $y \in (A \times B) \cap (A \times C)$. It would not be correct at this point to say that y equals some ordered pair (p, q), because $(A \times B) \cap (A \times C)$ does not have the form $X \times Y$ for some sets X and Y. We can say, however, that $y \in A \times B$ and $y \in A \times C$. Using the former we deduce that $y = (a, b)$ for some $a \in A$ and $b \in B$. Because $y \in A \times C$, we then have $(a, b) \in A \times C$. It follows that $b \in C$. Hence $b \in B \cap C$. Therefore $y = (a, b) \in A \times (B \cap C)$. We deduce that $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

Next, we show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$. In this part of the proof we take a slightly different approach than the one we have been using so far (though the standard method would work here too). By Lemma 3.2.4 (1) we know that $A \subseteq A$. Using the first sentence in Theorem 3.3.3 (1) we know that $B \cap C \subseteq B$ and $B \cap C \subseteq C$. By Part (1) of this theorem we deduce that $A \times (B \cap C) \subseteq A \times B$ and $A \times (B \cap C) \subseteq A \times C$. It now follows from the second sentence in Theorem 3.3.3 (1) that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

We conclude that $A \times (B \cap C) = (A \times B) \cap (A \times C)$. $\square$

Observe that $A \times B$ is not the same as $B \times A$, unless A and B happen to be equal. The following example shows that the statement analogous to Part (5) of Theorem 3.3.12, but with $\cup$ instead of $\cap$, is not true.

Example 3.3.13. Let $A = \{1, 2\}$ and $B = \{2, 3\}$ and $C = \{x, y\}$ and $D = \{y, z\}$. First, just to see that it works, we verify that Theorem 3.3.12 (5) holds for these sets. We see that $A \cap B = \{2\}$ and $C \cap D = \{y\}$, and so $(A \cap B) \times (C \cap D) = \{(2, y)\}$, and that $A \times C = \{(1, x), (1, y), (2, x), (2, y)\}$ and $B \times D = \{(2, y), (2, z), (3, y), (3, z)\}$, and so $(A \times C) \cap (B \times D) = \{(2, y)\}$. Hence $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

Now replace $\cap$ with $\cup$ in the above calculation. We then have $A \cup B = \{1, 2, 3\}$ and $C \cup D = \{x, y, z\}$, and so $(A \cup B) \times (C \cup D) = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z), (3, x), (3, y), (3, z)\}$. Using $A \times C$ and $B \times D$ as calculated in the previous paragraph, we see that $(A \times C) \cup (B \times D) = \{(1, x), (1, y), (2, x), (2, y), (2, z), (3, y), (3, z)\}$. Therefore $(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D)$. The difference between the situation in this paragraph and the previous one can be seen schematically in Figure 3.3.4, which is not a Venn diagram, and where we need to think of A, B, C and D as subsets of $\mathbb{R}$. $\Diamond$

<div align="center">

Exercises

</div>

Exercise 3.3.1. Let $A = \{1, 3, 5, 7\}$ and $B = \{1, 2, 3, 4\}$. Find each of the following sets.

(1) $A \cup B$.   (4) $A - B$.
(2) $A \cap B$.   (5) $B - A$.
(3) $A \times B$.

Fig. 3.3.4.
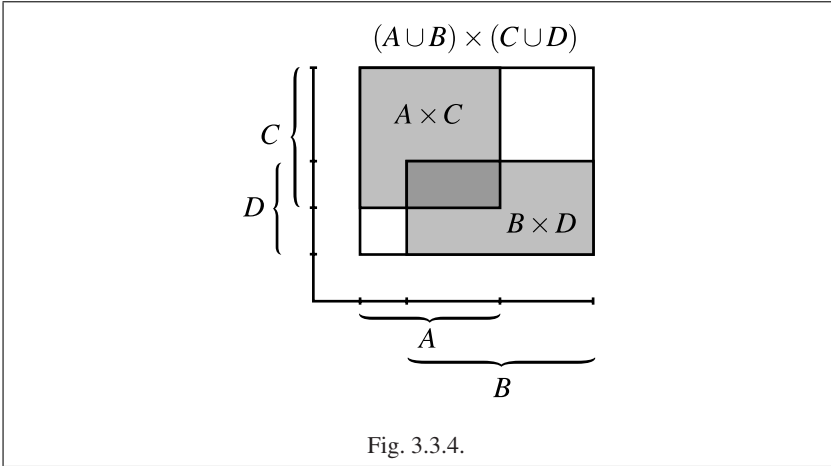
Exercise 3.3.2. Let $C = \{a,b,c,d,e,f\}$ and $D = \{a,c,e\}$ and $E = \{d,e,f\}$ and $F = \{a,b\}$. Find each of the following sets.

(1) $C - (D \cup E)$.   (4) $F \cap (D \cup E)$.
(2) $(C - D) \cup E$.   (5) $(F \cap D) \cup E$.
(3) $F - (C - E)$.   (6) $(C - D) \cup (F \cap E)$.

Exercise 3.3.3. Let $X = [0,5)$ and $Y = [2,4]$ and $Z = (1,3]$ and $W = (3,5)$ be intervals in $\mathbb{R}$. Find each of the following sets.

(1) $Y \cup Z$.   (4) $X \times W$.
(2) $Z \cap W$.   (5) $(X \cap Y) \cup Z$.
(3) $Y - W$.   (6) $X - (Z \cup W)$.

Exercise 3.3.4. Let

$$G = \{n \in \mathbb{Z} \mid n = 2m \text{ for some } m \in \mathbb{Z}\}$$
$$H = \{n \in \mathbb{Z} \mid n = 3k \text{ for some } k \in \mathbb{Z}\}$$
$$I = \{n \in \mathbb{Z} \mid n^2 \text{ is odd}\}$$
$$J = \{n \in \mathbb{Z} \mid 0 \leq n \leq 10\}.$$

Find each of the following sets.

(1) $G \cup I$.

(2) $G \cap I$.

(3) $G \cap H$.

(4) $J - G$.

(5) $I - H$.

(6) $J \cap (G - H)$.

Exercise 3.3.5. Given two sets A and B, are the sets $A - B$ and $B - A$ necessarily disjoint? Give a proof or a counterexample.

Exercise 3.3.6. [**Used in Theorem 3.3.3.**] Prove Theorem 3.3.3 (1) (2) (3) (6) (7) (8) (9).

Exercise 3.3.7. [**Used in Theorem 3.3.8.**] Prove Theorem 3.3.8 (1) (2) (3) (4) (5) (6).

Exercise 3.3.8. [**Used in Theorem 3.3.12.**] Prove Theorem 3.3.12 (1) (2) (4) (5).

Exercise 3.3.9. [**Used in Theorem 7.6.7.**] Let A and B be sets. Prove that $(A \cup B) - A = B - (A \cap B)$

Exercise 3.3.10. [**Used in Theorem 6.3.6.**] Let A, B and C be sets. Suppose that $C \subset A \cup B$, and that $C \cap A = \emptyset$. Prove that $C \subseteq B$.

Exercise 3.3.11. Let X be a set, and let $A, B, C \subseteq X$ be subsets. Suppose that $A \cap B = A \cap C$, and that $(X - A) \cap B = (X - A) \cap C$. Prove that $B = C$.

Exercise 3.3.12. Let A, B and C be sets. Prove that $(A - B) \cap C = (A \cap C) - B = (A \cap C) - (B \cap C)$.

Exercise 3.3.13. [**Used in Exercise 6.5.15.**] For real numbers a, b and c, we know that $a - (b - c) = (a - b) + c$. Let A, B and C be sets.

(1) Suppose that $C \subseteq A$. Prove that $A - (B - C) = (A - B) \cup C$.

(2) Does $A - (B - C) = (A - B) \cup C$ hold for all sets A, B and C? Prove or give a counterexample for this formula. If the formula is false, find and prove a modification of this formula that holds for all sets.

Exercise 3.3.14. Let A and B be sets. The **symmetric difference** of A and B, denoted $A \triangle B$, is the set $A \triangle B = (A - B) \cup (B - A)$.

Let X, Y and Z be sets. Prove the following statements.

(1) $X \triangle \emptyset = X$.

(2) $X \triangle X = \emptyset$.

(3) $X \triangle Y = Y \triangle X$.

(4) $X \triangle (Y \triangle Z) = (X \triangle Y) \triangle Z$.

(5) $X \cap (Y \triangle Z) = (X \cap Y) \triangle (X \cap Z)$.

(6) $X \triangle Y = (X \cup Y) - (X \cap Y)$.

Exercise 3.3.15. Prove or find a counterexample to the following statement. Let A, B and C be sets. Then $(A - B) \cup C = (A \cup B \cup C) - (A \cap B)$.

Exercise 3.3.16. Prove or find a counterexample to the following statement. Let A, B and C be sets. Then $(A \cup C) - B = (A - B) \cup (C - B)$.

Exercise 3.3.17. Let A, B and C be sets. Prove that $A \subseteq C$ if and only if $A \cup (B \cap C) = (A \cup B) \cap C$.

Exercise 3.3.18. Prove or give a counterexample for each of the following statements.

> **(1)** Let A and B be sets. Then $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.
> **(2)** Let A and B be sets. Then $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

Exercise 3.3.19. Let A, B and C be sets. Prove that $A \times (B - C) = (A \times B) - (A \times C)$.

Exercise 3.3.20. Let A and B be sets. Suppose that $B \subseteq A$. Prove that $A \times A - B \times B = [(A - B) \times A] \cup [A \times (A - B)]$.

Exercise 3.3.21. Let A and B be sets. Suppose that $A \neq B$. Suppose that E is a set such that $A \times E = B \times E$. Prove that $E = \emptyset$.

Exercise 3.3.22. Let X be a set. Suppose that X is finite. Which of the two sets $\mathcal{P}(X \times X) \times \mathcal{P}(X \times X)$ and $\mathcal{P}(\mathcal{P}(X))$ has more elements?

3.4 Families of Sets

So far we have dealt with unions and intersections of only two sets at a time. We now want to apply these operations to more than two sets.

For the sake of comparison, let us look at addition of real numbers. Formally, addition is what is called a binary operation, which takes pairs of numbers as input and produces single numbers as output. We will see a rigorous treatment of binary operations in Section 7.1, but for now it is sufficient to take an informal approach to this concept. In particular, we see that in principle it is possible to add only two numbers at a time. Of course, in practice it is often necessary to add three or more numbers together, and here is how it is done. Suppose that we want to compute $2 + 3 + 9$. We would proceed in one of two ways, either first computing $2 + 3 = 5$ and then computing $5 + 9 = 14$, or first computing $3 + 9 = 12$ and then computing $2 + 12 = 14$. As expected, we obtained the same answer both ways, and this common answer is what we would call the sum of the three numbers $2 + 3 + 9$. Another way of writing these two ways of computing the sum is as $(2 + 3) + 9$ and $2 + (3 + 9)$. It turns out that there is a general rule about addition, called the Associative Law, that says that in all cases of three numbers that are being added, the same result is obtained from either way of positioning the parentheses. This property of addition is stated in Theorem A.1 (1) in the Appendix. Hence, for any three numbers a, b and c, we can define the sum $a + b + c$ to be the number that results from computing either $(a + b) + c$ or $a + (b + c)$.

Intuitively, a similar approach would work for the sum of any finite collection of numbers, though to do so formally would require definition by recursion, a topic we will see in Section 6.4; see Example 6.4.4 (2) for the use of recursion for adding finitely many numbers. Sums of infinite collections of numbers are much trickier. The reader has most likely encountered the notion of a series of numbers, for example $\sum_{n=1}^{\infty} \frac{1}{n^2}$, in a calculus course. Not all such series actually add up to a real number, and the question of figuring out for which series that happens is somewhat tricky,

especially if done rigorously, because it involves limits; see any introductory real analysis text, for example [Blo11, Chapter 9], for details.

Let us now compare the above discussion of the addition of numbers to unions and intersections of sets. For the union and intersection of three sets, the exact analog holds because Theorem 3.3.3 (4) for union and intersection of sets is the exact analog of Theorem A.1 (1) for addition and multiplication of numbers. Hence, if we are given three sets A, B and C, and we wanted to form the union of all three of them, we could compute either one of $(A \cup B) \cup C$ and $A \cup (B \cup C)$, which are always equal, and we could label the result as $A \cup B \cup C$. The same idea holds for the intersection of three sets. In principle, we could extend this idea to unions and intersections of any finite collection of sets $A_1, A_2, \ldots, A_n$, where the word "finite" refers only to the number of sets, not the sizes of the individual sets, which could be infinite. Once again, to make such a definition work rigorously, we would need to use definition by recursion, and so we cannot do it properly yet. As for the union of an infinite sequence of sets $A_1, A_2, A_3, \ldots$, there is no simple analog for sets of series of numbers, and even if there were, series of numbers are rather tricky, and presumably series of sets would be too.

Fortunately, we can solve this problem for unions and intersections of sets in a very simple way that is not available to us with addition of numbers. For addition, we really do not have a choice but to add two numbers at a time, and then extend that by recursion to finite sums, and use limits for infinite sums. For unions and intersections, however, rather than defining unions and intersections of arbitrary collections of sets in terms of unions and intersections of two sets at a time, we can define unions and intersections of arbitrary collections of sets from scratch, using the case of two sets at a time simply by way of analogy.

For two sets A_1 and A_2, the union $A_1 \cup A_2$ is the set of all elements x such that $x \in A_1$ or $x \in A_2$. We cannot directly generalize the notion of "or" directly to an infinite collection of sets, because "or" is also defined for only two things at a time, but let us look at $A_1 \cup A_2$ slightly differently. Recall that for mathematics, the word "or" always means the inclusive or, that is, one or the other or both. Hence, instead of thinking of $A_1 \cup A_2$ as the set of all elements x such that $x \in A_1$ or $x \in A_2$, we can just as well think of it as the set of all elements x such that $x \in A_i$ for some $i \in \{1, 2\}$. In other words, we have replaced the use of "or" in the definition of the union of two sets with an existential quantifier. The advantage of this approach is that whereas "or" cannot be generalized to more than two things at a time, the existential quantifier can be used on sets of arbitrary size. Hence, if we have an infinite collection of sets $A_1, A_2, A_3, \ldots$, we can define the union of these sets as the set of all elements x such that $x \in A_i$ for some $i \in \mathbb{N}$. Using notation that is analogous to the notation for series of numbers, we then write

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \ldots = \{x \mid x \in A_n \text{ for some } n \in \mathbb{N}\}.$$

Now let us look at intersections. For two sets A_1 and A_2, the intersection $A_1 \cap A_2$ is the set of all elements x such that $x \in A_1$ and $x \in A_2$. The alternative approach is to

think of $A_1 \cap A_2$ as the set of all elements x such that $x \in A_i$ for all $i \in \{1,2\}$. Here we have replaced the use of "and" in the definition of the intersection of two sets with a universal quantifier. If we have an infinite collection of sets $A_1, A_2, A_3, \ldots$, we can define the intersection of these sets as the set of all elements x such that $x \in A_i$ for some $i \in \mathbb{N}$, and we write

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \ldots = \{x \mid x \in A_n \text{ for all } n \in \mathbb{N}\}.$$

Example 3.4.1.

(1) For each $i \in \mathbb{N}$, let $B_i = \{1, 2, \ldots, 3i\}$. Then $\bigcup_{i=1}^{\infty} B_i = \mathbb{N}$ and $\bigcap_{i=1}^{\infty} B_i = \{1, 2, 3\}$.

(2) Recall the notation for intervals in $\mathbb{R}$ in Definition 3.2.1. For each $k \in \mathbb{N}$, let $F_k = (\frac{1}{k}, 8 + \frac{3}{k})$. Then $\bigcup_{k=1}^{\infty} F_k = (0, 11)$ and $\bigcap_{k=1}^{\infty} F_k = (1, 8]$. ◇

What we have said so far, though correct, is not sufficient for our purposes. Suppose, for example, that for each real number x we define the set Q_x to be the set of all real numbers less than x, so that $Q_x = (-\infty, x)$. Though it is not obvious, and it will only be proved in Section 6.7, it turns out that there is no possible way to line up all the sets of the form Q_x in order analogously to $A_1, A_2, A_3, \ldots$. We are therefore not in precisely the same situation as discussed previously. However, in contrast to series of numbers such as $\sum_{n=1}^{\infty} \frac{1}{n^2}$, where the definition of the sum depends very much upon the order of the numbers in the series, for unions and intersections of sets the order of the sets does not matter at all. In particular, if we look at the definitions of $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$, we observe that we do not need to think of the sets $A_1, A_2, A_3, \ldots$ as written in order, and we can think of this collection of sets as having one set for each number in $\mathbb{N}$. We can therefore rewrite $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$ as $\bigcup_{i \in \mathbb{N}} A_i$ and $\bigcap_{i \in \mathbb{N}} A_i$, respectively.

The following definition, based upon the above ideas, will allow us to define unions and intersections in the most general situation possible. We note that this definition is based upon the informal distinction between sets and element; we will see a different approach when we discuss the Zermelo–Fraenkel Axioms for set theory in Section 3.5.

Definition 3.4.2. Let $\mathcal{A}$ be a set. The set $\mathcal{A}$ is called a **family of sets** if all the elements of $\mathcal{A}$ are sets. The family of sets $\mathcal{A}$ is **indexed** by I, denoted $\mathcal{A} = \{A_i\}_{i \in I}$, if there is a non-empty set I such that there is an element $A_i \in \mathcal{A}$ for each $i \in I$, and that every element of $\mathcal{A}$ equals A_i for exactly one $i \in I$. △

Observe that the empty set is a family of sets. When we define a family of sets, if we do not need to view the family of sets as indexed, we will write "let $\mathcal{A}$ be a family of sets." If we want to use an indexed family of sets, we will write "let I be a set, and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I"; in such cases we will often not give the family of sets a name such as $\mathcal{A}$.

Although it is often easier to think of, and work with, families of sets when they are indexed, it is important for various applications to have the non-indexed way of

working with families of sets as well. For example, suppose that we have a set A, and we want to consider the family of all finite subsets of A; we could write such a family as

$$\mathcal{A} = \{B \mid B \subseteq A \text{ and } B \text{ is finite}\}.$$

(We have not formally defined finiteness yet, but the above example is just for illustrative purposes; we will see the definition of finite sets in Section 6.5.) It is quite natural to consider such families of sets in many parts of mathematics (not just collections of finite subsets, but subsets characterized by other criteria as well), and there is no natural way to index the elements of such a family of sets. Actually, that is not quite true—we can index each element of $\mathcal{A}$ by itself! That is, we can write $\mathcal{A} = \{A_X\}_{X \in \mathcal{A}}$, which would lead us to think of any family of sets as "self-indexed." However, while that is technically correct, in practice viewing every family of sets as self-indexed is not particularly helpful, and so we will continue to think of families of sets written as $\mathcal{A}$ as non-indexed, and families of sets written as $\{A_i\}_{i \in I}$ as indexed. In our discussion of families of sets in this section, and our use of them in subsequent sections, we will use both indexed and non-indexed notation as suits each situation.

On the one hand, families of sets are just sets, and hence everything that we have previously said about sets still holds for families of sets. For example, given two families of sets, we could ask whether one is a subset of the other. On the other hand, because all the elements of a family of sets are themselves sets, then we can do something special with families of sets, which is to take the union and intersection of all the elements of the family of sets, which we define as follows.

Definition 3.4.3.   Let $\mathcal{A}$ be a family of sets. The **union** of the sets in $\mathcal{A}$, denoted $\bigcup_{X \in \mathcal{A}} X$, is defined as follows. If $\mathcal{A} \neq \emptyset$, then

$$\bigcup_{X \in \mathcal{A}} X = \{x \mid x \in A \text{ for some } A \in \mathcal{A}\};$$

if $\mathcal{A} = \emptyset$, then $\bigcup_{X \in \mathcal{A}} X = \emptyset$. The **intersection** of the sets in $\mathcal{A}$, denoted $\bigcap_{X \in \mathcal{A}} X$, is defined as follows. If $\mathcal{A} \neq \emptyset$, then

$$\bigcap_{X \in \mathcal{A}} X = \{x \mid x \in A \text{ for all } A \in \mathcal{A}\};$$

if $\mathcal{A} = \emptyset$, then $\bigcap_{X \in \mathcal{A}} X$ is not defined.

If $\mathcal{A} = \{A_i\}_{i \in I}$ is indexed by a set I, then we write

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\} \quad \text{and} \quad \bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for all } i \in I\}$$

to denote the union and intersection of the sets in $\mathcal{A}$, respectively.   △

Intuitively, the set $\bigcup_{i \in I} A_i$ is the set that contains everything that is in at least one of the sets A_i; the set $\bigcap_{i \in I} A_i$ is the set containing everything that is in all of the sets A_i. The same holds for the non-indexed notation.

Formally, the proper way to describe $\bigcup_{X \in \mathcal{A}} X$ is as "the union of the elements of the family of sets $\mathcal{A}$," but informally we simply say "the union of the sets in $\mathcal{A}$" or "the union of the family of sets $\mathcal{A}$," and similarly for intersection.

Example 3.4.4.

(1) For each $x \in \mathbb{R}$, let C_x be the interval $C_x = [-2, \sin x]$. Then $\bigcup_{x \in \mathbb{R}} C_x = [-2, 1]$ and $\bigcap_{x \in \mathbb{R}} C_x = [-2, -1]$.

(2) Let $\mathcal{F}$ be the family of all finite subsets of $\mathbb{N}$. Then $\bigcup_{X \in \mathcal{F}} X = \mathbb{N}$ and $\bigcap_{X \in \mathcal{F}} X = \emptyset$.   ◇

The following theorem gives some of the standard properties of unions and intersections of arbitrary families of sets, generalizing various properties we saw in Section 3.3. Part (1) of the theorem says that $\bigcap_{i \in I} A_i$ is the largest set contained in all the sets in $\{A_i\}_{i \in I}$, and Part (2) of the theorem says that $\bigcup_{i \in I} A_i$ is the smallest set containing all the sets in $\{A_i\}_{i \in I}$. To allow the reader to gain familiarity with both the indexed and the non-indexed notations, we state the theorem in both forms, proving one part of the theorem using one notation, and another part of the theorem using the other notation. Subsequent theorems will be stated in only one of these two styles (usually the indexed notation), leaving it to the reader to convert it to the other style as needed.

Theorem 3.4.5.
Non-Indexed Version: *Let $\mathcal{A}$ be a non-empty family of sets and let B be a set.*

1. $\bigcap_{X \in \mathcal{A}} X \subseteq A$ *for all $A \in \mathcal{A}$. If $B \subseteq X$ for all $X \in \mathcal{A}$, then $B \subseteq \bigcap_{X \in \mathcal{A}} X$.*
2. $A \subseteq \bigcup_{X \in \mathcal{A}} X$ *for all $A \in \mathcal{A}$. If $X \subseteq B$ for all $X \in \mathcal{A}$, then $\bigcup_{X \in \mathcal{A}} X \subseteq B$.*
3. $B \cap (\bigcup_{X \in \mathcal{A}} X) = \bigcup_{X \in \mathcal{A}} (B \cap X)$ *(Distributive Law).*
4. $B \cup (\bigcap_{X \in \mathcal{A}} X) = \bigcap_{X \in \mathcal{A}} (B \cup X)$ *(Distributive Law).*
5. $B - (\bigcup_{X \in \mathcal{A}} X) = \bigcap_{X \in \mathcal{A}} (B - X)$ *(De Morgan's Law).*
6. $B - (\bigcap_{X \in \mathcal{A}} X) = \bigcup_{X \in \mathcal{A}} (B - X)$ *(De Morgan's Law).*

Indexed Version: *Let I be a non-empty set, let $\{A_i\}_{i \in I}$ be a family of sets indexed by I and let B be a set.*

1. $\bigcap_{i \in I} A_i \subseteq A_k$ *for all $k \in I$. If $B \subseteq A_k$ for all $k \in I$, then $B \subseteq \bigcap_{i \in I} A_i$.*
2. $A_k \subseteq \bigcup_{i \in I} A_i$ *for all $k \in I$. If $A_k \subseteq B$ for all $k \in I$, then $\bigcup_{i \in I} A_i \subseteq B$.*
3. $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$ *(Distributive Law).*
4. $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$ *(Distributive Law).*
5. $B - (\bigcup_{i \in I} A_i) = \bigcap_{i \in I} (B - A_i)$ *(De Morgan's Law).*
6. $B - (\bigcap_{i \in I} A_i) = \bigcup_{i \in I} (B - A_i)$ *(De Morgan's Law).*

Proof. We will prove Parts (3) and (6), leaving the rest to the reader in Exercise 3.4.3.

(3). Let $x \in B \cap (\bigcup_{i \in I} A_i)$. Then $x \in B$ and $x \in \bigcup_{i \in I} A_i$. It follows that $x \in A_k$ for some $k \in I$. Hence $x \in B \cap A_k$. Therefore $x \in \bigcup_{i \in I} (B \cap A_i)$ by Part (2) of this theorem. Hence $B \cap (\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} (B \cap A_i)$.

Now let $y \in \bigcup_{i \in I} (B \cap A_i)$. Then $y \in B \cap A_j$ for some $j \in I$. Hence $y \in B$ and $y \in A_j$. Therefore $x \in \bigcup_{i \in I} A_i$ by Part (2) of this theorem. It follows that $y \in B \cap (\bigcup_{i \in I} A_i)$. Hence $\bigcup_{i \in I} (B \cap A_i) \subseteq B \cap (\bigcup_{i \in I} A_i)$.

We conclude that $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$.

(6). Let $a \in B - (\bigcap_{X \in \mathcal{A}} X)$. Then $a \in B$ and $a \notin \bigcap_{X \in \mathcal{A}} X$. Then $a \notin Y$ for some $Y \in \mathcal{A}$. Then $a \in B - Y$. Hence $a \in \bigcup_{X \in \mathcal{A}} (B - X)$ by Part (2) of this theorem. It follows that $B - (\bigcap_{X \in \mathcal{A}} X) \subseteq \bigcup_{X \in \mathcal{A}} (B - X)$.

Now let $b \in \bigcup_{X \in \mathcal{A}} (B - X)$. Then $b \in B - Z$ for some $Z \in \mathcal{A}$. Then $b \in B$ and $b \notin Z$. Hence $b \notin \bigcap_{X \in \mathcal{A}} X$. It follows that $b \in B - \bigcap_{X \in \mathcal{A}} X$. Therefore $\bigcup_{X \in \mathcal{A}} (B - X) \subseteq B - (\bigcap_{X \in \mathcal{A}} X)$.

We conclude that $B - (\bigcap_{X \in \mathcal{A}} X) = \bigcup_{X \in \mathcal{A}} (B - X)$. □

It can be verified that all the parts of Theorem 3.4.5 that involve union but not intersection hold also when $\mathcal{A} = \emptyset$; the parts of the theorem that involve intersection are not defined when $\mathcal{A} = \emptyset$.

It is interesting to compare the proof of Theorem 3.4.5 (3) with the proof of Theorem 3.3.3 (5). Though Theorem 3.4.5 (3) is a generalization of Theorem 3.3.3 (5), the proof of the generalized statement is slightly more concise than the proof of the simpler statement. The proof of Theorem 3.4.5 (3) is more concise precisely because it is phrased explicitly in terms of quantifiers, which allows us to avoid the need for cases as in the proof of Theorem 3.3.3 (5).

In addition to defining the union and intersection of families of sets, it is also possible to form the product of a family of sets, though doing so requires the use of functions, and hence we will wait until the end of Section 4.5 for the definition.

Exercises

Exercise 3.4.1. In each of the following parts, we are given a set B_k for each $k \in \mathbb{N}$. Find $\bigcup_{k \in \mathbb{N}} B_k$ and $\bigcap_{k \in \mathbb{N}} B_k$.

(1) $B_k = \{0, 1, 2, 3, \ldots, 2k\}$.

(2) $B_k = \{k - 1, k, k + 1\}$.

(3) $B_k = [\frac{3}{k}, \frac{5k+2}{k}) \cup \{10 + k\}$.

(4) $B_k = [-1, 3 + \frac{1}{k}] \cup [5, \frac{5k+1}{k})$.

(5) $B_k = (-\frac{1}{k}, 1] \cup (2, \frac{3k-1}{k}]$.

(6) $B_k = [0, \frac{k+1}{k+2}] \cup [7, \frac{7k+1}{k})$.

Exercise 3.4.2. In each of the following parts, you need to find a family of sets $\{E_k\}_{k \in \mathbb{N}}$ such that $E_k \subseteq \mathbb{R}$ for each $k \in \mathbb{N}$, that no two sets E_k are equal to each other and that the given conditions hold.

(1) $\bigcup_{k \in \mathbb{N}} E_k = [0, \infty)$ and $\bigcap_{k \in \mathbb{N}} E_k = [0, 1]$.

(2) $\bigcup_{k \in \mathbb{N}} E_k = (0, \infty)$ and $\bigcap_{k \in \mathbb{N}} E_k = \emptyset$.

(3) $\bigcup_{k \in \mathbb{N}} E_k = \mathbb{R}$ and $\bigcap_{k \in \mathbb{N}} E_k = \{3\}$.

(4) $\bigcup_{k \in \mathbb{N}} E_k = (2, 8)$ and $\bigcap_{k \in \mathbb{N}} E_k = [3, 6]$.

(5) $\bigcup_{k \in \mathbb{N}} E_k = [0, \infty)$ and $\bigcap_{k \in \mathbb{N}} E_k = \{1\} \cup [2, 3)$.

(6) $\bigcup_{k \in \mathbb{N}} E_k = \mathbb{Z}$ and $\bigcap_{k \in \mathbb{N}} E_k = \{\ldots, -2, 0, 2, 4, 6, \ldots\}$.

(7) $\bigcup_{k \in \mathbb{N}} E_k = \mathbb{R}$ and $\bigcap_{k \in \mathbb{N}} E_k = \mathbb{N}$.

Exercise 3.4.3. **[Used in Theorem 3.4.5.]** Prove Theorem 3.4.5 (1) (2) (4) (5). Do some in the indexed notation and some in the non-indexed notation.

Exercise 3.4.4. Let $\mathcal{A}$ and $\mathcal{B}$ be non-empty families of sets. Suppose that $\mathcal{A} \subseteq \mathcal{B}$.

(1) Prove that $\bigcup_{X \in \mathcal{A}} X \subseteq \bigcup_{Y \in \mathcal{B}} Y$.
(2) Prove that $\bigcap_{X \in \mathcal{A}} X \subseteq \bigcap_{Y \in \mathcal{B}} Y$.

Exercise 3.4.5. Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ and $\{B_i\}_{i \in I}$ be families of sets indexed by I. Suppose that $A_i \subseteq B_i$ for all $i \in I$.

(1) Prove that $\bigcup_{i \in I} A_i \subseteq \bigcup_{i \in I} B_i$.
(2) Prove that $\bigcap_{i \in I} A_i \subseteq \bigcap_{i \in I} B_i$.

Exercise 3.4.6. Let $\mathcal{A}$ be a non-empty family of sets and let B be a set.

(1) Prove that $(\bigcup_{X \in \mathcal{A}} X) - B = \bigcup_{X \in \mathcal{A}} (X - B)$.
(2) Prove that $(\bigcap_{X \in \mathcal{A}} X) - B = \bigcap_{X \in \mathcal{A}} (X - B)$.

Exercise 3.4.7. Let I be a non-empty set, let $\{A_i\}_{i \in I}$ be a family of sets indexed by I and let B be a set.

(1) Prove that $B \times (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \times A_i)$.
(2) Prove that $B \times (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \times A_i)$.

Exercise 3.4.8. Suppose that $\mathcal{W}$ is some property of subsets of $\mathbb{R}$ (for example, being finite). A subset $X \subseteq \mathbb{R}$ is called **co-$\mathcal{W}$** if $\mathbb{R} - X$ has property $\mathcal{W}$.

Let $\mathcal{A}$ be a non-empty family of sets. Suppose that X is a co-$\mathcal{W}$ subset of $\mathbb{R}$ for all $X \in \mathcal{A}$. For each of the properties $\mathcal{W}$ listed below, either prove that $\cup_{X \in \mathcal{A}} X$ is co-$\mathcal{W}$, or give a counterexample. Try to figure out a general rule for deciding when $\cup_{X \in \mathcal{A}} X$ is co-$\mathcal{W}$ for a given property $\mathcal{W}$.

(1) A subset of $\mathbb{R}$ has property $\mathcal{W}$ if and only if it is finite.
(2) A subset of $\mathbb{R}$ has property $\mathcal{W}$ if and only if it has at most 7 elements.
(3) A subset of $\mathbb{R}$ has property $\mathcal{W}$ if and only if it has precisely 7 elements.
(4) A subset of $\mathbb{R}$ has property $\mathcal{W}$ if and only if it contains only integers.
(5) A subset of $\mathbb{R}$ has property $\mathcal{W}$ if and only if it is finite, and has an even number of elements.

3.5 Axioms for Set Theory

Set theory is a very remarkable idea that works so very well, and is so broadly useful, that it is used as the basis for modern mathematics. Unfortunately, however, it does not work quite as nicely as we might have made it appear in the previous sections of this chapter. Early in the development of set theory, a number of "paradoxes" were discovered, the most well-known of which is Russell's Paradox, which is as follows.

Suppose that we could form the set of all sets; let S denote this set. Observe that $S \in S$. We then define the set $T = \{A \in S \mid A \notin A\}$. Is T a member of itself? Suppose first that $T \notin T$. Then $T \in T$. Now suppose that $T \in T$. Then $T \notin T$. There is something wrong here. The problem is that we are trying to use a set of all sets, and more generally the problem is that we have to be more careful how we quantify over sets. See [GG94, Section 5.3] for further comments on the paradoxes of set theory.

In our use of sets in this text, as well as in the use of sets in much of mathematics, problems such as Russell's Paradox do not arise because we do not use the set of all sets and similar problematic constructs. To treat set theory rigorously, however, some subtlety is needed. Various axiom systems for set theory have been developed that avoid paradoxes such as Russell's Paradox. See [Vau95, Introduction] for a succinct discussion of the history of set theory and its axiomatization.

The first axiom scheme for set theory was due to Zermelo in 1908. This scheme was subsequently modified into what is now the most commonly used axiom system for set theory, which is referred to as the Zermelo–Fraenkel Axioms. These axioms are often abbreviated as "ZF." There are a number of equivalent variations of ZF, of which we state one below. See [End77] or [Sto79, Chapter 7] for an accessible discussion of the ZF axioms, and see [Lev02] for a more advanced look at these axioms.

The ZF axioms are properly formulated in the context of symbolic logic, in which case the axioms are written out in logical notation. Because our purpose here is just to gain an informal familiarity with the ZF axioms, and because it would take us too far afield to develop the needed logic, we will write the axioms informally (though we will write the first one in logical symbols just to show that it can be done).

We need two additional comments before listing the axioms. First, whereas informally we tend to distinguish between sets and elements, for example we think of $A = \{1, 2\}$ as a set and each of 1 and 2 as elements, in the ZF axioms we make no such distinction. Everything in the ZF axioms is a set. It might seem strange to think of the numbers 1 and 2 as sets, but from the perspective of the ZF axioms the symbols "1" and "2" denote the sets $\{\emptyset\}$ and $\{\emptyset, \{\emptyset\}\}$, respectively. (We will say a bit more about this idea shortly.)

Once we assume that everything in the ZF axioms is a set, then the relation of elementhood, which is denoted by the symbol $\in$, is a relation between sets. That is, given two sets x and y, it might or might not be the case that $x \in y$. However, even if $x \in y$, we still think of both x and y as sets, regardless of whether or not one is an element of the other. Of course, if everything is a set, and we do not distinguish between what is a set and what is an element, we have to worry about potentially problematic constructions such as $x = \{x\}$, which would not specify what the set x is, because x is defined in terms of itself. Fortunately, the ZF axioms are designed to prevent such problems; this particular problem is disallowed by the Axiom of Regularity.

Of course, if everything in the ZF axioms is viewed as a set, then the concept of a "family of sets" as discussed in Section 3.4 is unnecessary, because every non-empty set is a family of sets. Nonetheless, for the informal approach to sets used on a daily basis in modern mathematics, and used throughout this text (other than during our discussion of the ZF Axioms), the distinction between sets and elements, and the notion of a family of sets, are quite useful, and we will continue to make use of these ideas.

Second, because the ZF axioms are formulated in terms of formal logic, and because we are not discussing such such logic, our informal treatment of the ZF axioms will necessarily be, indeed, informal. See [EFT94] and [Mal79] for more

about logic. In particular, whereas most of the axioms can be stated in terms of familiar logical notions (for example, "and," "or," "not" and "for all"), which we saw informally in Sections 1.2 and 1.5, two of the axioms (the Axiom of Selection and the Axiom of Replacement) use the concepts of logical properties of sets, which require a more extensive treatment of logic than we have the ability to provide here. Hence, our phrasing of these two axioms is, unfortunately, not entirely satisfactory.

Here, finally, are the ZF axioms.

Axiom of Extensionality Let x and y be sets. If x and y have the same elements, then $x = y$.

This axiom is simply another way of stating the definition of the equality of sets that we saw in Definition 3.2.5. This axiom can be written in logical notation as

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

We will not write the other axioms in this type of notation, but they all can, and should, be written that way in the context of a more detailed look at the axioms via the study of logic.

Axiom of Empty Set There is a set z such that $x \notin z$ for all sets x.

This axiom is also referred to as the Axiom of Null Set. By the Axiom of Extensionality there is only one set z as described in this axiom, and this set is usually denoted $\emptyset$.

Axiom of Pairing Let x and y be sets. There is a set z such that $w \in z$ if and only if $w = x$ or $w = y$.

The set z described in the axiom is unique by the Axiom of Extensionality, and it is denoted $\{x, y\}$. In this axiom it is not required that $x \neq y$, and we abbreviate $\{x, x\}$ by $\{x\}$.

Axiom of Union Let x be a set. There is a set z such that $w \in z$ if and only if there is some $y \in x$ such that $w \in y$.

Once again the set z described in the axiom is unique, and it is denoted $\cup x$. Because the ZF axioms allow us to view every set as a family of sets, then $\cup x$ is the same as what we informally defined as $\bigcup_{y \in x} y$ in Section 3.4.

Axiom of Power Set Let x be a set. There is a set z such that $w \in z$ if and only if $w \subseteq x$.

The notation "$w \subseteq x$" is simply an abbreviated way of writing the expression "$y \in w$ implies $y \in x$," so that it is valid to use that notation in the ZF axioms. Once again the set z described in this axiom is unique, and it is the same as what we informally defined as $\mathcal{P}(x)$ in Section 3.2.

Axiom of Regularity Let x be a set. Suppose that $x \neq \emptyset$. Then there is some $y \in x$ such that $x \cap y = \emptyset$.

This axiom is also referred to as the Axiom of Foundation. The notation "$x \cap y = \emptyset$" is simply an abbreviated way of writing the expression "there does not exist a set z such that $z \in x$ and $z \in y$," so that it valid to use that notation in the ZF axioms. This axiom is needed to rule out problematic situations such as a non-empty set x such that $x \in x$. To see why $x \in x$ is not allowed when $x \neq \emptyset$, observe that if there were such a set x, then the set $\{x\}$ would violate the Axiom of Regularity.

Axiom of Selection   Let $P(t)$ be a logical property of sets with one free variable t that can be formulated in the context of the ZF axioms. Let x be a set. Then there is a set z such that $y \in z$ if and only if $y \in x$ and $P(y)$ is true.

This axiom has a variety of names, including the Axiom of Specification, Axiom of Comprehension and Axiom of Separation. The set z described in the axiom is unique, and it is usually denoted $\{y \in x \mid P(y)\}$. It is very important to observe that this axiom states that we can take an existing set, and then form the subset of those elements that satisfy the given property. It is not possible to define a set of elements that satisfy a given property if it is not specified what set the elements belong to. Consider, for example, the definition of the union and intersection of a family of sets given in Definition 3.4.3, which said

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\} \quad \text{and} \quad \bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for all } i \in I\}.$$

In fact, Definition 3.4.3 is not valid as stated if we adhere to the Axiom of Selection, because we are not specifying which set the element x belongs to. It would be tempting to write something such as "let S be the set of all sets, and let $\bigcup_{i \in I} A_i = \{x \in S \mid x \in A_i \text{ for some } i \in I\}$, but that would not be valid, because we saw at the start of this section that the set of all sets is not a concept we can use. The reader might, quite reasonably, be troubled that we used a definition in Section 3.4 that was not technically valid, but no real harm was done (other than perhaps to the credibility of the author). Definition 3.4.3 conveys the correct intuitive idea behind the union and intersection of a family of sets, and given that we had not yet discussed the ZF axioms, it was the best we could do at the time. Moreover, the ZF axioms allow for a rigorous treatment of union and intersection, and this rigorous approach works precisely as did the intuitive approach used in Definition 3.4.3, so we can confidently continue to use union and intersection just as we have until now.

Interestingly, the way the ZF axioms treat union is quite different from the way it treats intersection. The ability to take the union of a family of sets is given axiomatically in the Axiom of Union; by contrast, the ability to take the intersection of a family of sets can be deduced from the ZF axioms, as follows. Let x be a non-empty set. Then $\bigcap_{z \in x} z$ is then defined to be $\{y \in \cup x \mid y \in z \text{ for all } z \in x\}$, which is possible by the Axiom of Selection.

Although we used the name "Axiom of Selection," this axiom is actually not a single axiom, but a collection of axioms, one axiom for each property $P(t)$. Such a collection of axioms is often called an "axiom schema." It is not possible to coalesce this collection of axioms into a single axiom, because it is not possible in the ZF axioms to quantify over all possible properties of sets.

Axiom of Infinity There is a set z such that $\emptyset \in z$, and if $x \in z$ then $x \cup \{x\} \in z$.

We can make use of $\emptyset$ and $\cup$ in the Axiom of Infinity because of the Axiom of Empty Set and the Axiom of Union, and we can make use of $\{x\}$ because of the Axiom of Power Set and the Axiom of Selection, though we omit the details of the latter. The set z in this axiom, which is not necessarily unique, can be thought of informally as a set that contains the sets

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots. \tag{3.5.1}$$

Intuitively, any such set z must be infinite, which leads to the name of the axiom. (We have not yet formally defined what it means for a set to be infinite; we will see that in Section 6.5.)

Axiom of Replacement Let $F(s,t)$ be a functional property of sets with two free variables s and t that can be formulated in the context of the ZF axioms. Let x be a set. Then there is a set z such that $y \in z$ if and only if there is some $w \in x$ such that $F(w,y)$ is true.

As with the Axiom of Selection, the Axiom of Replacement is also a collection of axioms, one for each functional property F. A functional property is the formal way of describing what is standardly called a function. We will discuss functions extensively in Chapter 4; in particular, we will see in Section 4.1 that functions can be described in terms of sets, and hence functional properties are valid in the ZF axioms. We will put off any further discussion of functions till Chapter 4. The Axiom of Replacement is used primarily for technical purposes in advanced set theory, and we will not discuss it any further. See [Pot04, Appendix A.3] for some philosophical reservations about the Axiom of Replacement, though other mathematicians do not seem to have qualms about this axiom.

The ZF axioms can be used not only to prove many useful facts about sets, but also to construct many familiar mathematical objects, for example the set of natural numbers. The basic idea of this construction is found in the list of sets in Equation 3.5.1. These sets should remind the reader of the numbers $0, 0+1, 0+1+1, 0+1+1+1, \ldots$, which intuitively are the non-negative integers; the natural numbers are then obtained by removing 0 from this set. The Axiom of Infinity guarantees the existence of at least one set w that contains these "numbers," though the set w is not necessarily unique. We then let z be the intersection of all subsets of w that contain these "numbers," and it can be seen that z is then the minimal such set. With some work, the set z is seen to contain precisely the sets listed in Equation 3.5.1, and is seen to behave just as one would expect the set of natural numbers together with 0 to behave; the choice of w turns out not to matter. The details of this construction may be found in [End77, Chapter 4].

Once the natural numbers have been defined, it is possible to construct the integers, the rational numbers and the real numbers from the natural numbers. See [Blo11, Chapter 1] for the construction of these number systems. Moreover, many branches of mathematics such as real analysis (the rigorous study of calculus) and Euclidean geometry are based upon the properties of the real numbers. Hence, if we

accept the ZF axioms, then we have at our disposal the familiar number systems with their standard properties, and a variety of branches of mathematics, all constructed completely rigorously.

A review of the ZF axioms raises the question of why these particular axioms and not others were chosen. The answer is that it would be possible to use variants of the axioms. These particular axioms were chosen because they seem to be convenient to work with, and because they suffice to imply everything that needs to be done with sets.

Is there any redundancy in the ZF axioms? In other words, is it possible to prove one or more of the axioms from the remaining ones? The answer is yes. For example, the Axiom of Infinity together with the Axiom of Selection imply the Axiom of Empty Set, because the Axiom of Infinity states that there is some set w, and the Axiom of Selection implies that we can define a new set $z = \{x \in w \mid x \neq x\}$, which in turn satisfies the Axiom of Empty Set. Hence, in principle, it would be possible to drop the Axiom of Empty Set from the ZF axioms if we want to have the smallest possible set of axioms. However, the Axiom of Empty Set is used regularly throughout mathematics, and because it is so important, it is standard to include this axiom in the ZF axioms, even though keeping it is redundant.

Similarly, though of a more technical nature, it is shown in [Lev02, Section I.5] that the Axiom of Selection can be proved using the Axiom of Replacement and other axioms, which means that the Axiom of Selection is redundant. In practice, however, the Axiom of Selection is used frequently throughout mathematics, whereas the Axiom of Replacement is not used nearly as often, so both axioms are included in the ZF axioms, the former to emphasize its usefulness, and the latter because it is needed for some technicalities.

Are the ZF axioms consistent? That is, are we certain that if we deduce everything that can be deduced from the ZF axioms, we would never encounter a logical contradiction? The answer is that we cannot be completely sure. In general, if someone starts with a set of axioms and deduces a specific logical contradiction, then we know that the set of axioms is inconsistent; on the other hand, if no one has yet produced a logical contradiction from a set of axioms, we cannot know if that is because no logical contradiction can possibly be deduced, or if that is because there is a logical contradiction waiting to be found and it has just not been found yet.

However, even if no one has definitively proved that the ZF axioms are consistent, we observe that these axioms have been designed to remove the known problems of naive set theory such as Russell's Paradox. As discussed at the start of the section, Russell's Paradox arises when we let S denote the set of all sets, and we then looked at the set $T = \{A \in S \mid A \notin A\}$. Observe, however, that if S is the set of all sets, then $S \in S$, and yet we saw that that was not possible in our discussion of the Axiom of Regularity. Without the existence of the set S, then we cannot use the Axiom of Selection to define the set T, because that axiom does not allow definitions of the form $T = \{A \mid A \notin A\}$.

Ultimately, the ZF axioms seem reasonable intuitively; they work well in providing a framework for set theory as we would want it; the known problems with naive set theory have been eliminated by the ZF axioms; and experts in the field have not

found any new problems that arise out of these axioms. Hence, we can feel confident that the ZF axioms are a very reasonable choice as the basis for mathematics. We simply cannot do any better than that.

In practice, most mathematicians who are not logicians use set theory in the informal and intuitive way that we saw in the previous sections of this chapter; most mathematicians accept the fact that set theory seems to work as it is supposed to, and do not worry about it beyond that. It is very good that there are logicians who make it their business to work out the foundations of mathematics, but most mathematicians want to prove theorems in their areas of interest (algebra, analysis, topology, combinatorics, etc.), and spending time worrying about the subtleties of the ZF axioms and the like would be too large a distraction. That attitude is certainly recommended for the reader (except when you study logic or set theory in courses dedicated to those fields), and that is the approach we take in this text. Nonetheless, even if most mathematicians do not explicitly think about the ZF axioms on a daily basis, it is well worth knowing that such an axiom system exists, and knowing roughly what it says.

Although we do not recommend getting too caught up in the details of the ZF axioms at this point, there is one additional axiom for set theory with which it is worth spending more time, namely, the famous Axiom of Choice. In contrast to the axioms of ZF, which arouse little controversy and are used implicitly by most mathematicians, the Axiom of Choice is thought by some to be controversial, and when used by mathematicians (and most do use it), it is used much more explicitly than the ZF axioms. The Axiom of Choice is often abbreviated as "AC," and when ZF is combined with AC, the resulting collection of axioms is often abbreviated as "ZFC."

Intuitively, the Axiom of Choice states that if we have a family of non-empty sets, we can simultaneously choose one element from each of the sets in the family. For a single non-empty set, there is no problem choosing an element from the set. Indeed, we regularly say things such as "let A be a non-empty set, and let $a \in A$." For a finite family of non-empty sets, we can choose an element from the first set, and then an element from the second set, and so on, and we will be done after a finite number of steps. Again, there is no problem in making such choices. The problem arises when we have an infinite family of sets (particularly an uncountable family—uncountability will be defined in Section 6.5). From both a practical and a logical point of view, we cannot assume that it is possible to perform an infinite number of steps one at a time, and expect the process ever to be completed. In particular, we cannot choose one element from each set in an infinite family of non-empty sets by making the choices one at a time. If we want to choose one element from each set in an infinite family of non-empty sets, we need to make the choices simultaneously. Such a simultaneous choice is not something we could physically do, and the ability to do so mathematically does not follow from the other axioms of set theory. Therefore, we need an additional axiom to guarantee our ability to make such choices, and that axiom is the Axiom of Choice.

There are a number of equivalent variants of the Axiom of Choice; we use the following. The most convenient, and useful, way of phrasing the Axiom of Choice is with the help of functions, but because we have not defined functions yet, we use the following version that is stated strictly in terms of sets. We will restate the Axiom of

Choice using functions in Section 4.1. Although the problem with choosing elements occurs only in infinite families of sets, the Axiom of Choice is stated for all sets in order to avoid special cases.

For the following version of the Axiom of Choice, recall that in the ZF axioms, all sets are viewed as families of sets.

Axiom of Choice Let x be a set. Suppose that if $y, w \in x$, then $y \neq \emptyset$ and $y \cap w = \emptyset$. Then there is a set z such that if $y \in x$, then $y \cap z$ contains a single element.

The set z in the Axiom of Choice contains one element from each set in x, and these elements can be thought of as having been "chosen" by z, which leads to the name of the axiom, though of course sets do not actually make choices. The requirement that if $y, w \in x$, then $y \neq \emptyset$ and $y \cap w = \emptyset$ guarantees that every set in x has something in it that can be chosen, and that nothing in z could belong to two different sets in x, so that there is genuinely one element in z for each set in x.

For practical applications, it is convenient to reformulate the Axiom of Choice in terms of families of sets indexed by a set. We start with the following definition.

Definition 3.5.1. Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I. The family of sets $\{A_i\}_{i \in I}$ is **pairwise disjoint** if $i, j \in I$ and $i \neq j$ imply that $A_i \cap A_j = \emptyset$.   △

We now restate the Axiom of Choice as follows.

Axiom 3.5.2 (Axiom of Choice for Pairwise Disjoint Sets—Family of Sets Version). *Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of non-empty sets indexed by I. Suppose that $\{A_i\}_{i \in I}$ is pairwise disjoint. Then there is a family of sets $\{C_i\}_{i \in I}$ such that $C_i \subseteq A_i$ and C_i has exactly one element for all $i \in I$.*

Axiom 3.5.2 has the requirement of pairwise disjoint sets because the original statement of the Axiom of Choice did. In practice, however, it is often necessary to apply this axiom to families of non-empty sets that are not necessarily pairwise disjoint. Fortunately, the following version of the Axiom of Choice, which does not assume pairwise disjoint sets, can be deduced from Axiom 3.5.2. A proof of that fact is left to the reader in Exercise 3.5.2. We name the following theorem "Axiom of Choice" without mentioning the fact that pairwise disjoint sets are not required because this version of the Axiom of Choice is the one that is commonly used, and it is the one which we will use subsequently.

Theorem 3.5.3 (Axiom of Choice—Family of Sets Version). *Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of non-empty sets indexed by I. Then there is a family of sets $\{C_i\}_{i \in I}$ such that $C_i \subseteq A_i$ and C_i has exactly one element for all $i \in I$.*

The Axiom of Choice is to be used only when there is no way to avoid it; that is, when we need to choose a single element from each set of a family of non-empty sets and when there is no explicit procedure for such a choice. This point was described amusingly by Bertrand Russell in [Rus19, Chapter 12] as follows. Suppose that a millionaire possesses an infinite number of pairs of boots, and an equal number of pairs of socks. If the millionaire wants to select one boot from each pair, he can

prescribe a specific method for doing so, for example by stating that the left shoe of each pair be chosen; in this case, the Axiom of Choice is not needed. On the other hand, if the millionaire wants to select one sock from each pair, he has no way to prescribe a specific method for doing so, because the two socks in each pair are indistinguishable; hence, for such a selection, an arbitrary choice must be made, and formally such a choice uses the Axiom of Choice (though Russell does not phrase it exactly that way).

For a more mathematical example, suppose that we have a family $\{[a_i, b_i]\}_{i \in I}$ of closed bounded intervals in $\mathbb{R}$, and suppose that we wanted to choose an element from each interval. We would not need to use the Axiom of Choice in this case, because we could, for example, choose the smallest element of each interval, which is a_i.

One of the reasons we single out the Axiom of Choice from the other axioms of set theory is because there are some mathematicians who do not accept the Axiom of Choice. It turns out that the Axiom of Choice is independent of the other axioms of ZF, and hence it can either be accepted or not without having to change the other axioms. This independence, which is due in part to Kurt Gödel in 1938 and in part to Paul Cohen in 1963, means that if the ZF axioms are consistent, then so are the ZF axioms together with the Axiom of Choice, and so are the ZF axioms together with the negation of the Axiom of Choice. For more about the Axiom of Choice, see [Mos06, Chapter 8], and [Moo82], which has a very extensive historical discussion, and [Pot04, Chapter 14], which has some philosophical discussion.

The author, and the majority of mathematicians, have no qualms about using the Axiom of Choice. Indeed, we will use the Axiom of Choice in a few places in this text, for example in the proof of Zorn's Lemma (Theorem 3.5.6) later in this section, and in the proof of Theorem 4.4.5. However, because some mathematicians have reservations about the Axiom of Choice, this axiom should always be mentioned when it is used.

In addition to using the Axiom of Choice directly, we will need a technical fact about sets that is known as Zorn's Lemma, and that is equivalent to the Axiom of Choice. We start with the following definition.

Definition 3.5.4. Let $\mathcal{P}$ be a non-empty family of sets.

1. Let $M \in \mathcal{P}$. The set M is a **maximal element** of $\mathcal{P}$ if there is no $Q \in \mathcal{P}$ such that $M \subsetneq Q$.
2. Let $\mathcal{C} \subseteq \mathcal{P}$. The family $\mathcal{C}$ is a **chain** if $A, B \in \mathcal{C}$ implies $A \subseteq B$ or $A \supseteq B$. $\triangle$

Intuitively, a chain in $\mathcal{P}$ is a subset of $\mathcal{P}$ for which the elements can be lined up in order of inclusion.

As we see in the following example, not every family of sets has a maximal element. In fact, the point of Zorn's Lemma is that it gives a criterion that guarantees the existence of such an element. Observe that a maximal element of a family of sets need not be the largest element of the family; that is, it need not have all the other elements of the family as subsets. A maximal element is simply one that is not a proper subset of any other element of the family. Also, a family of sets can have more than one maximal element.

Example 3.5.5.

(1) Let $\mathcal{P} = \{\{1\}, \{1,2\}, \{1,2,3\}, \{5\}\}$. Then $\mathcal{P}$ has two maximal elements, which are $\{1,2,3\}$ and $\{5\}$. There are nine chains in $\mathcal{P}$, which are

$$\emptyset, \{\{1\}\}, \{\{1,2\}\}, \{\{1,2,3\}\}, \{\{5\}\},$$
$$\{\{1\}, \{1,2\}\}, \{\{1\}, \{1,2,3\}\}, \{\{1,2\}, \{1,2,3\}\},$$
$$\{\{1\}, \{1,2\}, \{1,2,3\}\}.$$

(2) Let $Q = \mathcal{P}(\mathbb{N})$, let $\mathcal{S}$ denote the family of all finite subsets of $\mathbb{N}$ and let $\mathcal{C} = \{\{2\}, \{2,4\}, \{2,4,6\}, \ldots\}$. Then $\mathcal{C}$ is a chain in each of Q and $\mathcal{S}$. Clearly $\bigcup_{C \in \mathcal{C}} C = \{2,4,6,\ldots\}$. Then $\bigcup_{C \in \mathcal{C}} C \in Q$, but $\bigcup_{C \in \mathcal{C}} C \notin \mathcal{S}$. Observe also that Q has a maximal element, which is $\mathbb{N}$, whereas $\mathcal{S}$ has no maximal element, because any finite subset of $\mathbb{N}$ is a proper subset of many other finite subsets of $\mathbb{N}$. ◇

In Example 3.5.5 (2) we observe that in Q, the union of the elements of the chain $\mathcal{C}$ is in Q, and that Q has a maximal element; in $\mathcal{S}$, by contrast, neither of these facts holds. Zorn's Lemma, which we now state, shows that the situation just observed is no coincidence. More specifically, Zorn's Lemma says that if a family of sets contains the union of the elements of each chain in the family, then the family has a maximal element.

Theorem 3.5.6 (**Zorn's Lemma**). *Let $\mathcal{P}$ be a non-empty family of sets. Suppose that for each chain $\mathcal{C}$ in $\mathcal{P}$, the set $\bigcup_{C \in \mathcal{C}} C$ is in $\mathcal{P}$. Then $\mathcal{P}$ has a maximal element.*

Proof. Suppose that $\mathcal{P}$ does not have a maximal element. Then for every $A \in \mathcal{P}$, the set $T_A = \{Q \in \mathcal{P} \mid A \subsetneq Q\}$ is non-empty. Therefore $\{T_A\}_{A \in \mathcal{P}}$ is a family of non-empty sets. By the Axiom of Choice (Theorem 3.5.3) there is a family of sets $\{F_A\}_{A \in \mathcal{P}}$ such that $F_A \subseteq T_A$ and F_A has exactly one element for all $A \in \mathcal{P}$. For each $A \in \mathcal{P}$, let S_A be the single element in F_A, and then $S_A \in \mathcal{P}$ and $A \subsetneq S_A$ for all $A \in \mathcal{P}$.

Let $\mathcal{R} \subseteq \mathcal{P}$. We say that the family $\mathcal{R}$ is **chain-closed** if for each chain $\mathcal{C}$ in $\mathcal{R}$, the set $\bigcup_{C \in \mathcal{C}} C$ is in $\mathcal{R}$.

By hypothesis the family $\mathcal{P}$ is chain-closed. Let $\mathcal{M}$ be the intersection of all chain-closed families in $\mathcal{P}$. Let $\mathcal{C}$ be a chain in $\mathcal{M}$. Then $\mathcal{C}$ is a chain in $\mathcal{R}$ for all chain-closed families $\mathcal{R} \subseteq \mathcal{P}$, and hence $\bigcup_{C \in \mathcal{C}} C \in \mathcal{R}$ for all chain-closed families $\mathcal{R} \subseteq \mathcal{P}$, and therefore $\bigcup_{C \in \mathcal{C}} C \in \mathcal{M}$. Hence $\mathcal{M}$ is chain-closed.

Observe that $\emptyset$ is a chain in $\mathcal{M}$, and that $\bigcup_{C \in \emptyset} C = \emptyset$. Hence $\emptyset \in \mathcal{M}$, which means that $\mathcal{M} \neq \emptyset$.

Let $A \in \mathcal{P}$. Let $\mathcal{A} = \{X \in \mathcal{P} \mid S_A \subseteq X\}$. Then $\mathcal{A} \subseteq \mathcal{P}$. Let $\mathcal{C}$ be a chain in $\mathcal{A}$. Then $\mathcal{C}$ is a chain in $\mathcal{P}$, and hence $\bigcup_{C \in \mathcal{C}} C \in \mathcal{P}$ by hypothesis. If $C \in \mathcal{C}$ then $S_A \subseteq C$, and hence $S_A \subseteq \bigcup_{C \in \mathcal{C}} C$. Therefore $\bigcup_{C \in \mathcal{C}} C \in \mathcal{A}$. It follows that $\mathcal{A}$ is chain-closed. Therefore $\mathcal{M} \subseteq \mathcal{A}$. However, we note that $A \notin \mathcal{A}$, because otherwise we would have $S_A \subseteq A$, which would contradict the fact that $A \subsetneq S_A$. Hence $A \notin \mathcal{M}$.

Because $\mathcal{M} \subseteq \mathcal{P}$, and because $A \notin \mathcal{M}$ for all $A \in \mathcal{P}$, we deduce that $\mathcal{M} = \emptyset$, which is a contradiction. We conclude that $\mathcal{P}$ must have a maximal element. □

The statement of Zorn's Lemma in Theorem 3.5.6 is not the most general form of the Lemma. The most general version is stated in terms of partially ordered sets (also called posets), which we define in Section 7.4, rather than the more narrow context of set inclusion. Moreover, the most general version requires only that every chain has an upper bound, not necessarily a least upper bound; see Exercise 3.5.7 for the definitions of these terms in the context of set inclusion, and Section 7.4 for the definitions for posets. However, even though our version of Zorn's Lemma is not the strongest possible version, it suffices for our purposes, and it is easier to prove. Moreover, it turns out that our version of Zorn's Lemma is actually equivalent to the more general version; see [RR85, Section I.4] for details. Hence, we name Theorem 3.5.6 "Zorn's Lemma" without mentioning the fact that its statement is weaker than other versions. Also, we remark that Zorn's Lemma is not really a lemma, but is rather a very important theorem; the name of this theorem is standard, however, and we will stick with it.

In the proof of Zorn's Lemma (Theorem 3.5.6) we used the Axiom of Choice explicitly by writing out the appropriate family of sets. In practice, however, for the sake of not overly burdening the reader with unnecessary details, most proofs involving the Axiom of Choice use that axiom in a less formal manner, by simply saying that we are choosing something, but without explicitly writing things out in terms of sets, and sometimes without even mentioning the Axiom of Choice at all. For example, a more typical way of defining S_A in the proof of Zorn's Lemma would be: "Suppose that $\mathcal{P}$ does not have a maximal element. Then for every $A \in \mathcal{P}$, there is some $Q \in \mathcal{P}$ such that $A \subsetneqq Q$, and we let $s_A = Q$; if there is more than one such Q, we let s_A be any choice of such Q." We will also use this informal style of invoking the Axiom of Choice when we use it subsequently.

Would it have been possible to prove Zorn's Lemma without invoking the Axiom of Choice? The answer is no, because Zorn's Lemma is equivalent to the Axiom of Choice, by which we mean that if the ZF axioms are assumed together with the Axiom of Choice, it is possible to prove Zorn's Lemma (as we have seen), and if the ZF axioms are assumed together with Zorn's Lemma, it is possible to prove the Axiom of Choice (as will be seen in Exercise 4.1.11). Given that the Axiom of Choice is independent of the ZF axioms, which implies that it is not possible to deduce the Axiom of Choice from only the ZF axioms, it is therefore also not possible to deduce Zorn's Lemma from only the ZF axioms. Hence, we cannot avoid using the Axiom of Choice, or something else equivalent to it, in the proof of Zorn's Lemma. It is a matter of convenience—and choice—which of these two facts is taken as an axiom, and which is to be deduced. The Axiom of Choice is much more intuitively appealing than Zorn's Lemma, and that is perhaps one of the reasons why the former is more often taken axiomatically. On the other hand, there are situations where Zorn's is easier to use directly than the Axiom of Choice, for example in the proof of the Trichotomy Law for Sets (Theorem 6.5.13).

Besides being of great mathematical use, the equivalence of the Axiom of Choice and Zorn's Lemma also explains the following well-known joke (well-known among mathematicians, at least). Question: What is yellow and equivalent to the Axiom of Choice? Answer: Zorn's lemon.

There are also a number of other important facts in mathematics that are equivalent to the Axiom of Choice, a few of which are the following. See [RR85] for an extremely extensive list of statements that are equivalent to the Axiom of Choice.

1. The Trichotomy Law for Sets. See Theorem 6.5.13 for the statement of this theorem and a proof of it using Zorn's Lemma, and see [Sto79, Section 2.9] or [RR85, Section I.3] for the other implication.

2. The Well-Ordering Theorem. This theorem states that for any set, there is an order relation on the set that is well-ordered, which means that every subset has a least element. (An order relation is, informally, a relation that behaves similarly to the standard order on $\mathbb{R}$; a formal definition of an order relation is given in Section 7.4, where it is called a "total ordering" to distinguish it from a "partial ordering.") The standard order on $\mathbb{N}$ is well-ordered by the Well-Ordering Principle (Theorem 6.2.5), but the standard order on $\mathbb{R}$ is certainly not well-ordered. The Well-Ordering Theorem implies that in principle there is some other order on $\mathbb{R}$ that is well-ordered, though there does not appear to be a concrete description of such an order. A proof that the Well-Ordering Theorem implies the Axiom of Choice may be found in Exercise 7.4.18; a proof of the other implication may be found in [HJ99, Section 8.1] or [Sto79, Section 2.9].

3. If $\{A_i\}_{i \in I}$ is a family of non-empty sets indexed by I, then the product $\prod_{i \in I} A_i$ is not empty. See Section 4.5 for the definition of the product of a family of sets, and discussion of the equivalence of this fact with the Axiom of Choice.

4. For any infinite set A, the set $A \times A$ has the same cardinality as A. See Section 6.5 for the definition of infinite sets, and the definition of two sets having the same cardinality. This result is certainly not true for finite sets. See [Sto79, Sections 2.9 and 2.10] or [RR85, Section I.7] for details.

5. Any surjective function has a right inverse. See Section 4.4 for the definition of surjectivity, see Theorem 4.4.5 (1) for a proof that the Axiom of Choice implies this fact, and see Exercise 4.4.19 for the other implication.

We conclude this section with two quotes illustrating the controversy and confusion surrounding the Axiom of Choice.

As mentioned in Item (4) above, the statement "if A is an infinite set then $A \times A$ has the same cardinality as A" implies the Axiom of Choice. This fact is due to Alfred Tarski. In [Myc06] it is related: "Tarski told me the following story. He tried to publish his theorem … in the Comptes Rendus Acad. Sci. Paris but Fréchet and Lebesgue refused to present it. Fréchet wrote that an implication between two well known propositions is not a new result. Lebesgue wrote that an implication between two false propositions is of no interest. And Tarski said that after this misadventure he never tried to publish in the Comptes Rendus." It should be noted that Tarski, Fréchet and Lebesgue are all very important mathematicians of their era, and yet they had very different views about the Axiom of Choice.

Finally, the following widely cited quote, found among other places at [Sch], is due to Jerry Bona: "The Axiom of Choice is obviously true; the Well Ordering Principle is obviously false; and who can tell about Zorn's Lemma?" This quote is amusing precisely because it captures how difficult it is to be sure that the Axiom of Choice is true, because even though it seems very appealing intuitively, it is known to be equivalent to statements that are much less self-evident.

Exercises

Exercise 3.5.1. For each of the following families of intervals in $\mathbb{R}$, suppose that we wanted to choose an element from each interval simultaneously. Would we need to use the Axiom of Choice?

(1) Let $\{(a_i, b_i)\}_{i \in I}$ be a family of non-degenerate open bounded intervals in $\mathbb{R}$.
(2) Let $\{(c_i, \infty)\}_{i \in I}$ be a family of open unbounded intervals in $\mathbb{R}$.

Exercise 3.5.2. [Used in Section 3.5 and Exercise 4.4.19.] Prove that the version of the Axiom of Choice that assumes pairwise disjoint sets (Axiom 3.5.2) implies the version of the Axiom of Choice that does not make such an assumption (Theorem 3.5.3). The idea of the proof is that if we are given a non-empty set J, and a (not necessarily pairwise disjoint) family of sets $\{B_j\}_{j \in J}$ indexed by J, we can form a new family of sets $\{D_j\}_{j \in J}$ defined by $D_j = \{(x, j) \mid x \in B_j\}$ for all $j \in J$.

Exercise 3.5.3. Let $\mathcal{P} = \{\{1\}, \{2\}, \{1,2\}, \{2,3\}, \{1,2,3\}\}$. List all the chains in $\mathcal{P}$.

Exercise 3.5.4. Let $\mathcal{P}$ be a non-empty family of sets, and let $\mathcal{C}$ be a non-empty chain in $\mathcal{P}$. Suppose that $C \neq \emptyset$ for all $C \in \mathcal{C}$. Is $\bigcap_{C \in \mathcal{C}} C$ always non-empty? Give a proof or a counterexample.

Exercise 3.5.5. Let $\mathcal{P}$ and $\mathcal{Q}$ be non-empty families of sets, and let $\mathcal{C} \subseteq \mathcal{P}$ and $\mathcal{D} \subseteq \mathcal{Q}$ be chains. Is $\mathcal{C} \times \mathcal{D}$ always a chain in $\mathcal{P} \times \mathcal{Q}$? Give a proof or a counterexample.

Exercise 3.5.6. Let $\mathcal{P}$ be a non-empty family of sets, let I be a non-empty set and let $\{\mathcal{C}_i\}_{i \in I}$ be a family of chains in $\mathcal{P}$.

(1) Is $\bigcap_{i \in I} \mathcal{C}_i$ always a chain in $\mathcal{P}$? Give a proof or a counterexample.
(2) Is $\bigcup_{i \in I} \mathcal{C}_i$ always a chain in $\mathcal{P}$? Give a proof or a counterexample.

Exercise 3.5.7. [Used in Section 3.5.] Let $\mathcal{P}$ be a non-empty family of sets, let $\mathcal{C} \subseteq \mathcal{P}$ be a chain and let $A \in \mathcal{P}$. The set A is an **upper bound** of $\mathcal{C}$ if $X \subseteq A$ for all $X \in \mathcal{C}$. The set A is a **least upper bound** of $\mathcal{C}$ if it is an upper bound of $\mathcal{C}$, and $A \subseteq Z$ for any other upper bound Z of $\mathcal{C}$.

(1) Suppose that $\mathcal{C}$ has a least upper bound in $\mathcal{P}$. Prove that the least upper bound is unique.
(2) Suppose that $\bigcup_{C \in \mathcal{C}} C \in \mathcal{P}$. Must it be the case that $\bigcup_{C \in \mathcal{C}} C$ is the least upper bound of $\mathcal{C}$? Give a proof or a counterexample.
(3) Suppose that $\mathcal{C}$ has a least upper bound in $\mathcal{P}$. Must it be the case that the least upper bound equals $\bigcup_{C \in \mathcal{C}} C$? Give a proof or a counterexample.

(4) Give an example of a non-empty family Q of subsets of $\mathbb{R}$, and a chain $\mathcal{D} \subseteq Q$, such that $\mathcal{D}$ has an upper bound in Q but not a least upper bound.

4

Functions

A function is the abstract image of the dependence of one magnitude on another.

<div align="right">– A. D. Aleksandrov (1912–1999)</div>

4.1 Functions

The reader has encountered functions repeatedly in previous mathematics courses. In high school one learns about polynomial, exponential, logarithmic and trigonometric functions, among others. Although logarithms and trigonometry are often first encountered without thinking about functions (for example, sines and cosines are thought of in terms of solving right triangles), in calculus courses and above the focus shifts to the point of view of functions (for example, thinking of sine and cosine as functions defined on the entire real number line). The operation of taking a derivative, for example, is something that is done to functions. In applications of calculus, such as in physics or chemistry, it is crucial to think of exponentials, sines and cosines as functions. For example, sine and cosine functions are used to describe simple harmonic motion.

In modern mathematics, where we make use of set theory, functions play an even more important role than in calculus. For example, if we want to compare two sets to see if they have the same size (as discussed in Section 6.5), we use functions between the sets. In group theory, if we want to show that two groups are essentially the same, we use certain types of functions between groups, as discussed briefly in Section 7.3. The same idea holds in many other branches of modern mathematics.

But what is a function really? We all have an intuitive idea of what a function is, usually something of the form $f(x) = x^2$. However, a function need not be described by a formula, nor need it deal with numbers at all. For example, we can form the function that assigns to each person her biological mother; there is certainly no numerical formula that describes this function. We can think of a function informally as a machine, where the input is placed in an opening at the top, and for each object that

is put in, the machine spits a corresponding object out. See Figure 4.1.1. For example, if a function is given by the formula $f(x) = x^2$, then the machine takes numbers as input, and if we put $a = 5$ into the machine, then it will spit out $f(a) = 25$.

Fig. 4.1.1.
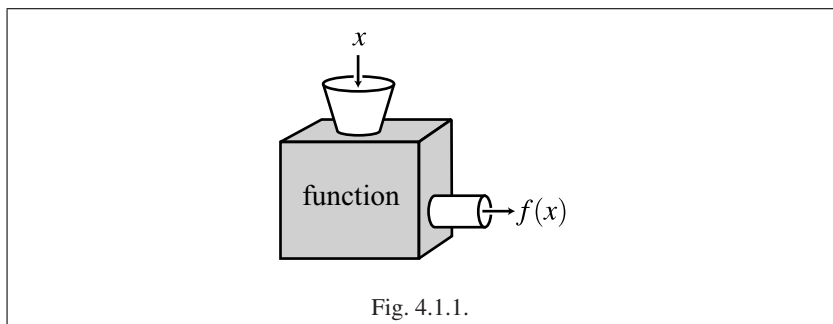
You may have seen a definition of functions that looks something like "a function is a rule of assignment that assigns to each member of one set a unique member of another set." Such a definition is often given in introductory calculus classes, and there is nothing blatantly incorrect about it, but it does not really say anything either. What is a "rule of assignment?" Well, it is a function—but then we are going in circles.

To get out of the above predicament, we give a definition of functions in terms of sets. This rigorous definition will be seen to fit our intuitive picture of functions quite nicely; we cannot formally prove that this definition is identical to our intuitive notion, because formal proofs cannot be applied to informal concepts. To get a feel for our definition, given below, let us consider the function that assigns to each person her biological mother. Although there is no numerical formula that describes this function, we can, however, completely specify this function in a different way, which is by means of a two-column list, where on the left-hand side we list all the people in the world, and on the right-hand side we list each person's mother. Part of this list would be

person	person's mother
Fred Smith	Mary Smith
Susan Levy	Miriam Cohen
Joe al-Haddad	Maryam Mansur
⋮	⋮

Even for functions that are described by nice formulas, we can also think of them as given by lists. Consider the function defined by the formula $f(x) = x^2$ for all integers x. We can make a list for this function, part of which would be

$$
\begin{array}{c|c}
x & x^2 \\
\hline
0 & 0 \\
1 & 1 \\
-1 & 1 \\
2 & 4 \\
5 & 25 \\
\vdots & \vdots
\end{array}
$$

Of course, the list for this function is infinite, so we cannot physically write it all down, but in principle such a list could be made.

By thinking of functions as lists, we have a uniform way of treating all functions, whether given by formulas or not. To make this approach more compatible with set theory, we make one modification. Instead of using a list consisting of two columns, we could use a one-column list, where each entry in the new list is an ordered pair representing the corresponding row of the original two-column list. So, for the function defined by $f(x) = x^2$ for all integers x, we have an infinite list of pairs, containing $(2,4)$, $(-2,4)$, $(5,25)$, and so on. For any given integer c, there will be one and only one ordered pair in this list that has c in its left-hand slot, namely, the pair (c,c^2). On the other hand, the number c^2 appears in the right-hand slot of two pairs, which are (c,c^2) and $(-c,c^2)$, unless $c = 0$. In fact, once we have the idea of representing a function by ordered pairs, we do not need to think of the collection of ordered pairs as being written in a list, but rather, we simply think of it as a set of ordered pairs, as we now see formally in the following definition.

Definition 4.1.1. Let A and B be sets. A **function** (also called a **map**) f from A to B, denoted $f: A \to B$, is a subset $F \subseteq A \times B$ such that for each $a \in A$, there is one and only one pair in F of the form (a,b). The set A is called the **domain** of f and the set B is called the **codomain** of f. △

Definition 4.1.1 is stated entirely in terms of sets, which shows that once we accept set theory as the basis of mathematics, then the use of functions requires no additional hypotheses.

It is important to observe that a function consists of three things: a domain, a codomain, and a subset of the product of the domain and the codomain satisfying a certain condition. Indeed, one way of defining a function is as a triple of sets (A,B,F) where F is a subset of $A \times B$ that satisfies the conditions given in Definition 4.1.1. However, we avoid writing this cumbersome triple notation by observing that in Definition 4.1.1 every function is defined as being from a set A to a set B, denoted $f: A \to B$, and therefore the domain and the codomain of a function are always specified in the definition of the function. Hence, to define a function properly, it is necessary to say "let A and B be sets, and let $f: A \to B$ be a function." We will sometimes be more concise and just say "let $f: A \to B$ be a function," where it is understood from the notation that A and B are sets. It will not suffice, however, to write only "let f be a function" without specifying the domain and codomain, unless the domain and codomain are known from the context.

The need to specify the domain and codomain of a function when defining a function is not a mere formality, but a necessity when treating functions rigorously. For example, consider the set $F = \{(n,n^2) \mid n \in \mathbb{Z}\}$. The set F is a subset of $\mathbb{Z} \times \mathbb{Z}$ that satisfies the conditions given in Definition 4.1.1, and hence F can be thought of as defining a function $\mathbb{Z} \to \mathbb{Z}$. However, the set F is also a subset of $\mathbb{Z} \times \mathbb{R}$ that satisfies the conditions in the definition of a function, and hence F can be thought of as defining a function $\mathbb{Z} \to \mathbb{R}$. Such ambiguity is not acceptable when we use functions in rigorous proofs, and so the domain and codomain of a function must be specified as part of the definition of a function.

Example 4.1.2.

(1) Let A and B be sets. A function from A to B is a subset of $A \times B$. When the sets A and B are finite, rather than thinking of such a subset of $A \times B$ in terms of ordered pairs of the form (a,b), where $a \in A$ and $b \in B$, we can think of the subset graphically in terms of a diagram with the sets A and B and arrows from certain elements of A to certain elements of B, where there is an arrow from a to b when (a,b) is in the subset. For example, let $A = \{a,b,c,d\}$ and $B = \{1,2,3,4\}$. Two diagrams with arrows from A to B are seen in Figure 4.1.2. In Part (i) of the figure the diagram corresponds to the subset $\{(a,2),(b,1),(c,4),(d,4)\} \subseteq A \times B$, and this subset is a function; in Part (ii) of the figure, the corresponding subset of $A \times B$ is $\{(a,1),(a,2),(b,3),(c,4)\}$, and it is not a function.
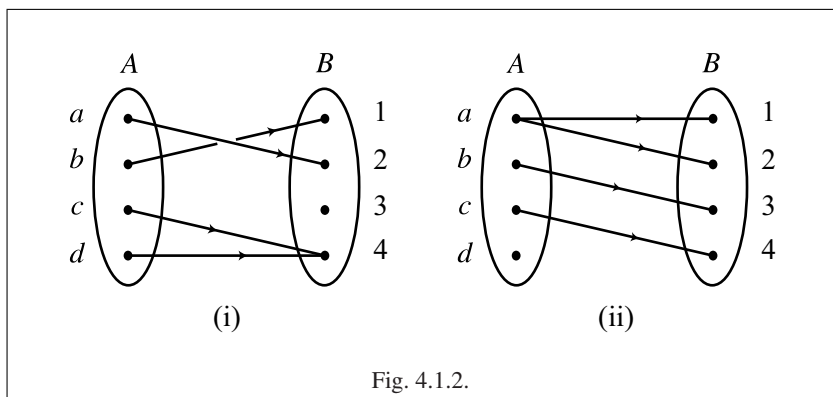
Fig. 4.1.2.

(2) A "rule of assignment" is given by assigning to each person her sister. Is this rule a function? The answer depends upon the choice of domain and codomain, which we have been sloppy in not stating. If the domain is all people, then we certainly do not have a function, because not everyone has a sister. Even if we restrict the domain to all people with sisters there is a problem, because some people have more than one sister, and we do not know which sister is being assigned. Therefore we need to restrict the domain even further to all people with precisely one sister. As for the codomain, it needs to be a set that contains at least all those women who

have siblings, and it could be any choice of such a set (different choices give rise to different functions).

(3) Consider the formula $f(x) = \sqrt{x^2 - 5x + 6}$. On its own, this formula does not properly define a function, because we are not given a domain and codomain. It is standard, however, when given a formula such as this to take as its domain the largest subset of $\mathbb{R}$ that can serve as a domain; in this case the set $(-\infty, 2] \cup [3, \infty)$ is taken as the domain. The codomain might as well be taken to be $\mathbb{R}$, though various subsets of $\mathbb{R}$ could be taken as the codomain as well, for example $[-17, \infty)$. ◊

We defined functions in terms of sets in Definition 4.1.1, but we can in fact recover the intuitive "rule of assignment" approach to functions. Let $f : A \to B$ be a function. Then for each $a \in A$ there is one and only one pair of the form (a, b) in the subset $F \subseteq A \times B$ that defines the function. In other words, for each $a \in A$ there is a unique corresponding $b \in B$, where this b is the unique element of B such that the pair (a, b) is in F. We could then define the term "$f(a)$" (which was not mentioned in our definition of functions) to be $f(a) = b$, where b is as just stated. Hence our formal definition of functions leads to the more usual notation for functions, and so we can now revert to using the more usual notation, though with one important caveat, which we now state.

The use of the "$f(x)$" notation, though legitimate when used properly, often leads to a very common mistake. It is customary in elementary courses (such as calculus) to write phrases such as "let $f(x)$ be a function." Such a phrase, however, is not technically valid. If $f : A \to B$ is a function, then the name of the function is "f," not "$f(x)$." The notation "$f(x)$" means the value of the function f at the element x in the domain; therefore $f(x)$ is an element of the codomain B, rather than the name of the function.

It is often mistakenly thought that "$f(x)$" is the name of the function because x is a "variable," rather than a specific element of the domain. In reality, however, there is no such thing as a variable in a function. It would be commonly understood that the notation "$f(c)$" denotes the value of the function f at the element c in the domain, and so $f(c)$ is an element of the codomain. Why should "$f(x)$" mean anything different from "$f(c)$," except that c is one choice of element in the domain, and x is another such element? Historically, following Descartes, mathematicians have often used letters such as x, y and z to denote "variables," and letters such as a, b and c to denote "constants," but from a rigorous standpoint there is no such distinction. In careful mathematical writing, we always use the notation f to denote the name of the function, and the notation $f(x)$ to denote an element of the codomain. This distinction between f and $f(x)$ might seem to be an overly picky technicality, but it is in fact nothing of the sort. A careless approach in this matter can lead to definite misunderstandings in some tricky situations, such as in Section 4.5.

The proper way to define a function is to state its domain and its codomain, and to state what the function "does" to each element of the domain (which is really the same as defining an appropriate subset of the product of the domain and the codomain). For example, we might write "let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \cos x$ for all $x \in \mathbb{R}$." The phrase "for all $x \in \mathbb{R}$" is crucial, and the definition would not be

correct without it. All the more so, simply stating "let $f(x) = \cos x$" does not define a function. A proper definition of a function based upon a formula must include both the domain and codomain of the function, and it must quantify the "variable" in the formula. We cannot assume that x "ranges over the whole domain" just because it is the letter x. We need the quantifier to tell us which elements of the domain are treated by the formula. Hence the entire statement of the definition of f given above is necessary.

Having just said that it is not correct to present a function by simply writing a formula, there are some situations in which presentations of functions by formulas are considered acceptable. If, in a given context, the domain and codomain can be plausibly guessed, then giving a formula can be sufficient. For example, in an introductory calculus class, we might be given a formula such as $f(x) = \sqrt{x^2 - 5x + 6}$. Because the functions considered in introductory calculus virtually all have domains and codomains that are subsets of $\mathbb{R}$, we could follow the standard practice, as in Example 4.1.2 (3), and take $(-\infty, 2] \cup [3, \infty)$ as the domain, and $\mathbb{R}$ as the codomain. However, because we now wish to attain a higher level of rigor than is found in more elementary mathematics courses, it is usually best to avoid all such informal conventions concerning definitions of functions, and give truly proper definitions, as discussed in the previous paragraph.

Not all functions, even with domain and codomain equal to $\mathbb{R}$, can be defined by a numerical formula. Even when a function is defined by a formula, it is not always possible to use a single formula, and sometimes the formula must be given in cases. Consider, for example, the function $f: \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \begin{cases} x, & \text{if } x \geq 0 \\ -1, & \text{if } x < 0. \end{cases}$$

In general, a function can be presented by breaking up the domain as the union of two or more pairwise disjoint subsets, and defining the function on each of the subsets. To see the subsets used for the above function f, we mention that a more proper, though less pleasant and less commonly used, way to write the above formula would be

$$f(x) = \begin{cases} x, & \text{if } x \in [0, \infty) \\ -1, & \text{if } x \in (-\infty, 0). \end{cases}$$

Whereas the most sensible way to break up the domain of a function is into pairwise disjoint subsets, it is sometimes more convenient to break up the domain into subsets that are not disjoint. For example, we might define a function $g: \mathbb{R} \to \mathbb{R}$ by

$$g(x) = \begin{cases} x^2, & \text{if } x \geq 3 \\ x+6, & \text{if } x \leq 3. \end{cases}$$

In contrast to the case in which the domain is broken up into pairwise disjoint subsets, where there is nothing to check, in this case we must verify that the formulas for the two subsets agree when evaluated at the element common to both subsets

(which is $x = 3$). Everything works out fine, because $3^2 = 9$ and $3 + 6 = 9$, and so the way we presented g makes sense. This situation is usually expressed by saying that the function g is **well-defined**. On the other hand, if a function is presented with overlapping subsets, and if the formulas do not agree on the overlap, then we do not have a function at all.

The concept of a function being well-defined has a more general meaning than what we stated above. In general, a function is said to be well-defined if there is some potential problem with the definition of the function, and it turns out that the problem does not in fact occur. In practice, saying that a function is well-defined usually means that one of two things has been verified: that every element of the domain is indeed taken into the codomain, or that the function has only one value for every element of the domain. Our use of the term well-defined in the previous paragraph is of the second type. An example of the first type of use of the term well-defined occurs in Exercise 4.4.8.

A look at the special case of functions $\mathbb{R} \to \mathbb{R}$ can help us gain some insight into functions generally. Let $f\colon \mathbb{R} \to \mathbb{R}$ be a function. Then f gives rise to a graph in $\mathbb{R}^2$, where the graph consists of all points in $\mathbb{R}^2$ of the form $(x, f(x))$, where $x \in \mathbb{R}$. For each such x, the definition of functions implies that there is one and only one corresponding value $f(x) \in \mathbb{R}$. Hence, for each $x \in \mathbb{R}$ there is one and only one point on the graph of f that is on the vertical line through x. See Figure 4.1.3. Conversely, suppose that we are given a curve in $\mathbb{R}^2$. Is this curve necessarily the graph of some function $g\colon \mathbb{R} \to \mathbb{R}$? If the curve has the property that it intersects each vertical line in the plane at precisely one point, then the curve will be the graph of some function $g\colon \mathbb{R} \to \mathbb{R}$; if this property does not hold, then the curve will not be the graph of such a function.

Fig. 4.1.3.
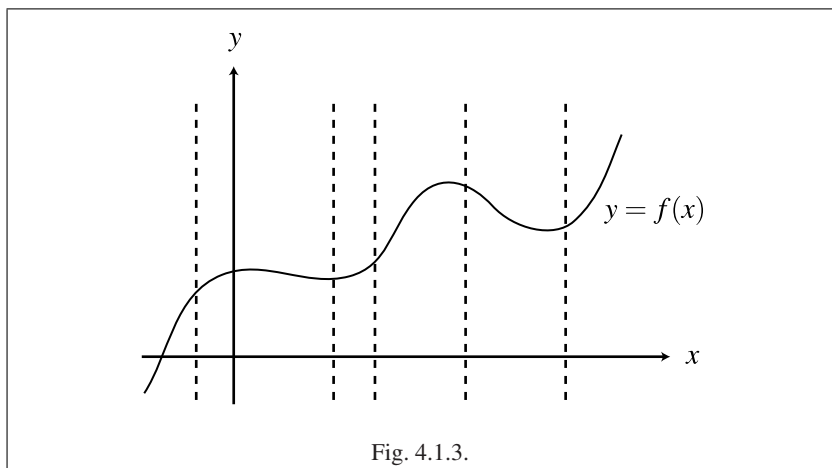
As we noted earlier, a function consists of three things: a domain, a codomain and a subset of the product of the domain and the codomain satisfying a certain

condition. For two functions to be considered equal, they need to have all three of these things be the same. If even one of these three things is changed, a different function is obtained. For example, the function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 + 1$ for all $x \in \mathbb{R}$ is not the same function as $g: \mathbb{R} \to (0, \infty)$ defined by $g(x) = x^2 + 1$ for all $x \in \mathbb{R}$, even though they both have the same formula and the same domain.

Let $f: A \to B$ and $g: C \to D$ be functions. To say that "$f = g$" means that $A = C$, that $B = D$ and that the two functions correspond to the same subset of $A \times B$. This last statement can be rephrased by saying that $f(x) = g(x)$ for all $x \in A$. Observe that the statement "$f(x) = g(x)$ for all $x \in A$" is not a statement about equivalent formulas for f and g, because the functions f and g might not be given by formulas at all, but is rather a statement about the equality of various elements in the codomain. That is, a single statement about functions, namely, the statement $f = g$, is equivalent to a collection of statements about elements in the codomain (once it is ascertained that the two functions have the same domain and codomain). A proof that f and g are equal typically has the following form.

Proof. (Argumentation)

$\vdots$

Therefore the domain of f is the same as the domain of g.

$\vdots$

(argumentation)

$\vdots$

Therefore the codomain of f is the same as the codomain of g.
    Let a be in the domain of f and g.

$\vdots$

(argumentation)

$\vdots$

Then $f(a) = g(a)$.
    Therefore $f = g$.   □

There are some particularly useful types of functions that are encountered throughout mathematics.

Definition 4.1.3. Let A and B be sets, and let $S \subseteq A$ be a subset.

1. A **constant map** $f: A \to B$ is any function of the form $f(x) = b$ for all $x \in A$, where $b \in B$ is some fixed element.
2. The **identity map** on A is the function $1_A: A \to A$ defined by $1_A(x) = x$ for all $x \in A$.
3. The **inclusion map** from S to A is the function $j: S \to A$ defined by $j(x) = x$ for all $x \in S$.
4. If $f: A \to B$ is a function, the **restriction** of f to S, denoted $f|_S$, is the function $f|_S: S \to B$ defined by $f|_S(x) = f(x)$ for all $x \in S$.

   5. If $g\colon S \to B$ is a function, an **extension** of g to A is any function $G\colon A \to B$ such that $G|_S = g$.

   6. The **projection maps** from $A \times B$ are the functions $\pi_1\colon A \times B \to A$ and $\pi_2\colon A \times B \to B$ defined by $\pi_1((a,b)) = a$ and $\pi_2((a,b)) = b$ for all $(a,b) \in A \times B$. For any finite collection of sets $A_1, \ldots, A_p$, projection maps

$$\pi_i\colon A_1 \times \cdots \times A_p \to A_i$$

   for all $i \in \{1, \ldots, p\}$ can be defined similarly. $\triangle$

Example 4.1.4.

   (1) Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \sin x$ for all $x \in \mathbb{R}$. Then the restriction of f to $\mathbb{Q}$ is the function $f|_{\mathbb{Q}}\colon \mathbb{Q} \to \mathbb{R}$ defined by $f|_{\mathbb{Q}}(x) = \sin x$ for all $x \in \mathbb{Q}$.

   (2) Let $X = \{a,b,c\}$, let $Y = \{a,b\}$ and let $Z = \{1,2,3\}$. Let $f\colon Y \to Z$ be defined by $f(a) = 3$ and $f(b) = 2$, and let $g,h\colon X \to Z$ be defined by $g(a) = 3$, and $g(b) = 2$, and $g(c) = 1$, and $h(a) = 3$, and $h(b) = 1$, and $h(c) = 2$. Then g is an extension of f, because $g|_Y = f$, but h is not an extension of f. There are other possible extensions of f.

   (3) We can think of $\mathbb{R}^2$ as $\mathbb{R} \times \mathbb{R}$. We then have the two projection maps $\pi_1\colon \mathbb{R}^2 \to \mathbb{R}$ and $\pi_2\colon \mathbb{R}^2 \to \mathbb{R}$ that are defined by $\pi_1((x,y)) = x$ and $\pi_2((x,y)) = y$ for all $(x,y) \in \mathbb{R}^2$. That is, the projection map π_1 picks out the first coordinate of the point (x,y), for all $(x,y) \in \mathbb{R}^2$, and similarly for π_2. $\lozenge$

   In addition to the general types of functions given in Definition 4.1.3, which we will use throughout this text, we will also make use of some standard functions $\mathbb{R} \to \mathbb{R}$, such as polynomials, exponentials, logarithms and trigonometric functions in various examples. It is beyond the scope of this text to define these standard functions, but they can indeed be defined rigorously, and all the familiar properties can be proved, so no harm is done in our using these functions. See [Blo11, Chapter 7] for rigorous definitions of such functions.

   We conclude this section with a brief comment about the Axiom of Choice, which was first discussed in Section 3.5. In that section we did not have functions at our disposal, and hence our statement of the axiom in Theorem 3.5.3 was in terms of families of sets. However, it is much more natural, and convenient, to use functions to state the Axiom of Choice, which we now do. We do not need to prove this new version of the Axiom of Choice, because it is simply a restatement of Theorem 3.5.3.

Theorem 4.1.5 (**Axiom of Choice—Functions Version**). *Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of non-empty sets indexed by I. Then there is a function $f\colon I \to \bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$.*

   The function given in Theorem 4.1.5 is called a **choice function** for $\{A_i\}_{i \in I}$. It is also possible to formulate a non-indexed version of the Axiom of Choice using functions, which we leave to the reader in Exercise 4.1.9.

$$\boxed{\textbf{Exercises}}$$

Exercise 4.1.1. Let $A = \{a,b,c\}$ and $B = \{1,2,3\}$. Which of the following subsets of $A \times B$ are functions $A \to B$?

   (1) $\{(b,1),(c,2),(a,3)\}$.   **(4)** $\{(a,1),(b,3)\}$.
   (2) $\{(a,3),(c,2),(a,1)\}$.   **(5)** $\{(c,1),(a,2),(b,3),(c,2)\}$.
   (3) $\{(c,1),(b,1),(a,2)\}$.   **(6)** $\{(a,3),(c,3),(b,3)\}$.

Exercise 4.1.2. Let X denote the set of all people. Which of the following descriptions define functions $X \to X$?

   (1) $f(a)$ is the mother of a.
   (2) $g(a)$ is a brother of a.
   (3) $h(a)$ is the best friend of a.
   (4) $k(a)$ is the firstborn child of a if she is a parent, and is the father of a otherwise.
   (5) $j(a)$ is the sibling of a if she has siblings, and is a otherwise.

Exercise 4.1.3. Which of the diagrams in Figure 4.1.4 represent functions?

Fig. 4.1.4.
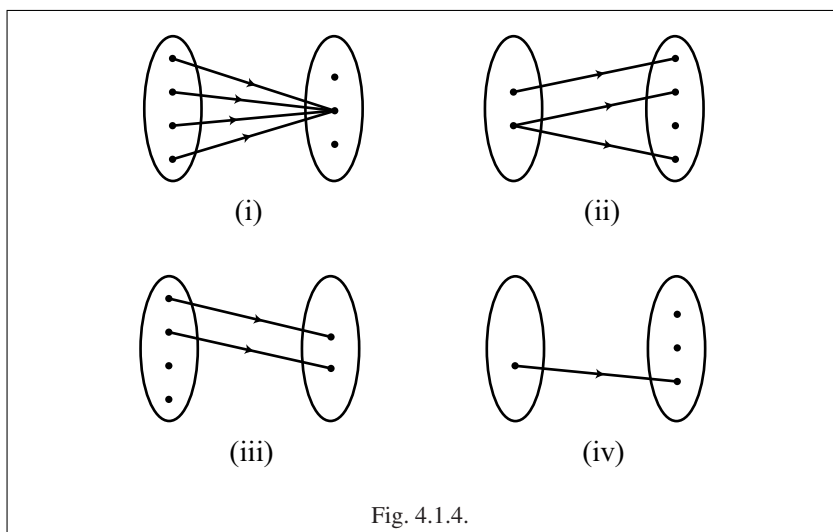
Exercise 4.1.4. Which of the following descriptions properly describe functions?

   (1) Let $f(x) = \cos x$.
   (2) To every person a, let $g(a)$ be the height of a in inches.
   (3) For every real number, assign the real number that is the logarithm of the original number.
   (4) Let $g \colon \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = e^x$.

Exercise 4.1.5. Which of the following formulas define functions $\mathbb{R} \to \mathbb{R}$?

(1) $f(x) = \sin x$ for all $x \in \mathbb{R}$.

(2) $p(x) = \frac{x^2+3}{x+5}$ for all $x \in \mathbb{R}$.

(3) $q(x) = \ln(x^4 + 1)$ for all $x \in \mathbb{R}$.

(4) $r(x) = \begin{cases} e^x, & \text{if } x \geq 0 \\ \cos x, & \text{if } x \leq 0. \end{cases}$

(5) $s(x) = \begin{cases} x^2, & \text{if } x \geq 1 \\ x^3, & \text{if } x \leq 0. \end{cases}$

(6) $t(x) = \begin{cases} x^3 - 2, & \text{if } x \geq 1 \\ |x|, & \text{if } x \leq 1. \end{cases}$

(7) $g(x) = \begin{cases} \sin x, & \text{if } x \geq \pi \\ x, & \text{if } x < \pi. \end{cases}$

Exercise 4.1.6. For each of the following formulas, find the largest subset $X \subseteq \mathbb{R}$ such that $g \colon X \to \mathbb{R}$ is a function.

(1) $g(x) = \frac{1}{x^4-3}$ for all $x \in X$.

(2) $g(x) = \sqrt{1-x^2}$ for all $x \in X$.

(3) $g(x) = 3\ln(\sin x)$ for all $x \in X$.

(4) $g(x) = \begin{cases} \sqrt{x}, & \text{if } x \in X \text{ and } x \geq 0 \\ x+1, & \text{if } x \in X \text{ and } x \leq 0. \end{cases}$

(5) $g(x) = \begin{cases} \tan \pi x + 4, & \text{if } x \in X \text{ and } x \geq 1 \\ 3x^2 + 1, & \text{if } x \in X \text{ and } x \leq 1. \end{cases}$

Exercise 4.1.7. Let A and B be sets, let $S \subseteq A$ be a subset and let $f \colon A \to B$ be a function. Let $g \colon A \to B$ be an extension of $f|_S$ to A. Does g equal f? Give a proof or a counterexample.

Exercise 4.1.8. **[Used in Theorem 4.5.4 and Section 8.7.]** Let X be a non-empty set, and let $S \subseteq X$ be a subset. The **characteristic map** for S in X, denoted χ_S, is the function $\chi_S \colon X \to \{0,1\}$ defined by

$$\chi_S(y) = \begin{cases} 1, & \text{if } y \in S \\ 0, & \text{if } y \in X - S. \end{cases}$$

Let $A, B \subseteq X$ be subsets. Prove that $\chi_A = \chi_B$ if and only if $A = B$. (Observe that "$\chi_A = \chi_B$" is a statement of equality of functions, whereas "$A = B$" is a statement of equality of sets.)

Exercise 4.1.9. **[Used in Section 4.1.]** Restate Theorem 4.1.5 in a non-indexed version.

Exercise 4.1.10. **[Used in Exercise 4.1.11.]** Let A and B be sets. A **partial function** from A to B is a function of the form $f_J \colon J \to B$, where $J \subseteq A$. We can think of partial functions from A to B as subsets of $A \times B$ that satisfy a certain condition.

Let f_J and g_K be partial functions from A to B. Prove that $f_J \subseteq g_K$ if and only if $J \subseteq K$ and $g_K|_J = f_J$.

Exercise 4.1.11. **[Used in Section 3.5.]** The purpose of this exercise is to prove that Zorn's Lemma (Theorem 3.5.6) implies the Axiom of Choice. Given that we used

the latter in the proof of the former, it will follow that the two results are equivalent. We make use here of the version of the Axiom of Choice stated in Theorem 4.1.5.

Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of non-empty sets indexed by I. Assume Zorn's Lemma. We will show that there is a choice function for $\{A_i\}_{i \in I}$.

(1) A **partial choice function** for $\{A_i\}_{i \in I}$ is a function $f_J : J \to \bigcup_{j \in J} A_j$ for some $J \subseteq I$ such that $f_J(j) \in A_j$ for all $j \in J$. If f_J is a partial choice function for $\{A_i\}_{i \in I}$, we can think of f_J as a subset of $J \times \bigcup_{j \in J} A_j \subseteq I \times \bigcup_{i \in I} A_i$.

(2) Let $\mathcal{P}$ be the set of all partial choice functions for $\{A_i\}_{i \in I}$, and let $\mathcal{C}$ be a chain in $\mathcal{P}$. Prove that $\bigcup_{C \in \mathcal{C}} C$ is in $\mathcal{P}$.   [Use Exercise 4.1.10.]

(3) By Zorn's Lemma the family of sets $\mathcal{P}$ has a maximal element. Let $f_K \in \mathcal{P}$ be such a maximal element. Prove that $K = I$. (Recall that the Axiom of Choice is not needed to choose an element from a single non-empty set.)

(4) Deduce Theorem 4.1.5.

4.2 Image and Inverse Image

Let A denote the set of all adults (defined for example to be people 18 years and older), and let $h : A \to \mathbb{R}$ be defined by letting $h(x)$ be the height in inches of person x. There are a number of things we might want to do with this function. For example, we might want to find the various heights found among all adults living in France. This set of heights would be written in set notation as $\{h(x) \mid x \text{ lives in France}\}$. Alternatively, and more useful to us, we could write this set as $\{r \in \mathbb{R} \mid r = h(x) \text{ for some } x \text{ who lives in France}\}$. What we are doing here is taking a subset of the domain, namely, all adults living in France, and finding the corresponding subset of the codomain, namely, all possible real numbers that arise as the heights of adults in France.

We might also want to find all the adults whose heights are at least 6 ft. and no more than 6 ft. 3 in. Because we are working in inches, we therefore want to find all people whose heights are in the interval $[72, 75]$. Hence, we want the set $\{x \in A \mid h(x) \in [72, 75]\}$. In this case we are taking a subset of the codomain, namely, a certain set of possible heights, and finding the corresponding subset of the domain, namely, all people whose heights are as desired.

The following definition generalizes the above process. Given a function $f : A \to B$, we want to take each subset P of A, and see where f sends all of its elements (which will give us a subset of B), and we want to take each subset Q of B, and see which elements of A are mapped into it by f (which will give us a subset of A).

Definition 4.2.1. Let A and B be sets, and let $f : A \to B$ be a function.

1. Let $P \subseteq A$. The **image** of P under f, denoted $f(P)$, is the set defined by

$$f(P) = \{b \in B \mid b = f(p) \text{ for some } p \in P\}.$$

The **range** of f (also called the **image** of f) is the set $f(A)$.

2. Let $Q \subseteq B$. The **inverse image** of Q under f, denoted $f^{-1}(Q)$, is the set defined by

$$f^{-1}(Q) = \{a \in A \mid f(a) \in Q\}. \qquad \triangle$$

See Figure 4.2.1 for a schematic drawing of $f(P)$ and $f^{-1}(Q)$.

Fig. 4.2.1.
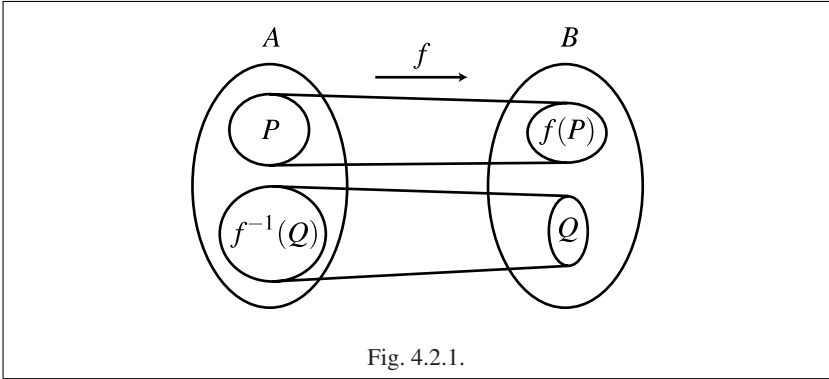
Example 4.2.2. Let $f \colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 6x$ for all $x \in \mathbb{R}$. It is straightforward to compute that $f([6,7]) = [0,7]$, that $f^{-1}([0,4]) = \left[3 - \sqrt{13}, 0\right] \cup \left[6, 3 + \sqrt{13}\right]$, that $f^{-1}([-12,-10]) = \emptyset$ and that the range of the function is $[-9, \infty)$; the details are left to the reader (it helps to graph the function). $\qquad \diamond$

In Part (1) of Definition 4.2.1 it would have been possible to have written

$$f(P) = \{f(p) \mid p \in P\},$$

and in Part (2) of the definition it would have been possible to have written

$$f^{-1}(Q) = \{a \in A \mid f(a) = q \text{ for some } q \in Q\}.$$

However, the method of defining these sets given in Definition 4.2.1 will be more useful to us than these alternatives.

The terms "range" and "codomain" are often confused, so precise use of language is needed.

The notations "$f(P)$" and "$f^{-1}(Q)$" are widely used, and so we will use them too, but they need some clarification. The notation "$f(P)$" is not formally meaningful, because only elements of the domain (not subsets of it) can be substituted into f. Writing $f(P)$ is an example of what mathematicians refer to as "abuse of notation," which means a way of writing something that is technically incorrect, but which is convenient to use and which causes no problems.

Unfortunately, it cannot be said that the notation "$f^{-1}(Q)$" causes no problems. We urge the reader to use this notation with caution, for the following reason. Later in this chapter, we will discuss the notion of an inverse function (in Definition 4.3.6).

If a function $f\colon A \to B$ has an inverse function (which is not true for all functions), then the inverse function is denoted f^{-1}. Even though this latter notation is very similar to the notation $f^{-1}(Q)$, the concept of an inverse image of a set and the concept of an inverse function are quite different, and it is the similarity of notation for different concepts that is the source of the problem. The inverse image $f^{-1}(Q)$ is a subset of the domain of f, and is always defined for any function f and any subset Q of the codomain. By contrast, the inverse function f^{-1} does not always exist; if it does exist, then it is a function $B \to A$, not a subset of A. It is very important to keep in mind that the notation $f^{-1}(Q)$ does not necessarily mean the image of the set Q under f^{-1}, because $f^{-1}(Q)$ is used even in cases where the function f^{-1} does not exist. Proofs about sets of the form $f^{-1}(Q)$ should not make use of an inverse function f^{-1} unless there is a specific reason to assume that f^{-1} exists.

The following example should further demonstrate that the notation $f^{-1}(D)$ should be used with caution, because in this context the notations "f" and "f^{-1}" do not necessarily "cancel each other out," as might be mistakenly assumed.

Example 4.2.3. Let $h\colon \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = x^2$ for all $x \in \mathbb{R}$. It is straightforward to compute that $h([0,3]) = [0,9]$ and $h([-2,2]) = [0,4]$. Then $h^{-1}(h([0,3])) = h^{-1}([0,9]) = [-3,3]$. We therefore see that $h^{-1}(h([0,3])) \neq [0,3]$. Similarly, we compute that $h(h^{-1}([-4,4])) = h([-2,2]) = [0,4]$, and hence $h(h^{-1}([-4,4])) \neq [-4,4]$. $\Diamond$

For the proof of the following theorem, as well as for subsequent results involving images and inverse images, we need two observations about proof strategies. First, suppose that we wish to prove that either of $f(P)$ or $f^{-1}(Q)$ is equal to some other set. Though we are dealing with functions, we observe that objects of the form $f(P)$ or $f^{-1}(Q)$ are sets, and to prove that they are equal to other sets (which is the only sort of thing to which they could be equal), we use the standard strategy for proving equality of sets, which is showing that each set is a subset of the other.

Second, we mention that statements of the form "$x \in f(P)$" and "$z \in f^{-1}(Q)$" are difficult to work with directly, and it is usually easier if we first transform such statements into equivalent ones that do not involve images and inverse images. More specifically, suppose that we start with a statement of the form "$x \in f(P)$." The definition of $f(P)$ then allows us to rewrite the statement as "$x = f(a)$ for some $a \in P$," and we observe that this latter statement does not involve the image of a set, making it easier to work with than the original statement. Conversely, a statement of the form "$x = f(a)$ for some $a \in P$" can be rewritten as "$x \in f(P)$." Similarly, suppose that we start with a statement of the form "$z \in f^{-1}(Q)$." The definition of $f^{-1}(Q)$ allows us to rewrite the statement as "$f(z) \in Q$," which again is easier to work with than the original statement. Conversely, a statement of the form "$f(z) \in Q$" can be rewritten as "$z \in f^{-1}(Q)$." As is the case with many problems in mathematics, going back to the definitions is often the best way to start creating a proof.

The following theorem, the proof of which uses the above mentioned strategies, gives some of the most basic properties of images and inverse images. Observe in Part (7) of the theorem that images are not quite as well behaved as inverse images.

Theorem 4.2.4. *Let A and B be sets, let $C, D \subseteq A$ and $S, T \subseteq B$ be subsets, and let $f \colon A \to B$ be a function. Let I and K be non-empty sets, let $\{U_i\}_{i \in I}$ be a family of subsets of A indexed by I, and let $\{V_k\}_{k \in K}$ be a family of subsets of B indexed by K.*

1. *$f(\emptyset) = \emptyset$ and $f^{-1}(\emptyset) = \emptyset$.*
2. *$f^{-1}(B) = A$.*
3. *$f(C) \subseteq S$ if and only if $C \subseteq f^{-1}(S)$.*
4. *If $C \subseteq D$, then $f(C) \subseteq f(D)$.*
5. *If $S \subseteq T$, then $f^{-1}(S) \subseteq f^{-1}(T)$.*
6. *$f\left(\bigcup_{i \in I} U_i\right) = \bigcup_{i \in I} f(U_i)$.*
7. *$f\left(\bigcap_{i \in I} U_i\right) \subseteq \bigcap_{i \in I} f(U_i)$.*
8. *$f^{-1}\left(\bigcup_{k \in K} V_k\right) = \bigcup_{k \in K} f^{-1}(V_k)$.*
9. *$f^{-1}\left(\bigcap_{k \in K} V_k\right) = \bigcap_{k \in K} f^{-1}(V_k)$.*

Proof. We will prove Parts (5) and (6), leaving the rest to the reader in Exercise 4.2.6.

(5). Suppose that $S \subseteq T$. Let $x \in f^{-1}(S)$. Then by definition $f(x) \in S$. Because $S \subseteq T$, it follows that $f(x) \in T$. Hence $x \in f^{-1}(T)$. We deduce that $f^{-1}(S) \subseteq f^{-1}(T)$.

(6). First, let $b \in f\left(\bigcup_{i \in I} U_i\right)$. Then $b = f(u)$ for some $u \in \bigcup_{i \in I} U_i$. Therefore $u \in U_j$ for some $j \in I$. Hence $b \in f(U_j) \subseteq \bigcup_{i \in I} f(U_i)$. It follows that $f\left(\bigcup_{i \in I} U_i\right) \subseteq \bigcup_{i \in I} f(U_i)$. Next, let $a \in \bigcup_{i \in I} f(U_i)$. Then $a \in f(U_k)$ for some $k \in I$. Hence $a = f(v)$ for some $v \in U_k$. Because $v \in \bigcup_{i \in I} U_i$, it follows that $a \in f\left(\bigcup_{i \in I} U_i\right)$. Therefore $\bigcup_{i \in I} f(U_i) \subseteq f\left(\bigcup_{i \in I} U_i\right)$. We conclude that $f\left(\bigcup_{i \in I} U_i\right) = \bigcup_{i \in I} f(U_i)$. $\qquad\square$

We conclude our discussion of images and inverse images with a slightly more abstract approach to the subject. Let $f \colon A \to B$ be a function. If $P \subseteq A$, then $f(P) \subseteq B$. That is, for every element $P \in \mathcal{P}(A)$, we obtain an element $f(P) \in \mathcal{P}(B)$. Hence, the process of taking images of subsets of A amounts to the fact that the function f induces a new function $f_* \colon \mathcal{P}(A) \to \mathcal{P}(B)$, which is defined by $f_*(P) = f(P)$ for all $P \in \mathcal{P}(A)$. Similarly, for every element $Q \in \mathcal{P}(B)$, we obtain an element $f^{-1}(Q) \in \mathcal{P}(A)$, and hence, the process of taking inverse images of subsets of B amounts to the fact that the function f induces a new function $f^* \colon \mathcal{P}(B) \to \mathcal{P}(A)$, which is defined by $f^*(P) = f^{-1}(Q)$ for all $Q \in \mathcal{P}(B)$. From that point of view, the terms "image" and "inverse image" are redundant. For example, the notation "$f_*(P)$" simply means the result of applying the function f_* to the element P in the domain of f_*, and hence we do not need to call "$f_*(P)$" by the special name "the image of P under f." However, although this more abstract point of view is a technically correct way to think of images and inverse images, it is usually more useful in the course of formulating proofs to think of images and inverse images as we have done until now, and so we will not be making use of this more abstract approach other than in a few exercises.

$$\boxed{\textbf{Exercises}}$$

Exercise 4.2.1. Find the range of each of the following functions.

(1) Let $f \colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^6 - 5$ for all $x \in \mathbb{R}$.

(2) Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^3 - x^2$ for all $x \in \mathbb{R}$.
(3) Let $h\colon \mathbb{R} \to (0, \infty)$ be defined by $h(x) = e^{x-1} + 3$ for all $x \in \mathbb{R}$.
(4) Let $p\colon \mathbb{R} \to \mathbb{R}$ be defined by $p(x) = \sqrt{x^4 + 5}$ for all $x \in \mathbb{R}$.
(5) Let $q\colon \mathbb{R} \to [-10, 10]$ be defined by $q(x) = \sin x + \cos x$ for all $x \in \mathbb{R}$.

Exercise 4.2.2. Let C be the set of all cows in the world. Let $m\colon C \to \mathbb{R}$ be the function defined by letting $m(c)$ equal the average daily milk production in gallons of cow c. Describe in words each of the following sets.

(1) $m(\{\text{Bessie}, \text{Bossie}\})$.
(2) $m(F)$, where F denotes all the cows in India.
(3) $m^{-1}([1,3])$.
(4) $m^{-1}([-5,3])$.
(5) $m^{-1}(\{0\})$.

Exercise 4.2.3. For each of the following functions $f\colon \mathbb{R} \to \mathbb{R}$ and each set $T \subseteq \mathbb{R}$, find $f(T)$, $f^{-1}(T)$, $f(f^{-1}(T))$ and $f^{-1}(f(T))$.

(1) Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = (x+1)^2$ for all $x \in \mathbb{R}$, and let $T = [-1,1]$.
(2) Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = (x+1)^2$ for all $x \in \mathbb{R}$, and let $T = [-5,2]$.
(3) Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \lceil x \rceil$ for all $x \in \mathbb{R}$, where $\lceil x \rceil$ is the smallest integer greater than or equal to x, and let $T = (1,3)$.
(4) Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \lfloor x \rfloor$ for all $x \in \mathbb{R}$, where $\lfloor x \rfloor$ is the greatest integer less than or equal to x, and let $T = [0,2] \cup (5,7)$.

Exercise 4.2.4. Let $g\colon \mathbb{R}^2 \to \mathbb{R}$ be defined by $g((x,y)) = xy$ for all $(x,y) \in \mathbb{R}$. Sketch each of the following subsets of $\mathbb{R}^2$.

(1) $g^{-1}(\{3\})$.   **(2)** $g^{-1}([-1,1])$.

Exercise 4.2.5. Let X and Y be sets, let $A \subseteq X$ and $B \subseteq Y$ be subsets and let $\pi_1\colon X \times Y \to X$ and $\pi_2\colon X \times Y \to Y$ be projection maps as defined in Section 4.1.

(1) Prove that $(\pi_1)^{-1}(A) = A \times Y$ and $(\pi_2)^{-1}(B) = X \times B$.
(2) Prove that $(\pi_1)^{-1}(A) \cap (\pi_2)^{-1}(B) = A \times B$.
(3) Let $P \subseteq X \times Y$. Does $\pi_1(P) \times \pi_2(P) = P$? Give a proof or a counterexample.

Exercise 4.2.6. [Used in Theorem 4.2.4.] Prove Theorem 4.2.4 (1) (2) (3) (4) (7) (8) (9).

Exercise 4.2.7. Find the flaw(s) in the following alleged proof of Theorem 4.2.4 (8), assuming that Parts (1)–(7) have already been proved: "Applying f to $f^{-1}\left(\bigcup_{k \in K} V_k\right)$ we obtain $f\left(f^{-1}\left(\bigcup_{k \in K} V_k\right)\right) = \bigcup_{k \in K} V_k$. Applying f to $\bigcup_{k \in K} f^{-1}(V_k)$, and using Part (6) of the theorem, we obtain $f\left(\bigcup_{k \in K} f^{-1}(V_k)\right) = \bigcup_{k \in K} f(f^{-1}(V_k)) = \bigcup_{k \in K} V_k$. Because applying f to both sides of the equation in Part (8) yields the same result, we deduce that the equation in Part (8) is true."

Exercise 4.2.8. In this exercise we show that it is not possible to strengthen Theorem 4.2.4 (3).

(1) Find an example of a function $f: A \to B$ together with sets $X \subseteq A$ and $Y \subseteq B$ such that $f(X) = Y$ and $X \neq f^{-1}(Y)$.

(2) Find an example of a function $g: J \to K$ together with sets $Z \subseteq J$ and $W \subseteq K$ such that $f^{-1}(W) = Z$ and $f(Z) \neq W$.

Exercise 4.2.9. Find an example to show that the "$\subseteq$" in Theorem 4.2.4 (7) cannot be replaced with "$=$." It is sufficient to use the intersection of two sets.

Exercise 4.2.10.

(1) Find an example of a function $f: A \to B$ and subsets $P, Q \subseteq A$ such that $P \subsetneq Q$, but that $f(P) = f(Q)$.

(2) Find an example of a function $g: C \to D$ and subsets $S, T \subseteq D$ such that $S \subsetneq T$, but that $g^{-1}(S) = g^{-1}(T)$.

Exercise 4.2.11. [Used in Exercise 4.4.11.] Let A and B be sets, let $P, Q \subseteq A$ be subsets and let $f: A \to B$ be a function.

(1) Prove that $f(P) - f(Q) \subseteq f(P - Q)$.

(2) Is it necessarily the case that $f(P - Q) \subseteq f(P) - f(Q)$? Give a proof or a counterexample.

Exercise 4.2.12. Let A and B be sets, let $C, D \subseteq B$ be subsets and let $f: A \to B$ be a function. Prove that $f^{-1}(D - C) = f^{-1}(D) - f^{-1}(C)$.

Exercise 4.2.13. Let A and B be sets, let $X \subseteq A$ and $Y \subseteq B$ be subsets and let $f: A \to B$ be a function.

(1) Prove that $X \subseteq f^{-1}(f(X))$.

(2) Prove that $f(f^{-1}(Y)) \subseteq Y$.

(3) Prove that $X = f^{-1}(f(X))$ if and only if $X = f^{-1}(Z)$ for some $Z \subseteq B$.

(4) Prove that $Y = f(f^{-1}(Y))$ if and only if $Y = f(W)$ for some $W \subseteq A$.

(5) Prove that $f(f^{-1}(f(X))) = f(X)$.

(6) Prove that $f^{-1}(f(f^{-1}(Y))) = f^{-1}(Y)$.

Exercise 4.2.14. Let A and B be sets, and let $f, g: A \to B$ be functions. Think of these functions as inducing functions $f_*, g_*: \mathcal{P}(A) \to \mathcal{P}(B)$, and functions $f^*, g^*: \mathcal{P}(B) \to \mathcal{P}(A)$. Prove that $f_* = g_*$ if and only if $f^* = g^*$ if and only if $f = g$.

Exercise 4.2.15. [Used in Exercise 6.5.15.] Let A be a non-empty set, and let $g: \mathcal{P}(A) \to \mathcal{P}(A)$ be a function. The function g is **monotone** if $X \subseteq Y$ implies $g(X) \subseteq g(Y)$ for all $X, Y \in \mathcal{P}(A)$.

Suppose that g is monotone.

(1) Let $\mathcal{D}$ be a family of subsets of A. Prove that $g\left(\bigcap_{X \in \mathcal{D}} X\right) \subseteq \bigcap_{X \in \mathcal{D}} g(X)$. It is not sufficient simply to cite Theorem 4.2.4 (7), because it is not necessarily the case that $g = f_*$ for some function $f: A \to A$.

(2) Prove that there is some $T \in \mathcal{P}(A)$ such that $g(T) = T$. Such an element T is called a **fixed point** of g. Use Part (1) of this exercise.

4.3 Composition and Inverse Functions

Functions can be combined to form new functions in a variety of ways. One simple way of combining functions that is seen in courses such as calculus is to add or multiply functions $\mathbb{R} \to \mathbb{R}$. Though very useful, this method of combining functions is not applicable to all sets, because the ability to add or multiply functions $\mathbb{R} \to \mathbb{R}$ relies upon the addition or multiplication of the real numbers, and not all sets have such operations. A more broadly applicable way of combining functions, also encountered in calculus, is seen when the Chain Rule for taking derivatives is used. This rule is used with functions such as $f \colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sqrt{x^2 + 3}$ for all $x \in \mathbb{R}$, which are built up out of a function "inside" a function. The following definition formalizes this notion.

Definition 4.3.1. Let A, B and C be sets, and let $f \colon A \to B$ and $g \colon B \to C$ be functions. The **composition** of f and g is the function $g \circ f \colon A \to C$ defined by

$$(g \circ f)(x) = g(f(x))$$

for all $x \in A$. △

Observe that the notation "$g \circ f$" in Definition 4.3.1 is the name of a single function $A \to C$, which we constructed out of the two functions f and g. By contrast, the notation "$(g \circ f)(x)$" denotes a single value in the set C. It would not be correct to write "$g \circ f(x)$," because $\circ$ is an operation that combines two functions, whereas "$f(x)$" is not a function but a single element in the set B. Observe also that for the composition of two functions to be defined, the codomain of the first function must equal the domain of the second function.

The reader who is encountering the notation $g \circ f$ for the first time might find it necessary to get used to the fact that it is "backwards" from what might be expected, because $g \circ f$ means doing f first and then g even though we generally read from left to right in English. Think of "$\circ$" as meaning "following." We will stick with the "$\circ$" notation in spite of any slight confusion it might cause at first, because it is extremely widespread, and because the reader will find that it works well once she is used to it.

Example 4.3.2.

(1) Let P be the set of all people, and let $m \colon P \to P$ be the function that assigns to each person her mother. Then $m \circ m$ is the function that assigns to each person her maternal grandmother.

(2) Let $f, g \colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$ and $g(x) = x + 3$ for all $x \in \mathbb{R}$. Then both $f \circ g$ and $g \circ f$ are defined, and $(f \circ g)(x) = (x+3)^2$ for all $x \in \mathbb{R}$, and $(g \circ f)(x) = x^2 + 3$ for all $x \in \mathbb{R}$.

(3) Let $k \colon \mathbb{R} \to \mathbb{R}$ be defined by $k(x) = \sin x$ for all $x \in \mathbb{R}$, and let $h \colon (0, \infty) \to \mathbb{R}$ be defined by $h(x) = \ln x$ for all $x \in (0, \infty)$. Then $k \circ h$ is defined, and is given by $(k \circ h)(x) = \sin(\ln x)$ for all $x \in (0, \infty)$. On the other hand, we cannot form the composition $h \circ k$, because the domain of h is not the same as the codomain of k, reflecting the observation that $\ln(\sin x)$ is not defined for all $x \in \mathbb{R}$. ◊

One way to visualize the composition of functions is to use "commutative diagrams." If $f: A \rightarrow B$ and $g: B \rightarrow C$ are functions, then we can form $g \circ f: A \rightarrow C$, and we can represent all three of these functions in the following diagram.

$$
\begin{array}{ccc}
A & & \\
\downarrow{\scriptstyle f} & \searrow{\scriptstyle g \circ f} & \\
B & \xrightarrow[\;\;g\;\;]{} & C
\end{array}
$$
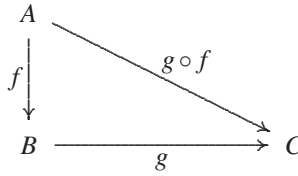
This diagram is referred to as a commutative diagram, which means that if we start with any element $x \in A$, and trace what happens to it going along either of the two possible paths from A to C, we end up with the same result. If we go first down and then across, the result is $g(f(x))$, and if we go diagonally, the result is $(g \circ f)(x)$. Commutative diagrams (often much more complicated than the one seen above) are important in some branches of mathematics, for example algebraic topology.

An example of the use of the composition of functions is coordinate functions. In multivariable calculus it is standard to write functions into $\mathbb{R}^n$ in terms of coordinate functions, and we can now generalize this notion to arbitrary sets.

Definition 4.3.3. Let B be a set, let $A_1,\ldots,A_n$ be sets for some $n \in \mathbb{N}$ and let $f: B \rightarrow A_1 \times \cdots \times A_n$ be a function. For each $i \in \{1,\ldots,n\}$, the i-th **coordinate function** of f, denoted f_i, is the function $f_i: B \rightarrow A_i$ defined by $f_i = \pi_i \circ f$, where $\pi_i: A_1 \times \cdots \times A_n \rightarrow A_i$ is the projection map. △

The fact that $f_i = \pi_i \circ f$ for all $i \in \{1,\ldots,n\}$, as given in Definition 4.3.3, means that $f(x) = (f_1(x),\ldots,f_n(x))$ for all $x \in B$. In some texts this fact is abbreviated by writing $f = (f_1,\ldots,f_n)$, or alternatively by writing $f = f_1 \times \cdots \times f_n$. However, although the notations $(f_1,\ldots,f_n)$ and $f_1 \times \cdots \times f_n$ could be formally defined to be the function we have denoted f, the reader is urged to use these two notations with caution, or to avoid them at all, for the following reason. Whereas writing $f(x) = (f_1(x),\ldots,f_n(x))$ is perfectly sensible, the two sides of the equation being different expressions for the same element of $A_1 \times \cdots \times A_n$, using the notation $f = (f_1,\ldots,f_n)$ might mistakenly suggest that the function f is an element of the product of n sets, which is not necessarily true, and using the notation $f = f_1 \times \cdots \times f_n$ might mistakenly suggest that f is the product of n sets, which is also not necessarily true.

Coordinate functions when $n = 2$ can be represented by the following commutative diagram. Each triangle of functions in the diagram is commutative in the sense described previously.

$$
\begin{array}{ccc}
& B & \\
\swarrow{\scriptstyle f_1} \quad & \downarrow{\scriptstyle f} & \quad \searrow{\scriptstyle f_2} \\
A_1 \xleftarrow[\;\pi_1\;]{} & A_1 \times A_2 & \xrightarrow[\;\pi_2\;]{} A_2
\end{array}
$$
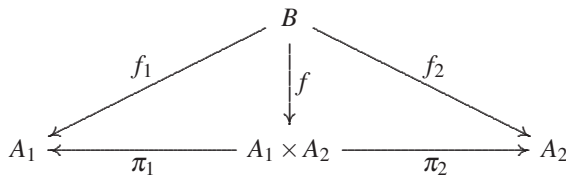
Example 4.3.4. Let $f\colon \mathbb{R}^2 \to \mathbb{R}^3$ be defined by

$$f((x,y)) = (xy, \sin x^2, x+y^3)$$

for all $(x,y) \in \mathbb{R}^2$. The three coordinate functions of f are $f_1, f_2, f_3 \colon \mathbb{R}^2 \to \mathbb{R}$ defined by

$$f_1((x,y)) = xy, \quad f_2((x,y)) = \sin x^2, \quad \text{and} \quad f_3((x,y)) = x+y^3$$

for all $(x,y) \in \mathbb{R}^2$.   ◇

Which of the familiar properties of operations (for example commutativity and associativity) hold for the composition of functions? The Commutative Law, which for the real numbers and addition states that $a+b = b+a$ for all $a,b \in \mathbb{R}$, does not hold for functions and composition, for two reasons. First, suppose that we have functions $f\colon A \to B$ and $g\colon B \to C$, so that we can form $g \circ f$. Unless it happens to be the case that $A = C$, then we could not even form $f \circ g$, and so commutativity is not relevant. Even in situations where we can form composition both ways, however, the Commutative Law does not always hold, as seen in Example 4.3.2 (2). The following lemma shows, however, that some nice properties do hold for composition.

Lemma 4.3.5. *Let A, B, C and D be sets, and let $f\colon A \to B$ and $g\colon B \to C$ and $h\colon C \to D$ be functions.*

1. $(h \circ g) \circ f = h \circ (g \circ f)$ *(Associative Law).*
2. $f \circ 1_A = f$ *and* $1_B \circ f = f$ *(Identity Law).*

Proof.

(1). It is seen from the definition of composition that both $(h \circ g) \circ f$ and $h \circ (g \circ f)$ have the same domain, the set A, and the same codomain, the set D. If $a \in A$, then

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$
$$= h((g \circ f)(a)) = (h \circ (g \circ f))(a).$$

Hence $(h \circ g) \circ f = h \circ (g \circ f)$.

(2). This part is straightforward, and is left to the reader.   □

Do functions have inverses under composition? That is, for any given function is there another that "cancels it out" by composition? In arithmetic, for example, we can cancel out the number 3 by adding -3 to it, which yields 0. For functions, the operation addition and the number 0 are replaced with composition of functions and the identity map, respectively. However, the non-commutativity of composition means that we need a bit more care when we define "canceling out" for functions than we do with addition (which is commutative).

Definition 4.3.6. Let A and B be sets, and let $f\colon A \to B$ and $g\colon B \to A$ be functions.

1. The function g is a **right inverse** for f if $f \circ g = 1_B$.
2. The function g is a **left inverse** for f if $g \circ f = 1_A$.

3. The function g is an **inverse** for f if it is both a right inverse and a left inverse. △

Definition 4.3.6 (1) (2) was stated in the most concise possible way using only the names of the functions involved. In practice, however, it is often convenient to use the fact that $f \circ g = 1_B$ means $f(g(x)) = x$ for all $x \in B$, and that $g \circ f = 1_A$ means $g(f(x)) = x$ for all $x \in A$. Also, although we used the term "an inverse" in Definition 4.3.6 (3), it is seen in Part (1) of the following result that we could actually have written "the inverse."

Lemma 4.3.7. *Let A and B be sets, and let $f : A \to B$ be a function.*

1. *If f has an inverse, then the inverse is unique.*
2. *If f has a right inverse g and a left inverse h, then $g = h$, and hence f has an inverse.*
3. *If g is an inverse of f, then f is an inverse of g.*

Proof.

(1). Suppose that $g, h : B \to A$ are both inverses of f. We will show that $g = h$. By hypothesis on g and h we know, among other things, that $f \circ g = 1_B$ and $h \circ f = 1_A$. Using Lemma 4.3.5 repeatedly we then have

$$g = 1_A \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ 1_B = h.$$

(2). The proof is the same as in Part (1).

(3). Suppose that $g : B \to A$ is an inverse of f. Then $g \circ f = 1_A$ and $f \circ g = 1_B$. By the definition of inverses, it follows that f is an inverse of g. □

Observe that the proof of Lemma 4.3.7 (1) is virtually identical to the proof of the uniqueness part of Theorem 2.5.2. The same proof in a more generalized setting is also used for Lemma 7.2.4. Lemma 4.3.7 (1) allows us to make the following definition.

Definition 4.3.8. Let A and B be sets, and let $f : A \to B$ be a function. If f has an inverse, the inverse is denoted $f^{-1} : B \to A$. △

It is important to keep in mind the great difference in meaning between the notation "$f^{-1}(Q)$" discussed in Section 4.2 and the notation "f^{-1}" given in Definition 4.3.8. The notation $f^{-1}(Q)$ denotes a set, not a function, and it exists even if the function f^{-1} does not exist. In particular, the use of the notation $f^{-1}(Q)$ should not be taken as implying that f has an inverse.

Moreover, suppose that the inverse function f^{-1} does exist. Then the notation $f^{-1}(Q)$ has two meanings, which are the inverse image of Q under f and the image of Q under f^{-1}. The former of these meanings is the set $\{a \in A \mid f(a) \in Q\}$, and the latter of these meanings is the set $\{a \in A \mid a = f^{-1}(q) \text{ for some } q \in Q\}$. Fortunately, as the reader can verify, these two sets are equal, and so there is no ambiguity in the meaning of the notation $f^{-1}(Q)$ in those cases when f^{-1} exists.

We note that if $f\colon A \to B$ has an inverse $f^{-1}\colon B \to A$, then $f^{-1}(f(x)) = x$ for all $x \in A$ and $f(f^{-1}(x)) = x$ for all $x \in B$. Another way of stating the relation between f and f^{-1} is to say that $y = f^{-1}(x)$ if and only if $x = f(y)$ for all $y \in A$ and $x \in B$. This latter formulation will not be particularly useful to us in the construction of rigorous proofs, but we mention it because the reader has likely encountered it in precalculus and calculus courses, for example where the natural logarithm function ln is defined by saying that $y = \ln x$ if and only if $x = e^y$. Moreover, we observe that to say $y = f^{-1}(x)$ if and only if $x = f(y)$ for all $y \in A$ and $x \in B$ means that f^{-1} is obtained from f by interchanging the roles of x and y, a fact that has a very important application if we look at the particular case where $A, B \subseteq \mathbb{R}$. In that case, the graph of f^{-1} can be obtained from the graph of f by reflecting the x-y plane in the line $y = x$, which precisely has the effect of interchanging the roles of x and y. See Figure 4.3.1 for an example of such graphs.

Fig. 4.3.1.
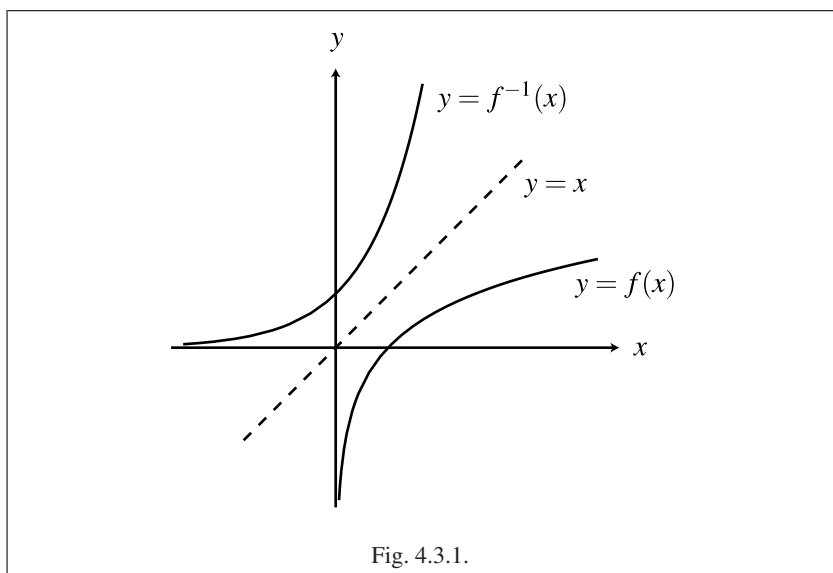
As seen in the following example, some functions have neither right nor left inverse, some have only one but not the other, and some have both. Moreover, if a function has only a right inverse or a left inverse but not both, the right inverse or left inverse need not be unique.

Example 4.3.9.

(1) Let $k\colon (0,1) \to (3,5)$ be defined by $k(x) = 2x + 3$ for all $x \in (0,1)$. We claim that k has an inverse, the function $j\colon (3,5) \to (0,1)$ defined by $j(x) = \frac{x-3}{2}$ for all $x \in (3,5)$. We compute $j(k(x)) = \frac{(2x+3)-3}{2} = x$ for all $x \in (0,1)$, and hence $j \circ k = 1_{(0,1)}$. Similarly, we compute $k(j(x)) = 2 \cdot \frac{x-3}{2} + 3 = x$ for all $x \in (3,5)$, and hence

$k \circ j = 1_{(3,5)}$. Therefore j is both a right inverse and a left inverse for k, and hence it is an inverse for k. We conclude that $j = k^{-1}$.

(2) Let $f \colon \mathbb{R} \to [0, \infty)$ be defined by $f(x) = x^2$ for all $x \in \mathbb{R}$. This function has no left inverse, but many right inverses, of which we will see two. Let $g, h \colon [0, \infty) \to \mathbb{R}$ be defined by $g(x) = \sqrt{x}$ and $h(x) = -\sqrt{x}$ for all $x \in [0, \infty)$. Both g and h are right inverses for f, because $(f \circ g)(x) = f(g(x)) = (\sqrt{x})^2 = x$ for all $x \in [0, \infty)$, and $(f \circ h)(x) = f(h(x)) = (-\sqrt{x})^2 = x$ for all $x \in [0, \infty)$. To see that f has no left inverse, suppose to the contrary that f has a left inverse $m \colon [0, \infty) \to \mathbb{R}$. How should we define $m(9)$? Because m is a left inverse for f, we know that $m \circ f = 1_{\mathbb{R}}$. Hence $m(f(x)) = x$ for all $x \in \mathbb{R}$. We would then need to have $m(9) = m(3^2) = (m \circ f)(3) = 3$, but we would also need to have $m(9) = m((-3)^2) = (m \circ f)(-3) = -3$. Therefore there is no possible way to define $m(9)$, and hence m does not exist. It follows that f has no left inverse. (Observe that we could have used any other positive number instead of 9.)

(3) Let $p \colon [0, \infty) \to \mathbb{R}$ be defined by $p(x) = x^2$ for all $x \in [0, \infty)$. Then p has no right inverse, but many left inverses, of which we will see two. Let $q, r \colon \mathbb{R} \to [0, \infty)$ be defined by

$$q(x) = \begin{cases} \sqrt{x}, & \text{if } x \geq 0 \\ 1, & \text{if } x < 0, \end{cases} \qquad r(x) = \begin{cases} \sqrt{x}, & \text{if } x \geq 0 \\ \sin x, & \text{if } x < 0. \end{cases}$$

Both q and r are left inverses for p, because $(q \circ p)(x) = q(p(x)) = \sqrt{x^2} = x$ for all $x \in [0, \infty)$, and $(r \circ p)(x) = r(p(x)) = \sqrt{x^2} = x$ for all $x \in [0, \infty)$. To see that p has no right inverse, suppose to the contrary that p has a right inverse $u \colon \mathbb{R} \to [0, \infty)$. How should we define $u(-4)$? Because u is a right inverse for p, we know that $p \circ u = 1_{\mathbb{R}}$. Hence $p(u(x)) = x$ for all $x \in \mathbb{R}$. Therefore $(u(x))^2 = x$ for all $x \in \mathbb{R}$. Hence we would need to have $(u(-4))^2 = -4$, which is impossible, because $u(-4)$ is a real number, and no real number squared is negative. Therefore there is no possible way to define $u(-4)$, and hence u does not exist. It follows that p has no right inverse.

(4) Let $s \colon \mathbb{R} \to \mathbb{R}$ be defined by $s(x) = x^2$ for all $x \in \mathbb{R}$. The function s has no left inverse by from the same argument used to show that the function f in Part (2) of this example had no left inverse, and s has no right inverse by the same argument used to show that the function p in Part (3) of this example had no right inverse.   ◇

<div align="center">

───
| **Exercises** |
───

</div>

Exercise 4.3.1. For each pair of functions f and g given below, find formulas for $f \circ g$ and $g \circ f$ (simplifying when possible).

(1) Let $f \colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = e^x$ for all $x \in \mathbb{R}$, and let $g \colon \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = \sin x$ for all $x \in \mathbb{R}$.

(2) Let $f \colon (0, \infty) \to (0, \infty)$ be defined by $f(x) = x^7$ for all $x \in \mathbb{R}$, and let $g \colon (0, \infty) \to (0, \infty)$ be defined by $g(x) = x^{-3}$ for all $x \in (0, \infty)$.

(3) Let $f \colon \mathbb{R} \to [0, \infty)$ be defined by $f(x) = x^6$ for all $x \in \mathbb{R}$, and let $g \colon [0, \infty) \to \mathbb{R}$ be defined by $g(x) = \sqrt[6]{x}$ for all $x \in [0, \infty)$.

(4) Let $f: \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = \lfloor x \rfloor$ for all $x \in \mathbb{R}$, and let $g: \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = \lceil x \rceil$ for all $x \in \mathbb{R}$, where $\lfloor x \rfloor$ and $\lceil x \rceil$ are respectively the greatest integer less than or equal to x and the least integer greater than or equal to x.

Exercise 4.3.2. For each of the following functions $f: \mathbb{R} \to \mathbb{R}$, find functions $g, h: \mathbb{R} \to \mathbb{R}$, neither of which is the identity map, such that $f = h \circ g$.

(1) $f(x) = \sqrt[3]{x + 7}$ for all $x \in \mathbb{R}$.
(2) $f(x) = \sqrt[3]{x} + 7$ for all $x \in \mathbb{R}$.
(3) $f(x) = \begin{cases} x^6, & \text{if } 0 \le x \\ x^4, & \text{if } x < 0. \end{cases}$
(4) $f(x) = \begin{cases} x^3, & \text{if } 0 \le x \\ x, & \text{if } x < 0. \end{cases}$

Exercise 4.3.3. Let $f, g: \mathbb{R} \to \mathbb{R}$ be defined by

$$f(x) = \begin{cases} 1 - 2x, & \text{if } x \ge 0 \\ |x|, & \text{if } x < 0, \end{cases} \qquad g(x) = \begin{cases} 3x, & \text{if } x \ge 0 \\ x - 1, & \text{if } x < 0. \end{cases}$$

Find $f \circ g$ and $g \circ f$.

Exercise 4.3.4.

(1) Find two functions $h, k: \mathbb{R} \to \mathbb{R}$ such that neither h nor k is a constant map, but $k \circ h$ is a constant map.
(2) Find two functions $s, t: \mathbb{R} \to \mathbb{R}$ such that $s \ne 1_{\mathbb{R}}$ and $t \ne 1_{\mathbb{R}}$, but $t \circ s = 1_{\mathbb{R}}$.

Exercise 4.3.5. [Used in Theorem 6.3.11 and Theorem 6.6.5.] Let A and B be sets, let $U \subseteq A$ and $V \subseteq C$ be subsets, and let $f: A \to B$ and $g: B \to C$ be functions. Prove that

$$(g \circ f)(U) = g(f(U)) \quad \text{and} \quad (g \circ f)^{-1}(V) = f^{-1}(g^{-1}(V)).$$

Exercise 4.3.6. Let A, B and C be sets, and let $f: A \to B$ and $g: B \to C$ be functions. Suppose that f and g have inverses. Prove that $g \circ f$ has an inverse, and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Exercise 4.3.7. Find two right inverses for each of the following functions.

(1) Let $h: \mathbb{R} \to [0, \infty)$ be defined by $h(x) = |x|$ for all $x \in \mathbb{R}$.
(2) Let $k: \mathbb{R} \to [1, \infty)$ be defined by $k(x) = e^{x^2}$ for all $x \in \mathbb{R}$.

Exercise 4.3.8. Find two left inverses for each of the following functions.

(1) Let $f: [0, \infty) \to \mathbb{R}$ be defined by $f(x) = x^3 + 4$ for all $x \in [0, \infty)$.
(2) Let $g: \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = e^x$ for all $x \in \mathbb{R}$.

Exercise 4.3.9. Let $h, k \colon \mathbb{R} \to \mathbb{R}$ be defined by

$$h(x) = \begin{cases} 4x + 1, & \text{if } x \geq 0 \\ x, & \text{if } x < 0, \end{cases} \qquad k(x) = \begin{cases} 3x, & \text{if } x \geq 0 \\ x + 3, & \text{if } x < 0. \end{cases}$$

Find an inverse for $k \circ h$.

Exercise 4.3.10. Let A and B be sets, and let $f \colon A \to B$ be a function. Prove that if f has two distinct left inverses then it has no right inverse, and that if f has two distinct right inverses then it has no left inverse.

Exercise 4.3.11. Let B be a set, let $A_1, \ldots, A_k$ be sets for some $k \in \mathbb{N}$, let $U_i \subseteq A_i$ be a subset for all $i \in \{1, \ldots, k\}$ and let $f \colon B \to A_1 \times \cdots \times A_k$ be a function. Prove that

$$f^{-1}(U_1 \times \cdots \times U_k) = \bigcap_{i=1}^{k} (f_i)^{-1}(U_i),$$

where the f_i are the coordinate functions of f.

Exercise 4.3.12. Let B be a set, let $A_1, \ldots, A_k$ be sets for some $k \in \mathbb{N}$ and let $h_i \colon B \to A_i$ be a function for each $i \in \{1, \ldots, k\}$. Prove that there is a unique function $g \colon B \to A_1 \times \cdots \times A_k$ such that $\pi_i \circ g = h_i$ for all $i \in \{1, \ldots, k\}$, where $\pi_i \colon A_1 \times \cdots \times A_k \to A_i$ is the projection map. This exercise can be represented by the following commutative diagram.

Exercise 4.3.13. This exercise and the next give examples of definitions of functions by universal property. Rather than defining what a certain function is, we state how it should behave, and then prove that there exists a function satisfying the given behavior. Such constructions are important in category theory, a branch of mathematics that provides a useful (though abstract) language for many familiar mathematical ideas, and has applications to various aspects of mathematics, logic and computer science. See [AM75] or [Kri81] for an introduction to category theory, and [Pie91] for some uses of category theory in computer science.

Let A and B be sets, and let $f, g \colon A \to B$ be functions. Prove that there exist a set E and a function $e \colon E \to A$ such that $f \circ e = g \circ e$, and that for any set C and function $h \colon C \to A$ such that $f \circ h = g \circ h$, there is a unique function $t \colon C \to E$ such that $h = e \circ t$. This last condition is represented by the following commutative diagram. The function e is called an **equalizer** of f and g. To define E, consider subsets of A.
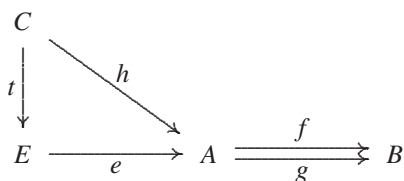
Exercise 4.3.14. This exercise is similar to Exercise 4.3.13. Let A, B and C be sets, and let $f\colon A \to C$ and $g\colon B \to C$ be functions. Prove that there exist a set P and functions $h\colon P \to A$ and $k\colon P \to B$ such that $f \circ h = g \circ k$, and that for any set X and functions $s\colon X \to A$ and $t\colon X \to B$ such that $f \circ s = g \circ t$, there is a unique function $u\colon X \to P$ such that $s = h \circ u$ and $t = k \circ u$. This last condition is represented by the following commutative diagram. The set P together with the functions h and k are called a **pullback** of f and g. To define P, consider subsets of $A \times B$.
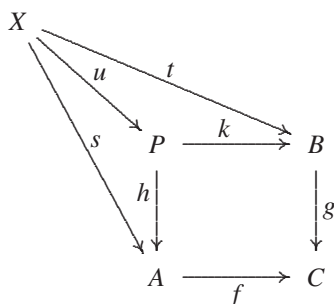
4.4 Injectivity, Surjectivity and Bijectivity

As we saw in Example 4.3.9, there exist functions with neither right inverse nor left inverse; others with a right inverse but not a left inverse; others with a left inverse but not a right inverse; and yet others with both a right and a left inverse, and hence with an inverse by Lemma 4.3.7 (2). Unfortunately, it is not always easy to verify whether a function has a right inverse, left inverse or both directly from the definition, because such verification entails finding a suitable candidate for the appropriate type of inverse, and doing so for any but the simplest functions is often quite difficult, and at times virtually impossible. Given the importance of inverse functions in many parts of mathematics, it would be very nice if there were some convenient criteria by which to check whether a function in principle has a right inverse, left inverse or both without having to produce the desired function. Remarkably, there are such criteria, as seen in Theorem 4.4.5 below.

To understand the criteria for the existence of right inverses and left inverses, we start with an example.

Example 4.4.1. Let P be the set of all people, and let $m\colon P \to P$ be the function that assigns to each person her mother. Does this function have a right inverse or a left inverse? Suppose first that $g\colon P \to P$ is a right inverse for m. That would mean that

$m \circ g = 1_P$, and therefore $m(g(x)) = x$ for every $x \in P$. Let $y \in P$, and suppose that y is a man. Then $m(g(y)) = y$, which would mean that y is the mother of $g(y)$, and that is not possible, because y cannot be anyone's mother. Therefore m has no right inverse. Observe that the obstacle to finding a right inverse for m is that there are objects in the codomain (namely, all men and some women) who are not in the range of m (which is the set of mothers).

Now suppose that $h \colon P \to P$ is a left inverse for m. That would mean that $h \circ m = 1_P$, and therefore $h(m(x)) = x$ for every person x. Here we will encounter a different problem than with the proposed right inverse. Let $a, b \in P$, and suppose that a and b are siblings. Then $m(a) = m(b)$, and hence $h(m(a)) = h(m(b))$. Because $h(m(x)) = x$ for every $x \in P$, we deduce that $a = b$, which is a contradiction. Hence m has no left inverse. The obstacle to finding a left inverse for f is that there are two different objects in the domain (namely, a pair of siblings) that are mapped to the same element of the codomain (namely, their mother). ◇

It turns out that the two problems identified in Example 4.4.1 are the only obstacles to finding right inverses and left inverses, respectively. We now give names to functions that do not have these problems.

Definition 4.4.2. Let A and B be sets, and let $f \colon A \to B$ be a function.

1. The function f is **injective** (also called **one-to-one** or **monic**) if $x \neq y$ implies $f(x) \neq f(y)$ for all $x, y \in A$; equivalently, if $f(x) = f(y)$ implies $x = y$ for all $x, y \in A$.
2. The function f is **surjective** (also called **onto** or **epic**) if for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$; equivalently, if $f(A) = B$.
3. The function f is **bijective** if it is both injective and surjective.   △

Observe that a function is surjective if and only if its range equals its codomain.

There exist functions that are both injective and surjective, that are surjective but not injective, that are injective but not surjective and that are neither injective nor surjective. Examples of such functions are seen graphically in Figure 4.4.1, and via formulas in the following example respectively.

Fig. 4.4.1.
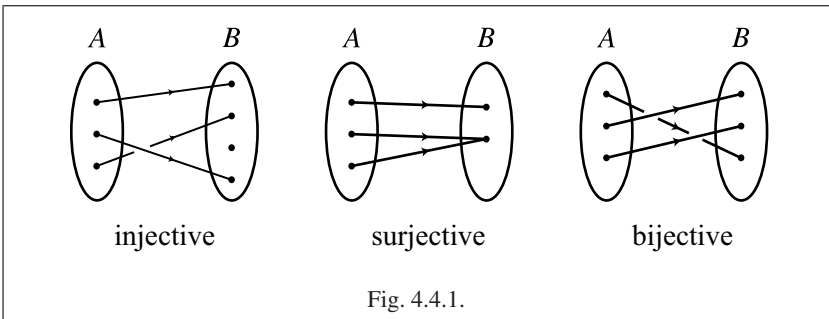
Example 4.4.3.

(1) Let $k\colon [0,\infty) \to [0,\infty)$ be defined by $k(x) = x^2$ for all $x \in [0,\infty)$. This function is surjective and injective, and hence bijective. First, we show that k is injective. Let $x,y \in [0,\infty)$. Suppose that $k(x) = k(y)$. Then $x^2 = y^2$. It follows that $\sqrt{x^2} = \sqrt{y^2}$, and because $x \geq 0$ and $y \geq 0$, we deduce that $x = \sqrt{x^2} = \sqrt{y^2} = y$. Hence k is injective. Second, we show that k is surjective. Let $b \in [0,\infty)$. Then $\sqrt{b} \in [0,\infty)$, and so $k(\sqrt{b}) = (\sqrt{b})^2 = b$. Hence k is surjective.

(2) Let $g\colon [0,\infty) \to \mathbb{R}$ be defined by $g(x) = x^2$ for all $x \in [0,\infty)$. This function is injective but not surjective. The proof of the injectivity of g is the same as the proof of the injectivity of the function k in Part (1) of this example. The reason that g is not surjective is that $g(a) \neq -2$ for any $a \in [0,\infty)$, though -2 is in the codomain of g.

(3) Let $h\colon \mathbb{R} \to [0,\infty)$ be defined by $h(x) = x^2$ for all $x \in \mathbb{R}$. This function is surjective but not injective. The proof of the surjectivity of h is the same as the proof of the surjectivity of the function k in Part (1) of this example. The reason h is not injective is because $h(-3) = 9 = h(3)$ even though $-3 \neq 3$. (Observe that instead of ± 3 we could have used $\pm a$ for any positive number a, but a single instance where the definition of injectivity fails is sufficient.)

(4) Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$ for all $x \in \mathbb{R}$. This function is neither injective nor surjective, which is seen using the same arguments as the corresponding arguments for g and h in Parts (2) and (3) of this example.   ◊

Observe from Example 4.4.3 that injectivity and surjectivity very much depend upon the choice of domain and codomain of a function. That is one of the reasons why we need to specify the domain and codomain when we define a function.

In many texts, especially at the elementary level, the terms "one-to-one" and "onto" are used instead of "injective" and "surjective," respectively, and the reader should therefore be familiar with the former terms, though the author finds the latter terms (also widely used) to be preferable. The term "one-to-one" is awkward, and the word "onto" is a preposition (in contrast to the adjective "one-to-one"), and as such is not grammatically parallel to "one-to-one." By contrast, the two adjectives "injective" and "surjective" are grammatically parallel, reflecting the parallel roles of these two concepts, as the reader will soon see. Moreover, some texts use the word "onto" as if it were an adjective, leading to grammatically problematic phrases such as "the function f is a one-to-one and onto function." Other texts are careful to use "onto" as a preposition, leading to awkward (though correct) phrases such as "the function f is a one-to-one function from A onto B," which again make the two concepts seem not parallel. (If the reader really prefers to use prepositions rather than adjectives to describe functions, the author's proposed scheme would be that an arbitrary function $f\colon A \to B$ is described as a function from A *to* B; an injective function is described as a function from A *into* B; a surjective function is described as a function from A *onto* B; and a bijective function is described as a function from A *unto* B. The author would not necessarily recommend the use of this scheme, but it is grammatically consistent.)

One way of thinking about injectivity, surjectivity and bijectivity is as follows. Let $f: A \to B$ be a function. The function f is injective if and only if for each $b \in B$, there is at most one element in the inverse image $f^{-1}(\{b\})$; the function f is surjective if and only if for each $b \in B$, there is at least one element in the inverse image $f^{-1}(\{b\})$; the function f is bijective if and only if for each $b \in B$, there is precisely one element in the inverse image $f^{-1}(\{b\})$. Consider now the special case of a function $f: \mathbb{R} \to \mathbb{R}$. Then the function f is injective if and only if each horizontal line in the plane intersects its graph at most once; see Figure 4.4.2 (i). The function f is surjective if and only if each horizontal line intersects its graph at least once; see Figure 4.4.2 (ii). The function f is bijective if and only if each horizontal line intersects its graph once and only once.

Fig. 4.4.2.
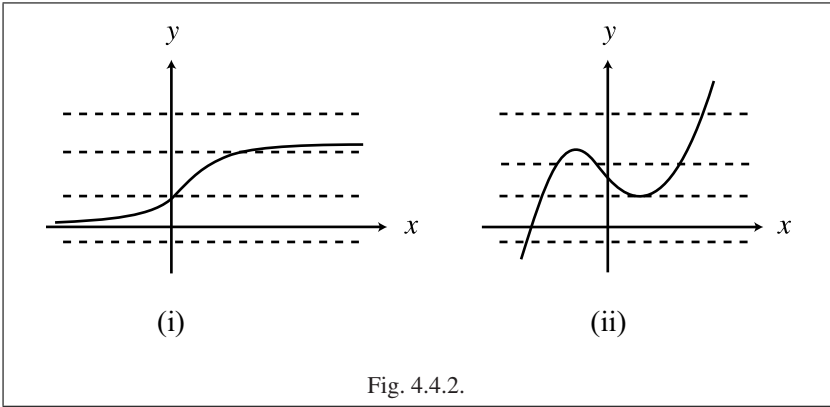
There are standard strategies for proving that a function is each of injective and surjective. Let $f: A \to B$ be a function. If we wish to prove that f is injective, then we need to show that $f(x) = f(y)$ implies $x = y$ for all $x, y \in A$. As usual, if we need to show that something is true for all $x, y \in A$, we will choose arbitrary x and y, and then prove the desired property for this choice. Hence, a proof of the injectivity of f typically has the following form.

Proof. Let $x, y \in A$. Suppose that $f(x) = f(y)$.

$\vdots$

(argumentation)

$\vdots$

Then $x = y$. Hence f is injective. ☐

If we wish to prove that f is surjective, we need to show that for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$. A proof of the surjectivity of f would therefore have the following form.

Proof. Let $b \in B$.

$$\vdots$$

Let $a = \dots$

$$\vdots$$

(argumentation)

$$\vdots$$

Then $b = f(a)$. Hence f is surjective. $\square$

We will use the above strategies repeatedly, starting with the proof of the following lemma, which shows that composition of functions behaves nicely with respect to injectivity, surjectivity and bijectivity.

Lemma 4.4.4. *Let A, B and C be sets, and let $f : A \to B$ and $g : B \to C$ be functions.*

1. *If f and g are injective, then $g \circ f$ is injective.*
2. *If f and g are surjective, then $g \circ f$ is surjective.*
3. *If f and g are bijective, then $g \circ f$ is bijective.*

Proof.

(1). Suppose that f and g are injective. We wish to show that $g \circ f : A \to C$ is injective. Let $x, y \in A$. We will show that $(g \circ f)(x) = (g \circ f)(y)$ implies $x = y$. Suppose that $(g \circ f)(x) = (g \circ f)(y)$. Then $g(f(x)) = g(f(y))$. Because g is injective, we deduce that $f(x) = f(y)$. Because f is injective, we deduce that $x = y$.

(2). Suppose that f and g are surjective. We wish to show that $g \circ f : A \to C$ is surjective. Let $c \in C$. We will show that there exists some element $a \in A$ such that $(g \circ f)(a) = p$. Because $c \in C$ and g is surjective, there is some $b \in B$ such that $g(b) = c$. Because f is surjective, we know that there is some $a \in A$ such that $f(a) = b$. It follows that $(g \circ f)(a) = g(f(a)) = g(b) = c$.

(3). This part is derived easily from Parts (1) and (2) of this lemma. $\square$

As seen in Exercise 4.4.14, the converse to each of the parts of Lemma 4.4.4 is not true, though a partial result does hold.

The following theorem, which is extremely useful throughout mathematics (and is perhaps the author's favorite theorem in this text), answers the question posed at the start of this section concerning criteria for the existence of inverse functions.

Theorem 4.4.5. *Let A and B be non-empty sets, and let $f : A \to B$ be a function.*

1. *The function f has a right inverse if and only if f is surjective.*
2. *The function f has a left inverse if and only if f is injective.*
3. *The function f has an inverse if and only if f is bijective.*

Proof.

(1). Suppose that f has a right inverse g. Then $f \circ g = 1_B$. We wish to show that f is surjective. Let $b \in B$. We need to find an element $a \in A$ such that $f(a) = b$. Let $a = g(b)$. Then $f(g(b)) = (f \circ g)(b) = 1_B(b) = b$.

Now suppose that f is surjective. We wish to show that f has a right inverse, which means that we need to find a function $h \colon B \to A$ such that $f \circ h = 1_B$. We define h as follows. For each $b \in B$, the surjectivity of f implies that there is at least one element $a \in A$ such that $f(a) = b$; let $h(b) = a$ for some choice of such a (it doesn't matter which one). It is now true by definition that $f(h(b)) = b$ for all $b \in B$. Hence $f \circ h = 1_B$.

(2). Left to the reader in Exercise 4.4.9.

(3). This part follows from Parts (1) and (2) of this theorem, together with Lemma 4.3.7 (2). □

The alert reader will have noticed that in the proof of Part (1) of Theorem 4.4.5, we had to choose, simultaneously, one element $a \in A$ such that $f(a) = b$, for each $b \in B$. That is, we implicitly made use of the Axiom of Choice which was discussed in Section 3.5, and reformulated in terms of function in Section 4.1. As is common, for the sake of brevity and in order to avoid distraction from the essential idea of the proof of Theorem 4.4.5, we did not explicitly make use of the Axiom of Choice in that proof, though it would certainly have been possible to have done so. For example, we could have written: "We define h as follows. The surjectivity of f implies that the set $f^{-1}(\{b\})$ is non-empty for each $b \in B$. Then $\left\{ f^{-1}(\{b\}) \right\}_{b \in B}$ is a family of non-empty sets. By the Axiom of Choice (Theorem 4.1.5) there is a function $h \colon B \to \bigcup_{b \in B} f^{-1}(\{b\})$ such that $h(b) \in f^{-1}(\{b\})$ for all $b \in B$. It is now true by definition that $f(h(b)) = b$ for all $b \in B$. Hence $f \circ h = 1_B$." The reader might wonder whether it would have been possible to prove Theorem 4.4.5 (1) without the Axiom of Choice or something equivalent, but it turns out that that would not have been possible, because Theorem 4.4.5 (1) is in fact equivalent to the Axiom of Choice, as seen in Exercise 4.4.19. Interestingly, as the reader will see if she does Exercise 4.4.9, the proof of Theorem 4.4.5 (2) does not require the Axiom of Choice.

The following result concerning "cancellation" of functions is a typical application of Theorem 4.4.5.

Theorem 4.4.6. *Let A and B be non-empty sets, and let $f \colon A \to B$ be a function.*

1. *The function f is injective if and only if $f \circ g = f \circ h$ implies $g = h$ for all functions $g, h \colon Y \to A$ for all sets Y.*
2. *The function f is surjective if and only if $g \circ f = h \circ f$ implies $g = h$ for all functions $g, h \colon B \to X$ for all sets X.*

Proof. We will prove Part (2), leaving the remaining part to the reader in Exercise 4.4.15.

(2). First assume that f is surjective. Let $g, h \colon B \to X$ be functions such that $g \circ f = h \circ f$ for some set X. By Theorem 4.4.5 (1), the function f has a right inverse

$q\colon B \to A$. Then $(g \circ f) \circ q = (h \circ f) \circ q$. Using Lemma 4.3.5 and the definition of right inverses, it follows that $g \circ (f \circ q) = h \circ (f \circ q)$, and hence $g \circ 1_B = h \circ 1_B$, and therefore $g = h$.

Now assume f is not surjective. Let $b \in B$ be an element that is not in the range of f. Let $X = \{1,2\}$, and let $g, h\colon B \to X$ be defined by $g(y) = 1$ for all $y \in B$, and by $h(y) = 1$ for all $y \in B - \{b\}$ and $h(b) = 2$. It can then be verified that $g \circ f = h \circ f$, even though $g \neq h$. The desired result now follows using the contrapositive. $\square$

Exercises

Exercise 4.4.1. Is each of the following functions injective, surjective, both or neither? Prove your answers. Feel free to use standard properties of functions such as polynomials, logarithms and the like.

(1) Let $t\colon (1,\infty) \to \mathbb{R}$ be defined by $t(x) = \ln x$ for all $x \in (1,\infty)$.
(2) Let $s\colon \mathbb{R} \to \mathbb{R}$ be defined by $s(x) = x^4 - 5$ for all $x \in \mathbb{R}$.
(3) Let $g\colon [0,\infty) \to [0,1)$ be defined by $g(x) = \frac{x}{1+x}$ for all $x \in [0,\infty)$.
(4) Let $k\colon \mathbb{R}^2 \to \mathbb{R}$ be defined by $k((x,y)) = x^2 + y^2$ for all $(x,y) \in \mathbb{R}^2$.
(5) Let $Q\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$ be defined by $Q(n) = \{1,2,\ldots,n\}$ for all $n \in \mathbb{N}$.

Exercise 4.4.2. In each of the four cases below, we are given a function f such that $f(x) = 3x + 5$ for all x in the domain. Is each function injective, surjective, both or neither?

(1) $f\colon \mathbb{Z} \to \mathbb{Z}$.
(2) $f\colon \mathbb{Q} \to \mathbb{Q}$.
(3) $f\colon \mathbb{Q} \to \mathbb{R}$.
(4) $f\colon \mathbb{R} \to \mathbb{R}$.

Exercise 4.4.3. [Used in Example 6.5.3.] Let $f\colon \mathbb{R} \to (-1,1)$ be defined by

$$f(x) = \begin{cases} \frac{x^2}{1+x^2}, & \text{if } x \geq 0 \\ \frac{-x^2}{1+x^2}, & \text{if } x < 0. \end{cases}$$

Prove that f is bijective. Use only the methods we have used in this text, including the standard algebraic properties of the real numbers; do not use calculus.

Exercise 4.4.4. Let A and B be sets, and let $S \subseteq A$ be a subset. We will use various definitions from Section 4.1.

(1) Prove that the identity map $1_A\colon A \to A$ is bijective.
(2) Prove that inclusion map $j\colon S \to A$ is injective.
(3) Let $f\colon A \to B$ be a function. Suppose that f is injective. Is the restriction $f|_S$ necessarily injective? Give a proof or a counterexample.
(4) Let $g\colon A \to B$ be a function. Suppose that g is surjective. Is the restriction $g|_S$ necessarily surjective? Give a proof or a counterexample.
(5) Let $h\colon S \to B$ be a function, and let $H\colon A \to B$ be an extension of h. Suppose that h is injective. Is H necessarily injective? Give a proof or a counterexample.

(6) Let $k\colon S \to B$ be a function, and let $K\colon A \to B$ be an extension of k. Suppose that k is surjective. Is K necessarily surjective? Give a proof or a counterexample.

(7) Prove that the projection maps $\pi_1\colon A \times B \to A$ and $\pi_2\colon A \times B \to B$ are surjective. Are the projection maps injective?

Exercise 4.4.5. Let A and B be sets. Prove that there is a bijective function $f\colon A \times B \to B \times A$.

Exercise 4.4.6. [Used in Section 3.3.] Let A, B and C be sets. Prove that there is a bijective function $g\colon (A \times B) \times C \to A \times (B \times C)$.

Exercise 4.4.7. Let A be a set. Let $\phi\colon \mathcal{P}(A) \to \mathcal{P}(A)$ be defined by $\phi(X) = A - X$ for all $X \in \mathcal{P}(A)$. Prove that ϕ is bijective.

Exercise 4.4.8. [Used in Exercise 6.7.9.] This exercise makes use of Exercise 2.4.3. Let

$$\mathbb{L} = \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ and } b \text{ are relatively prime}\},$$

and let $U, D\colon \mathbb{L} \to \mathbb{L}$ be defined by $U((a,b)) = (a+b,b)$ and $D((a,b)) = (a, a+b)$ for all $(a,b) \in \mathbb{L}$. These functions are well-defined by Exercise 2.4.3.

(1) Prove that $(1,1) \notin U(\mathbb{L})$ and $(1,1) \notin D(\mathbb{L})$.
(2) Prove that $U((a,b)) \neq (a,b)$ and $D((a,b)) \neq (a,b)$ for all $(a,b) \in \mathbb{L}$.
(3) Prove that U and D are injective.
(4) Prove that $U(\mathbb{L}) \cap D(\mathbb{L}) = \emptyset$.

Exercise 4.4.9. [Used in Theorem 4.4.5.] Prove Theorem 4.4.5 (2).

Exercise 4.4.10. In Theorem 4.4.5 it was assumed that A and B are non-empty sets. Which parts of the theorem still hold when A or B is empty? (Do not forget the case where A and B are both empty.)

Exercise 4.4.11. [Used in Exercise 6.5.15 and Theorem 6.6.5.] Let A and B be sets, let $P, Q \subseteq A$ be subsets and let $f\colon A \to B$ be a function. Suppose that f is injective. Prove that $f(P - Q) = f(P) - f(Q)$.   [Use Exercise 4.2.11.]

Exercise 4.4.12. Let A and B be sets, and let $f\colon A \to B$ be a function.

(1) Prove that f is injective if and only if $E = f^{-1}(f(E))$ for all subsets $E \subseteq A$.
(2) Prove that f is surjective if and only if $F = f(f^{-1}(F))$ for all subsets $F \subseteq B$.

Exercise 4.4.13. [Used in Lemma 6.5.11, Theorem 6.5.13, Theorem 6.6.8 and Theorem 7.7.10.] Let A and B be sets, and let $f\colon A \to B$ and $g\colon B \to A$ be functions.

(1) Suppose that f is injective, and that g is a left inverse of f. Prove that g is surjective.
(2) Suppose that f is surjective, and that g is a right inverse of f. Prove that g is injective.
(3) Suppose that f is bijective, and that g is the inverse of f. Prove that g is bijective.

Exercise 4.4.14. **[Used in Section 4.4.]** Let A, B and C be sets, and let $f: A \to B$ and $g: B \to C$ be functions.

(1) Prove that if $g \circ f$ is injective, then f is injective.
(2) Prove that if $g \circ f$ is surjective, then g is surjective.
(3) Prove that if $g \circ f$ is bijective, then f is injective, and g is surjective.
(4) Find an example of functions $f: A \to B$ and $g: B \to C$ such that $g \circ f$ is bijective, but f is not surjective, and g is not injective. Hence Parts (1)–(3) of this exercise are the best possible results.

Exercise 4.4.15. **[Used in Theorem 4.4.6.]** Prove Theorem 4.4.6 (1).

Exercise 4.4.16. Let A and B be sets, and let $h: A \to B$ be a function. Prove that h is injective if and only if $h(X \cap Y) = h(X) \cap h(Y)$ for all $X, Y \subseteq A$.

Exercise 4.4.17. Let A and B be sets, and let $f: A \to B$ be a function. Prove that f is surjective if and only if $B - f(X) \subseteq f(A - X)$ for all $X \subseteq A$.

Exercise 4.4.18. Let A and B be sets, and let $f: A \to B$ be a function. As discussed at the end of Section 4.2, we can think of f as inducing a function $f_*: \mathcal{P}(A) \to \mathcal{P}(B)$, and a function $f^*: \mathcal{P}(B) \to \mathcal{P}(A)$.

(1) Prove that f_* is injective if and only if f is injective.
(2) Prove that f_* is surjective if and only if f is surjective.
(3) Prove that f^* is injective if and only if f is surjective.
(4) Prove that f^* is surjective if and only if f is injective.
(5) Prove that f_* is bijective if and only if f^* is bijective if and only if f is bijective.
(6) Suppose that f is bijective. Prove that f_* and f^* are inverses of each other.

Exercise 4.4.19. **[Used in Section 3.5 and Section 4.4.]** Suppose that every surjective function has a right inverse. Prove the Axiom of Choice. By Exercise 3.5.2, it is sufficient to prove the Axiom of Choice for Pairwise Disjoint Sets. Although Exercise 3.5.2 was stated for the family of sets versions of the Axiom of Choice, that exercise also applies to functions versions of the axiom (which are equivalent to the family of sets versions). We did not explicitly state what would be called the Axiom of Choice for Pairwise Disjoint Sets—Functions Version, but the reader can figure out what that version would be (by comparing the statements of Axiom 3.5.2 and Theorem 4.1.5), and make use of that version in this exercise.

Exercise 4.4.20. **[Used in Exercise 4.4.21.]** Let A be a non-empty set, and let $f: A \to A$ be a function. Suppose that f is bijective. For each $n \in \mathbb{N}$, let f^n denote the function $A \to A$ given by

$$f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

The function f^n is the n-**fold iteration** of f. (Such a definition, while intuitively reasonable, is not entirely rigorous, because the use of $\cdots$ is not rigorous; a completely rigorous definition will be given in Example 6.4.2 (2).)

We now extend the definition of f^n to all $n \in \mathbb{Z}$. Let $f^0 = 1_A$. Because f is bijective, it follows from Exercise 6.4.4 that f^n is bijective. Hence f^n has an inverse. For each $n \in \mathbb{N}$, let $f^{-n} = (f^n)^{-1}$. It can be verified that $f^a \circ f^b = f^{a+b}$ and $(f^a)^b = f^{ab}$ for all $a, b \in \mathbb{Z}$, though we omit the details for the sake of getting to the interesting part of this exercise; the interested reader can find the details of the first of these equalities, though in a different setting, in the proof of [Blo11, Lemma 2.5.9].

(1) Let $x, y, z \in A$. Prove that the following three properties hold.
   a. $x = f^n(x)$ for some $n \in \mathbb{Z}$.
   b. If $y = f^n(x)$ for some $n \in \mathbb{Z}$, then $x = f^m(y)$ for some $m \in \mathbb{Z}$.
   c. If $y = f^n(x)$ for some $n \in \mathbb{Z}$, and $z = f^m(y)$ for some $m \in \mathbb{Z}$, then $z = f^p(x)$ for some $p \in \mathbb{Z}$.
   (In Section 5.3 we will see that these three properties are particularly important.)

(2) Let $a \in A$. The **orbit** of a with respect to f, denoted O_a, is the set defined by $O_a = \{f^n(a) \mid n \in \mathbb{Z}\}$.
   Let $x, y \in A$. Prove that the following properties hold.
   a. If $y = f^m(x)$ for some $m \in \mathbb{Z}$, then $O_x = O_y$.
   b. If $y \neq f^n(x)$ for any $n \in \mathbb{Z}$, then $O_x \cap O_y = \emptyset$.
   c. $x \in O_y$ if and only if $y \in O_x$.
   d. $A = \bigcup_{x \in A} O_x$.
   Putting these observations together, we see that A can be broken up into disjoint sets, each of which is the orbit of all its members. (Using the terminology of Section 5.3, we will say that the orbits of f form a partition of A.)

(3) Give an example of a bijective function $\mathbb{Z} \to \mathbb{Z}$ with infinitely many orbits. For each $r \in \mathbb{N}$, give an example of a bijective function $\mathbb{Z} \to \mathbb{Z}$ with precisely r orbits.

Exercise 4.4.21. This exercise makes use of Exercise 4.4.20. Let A be a non-empty set, and let $f : A \to A$ be a function. Suppose that f is bijective. Suppose further that A is finite; the results in this exercise are valid only for finite sets. Let $x, y \in A$.

(1) Prove that $f^m = 1_A$ for some $m \in \mathbb{N}$. Use the fact that because A is finite, there are only finitely many bijective functions $A \to A$; this fact is proved in Theorem 7.7.4 (3). Let $r \in \mathbb{N}$ be the smallest natural number such that $f^r = 1_A$. (It makes sense intuitively that there is such a smallest natural number; formally we make use of the Well-Ordering Principle (Theorem 6.2.5).)

(2) Suppose that $y = f^i(x)$ for some $i \in \mathbb{Z}$. Prove that there is some $s \in \mathbb{N} \cup \{0\}$ such that $y = f^s(x)$.

(3) Prove that if $f^k(x) = x$ for some $k \in \mathbb{Z}$, then $f^k(w) = w$ for all $w \in O_x$.

(4) The **stabilizer** of x with respect to f, denoted f_x, is the set defined by $f_x = \{m \in \mathbb{Z} \mid f^m(x) = x \text{ and } 0 \leq m < r\}$. Suppose that $y \in O_x$. Prove that $f_y = f_x$.

(5) Prove that there is some $v \in \mathbb{N}$ such that $f^v(x) = x$. Use the fact that A is finite. The **order** of x with respect to f, denoted n_x, is the smallest $q \in \mathbb{N}$ such that $f^q(x) = x$.

(6) Prove that $O_x = \{f^0(x), f^1(x), f^2(x), \ldots, f^{n_x - 1}(x)\}$. Use the Division Algorithm (Theorem A.5 in the Appendix).

(7) Prove that $n_x | r$.

(8) Prove that if $k \in f_x$, then $n_x | k$.

(9) Prove that $r = |O_x| \cdot |f_x|$.

(10) Prove that $r = \sum_{y \in O_x} |f_y|$.

(11) Because A is finite, there are finitely many distinct orbits in A. Let B denote the number of distinct orbits of f. Prove that $r \cdot B = \sum_{y \in A} |f_y|$.

(12) For each $m \in \{0, \ldots, r-1\}$, the **fixed set** of m, denoted A_m, is the set defined by $A_m = \{z \in A \mid f^m(z) = z\}$. Prove that $r \cdot B = \sum_{i=0}^{r-1} |A_i|$. This result is a special case of Burnside's Formula; see [Fra03, Section 17] for details.

4.5 Sets of Functions

We now go to one level higher of abstraction than we have seen so far. Until now we have looked at one function at a time; now we discuss sets of functions, for example the set of all functions from one set to another. Such sets are useful in many branches of mathematics, for example linear algebra, and hence are well worth studying. We will use sets of functions briefly at the end of Section 6.7, and a bit more extensively in Section 7.7. The material in this section is among the most conceptually difficult in this book, but the reader who has understood the previous material can, with sufficient effort, master the present section as well. We start with the following definition.

Definition 4.5.1. Let A and B be sets. The set of all functions $A \to B$ is denoted $\mathcal{F}(A,B)$. △

For any set A and B, we observe that $\mathcal{F}(A,B)$ is also a set, where each element of the set $\mathcal{F}(A,B)$ is a function $A \to B$. There is no theoretical problem with having a set that has elements that are functions, though sometimes it is hard to get an intuitive picture of what is going on with such sets. Results about sets of functions are proved no differently from results about sets containing intuitively simpler objects such as numbers.

Example 4.5.2.

(1) If $A \neq \emptyset$ and $B = \emptyset$, then $\mathcal{F}(A,B) = \emptyset$. If $A = \emptyset$, then $\mathcal{F}(A,B) = \{\emptyset\}$. If $A \neq \emptyset$ and $B \neq \emptyset$, then $\mathcal{F}(A,B) \neq \emptyset$, because there is at least one constant map $A \to B$.

(2) Let $A = \{1,2\}$ and $B = \{x,y\}$. Then $\mathcal{F}(A,B) = \{f,g,h,k\}$, where the functions $f,g,h,k \colon A \to B$ are defined by $f(1) = x$ and $f(2) = x$, by $g(1) = x$ and $g(2) = y$, by $h(1) = y$ and $h(2) = x$, and by $k(1) = y$ and $k(2) = y$.

(3) The set $\mathcal{F}(\mathbb{R}, \mathbb{R})$ has a number of useful subsets, including the set $C(\mathbb{R}, \mathbb{R})$ of all continuous functions $\mathbb{R} \to \mathbb{R}$, and the set $D(\mathbb{R}, \mathbb{R})$ of all differentiable functions $\mathbb{R} \to \mathbb{R}$. Observe that $D(\mathbb{R}, \mathbb{R}) \subsetneq C(\mathbb{R}, \mathbb{R}) \subsetneq \mathcal{F}(\mathbb{R}, \mathbb{R})$. We can define some useful functions between these three sets, for example $K \colon D(\mathbb{R}, \mathbb{R}) \to \mathcal{F}(\mathbb{R}, \mathbb{R})$ defined by $K(f) = f'$ for all $f \in D(\mathbb{R}, \mathbb{R})$. We observe that the function K is not injective. For instance, let $f, g \in D(\mathbb{R}, \mathbb{R})$ be defined by $f(x) = x^2 + 5$ and $g(x) = x^2 + 7$ for all $x \in \mathbb{R}$. Then $K(f) = K(g)$, even though $f \neq g$. Though it is not obvious, the function

K is also not surjective; in other words, there are functions $\mathbb{R} \to \mathbb{R}$ that do not have antiderivatives. A proof of this fact is beyond the scope of this book, and can be found in [Blo11, Example 4.4.11].

(4) We can give an intuitive interpretation of the set $\mathcal{F}(\mathbb{N}, \mathbb{R})$ as follows. Let $f \in \mathcal{F}(\mathbb{N}, \mathbb{R})$. Then we obtain a sequence of real numbers by writing $f(1)$, $f(2)$, $f(3)$, …. Conversely, given a sequence of real numbers a_1, a_2, a_3, …, we can define an element $g \in \mathcal{F}(\mathbb{N}, \mathbb{R})$ by setting $g(1) = a_1$, and $g(2) = a_2$, and so on. Hence each element of $\mathcal{F}(\mathbb{N}, \mathbb{R})$ corresponds to a sequence of real numbers, and conversely. In fact, the formal definition of a sequence of real numbers is simply an element of $\mathcal{F}(\mathbb{N}, \mathbb{R})$. ◊

There are many possible results that can be proved concerning sets of functions; we give two typical results. We start with a relatively simple lemma, which will be of use later on.

Lemma 4.5.3. *Let A, B, C and D be sets, and let $f\colon A \to C$ and $g\colon B \to D$ be functions. Suppose that f and g are bijective. Then there is a bijective function from $\mathcal{F}(A,B)$ to $\mathcal{F}(C,D)$.*

Proof. Because f and g are both bijective, they have inverses f^{-1} and g^{-1}, respectively. Let $\Phi\colon \mathcal{F}(A,B) \to \mathcal{F}(C,D)$ be defined by $\Phi(h) = g \circ h \circ f^{-1}$ for all $h \in \mathcal{F}(A,B)$. The function Φ is represented in the commutative diagram following this proof. It is straightforward to see that $\Phi(h) \in \mathcal{F}(C,D)$ for all $h \in \mathcal{F}(A,B)$, so Φ is well-defined. We need to show that Φ is bijective. Let $h,k \in \mathcal{F}(A,B)$. Suppose that $\Phi(h) = \Phi(k)$. Then $g \circ h \circ f^{-1} = g \circ k \circ f^{-1}$. Hence $g^{-1} \circ (g \circ h \circ f^{-1}) \circ f = g^{-1} \circ (g \circ k \circ f^{-1}) \circ f$, and making repeated use of Lemma 4.3.5 it follows that $h = k$. Therefore Φ is injective. Now let $r \in \mathcal{F}(C,D)$. Let $t = g^{-1} \circ r \circ f$. It can be seen that $t \in \mathcal{F}(A,B)$. We compute $\Phi(t) = g \circ t \circ f^{-1} = g \circ (g^{-1} \circ r \circ f) \circ f^{-1} = r$. It follows that Φ is surjective. Hence Φ is bijective. □

$$
\begin{array}{ccc}
A & \xrightarrow{\ h\ } & B \\
\downarrow f & & \downarrow g \\
C & \xrightarrow[\Phi(h)]{} & D
\end{array}
$$

Our next result, which is a bit more complicated than the previous one, gives a relation between power sets and sets of functions. More precisely, let A be a set. The theorem says that there is a bijective function from $\mathcal{P}(A)$ to $\mathcal{F}(A, \{0,1\})$. What, intuitively, is the relation between elements of $\mathcal{P}(A)$, each of which is a subset of A, and elements of $\mathcal{F}(A, \{0,1\})$, each of which is a function $A \to \{0,1\}$? Let $S \in \mathcal{P}(A)$, so that $S \subseteq A$. We want to associate with this set S a function $A \to \{0,1\}$. To do so, observe that we can divide A into the two disjoint subsets S and $A - S$. We then define a function from A to $\{0,1\}$ by assigning the value of 1 to every element in S, and 0 to

every element in $A - S$. For different choices of S, we will obtain different functions $A \rightarrow \{0,1\}$. For convenience, we will use the notation and result of Exercise 4.1.8. This theorem might seem rather technical, but we will use it in a few places, for example Example 6.3.5, which is about switching circuits, and Example 6.7.6 (via the proof of Exercise 6.7.7), which is about programming languages.

Theorem 4.5.4. *Let A be a set. Then there is a bijective function from $\mathcal{P}(A)$ to $\mathcal{F}(A,\{0,1\})$.*

Proof. If $A = \emptyset$, then $\mathcal{P}(\emptyset) = \{\emptyset\}$ by Example 3.2.9 (1), and $\mathcal{F}(A,\{0,1\}) = \{\emptyset\}$ by Example 4.5.2 (1), and therefore the identity map is a bijective function from $\mathcal{P}(A)$ to $\mathcal{F}(A,\{0,1\})$. Now suppose that $A \neq \emptyset$. Recall the notation of Exercise 4.1.8.

Let $\Phi \colon \mathcal{P}(A) \rightarrow \mathcal{F}(A,\{0,1\})$ be defined $\Phi(S) = \chi_S$ for all $S \in \mathcal{P}(A)$. We give two proofs that Φ is bijective, because each is instructive.

First Proof: We will show that Φ is bijective by showing that it is injective and surjective, starting with the former. Let $S, T \in \mathcal{P}(A)$. Suppose that $\Phi(S) = \Phi(T)$. Then $\chi_S = \chi_T$, and it follows from Exercise 4.1.8 that $S = T$. Therefore Φ is injective.

We now show that Φ is surjective. Let $f \in \mathcal{F}(A,\{0,1\})$. Let $S = f^{-1}(\{1\})$, so that $S \in \mathcal{P}(A)$. We will show that $\Phi(S) = f$, which is the same as showing that $\chi_S = f$. Both χ_S and f are functions $A \rightarrow \{0,1\}$. Observe that $A - S = f^{-1}(\{0\})$. Then, if $y \in A$, we see that

$$\chi_S(y) = \begin{cases} 1, & \text{if } y \in S \\ 0, & \text{if } y \in A - S \end{cases} = \begin{cases} 1, & \text{if } y \in f^{-1}(\{1\}) \\ 0, & \text{if } y \in f^{-1}(\{0\}) \end{cases}$$

$$= \begin{cases} 1, & \text{if } f(y) = 1 \\ 0, & \text{if } f(y) = 0 \end{cases} = f(y).$$

Hence $\chi_S = f$, and it follows that Φ is surjective.

Second Proof: We will show that Φ is bijective by producing an inverse for it. Let $\Psi \colon \mathcal{F}(A,\{0,1\}) \rightarrow \mathcal{P}(A)$ be defined by $\Psi(f) = f^{-1}(\{1\})$ for all $f \in \mathcal{F}(A,\{0,1\})$. We will show that Ψ is an inverse for Φ by showing that

$$\Psi \circ \Phi = 1_{\mathcal{P}(A)} \quad \text{and} \quad \Phi \circ \Psi = 1_{\mathcal{F}(A,\{0,1\})}.$$

Let $S \in \mathcal{P}(A)$. Then

$$(\Psi \circ \Phi)(S) = \Psi(\Phi(S)) = [\chi_S]^{-1}(\{1\}) = S.$$

It follows that $\Psi \circ \Phi = 1_{\mathcal{P}(A)}$.

Let $f \in \mathcal{F}(A,\{0,1\})$. Then

$$(\Phi \circ \Psi)(f) = \Phi(\Psi(f)) = \Phi(f^{-1}(\{1\})) = \chi_{f^{-1}(\{1\})}.$$

We therefore need to show that $\chi_{f^{-1}(\{1\})} = f$. Observe that $A - f^{-1}(\{1\}) = f^{-1}(\{0\})$. Then, if $y \in A$, we see that

$$\chi_{f^{-1}(\{1\})}(y) = \begin{cases} 1, & \text{if } y \in f^{-1}(\{1\}) \\ 0, & \text{if } y \in A - f^{-1}(\{1\}) \end{cases}$$

$$= \begin{cases} 1, & \text{if } f(y) = 1 \\ 0, & \text{if } f(y) = 0 \end{cases} = f(y).$$

Hence $\chi_{f^{-1}(\{1\})} = f$, and we conclude that $\Phi \circ \Psi = 1_{\mathcal{F}(A,\{0,1\})}$.   □

In addition to the set of all functions from one set to another, there are a number of other sets of functions that are of interest. We now define two types of sets of functions, though there are many other such sets of functions that the reader might encounter during further study of mathematics, for example the set of all linear maps from one vector space to another, which is an important concept in linear algebra.

Definition 4.5.5. Let A and B be sets. The set of all injective functions $A \to B$ is denoted $I(A,B)$, and the set of all bijective functions $A \to B$ is denoted $\mathcal{B}(A,B)$.   △

It is also possible to look at the set of all surjective functions from one set to another, but we will not need it later on, and so we will not treat it here. For any sets A and B, we observe that $\mathcal{B}(A,B) \subseteq I(A,B) \subseteq \mathcal{F}(A,B)$. Unlike the set $\mathcal{F}(A,B)$, which is never the empty set as long as both A and B are not empty, the set $\mathcal{B}(A,B)$ will be the empty set whenever A and B do not have "the same size" (a concept that is intuitively clear for finite sets, and that will be discussed for both finite sets and infinite sets in Section 6.5). Similarly, the set $I(A,B)$ will be empty whenever A is "larger" than B.

Example 4.5.6.

(1) Let A and B be the sets given in Example 4.5.2 (2). It is seen that $\mathcal{B}(A,B) = I(A,B) = \{g,h\}$.

(2) Let $A = \{1,2\}$ and $C = \{x,y,z\}$. Then $\mathcal{B}(A,C) = \emptyset$. As the reader is asked to show in Exercise 4.5.8, it turns out that $I(A,C)$ has six elements. This example is a special case of general results given in Theorem 7.7.4.   ◇

Finally, we use sets of functions to resolve an issue that was left outstanding in Chapter 3. In Section 3.3 we defined the union, intersection and product of two sets. In Section 3.4 we showed how the definitions of union and intersection can be extended to arbitrary families of sets, rather than just two sets at a time, but we did not state how to form the product of an arbitrary family of sets, because we did not have the needed tools. We are now ready for the definition.

We defined the product of two sets in terms of ordered pairs. Intuitively, an ordered pair is something that picks out a "first" element and a "second" one. To generalize this idea, we reformulate the notion of an ordered pair by using functions. (However, we could not have used this reformulation instead of our original discussion of ordered pairs in Section 3.3, because we needed ordered pairs to define functions.)

Let A and B be sets. We can think of an ordered pair (a,b) with $a \in A$ and $b \in B$ as a function $f\colon \{1,2\} \to A \cup B$ that satisfies the conditions $f(1) \in A$ and $f(2) \in B$. The

element $f(1)$ is the first element in the ordered pair, and $f(2)$ is the second element in the ordered pair. Hence the product $A \times B$ can be thought of as the set of functions

$$\{f \in \mathcal{F}(\{1,2\}, A \cup B) \mid f(1) \in A \text{ and } f(2) \in B\}.$$

This reformulation of the definition of $A \times B$ can be generalized to arbitrary families of sets. We use the indexed form of such families, though the non-indexed version would work as well.

Definition 4.5.7. Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I. The **product** of the family of sets, denoted $\prod_{i \in I} A_i$, is the set defined by

$$\prod_{i \in I} A_i = \{f \in \mathcal{F}(I, \bigcup_{i \in I} A_i) \mid f(i) \in A_i \text{ for all } i \in I\}.$$

If all the sets A_i are equal to a single set A, the product $\prod_{i \in I} A_i$ is denoted by A^I.   △

It is not hard to verify that if I is a non-empty set, and if A is a set, then $A^I = \mathcal{F}(I, A)$. An example of this fact is $\mathbb{R}^{\mathbb{N}} = \mathcal{F}(\mathbb{N}, \mathbb{R})$. Given our discussion in Example 4.5.2 (4), we therefore see that $\mathbb{R}^{\mathbb{N}}$ is the set of sequences of real numbers.

The reader might have noticed that Definition 4.5.7 looks somewhat familiar, and that would be good, because it will help us address a subtlety about this definition that we have so far glossed over. It is fine to write such a definition, but simply writing something does not always suffice to make it work. In this specific case, we need to ask whether for any family of non-empty sets $\{A_i\}_{i \in I}$, there actually is something in the set $\prod_{i \in I} A_i$. In other words, is there at least one function $f: I \to \bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ for all $i \in I$? Such a function would choose a single element from each set A_i. Our ability to make such a choice is exactly what is axiomatized in the Axiom of Choice, and that is what looks so familiar in Definition 4.5.7. If the reader compares the statement of the Axiom of Choice given in Theorem 4.1.5 with Definition 4.5.7, it is immediately evident that not only does the Axiom of Choice imply the following theorem, but the following theorem implies the Axiom of Choice; that is, the Axiom of Choice and the following theorem are equivalent.

Theorem 4.5.8. *Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of non-empty sets indexed by I. Then $\prod_{i \in I} A_i \neq \emptyset$.*

Exercises

Exercise 4.5.1. Let $X = \{l, m, n\}$ and $Y = \{\alpha, \beta\}$. Describe all the elements of $\mathcal{F}(X, Y)$.

Exercise 4.5.2. **[Used in Theorem 7.7.4.]** Let A and B be sets. Prove that if A or B has one element, there is a bijective function from $\mathcal{F}(A, B)$ to B.

Exercise 4.5.3. Let A and B be non-empty sets. Let $\Phi: \mathcal{F}(A, B) \to \mathcal{F}(\mathcal{P}(A), \mathcal{P}(B))$ be the function defined by $\Phi(f) = f_*$ for all $f \in \mathcal{F}(A, B)$, where $f_*: \mathcal{P}(A) \to \mathcal{P}(B)$ is defined at the end of Section 4.2. Is Φ injective, surjective, both or neither?

Exercise 4.5.4. Let A, B and C be sets. Suppose that $A \subseteq B$.

(1) Prove that $\mathcal{F}(C,A) \subseteq \mathcal{F}(C,B)$.
(2) Prove that there is an injective function $\mathcal{F}(A,C) \to \mathcal{F}(B,C)$.

Exercise 4.5.5. Let A, B, C be sets. Prove that there is a bijective function from $\mathcal{F}(C, A \times B)$ to $\mathcal{F}(C,A) \times \mathcal{F}(C,B)$.

Exercise 4.5.6. Let A, B, C be sets. Prove that there is a bijective function from $\mathcal{F}(A, \mathcal{F}(B,C))$ to $\mathcal{F}(B, \mathcal{F}(A,C))$.

Exercise 4.5.7. Let A be a set, and let $g \colon A \to A$ be a function. Suppose that g is bijective.

(1) Let $\Omega_g \colon \mathcal{F}(A,A) \to \mathcal{F}(A,A)$ be defined by $\Omega_g(f) = g \circ f$ for all $f \in \mathcal{F}(A,A)$. Prove that Ω_g is bijective.
(2) Let $\Lambda_g \colon \mathcal{F}(A,A) \to \mathcal{F}(A,A)$ be defined by $\Lambda_g(f) = g \circ f \circ g^{-1}$ for all $f \in \mathcal{F}(A,A)$. Prove that Λ_g is bijective. Also, prove that $\Lambda_g(h \circ k) = \Lambda_g(h) \circ \Lambda_g(k)$ for all $h, k \in \mathcal{F}(A,A)$.

Exercise 4.5.8. [Used in Example 4.5.6.] Let $A = \{1,2\}$ and $C = \{x,y,z\}$. Describe explicitly all the elements of $I(A,C)$.

Exercise 4.5.9. [Used in Section 7.7.] Let A, B, C and D be sets, and let $f \colon A \to C$ and $g \colon B \to D$ be functions. Suppose that f and g are bijective.

(1) Prove that there is a bijective function from $I(A,B)$ to $I(C,D)$.
(2) Prove that there is a bijective function from $\mathcal{B}(A,B)$ to $\mathcal{B}(C,D)$.

Exercise 4.5.10. [Used in Theorem 7.7.4 and Theorem 7.7.12.] Let A and B be sets, and let $a \in A$ and $b \in B$.

(1) Prove that there is a bijective function from $\{f \in \mathcal{F}(A,B) \mid f(a) = b\}$ to $\mathcal{F}(A - \{a\}, B)$.
(2) Prove that there is a bijective function from $\{f \in I(A,B) \mid f(a) = b\}$ to $I(A - \{a\}, B - \{b\})$.
(3) Prove that there is a bijective function from $\{f \in \mathcal{B}(A,B) \mid f(a) = b\}$ to $\mathcal{B}(A - \{a\}, B - \{b\})$.

Exercise 4.5.11. Let A be a set. Let $\Phi \colon \mathcal{B}(A,A) \to \mathcal{B}(A,A)$ be defined by $\Phi(f) = f^{-1}$ for all $f \in \mathcal{B}(A)$. Prove that Φ is bijective.

Exercise 4.5.12. Let A be a set. A $\mathbb{Z}$-**action** on A is a function $\Gamma \colon \mathbb{Z} \to \mathcal{B}(A,A)$ that satisfies the following two properties: (1) $\Gamma(0) = 1_A$, and (2) $\Gamma(a+b) = \Gamma(a) \circ \Gamma(b)$ for all $a, b \in \mathbb{Z}$.

(1) Prove that $\Gamma(-a) = [\Gamma(a)]^{-1}$ for all $a \in \mathbb{Z}$.
(2) Suppose that $\Gamma(e) = 1_A$ for some $e \in \mathbb{Z}$. Prove that $\Gamma(ne) = 1_A$ for all $n \in \mathbb{Z}$.
(3) Give two different examples of $\mathbb{Z}$-actions on $\mathbb{R}$.
(4) Give two different examples of $\mathbb{Z}$-actions on the set $\{1,2,3,4\}$.

5

Relations

Mathematicians do not study objects, but relations between objects.
— Henri Poincaré (1854–1912)

5.1 Relations

In colloquial usage we say that there is a "relation" between two things if there is some connection between them. An example of a relation between people is that of having the same color hair, and another example is that of one person being the child of another person. In mathematics we also discuss relations between objects, but, as is often the case, the technical meaning of the word "relation" in mathematics is not entirely the same as the colloquial use of the word. Some examples of relations between mathematical objects are very familiar, such as the relations $=$ and $<$ between real numbers. We saw some other relations in previous chapters, without having used the term "relation." For example, we can define a relation between integers by saying that two integers a and b are related if and only if $a|b$. Relations (and especially equivalence relations, as discussed in Section 5.3), are used in crucial ways in many branches of mathematics, for example abstract algebra, number theory, topology and geometry.

To get a feeling for the formal approach to relations, consider the relation of one person being a biological parent of another person. If we take any two people at random, say persons X and Y, then either X is a parent of Y or not. We can decide whether X is the parent of Y because we know the meaning of the word "parent," and we know how to verify whether the condition of being someone's parent is fulfilled. Alternatively, rather than relying on our knowledge of what being a parent means, we could list all pairs of people (X, Y), where X is a parent of Y. To verify whether two given people are a parent–child pair, we would then simply check two people against the list; such verification could be done by someone who did not know what the words "parent" and "child" meant.

Similar to our formal definition of functions in Section 4.1, the formal approach to relations between mathematical objects is done in terms of listing pairs of related

objects. A mathematical relation might be randomly constructed, and is not necessarily based on any inherent connection between "related" objects, in contrast to the colloquial use of the word "relation." To get the most broadly applicable definition, we allow relations between different types of objects (for example, a relation between people and numbers), rather than only between two objects of the same type.

Definition 5.1.1. Let A and B be sets. A **relation** R from A to B is a subset $\bar{R} \subseteq A \times B$. If $a \in A$ and $b \in B$, we write $a\,R\,b$ if $(a,b) \in R$, and $a\,R\!\!\!/\,b$ if $(a,b) \notin \bar{R}$. A **relation on** A is a relation from A to A.   △

Example 5.1.2.

(1) Let $A = \{1,2,3\}$ and $B = \{x,y,z\}$. There are many possible relations from A to B, one example of which would be the relation E defined by the set $\bar{E} = \{(1,y),(1,z),(2,y)\}$. Then $1\,E\,y$, and $1\,E\,z$, and $2\,E\,y$, but $3\,E\!\!\!/\,x$.

(2) Let P be the set of all people. Define a relation on P by having person x related to person y if and only if x and y have at least one parent in common.

(3) The symbols $<$ and $\le$ both represent relations on $\mathbb{R}$.

(4) Let P be the set of all people, and let B be the set of all books. Define a relation from P to B by having person x related to book b if and only if x has read b.

(5) Let A be a set. The symbol "$\subseteq$" represents a relation on $\mathcal{P}(A)$, where $P, Q \in \mathcal{P}(A)$ are related if and only if $P \subseteq Q$.

(6) Let $f \colon A \to B$ be a function. Then f is defined by a subset of $A \times B$ satisfying a certain condition. Hence f is also a relation from A to B. The concept of a relation is therefore seen to be more general than the concept of a function. In principle, it would have been logical to have the chapter on relations before the chapter on functions, and to view functions as a special case of relations. In practice, however, most mathematicians do not think of functions as special types of relations when they use functions on a daily basis, and therefore functions deserve their own treatment independent of the study of relations.   ◇

Let R and S be relations from A to B. To say that "$R = S$" means that the two relations are both defined by the same subset of $A \times B$. This criterion can be rephrased by saying that $x\,R\,y$ if and only if $x\,S\,y$, for all $x \in A$ and $y \in B$. A proof that R and S are equal typically has the following form.

Proof. Let $x \in A$ and $y \in B$. First, suppose that $x\,R\,y$.

$\vdots$

(argumentation)

$\vdots$

Then $x\,S\,y$.
     Second, suppose that $x\,S\,y$.

$\vdots$

(argumentation)

$\vdots$

Then $x\,R\,y$.

Therefore $R = S$.   □

We will see an example of this strategy in the proof of Theorem 5.3.18.

Just as a person might wish to find out who all of her relatives are, if we have a relation from a set A to a set B, it is sometimes useful to find all the elements of B that are related to a given element in A.

Definition 5.1.3. Let A and B be non-empty sets, let R be a relation from A to B, and let $x \in A$. The **relation class** of x with respect to R, denoted $R[x]$, is the set defined by

$$R[x] = \{y \in B \mid x\,R\,y\}.$$

If the relation R is understood from the context, we will often write $[x]$ instead of $R[x]$.   △

Example 5.1.4. We continue the first three parts of Example 5.1.2.

(1) For this relation we see that $[1] = \{y, z\}$, and $[2] = \{y\}$, and $[3] = \emptyset$.

(2) There are a number of distinct cases here, and we will examine a few of them. If x is the only child of each of her parents, then $[x] = \{x\}$, where we observe that x has the same parents as herself. If y and z are the only two children of each of their parents, then $[y] = \{y, z\} = [z]$. If a has one half-sibling b by her father, and another half-sibling c by her mother, and each of b and c has no other siblings or half-siblings, then $[a] = \{a, b, c\}$, and $[b] = \{a, b\}$, and $[c] = \{a, c\}$.

(3) For the relation $<$, we see that $[x] = (x, \infty)$ for all $x \in \mathbb{R}$, and for the relation $\leq$, we see that $[x] = [x, \infty)$ for all $x \in \mathbb{R}$.   ◇

In Example 5.1.4 we saw various possible behaviors of relation classes. The relation class of an element may be empty, for example $[3]$ in Part (1) of the example. The relation class of an element need not contain that element, for example $[x]$ for any $x \in \mathbb{R}$ with respect to the relation $<$ in Part (3) of the example. Different elements may have overlapping relation classes, for example $[b]$ and $[c]$ in Part (2) of the example. In fact, different elements can have identical relation classes, for example $[y]$ and $[z]$ in Part (2) of the example. In Section 5.3 we will discuss a certain type of relation with particularly nicely behaved relation classes.

In the following definition we give three such properties of relations that will be useful to us in the next two sections, and in many parts of mathematics.

Definition 5.1.5. Let A be a non-empty set, and let R be a relation on A.

1. The relation R is **reflexive** if $x\,R\,x$, for all $x \in A$.
2. The relation R is **symmetric** if $x\,R\,y$ implies $y\,R\,x$, for all $x, y \in A$.
3. The relation R is **transitive** if $x\,R\,y$ and $y\,R\,z$ imply $x\,R\,z$, for all $x, y, z \in A$.   △

As seen in the following example, a relation can have any combination of the above three properties. In most of the parts of this example we leave it to the reader to verify that the given relation has the stated properties.

Example 5.1.6.

(1) The relation of congruence of triangles in the plane is reflexive, symmetric and transitive.

(2) The relation of one person weighing within 5 lbs of another person is reflexive and symmetric, but not transitive. The relation is not transitive, because if A, B and C are people who weigh 130, 133 and 136 lbs respectively, then A is related to B, and B is related to C, but A is not related to C. The relation is reflexive, because any person is within 0 lbs of her own weight. The relation is symmetric, because if X and Y are people who weigh within 5 lbs of each other, then Y and X weigh within 5 lbs of each other.

(3) The relation $\leq$ on $\mathbb{R}$ is reflexive and transitive, but not symmetric.

(4) Let $C = \{1,2,3\}$, and let P be the relation on C defined by the set $\bar{P} = \{(2,2),(3,3),(2,3),(3,2)\}$. Then P is symmetric and transitive, but not reflexive.

(5) Let $B = \{x,y,z\}$, and let E be the relation on B defined by the set $\bar{E} = \{(x,x),(y,y),(z,z),(x,y),(y,z)\}$. Then E is reflexive, but neither symmetric nor transitive. The relation is reflexive, because (x,x), and (y,y) and (z,z) are all in $\bar{E}$, and therefore $x E x$, and $y E y$ and $z E z$. The relation is not symmetric, because $x E y$ but $y \not{E} x$. The relation is not transitive, because $x E y$ and $y E z$, but $x \not{E} z$.

(6) The relation of one person being the cousin of another is symmetric, but neither reflexive nor transitive.

(7) The relation $<$ on $\mathbb{R}$ is transitive, but neither reflexive nor symmetric. Let $x,y,z \in \mathbb{R}$. The relation is transitive, because if $x,y,z \in \mathbb{R}$, and if $x < y$ and $y < z$, then $x < z$. The relation is not reflexive, because it is never the case that $x < x$, for any $x \in \mathbb{R}$. (Observe that we have much more here than the minimum needed to prove that the relation $<$ is not reflexive; it would have sufficed to know that $z \not< z$ for a single $z \in \mathbb{R}$.) The relation is not symmetric, because if $x,y \in \mathbb{R}$, and $x < y$, it is never the case that $y < x$. (Again, we have much more than is minimally needed to prove that $<$ is not symmetric.)

(8) The relation of one person being the daughter of another person is neither reflexive, symmetric nor transitive.   ◊

There are standard proof strategies for proving that a relation is reflexive, symmetric or transitive. Let A be a non-empty set, and let R be a relation on A.

If we wish to prove that R is reflexive, we need to show that for every $x \in A$, the condition $x R x$ is true. Hence, a proof of the reflexivity of R typically has the following form.

Proof. Let $x \in A$.

$\vdots$

(argumentation)

$\vdots$

Then $x R x$. Hence R is reflexive.   □

If we wish to prove that R is symmetric, we need to show that $x R y$ implies $y R x$ for every $x,y \in A$. Observe that to prove that R is symmetric, we do not prove that

either $x \, R \, y$ or $y \, R \, x$ is true (in fact they might not be true for some values of $x, y \in A$), but only that $x \, R \, y$ implies $y \, R \, x$. Hence, a proof of the symmetry of R typically has the following form.

Proof. Let $x, y \in A$. Suppose that $x \, R \, y$.

$$\vdots$$

(argumentation)

$$\vdots$$

Then $y \, R \, x$. Hence R is symmetric.   □

If we wish to prove that R is transitive, we need to show that $x \, R \, y$ and $y \, R \, z$ together imply $x \, R \, z$ for every $x, y, z \in A$. Again, observe that we do not prove that $x \, R \, y$ and $y \, R \, z$ are true, but only that they imply $x \, R \, z$. Hence, a proof of the transitivity of R typically has the following form.

Proof. Let $x, y, z \in A$. Suppose that $x \, R \, y$ and $y \, R \, z$.

$$\vdots$$

(argumentation)

$$\vdots$$

Then $x \, R \, z$. Hence R is transitive.   □

<div align="center">

Exercises

</div>

Exercise 5.1.1. For each of the following relations on $\mathbb{Z}$, find the relation classes $[3]$ and $[-3]$ and $[6]$.

(1) Let S be the relation defined by $a \, S \, b$ if and only if $a = |b|$, for all $a, b \in \mathbb{Z}$.
(2) Let D be the relation defined by $a \, D \, b$ if and only if $a|b$, for all $a, b \in \mathbb{Z}$.
(3) Let T be the relation defined by $a \, T \, b$ if and only if $b|a$, for all $a, b \in \mathbb{Z}$.
(4) Let Q be the relation defined by $a \, Q \, b$ if and only if $a + b = 7$, for all $a, b \in \mathbb{Z}$.

Exercise 5.1.2. For each of the following relations on $\mathbb{R}^2$, give a geometric description of the relation classes $[(0,0)]$ and $[(3,4)]$.

(1) Let S be the relation defined by $(x, y) \, S \, (z, w)$ if and only if $y = 3w$, for all $(x, y), (z, w) \in \mathbb{R}^2$.
(2) Let T be the relation defined by $(x, y) \, T \, (z, w)$ if and only if $x^2 + 3y^2 = 7z^2 + w^2$, for all $(x, y), (z, w) \in \mathbb{R}^2$.
(3) Let Z be the relation defined by $(x, y) \, Z \, (z, w)$ if and only if $x = z$ or $y = w$, for all $(x, y), (z, w) \in \mathbb{R}^2$.

Exercise 5.1.3. Let $A = \{1, 2, 3\}$. Each of the following subsets of $A \times A$ defines a relation on A. Is each relation reflexive, symmetric and/or transitive?

(1) $\bar{M} = \{(3, 3), (2, 2), (1, 2), (2, 1)\}$.
(2) $\bar{N} = \{(1, 1), (2, 2), (3, 3), (1, 2)\}$.

(3) $\bar{O} = \{(1,1),(2,2),(1,2)\}$.
(4) $\bar{P} = \{(1,1),(2,2),(3,3)\}$.
(5) $\bar{Q} = \{(1,2),(2,1),(1,3),(3,1),(1,1)\}$.
(6) $\bar{R} = \{(1,2),(2,3),(3,1)\}$.
(7) $\bar{T} = \{(1,1),(1,2),(2,2),(2,3),(3,3),(1,3)\}$.

Exercise 5.1.4. Is each of the following relations reflexive, symmetric and/or transitive?

(1) Let S be the relation on $\mathbb{R}$ defined by $x\,S\,y$ if and only if $x = |y|$, for all $x,y \in \mathbb{R}$.
(2) Let P be the set of all people, and let R be the relation on P defined by $x\,R\,y$ if and only if x and y were not born in the same city, for all $x,y \in P$.
(3) Let T be the set of all triangles in the plane, and let G be the relation on T defined by $s\,G\,t$ if and only if s has greater area than t, for all triangles $s,t \in T$.
(4) Let P be the set of all people, and let M be the relation on P defined by $x\,M\,y$ if and only if x and y have the same mother, for all $x,y \in P$.
(5) Let P be the set of all people, and let N be the relation on P defined by $x\,N\,y$ if and only if x and y have the same color hair or the same color eyes, for all $x,y \in P$.
(6) Let D be the relation on $\mathbb{N}$ defined by $a\,D\,b$ if and only if $a|b$, for all $a,b \in \mathbb{N}$.
(7) Let T be the relation on $\mathbb{Z} \times \mathbb{Z}$ defined by $(x,y)\,T\,(z,w)$ if and only if there is a line in $\mathbb{R}^2$ that contains (x,y) and (z,w) and has slope an integer, for all $(x,y),(z,w) \in \mathbb{Z} \times \mathbb{Z}$.

Exercise 5.1.5. Let A be a set, and let R be a relation on A. Suppose that R is defined by the set $\bar{R} \subseteq A \times A$. Let R' be the relation on A defined by the set $(A \times A) - \bar{R}$.

(1) If R reflexive, is R' necessarily reflexive, necessarily not reflexive or not necessarily either?
(2) If R symmetric, is R' necessarily symmetric, necessarily not symmetric or not necessarily either?
(3) If R transitive, is R' necessarily transitive, necessarily not transitive or not necessarily either?

Exercise 5.1.6. Let A be a set, and let R be a relation on A. Suppose that R is symmetric and transitive. Find the flaw in the following alleged proof that this relation is necessarily reflexive; there must be a flaw by Example 5.1.6 (4). "Let $x \in A$. Choose $y \in A$ such that $x\,R\,y$. By symmetry know that $y\,R\,x$, and then by transitivity we see that $x\,R\,x$. Hence R is reflexive."

Exercise 5.1.7. Let A be a set, and think of $\subseteq$ as defining a relation on $\mathcal{P}(A)$, as stated in Example 5.1.2 (5). Is this relation reflexive, symmetric and/or transitive?

Exercise 5.1.8. Let A be a set, and let R be a relation on A.

(1) Suppose that R is reflexive. Prove that $\bigcup_{x \in A}[x] = A$.
(2) Suppose that R is symmetric. Prove that $x \in [y]$ if and only if $y \in [x]$, for all $x,y \in A$.
(3) Suppose that R is transitive. Prove that if $x\,R\,y$, then $[y] \subseteq [x]$, for all $x,y \in A$.

Exercise 5.1.9. Let A and B be sets, let R be a relation on A and let $f\colon A \to B$ be a function. The function f **respects** the relation R if $x\,R\,y$ implies $f(x) = f(y)$, for all $x, y \in A$. Which of the following functions respects the given relation?

(1) Let $f\colon \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^6$ for all $x \in \mathbb{R}$; let S be the relation on $\mathbb{R}$ defined by $x\,S\,y$ if and only if $|x| = |y|$, for all $x, y \in \mathbb{R}$.

(2) Let $g\colon \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = \cos x$ for all $x \in \mathbb{R}$; let W be the relation on $\mathbb{R}$ defined by $x\,W\,y$ if and only if $x - y = \frac{\pi k}{2}$ for some $k \in \mathbb{Z}$, for all $x, y \in \mathbb{R}$.

(3) Let $h\colon \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = \lfloor x \rfloor$ for all $x \in \mathbb{R}$, where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x; let T be the relation on $\mathbb{R}$ defined by $x\,T\,y$ if and only if $|x - y| < 1$, for all $x, y \in \mathbb{R}$.

(4) Let $k\colon \mathbb{R}^2 \to \mathbb{R}$ be defined by $k((x,y)) = 3x^2 + 6xy + 3y^2$ for all $(x,y) \in \mathbb{R}^2$; let M be the relation on $\mathbb{R}^2$ defined by $(x,y)\,M\,(z,w)$ if and only if $x + y = z + w$, for all $(x,y), (z,w) \in \mathbb{R}^2$.

Exercise 5.1.10. Let A and B be sets, let R be a relation on A and let $f\colon A \to B$ be a function. Suppose that f is injective, and that it respects the relation R, as defined in Exercise 5.1.9. What, if anything, can be proved about the relation R?

Exercise 5.1.11. Let A and B be sets, let R and S be relations on A and B, respectively, and let $f\colon A \to B$ be a function. The function f is **relation preserving** if $x\,R\,y$ if and only if $f(x)\,S\,f(y)$, for all $x, y \in A$.

(1) Suppose that f is bijective and relation preserving. Prove that f^{-1} is relation preserving.

(2) Suppose that f is surjective and relation preserving. Prove that R is reflexive, symmetric or transitive if and only if S is reflexive, symmetric or transitive, respectively.

5.2 Congruence

In this section we discuss a very important type of relation on the set of integers, which will serve to illustrate the general topic discussed in the next section, and is also a valuable tool in various parts of mathematics and its applications, for example number theory, cryptography and calendars. See [Ros05, Chapters 4 and 5] for further discussion of congruence and its applications, and see [Kob87] for a treatment of congruence and cryptography.

The idea of congruence is based upon the notion of "clock arithmetic," a term sometimes used in elementary mathematics. (For the reader who has not seen "clock arithmetic," it will be sufficient to have seen a clock). For the sake of uniformity, we will make all references to time using the American 12-hour system (ignoring a.m. vs. p.m.), as opposed to the 24-hour system used many places around the world, and in the U.S. military.

Suppose that it is 2 o'clock, and you want to know what time it will be in 3 hours. Clearly the answer is $2 + 3 = 5$ o'clock. Now suppose that it is 7 o'clock, and you want to know what time it will be in 6 hours. A similar calculation would yield

$7 + 6 = 13$ o'clock, but the correct answer would be 1 o'clock, which is found by subtracting 12 from 13, because 13 is greater than 12. Similarly, if it is 11 o'clock and you want to know what time it will be after 30 hours, you first compute $11 + 30 = 41$, and you obtain a number from 1 to 12 by subtracting the number 12 as many times as needed from 41 until a number in the 1 to 12 range is obtained. This method yields $41 - 36 = 5$ o'clock.

Let us now drop the "o'clock." In the previous paragraph, there were two conflicting things we wanted to accomplish: to restrict ourselves to the integers from 1 to 12, and to be able to add numbers even when it took us outside of the 1 to 12 range. To resolve this problem, we took any number that was outside the desired range, and reduced it by multiples of 12 until we were back in the 1 to 12 range, where by "multiple" we mean in integer multiple. For example, we reduced 41 to 5 by subtracting 3 times 12. We therefore consider 41 and 5 as equivalent from the point of view of clocks (though of course these two numbers are not necessarily equivalent from other points of view). In general, two integers are equivalent in this approach if they differ by some multiple of 12. For example, we see that 28 and 4 are equivalent in this sense, but 17 and 3 are not.

We used the number 12 in the above discussion because of our familiarity with clocks, but, as we state formally in the following definition, the same procedure works with any other natural number replacing 12.

Definition 5.2.1. Let $n \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. The number a is **congruent** to the number b **modulo** n, denoted $a \equiv b \pmod{n}$, if $a - b = kn$ for some $k \in \mathbb{Z}$.   △

Example 5.2.2. We see that $19 \equiv -5 \pmod 4$, because $19 - (-5) = 24 = 6 \cdot 4$; and $7 \equiv 7 \pmod 3$, because $7 - 7 = 0 = 0 \cdot 3$; and $13 \not\equiv 2 \pmod 9$, because $13 - 2 = 11$ and 11 is not a multiple of 9.   ◊

For each $n \in \mathbb{N}$, we obtain a relation on $\mathbb{Z}$ given by congruence modulo n. The following lemma shows that for each n, this relation is reflexive, symmetric and transitive, as defined in Section 5.1.

Lemma 5.2.3. *Let $n \in \mathbb{N}$, and let $a, b, c \in \mathbb{Z}$.*

1. $a \equiv a \pmod n$.
2. *If $a \equiv b \pmod n$ then $b \equiv a \pmod n$.*
3. *If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.*

Proof.

(1). Observe that $a - a = 0 \cdot n$.

(2). Suppose that $a \equiv b \pmod n$. Then $a - b = kn$ for some $k \in \mathbb{Z}$. Hence $b - a = (-k)n$. Because $-k \in \mathbb{Z}$, it follows that $b \equiv a \pmod n$.

(3). Suppose that $a \equiv b \pmod n$ and $b \equiv c \pmod n$. Then $a - b = kn$ and $b - c = jn$ for some $k, j \in \mathbb{Z}$. Adding these two equations we obtain $a - c = (k + j)n$. Because $k + j \in \mathbb{Z}$, it follows that $a \equiv c \pmod n$.   □

We now prove a more substantial result about congruence modulo n. The proof of this theorem makes use of an important fact about the integers known as the Division Algorithm, which is stated as Theorem A.5 in the Appendix.

Theorem 5.2.4. *Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. Then there is a unique $r \in \{0,\ldots,n-1\}$ such that $a \equiv r \pmod{n}$.*

Proof. To prove uniqueness, suppose that there are $x, y \in \{0,\ldots,n-1\}$ such that $a \equiv x \pmod{n}$ and $a \equiv y \pmod{n}$. It follows from Lemma 5.2.3 (2) that $x \equiv a \pmod{n}$, and from Lemma 5.2.3 (3) that $x \equiv y \pmod{n}$. That is, we have $x - y = pn$ for some $p \in \mathbb{Z}$. On the other hand, because $x, y \in \{0,\ldots,n-1\}$, it follows that $-(n-1) \le x - y \le n - 1$. We deduce that $p = 0$, and hence that $x = y$.

To prove existence, we use the Division Algorithm (Theorem A.5) to deduce that there are $q, r \in \mathbb{Z}$ such that $a = nq + r$ and $0 \le r < n$. Hence $a - r = qn$, and therefore $a \equiv r \pmod{n}$. □

We can restate Theorem 5.2.4 without reference to congruence modulo n.

Corollary 5.2.5. *Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. Then precisely one of the following holds: either $a = nk$ for some $k \in \mathbb{Z}$, or $a = nk + 1$ for some $k \in \mathbb{Z}$, or $a = nk + 2$ for some $k \in \mathbb{Z}$, ..., or $a = nk + (n-1)$ for some $k \in \mathbb{Z}$.*

If we use $n = 2$ in Corollary 5.2.5, we deduce the following familiar result.

Corollary 5.2.6. *Let $a \in \mathbb{Z}$. Then a is even or odd, but not both.*

Another way to think about Theorem 5.2.4 is by using relation classes with respect to congruence modulo n. Let us examine the case $n = 5$, where we list a few of the relation classes:

$$\vdots$$
$$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$
$$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$$
$$[5] = \{\ldots, -5, 0, 5, 10, 15 \ldots\}.$$
$$\vdots$$

We see that the relation classes repeat themselves every five integers. Hence

$$[0] = [5] = [10] = \cdots$$
$$[1] = [6] = [11] = \cdots$$
$$[2] = [7] = [12] = \cdots$$
$$[3] = [8] = [13] = \cdots$$
$$[4] = [9] = [14] = \cdots .$$

Although a relation class is defined for every integer, there are in fact only five distinct classes. Moreover, these classes are disjoint, and their union is all of $\mathbb{Z}$. The analogous result holds for arbitrary n, as stated in the following theorem.

Theorem 5.2.7. *Let $n \in \mathbb{N}$.*

1. *Let $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{n}$, then $[a] = [b]$. If $a \not\equiv b \pmod{n}$, then $[a] \cap [b] = \emptyset$.*
2. *$[0] \cup [1] \cup \ldots \cup [n-1] = \mathbb{Z}$.*

Proof.

(1). Suppose that $a \equiv b \pmod{n}$. Let $x \in [a]$. Then by the definition of relation classes we know that $a \equiv x \pmod{n}$. By Lemma 5.2.3 (2) it follows that $b \equiv a \pmod{n}$, and hence by Lemma 5.2.3 (3) we deduce that $b \equiv x \pmod{n}$. Therefore $x \in [b]$, and hence $[a] \subseteq [b]$. A similar argument shows that $[b] \subseteq [a]$. We conclude that $[a] = [b]$.

Now assume that $a \not\equiv b \pmod{n}$. We use proof by contradiction. Suppose that $[a] \cap [b] \neq \emptyset$. Hence there is some $y \in [a] \cap [b]$. Then $y \in [a]$ and $y \in [b]$, so that $a \equiv y \pmod{n}$ and $b \equiv y \pmod{n}$. By Lemma 5.2.3 (2) we see that $y \equiv b \pmod{n}$, and by Lemma 5.2.3 (3) it follows that $a \equiv b \pmod{n}$, which is a contradiction. We conclude that $[a] \cap [b] = \emptyset$.

(2). By definition $[a] \subseteq \mathbb{Z}$ for all $a \in \mathbb{Z}$, and therefore $[0] \cup \ldots \cup [n-1] \subseteq \mathbb{Z}$. Let $x \in \mathbb{Z}$. By Theorem 5.2.4 there is a unique $r \in \{0, \ldots, n-1\}$ such that $x \equiv r \pmod{n}$. It follows from Lemma 5.2.3 (2) that $r \equiv x \pmod{n}$. Hence $x \in [r]$. Because $r \in \{0, \ldots, n-1\}$, it follows that $x \in [0] \cup \ldots \cup [n-1]$. Therefore $\mathbb{Z} \subseteq [0] \cup \ldots \cup [n-1]$. We conclude that $[0] \cup \ldots \cup [n-1] = \mathbb{Z}$. $\square$

Theorem 5.2.7 shows that relation classes for congruence modulo n are much better behaved than relation classes for arbitrary relations, as seen in Example 5.1.4. We are now ready for the following definition.

Definition 5.2.8. Let $n \in \mathbb{N}$. The set of **integers modulo** n, denoted $\mathbb{Z}_n$, is the set defined by $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$, where the relation classes are for congruence modulo n. $\triangle$

The set $\mathbb{Z}_n$ is also denoted $\mathbb{Z}/n\mathbb{Z}$ in some texts, for reasons that will become apparent if the reader learns about group theory.

Example 5.2.9. The integers modulo 12 is the set $\mathbb{Z}_{12} = \{[0], [1], \ldots, [11]\}$. This set has 12 elements, each of which is itself a set (namely, a relation class), but which is viewed here as a single element in the set $\mathbb{Z}_{12}$. The relation classes in $\mathbb{Z}_{12}$ could each be described differently. For example, we see that $[0] = [12]$, and so $\mathbb{Z}_{12} = \{[12], [1], \ldots, [11]\}$, which is what we see on the face of a clock. For mathematical purposes it is more convenient to write $[0]$ rather than $[12]$, and so we will continue to write $\mathbb{Z}_{12}$ as we did originally; it would also be nice to have the 12 on clocks replaced with 0, but historical practice holds sway over mathematics in this situation. There are, of course, many other ways to rewrite the elements of $\mathbb{Z}_{12}$, for

example $\mathbb{Z}_{12} = \{[-36], [25], [-10], \ldots, [131]\}$, and so it would in principle be possible to replace the number on a clock with $-36, 25, -10, \ldots, 131$, though presumably only mathematicians would find that amusing. $\Diamond$

For each $n \in \mathbb{N}$, the set $\mathbb{Z}_n$ has n elements. Of course, for each $n \in \mathbb{N}$, there are many sets with n elements, but what makes $\mathbb{Z}_n$ particularly useful is that there is a natural way to define addition and multiplication on it, as seen in the following definition. Addition and multiplication are examples of binary operations, which produce one output for every pair of inputs. Binary operations will be discussed in Section 7.1, but for now it is sufficient to think of addition and multiplication on $\mathbb{Z}_n$ simply as analogs of the familiar addition and multiplication of real numbers.

Definition 5.2.10. Let $n \in \mathbb{N}$. Let $+$ and $\cdot$ be the binary operations on $\mathbb{Z}_n$ defined by $[a] + [b] = [a+b]$ and $[a] \cdot [b] = [ab]$ for all $[a], [b] \in \mathbb{Z}_n$. $\triangle$

As reasonable as Definition 5.2.10 seems, there is a potential problem. Let $n \in \mathbb{N}$, and let $[a], [b], [c], [d] \in \mathbb{Z}_n$. Suppose that $[a] = [c]$ and $[b] = [d]$. Do $[a+b] = [c+d]$ and $[ab] = [cd]$ necessarily hold? If not, then we could not say that $[a] + [b] = [c] + [d]$ and $[a] \cdot [b] = [c] \cdot [d]$, and then $+$ and $\cdot$ would not be well-defined binary operations on $\mathbb{Z}_n$, because $[a] + [b]$ and $[a] \cdot [b]$ would depend not just on the relation classes $[a]$ and $[b]$, but on the particular choice of a and b. This sort of verification is often needed whenever something is defined for relation classes by using representative elements of the classes. Neglecting such verification is a common mistake. Fortunately, everything works as desired in the present case, which we verify using the following lemma.

Lemma 5.2.11. *Let $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$. Suppose that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then $a + b \equiv c + d \pmod{n}$ and $ab \equiv cd \pmod{n}$.*

Proof. There exist $k, j \in \mathbb{Z}$ such that $a - c = kn$ and $b - d = jn$. Then $a = c + kn$ and $b = d + jn$, and therefore

$$a + b = (c + kn) + (d + jn) = c + d + (k + j)n,$$
$$ab = (c + kn)(d + jn) = cd + (cj + dk + kjn)n.$$

The desired result now follows. $\square$

From Lemma 5.2.11, together with Theorem 5.2.7 (1), we deduce the following corollary, which we state without proof. This corollary tells us that $+$ and $\cdot$ as given in Definition 5.2.10 are indeed well-defined for each $\mathbb{Z}_n$.

Corollary 5.2.12. *Let $n \in \mathbb{N}$, and let $[a], [b], [c], [d] \in \mathbb{Z}_n$. Suppose that $[a] = [c]$ and $[b] = [d]$. Then $[a+b] = [c+d]$ and $[ab] = [cd]$.*

It is important to observe that the binary operations $+$ and $\cdot$ are different in each set $\mathbb{Z}_n$. For example, in $\mathbb{Z}_7$ we see that $[6] + [4] = [10] = [3]$, whereas in $\mathbb{Z}_9$ we see that $[6] + [4] = [10] = [1]$.

One nice way of working with the $+$ and $\cdot$ on $\mathbb{Z}_n$ is to make operation tables, which are analogous to the multiplication tables often used in elementary school.

(See Section 7.1 for more discussion of such operation tables.) Consider the following tables for $\mathbb{Z}_6$.

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

The table for $+$ has a very nice pattern, in which the entries are constant on each line of slope 1. Moreover, every element of $\mathbb{Z}_6$ appears precisely once in each row and in each column of the table. These same properties hold in the table for $+$ for every $\mathbb{Z}_n$. The table for $\cdot$ for $\mathbb{Z}_6$ is not as well behaved. For example, not every element of $\mathbb{Z}_6$ appears in each row and in each column, though some rows and columns do have all elements. However, the tables for $\cdot$ for the other $\mathbb{Z}_n$ do not all behave the same as for $\mathbb{Z}_6$. The issue has to do with prime numbers, and whether or not various numbers have common factors. A thorough study of these questions makes use of some number theoretic issues. See [Fra03, Section 20] for details.

A related question is whether equations of the form $[a] \cdot x = [b]$ can be solved in any $\mathbb{Z}_n$. The analogous equation involving real numbers, that is, an equation of the form $ax = b$, always has a unique solution whenever $a \neq 0$. The situation in $\mathbb{Z}_n$ is more complicated. Consider the equation $[4] \cdot x = [3]$. In $\mathbb{Z}_{11}$ there is a unique solution, which is $x = [9]$, as can be verified simply by trying each element of $\mathbb{Z}_{11}$ as a possible candidate for x. In $\mathbb{Z}_{12}$ the same equation has no solution, as can again be verified by trying each element of $\mathbb{Z}_{12}$. The equation $[3] \cdot x = [0]$ has three solutions in $\mathbb{Z}_6$, which are $x = [0], [2], [4]$, as can be seen using the operation table for $\cdot$ for $\mathbb{Z}_6$. We therefore see that in $\mathbb{Z}_6$ it is possible to have two non-zero elements such that their product is $[0]$, in contrast to the situation for multiplication of real numbers. See [Fra03, Section 20] for further discussion of this type of equation in $\mathbb{Z}_n$.

Our final comment about $\mathbb{Z}_n$ takes us back to our initial discussion of clocks, where we took the number 41 (which was the result of starting at 11 o'clock and adding 30 hours), and we then subtracted the number 12 as many times as needed from 41 until a number in the 1 to 12 range was obtained; in this case we obtained the number 5. There are, of course, infinitely many numbers in $\mathbb{Z}$ that, when treated in this same way, will yield the number 5. Rather than thinking of the number 5 here as an integer, it is more correct to think of it as an element of $\mathbb{Z}_{12}$. That is, we think of taking infinitely many elements of $\mathbb{Z}$, and we send them all to a single element in $\mathbb{Z}_{12}$. Of course, there is nothing special about the number 5, and there is nothing special about working modulo 12. We now use functions to formalize this process.

Definition 5.2.13. Let $n \in \mathbb{N}$. The **canonical map** for congruence modulo n is the function $\gamma \colon \mathbb{Z} \to \mathbb{Z}_n$ defined by $\gamma(a) = [a]$ for all $a \in \mathbb{Z}$. $\triangle$

Observe that there is a distinct function γ for each $n \in \mathbb{N}$, but to avoid unnecessarily cumbersome notation (such as γ_n), we will assume that the number n is always known from the context.

The canonical map $\gamma \colon \mathbb{Z} \to \mathbb{Z}_n$ is a special case of a more general type of canonical map that will be seen in Definition 5.3.8.

We now see two simple results about the canonical map that are examples of more general, though rather different, phenomena we will see subsequently.

Lemma 5.2.14. *Let $n \in \mathbb{N}$, let B be a set and let $f \colon \mathbb{Z} \to B$ be a function. Suppose that if $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{n}$, then $f(a) = f(b)$. Then there exists a unique function $g \colon \mathbb{Z}_n \to B$ such that $f = g \circ \gamma$.*

Proof. Left to the reader in Exercise 5.2.10. $\qquad\square$

Using the terminology of Exercise 5.1.9, we say that the function f in Lemma 5.2.14 respects congruence modulo n. The condition $f = g \circ \gamma$ in Lemma 5.2.14 is represented by the following commutative diagram (as discussed in Section 4.3).

$$
\begin{array}{ccc}
\mathbb{Z} & \xrightarrow{\;\;f\;\;} & B \\
\gamma \downarrow & \nearrow{\scriptstyle g} & \\
\mathbb{Z}_n & &
\end{array}
$$
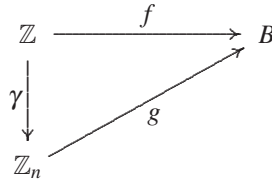
In contrast to Lemma 5.2.14, which can be generalized to all equivalence relations, as seen in Lemma 5.3.9, the following property of the canonical map for congruence modulo n is not applicable to most equivalence relations, though it can be generalized in a very different way, as discussed in Section 7.3.

Lemma 5.2.15. *Let $n \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. Then $\gamma(a+b) = \gamma(a) + \gamma(b)$ and $\gamma(ab) = \gamma(a) \cdot \gamma(b)$.*

Proof. Left to the reader in Exercise 5.2.11. $\qquad\square$

Exercises

Exercise 5.2.1. Which of the following are true and which are false?

(1) $13 \equiv 5 \pmod 2$.

(2) $21 \equiv 7 \pmod 5$.

(3) $7 \equiv 0 \pmod 2$.

(4) $3 \equiv 28 \pmod 5$.

(5) $23 \equiv 23 \pmod 7$.

Exercise 5.2.2. Solve each of the following equations in the given set $\mathbb{Z}_n$. (In some cases there is no solution.)

   (1) $[5]+x=[1]$ in $\mathbb{Z}_9$.

   (2) $[2]\cdot x=[7]$ in $\mathbb{Z}_{11}$.

   (3) $x\cdot[6]=[4]$ in $\mathbb{Z}_{15}$.

   (4) $x\cdot[6]=[2]$ in $\mathbb{Z}_{10}$.

   (5) $[3]\cdot x+[4]=[1]$ in $\mathbb{Z}_5$.

Exercise 5.2.3. Find $n\in\mathbb{N}$ and $a,b\in\mathbb{Z}$ such that $a^2\equiv b^2\pmod{n}$ but $a\not\equiv b$ $\pmod{n}$.

Exercise 5.2.4. Let $n,q\in\mathbb{N}$, and let $a,b\in\mathbb{Z}$. Suppose that $a\equiv b\pmod{n}$, and that $q|n$. Prove that $a\equiv b\pmod{q}$.

Exercise 5.2.5. Let $n\in\mathbb{N}$, and let $a,b\in\mathbb{Z}$. Suppose that $a\equiv b\pmod{n}$. Prove that $n|a$ if and only if $n|b$.

Exercise 5.2.6. Prove or give a counterexample for each of the following proposed cancellation laws.

   (1) Let $n\in\mathbb{N}$, and let $a,b,c\in\mathbb{Z}$. Then $a+c\equiv b+c\pmod{n}$ implies $a\equiv b$ $\pmod{n}$.

   (2) Let $n\in\mathbb{N}$, and let $a,b,c\in\mathbb{Z}-\{0\}$. Suppose that c is not a multiple of n. Then $ac\equiv bc\pmod{n}$ implies $a\equiv b\pmod{n}$.

Exercise 5.2.7. For this exercise we use factorials. If $m\in\mathbb{N}$, then the factorial of m is $m!=m(m-1)(m-2)\cdots2\cdot1$. It is assumed that the reader is familiar with factorials informally; a formal definition of this concept is given in Example 6.4.4 (1), where the "$\cdots$" are avoided.

   Let $n\in\mathbb{N}$. Suppose that $n>1$, and that $(n-1)!\equiv-1\pmod{n}$. Prove that n is a prime number. The converse to this result, known as Wilson's Theorem, is also true, but has a slightly lengthier proof; see [AR89, Section 3.5] or [Ros05, Section 6.1] for details.

Exercise 5.2.8. Let $n\in\mathbb{Z}$. Prove that $n^3\equiv n\pmod{6}$.

Exercise 5.2.9. Let $n\in\mathbb{Z}$. Prove that precisely one of the following is true: $n^2\equiv0$ $\pmod{16}$, or $n^2\equiv1\pmod{8}$, or $n^2\equiv4\pmod{16}$.

Exercise 5.2.10. **[Used in Lemma 5.2.14.]** Prove Lemma 5.2.14.

Exercise 5.2.11. **[Used in Lemma 5.2.15.]** Prove Lemma 5.2.15.

Exercise 5.2.12. **[Used in Exercise 5.2.13 and Section 8.3.]** Is there a relation between a natural number and the sum of its digits? We now have the tools to answer this question. Let $x\in\mathbb{N}$. We can write x in decimal notation as $a_m a_{m-1}\cdots a_2 a_1$, where a_i is an integer such that $0\le a_i\le 9$ for all $i\in\{1,\ldots,m\}$. That notation means $x=\sum_{i=1}^m a_i\,10^i$. The sum of the digits of x is therefore $\sum_{i=1}^m a_i$. Prove that

$$\sum_{i=1}^m a_i\,10^{i-1}\equiv\sum_{i=1}^m a_i\pmod{9}.$$

You may use the fact that the statement of Lemma 5.2.11 can be extended to sums and products of any finite number of integers.

Exercise 5.2.13. This exercise continues Exercise 5.2.12. For each part of this exercise, it is acceptable to use informal arguments, because rigorous proofs require proof by induction, which we have not yet seen (we will see it in detail in Section 6.3).

Let $a, b \in \mathbb{N}$.

(1) Let $\Sigma(a)$ denote the sum of the digits of a. For any $m \in \mathbb{N}$, let $\Sigma^m(a)$ denote $\Sigma(\Sigma(\Sigma(\cdots \Sigma(a) \cdots)))$, with Σ repeated m times. Let $\Sigma^0(a) = a$. Prove that there is some $r \in \mathbb{N} \cup \{0\}$ such that $\Sigma^r(a)$ has a single digit.

(2) Let $M(a)$ denote the smallest $n \in \mathbb{N}$ such that $\Sigma^n(a)$ is a single digit. (It makes sense intuitively that there is such a smallest natural number; formally we make use of the Well-Ordering Principle (Theorem 6.2.5).) If a has only one digit, let $M(a) = 0$. Does $M(a+b) = M(a) + M(b)$ always hold? Give a proof or a counterexample. Does $M(a+b) \geq M(a) + M(b)$ always hold? Give a proof or a counterexample. Does $M(a+b) \leq M(a) + M(b)$ always hold? Give a proof or a counterexample.

(3) Let $\bar{\Sigma}(a)$ be an abbreviation for $\Sigma^{M(a)}(a)$; that is, the number $\bar{\Sigma}(a)$ is the result of repeatedly adding the digits of the number a until a single digit remains. (This process is used in *gematria*, a method employed in Jewish mysticism, as well as in similar constructions in Greek and Arab traditions; see [Ifr85, Chapter 21] for details.) Does $\bar{\Sigma}(a+b) = \bar{\Sigma}(a) + \bar{\Sigma}(b)$ always hold? Give a proof or a counterexample. Does $\bar{\Sigma}(ab) = \bar{\Sigma}(a) \cdot \bar{\Sigma}(b)$ always hold? Give a proof or a counterexample.

(4) Prove that $\bar{\Sigma}(a+b) = \bar{\Sigma}(\bar{\Sigma}(a) + \bar{\Sigma}(b))$ and $\bar{\Sigma}(ab) = \bar{\Sigma}(\bar{\Sigma}(a) \cdot \bar{\Sigma}(b))$.

5.3 Equivalence Relations

In Lemma 5.2.3 we saw that for each $n \in \mathbb{N}$, congruence modulo n satisfied the three properties of reflexivity, symmetry and transitivity. It turns out that many important relations found throughout mathematics satisfy these three properties.

Definition 5.3.1. Let A be a set, and let $\sim$ be a relation on A. The relation $\sim$ is an **equivalence relation** if it is reflexive, symmetric and transitive. $\triangle$

Example 5.3.2. Some examples of equivalence relations are equality on the set $\mathbb{R}$; congruence modulo n on $\mathbb{Z}$ for any $n \in \mathbb{N}$; similarity of triangles on the set of all triangles in the plane; being the same age on the set of all people. $\diamond$

Because we can form relation classes for arbitrary relations, we can in particular form them for equivalence relations. Because relation classes for equivalence relations turn out to behave particularly nicely, and are of great importance, we give them a special name.

Definition 5.3.3. Let A be a non-empty set, and let $\sim$ be an equivalence relation on A. The relation classes of A with respect to $\sim$ are called **equivalence classes**. $\triangle$

For the rest of this section, in order to avoid trivial cases, we will restrict our attention to non-empty sets. We start with the following theorem, which generalizes

Theorem 5.2.7, and which shows that equivalence classes are much better behaved than arbitrary relation classes, as seen in Example 5.1.4. The proof of Part (1) of the following proposition, which is left to the reader as an exercise, is simply a rewriting of the proof of Theorem 5.2.7 (1) in the more general setting of equivalence classes.

Theorem 5.3.4. *Let A be a non-empty set, and let $\sim$ be an equivalence relation on A.*

> 1. *Let $x, y \in A$. If $x \sim y$, then $[x] = [y]$. If $x \not\sim y$, then $[x] \cap [y] = \emptyset$.*
> 2. *$\bigcup_{x \in A}[x] = A$.*

Proof. We will prove Part (2), leaving the remaining part to the reader in Exercise 5.3.6.

(2). By definition $[x] \subseteq A$ for all $x \in A$, and hence $\bigcup_{x \in A}[x] \subseteq A$. Now let $q \in A$. By reflexivity we see that $q \sim q$, and therefore $q \in [q] \subseteq \bigcup_{x \in A}[x]$. Hence $A \subseteq \bigcup_{x \in A}[x]$. We conclude that $\bigcup_{x \in A}[x] = A$.   □

A careful look at the proofs of both parts of Theorem 5.3.4 reveals that the proof of Part (1) uses the symmetry and transitivity of the relation, and the proof of Part (2) uses reflexivity; we therefore see precisely where the three properties in the definition of equivalence relation are used in this proof.

There is a redundancy in the expression $\bigcup_{x \in A}[x]$ in Theorem 5.3.4 (2), because some of the sets $[x]$ might be equal to one another. For example, Theorem 5.3.4 (2) applied to congruence modulo n for a given $n \in \mathbb{N}$ would say that $\cdots \cup [-1] \cup [0] \cup [1] \cup [2] \cup \cdots = \mathbb{Z}$, which is not nearly as strong as the statement in Theorem 5.2.7 (2), which says that $[0] \cup [1] \cup \ldots \cup [n-1] = \mathbb{Z}$, and which has no redundancy. The reason that the statement in Theorem 5.2.7 (2) is stronger is that in the particular case of congruence modulo n we made use of the Division Algorithm (Theorem A.5 in the Appendix), which has no analog for arbitrary equivalence relations.

The following corollary is derived immediately from Theorem 5.3.4 (1).

Corollary 5.3.5. *Let A be a non-empty set, let $\sim$ be an equivalence relation on A and let $x, y \in A$. Then $[x] = [y]$ if and only if $x \sim y$.*

Recall that in Section 5.2, for each $n \in \mathbb{N}$ we formed the set $\mathbb{Z}_n$ of all equivalence classes of $\mathbb{Z}$ with respect to congruence modulo n. We now turn to the analog of this construction for arbitrary equivalence relations.

Definition 5.3.6. Let A be a non-empty set, and let $\sim$ be an equivalence relation on A. The **quotient set** of A with respect to $\sim$, denoted $A/\sim$, is the set defined by $A/\sim = \{[x] \mid x \in A\}$.   △

The set $A/\sim$ in Definition 5.3.6 is the set of all equivalence classes of A with respect to $\sim$. As in all sets, each element of the set $A/\sim$ occurs only once in the set, even if it might not appear that way from the expression $\{[x] \mid x \in A\}$. That is, even though this expression might make it appear as if there is one element of the form $[x]$ in $A/\sim$ for each $x \in A$, that is not the case in general, because it will often happen that $[x] = [y]$ for some distinct $x, y \in A$, that is, when $x \sim y$ by Corollary 5.3.5. Looked

at another way, each equivalence class is named after each of its elements, so that a single equivalence class may have many names, but it is still a single set, and a single element of $A/\sim$.

Example 5.3.7. Let P be the set of all people, and let $\sim$ be the relation on P defined by $x \sim y$ if and only if x and y are the same age (in years). If person x is 19 years old, then the equivalence class of x is the set of all 19-year-olds. Each element of the quotient set $P/\sim$ is itself a set, where there is one such set consisting of all 1-year-olds, another consisting of all 2-year-olds, and so on. Although there are billions of people in P, there are fewer than 125 elements in $P/\sim$, because no currently living person has reached the age of 125. $\Diamond$

In the following definition, which generalizes Definition 5.2.13, we use functions to relate a set and its quotient set.

Definition 5.3.8. Let A be a non-empty set, and let $\sim$ be an equivalence relation on A. The **canonical map** for A and $\sim$ is the function $\gamma \colon A \to A/\sim$ defined by $\gamma(x) = [x]$ for all $x \in A$. $\triangle$

We now have a generalization of Lemma 5.2.14.

Lemma 5.3.9. *Let A and B be non-empty sets, let $\sim$ be an equivalence relation on A and let $f \colon A \to B$ be a function. Suppose that $a \sim y$ implies $f(x) = f(y)$, for all $x, y \in A$. Then there exists a unique function $g \colon A/\sim \to B$ such that $f = g \circ \gamma$, where $\gamma \colon A \to A/\sim$ is the canonical map.*

Proof. Left to the reader in Exercise 5.3.7. $\square$

Using the terminology of Exercise 5.1.9, we say that the function f in Lemma 5.3.9 respects $\sim$. The condition $f = g \circ \gamma$ in Lemma 5.2.14 is represented by the following commutative diagram (as discussed in Section 4.3).
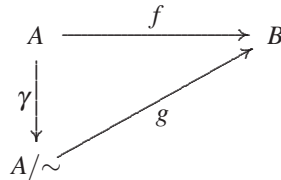
Suppose that we have a quotient set $A/\sim$. We see from Theorem 5.3.4 that any two distinct equivalence classes in $A/\sim$ are disjoint, and that the union of all the equivalence classes is the original set A. We can therefore think of $A/\sim$ as the result of breaking up the set A into disjoint subsets. The following definition generalizes this notion of breaking up a set into disjoint subsets.

Definition 5.3.10. Let A be a non-empty set. A **partition** of A is a family $\mathcal{D}$ of non-empty subsets of A such that

    (a) if $P, Q \in \mathcal{D}$ and $P \neq Q$, then $P \cap Q = \emptyset$;
    (b) $\bigcup_{P \in \mathcal{D}} P = A$. $\triangle$

Definition 5.3.10 (a) can be rephrased more concisely by saying that $\mathcal{D}$ is pairwise disjoint, using the terminology of Definition 3.5.1, though here we use the non-indexed version of the definition. A schematic representation of a partition of a set is seen in Figure 5.3.1. Another way of looking at partitions is to observe that if $\mathcal{E}$ is a family of subsets of a set A, then $\mathcal{E}$ is a partition of A if and only if for each $x \in A$, there is one and only one $P \in \mathcal{E}$ such that $x \in P$.

Fig. 5.3.1.
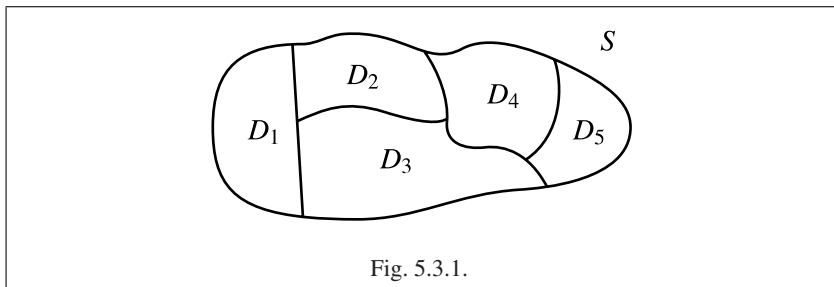
It is important to distinguish between the mathematical usage of the word "partition" and the colloquial usage of the word. In the colloquial usage, a partition that one places in a room is something that divides the room into smaller parts; in the mathematical usage, it is the collection of those smaller parts of the room that forms the partition of the room, not the dividers between the smaller parts. In Figure 5.3.1, the partition of the set S has five elements, namely, the sets $D_1, \ldots, D_5$, each of which contains all the elements in the region of the plane with the appropriate label; the curved lines that separate these five regions do not have a name in mathematical usage (and indeed, they exist only in pictures, not in actual sets). Observe also that the word "partition" refers only to the family of sets, not to the elements of the family. In Figure 5.3.1, the partition is the family $\mathcal{D} = \{D_1, \ldots, D_5\}$; the elements $D_1, \ldots, D_5$ of $\mathcal{D}$ are not themselves called "partitions," but rather "elements of the partition."

Example 5.3.11.

(1) Let E denote the set of even integers, and let O denote the set of odd integers. Then $\mathcal{D} = \{E, O\}$ is a partition of $\mathbb{Z}$.

(2) Let $\mathcal{C} = \{[n, n+1)\}_{n \in \mathbb{Z}}$. Then $\mathcal{C}$ is a partition of $\mathbb{R}$.

(3) Let $\mathcal{G} = \{(n-1, n+1)\}_{n \in \mathbb{Z}}$. Then $\mathcal{G}$ is not a partition of $\mathbb{R}$, because it is not pairwise disjoint. For example, we observe that $(1-1, 1+1) \cap (2-1, 2+1) = (1, 2)$. $\qquad \diamond$

Using the terminology of partitions, we can now state the following immediate corollary to Theorem 5.3.4.

Corollary 5.3.12. *Let A be a non-empty set, and let $\sim$ be an equivalence relation on A. Then $A/\sim$ is a partition of A.*

We see from Corollary 5.3.12 that there is a connection between equivalence relations on a set and partitions of the set. This connection can be made more precise

using bijective functions. To state our result, we will need the following definition, which takes us to one higher level of abstraction than we have seen until now in our discussion of relations.

Definition 5.3.13. Let A be a non-empty set. Let $\mathcal{E}(A)$ denote the set of all equivalence relations on A. Let $\mathcal{T}_A$ denote the set of all partitions of A. △

For a given set A, it is important to keep in mind what the elements of $\mathcal{E}(A)$ and $\mathcal{T}_A$ are. Each element of $\mathcal{E}(A)$ is an equivalence relation on A, which formally is a subset of $A \times A$ that satisfies certain conditions. Each element of $\mathcal{T}_A$ is a partition of A, which is a family of subsets of A that satisfy certain conditions.

Example 5.3.14. Let $A = \{1,2,3\}$. Then $\mathcal{T}_A = \{\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_5\}$, where

$$\mathcal{D}_1 = \{\{1\},\{2\},\{3\}\}, \qquad\qquad \mathcal{D}_4 = \{\{2,3\},\{1\}\},$$
$$\mathcal{D}_2 = \{\{1,2\},\{3\}\}, \qquad\qquad \mathcal{D}_5 = \{\{1,2,3\}\}.$$
$$\mathcal{D}_3 = \{\{1,3\},\{2\}\},$$

Also, we see that $\mathcal{E}(A) = \{R_1, R_2, \ldots, R_5\}$, where these relations are defined by the sets

$$\bar{R}_1 = \{(1,1),(2,2),(3,3)\},$$
$$\bar{R}_2 = \{(1,1),(2,2),(3,3),(1,2),(2,1)\},$$
$$\bar{R}_3 = \{(1,1),(2,2),(3,3),(1,3),(3,1)\},$$
$$\bar{R}_4 = \{(1,1),(2,2),(3,3),(2,3),(3,2)\},$$
$$\bar{R}_5 = \{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)\}.$$

It is straightforward to verify that each of the relations R_i listed above is an equivalence relation on A. ◇

Is it a coincidence that the sets $\mathcal{E}(A)$ and $\mathcal{T}_A$ in Example 5.3.14 have the same number of elements? In fact, we will see shortly that for any set A, whether finite or infinite, there is a correspondence between the equivalence relations on A and the partitions of A. To state this correspondence precisely, we start by defining, for each non-empty set A, a function from $\mathcal{E}(A)$ to $\mathcal{T}_A$, and a function in the other direction. It is not entirely obvious that these functions make sense, but they do indeed work, as noted in the lemma following the definition.

Definition 5.3.15. Let A be a non-empty set. Let $\Phi\colon \mathcal{E}(A) \to \mathcal{T}_A$ be defined as follows. If $\sim$ is an equivalence relation on A, let $\Phi(\sim)$ be the family of sets $A/\sim$. Let $\Psi\colon \mathcal{T}_A \to \mathcal{E}(A)$ be defined as follows. If $\mathcal{D}$ is a partition of A, let $\Psi(\mathcal{D})$ be the relation on A defined by $x\,\Psi(\mathcal{D})\,y$ if and only if there is some $P \in \mathcal{D}$ such that $x,y \in P$, for all $x,y \in A$. △

Observe that there is a distinct function Φ and a distinct function Ψ for each non-empty set A, but to avoid unnecessarily cumbersome notation (such as Φ_A and Ψ_A), we will assume that the set A is always known from the context.

Lemma 5.3.16. *Let A be a non-empty set. The functions Φ and Ψ are well-defined.*

Proof. To prove the lemma, we need to show the following two things: (1) For any equivalence relation $\sim$ on A, the family of sets $\Phi(\sim)$ is a partition of A; and (2) for any partition $\mathcal{D}$ of A, the relation $\Psi(\mathcal{D})$ is an equivalence relation on A. The first of these claims follows immediately from the definition of Φ and Corollary 5.3.12. The second claim is left to the reader in Exercise 5.3.11. □

Example 5.3.17.

(1) Let $\sim$ be the relation on $\mathbb{R}^2$ defined by $(x,y) \sim (z,w)$ if and only if $y - x = w - z$, for all $(x,y), (z,w) \in \mathbb{R}^2$. It can be verified that $\sim$ is an equivalence relation. We want to describe the partition $\Phi(\sim)$ of $\mathbb{R}^2$. Let $(x,y) \in \mathbb{R}^2$. Then $[(x,y)] = \{(z,w) \in \mathbb{R}^2 \mid w - z = y - x\}$. Let $c = y - x$. Then $[(x,y)] = \{(z,w) \in \mathbb{R}^2 \mid w = z + c\}$, which is just a line in $\mathbb{R}^2$ with slope 1 and y-intercept c. Hence $\Phi(\sim)$ is the collection of all lines in $\mathbb{R}^2$ with slope 1.

(2) Let $\mathcal{C}$ be the partition of $\mathbb{R}$ given in Example 5.3.11 (2). We want to describe the equivalence relation $\Psi(\mathcal{C})$. For convenience let $\approx = \Psi(\mathcal{C})$. Suppose that $x, y \in \mathbb{R}$. Then $x \approx y$ if and only if there is some $n \in \mathbb{Z}$ such that $x, y \in [n, n+1)$. Using the notation $\lfloor x \rfloor$ to denote the greatest integer less than or equal to x, we see that $x \approx y$ if and only if $\lfloor x \rfloor = \lfloor y \rfloor$.

(3) Let $\mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_5$ be the partitions and $R_1, R_2, \ldots, R_5$ be the relations given in Example 5.3.14. It can be verified that $\Phi(R_i) = \mathcal{D}_i$ and $\Psi(\mathcal{D}_i) = R_i$ for all $i \in \{1, \ldots, 5\}$; details are left to the reader. ◇

In Example 5.3.17 (3), we see that Φ and Ψ are inverses of each other. Quite remarkably, the following theorem says that the same result holds for any non-empty set. Consequently, we have a complete picture of the connection between equivalence relations and partitions for a given set A: there is a bijective function from the set of equivalence relations on A and the set of partitions of A. That is, to each equivalence relation on A there corresponds a unique partition of A, and vice versa. Moreover, not only do we know in principle that there is such a correspondence, but, even better, we have an explicit description of this correspondence, namely, the functions Φ and Ψ.

Theorem 5.3.18. *Let A be a non-empty set. Then the functions Φ and Ψ are inverses of each other, and hence both are bijective.*

Proof. We need to show that

$$\Psi \circ \Phi = 1_{\mathcal{E}(A)} \quad \text{and} \quad \Phi \circ \Psi = 1_{\mathcal{T}_A}.$$

First, we prove that $\Psi \circ \Phi = 1_{\mathcal{E}(A)}$. Let $\sim \in \mathcal{E}(A)$ be an equivalence relation on A. Let $\approx = \Psi(\Phi(\sim))$. We will show that $\approx = \sim$, and it will then follow that $\Psi \circ \Phi = 1_{\mathcal{E}(A)}$. For convenience let $\mathcal{D} = \Phi(\sim)$, so that $\approx = \Psi(\mathcal{D})$.

Let $x, y \in A$. Suppose that $x \approx y$. Then by the definition of Ψ there is some $D \in \mathcal{D}$ such that $x, y \in D$. By the definition of Φ, we know that D is an equivalence class of $\sim$, so that $D = [q]$ for some $q \in A$. Then $q \sim x$ and $q \sim y$, and by the symmetry

and transitivity of $\sim$ it follows that $x \sim y$. Now suppose that $x \sim y$. Then $y \in [x]$. By the reflexivity of $\sim$, we know that $x \in [x]$. The definition of Φ implies that $[x] \in \mathcal{D}$. Hence, by the definition of Ψ, it follows that $x \approx y$. Therefore $x \approx y$ if and only if $x \sim y$. We conclude that $\approx \; = \; \sim$.

Second, we prove that $\Phi \circ \Psi = 1_{\mathcal{T}_A}$. Let $\mathcal{D} \in \mathcal{T}_A$ be a partition of A. Let $\mathcal{F} = \Phi(\Psi(\mathcal{D}))$. We will show that $\mathcal{F} = \mathcal{D}$, and it will then follow that $\Phi \circ \Psi = 1_{\mathcal{T}_A}$. For convenience let $\approx \; = \Psi(\mathcal{D})$, so that $\mathcal{F} = \Phi(\approx)$.

Let $B \in \mathcal{F}$. Then by the definition of Φ we know that B is an equivalence class of $\approx$, so that $B = [z]$ for some $z \in A$. Because $\mathcal{B}$ is a partition of A, then there is a unique $P \in \mathcal{B}$ such $z \in P$. Let $w \in A$. Then by the definition of Ψ we see that $z \approx w$ if and only if $w \in P$. It follows that $w \in [z]$ if and only if $w \in P$, and hence $P = [z]$. Hence $B = [z] = P \in \mathcal{B}$. Therefore $\mathcal{F} \subseteq \mathcal{B}$.

Let $C \in \mathcal{B}$. Let $y \in C$. As before, it follows from the definition of Ψ that $C = [y]$. Therefore by the definition of Φ we see that $C \in \Phi(\approx) = \mathcal{F}$. Hence $\mathcal{B} \subseteq \mathcal{F}$. We conclude that $\mathcal{F} = \mathcal{B}$. $\qquad\qquad\square$

Exercises

Exercise 5.3.1. Which of the following relations is an equivalence relation?

(1) Let M be the relation on $\mathbb{R}$ defined by $x\,M\,y$ if and only if $x - y$ is an integer, for all $x, y \in \mathbb{R}$.

(2) Let S be the relation on $\mathbb{R}$ defined by $x\,S\,y$ if and only if $x = |y|$, for all $x, y \in \mathbb{R}$.

(3) Let T be the relation on $\mathbb{R}$ defined by $x\,T\,y$ if and only if $\sin x = \sin y$, for all $x, y \in \mathbb{R}$.

(4) Let P be the set of all people, and let Z be the relation on P defined by $x\,Z\,y$ if and only if x and y are first cousins, for all $x, y \in P$.

(5) Let P be the set of all people, and let R be the relation on P defined by $x\,R\,y$ if and only if x and y have the same maternal grandmother, for all $x, y \in P$.

(6) Let L be the set of all lines in the plane, and let W be the relation on L defined by $\alpha\,W\,\beta$ if and only if α and β are parallel, for all $\alpha, \beta \in L$.

Exercise 5.3.2. For each of the following equivalence relations on $\mathbb{R}$, find the equivalence classes $[0]$ and $[3]$.

(1) Let R be the relation defined by $a\,R\,b$ if and only if $|a| = |b|$, for all $a, b \in \mathbb{R}$.

(2) Let S be the relation defined by $a\,S\,b$ if and only if $\sin a = \sin b$, for all $a, b \in \mathbb{R}$.

(3) Let T be the relation defined by $a\,T\,b$ if and only if there is some $n \in \mathbb{Z}$ such that $a = 2^n b$, for all $a, b \in \mathbb{N}$.

Exercise 5.3.3. For each of the following equivalence relations on $\mathbb{R}^2$, give a geometric description of the equivalence classes $[(0,0)]$ and $[(3,4)]$.

(1) Let Q be the relation defined by $(x, y)\,Q\,(z, w)$ if and only if $x^2 + y^2 = z^2 + w^2$, for all $(x, y), (z, w) \in \mathbb{R}^2$.

(2) Let U be the relation defined by $(x, y)\,U\,(z, w)$ if and only if $|x| + |y| = |z| + |w|$, for all $(x, y), (z, w) \in \mathbb{R}^2$.

(3) Let V be the relation defined by $(x,y) \, V \, (z,w)$ if and only if $\max\{|x|,|y|\} = \max\{|z|,|w|\}$, for all $(x,y),(z,w) \in \mathbb{R}^2$.

Exercise 5.3.4. Let A and B be sets, and let $f \colon A \to B$ be a function. Let $\sim$ be the relation on A defined by $x \sim y$ if and only if $f(x) = f(y)$, for all $x,y \in A$.

(1) Prove that $\sim$ is an equivalence relation.
(2) What can be proved about the equivalence classes of $\sim$? Does the answer depend upon whether f is injective and/or surjective?

Exercise 5.3.5. Let A be a set, and let $\asymp$ be a relation on A. Prove that $\asymp$ is an equivalence relation if and only if the following two conditions hold.

(1) $x \asymp x$, for all $x \in A$.
(2) $x \asymp y$ and $y \asymp z$ implies $z \asymp x$, for all $x,y,z \in A$.

Exercise 5.3.6. [Used in Theorem 5.3.4.] Prove Theorem 5.3.4 (1).

Exercise 5.3.7. [Used in Lemma 5.3.9.] Prove Lemma 5.3.9.

Exercise 5.3.8. Which of the following families of subsets of $\mathbb{R}$ are partitions of $[0,\infty)$?

(1) $\mathcal{H} = \{[n-1,n)\}_{n\in\mathbb{N}}$.
(2) $\mathcal{G} = \{[x-1,x)\}_{x\in[0,\infty)}$.
(3) $\mathcal{F} = \{\{x\}\}_{x\in[0,\infty)}$.
(4) $I = \{[n-1,n+1)\}_{n\in\mathbb{N}}$.
(5) $\mathcal{J} = \{[0,n)\}_{n\in\mathbb{N}}$.
(6) $\mathcal{K} = \{[2^{n-1}-1,2^n-1)\}_{n\in\mathbb{N}}$.

Exercise 5.3.9. For each of the following equivalence relations, describe the corresponding partition. Your description of each partition should have no redundancy, and should not refer to the name of the relation.

(1) Let P be the set of all people, and let $\asymp$ be the relation on P defined by $x \asymp y$ if and only if x and y have the same mother, for all $x,y \in P$.
(2) Let $\sim$ be the relation on $\mathbb{R} - \{0\}$ defined by $x \sim y$ if and only if $xy > 0$, for all $x,y \in \mathbb{R} - \{0\}$.
(3) Let $\approx$ be the relation on $\mathbb{R}^2$ defined by $(x,y) \approx (z,w)$ if and only if $(x-1)^2 + y^2 = (z-1)^2 + w^2$, for all $(x,y),(z,w) \in \mathbb{R}^2$.
(4) Let L be the set of all lines in $\mathbb{R}^2$, and let $\eqsim$ be the relation on L defined by $l_1 \eqsim l_2$ if and only if l_1 is parallel to l_2 or is equal to l_2, for all $l_1,l_2 \in L$.

Exercise 5.3.10. For each of the following partitions, describe the corresponding equivalence relation. Your description of each equivalence relation should not refer to the name of the partition.

(1) Let $\mathcal{E}$ be the partition of $A = \{1,2,3,4,5\}$ defined by $\mathcal{E} = \{\{1,5\},\{2,3,4\}\}$.
(2) Let $\mathcal{Z}$ be the partition of $\mathbb{R}$ defined by $\mathcal{Z} = \{T_x\}_{x\in\mathbb{R}}$, where $T_x = \{x,-x\}$ for all $x \in \mathbb{R}$.
(3) Let $\mathcal{D}$ be the partition of $\mathbb{R}^2$ consisting of all circles in $\mathbb{R}^2$ centered at the origin (the origin is considered a "degenerate" circle).
(4) Let $\mathcal{W}$ be the partition of $\mathbb{R}$ defined by $\mathcal{W} = \{[n,n+2) \mid n \text{ is an even integer}\}$.

Exercise 5.3.11. [Used in Lemma 5.3.16.] Prove Item (2) in the proof of Lemma 5.3.16.

Exercise 5.3.12. Let X and Y be sets, and let $h\colon X \to Y$ be a function. Let $\asymp$ be the relation on X defined by $s \asymp t$ if and only if $h(s) = h(t)$, for all $s, t \in X$.

(1) Prove that $\asymp$ is an equivalence relation on X.
(2) Let $\gamma\colon X \to X/\!\asymp$ be the canonical map. Let $j\colon h(X) \to Y$ be the inclusion map. Prove that there is a unique bijective function $\hat{h}\colon X/\!\asymp \to h(X)$ such that $h = j \circ \hat{h} \circ \gamma$. This last condition is represented by the following commutative diagram (as discussed in Section 4.3).

$$
\begin{array}{ccc}
X & \xrightarrow{\ \ f\ \ } & Y \\
\Big\downarrow{\scriptstyle\gamma} & & \Big\uparrow{\scriptstyle j} \\
X/\!\asymp & \xrightarrow[\ \hat{h}\ ]{} & h(X)
\end{array}
$$

Observe that γ is surjective (because $\asymp$ is reflexive), that $\hat{h}$ is bijective and that j is injective. Hence any function can be written as a composition of a surjective function, a bijective function and an injective function.

Exercise 5.3.13. [Used in Exercise 5.3.14.] Let A be a non-empty set. Let $\mathcal{R}(A)$ denote the set of all relations on A, and let $\mathcal{S}_A$ denote the set of all families of subsets of A.

(1) Clearly $\mathcal{E}(A) \subseteq \mathcal{R}(A)$ and $\mathcal{T}_A \subseteq \mathcal{S}_A$. Are these inclusions proper?
(2) Express the sets $\mathcal{R}(A)$ and $\mathcal{S}_A$ in terms of products of sets and power sets.
(3) Let $A = \{1, 2\}$. What are $\mathcal{R}(A)$ and $\mathcal{S}_A$?
(4) Suppose that A is a finite set. Express $|\mathcal{R}(A)|$ and $|\mathcal{S}_A|$ in terms of $|A|$. Do $\mathcal{R}(A)$ and $\mathcal{S}_A$ have the same number of elements? Use Example 3.2.9 (2) and Example 3.3.10 (3).

Exercise 5.3.14. This exercise makes use of the definitions given at the start of Exercise 5.3.13. We generalize the functions Φ and Ψ given in Definition 5.3.15 as follows. Let A be a non-empty set. Let $\widetilde{\Phi}\colon \mathcal{R}(A) \to \mathcal{S}_A$ be defined as follows. If $\propto$ is a relation on A, let $\Phi(\propto)$ be the family of all relation classes of A with respect to $\propto$. Let $\widetilde{\Psi}\colon \mathcal{S}_A \to \mathcal{R}(A)$ be defined as follows. If $\mathcal{D}$ is a family of subsets of A, let $\Psi(\mathcal{D})$ be the relation on A defined by $x\,\Psi(\mathcal{D})\,y$ if and only if there is some $D \in \mathcal{D}$ such that $x, y \in D$, for all $x, y \in A$. (There is a distinct function $\widetilde{\Phi}$ and a distinct function $\widetilde{\Psi}$ for each non-empty set A, but we will assume that the set A is always known from the context.)

(1) Find a set B and an element $\mathcal{D} \in \mathcal{S}_B$ such that $\widetilde{\Psi}(\mathcal{D})$ is not reflexive. Find a set C and an element $\mathcal{E} \in \mathcal{S}_C$ such that $\widetilde{\Psi}(\mathcal{E})$ is not transitive.
(2) Suppose that A is finite and has at least two elements. Prove that each of $\widetilde{\Phi}$ and $\widetilde{\Psi}$ is neither injective nor surjective. Is it necessary to restrict our attention to sets with at least two elements?

(3) Suppose that A has at least two elements. Describe the images of the functions $\widetilde{\Phi}$ and $\widetilde{\Psi}$, and prove your results. For $\widetilde{\Phi}$ restrict your attention to the case where A is finite.

6

Finite Sets and Infinite Sets

These are among the marvels that surpass the bounds of our imagination, and that must warn us how gravely one errs in trying to reason about infinites by using the same attributes that we apply to finites.

– Galileo Galilei (1564–1642)

6.1 Introduction

Infinite sets appear to behave more strangely than finite ones, at least from our perspective as human beings, whose daily experience is of the finite. The difficulty of dealing with infinite sets was raised by the ancient Greek Zeno in his four "paradoxes"; see [Ang94, Chapter 8] or [Boy91, pp. 74–76] for details. From a modern perspective Zeno's paradoxes are not paradoxes at all, and can be resolved using tools from real analysis, developed long after Zeno. However, these paradoxes had a historical impact on the study of the infinite, and they indicate how much trickier it is to understand the infinite than the finite.

In order to have a better understanding of sets, and in order to develop tools that are very important in a variety of branches of mathematics, we need to understand how to compare "sizes" of sets, and in particular to understand the difference between finite sets and infinite sets, and between countably infinite sets and uncountable sets (both of which are types of infinite sets that will be defined in this chapter). In Section 6.5 we discuss the general notion of the cardinality of sets, which is the proper way to understand the intuitive notion of the "size" of sets, and we define finite sets, countable sets and uncountable sets. In Section 6.6 we discuss some important properties of finite sets and countable sets. In Section 6.7 we apply the ideas of Sections 6.5 and 6.6 to study the cardinalities of the standard number systems. (Further topics pertaining to combinatorial questions about finite sets may be found in Sections 7.6 and 7.7.)

As will be seen in Sections 6.5 and 6.6, the distinctions between finite sets, countable sets and uncountable sets are very much tied to properties of the natural numbers. We therefore start this chapter with a summary of some of the basic properties

of the natural numbers in Section 6.2. We will not prove these properties (doing so would take us too far afield), but these properties are very familiar, and the reader can either take them on faith, or look at the proofs found in the supplied references. One of the most important properties of the natural numbers, indeed one of the defining properties of that set of numbers, is the ability to do proof by induction, often referred to as the Principle of Mathematical Induction. We discuss proof by induction in detail in Section 6.3, both because it is a very useful technique for proofs of certain types of statements found in many parts of mathematics, and because in particular it is helpful in proving some aspects of the natural numbers that are needed in later sections of this chapter. Another fundamental feature of the natural numbers is definition by recursion, which is related to, but not identical with, proof by induction. We discuss definition by recursion in Section 6.4, again both to gain a general understanding of that concept and because it will be useful later in the chapter.

6.2 Properties of the Natural Numbers

Many of the topics in the present chapter depend crucially upon the properties of the natural numbers. We will not prove these properties in this text, but will present a very brief summary of the minimum that is needed for our subsequent discussion. The curious reader can find proofs of all the relevant properties of the natural numbers in [Blo11, Chapters 1 and 2].

Any rigorous treatment of the natural numbers must ultimately rely upon some axioms. There are two standard axiomatic approaches to developing the natural numbers. One approach, involving the minimal axiomatic assumptions and the most effort deducing facts from the axioms, is to assume the Peano Postulates for the natural numbers, stated below as Axiom 6.2.1. From these postulates, it is then possible to prove all the expected properties of the natural numbers, and, no less important, it is possible to construct first the integers, then the rational numbers and then the real numbers. This process is not brief, and some of the proofs are a bit tricky, though in principle all that is needed as background for such a construction is the material about sets, functions and relations that we have seen in previous chapters of this text. The details of this approach may be found in [Blo11, Chapter 1]. The other approach is to assume axioms for the real numbers, and then to locate the natural numbers inside the real numbers, and then prove all the usual properties of the natural numbers using the properties of the real numbers. This approach is shorter than the previous approach, though it is ultimately less satisfying, because much more is being assumed axiomatically. The details of this approach may be found in [Blo11, Chapter 2].

The Peano Postulates for the natural numbers are based on the insight that the most fundamental property of the natural numbers is the ability to do proof by induction. Although it might seem that in order to do proof by induction it would also be necessary to be able to do other things with the natural numbers such as addition, it turns out that very little indeed is needed to do proof by induction. We need to have a set, denoted $\mathbb{N}$; we need to have a distinguished element in the set, denoted 1, with which to start proof by induction; and we need to have a function from the set

to itself, denoted $s \colon \mathbb{N} \to \mathbb{N}$, which intuitively takes each natural number to its successor. Intuitively, we think of the successor of a natural number as being the result of adding 1 to the number, though formally the notion of addition does not appear in the statement of the Peano Postulates.

Of course, not every set with a distinguished element and a function from the set to itself behaves the way the natural numbers ought to behave, and hence the Peano Postulates require that three entities $\mathbb{N}$, 1 and s satisfy a few simple properties. One of these properties, listed as Part (c) of Axiom 6.2.1 below, is just the formal statement that proof by induction works. This discussion might seem quite mysterious to the reader who has not previously encountered proof by induction, but we appeal to the patience of such reader, who will see a thorough discussion of this topic in Section 6.3.

Axiom 6.2.1 (Peano Postulates). *There exists a set $\mathbb{N}$ with an element $1 \in \mathbb{N}$ and a function $s \colon \mathbb{N} \to \mathbb{N}$ that satisfy the following three properties.*

    a. *There is no $n \in \mathbb{N}$ such that $s(n) = 1$.*
    b. *The function s is injective.*
    c. *Let $G \subseteq \mathbb{N}$ be a set. Suppose that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = \mathbb{N}$.*

If we think intuitively of the function s in the Peano Postulates as taking each natural number to its successor, then Part (a) of the postulates says that 1 is the first number in $\mathbb{N}$, because it is not the successor of anything.

Although it does not say in the Peano Postulates (Axiom 6.2.1) that the set $\mathbb{N}$ is unique, in fact that turns out to be true. See [Blo11, Exercise 1.2.8] for a proof. We can therefore make the following definition.

Definition 6.2.2. The set of **natural numbers** is the set $\mathbb{N}$, the existence of which is given in the Peano Postulates.   △

How do we know that there is a set, and an element of the set, and a function of the set to itself, that satisfy the Peano Postulates? There are two approaches to resolving this matter. When we do mathematics, we have to take something as axiomatic, which we use as the basis upon which we prove all our other results. Hence, one approach to the Peano Postulates is to recognize their very reasonable and minimal nature, and to be satisfied with taking them axiomatically. Alternatively, if one takes the Zermelo–Fraenkel Axioms as the basis for set theory, then it is not necessary to assume additionally that the Peano Postulates hold, because the existence of something satisfying the Peano Postulates can be derived from the Zermelo–Fraenkel Axioms. See [End77, Chapter 4] for details.

The Peano Postulates are very minimal, and the reader might wonder how we can be sure that so minimal a hypothesis really characterizes the natural numbers as we intuitively know them. The answer is that we cannot resolve such a question rigorously, because we cannot prove things about our intuition. What does turn out to be true, as seen rigorously in [Blo11, Chapter 1], is that from the Peano Postulates we can define all the other familiar aspects of the natural numbers such as addition

and multiplication, and we can prove that these operations satisfy all the properties we would intuitively expect. Could it happen that one day someone will deduce something from the Peano Postulates that we would not want to attribute to the natural numbers as we intuitively conceive of them? In principle that could happen, but given that the Peano Postulates have been around for over a hundred years, and have been used extensively by many mathematicians, and no problems have yet been found, it seems quite unlikely that any secret problems are lurking around unseen.

If one goes through the full development of the natural numbers starting from the Peano Postulates, the first major theorem one encounters is the one we now state. This theorem is used in particular in the definition of addition and multiplication of the natural numbers, and although we will not go over those definitions (see the reference given above), this theorem has many other applications in many parts of mathematics. This theorem, called Definition by Recursion, is in fact so valuable that it merits a section of its own, Section 6.4.

Definition by Recursion allows us to define functions with domain $\mathbb{N}$ by defining a function at 1, and then defining it at $n+1$ in terms of the definition of the function at n. It is important to recognize that recursion, while intimately related to induction, is not the same as induction (though it is sometimes mistakenly thought to be); the essential difference is that induction is used to prove statements about things that are already defined, whereas recursion is used to define things. The proof of the following theorem, which relies upon nothing but the Peano Postulates (Axiom 6.2.1), is somewhat tricky; see [Blo11, Theorem 2.5.5] for details.

Theorem 6.2.3 (Definition by Recursion). *Let A be a set, let $b \in A$ and let $k \colon A \to A$ be a function. Then there is a unique function $f \colon \mathbb{N} \to A$ such that $f(1) = b$ and $f \circ s = k \circ f$.*

The equation $f \circ s = k \circ f$ in the statement of Definition by Recursion (Theorem 6.2.3) means that $f(s(n)) = k(f(n))$ for all $n \in \mathbb{N}$. If $s(n)$ were to be interpreted as $n+1$, as indeed it is once addition for $\mathbb{N}$ is rigorously defined (a definition that requires Definition by Recursion), then $f(s(n)) = k(f(n))$ would mean that $f(n+1) = k(f(n))$, which looks more familiar intuitively. Additionally, the equation $f \circ s = k \circ f$ can be represented by the following commutative diagram, which as always means that going either way around the square yields the same result.

$$
\begin{array}{ccc}
\mathbb{N} & \xrightarrow{\ s\ } & \mathbb{N} \\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\
H & \xrightarrow[\ k\ ]{} & H
\end{array}
$$

Once Definition by Recursion has been established, it is possible to define addition, multiplication and the relation less than for the natural numbers, and it is then possible to prove all the standard properties of these numbers; many of the proofs, not surprisingly, are by induction. The following theorem lists some of the most basic properties of addition, multiplication and less than for the natural numbers, though

of course not all such properties are listed. Again, all the details can be found in the reference cited above.

Theorem 6.2.4. *Let $a, b, c, d \in \mathbb{N}$.*

1. *If $a + c = b + c$, then $a = b$.*
2. *$(a + b) + c = a + (b + c)$.*
3. *$s(a) = a + 1$.*
4. *$a + b = b + a$.*
5. *$a \cdot 1 = a = 1 \cdot a$.*
6. *$(a + b)c = ac + bc$.*
7. *$ab = ba$.*
8. *$c(a + b) = ca + cb$.*
9. *$(ab)c = a(bc)$.*
10. *If $ac = bc$ then $a = b$.*
11. *$a \geq a$, and $a \not> a$, and $a + 1 > a$.*
12. *$a \geq 1$, and if $a \neq 1$ then $a > 1$.*
13. *If $a < b$ and $b < c$, then $a < c$; if $a \leq b$ and $b < c$, then $a < c$; if $a < b$ and $b \leq c$, then $a < c$; if $a \leq b$ and $b \leq c$, then $a \leq c$.*
14. *$a < b$ if and only if $a + c < b + c$.*
15. *$a < b$ if and only if $ac < bc$.*
16. *Precisely one of the following holds: $a < b$, or $a = b$, or $a > b$ (Trichotomy Law).*
17. *$a \leq b$ or $b \leq a$.*
18. *If $a \leq b$ and $b \leq a$, then $a = b$.*
19. *It cannot be that $b < a < b + 1$.*
20. *$a < b$ if and only if $a + 1 \leq b$.*
21. *If $a < b$, there is a unique $p \in \mathbb{N}$ such that $a + p = b$.*

Observe that Theorem 6.2.4 (3) states that the function s is just what we thought it would be. Most of the parts of Theorem 6.2.4 are very familiar to the reader, and most—though not all—also apply to all real numbers, not just the natural numbers. Parts (12) and (15) are specific to the natural numbers, because, intuitively, these numbers do not include zero, negative numbers and fractions. Parts (19) and (20) are both ways of saying that the natural numbers are "discrete," a feature not shared by the rational numbers or the real numbers.

The integers are also discrete in the sense of Theorem 6.2.4 (19) (20), so discreteness does not distinguish between the set of natural numbers and the set of integers. There is, however, a very important difference between the natural numbers and the integers, which is that the integers intuitively "go to infinity" in two directions, whereas the natural numbers do so in only one direction. The following theorem intuitively combines the discreteness of the natural numbers together with this idea of "going to infinity" in only one direction. This theorem has many uses throughout mathematics; we will use it later in this chapter. See [Blo11, Theorem 2.4.6] for a proof.

Theorem 6.2.5 (Well-Ordering Principle). *Let $A \subseteq \mathbb{N}$ be a set. If A is non-empty, then there is a unique $m \in A$ such that $m \leq a$ for all $a \in A$.*

The hard part of the proof of the Well-Ordering Principle (Theorem 6.2.5) is the existence of the number m given in the statement of the theorem; the uniqueness is very simple, following immediately from Theorem 6.2.4 (18).

Finally, we note that in various places in this chapter, we will need to use subsets of the natural numbers of the form $\{a, \ldots, b\}$. Because the concept of "..." is not in itself a rigorous one, we make this notation precise by using the following definition. There is nothing subtle in the following definition, but it is important to emphasize that writing "..." alone is not rigorous, except when we give it a rigorous meaning in specific cases, such as the following.

Definition 6.2.6. Let $a, b \in \mathbb{N}$. The sets $\{a, \ldots, b\}$ and $\{a, \ldots\}$ are defined by

$$\{a, \ldots, b\} = \{x \in \mathbb{N} \mid a \leq x \leq b\} \quad \text{and} \quad \{a, \ldots\} = \{x \in \mathbb{N} \mid a \leq x\}. \qquad \triangle$$

Because 0 is not a natural number, then technically the set $\{1, \ldots, 0\}$ is not defined. However, in order to avoid special cases in some proofs, we will allow ourselves to write the nonsensical expression "$\{1, \ldots, 0\}$," and it should be interpreted as the empty set.

For the exercises in this section, the reader should use only the properties of the natural numbers stated in this section. Subsequently, the reader should feel free to use any standard properties of the natural numbers, as we have done until now. For the rest of this chapter, we will at times refer to some of the properties of the natural numbers stated in this section to emphasize their role in various proofs.

$$\boxed{\text{Exercises}}$$

Exercise 6.2.1. **[Used in Theorem 6.3.11 and Exercise 6.3.16.]** Let $n \in \mathbb{N}$. Prove that $\{1, \ldots, n+1\} - \{1, \ldots, n\} = \{n+1\}$.

Exercise 6.2.2. **[Used in Theorem 6.6.5.]** Let $a, b \in \mathbb{N}$. Suppose that $a < b$.

(1) Let $k \in \mathbb{N}$. Prove that there is a bijective function $\{a, \ldots, b\} \rightarrow \{a+k, \ldots, b+k\}$.
(2) Let $p \in \mathbb{N}$ be the unique element such that $a + p = b$, using Theorem 6.2.4 (21). Prove that there is a bijective function $\{a, \ldots, b\} \rightarrow \{1, \ldots, p+1\}$.

Exercise 6.2.3. **[Used in Theorem 6.3.6.]** Let $b \in \mathbb{N}$. Prove that $\{1, \ldots, b\} \cup \{b+1, \ldots\} = \mathbb{N}$ and $\{1, \ldots, b\} \cap \{b+1, \ldots\} = \emptyset$

Exercise 6.2.4. **[Used in Theorem 6.4.5.]** Let H be a non-empty set, let $a, b \in H$ and let $p \colon H \times H \rightarrow H$ be a function. Prove that there is a unique function $g \colon \mathbb{N} \rightarrow H$ such that $g(1) = a$, that $g(s(1)) = b$ and that $g(s(s(n))) = p((g(n), g(s(n))))$ for all $n \in \mathbb{N}$.

The main step of the proof is to apply Definition by Recursion (Theorem 6.2.3) to the set $H \times H$, the element (a, b) and the function $k \colon H \times H \rightarrow H \times H$ defined by $k((x, y)) = (y, p(x, y))$ for all $(x, y) \in H \times H$. Use the result of that step to find the desired function g.

Exercise 6.2.5. [**Used in Theorem 6.4.3.**] Let H be a non-empty set, let $e \in H$ and let $q: H \times \mathbb{N} \to H$ be a function. Prove that there is a unique function $h: \mathbb{N} \to H$ such that $h(1) = e$, and that $h(s(n)) = q((h(n), n))$ for all $n \in \mathbb{N}$.

The main step of the proof is to apply Definition by Recursion (Theorem 6.2.3) to the set $H \times \mathbb{N}$, the element $(e, 1)$ and the function $r: H \times \mathbb{N} \to H \times \mathbb{N}$ defined by $r((x, m)) = (q(x, m), s(m))$ for all $(x, m) \in H \times \mathbb{N}$. Use the result of that step to find the desired function h.

6.3 Mathematical Induction

Mathematical induction is a very useful method of proving certain types of statements that involve the natural numbers. It is quite distinct from the informal concept of "inductive reasoning," which refers to the process of going from specific examples to more general statements, and which is not restricted to mathematics. When we use the phrase "proof by induction" we will always refer to the mathematical sort of induction, not this other use of the term.

More precisely, mathematical induction is a method that can be used to prove statements of the form $(\forall n \in \mathbb{N})(P(n))$, where $P(n)$ is a statement with a free variable n that is a natural number. For example, we will shortly prove that the statement $P(n) = $ "$8^n - 3^n$ is divisible by 5" is true for all natural numbers n. How you originally thought of trying to prove such a statement might have occurred in many ways, one of which is by playing around with various numerical examples, for example looking at $8^1 - 3^1$, at $8^2 - 3^2$, and at $8^3 - 3^3$, and then using informal "inductive reasoning" to conjecture that $8^n - 3^n$ is divisible by 5 for all natural numbers n. Such reasoning by example does not, of course, constitute a proof that this conjecture is really true. For such a proof we will use induction. The formal statement of this method, usually referred to as the Principle of Mathematical Induction, abbreviated PMI, is stated below. (For a more general look at proof by induction, see [End72, Section 1.2].)

The intuitive notion of PMI is that to show that a statement about the natural numbers is true for all natural numbers, it is sufficient to show that the statement holds for $n = 1$, and that if it holds for $n = 1$ then it holds for $n = 2$, and that if it holds for $n = 2$ then it holds for $n = 3$, continuing ad infinitum. Of course, we cannot prove infinitely many such implications, but it is sufficient to prove that the statement is true for $n = 1$, and that for an arbitrary natural number n, if the statement holds for n then it holds for $n + 1$.

Our statement of PMI is given as Theorem 6.3.1 below, and it is stated without proof, because it is just a restatement of Part (c) of the Peano Postulates (Axiom 6.2.1). Formally, the statement of PMI gives criteria that guarantee that a subset of $\mathbb{N}$ subject to certain criteria is in fact all of $\mathbb{N}$. We will see how to use these criteria in practice shortly.

Theorem 6.3.1 (**Principle of Mathematical Induction**)**.** *Let $G \subseteq \mathbb{N}$. Suppose that*

  a. $1 \in G$;

    b. *if $n \in G$, then $n+1 \in G$.*

Then $G = \mathbb{N}$.

It is important to make use of Part (b) of PMI precisely as it is written. This part has the form $P \rightarrow Q$. To show that Part (b) is true in some given situation, we do not show that P is true or that Q is true, but only that the conditional statement $P \rightarrow Q$ is true. In other words, to prove Part (b) of PMI, we do not show directly that $n \in G$, nor that $n+1 \in G$, but only that $n \in G$ implies $n+1 \in G$. This fact is what makes PMI so convenient to use.

We now have our first example of proof by induction.

Proposition 6.3.2. *If $n \in \mathbb{N}$, then $8^n - 3^n$ is divisible by 5.*

Proof. Let
$$G = \{n \in \mathbb{N} \mid 8^n - 3^n \text{ is divisible by 5}\}.$$

We will use PMI to show that $G = \mathbb{N}$, and it will then follow that $8^n - 3^n$ is divisible by 5 for all $n \in \mathbb{N}$, which is what we need to prove. First, we observe that $G \subseteq \mathbb{N}$ by definition, and hence PMI is applicable. To use PMI, we need to show two things, which are that $1 \in G$, and that if $n \in G$ then $n+1 \in G$. We start with the first of these. Observe that $8^1 - 3^1 = 5$, and therefore $8^1 - 3^1$ is indeed divisible by 5. Hence $1 \in G$, which is Part (a) of the statement of PMI.

To show Part (b) of the statement of PMI, let $n \in G$. We then need to deduce that $n+1 \in G$. Because $n \in G$, we know that $8^n - 3^n$ is divisible by 5, which means that there is some $k \in \mathbb{Z}$ such that $8^n - 3^n = 5k$ (recall the definition of divisibility in Section 2.2). To show that $n+1 \in G$ will require showing that $8^{n+1} - 3^{n+1}$ is divisible by 5; we can make use of our hypothesis that $8^n - 3^n$ is divisible by 5 in this proof. We compute

$$8^{n+1} - 3^{n+1} = 8 \cdot 8^n - 3 \cdot 3^n = (5 \cdot 8^n + 3 \cdot 8^n) - 3 \cdot 3^n$$
$$= 5 \cdot 8^n + 3 \cdot (8^n - 3^n) = 5 \cdot 8^n + 3(5k) = 5(8^n + 3k).$$

Because n and k are integers, then $8^n + 3k$ is an integer, and hence $8^{n+1} - 3^{n+1}$ is divisible by 5. It follows that $n+1 \in G$. We have therefore proved that Part (b) of the statement of PMI holds. PMI now implies that $G = \mathbb{N}$, and the result is proved.   □

The strategy used in the proof of Proposition 6.3.2 is quite typical. We first defined the set G; we then showed separately that Parts (a) and (b) of the statement of PMI each hold; and we then concluded that the desired result is true. It is often possible to make a proof by induction less cumbersome by avoiding mentioning the set G explicitly. Suppose that we are trying to show that the statement $P(n)$ holds for all $n \in \mathbb{N}$. The formal way to proceed would be to define the set G to be those natural numbers for which $P(n)$ is satisfied, and then verify that $G = \mathbb{N}$ by showing that $1 \in G$, and that $n \in G$ implies $n+1 \in G$, for all $n \in \mathbb{N}$. The less cumbersome, but just as valid, way of proceeding is to state that we are trying to prove that the statement $P(n)$ holds for all $n \in \mathbb{N}$ by induction. We then show that $P(1)$ holds, and that if $P(n)$ holds so does $P(n+1)$ for all $n \in \mathbb{N}$. The latter of these two parts is often referred

to as the "inductive step," and the assumption that $P(n)$ holds in the inductive step is often referred to as the "inductive hypothesis." It is often convenient to use clearly equivalent variants of the inductive step, for example showing that if $P(n-1)$ holds then so does $P(n)$ for all $n \in \mathbb{N}$ such that $n \geq 2$. We will see more significant variants of the inductive step shortly.

The following example of proof by induction, which we write in the less cumbersome style mentioned above, is quite standard. We note, as always, that "$\cdots$," as in the following proposition, is not completely rigorous, unless a valid definition of "$\cdots$" is provided for the particular case under consideration. Such a definition for the type of formula in the following proposition is found in Example 6.4.4 (2); we will not discuss this use of "$\cdots$" more extensively at present, to avoid a detour from our task at hand, which is proof by induction.

Proposition 6.3.3. *If $n \in \mathbb{N}$, then*

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{6.3.1}$$

Proof. We prove the result by induction on n. First, suppose that $n = 1$. Then $1 + 2 + \cdots + n = 1$, and $\frac{n(n+1)}{2} = \frac{1 \cdot (1+1)}{2} = 1$. Therefore Equation 6.3.1 holds for the case $n = 1$. Now let $n \in \mathbb{N}$. Suppose that Equation 6.3.1 holds for this n. It then follows from that equation that

$$1 + 2 + \cdots + (n+1) = \{1 + 2 + \cdots + n\} + (n+1)$$
$$= \frac{n(n+1)}{2} + (n+1)$$
$$= (n+1)\left(\frac{n}{2} + 1\right)$$
$$= \frac{(n+1)(n+2)}{2}$$
$$= \frac{(n+1)[(n+1)+1]}{2}.$$

This last expression is precisely the right-hand side of Equation 6.3.1 with $n+1$ replacing n. Hence we have proved the inductive step. Therefore Equation 6.3.1 holds for all $n \in \mathbb{N}$. □

It is important to observe that proof by induction shows only that a statement of the form $P(n)$ is true for each $n \in \mathbb{N}$. We cannot prove that $P(n)$ is true for $n = \infty$, whatever this might mean. A proof by induction does show that $P(n)$ holds for infinitely many numbers n, but each such number is a finite number. We do not consider ∞ to be a natural number (or any other type of real number), and so PMI does not apply to it.

Proof by induction is not always as straightforward as it appears. The following example is a well-known alleged "proof" by induction, which clearly cannot be valid.

Example 6.3.4. We will prove that all horses have the same color. More precisely, we will show that the statement "for any set of n horses, all the horses in the set have

the same color," is true for all $n \in \mathbb{N}$. Because there are only finitely many horses in the world, it will then follow that all existing horses have the same color. First, suppose that $n = 1$. It is certainly true that for any set of one horse, all the horses in the set have the same color. Next, suppose that the result is true for n, so that for any set of n horses, all the horses in the set have the same color. We need to show that the result is true for $n+1$. Let $\{H_1, \ldots, H_{n+1}\}$ be a set of $n+1$ horses. The set $\{H_1, \ldots, H_n\}$ has n horses, so by the inductive hypothesis all the horses in this set have the same color. On the other hand, the set $\{H_2, \ldots, H_{n+1}\}$ also has n horses, so all horses in this set have the same color. In particular, it then follows that H_n and H_{n+1} have the same color. Combining this fact with the previous observation that horses $H_1, \ldots, H_n$ all have the same color, it follows that $H_1, \ldots, H_{n+1}$ all have the same color. We have therefore proved the inductive step. Hence all horses have the same color.

The reader is asked in Exercise 6.3.5 to find the flaw in the above argument. ◊

The following example gives an application of induction to switching circuits, and hence to computers, which are built out of such circuits.

Example 6.3.5. Digital computers are based on circuits in which each input and each output is either on or off (as the result of having, or not having, electric current). These two states are often represented as 1 or 0, respectively. At its simplest, a switching circuit is a device with some number of inputs, say $x_1, \ldots, x_n$, and one output, say y; each input and the output can have values 1 or 0 only. The switching circuit takes each collection of values of the inputs, and produces a corresponding value for the output. A switching circuit can therefore be viewed as a function $f: \{0,1\}^n \rightarrow \{0,1\}$, and it can also be represented schematically by the type of diagram seen in Figure 6.3.1.

Fig. 6.3.1.
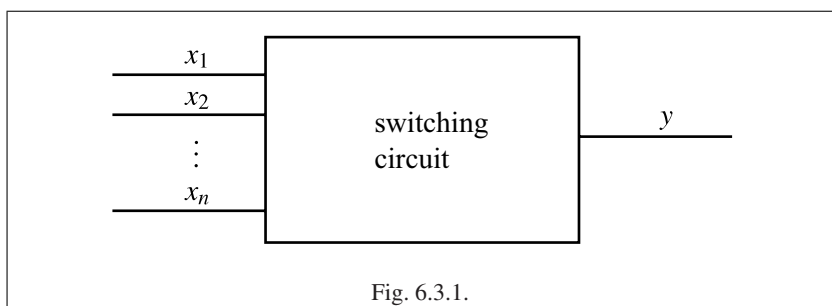
Different types of calculations require different switching circuits. For each $n \in \mathbb{N}$, there are 2^{2^n} possible switching circuits with n inputs; for the sake of keeping to the topic at hand, we will omit the proof of this fact, other than to note that it is an application of Theorem 4.5.4, combined with basic facts about the sizes of products of finite sets and the sizes of power sets of finite sets, which are proved in Sections 7.6 and 7.7, together with proof by induction. The important point to keep in mind for

the present example is that even for fairly small values of n, the number of possible switching circuits with n inputs is quite large; for example, when $n = 5$ there are over 4 billion possible switching circuits. From a manufacturing point of view, it would therefore be very unfortunate if each possible switching circuit would have to be built by an independent process. Fortunately, as we will now show, all switching circuits can be built up out a small number of simple (and familiar) components.

In Exercise 1.3.13 we discussed the notion of binary and unary logical operations, of which $\wedge$, $\vee$ and $\neg$ are examples; we also defined a new binary logical operation, denoted $\overline{\wedge}$. If we replace the values T and F that we used in our discussion of logic with the values 1 and 0, respectively, then we see that a unary logical operation is nothing but a switching circuit with one input, and a binary logical operation is a switching circuit with two inputs. It is common to denote $\neg$, $\wedge$, $\vee$ and $\overline{\wedge}$ with schematic symbols, such as those shown in Figure 6.3.2.

not   and   or   nand
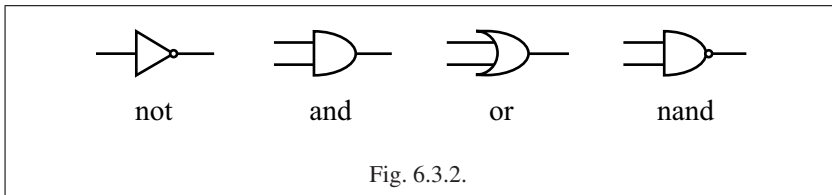
Fig. 6.3.2.

We now prove by induction that every switching circuit can be built up out of $\wedge$, $\vee$ and $\neg$ circuits. The induction is on n, the number of inputs in our switching circuits. That the result is true for $n = 1$ and for $n = 2$ follows immediately from Exercise 1.3.13 (2). Now suppose that the result is true for all switching circuits with n inputs. Let C be a switching circuit with $n + 1$ inputs, labeled $x_1, \ldots, x_{n+1}$. We define two new switching circuits C_0 and C_1 as follows. Let C_0 be the switching circuit with inputs $x_1, \ldots, x_n$, such that the output of C_0 for each collection of values of $x_1, \ldots, x_n$ equals the output of C for the same values of $x_1, \ldots, x_n$ and the value $x_{n+1} = 0$. Define C_1 similarly, using $x_{n+1} = 1$. The reader can then verify that the circuit shown in Figure 6.3.3 has the same output as C for each collection of values of $x_1, \ldots, x_{n+1}$. Because C_0 and C_1 both have n inputs, it follows from the inductive hypothesis that each can be constructed out of $\wedge$, $\vee$ and $\neg$ circuits. Hence C can be constructed out of $\wedge$, $\vee$ and $\neg$ circuits. By induction, it follows that every switching circuit can be made out of our three building blocks. Even better, Exercise 1.3.13 (3) shows that every switching circuit can be built out of only $\overline{\wedge}$ circuits.

See [LP98, Sections 2.7 and 2.8] or [Fab92] for more about switching circuits.
◊

There are various alternative versions of PMI, each of which is useful in certain situations where PMI might not be directly applicable. There do not seem to be standard names for these variants. Different texts use terms such as "Extended Principle of Mathematical Induction," "Second Principle of Mathematical Induction," and the like. We will simply call them Principle of Mathematical Induction—Variant 1,

Variant 2 and Variant 3, respectively, using the abbreviations PMI-V1, PMI-V2 and PMI-V3. All three variants work similarly to PMI, in that they all have two parts, the second of which is the inductive step.
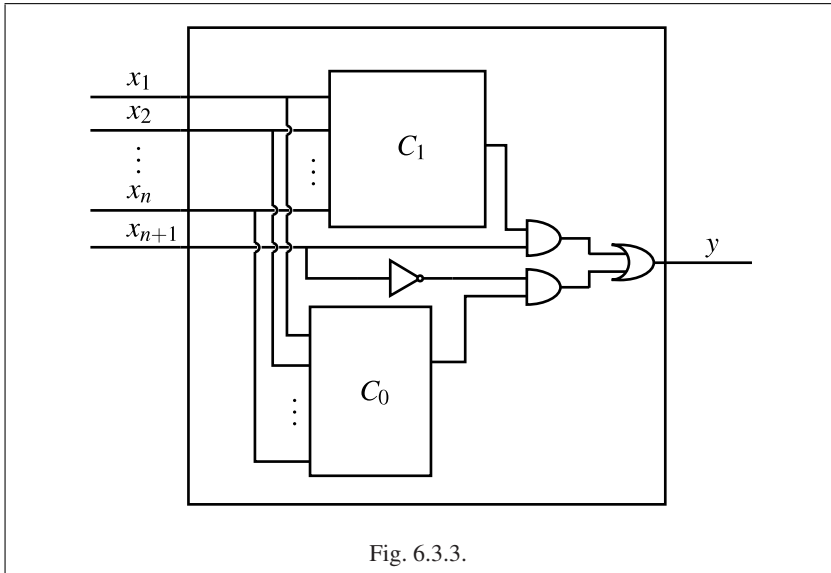
Fig. 6.3.3.

The first of the variants on PMI is useful when we wish to prove that a statement $P(n)$ is true for all natural numbers n such that $n \geq k_0$, for some given natural number k_0.

Theorem 6.3.6 (Principle of Mathematical Induction—Variant 1). *Let $G \subseteq \mathbb{N}$, and let $k_0 \in \mathbb{N}$. Suppose that*

   a. $k_0 \in G$;
   b. *if $n \in \{k_0, \dots\}$ and $n \in G$, then $n+1 \in G$.*

Then $\{k_0, \dots\} \subseteq G$.

Proof. First, suppose that $k_0 = 1$. It then follows from Theorem 6.2.4 (12) that the condition "$n \geq k_0$" is true for all $n \in \mathbb{N}$. In particular, we see that $\{k_0, \dots\} = \mathbb{N}$. Because $G \subseteq \mathbb{N}$, the statement "$\{k_0, \dots\} \subseteq G$" is then equivalent to "$G = \mathbb{N}$." It follows that when $k_0 = 1$, the statement of PMI-V1 is equivalent to the statement of PMI (Theorem 6.3.1), and so there is nothing to prove in this case. From now on assume that $k_0 \neq 1$. By Theorem 6.2.4 (12) (21) there is some $b \in \mathbb{N}$ such that $b+1 = k_0$.

Let $G' = \{1, \dots, b\} \cup G$. We will show that $G' = \mathbb{N}$. It will then follow that $\{1, \dots, b\} \cup G = \mathbb{N}$, and hence that $\{k_0, \dots\} \subseteq G$ by using Exercise 6.2.3 and Exercise 3.3.10.

We now use PMI to show that $G' = \mathbb{N}$. By definition we know that $1 \in G'$. Suppose that $g \in G'$. We will show that $g + 1 \in G'$, and the proof will be complete. By Theorem 6.2.4 (16) we know that precisely one of the following holds: either $g < b$, or $g = b$, or $g > b$. We treat each case separately.

Case 1: Suppose that $g < b$. Then $g + 1 \le b$ by Theorem 6.2.4 (20). By Part (12) of the same theorem, we know that $1 \le g + 1$, and hence $g + 1 \in \{1, \ldots, b\} \subseteq G'$.

Case 2: Suppose that $g = b$. Then $g + 1 = b + 1 = k_0$. Hence $g + 1 \in G \subseteq G'$.

Case 3: Suppose that $g > b$. Then $g \not\le b$ by Theorem 6.2.4 (16), and hence $g \notin \{1, \ldots, b\}$. Because $g \in G' = \{1, \ldots, b\} \cup G$, it follows that $g \in G$. Moreover, because $g > b$, we know by Theorem 6.2.4 (20) that $g \ge b + 1 = k_0$, and hence $g \in \{k_0, \ldots\}$. We now use the hypothesis on G to see that $g + 1 \in G \subseteq G'$. $\qquad \square$

Observe that in PMI-V1 we do not deduce that $G = \mathbb{N}$, only that $\{k_0, \ldots\} \subseteq G$. It might be the case that the set G contains numbers less than k_0, but we cannot deduce that from the statement of PMI-V1. The following proof is an example of the use of PMI-V1. As always, note the difference between the scratch work and the actual proof.

Proposition 6.3.7. *If $n \in \mathbb{N}$ and $n \ge 5$, then $4^n > n^4$.*

Scratch Work. For the case $n = 5$, it is easy to verify that $4^5 > 5^4$. Now suppose that we know the result for some n, so that $4^n > n^4$. We want to deduce that $4^{n+1} > (n+1)^4$. By brute force multiplication, or using the binomial formula (Theorem 7.7.14), we see that $(n+1)^4 = n^4 + 4n^3 + 6n^2 + 4n + 1$. Because this expression has a number of pieces, it might be helpful to write $4^{n+1} = 4 \cdot 4^n = 4^n + 4^n + 4^n + 4^n$. Because we know that $4^n > n^4$, it would suffice to show the three inequalities $4^n > 4n^3$ and $4^n > 6n^2$ and $4^n > 4n + 1$ hold. To show these inequalities, we can make use of the fact that $n \ge 5$, as well as the fact that $4^n > n^4$. First, we observe that $4n^3 < 5n^3 \le n \cdot n^3 = n^4 < 4^n$. Next, we observe that $6n^2 < 5^2 n^2 \le n^2 n^2 = n^4 < 4^n$. Finally, we have $4n + 1 < 4n + n = 5n \le n \cdot n < n^4 < 4^n$. Putting all these observations together will do the trick. $\qquad ///$

Proof. We prove the result by induction on n, making use of PMI-V1 with $k_0 = 5$. First, suppose that $n = 5$. Then $4^5 = 1024 > 625 = 5^4$. Hence the desired result holds when $n = 5$. Now suppose that the result holds for some $n \in \mathbb{N}$ such that $n \ge 5$, which means that $4^n > n^4$ for this n. We start with three preliminary observations, which are

$$4^n > n^4 > n^2 \ge 5n = 4n + n > 4n + 1,$$

and

$$4^n > n^4 \ge 5^2 n^2 > 6n^2,$$

and

$$4^n > n^4 > 4n^3.$$

Combining the three inequalities with the inductive hypothesis we obtain

$$4^{n+1} = 4 \cdot 4^n = 4^n + 4^n + 4^n + 4^n > n^4 + 4n^3 + 6n^2 + (4n + 1) = (n+1)^4.$$

Therefore the desired result holds for $n+1$. The proof is then complete by PMI-V1. $\qquad\square$

The second variant on PMI again reverts to starting at $n=1$, and to deducing that the set G equals all of $\mathbb{N}$, but it has a slightly different type of inductive step than either PMI or PMI-V1.

Theorem 6.3.8 (**Principle of Mathematical Induction—Variant 2**). *Let $G \subseteq \mathbb{N}$. Suppose that*

    a. $1 \in G$;
    b. if $n \in \mathbb{N}$ and $\{1,\ldots,n\} \subseteq G$, then $n+1 \in G$.

Then $G = \mathbb{N}$.

Proof. Suppose that $G \neq \mathbb{N}$; we will derive a contradiction. Let $H = \mathbb{N} - G$. Because $H \subseteq \mathbb{N}$ and $H \neq \emptyset$, the Well-Ordering Principle (Theorem 6.2.5) implies that there is some $m \in H$ such that $m \leq h$ for all $h \in H$. Because $1 \in G$ we know that $1 \notin H$, and therefore $m \neq 1$. By Theorem 6.2.4 (12) (21) there is some $b \in \mathbb{N}$ such that $b+1 = m$.

Let $p \in \{1,\ldots,b\}$. It follows that $p \leq b < b+1 = m$ by Theorem 6.2.4 (11). Part (16) of the same theorem implies that $p \ngeq m$. Therefore $p \notin H$, and so $p \in G$. We have therefore shown that $\{1,\ldots,b\} \subseteq G$. Part (b) of the hypothesis on G then says that $b+1 \in G$, which means that $m \in G$. This last statement is a contradiction to the fact that $m \in H$. We conclude that $G = \mathbb{N}$. $\qquad\square$

When using PMI-V2, the inductive step involves showing that if the desired statement is assumed to hold for all values in $\{1,\ldots,n\}$, then it holds for $n+1$. This method contrasts with PMI and PMI-V1, where we showed that if the statement is assumed to hold only for n, then it holds for $n+1$. It might appear as if we are unfairly making life easier for ourselves when we use PMI-V2, by allowing a larger hypothesis in order to derive the same conclusion, but PMI-V2 has been derived rigorously from PMI, and so we are free to use it whenever we need to. (The proof of PMI-V2 does not appear to make use of PMI, but the latter is nonetheless used implicitly, because it is needed for the proof of the Well-Ordering Principle (Theorem 6.2.5); see [Blo11, Theorem 2.4.6] for details.)

Our third variant on PMI combines the first two variants.

Theorem 6.3.9 (**Principle of Mathematical Induction—Variant 3**). *Let $G \subseteq \mathbb{N}$, and let $k_0 \in \mathbb{N}$. Suppose that*

    a. $k_0 \in G$;
    b. if $n \in \{k_0,\ldots\}$ and $\{k_0,\ldots,n\} \subseteq G$, then $n+1 \in G$.

Then $\{k_0,\ldots\} \subseteq G$.

Proof. Left to the reader in Exercise 6.3.13. $\qquad\square$

An example of using PMI-V3 is the proof of the following theorem, which is a basic tool in number theory. An examination of the proof reveals why PMI-V3 is used in this case rather than PMI-V1. Recall the definition of prime numbers in Definition 2.3.6.

Theorem 6.3.10. *Let $n \in \mathbb{N}$. Suppose that $n \geq 2$. Then n is either a prime number or a product of finitely many prime numbers.*

Proof. We will use PMI-V3 with $k_0 = 2$. First, suppose that $n = 2$. Because 2 is a prime number, the desired result is true for $n = 2$. Now let $n \in \mathbb{N}$. Suppose that $n \geq 2$, and that the desired result holds for all natural numbers in the set $\{2, \ldots, n\}$; that is, we assume that each of the numbers in $\{2, \ldots, n\}$ is either a prime number or a product of finitely many prime numbers. We need to show that $n + 1$ is either a prime number or a product of finitely many prime numbers. There are two cases, depending upon whether or not $n + 1$ is a prime number. If $n + 1$ is a prime number, then there is nothing to prove. Now assume that $n + 1$ is not a prime number. Then there are natural numbers a and b such that $n + 1 = ab$, and that $1 < a < n + 1$ and $1 < b < n + 1$. Therefore $a, b \in \{2, \ldots, n\}$. By the inductive hypothesis we know that each of a and b is either a prime number or a product of finitely many prime numbers. It now follows that $n + 1 = ab$ is the product of finitely many prime numbers. $\square$

The above result can be proved for all integers (and not just natural numbers), and it can also be proved that the decomposition into prime numbers is unique. The version of the theorem for integers that includes both existence and uniqueness is known as the Fundamental Theorem of Arithmetic. See [Ros05, Section 3.5] for details.

We conclude this section with the following somewhat technical theorem about functions between sets of the form $\{1, \ldots, n\}$; we will need this theorem when we discuss properties of finite sets in Section 6.6.

Theorem 6.3.11. *Let $n, k \in \mathbb{N}$.*

1. *Let $f \colon \{1, \ldots, n\} \to \mathbb{N}$ be a function. Then there is some $q \in \{1, \ldots, n\}$ such that $f(q) \geq f(i)$ for all $i \in \{1, \ldots, n\}$.*
2. *Let $S \subseteq \{1, \ldots, n\}$ be a non-empty subset. Then there is a bijective function $g \colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $g(S) = \{1, \ldots, r\}$ for some $r \in \mathbb{N}$ such that $r \leq n$. If S is a proper subset of $\{1, \ldots, n\}$, then $r < n$.*
3. *Let $f \colon \{1, \ldots, n\} \to \{1, \ldots, k\}$ be a function. If f is bijective, then $n = k$. If f is injective but not surjective, then $n < k$.*

Proof. We will prove Part (3), leaving the rest to the reader in Exercise 6.3.16.

(3). First, suppose that f is bijective. We prove the result by induction on k, where for each k we will assume that n is arbitrary. Suppose that $k = 1$. Then $\{1, \ldots, k\} = \{1\}$. If $p \colon \{1, \ldots, n\} \to \{1, \ldots, k\}$ is a bijective function, then $\{1, \ldots, n\}$ must also have one element, which implies that $n = 1$. Hence $n = k$.

Now suppose that the result is true for some $k \in \mathbb{N}$. Let $h \colon \{1, \ldots, n\} \to \{1, \ldots, k+1\}$ be a function. Suppose that h is bijective. We know that $k + 1 > k \geq 1$. It follows that

$\{1,\ldots,k+1\}$ has more than one element, and hence it must be the case that $n > 1$ in order for h to be bijective. By Theorem 6.2.4 (21) we see that there is some $q \in \mathbb{N}$ such that $q+1 = n$. There are now two cases.

Suppose first that $h(n) = k+1$. Let $\hat{h}\colon \{1,\ldots,q\} \to \{1,\ldots,k\}$ be defined by $\hat{h}(a) = h(a)$ for all $a \in \{1,\ldots,q\}$, which makes sense because of Exercise 6.2.1 and the fact that h is injective. Because h is bijective, and because $h(n) = k+1$, it follows that $\hat{h}$ is bijective. The inductive hypothesis applied to $\hat{h}$ implies that $q = k$. It follows that $n = q+1 = k+1$. Hence the result holds for $k+1$.

Suppose second that $h(n) \neq k+1$. Then, using Exercise 6.2.1 again, together with the fact that h is bijective, we deduce that $k+1 = h(s)$ for a unique $s \in \{1,\ldots,q\}$. Let $\tilde{h}\colon \{1,\ldots,n\} \to \{1,\ldots,k+1\}$ be defined by

$$\tilde{h}(a) = \begin{cases} h(n), & \text{if } a = s \\ k+1, & \text{if } a = n \\ h(a), & \text{otherwise.} \end{cases}$$

Then $\tilde{h}$ is bijective, and $\tilde{h}(n) = k+1$. By applying the previous case to $\tilde{h}$, we deduce that $n = k+1$. The proof in the case that f is bijective is now complete.

Next, suppose that f is injective but not surjective. Then $f(\{1,\ldots,n\}) \subsetneqq \{1,\ldots,k\}$. Let $\hat{f}\colon \{1,\ldots,n\} \to f(\{1,\ldots,n\})$ be defined by $\hat{f}(a) = f(a)$ for all $a \in \{1,\ldots,n\}$. Then $\hat{f}(\{1,\ldots,n\}) = f(\{1,\ldots,n\})$, and $\hat{f}$ is bijective. By Part (2) of this theorem there is a bijective function $g\colon \{1,\ldots,k\} \to \{1,\ldots,k\}$, such that $g(f(\{1,\ldots,n\})) = \{1,\ldots,r\}$ for some $r \in \mathbb{N}$ such that $r < k$. Let $\hat{g}\colon f(\{1,\ldots,n\}) \to \{1,\ldots,r\}$ be defined by $\hat{g}(a) = g(a)$ for all $a \in f(\{1,\ldots,n\})$. Then $\hat{g}$ is bijective. It follows from Exercise 4.3.5 that $(\hat{g} \circ \hat{f})(\{1,\ldots,n\}) = \hat{g}(\hat{f}(\{1,\ldots,n\})) = \hat{g}(f(\{1,\ldots,n\})) = \{1,\ldots,r\}$. Because $\hat{f}$ and $\hat{g}$ are both bijective, then $\hat{g} \circ \hat{f}\colon \{1,\ldots,n\} \to \{1,\ldots,r\}$ is bijective by Lemma 4.4.4 (3). It now follows from what we proved about bijective functions that $n = r$. We deduce that $n < k$. $\qquad\square$

<div align="center">

Exercises

</div>

Exercise 6.3.1. Prove that each of the following formulas holds for all $n \in \mathbb{N}$.

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

(2) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(3) $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$.

(4) $1^3 + 3^3 + \cdots + (2n-1)^3 = n^2(2n^2-1)$.

(5) $1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$.

(6) $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.

Exercise 6.3.2. Prove that $1 + 2n \leq 3^n$ for all $n \in \mathbb{N}$.

Exercise 6.3.3. Let $a, b \in \mathbb{N}$. Prove that $a^n - b^n$ is divisible by $a - b$ for all $n \in \mathbb{N}$.

Exercise 6.3.4. [Used in Theorem 6.6.7.] Let $f: \mathbb{N} \to \mathbb{N}$ be a function. Suppose that $f(n) < f(n+1)$ for all $n \in \mathbb{N}$. Prove that $f(n) \geq n$ for all $n \in \mathbb{N}$. Be explicit about which properties of $\mathbb{N}$, as stated in Section 6.2, you are using.

Exercise 6.3.5. [Used in Example 6.3.4.] Find the flaw in Example 6.3.4.

Exercise 6.3.6. For which values of $n \in \mathbb{N}$ does the inequality $n^2 - 9n + 19 > 0$ hold? Prove your answer by induction.

Exercise 6.3.7. Prove that $\left(1 + \frac{1}{n}\right)^n < n$ for all $n \in \mathbb{N}$ such that $n \geq 3$.

Exercise 6.3.8. Prove that $7n < 2^n$ for all $n \in \mathbb{N}$ such that $n \geq 6$.

Exercise 6.3.9. Prove $3^n > n^3$ for all $n \in \mathbb{N}$ such that $n \geq 4$.

Exercise 6.3.10. Prove that

$$\sum_{i=1}^{n} \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$$

for all $n \in \mathbb{N}$.

Exercise 6.3.11. Prove that

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

for all $n \in \mathbb{N}$ such that $n \geq 2$. (The symbol $\prod$ denotes the product of all the terms.)

Exercise 6.3.12. Prove that

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > \sqrt{n}$$

for all $n \in \mathbb{N}$ such that $n \geq 2$.

Exercise 6.3.13. [Used in Theorem 6.3.9.] Prove Theorem 6.3.9.

Exercise 6.3.14. [Used in Theorem 6.6.9 and Exercise 6.6.12.] Let $f: \mathbb{N} \to \mathbb{N} \cup \{0\}$ be a function. Suppose that $f(1) = 0$, and that if $n < m$ then $f(n) < f(m)$, for all $n, m \in \mathbb{N}$. Prove that for each $x \in \mathbb{N}$, there are unique $n, p \in \mathbb{N}$ such that $f(n) < x \leq f(n+1)$ and $x = f(n) + p$. (If, for example, we let $b \in \mathbb{N}$, and we use the function f defined by $f(n) = (n-1)b$ for all $n \in \mathbb{N}$, then we obtain a variant of the Division Algorithm (Theorem A.5).)

Exercise 6.3.15. [Used in Theorem 6.4.8.] Let $p \in \mathbb{N}$, and let $G \subseteq \mathbb{N}$. Suppose that

    a. $1 \in G$;
    b. if $n \in \{1, \ldots, p-1\}$ and $\{1, \ldots, n\} \subseteq G$, then $n+1 \in G$.

Prove that $\{1, \ldots, p\} \subseteq G$.

Exercise 6.3.16. [Used in Theorem 6.3.11.] Prove Theorem 6.3.11 (1) (2).

<div align="right">[Use Exercise 6.2.1.]</div>

Exercise 6.3.17. Let $k, m \in \mathbb{N}$, and let $f \colon \{1, \ldots, m\} \to \{1, \ldots, k\}$ be a function. Prove that if $m > k$, then f is not injective. A combinatorial interpretation of this fact is known as the **Pigeonhole Principle**, which says that if m objects are placed in k boxes, where $m > k$, then there will be a box with more than one object in it. Though this principle may seem innocuous, it is very important in combinatorics. See [Rob84, Section 8.1] for further discussion and applications.

6.4 Recursion

Consider the familiar sequence $1, 2, 4, 8, 16, \ldots$. If we let a_n denote the nth term of the sequence, then $a_n = 2^{n-1}$ for all $n \in \mathbb{N}$. Such a formula describes each term of the sequence explicitly in terms of n, and is a very convenient way of describing the sequence. There is, however, another useful way of describing this sequence, which is by stating that $a_1 = 1$, and that $a_{n+1} = 2a_n$ for all $n \in \mathbb{N}$. Such a description is called a **recursive** description of the sequence. Recursion, of which we will see some interesting examples shortly, is important not only in mathematics, but also in logic, and in the application of logic to computer science; see [Rob86] or [DSW94, Chapter 3] for details. See [End72, Section 1.2] for a more general look at the mathematical approach to recursion, and see [Rob84, Section 5.1] for various applied uses of recursion.

Given a sequence for which we already have an explicit formula for each a_n in terms of n, it can be useful to find a recursive formula, but there is no question that the sequence exists. What about a sequence for which we have only a recursive description, but no explicit formula? For example, suppose that we have the recursive description $c_1 = 4$, and $c_{n+1} = 3 + 2c_n$ for all $n \in \mathbb{N}$. Is there a sequence $c_1, c_2, c_3, \ldots$ satisfying such a description? That is, does this description actually define a sequence? It does appear intuitively as if there is such a sequence, because we can proceed "inductively," producing one element at a time. We know that $c_1 = 4$. We then compute $c_2 = 3 + 2c_1 = 3 + 2 \cdot 4 = 11$, and $c_3 = 3 + 2c_2 = 3 + 2 \cdot 11 = 25$, and so on. We could continue indefintely in this way, and it would seem that the sequence $c_1, c_2, c_3, \ldots$ is defined for all $n \in \mathbb{N}$. Our intuition will turn out to be correct, and the sequence is indeed defined, and moreover uniquely defined, for all $n \in \mathbb{N}$. In fact, we will give an explicit formula for this sequence in Example 6.4.2.

However, although the method of definition by recursion for defining sequences can be made completely rigorous, it is not as simple as we made it appear in the previous paragraph. Just saying "proceed inductively" is not satisfactory. Proof by induction, as discussed in Section 6.3, works for something that is already defined; here, by contrast, we are defining something, so proof by induction is not applicable. Of course, once something is defined by recursion, it is very common to prove things about it using induction.

There are a number of variations of the process of definition by recursion, the most basic of which is as follows. Suppose that we are given a number $b \in \mathbb{R}$, and a function $h \colon \mathbb{R} \to \mathbb{R}$. We then want to define a sequence $a_1, a_2, \ldots$ such that $a_1 = b$ and that $a_{n+1} = h(a_n)$ for all $n \in \mathbb{N}$. To be more precise, recall from Example 4.5.2 (4)

that the formal definition of a sequence of real numbers is simply a function $f\colon \mathbb{N} \to \mathbb{R}$, which can be converted to the more standard notation for sequences by letting $a_n = f(n)$ for all $n \in \mathbb{N}$. Although the sequences discussed in Example 4.5.2 (4) were in $\mathbb{R}$, the same approach applies to sequences in any set, so that a sequence in the set A is simply a function $f\colon \mathbb{N} \to A$.

We can now state the theorem that guarantees the validity of definition by recursion. We have in fact already seen this theorem in Section 6.2, stated as Theorem 6.2.3, and we are simply restating it here in a form that is more familiar and easy to use.

Theorem 6.4.1 (**Definition by Recursion**). *Let A be a set, let $b \in A$ and let $k\colon A \to A$ be a function. Then there is a unique function $f\colon \mathbb{N} \to A$ such that $f(1) = b$, and that $f(n+1) = k(f(n))$ for all $n \in \mathbb{N}$.*

Stated more informally, Definition by Recursion (Theorem 6.4.1) says that if A is a set, if $b \in A$ and if $k\colon A \to A$ is a function, then there is a unique sequence $a_1, a_2, a_3, \ldots$ in A such that $a_1 = b$, and that $a_{n+1} = k(a_n)$ for all $n \in \mathbb{N}$.

Example 6.4.2.

(1) We previously asked whether there is a sequence that satisfies the conditions $c_1 = 4$, and $c_{n+1} = 3 + 2c_n$ for all $n \in \mathbb{N}$. We can now treat this example rigorously. Let $b = 4$, and let $h\colon \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = 3 + 2x$ for all $x \in \mathbb{R}$. Then Definition by Recursion (Theorem 6.4.1) tells us that there is a unique function $f\colon \mathbb{N} \to \mathbb{R}$ such that $f(1) = 4$, and that $f(n+1) = 3 + 2f(n)$ for all $n \in \mathbb{N}$. If we let $c_n = f(n)$ for all $n \in \mathbb{N}$, then the sequence $c_1, c_2, c_3, \ldots$ satisfies the conditions $c_1 = 4$, and $c_{n+1} = 3 + 2c_n$ for all $n \in \mathbb{N}$.

Definition by Recursion tells us only that the sequence $c_1, c_2, c_3, \ldots$ with the desired properties exists; it does not give us an explicit formula for this sequence. It is not always possible to find an explicit formula for every sequence defined by recursion, although in the present case such a formula can be found. By calculating the first few terms of the sequence, and a bit of trial and error, it is possible to guess the formula $c_n = 7 \cdot 2^{n-1} - 3$ for all $n \in \mathbb{N}$. To prove that this formula holds, we use PMI. First, we show that the formula holds for $n = 1$, which is seen by computing $7 \cdot 2^{1-1} - 3 = 4$, and observing that $c_1 = 4$. Next, suppose that the result holds for some $n \in \mathbb{N}$, which means that $c_n = 7 \cdot 2^{n-1} - 3$ for this n. We then show that the result holds for $n+1$, which we accomplish by computing

$$c_{n+1} = 3 + 2c_n = 3 + 2\{7 \cdot 2^{n-1} - 3\} = 7 \cdot 2^{(n+1)-1} - 3.$$

It then follows from PMI that the formula holds for all $n \in \mathbb{N}$.

(2) Let A be a non-empty set, and let $f\colon A \to A$ be a function. For any $n \in \mathbb{N}$, we would like to define a function, denoted f^n, by the formula

$$f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

However, anything involving "$\cdots$" is not rigorous, unless the "$\cdots$" is an abbreviation for something that has been rigorously defined, which we can do in the present case by using Definition by Recursion.

Recall the notation $\mathcal{F}(A,A)$ defined in Section 4.5. Let $k\colon \mathcal{F}(A,A) \to \mathcal{F}(A,A)$ be defined by $k(g) = f \circ g$ for all $g \in \mathcal{F}(A,A)$. We can then apply Definition by Recursion (Theorem 6.4.1) to the set $\mathcal{F}(A,A)$, the element $f \in \mathcal{F}(A,A)$ and the function $k\colon \mathcal{F}(A,A) \to \mathcal{F}(A,A)$, and we deduce that there is a unique function $\phi\colon \mathbb{N} \to \mathcal{F}(A,A)$ such that $\phi(1) = f$ and that $\phi(n+1) = k(\phi(n)) = (f \circ \phi)(n)$ for all $n \in \mathbb{N}$. We now simply let the notation "f^n" be defined to mean $\phi(n)$, for all $n \in \mathbb{N}$. Then $f^1 = f$, and $f^{n+1} = f \circ f^n$ for all $n \in \mathbb{N}$, just as expected. We refer to f^n as the n-**fold iteration** of f. This topic was discussed briefly in Exercise 4.4.20 and Exercise 4.4.21, where we assumed that f^n was defined intuitively, because we did not yet have Definition by Recursion at our disposal. Iterations of functions are widely used in mathematics, and in particular are central to the study of dynamical systems and chaos; see [ASY97].   ◇

In the formulation of Definition by Recursion we have used so far, we defined a sequence $a_1, a_2, a_3, \ldots$ in a set A by specifying that $a_1 = b$, and that $a_{n+1} = k(a_n)$ for all $n \in \mathbb{N}$, where b and k are the appropriate objects. In particular, each a_{n+1} is a function of a_n alone. In some situations, however, we might need a more complicated formula for a_{n+1}. For example, suppose that we want to define a sequence by specifying that $a_1 = 1$, and $a_{n+1} = n + a_n$ for all $n \in \mathbb{N}$. Such a definition of a sequence is not covered by Definition by Recursion (Theorem 6.4.1), though it does turn out to produce a well-defined sequence, which starts $1, 2, 4, 7, 11, \ldots$. The following result, a variant of Definition by Recursion, shows that everything works out as expected.

Theorem 6.4.3. *Let A be a set, let $b \in A$ and let $t\colon A \times \mathbb{N} \to A$ be a function. Then there is a unique function $g\colon \mathbb{N} \to A$ such that $g(1) = b$, and that $g(n+1) = t((g(n),n))$ for all $n \in \mathbb{N}$.*

Proof. This theorem is just a restatement of Exercise 6.2.5.   □

Example 6.4.4.

(1) We want to define a sequence by specifying that $a_1 = 1$, and that $a_{n+1} = (n+1)a_n$ for all $n \in \mathbb{N}$. Using Theorem 6.4.3 with $b = 1$, and with $t\colon \mathbb{R} \times \mathbb{N} \to \mathbb{R}$ defined by $t(x,m) = (m+1)x$ for all $(x,m) \in \mathbb{R} \times \mathbb{N}$, we see that there is a unique sequence satisfying these conditions. This sequence starts $1, 2, 6, 24, 120, \ldots$, and consists of the familiar factorial numbers. We use the symbol $n!$ to denote a_n, for all $n \in \mathbb{N}$. The reader might wonder whether we could have dispensed with the Definition by Recursion entirely, and have simply defined a_n to be $n!$ for all $n \in \mathbb{N}$, but that would be doing things backwards. The notation $n!$ is informally defined by writing $n! = n(n-1)(n-2)\cdots 2 \cdot 1$, but this is not a rigorous definition, because of the appearance of "$\cdots$." The formal way to define $n!$ is to say that it is the value of a_n for the sequence we have defined by recursion; doing so then gives a rigorous meaning to the $\cdots$ appearing in the expression $n(n-1)(n-2)\cdots 2 \cdot 1$. From Definition by Recursion, we deduce immediately that $(n+1)! = (n+1)n!$ for all $n \in \mathbb{N}$, because that is the result of substituting $n!$ for a_n in the condition $a_{n+1} = (n+1)a_n$.

(2) In Proposition 6.3.3 we wrote the expression "$1 + 2 + \cdots + n$," and in Exercise 6.3.1 we had similar expressions, such as "$1^2 + 2^2 + \cdots + n^2$." We now

use Theorem 6.4.3 to give this use of "$\cdots$" a rigorous definition. In general, let $f\colon \mathbb{N} \to \mathbb{R}$ be a function. We want to give a rigorous meaning to the expression "$f(1) + f(2) + \cdots + f(n)$."

Let $q\colon \mathbb{R} \times \mathbb{N} \to \mathbb{R}$ be defined by $q((x,n)) = x + f(n+1)$ for all $(x,n) \in \mathbb{R} \times \mathbb{N}$. We then apply Theorem 6.4.3 to the set $\mathbb{R}$, the element $f(1) \in \mathbb{R}$ and the function q, and we deduce that there is a unique function $h\colon \mathbb{N} \to \mathbb{R}$ such that $h(1) = f(1)$, and that $h(n+1) = q((h(n), n)) = h(n) + f(n+1)$ for all $n \in \mathbb{N}$. We now let the notation "$f(1) + f(2) + \cdots + f(n)$" be defined to mean $h(n)$, for all $n \in \mathbb{N}$. $\diamond$

Our next version of Definition by Recursion is used for a particularly interesting sequence, namely, the well-known Fibonacci sequence, which starts

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 \ldots.$$

The numbers in this sequence are referred to as Fibonacci numbers, named after the medieval mathematician Fibonacci (also known as Leonardo of Pisa), who discovered these numbers when investigating a mathematical problem concerning rabbits. See [Hun70, Chapter 12] for details.

The Fibonacci numbers arise in a variety of unexpected places, such as in phyllotaxis, which is the study of certain numbers that arise in plants, for example, the numbers of petals in flowers, the numbers of spirals in pine cones, and others. See Figure 6.4.1 for some of the spirals formed by the seeds of a sunflower; it often happens that the number of spirals in each direction is a Fibonacci number (we note that the number of spirals in each of the two directions are not necessarily equal). See [Cox61, Chapter 11] and [Rob84, Section 5.1.2] for further discussion and references to the use of Fibonacci numbers in phyllotaxis and other areas. Why the Fibonacci numbers show up in the study of plants appears not to be known, as stated in [Rob84, pp. 202–203]. On the other hand, in [Tho59, Chapter XIV], an earlier study of growth, form and shape in biological phenomena, it is claimed that there are mathematical reasons for the Fibonacci numbers appearing in pine cones and the like; the reader should decide for herself what to make of that author's arguments. Even he says, however, "We come then without much ado to the conclusion that while the Fibonacci series stares us in the face in the fir-cone, it does so for mathematical reasons; and its supposed usefulness, and the hypothesis of its introduction into plant structure through natural selection, are matters which deserve no place in the plain study of botanical phenomena. As Sachs shrewdly recognized years ago, all such speculations as these hark to a school of mystical idealism."

What concerns us here is not biology but the mathematical properties of the Fibonacci numbers. Some mathematically serious treatments of the Fibonacci numbers are found in [Knu73, Section 1.2.8], [GKP94, Section 6.6] and [HHP97, Chapter 3]. See [Gar87] or [Hun70] for slightly more offbeat discussions of the Fibonacci numbers.

Let the elements of the Fibonacci sequence be denoted $F_1, F_2, \ldots$. An examination of the sequence reveals its basic pattern, which is $F_{n+2} = F_{n+1} + F_n$ for all $n \in \mathbb{N}$. Formally, the Fibonacci sequence is the unique sequence specified by $F_1 = 1$, and $F_2 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n \in \mathbb{N}$. This type of definition of a sequence is

not covered by either Theorem 6.4.1 or Theorem 6.4.3, but the following variant of these theorems suffices.
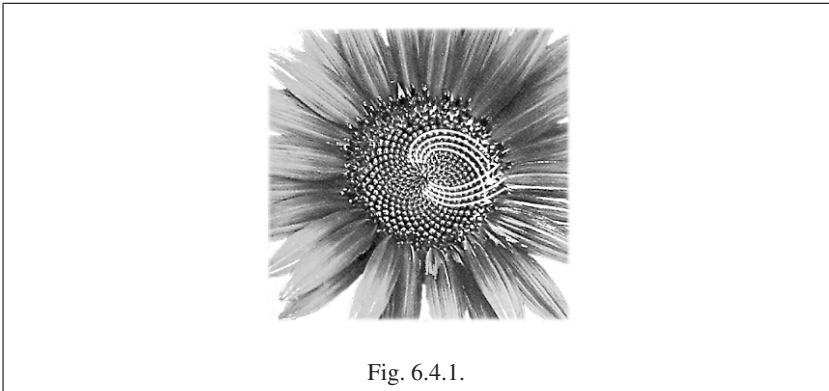
Fig. 6.4.1.

Theorem 6.4.5. *Let A be a set, let $a, b \in A$ and let $p\colon A \times A \to A$ be a function. Then there is a unique function $f\colon \mathbb{N} \to A$ such that $f(1) = a$, that $f(2) = b$ and that $f(n+2) = p((f(n), f(n+1)))$ for all $n \in \mathbb{N}$.*

Proof. This theorem is just a restatement of Exercise 6.2.4. □

The Fibonacci sequence is defined using Theorem 6.4.5 with $a = 1$, with $b = 1$, and with $p\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $p((x, y)) = x + y$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. The following proposition gives a few examples of formulas involving the sums and products of Fibonacci numbers. For more such formulas (of which there are remarkably many), see [Knu73, Section 1.2.8 and exercises] and [GKP94, Section 6.6], as well as the exercise at the end of this section.

Proposition 6.4.6. *Let $n \in \mathbb{N}$.*

1. *$F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.*
2. *$F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$.*
3. *If $n \geq 2$, then $(F_n)^2 - F_{n+1} F_{n-1} = (-1)^{n+1}$.*

Proof. We will prove Part (3), leaving the rest to the reader in Exercise 6.4.6.

(3). We use induction, using PMI-V3 with $k_0 = 2$. We see that $(F_2)^2 - F_3 F_1 = 1^2 - 2 \cdot 1 = -1 = (-1)^{2+1}$, so the equation holds for $n = 2$. Now let $n \in \mathbb{N}$. Suppose that $n \geq 3$, and that the equation holds for all values in $\{2, \ldots, n\}$. (Given that we already know that the equation holds for $n = 2$, it will suffice to prove that it holds for $n \geq 3$, and restricting to such values of n allows the following argument to work without special cases.) We compute

$$(F_{n+1})^2 - F_{n+2} F_n = (F_n + F_{n-1})^2 - (F_{n+1} + F_n) F_n$$

$$= (F_n)^2 + 2F_nF_{n-1} + (F_{n-1})^2 - F_{n+1}F_n - (F_n)^2$$
$$= (F_{n-1})^2 + F_n(2F_{n-1} - F_{n+1})$$
$$= (F_{n-1})^2 + F_n(2F_{n-1} - (F_n + F_{n-1}))$$
$$= (F_{n-1})^2 + F_n(F_{n-1} - F_n)$$
$$= (F_{n-1})^2 - F_nF_{n-2} = (-1)^{(n-1)+1} = (-1)^{(n+1)+1},$$

where the last line holds by the inductive hypothesis.   □

Although the natural way to think of the Fibonacci numbers is in terms of Definition by Recursion, it turns out that there is also an explicit formula for these numbers, which is

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \tag{6.4.1}$$

for all $n \in \mathbb{N}$. This formula, which is proved in Exercise 6.4.12 (4), is known as Binet's formula (though it is attributed to Euler and Daniel Bernoulli in [GKP94, Section 6.6] and [Tho59, Chapter XIV]). For those familiar with the "golden ratio," which equals $\frac{1+\sqrt{5}}{2}$ and is often denoted ϕ, observe that Binet's formula is $F_n = \frac{1}{\sqrt{5}}\{\phi^n - \left(\frac{-1}{\phi}\right)^n\}$ for all $n \in \mathbb{N}$. See Exercise 6.4.14 for another relation between the Fibonacci numbers and the golden ratio. See [Hun70] for more on the golden ratio.

We conclude this section with an even more complicated version of Definition by Recursion than the ones we have seen so far. We will need this additional version in the proof of Theorem 6.6.7, which is part of our discussion of countable sets. The reader might find the following definition and proof to be somewhat technical upon first reading, but hopefully will not be deterred from working through the proof, which uses a clever construction.

The idea of this variation of Definition by Recursion is that we want to have each term of the sequence be dependent upon all the terms that came earlier in the sequence, not just the previous term, or the previous two terms, or any other fixed number of previous terms. In other words, we want to define a sequence $c_1, c_2, c_3, \ldots$ by specifying c_1, and by specifying c_{n+1} in terms of $c_1, \ldots, c_n$, for each $n \in \mathbb{N}$. That is, we want c_2 to depend upon c_1, and c_3 to depend upon c_1 and c_2, and so on. The complication here is that there cannot be a single function to specify c_{n+1} in terms of $c_1, \ldots, c_n$ that works for all $n \in \mathbb{N}$, because any single function must have a fixed number of "variables." To resolve this matter, we use the following definition.

Definition 6.4.7. Let A be a set. Let $\mathcal{G}(A)$ be the set defined by

$$\mathcal{G}(A) = \bigcup_{n=1}^{\infty} \mathcal{F}(\{1, \ldots, n\}, A). \qquad \triangle$$

Theorem 6.4.8. *Let A be a set, let $b \in A$ and let $k \colon \mathcal{G}(A) \to A$ be a function. Then there is a unique function $f \colon \mathbb{N} \to A$ such that $f(1) = b$, and that $f(n+1) = k(f|_{\{1,\ldots,n\}})$ for all $n \in \mathbb{N}$.*

Proof. We follow [Mun00, Section 8].

Uniqueness: Let $s, t: \mathbb{N} \to A$ be functions. Suppose that $s(1) = b$ and $t(1) = b$, and that $s(n+1) = k(s|_{\{1,\ldots,n\}})$ and $t(n+1) = k(t|_{\{1,\ldots,n\}})$ for all $n \in \mathbb{N}$. We will show that $s(n) = t(n)$ for all $n \in \mathbb{N}$ by induction on n, using PMI-V2 (Theorem 6.3.8). By hypothesis we know that $s(1) = b = t(1)$. Next, let $n \in \mathbb{N}$ and suppose that $s(j) = t(j)$ for all $j \in \{1, \ldots, n\}$. Then $s|_{\{1,\ldots,n\}} = t|_{\{1,\ldots,n\}}$, and therefore $s(n+1) = k(s|_{\{1,\ldots,n\}}) = k(t|_{\{1,\ldots,n\}}) = t(n+1)$. It now follows from PMI-V2 that $s(n) = t(n)$ for all $n \in \mathbb{N}$, which means that $s = t$.

Existence: There are three steps in the definition of f.

Step 1. We will shown that for each $p \in \mathbb{N}$, there is a function $h_p: \{1, \ldots, p\} \to A$ such that $h_p(1) = b$, and that $h_p(n+1) = k(h_p|_{\{1,\ldots,n\}})$ for all $n \in \{1, \ldots, p-1\}$.

The proof is by induction on p. First, let $p = 1$. Then $\{1, \ldots, p\} = \{1\}$. Let $h_1: \{1, \ldots, 1\} \to A$ be defined by $h_1(1) = b$. Observe that $\{1, \ldots, p-1\} = \{1, \ldots, 0\} = \emptyset$, and hence $h_1(n+1) = k(h_1|_{\{1,\ldots,n\}})$ for all $n \in \{1, \ldots, p-1\}$ is necessarily true.

Next, let $p \in \mathbb{N}$. Suppose there is a function $h_p: \{1, \ldots, p\} \to A$ such that $h_p(1) = b$, and that $h_p(n+1) = k(h_p|_{\{1,\ldots,n\}})$ for all $n \in \{1, \ldots, p-1\}$. Let $h_{p+1}: \{1, \ldots, p+1\} \to A$ be defined by

$$h_{p+1}(n) = \begin{cases} h_p(n), & \text{if } n \in \{1, \ldots, p\} \\ k(h_p), & \text{if } n = p+1. \end{cases}$$

Then $h_{p+1}|_{\{1,\ldots,p\}} = h_p$. It follows that $h_{p+1}(1) = h_p(1) = b$, that $h_{p+1}(n+1) = h_p(n+1) = k(h_p|_{\{1,\ldots,n\}}) = k(h_{p+1}|_{\{1,\ldots,n\}})$ for all $n \in \{1, \ldots, p-1\}$ and that $h_{p+1}(p+1) = k(h_p) = k(h_{p+1}|_{\{1,\ldots,p\}})$. Hence h_{p+1} has the desired properties. The proof of this step is then complete by PMI.

Step 2. Let $p, q \in \mathbb{N}$. Suppose that $p < q$. We will show that $h_q(n) = h_p(n)$ for all $n \in \{1, \ldots, p\}$ by using Exercise 6.3.15. By Step 1 we know that $h_q(1) = b = h_p(1)$. Next, suppose that $n \in \{1, \ldots, p-1\}$ and that $h_q(j) = h_p(j)$ for all $j \in \{1, \ldots, n\}$. Hence $h_q|_{\{1,\ldots,n\}} = h_p|_{\{1,\ldots,n\}}$. Then by Step 1 we see that $h_q(n+1) = k(h_q|_{\{1,\ldots,n\}}) = k(h_p|_{\{1,\ldots,n\}}) = h_p(n+1)$. It now follows from Exercise 6.3.15 that $h_q(n) = h_p(n)$ for all $n \in \{1, \ldots, p\}$.

Step 3. Let $f: \mathbb{N} \to A$ be defined by $f(n) = h_n(n)$ for all $n \in \mathbb{N}$. Then $f(1) = h_1(1) = b$ by Step 1. Let $p \in \mathbb{N}$. If $j \in \{1, \ldots, p\}$, then $j < p+1$, and it follows from Step 2 that $h_{p+1}(j) = h_j(j) = f(j)$. Hence $h_{p+1}|_{\{1,\ldots,p\}} = f|_{\{1,\ldots,p\}}$. Using Step 1 we then see that $f(p+1) = h_{p+1}(p+1) = k(h_{p+1}|_{\{1,\ldots,p\}}) = k(f|_{\{1,\ldots,p\}})$. We therefore see that f satisfies the desired properties. $\qquad \square$

Exercises

Exercise 6.4.1. Let $r_1, r_2, r_3, \ldots$ be the sequence defined by $r_1 = 1$, and $r_{n+1} = 4r_n + 7$ for all $n \in \mathbb{N}$. Prove that $r_n = \frac{1}{3}\left(10 \cdot 4^{n-1} - 7\right)$ for all $n \in \mathbb{N}$.

Exercise 6.4.2. Let $b_1, b_2, b_3, \ldots$ be the sequence defined by $b_1 = 1$, and $b_2 = 1$, and $b_n = \frac{1}{3}\left(b_{n-1} + \frac{3}{b_{n-2}}\right)$ for all $n \in \mathbb{N}$ such that $n \geq 3$. Prove that $1 \leq b_n \leq \frac{3}{2}$ for all $n \in \mathbb{N}$.

Exercise 6.4.3. Let $d_1, d_2, d_3, \ldots$ be the sequence defined by $d_1 = 2$, and $d_2 = 3$, and $d_n = d_{n-1} \cdot d_{n-2}$ for all $n \in \mathbb{N}$ such that $n \geq 3$. Find an explicit formula for d_n, and prove that your formula works.

Exercise 6.4.4. [Used in Exercise 4.4.20.] Let A be a non-empty set, and let $f : A \to A$ be a function. Suppose that f is bijective. Prove that f^n is bijective for each $n \in \mathbb{N}$.

Exercise 6.4.5. For each $n \in \mathbb{N}$, find an example of a function $f : A \to A$ for some set A such that f^n is a constant map, but f^r is not a constant map for all $r \in \{1, \ldots, n-1\}$.

Exercise 6.4.6. [Used in Proposition 6.4.6.] Prove Proposition 6.4.6 (1) (2).

Exercise 6.4.7. [Used in Section 8.6.] Let $n \in \mathbb{N}$.

(1) Prove that $2|F_n$ if and only if $3|n$.
(2) Prove that $3|F_n$ if and only if $4|n$.
(3) Prove that $4|F_n$ if and only if $6|n$.

Exercise 6.4.8. [Used in Section 8.6.] Let $n \in \mathbb{N}$. Suppose that $n > 5$. Prove that $F_n = 5F_{n-4} + 3F_{n-5}$.

Exercise 6.4.9. [Used in Section 8.6.] Let $n, k \in \mathbb{N}$. Suppose that $k \geq 2$. Prove that each of the following holds.

(1) $F_{n+k} = F_k F_{n+1} + F_{k-1} F_n$.
(2) $F_n | F_{kn}$.

Exercise 6.4.10. Define a sequence by specifying that $G_1 = 1$, that $G_2 = 1$ and that $G_{n+2} = G_{n+1} + G_n + G_{n+1}G_n$ for all $n \in \mathbb{N}$. Prove that $G_n = 2^{F_n} - 1$ for all $n \in \mathbb{N}$.

Exercise 6.4.11. Let $n \in \mathbb{N}$.

(1) Let $\phi = \frac{1+\sqrt{5}}{2}$ and $\phi' = \frac{1-\sqrt{5}}{2} = \frac{-1}{\phi}$. Prove that $\phi^n + \phi'^n$ is an integer.
(2) Prove that the integer $5(F_n)^2 + 4(-1)^n$ is a perfect square.

Exercise 6.4.12. [Used in Section 6.4.] The purpose of this exercise is to prove Binet's formula (Equation 6.4.1). Let $c, d \in \mathbb{R}$. Suppose that c and d are non-zero, and that the equation $x^2 - cx - d = 0$ has two distinct real solutions r_1 and r_2. Let $A_1, A_2, A_3, \ldots$ be a sequence satisfying $A_{n+2} = cA_{n+1} + dA_n$ for all $n \in \mathbb{N}$. (By Theorem 6.4.5 there is a unique such sequence for each choice of A_1 and A_2.) Let

$$P = \frac{r_2 A_1 - A_2}{r_1(r_2 - r_1)} \quad \text{and} \quad Q = \frac{r_1 A_1 - A_2}{r_2(r_1 - r_2)}.$$

(1) Let $D_1, D_2, D_3, \ldots$ be the sequence defined by the explicit formula $D_n = P(r_1)^n + Q(r_2)^n$ for all $n \in \mathbb{N}$. Verify that $D_1 = A_1$ and $D_2 = A_2$.
(2) Prove that $D_{n+2} = cD_{n+1} + dD_n$ for all $n \in \mathbb{N}$.
(3) Use Theorem 6.4.5 to deduce that $A_n = D_n$ for all $n \in \mathbb{N}$.

(4) Apply Part (3) of this exercise to the Fibonacci sequence, and deduce Equation 6.4.1.

Exercise 6.4.13. We discuss a curious geometric puzzle; see [Wea38] for the history of this puzzle. Start with a square that has sides of length 13 units. Dissect the square into four pieces, as depicted in Figure 6.4.2 (i). The four pieces can be rearranged into a rectangle, as shown in Figure 6.4.2 (ii). Try making the puzzle out of paper, and doing the rearranging. The curious thing is that the area of the square is $13^2 = 169$, whereas the area of the rectangle is $21 \cdot 8 = 168$. How can it happen that the same four pieces form shapes with different area?
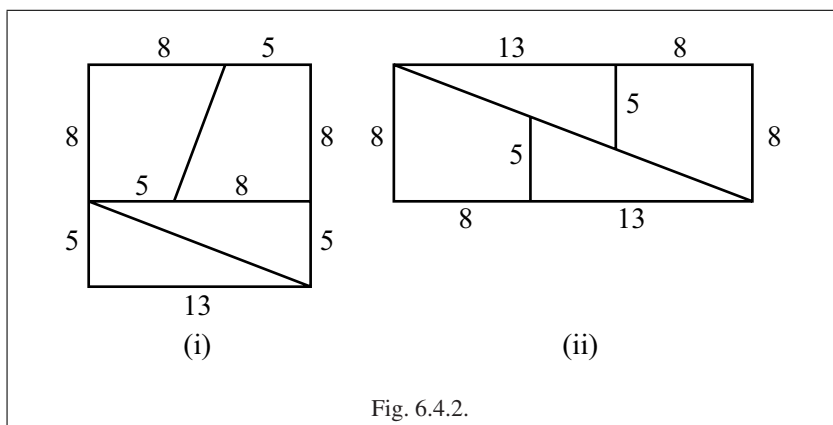
Fig. 6.4.2.

(1) Explain the puzzle by showing that there is a slight overlap among the pieces.
(2) We now generalize the above puzzle. Rather than starting with a square with sides of length 13 units, and breaking the sides up into pieces of length 8 and 5, we start with an arbitrary square, and break its sides into pieces of lengths a and b. Find the only possible value for the ratio $\frac{a}{b}$ so that there is no overlap or underlap when the pieces are rearranged into a rectangle.
(3) We continue Part (2) of this exercise. Suppose that we want a puzzle with a and b both natural numbers (as is the case in the original puzzle). Because the areas of both the square and rectangle will be integers in this case, the difference of these areas, which is the amount of overlap or underlap, will also be an integer. Hence, with a and b both natural numbers, the minimal overlap will be ± 1. This minimal overlap is very hard to notice when the puzzle is made out of pieces of paper, which is why it fools people. A larger overlap or underlap would be much easier to spot. Prove that if a and b are consecutive Fibonacci numbers, then the overlap or underlap is minimal. Observe that the original puzzle did use consecutive Fibonacci numbers. (It can be shown, moreover, that no two natural numbers other than two consecutive Fibonacci numbers have the minimal overlap or underlap, though that requires a more difficult proof.)

Exercise 6.4.14. **[Used in Section 6.4 and Section 7.8.]** This exercise is for the reader who is familiar, at least informally, with limits of sequences. (We will discuss limits of sequences rigorously, albeit briefly, in Section 7.8; see any introductory text in real analysis, for example [Blo11, Chapter 8], for details.) We saw in Equation 6.4.1 that the Fibonacci numbers can be computed using the number $\phi = \frac{1+\sqrt{5}}{2} = 1.618\ldots$. There is another relation between the Fibonacci numbers and ϕ, which is seen by looking at successive ratios of Fibonacci numbers, that is, the numbers

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \ldots .$$

A calculation of the first few terms of this sequence shows that they appear to approach the number $1.618\ldots$, which looks suspiciously like ϕ, at least up to a few decimal places. In fact, it can be proved that

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \phi.$$

The proof of this equation has two parts: (1) that the limit exists and (2) that the limit equals ϕ. The reader is asked to prove Part (2), assuming that Part (1) is true. (Proving Part (1) is more advanced, requiring a knowledge of Cauchy sequences and the completeness of the real numbers. See [Blo11, Example 8.4.10] for a detailed proof of Part (1).)

6.5 Cardinality of Sets

Intuitively, we know what it means to talk about the "size" of a finite set, and it seems intuitively clear that finite sets come in different sizes. What about infinite sets? Does it make sense to discuss the "size" of an infinite set, and if it does, do infinite sets come in different sizes? Galileo, writing in the early seventeenth century in [Gal74, pp. 38–47], thought that all infinite sets had the same size. Though he had some very good insights into infinite sets, even the brilliant Galileo was mistaken on this matter, as we shall see below. A correct understanding of the sizes of infinite sets was due to Cantor, the developer of set theory, two and a half centuries after Galileo. In the remaining sections of this chapter we will see a number of important arguments by Cantor; these ideas helped propel set theory into its prominent role in modern mathematics.

How do we determine when two sets have the same size? It might appear at first glance that to answer this question we would need to be able to compute the size of each of the two sets before we could compare them, and the need for finding the "size" of an infinite set might seem to be an insurmountable obstacle if we want to compare the sizes of different infinite sets. It turns out, and this is a great insight, that it is possible to discuss whether two sets have the "same size" without first having to figure out the size of each set.

We start with a simple example. Suppose that a group of people want to stay at a hotel, with each person in a separate room. The hotel manager will take the group

only if it completely fills up the hotel, and so it is necessary to figure out whether the right number of rooms are vacant. This is a very simple problem to solve, but there are in fact two ways to proceed. One way would be to count the number of people, and count the number of free rooms, and then see if the two numbers are the same. Another way would be to make a list of people, a list of free rooms, and then start going down the two lists, matching up each successive person with a distinct vacant room; if all the people and all the rooms are taken care of by this process, then everyone would be happy. The method of matching up people and rooms is cumbersome, but unlike counting, it has the advantage of working even if the number of people and the number of rooms are infinite. The method of counting, by contrast, works only when everything is finite.

To determine whether two sets have the same size, we will try to pair up the elements of the two sets. Our tool for "pairing up" is bijective functions, as in the following definition.

Definition 6.5.1. Let A and B be sets. The sets A and B have the **same cardinality**, denoted $A \sim B$, if there is a bijective function $f : A \to B$. △

Observe that Definition 6.5.1 refers only to whether *two* sets have the "same cardinality"; nothing is stated about the "cardinality" (which means size) of each of the two sets. Using bijective functions allows us to compare two sets, but not to say anything about each of the individual sets.

If two sets have the same cardinality, then by definition there is a bijective function from one to the other. Unless each of the two sets has only zero or one element, there will in fact be more than one such bijective function. When proving that two sets have the same cardinality, it is sufficient to find a single bijective function.

The following lemma gives the basic properties of $\sim$, which should look familiar.

Lemma 6.5.2. *Let A, B and C be sets.*

    1. $A \sim A$.
    2. If $A \sim B$, then $B \sim A$.
    3. If $A \sim B$ and $B \sim C$, then $A \sim C$.

Proof. See Exercise 6.5.3. □

Lemma 6.5.2 might lead the reader to think of $\sim$ as an equivalence relation, but we need to proceed with caution here. If $\sim$ were a relation, on what set would it be a relation? We might want to think of $\sim$ as a relation on the set of all sets, because for any two sets A and B, it must be the case that either $A \sim B$ or $A \nsim B$. However, because of foundational problems such as Russell's Paradox, which was discussed in Section 3.5, we avoid things such as the set of all sets. Hence, although $\sim$ satisfies the three properties of an equivalence relation, it is not technically a relation on a set at all. If, however, all sets of interest are subsets of a given set X, then it is correct to say that $\sim$ is an equivalence relation on $\mathcal{P}(X)$.

We now have some examples of sets that have the same cardinality.

Example 6.5.3.

(1) Though he made one major mistake concerning infinite sets (to be discussed shortly), Galileo understood the idea of using bijective functions (as we now call them) to show that two sets have the same cardinality. In the following quote from [Gal74, pp. 40–41], Galileo discusses some sets of positive natural numbers in a dialogue between two of his protagonists.

Salviati. ...If I say that all numbers, including squares and non-squares, are more [numerous] than the squares alone, I shall be saying a perfectly true proposition; is that not so?

Simplicio. One cannot say otherwise.

Salviati. Next, I ask how many are the square numbers; and it may be truly answered that they are just as many as are their own roots, because every square has its root, and every root its square; nor is there any square that has more than just one root, or any root that has more than just one square.

Simplicio. Precisely so.

Salviati. But if I were to ask how many *roots* there are, it could not be denied that those are as numerous as all the numbers, because there is no number that is not the root of some square. That being the case, it must be said that the square numbers are as numerous as all numbers, because they are as many as their roots, and all numbers are roots.

In modern terminology, Galileo states that the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ and the set of squares $S = \{1, 4, 9, 16, \ldots\}$ have the same cardinality. Galileo's argument is precisely the same as our modern one, which is that there is a bijective function $h\colon \mathbb{N} \to S$. The function h that Galileo suggests is the most natural one to use, namely, the function defined by $h(n) = n^2$ for all $n \in \mathbb{N}$. That h is bijective follows from the fact that $k\colon S \to \mathbb{N}$ defined by $k(n) = \sqrt{n}$ for all $n \in S$ is an inverse of h, where we make use of Theorem 4.4.5 (3).

(2) The set of natural numbers $\mathbb{N}$ and the set of integers $\mathbb{Z}$ have the same cardinality. One choice of a bijective function $f\colon \mathbb{N} \to \mathbb{Z}$ is the one defined by

$$f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even} \\ -\frac{n-1}{2}, & \text{if } n \text{ is odd.} \end{cases}$$

It is left to the reader to verify that this function is bijective.

(3) Let $a, b, c, d \in \mathbb{R}$. Suppose that $a < b$ and $c < d$. We will show that $[a, b] \sim [c, d]$, that $(a, b) \sim (c, d)$, and similarly for half-open intervals. Let $g\colon [a, b] \to [c, d]$ be defined by

$$g(x) = \frac{d - c}{b - a}(x - a) + c$$

for all $x \in [a, b]$. It is straightforward to verify that the function g is bijective; we leave the details to the reader. It follows that $[a, b] \sim [c, d]$. A similar argument shows that $(a, b) \sim (c, d)$, and similarly for half-open intervals; we omit the details.

(4) Let $a, b \in \mathbb{R}$. Suppose that $a < b$. We will show that $(a, b) \sim \mathbb{R}$. By Part (3) of this example we know that $(a, b) \sim (-1, 1)$. Hence, it is sufficient to show that

$(-1,1) \sim \mathbb{R}$. Actually, we have already done all the work of proving that fact, because in Exercise 4.4.3 there is an example of a bijective function $f: \mathbb{R} \to (-1,1)$. (Instead of this function f, it is common to use the function $h: \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$ defined by $h(x) = \tan x$ for all $x \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, and then to use known properties of the tangent function to show that h is a bijective function. However, it is beyond the scope of this book to give a rigorous treatment of the tangent function, and so we have provided the more elementary function f.) $\Diamond$

For a better analysis of the cardinality of sets, we need to make various useful distinctions, such as finite sets vs. infinite sets. We have used the notion of finiteness intuitively until now in this text, but we are now prepared to deal with this concept more precisely. The simplest approach to finiteness makes use of subsets of the natural numbers of the form $\{1, \ldots, n\}$; recall the definition of such sets given in Definition 6.2.6. More generally, observe in the following definition how important the set $\mathbb{N}$ is in understanding the cardinality of sets (this set is referred to directly or indirectly in the first four parts of the definition).

Definition 6.5.4.

1. A set is **finite** if it is either the empty set or it has the same cardinality as $\{1, \ldots, n\}$ for some $n \in \mathbb{N}$.
2. A set is **infinite** if it is not finite.
3. A set is **countably infinite** if it has the same cardinality as $\mathbb{N}$.
4. A set is **countable** (also called **denumerable**) if it is finite or countably infinite.
5. A set is **uncountable** if it is not countable. $\triangle$

The reader is asked to prove in Exercise 6.5.5 that if A and B are sets such that $A \sim B$, and if A is finite, infinite, countably infinite, countable or uncountable, then so is B. We will use this simple fact, without explicitly mentioning it, throughout the rest of this chapter.

It is evident that three of the types of sets described in Definition 6.5.4 in fact exist. There are finite sets, because the set $\{1, \ldots, n\}$ is finite for all $n \in \mathbb{N}$; there are countably infinite sets, because $\mathbb{N}$ is countably infinite; and there are countable sets, because there are countably infinite sets. On the other hand, it is not immediately evident whether there are infinite sets, and whether there are uncountable sets. We will show that there are uncountable sets shortly, but we first turn to the existence of infinite sets. The reader might think that this fact is self-evident, because we have already remarked that there exist countably infinite sets. However, the terms "countably infinite" and "infinite" were defined entirely separately, and it is not true simply by definition that a "countably infinite" set is in fact "infinite," and so a proof is needed. The following lemma resolves this matter.

Lemma 6.5.5.

1. *The set $\mathbb{N}$ is infinite.*
2. *A countably infinite set is infinite.*

Proof.

(1). Suppose that $\mathbb{N}$ is finite. Because $\mathbb{N} \neq \emptyset$, then there is some $n \in \mathbb{N}$ such that $\mathbb{N} \sim \{1,\ldots,n\}$. Let $f \colon \{1,\ldots,n\} \to \mathbb{N}$ be a bijective function. It then follows from Theorem 6.3.11 (1) that there is some $k \in \{1,\ldots,n\}$ such that $f(k) \geq f(i)$ for any $i \in \{1,\ldots,n\}$. Therefore $f(k)+1 > f(i)$ for all $i \in \{1,\ldots,n\}$. Hence $f(k)+1 \notin f(\{1,\ldots,n\})$. Because $f(k)+1 \in \mathbb{N}$, we deduce that f is not surjective, which is a contradiction. Hence $\mathbb{N}$ is not finite, and so it is infinite.

(2). Let B be a set. Suppose that B is countably infinite. Then $B \sim \mathbb{N}$. Suppose further that B is finite. It would then follow from Exercise 6.5.5 that $\mathbb{N}$ is finite, which is a contradiction to Part (1) of this lemma. Hence B is infinite. $\square$

From Part (1) of Lemma 6.5.5 we see that there are infinite sets.

The one remaining question about Definition 6.5.4 is whether there are any uncountable sets. This issue is not at all trivial, and in fact it has fooled many great minds. For example, shortly after the quote from Galileo given above, Galileo continues as follows.

> *Salviati.* I don't see how any other decision can be reached than to say that all the numbers are infinitely many; all squares infinitely many; all their roots infinitely many; that the multitude of squares is not less than that of all numbers nor is the latter greater than the former. And in final conclusion, the attributes of equal, greater, and less have no place in infinite, but only in bounded quantities. So when Simplicio proposes to me several unequal lines, and asks me how it can be that there are not more points in the greater than in the lesser, I reply to him that there are neither more, nor less, nor the same number, but in each there are infinitely many. Or truly, might I not reply to him that the points in one are as many as the square numbers; in another and greater line, as many as all numbers; and in some tiny little [line], only as many as the cube numbers ....

In this quote Galileo essentially says that all infinite sets have the same cardinality, which would make them all countably infinite in our terminology. In fact, we will see in Corollary 6.5.8 below that Galileo was wrong, and that there are indeed uncountable sets. To prove that corollary, we make use of the cardinality of the power set of a set. We start with an example.

Example 6.5.6. Let $A = \{1,2\}$. Then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$. Therefore $A \not\sim \mathcal{P}(A)$. $\diamond$

The following theorem shows that Example 6.5.6 is typical.

Theorem 6.5.7. *Let A be a set. Then $A \not\sim \mathcal{P}(A)$.*

Proof. There are two cases. First, suppose that $A = \emptyset$. Observe that $\mathcal{P}(A) = \{\emptyset\}$, and therefore there cannot be a bijective function $\mathcal{P}(A) \to A$, because there cannot be a function from a non-empty set to the empty set. Hence $\mathcal{P}(A) \not\sim A$.

Next, suppose that $A \neq \emptyset$. Suppose further that $A \sim \mathcal{P}(A)$. Then there is a bijective function $f \colon A \to \mathcal{P}(A)$. Let $D = \{a \in A \mid a \notin f(a)\}$. Observe that $D \subseteq A$, and so $D \in \mathcal{P}(A)$. Because f is surjective, there is some $d \in A$ such that $f(d) = D$. Is $d \in D$? Suppose that $d \in D$. Then by the definition of D we see that $d \notin f(d) = D$. Suppose that $d \notin D$. Then $d \in f(d) = D$. We therefore have a contradiction, and so $A \not\sim \mathcal{P}(A)$. $\qquad \square$

In the following proof we will use Theorem 6.6.5 (1) from Section 6.6, though there is no circular reasoning here, because the proof of Theorem 6.6.5 does not make use of the corollary we are about to prove.

Corollary 6.5.8. *The set $\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof. By Theorem 6.5.7 we know that $\mathcal{P}(\mathbb{N}) \not\sim \mathbb{N}$, and so $\mathcal{P}(\mathbb{N})$ is not countably infinite. If we could show that $\mathcal{P}(\mathbb{N})$ were not finite, then it would follow that it is not countable. Suppose that $\mathcal{P}(\mathbb{N})$ is finite. Let $T = \{\{n\} \mid n \in \mathbb{N}\} \subseteq \mathcal{P}(\mathbb{N})$. It follows from Theorem 6.6.5 (1) that T is finite. However, it is evident that $T \sim \mathbb{N}$, and this would imply that $\mathbb{N}$ is finite, which is a contradiction to Lemma 6.5.5 (1). We conclude that $\mathcal{P}(\mathbb{N})$ is uncountable. $\qquad \square$

Corollary 6.5.8 is not entirely satisfying, because, even though its proof is short, it would be nice to see a more familiar and concrete set that is uncountable. In fact, we will see in Theorem 6.7.3 that the set $\mathbb{R}$ is uncountable.

Putting all our results so far together, we deduce that any set is precisely one of finite, countably infinite or uncountable, and that there are sets of each type.

We conclude this section with two important theorems concerning cardinalities of sets. The proofs of these theorems are much trickier than what we have seen so far in this section. We start with the following definition.

Definition 6.5.9. Let A and B be sets. We say that $A \preccurlyeq B$ if there is an injective function $f \colon A \to B$; we say that $A \prec B$ if $A \preccurlyeq B$ and $A \not\sim B$. $\qquad \triangle$

Intuitively, if $A \prec B$, then A has "smaller size" than B.

Some basic properties of the relation $\preccurlyeq$ are given in Exercise 6.5.11. It is simple to see that for any set A, there is an injective function $A \to \mathcal{P}(A)$, and hence $A \preccurlyeq \mathcal{P}(A)$; by Theorem 6.5.7 we see that $A \prec \mathcal{P}(A)$. Applying this fact to the set $\mathbb{N}$, and then to $\mathcal{P}(\mathbb{N})$, to $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ and so on, we deduce that

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \cdots .$$

Because all the sets in this sequence other than the first are uncountable, we therefore see that there are infinitely many different cardinalities among the uncountable sets. A commonly used notation due to Cantor is the notation $\aleph_0$, which denotes the cardinality of $\mathbb{N}$. Observe that $\aleph_0$ is not a real number, though it is referred to as a "cardinal number." Motivated by an observation made in Example 3.2.9 (2), it is common to denote the cardinality of $\mathcal{P}(\mathbb{N})$ by $2^{\aleph_0}$. (It is also possible to define cardinal numbers $\aleph_1, \aleph_2, \ldots$, though we will not do so; see [Vau95, Section 7.5] for details.)

Our two theorems about cardinalities of sets are conveniently expressed using the concept of $\preccurlyeq$. Although our notation (which looks suspiciously like $\leq$) might make it appear as if these results are trivial, in fact neither is trivial at all.

Our first theorem, called the Schroeder–Bernstein Theorem (also known as the Cantor–Bernstein Theorem), not only has aesthetic appeal (by proving the analog for $\preccurlyeq$ of the fact that if $a \leq b$ and $b \leq a$, then $a = b$, for all $a, b \in \mathbb{R}$), but it is quite useful as well, as we will see after the theorem.

Theorem 6.5.10 (Schroeder–Bernstein Theorem). *Let A and B be sets. Suppose that $A \preccurlyeq B$ and $B \preccurlyeq A$. Then $A \sim B$.*

The idea of the proof of the Schroeder–Bernstein Theorem, the bulk of which is contained in the proof of the following lemma, is as follows. Let A, B and C be sets. Suppose that $C \subseteq B \subseteq A$, and that $A \preccurlyeq C$. We want to show that $A \sim B$. By definition there is an injective function $g \colon A \to C$. We need to define a bijective function $h \colon A \to B$. It would be tempting to define the function h by

$$h(x) = \begin{cases} g(x), & \text{if } x \in A - B \\ x, & \text{if } x \in B. \end{cases}$$

However, although h is certainly surjective, and although the restriction of h to each of $A - B$ and B is injective, it is not the case that h as a whole is injective, because there is overlap between $g(A - B)$ and B. We would then want to modify h by letting it equal the identity on only some subset of B, which would hopefully eliminate the overlap, though without ruining surjectivity.

More specifically, let $X = g(A - B)$. A good guess at how to modify h would be to have h equal the identity on $B - X$, and have h equal g on $(A - B) \cup X$. Unfortunately, although there is no overlap anymore involving $g(A - B)$ and $B - X$, we may have created a problem involving $g(X)$ and $B - X$. We would then need to modify h again, this time having h equal the identity on $B - X - g(X)$, and having h equal g on $(A - B) \cup X \cup g(X)$. This process never stops, but if we do not mind using an infinite process, which can be done using recursion, the function h can be defined in such a way that it is bijective. For convenience, the function h actually used in the proof of the following lemma looks a bit different from the above, but it is just another way of writing the same thing.

Lemma 6.5.11. *Let A, B and C be sets. Suppose that $C \subseteq B \subseteq A$, and that $A \preccurlyeq C$. Then $A \sim B$.*

Proof. By definition there is an injective function $g \colon A \to C$.

Let $T_0 = A - B$. We now use Definition by Recursion (Theorem 6.4.1) to define a sequence of subsets of A by specifying $T_1 = g(T_0)$, and $T_{n+1} = g(T_n)$ for all $n \in \mathbb{N}$. This definition is valid, because we can think of this sequence of subsets of A as a sequence of elements of $\mathcal{P}(A)$. Let $T = \bigcup_{n=0}^{\infty} T_n$. By Theorem 4.2.4 (6) we see that

$$g(T) = g\left(\bigcup_{n=0}^{\infty} T_n \right) = \bigcup_{n=0}^{\infty} g(T_n) = \bigcup_{n=0}^{\infty} T_{n+1} = \bigcup_{n=1}^{\infty} T_n \subseteq T.$$

Also, observe that $T_0 \subseteq T$, which means that $A - B \subseteq T$, and it follows from Theorem 3.3.8 (4) (6) that $A - T \subseteq A - (A - B) = B$.

Let $h: A \to B$ be defined by

$$h(x) = \begin{cases} g(x), & \text{if } x \in T \\ x, & \text{if } x \in A - T. \end{cases}$$

This definition makes sense because $g(T) \subseteq C \subseteq B$ and $A - T \subseteq B$.

We now show that h is bijective. Let $x, y \in A$. Suppose that $h(x) = h(y)$. If $x, y \in T$, then $h(x) = h(y)$ implies $g(x) = g(y)$, and hence $x = y$ by the injectivity of g. If $x, y \in A - T$, then $h(x) = h(y)$ implies $x = y$. If $x \in T$ and $y \in A - T$, then $h(x) = h(y)$ implies $g(x) = y$, which implies that $y \in g(T) \subseteq T$, which is a contradiction, and hence this case is not possible. The case where $x \in A - T$ and $y \in T$ is similarly not possible. We conclude that h is injective.

Let $b \in B$. First, suppose that $b \in T$. Because $b \notin A - B = T_0$, then $b \in T_k$ for some $k \in \mathbb{N}$. Hence $b \in g(T_{k-1})$, which means that $b = g(z)$ for some $z \in T_{k-1} \subseteq T$. Because $z \in T$, then $b = h(z)$. Second, suppose that $b \in B - T$. Then $b \in A - T$, and hence $h(b) = b$. We conclude that h is surjective, and it follows that h is bijective.   □

Proof Theorem 6.5.10 (Schroeder–Bernstein Theorem). By definition there are injective functions $p: A \to B$ and $q: B \to A$. Then $p(A) \subseteq B$, and $q(p(A)) \subseteq q(B) \subseteq A$. By Exercise 6.5.4 we know that $q(p(A)) \sim A$ and $q(B) \sim B$. From the former it follows that $A \preccurlyeq q(p(A))$, and we then use Lemma 6.5.11 to deduce that $A \sim q(B)$. Hence $A \sim B$.   □

To obtain a more concrete understanding of the proof of the Schroeder–Bernstein Theorem (Theorem 6.5.10), the reader is asked in Exercise 6.5.12 to compute the sets $T_0, T_1, \ldots$ and the function h in the proof of Lemma 6.5.11 for a simple example.

The benefit of using the Schroeder–Bernstein Theorem is that there are cases where it is easier to find two injective functions than a single bijective function.

Example 6.5.12. Let $a, b \in \mathbb{R}$. Suppose that $a < b$. We will use the Schroeder–Bernstein Theorem (Theorem 6.5.10) to prove that $[a, b] \sim (a, b)$. By Example 6.5.3 (3) we know that $[a, b] \sim [-1, 1]$ and $(a, b) \sim (-1, 1)$. Hence, it will suffice to prove that $(-1, 1) \sim [-1, 1]$. Let $f: (-1, 1) \to [-1, 1]$ be defined by $f(x) = x$ for all $x \in (-1, 1)$, and let $g: [-1, 1] \to (-1, 1)$ be defined by $g(x) = \frac{x}{2}$ for all $x \in [-1, 1]$. Then both f and g are injective, and hence $(-1, 1) \preccurlyeq [-1, 1]$ and $[-1, 1] \preccurlyeq (-1, 1)$. The Schroeder–Bernstein Theorem now implies that $[-1, 1] \sim (-1, 1)$, and therefore $[a, b] \sim (a, b)$.

Similar arguments, making use of the Schroeder–Bernstein Theorem together with Example 6.5.3 (4), show that any two of the following intervals have the same cardinality: $[a, b]$, $[a, b)$, $(a, b]$, (a, b), $[a, \infty)$, (a, ∞), $(-\infty, b]$, $(-\infty, b)$ and $(-\infty, \infty)$. The reader is asked to proved the details of one specific case in Exercise 6.5.13 (1).

We mention that whereas the above proof that $(a, b) \sim [a, b]$ is short, it is not entirely satisfying, because it would be nicer to see an explicit bijective function $f: [a, b] \to (a, b)$. The reader is asked to find such a function in Exercise 6.5.14,

though doing so is admittedly trickier than using the Schroeder–Bernstein Theorem.

$\diamond$

The proof of the following theorem, called the Trichotomy Law for Sets, relies upon the Axiom of Choice. It is not just for convenience that we make use of this axiom, but it is a necessity, because the Trichotomy Law for Sets is in fact equivalent to the Axiom of Choice; see [Sto79, Section 2.9] or [RR85, Section I.3] for details. Rather than using the Axiom of Choice directly in this proof, we use Zorn's Lemma (Theorem 3.5.6), which is equivalent to the Axiom of Choice, and is easier to use in the present situation.

Theorem 6.5.13 (**Trichotomy Law for Sets**). *Let A and B be sets. Then $A \preccurlyeq B$ or $B \preccurlyeq A$.*

Proof. We need to show that there is an injective function $f: A \to B$ or an injective function $g: B \to A$. If A or B is empty these functions exist trivially, so we will assume that A and B are both non-empty.

A **partial function** from A to B is a function of the form $f: J \to B$, where $J \subseteq A$. We can think of a partial function from A to B as a subset $F \subseteq A \times B$ such that for each $a \in A$, there is at most one pair in F of the form (a, b). Hence, we can apply the concepts of subset and union to partial functions from A to B.

Let $\mathcal{P}$ be the set of all injective partial functions from A to B. Observe that $\mathcal{P} \neq \emptyset$, because $\emptyset \in \mathcal{P}$. Let $\mathcal{C}$ be a chain in $\mathcal{P}$. We claim that $\bigcup_{F \in \mathcal{C}} F \in \mathcal{P}$. Suppose that $(a, b), (a, c) \in \bigcup_{F \in \mathcal{C}} \mathcal{C}$, for some $a \in A$ and $b, c \in B$. Then $(a, b) \in G$ and $(a, c) \in H$ for some partial functions $G, H \in \mathcal{C}$. Because $\mathcal{C}C$ is a chain, we know that $G \subseteq H$ or $G \supseteq H$. Without loss of generality assume that $G \subseteq H$. Then (a, b) and (a, c) are both in H, and because H is a partial function, then it must be the case that $b = c$. We conclude that $\bigcup_{F \in \mathcal{C}} F$ is a partial function from A to B. Next, suppose that $(c, e), (d, e) \in \bigcup_{F \in \mathcal{C}} \mathcal{C}$, for some $c, d \in A$ and $e \in B$. A similar argument shows that (c, e) and (d, e) must both be in some $K \in \mathcal{C}$, and because K is an injective partial function, then it must be the case that $c = d$. We conclude that $\bigcup_{F \in \mathcal{C}} F$ is an injective partial function from A to B, and hence that $\bigcup_{F \in \mathcal{C}} F \in \mathcal{P}$.

By Zorn's Lemma (Theorem 3.5.6) the family of sets $\mathcal{P}$ has a maximal element. Let $M \in \mathcal{P}$ be such a maximal element. Then M is an injective partial function from A to B. There are now three cases. First, suppose that for each $a \in A$, there is a pair of the form (a, b) in M. Then M is an injective function $A \to B$. Second, suppose that for each $d \in B$, there is a pair of the form $(c, d) \in M$. Then M is a bijective partial function from A to B, and using Exercise 4.4.13 (3) we see that the inverse function of M can be viewed as an injective function $B \to A$. Third, suppose that neither of the previous two cases holds. Then there is some $x \in A$ such that there is no pair of the form (x, b) in M, and there is some $y \in B$ such that there is no pair of the form $(a, y) \in M$. Let $N = M \cup \{(x, y)\}$. It is left to the reader to verify that N is an injective partial function from A to B, and hence that $N \in \mathcal{P}$. Because $M \subsetneq N$, we have a contradiction to the fact that M is a maximal element of $\mathcal{P}$, and so this third case cannot happen. $\qquad \square$

<div align="center">

Exercises

</div>

Exercise 6.5.1. Prove that the set of all integers that are multiples of 5 has the same cardinality as the set of all integers.

Exercise 6.5.2. Prove that the disk $\mathbb{R}^2$ of radius 3 centered at $(1,2)$ has the same cardinality as the unit disk in $\mathbb{R}^2$ centered at the origin.

Exercise 6.5.3. [Used in Lemma 6.5.2.] Prove Lemma 6.5.2.

Exercise 6.5.4. [Used repeatedly.] Let A and B be sets, let $X \subseteq A$ be a subset and let $f \colon A \to B$ be a function. Suppose that f is injective. Prove that $X \sim f(X)$.

Exercise 6.5.5. [Used repeatedly.] Let A and B be sets. Suppose that $A \sim B$. Prove that if A is finite, infinite, countably infinite, countable or uncountable, then so is B.

Exercise 6.5.6. [Used in Theorem 6.7.4 and Exercise 6.7.1.]

(1) Give an example of sets A, B and C such that $A \sim B$ and $A \cup C \not\sim B \cup C$.
(2) Let A, B and C be sets. Suppose that $A \sim B$ and that $A \cap C = \emptyset$ and $B \cap C = \emptyset$. Prove that $A \cup C \sim B \cup C$.
(3) Let A, B and C be sets. Suppose that $A \cup C \sim B \cup C$ and that $A \cap C = \emptyset$ and $B \cap C = \emptyset$. Is it necessarily the case that $A \sim B$? Give a proof or a counterexample.

Exercise 6.5.7. Let A and B be sets. Prove that $A \sim B$ implies that $\mathcal{P}(A) \sim \mathcal{P}(B)$.

Exercise 6.5.8. [Used in Theorem 6.7.1.] Let A and F be sets. Suppose that F is finite, and that A is respectively finite, infinite, countably infinite, countable or uncountable.

(1) Prove that $A - F$ is respectively finite, infinite, countably infinite, countable or uncountable.
(2) Prove that $A \cup F$ is respectively finite, infinite, countably infinite, countable or uncountable.

Exercise 6.5.9. Let A be a set, and let x be an element (not necessarily in A). Prove that $A \times \{x\} \sim A$.

Exercise 6.5.10. Let A, B, C and D be sets. Suppose that $A \sim B$ and $C \sim D$. Prove that $A \times C \sim B \times D$.

Exercise 6.5.11. [Used in Section 6.5.] Let A, B and C be sets.

(1) Prove that $\emptyset \preccurlyeq A$.
(2) Prove that $A \preccurlyeq A$.
(3) Prove that if $A \preccurlyeq B$ and $B \preccurlyeq C$, then $A \preccurlyeq C$.

Exercise 6.5.12. [Used in Section 6.5.] Let $A = \mathbb{N}$, let $B = \{2,3,\ldots\}$ and let $C = \{2,3,\ldots\}$. It is evident how to define a bijective function $A \to B$, and we do not need the Schroeder–Bernstein Theorem (Theorem 6.5.10) to find such a function. However, in order to see a concrete example of how the proof of Lemma 6.5.11 (and hence of the Schroeder–Bernstein Theorem) works, the reader is asked to compute the sets $T_0, T_1, \ldots$ and the function $h \colon A \to B$ defined in the proof of Lemma 6.5.11 using the function $g \colon A \to C$ defined by $g(x) = x + 5$ for all $x \in A$.

Exercise 6.5.13. Let $a, b, c, d \in \mathbb{R}$. Suppose that $a < b$ and $c < d$. Use the Schroeder–Bernstein Theorem (Theorem 6.5.10) to prove the following statements.

   (1) [Used in Example 6.5.12.] $[a, b) \sim \mathbb{R}$.
   (2) Let $X, Y \subseteq \mathbb{R}$ be subsets. If $(a, b) \subseteq X$ and $(c, d) \subseteq Y$, then $X \sim Y$.

Exercise 6.5.14. [Used in Example 6.5.12.] Let $a, b \in \mathbb{R}$. Suppose that $a < b$. We saw in Example 6.5.12 that $[a, b] \sim (a, b)$. That proof was apparently brief, though the brevity was illusory, because the proof relied upon our work proving first Zorn's Lemma (Theorem 3.5.6), and then the Schroeder–Bernstein Theorem (Theorem 6.5.10). Moreover, the proof in Example 6.5.12 did not explicitly exhibit a bijective function between the two intervals, and as such is not as concrete as possible.

In this exercise the reader is asked to prove that $[a, b] \sim (a, b)$ by finding a bijective function $f : [a, b] \to (a, b)$. Consider functions that are not continuous.

Exercise 6.5.15. The proof of the Schroeder–Bernstein Theorem (Theorem 6.5.10), the bulk of which is found in the proof of Lemma 6.5.11, makes use of Definition by Recursion, and hence it makes use of the properties of the natural numbers. However, the statement of the Schroeder–Bernstein Theorem does not involve the natural numbers, and it would be nice to have a proof of the theorem that does not involve any particular set of numbers. The purpose of this exercise is to provide such a proof of Lemma 6.5.11. This alternative proof is, unfortunately, even less transparent than the proof of the lemma found in the text. Essentially, the idea is to replace the recursive process with the notion of a fixed point, as defined in Exercise 4.2.15.

Let A, B and C be sets. Suppose that $C \subseteq B \subseteq A$, and that $A \preccurlyeq C$. Then there is an injective function $f : A \to C$.

   (1) Let $g : \mathcal{P}(A) \to \mathcal{P}(A)$ be defined by $g(X) = [B - f(A)] \cup f(X)$ for all $X \in \mathcal{P}(A)$. It follows from Theorem 4.2.4 (4) that g is monotone, as defined in Exercise 4.2.15. We then use that exercise to deduce that there is some $V \in \mathcal{P}(A)$ such that $g(V) = V$. Prove that $B = V \cup [f(A) - f(V)]$, and that $V \cap [f(A) - f(V)] = \emptyset$.   [Use Exercise 3.3.13 (1).]
   (2) Let $h : A \to B$ be defined by

$$h(x) = \begin{cases} f(x), & \text{if } x \in A - V \\ x, & \text{if } x \in V. \end{cases}$$

       Prove that this function is well-defined. More specifically, prove that $h(x) \in B$ for all $x \in A$.   [Use Exercise 4.4.11.]
   (3) Prove that the function h defined in Part (2) of this exercise is bijective. Conclude that $A \sim B$.   [Use Exercise 4.4.11.]

6.6 Finite Sets and Countable Sets

In Section 6.5 we looked at the general idea of sets having the same cardinality. We now give a more detailed look at two of the types of sets we saw in Definition 6.5.4, namely, finite sets and countable sets.

For sets in general, we did not assign a numerical value to each set that would be called the "size" of the set, because for infinite sets we would need to assign something other than real numbers (each of which is finite), and given what we have at our disposal in this text there are no other such "numbers" we can use. See [Pot04, Chapters 9 and 12] and [HJ99, Chapters 5 and 6] for discussion of cardinal and ordinal numbers, which are different types of "infinite numbers" that are relevant to the cardinality of sets.

For finite sets, however, we can assign a number to each set that represents how many elements are in the set. In Section 3.2 we mentioned the notation $|A|$ for the number of elements of a finite set A, and we subsequently used this notion repeatedly in an informal manner. We are now in a position to make this concept rigorous.

Definition 6.6.1. Let A be a set. Suppose that A is finite. The **cardinality** of A, denoted $|A|$, is defined as follows. If $A = \emptyset$, let $|A| = 0$. If $A \neq \emptyset$, let $|A| = n$, where $A \sim \{1, \ldots, n\}$.   △

The alert reader might have noticed a potential problem with Definition 6.6.1. Could it happen that a set has the same cardinality as both $\{1, \ldots, n\}$ and $\{1, \ldots, m\}$ for two different natural numbers n and m? If that could happen, then Definition 6.6.1 would make no sense. Our intuition tells us that this problem cannot occur, but that fact needs to be proved. Actually, we have already done the hard work of proving that fact in Theorem 6.3.11 (3), which immediately implies the following lemma, which we state without proof.

Lemma 6.6.2. *Let $n, m \in \mathbb{N}$. Then $\{1, \ldots, n\} \sim \{1, \ldots, m\}$ if and only if $n = m$.*

We leave it to the reader to deduce the following corollary to Lemma 6.6.2.

Corollary 6.6.3. *Let A and B be sets. Suppose that A and B are finite. Then $A \sim B$ if and only if $|A| = |B|$.*

Although Corollary 6.6.3 seems rather obvious, it actually tells us something of real substance. Recall the problem of finding hotel rooms for people mentioned at the start of this section. We stated that there were two ways to compare the size of the set of people wanting to stay at the hotel and the size of the set of available hotel rooms: pairing up elements of the two sets, or counting the number of elements in each set and comparing the numbers. In the two approaches we compare different things, namely, sets in the first approach and numbers in the second. Corollary 6.6.3 tells us that we will always obtain the same result by either method.

Example 6.6.4. Let $B = \{1, 4, 9, 16\}$. We can formally show that $|B| = 4$ by showing that $B \sim \{1, \ldots, 4\} = \{1, 2, 3, 4\}$. To prove this last claim, let $h: B \to \{1, \ldots, 4\}$ be defined by $h(x) = \sqrt{x}$ for all $x \in B$. It is easy to verify that the function h is bijective. Needless to say, the use of a formal proof to demonstrate that $|B| = 4$ in this particular case is a bit of overkill, and we will not feel the need to give any more such proofs concerning the cardinalities of such finite sets. It is nice to know, however, that such proofs can be constructed.   ◇

We now see the most basic properties of the cardinalities of finite sets. The reader has probably used these properties many times without having had a second thought,

though of course the properties need to be proved. Additional properties of the cardinalities of finite sets may be found in Sections 7.6 and 7.7.

Theorem 6.6.5. *Let A be a set. Suppose that A is finite.*

1. *If $X \subseteq A$, then X is finite.*
2. *If $X \subseteq A$, then $|A| = |X| + |A - X|$.*
3. *If $X \subsetneqq A$, then $|X| < |A|$.*
4. *If $X \subsetneqq A$, then $X \not\sim A$.*

Proof.

(1). This part of the theorem follows immediately from Theorem 6.3.11 (2).

(2). If $A - X = \emptyset$, then the result is trivial, so assume otherwise. Let $n = |A|$. Because $A - X \neq \emptyset$, then $A \neq \emptyset$, and therefore $n \neq 0$. Let $f : A \to \{1, \ldots, n\}$ be a bijective function. We can then apply Theorem 6.3.11 (2) to the subset $f(X)$ of $\{1, \ldots, n\}$ to find a bijective function $g : \{1, \ldots, n\} \to \{1, \ldots, n\}$ such that $g(f(X)) = \{1, \ldots, k\}$ for some $k \in \mathbb{N}$ such that $k \leq n$. By Lemma 4.4.4 (3) we see that $g \circ f$ is bijective. It then follows from Exercise 6.5.4 and Exercise 4.3.5 that $X \sim \{1, \ldots, k\}$, which means that $|X| = k$. Using Exercise 4.3.5 again and Exercise 4.4.11, we see that

$$(g \circ f)(A - X) = (g \circ f)(A) - (g \circ f)(X) = g(f(A)) - g(f(X))$$
$$= \{1, \ldots, n\} - \{1, \ldots, k\} = \{k+1, \ldots, n\}.$$

It follows from Exercise 6.5.4 that $A - X \sim \{k+1, \ldots, n\}$. By Exercise 6.2.2 (2) there is a bijective function from $\{k+1, \ldots, n\}$ to $\{1, \ldots, n-k\}$. We deduce that $A - X \sim \{1, \ldots, n-k\}$, and hence that $|A - X| = n - k$. The desired result now follows.

(3). This part of the theorem follows from Part (2).

(4). This part of the theorem follows from Part (3) and Corollary 6.6.3.   □

The following result is a simple corollary to Theorem 6.6.5 (1); details are left to the reader.

Corollary 6.6.6. *Let A be a set. Then A is infinite if and only if it contains an infinite subset.*

Theorem 6.6.5 (4) might seem trivial, but it should not be taken for granted, because it does not hold for all sets. For example, the set of natural numbers $\mathbb{N}$ is a proper subset of $\mathbb{Z}$, and yet we saw in Example 6.5.3 (2) that $\mathbb{N} \sim \mathbb{Z}$. In fact, as we will see in Theorem 6.6.12 below, Theorem 6.6.5 (4) completely characterizes finite sets. In order to prove this characterization, however, we need to learn more about countable sets, and it is to that topic that we now turn.

Formally, a set is countably infinite if it has the same cardinality as $\mathbb{N}$. Intuitively, that means that a set is countably infinite if its elements can be "lined up" in some order, so that the set has a first element, a second element and so on, in the same way that the elements of $\mathbb{N}$ are lined up. As an example of how to line up the elements of a countably infinite set, recall Example 6.5.3 (2), in which we saw a bijective function

$f\colon \mathbb{N} \to \mathbb{Z}$, which showed that $\mathbb{Z}$ is countably infinite. If we think of the integers in increasing order, which we standardly write as $\ldots, -2, -1, 0, 1, 2, \ldots$, then there is no obvious "first integer," "second integer" and so on. However, we can use the bijective function f to line up the integers in an alternative way. Because the function f is bijective, we know that the sequence $f(1), f(2), f(3), f(4), \ldots$ contains each integer once and only once. Using the definition of the function f, we see that $f(1)$, $f(2), f(3), f(4), \ldots$ equals $0, 1, -1, 2, -2, \ldots$, and we therefore have the entire set of integers nicely arranged in a way that has a first element, second element and so on. Of course, this arrangement of the integers is not in order of increasing size, but it would be too much to expect that. We saw in Corollary 6.5.8 that there are uncountable sets, which means that there are infinite sets that cannot be lined up so that there is a first element, a second element and so on.

For our first result about countable sets, recall that Theorem 6.6.5 (1) stated that a subset of a finite set is finite. The following theorem shows that the analogous result is true for countable sets as well. This theorem shows why it is often useful to work with the broader concept of countable sets, rather than the narrower concept of countably infinite sets, because the theorem would not be true if we replaced "countable" with "countably infinite"; observe that a subset of a countably infinite set need not be countably infinite, because it can be finite.

The intuitive idea of the proof of the theorem is as follows. The interesting case in the proof is when X is an infinite subset of $\mathbb{N}$. Because X is non-empty, we can apply the Well-Ordering Principle (Theorem 6.2.5) to find some $c_1 \in X$ such that $c_1 \leq x$ for all $x \in X$. Then $c_1 < x$ for all $x \in X - \{c_1\}$. Let $X_2 = X - \{c_1\}$. Because X is infinite, then $X_2 \neq \emptyset$, and by the same argument as before there is some $c_2 \in X_2$ such that $c_2 < x$ for all $x \in X_2 - \{c_2\} = X - \{c_1, c_2\}$. Let $X_3 = X - \{c_1, c_2\}$. We can continue this process forever, and we therefore obtain a sequence $c_1, c_2, c_3, \ldots$ in X such that $c_1 < c_2 < c_3 < \cdots$. The rest of the proof consists of showing that this sequence in fact contains all the elements of X. Because all the elements of X can be lined up $c_1, c_2, c_3, \ldots$, and because X is infinite, it follows that X is countably infinite. However, the phrase "we can continue this process forever" is not rigorous, and we make this proof rigorous by using the version of Definition by Recursion given in Theorem 6.4.8. The function $f\colon \mathbb{N} \to A$ in the proof replaces the sequence $c_1, c_2, c_3, \ldots$. Before proceeding, the reader should review the notation given in Definition 6.4.7.

Theorem 6.6.7. *Let A be a set. Suppose that A is countable. If $X \subseteq A$, then X is countable.*

Proof. We follow [Mun00, Section 7]. Let $X \subseteq A$.

If A is finite, then by Theorem 6.6.5 (1) we know that X is finite, and hence it is countable. Now assume that A is countably infinite. We will prove the theorem for the special case that $A = \mathbb{N}$. For the general case, we observe that if A is countably infinite, then there is a bijective function $f\colon A \to \mathbb{N}$, and the desired result follows from the fact that $X \sim f(X)$, which holds by Exercise 6.5.4, and that $f(X)$ is a subset of $\mathbb{N}$.

Suppose that $A = \mathbb{N}$. If X is finite, then it is countable by definition, and there is nothing to prove. Now suppose that X is infinite.

By the Well-Ordering Principle (Theorem 6.2.5), there is a unique element $b \in X$ such that $b \leq x$ for all $x \in X$. Let $k \colon G(X) \to X$ be defined as follows. Let $g \in G(X)$. Then $g \in \mathcal{F}(\{1,\ldots,n\}, X)$ for some $n \in \mathbb{N}$, which means that g is a function $\{1,\ldots,n\} \to X$. It follows from Exercise 6.6.3 that g cannot be surjective, and hence $X - g(\{1,\ldots,n\}) \neq \emptyset$. Using the Well-Ordering Principle again we see that there is a unique element $z_g \in X - g(\{1,\ldots,n\})$ such that $z_g \leq x$ for all $x \in X - g(\{1,\ldots,n\})$. We then let $k(g) = z_g$.

We can apply Theorem 6.4.8 to b and k as above, and we deduce that there is a unique function $f \colon \mathbb{N} \to A$ such that $f(1) = b$, and that $f(n+1) = k(f|_{\{1,\ldots,n\}})$ for all $n \in \mathbb{N}$. Hence $f(1) \leq x$ for all $x \in X$, and if $n \in \mathbb{N}$, then $f(n+1) \in X - [f|_{\{1,\ldots,n\}}](\{1,\ldots,n\}) = X - f(\{1,\ldots,n\})$, and so $f(n+1) \leq y$ for all $y \in X - f(\{1,\ldots,n\})$.

Let $r \in \mathbb{N}$. Then $f(r) \leq y$ for all $y \in X - f(\{1,\ldots,r-1\})$, where we think of $\{1,\ldots,0\}$ as the empty set when $r = 1$. Because $f(r+1) \in X - f(\{1,\ldots,r\}) \subseteq X - f(\{1,\ldots,r-1\})$, it follows that $f(r) < f(r+1)$. By Exercise 6.3.4 we see that $f(n) \geq n$ for all $n \in \mathbb{N}$.

We now show that f is bijective. Let $i, j \in \mathbb{N}$. Suppose that $i \neq j$. Without loss of generality assume that $i < j$. Then $i \leq j - 1$, and also $j > 1$, so that $j - 1 \in \mathbb{N}$. It follows that $f(i) \in f(\{1,\ldots,j-1\})$, and as observed above we know that $f(j) \in X - f(\{1,\ldots,j-1\})$. Therefore $f(i) \neq f(j)$, and we deduce that f is injective.

Let $m \in X$. Suppose that $m \neq f(p)$ for any $p \in \mathbb{N}$. Using a previous observation we know that $m \leq f(m)$, and hence $m < f(m)$. On the other hand, we saw above that $f(m) \leq y$ for all $y \in X - f(\{1,\ldots,m-1\})$. By hypothesis on m we know that $m \notin f(\{1,\ldots,m-1\})$, and it follows that $f(m) \leq m$, which is a contradiction. Therefore f is surjective.

We conclude that f is bijective, which implies that $X \sim \mathbb{N}$. Hence X is countably infinite, and therefore countable. $\qquad\square$

In order to show that a set is countable, it is necessary to show that it is either finite or countably infinite. It will be convenient to unify these two cases via the following theorem, which also has the advantage of allowing us to show only that a function is injective or surjective, rather than having to show that it is bijective. We will use this theorem in subsequent proofs.

Theorem 6.6.8. *Let A be a non-empty set. The following are equivalent.*

    a. *The set A is countable.*
    b. *There is an injective function $f \colon A \to \mathbb{N}$.*
    c. *There is a surjective function $g \colon \mathbb{N} \to A$.*

Proof.

(a) $\Rightarrow$ (b). Suppose that A is countable. There are two cases, depending upon whether A is finite or countably infinite. If A is finite, there is a bijective function $k \colon A \to \{1,\ldots,n\}$ for some $n \in \mathbb{N}$, and hence there is an injective function $\hat{k} \colon A \to \mathbb{N}$, because $\{1,\ldots,n\} \subseteq \mathbb{N}$. If A is countably infinite, there is a bijective function $h \colon X \to \mathbb{N}$, which is injective.

(b) ⇒ (a). Suppose that there is an injective function $f\colon A \to \mathbb{N}$. Because f is injective, it follows from Exercise 6.5.4 that $A \sim f(A)$. By Theorem 6.6.7 we know that $f(A)$ is countable, and therefore A is countable.

(b) ⇔ (c). Suppose that there is an injective function $f\colon A \to \mathbb{N}$. By Theorem 4.4.5 (2) the function f has a left inverse, say $g\colon \mathbb{N} \to A$. By Exercise 4.4.13 (1) we see that g is surjective. The other implication is proved similarly, and we omit the details.   □

Are unions, intersections and products of countable sets always countable? The answer is yes for intersections, as seen in Theorem 6.6.9 (1) below, but not always for unions and products. For example, let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I. If I is uncountable, and if each A_i has at least one element that is not in any other set A_k, then $\bigcup_{i \in I} A_i$ will have a subset that has the same cardinality as I, and hence it is uncountable by Exercise 6.6.7. Also, the set $\{0,1\}$ is countable, and yet $\{0,1\}^{\mathbb{N}}$ is uncountable, as can be seen using the comment after Definition 4.5.7 together with Exercise 6.7.7.

The best we can do regarding unions and products of countable sets is seen in the following two theorems. To form an intuitive picture of why the union of countably many countable sets is itself countable, consider first the union of two countable sets A and B. We can line up each of their elements as $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$. We can then line up the elements of $A \cup B$ as $a_1, b_1, a_2, b_2, \ldots$, where we drop any element that is the same as an element previously listed (which could happen because A and B might have elements in common). A picture for the union of countably many countable sets is seen in Figure 6.6.1, where the elements of the union are "lined up" in the order shown by the arrows, and where again we drop any element that is the same as an element previously listed.
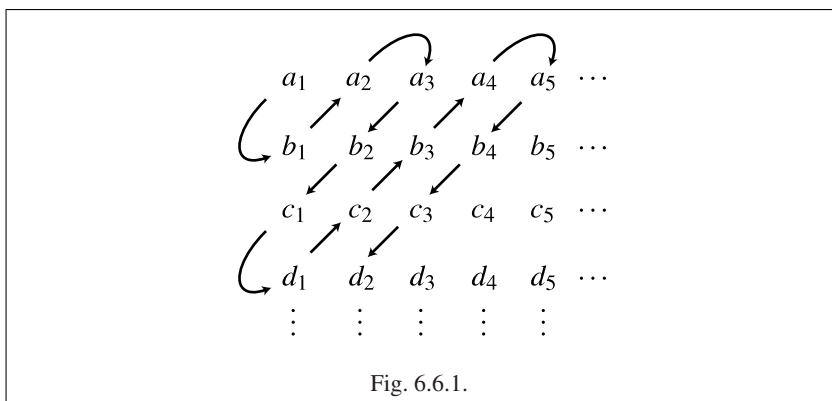
Fig. 6.6.1.

Theorem 6.6.9. *Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I. Suppose that A_i is countable for each $i \in I$.*

1. $\bigcap_{i \in I} A_i$ is countable.
2. If I is countable, then $\bigcup_{i \in I} A_i$ is countable.

Proof.

(1). Choose some $k \in I$. Then $\bigcap_{i \in I} A_i \subseteq A_k$, and hence $\bigcap_{i \in I} A_i$ is countable by Theorem 6.6.7.

(2). If $A_i = \emptyset$ for all $i \in I$, then $\bigcup_{i \in I} A_i = \emptyset$, which implies that $\bigcup_{i \in I} A_i$ is finite, and hence countable. Now assume that $A_k \neq \emptyset$ for some $k \in I$. Because the empty set contributes nothing to a union of sets, the set $\bigcup_{i \in I} A_i$ will not be changed if we delete from I those elements $s \in I$ such that $A_s = \emptyset$. Let us assume that that has been done, and therefore that $A_i \neq \emptyset$ for all $i \in I$.

There are two cases, depending upon whether I is countably infinite or is finite. We prove the former case, leaving the other case to the reader in Exercise 6.6.12. Because we are assuming that I is countably infinite, without loss of generality we may assume that $I = \mathbb{N}$.

Because A_i is countable for all $i \in I$, then by Theorem 6.6.8 there is a surjective function $f_i \colon \mathbb{N} \to A_i$ for each $i \in I$. Let $g \colon \mathbb{N} \to \bigcup_{i \in I} A_i$ be defined as follows. Let $r \in \mathbb{N}$. We can apply Exercise 6.3.14 to the function $f \colon \mathbb{N} \to \mathbb{N}$ defined by $f(n) = \frac{(n-1)n}{2}$ for all $n \in \mathbb{N}$, and we deduce that there are unique $n, p \in \mathbb{N}$ such that $\frac{(n-1)n}{2} < r \leq \frac{n(n+1)}{2}$ and $r = \frac{(n-1)n}{2} + p$. Let $g(r) = f_{n-p+1}(p)$.

Let $x \in \bigcup_{i \in I} A_i$. Then $x \in A_k$ for some $k \in I$. Because f_k is surjective, there is some $w \in \mathbb{N}$ such that $x = f_k(w)$. Let $t = k + w - 1$. The reader can then verify that $g\left(\frac{(t-1)t}{2} + w\right) = f_{t-w+1}(w) = f_k(w) = x$. Therefore g is surjective, and it follows from Theorem 6.6.8 that $\bigcup_{i \in I} A_i$ is countable. $\qquad\square$

Observe that in the proof of Theorem 6.6.9 (2), we simultaneously had to choose a surjective function $f_i \colon \mathbb{N} \to A_i$ for each $i \in I$; there really is a choice to be made, because there is more than one such function for each $i \in I$ (except when A_i has only one element in it). Hence, we are making use of the Axiom of Choice (Theorem 4.1.5). To use that axiom formally in this proof, we would let $\mathcal{S}_i$ denote the set of all surjective functions $\mathbb{N} \to A_i$ for each $i \in I$, and we would apply the Axiom of Choice to the family of sets $\{\mathcal{S}_i\}_{i \in I}$; we omit the details. It is pointed out in [Vau95, p. 56] that any proof of Theorem 6.6.9 (2) requires the Axiom of Choice.

Theorem 6.6.10. *Let $A_1, \ldots, A_n$ be sets for some $n \in \mathbb{N}$. Suppose that $A_1, \ldots, A_n$ are countable. Then $A_1 \times \cdots \times A_n$ is countable.*

Proof. The result is trivial when $n = 1$. In Exercise 6.6.8 there is a proof of this result for the case $n = 2$. The general result follows by induction on n; the details are left to the reader. $\qquad\square$

Infinite sets come in different cardinalities, for example countable and uncountable. As remarked after Definition 6.5.9, among the uncountable sets there are sets of different cardinalities. Among all the different types of infinite sets, it would seem

intuitively plausible that countably infinite sets are the "smallest." We now have the tools to prove this fact.

Theorem 6.6.11. *Let A be a set. If A is infinite, then A has a countably infinite subset.*

Proof. Suppose that A is infinite. By the Trichotomy Law for Sets (Theorem 6.5.13) we know that $\mathbb{N} \preccurlyeq A$ or $A \preccurlyeq \mathbb{N}$.

First, suppose that $\mathbb{N} \preccurlyeq A$. Then there is an injective function $f \colon \mathbb{N} \to A$. By Exercise 6.5.4 we know that $\mathbb{N} \sim f(\mathbb{N})$. Hence $f(\mathbb{N})$ is a countably infinite subset of A.

Second, suppose that $A \preccurlyeq \mathbb{N}$. Then there is an injective function $g \colon A \to \mathbb{N}$. By Exercise 6.5.4 again we know that $A \sim g(A)$. Because $g(A) \subseteq \mathbb{N}$, it follows from Theorem 6.6.7 that $g(A)$ is countable. Hence A is countable. Because A is infinite, then it must be countably infinite, and hence A has a countably infinite subset, namely, itself. ☐

We conclude this section with the following promised characterization of finite sets, for which we now have the necessary tools.

Theorem 6.6.12. *Let A be a set. Then A is finite if and only if A has no proper subset with the same cardinality as A.*

Proof. Suppose that A is finite. Let $X \subsetneqq A$. Theorem 6.6.5 (4) implies that $X \nsim A$.

Suppose that A is infinite. Then by Theorem 6.6.11 we know that A has a countably infinite subset. Let $X \subseteq A$ be countably infinite. By Exercise 6.6.6 there is a function $f \colon X \to X$ that is injective but not surjective. Let $g \colon A \to A$ be defined by

$$g(a) = \begin{cases} f(a), & \text{if } a \in X \\ a, & \text{if } a \in A - X. \end{cases}$$

It is left to the reader to verify that g is injective but not surjective. Because g is injective it follows from Exercise 6.5.4 that $A \sim g(A)$, and because g is not surjective we see that $g(A) \subsetneqq A$. ☐

The proof of Theorem 6.6.12 may be short, but it is not at all trivial, because it uses Theorem 6.6.11, which in turn uses the Trichotomy Law for Sets (Theorem 6.5.13), which in turn relies upon the Axiom of Choice.

The characterization of finite sets in Theorem 6.6.12 is quite nice, because it does not make any reference to the natural numbers. Some authors in fact take this property as the definition of finiteness, and deduce our definition. An alternative way of stating this characterization of finiteness is that if A is a finite set, then a function $f \colon A \to A$ is bijective if and only if it is injective if and only if it is surjective. The reader is asked to prove this fact in Exercise 6.6.4. For an infinite set B, by contrast, a surjective or injective function $g \colon B \to B$ need not be bijective; an example of an injective function that is not surjective is used in the proof of Theorem 6.6.12, and any left inverse of such a function would be surjective but not injective.

Exercises

Exercise 6.6.1. **[Used in Theorem 7.6.7.]** Let A and B be sets. Suppose that A and B are finite. Prove that $A \cup B$ is finite.

Exercise 6.6.2. **[Used in Lemma 8.2.2.]** Let $A \subseteq \mathbb{N}$ be a subset. Suppose that there is some $M \in \mathbb{N}$ such that $a \leq M$ for all $a \in A$. Prove that A is finite.

Exercise 6.6.3. **[Used in Theorem 6.6.7.]** Let A be a set. Prove that A is finite if and only if there is an injective function $f : A \to \{1, \ldots, n\}$ for some $n \in \mathbb{N}$ if and only if there is a surjective function $f : \{1, \ldots, n\} \to A$ for some $n \in \mathbb{N}$.

Exercise 6.6.4. **[Used in Section 6.6 and Theorem 7.7.4.]** Let A and B be sets, and let $f : A \to B$ be a function. Suppose that A and B are finite sets, and that $|A| = |B|$. Prove that f is bijective if and only if f is injective if and only if f is surjective.

Exercise 6.6.5. **[Used in Section 8.2.]** Let $F \subseteq \mathbb{N}$ be a set. Suppose that F is finite and non-empty. Use Theorem 6.3.11 (1) to prove that there is some $k \in F$ such that $p \leq k$ for all $p \in F$.

Exercise 6.6.6. **[Used in Theorem 6.6.12.]** Let X be a set. Suppose that X is countably infinite. Prove that there is a function $f : X \to X$ that is injective but not surjective.

Exercise 6.6.7. **[Used in Section 6.6 and Exercise 6.7.7.]** Let A be a set. Prove that A is uncountable if and only if it contains an uncountable subset.

Exercise 6.6.8. **[Used in Theorem 6.6.10.]** Let A and B be sets. Suppose that A and B are countable. Prove that $A \times B$ is countable.

Exercise 6.6.9. Let A and F be sets. Suppose that A is countably infinite set, and that F is finite and non-empty.

   (1) Prove that $A \times F$ is countably infinite by constructing an explicit bijective function $A \times F \to \mathbb{N}$. Suppose that $F \sim \{1, \ldots, n\}$ for some $n \in \mathbb{N}$. First, find a bijective function $g : \mathbb{N} \times \{1, \ldots, n\} \to \mathbb{N}$, using the Division Algorithm (Theorem A.5 in the Appendix). Second, use the function g to define a bijective function $f : A \times F \to \mathbb{N}$. Prove that the functions you have defined are bijective.
   (2) Prove that $A \times F$ is countably infinite by using results in the text, but without finding an explicit bijective function $A \times F \to \mathbb{N}$.

Exercise 6.6.10. Let A be an uncountable set, and let T be any non-empty set. Prove that $A \times T$ is uncountable.

Exercise 6.6.11. Let A and B be sets.

   (1) Let $f : A \to B$ be a function. Suppose that f has a left inverse but no right inverse. Prove that if A is infinite, or if $B - f(A)$ is infinite and A has at least two elements, then f has infinitely many left inverses.
   (2) Let $k : A \to B$ be a function. Suppose that k has a right inverse but no left inverse. Let

$$S = \{b \in B \mid k^{-1}(\{b\}) \text{ has more than one element}\}.$$

Prove that if S is infinite, or if $k^{-1}(\{t\})$ is infinite for some $t \in S$, then k has infinitely many right inverses.

Exercise 6.6.12. [Used in Theorem 6.6.9.] Prove Theorem 6.6.9 (2) in the case that I is finite. Without loss of generality we may assume that $I = \{1, \ldots, s\}$ for some $s \in \mathbb{N}$. The fact that the result has been proved in the case where I is countably infinite can be used in the proof of the finite case. [Use Exercise 6.3.14.]

6.7 Cardinality of the Number Systems

In this section we use the results of the previous sections of this chapter to discuss the cardinality of the standard number systems, which are the natural numbers, the integers, the rational numbers, the real numbers and the complex numbers. Of course, the set $\mathbb{N}$ is countably infinite by definition. We know by Lemma 6.5.5 (1) that $\mathbb{N}$ is infinite. Because all the other number systems under discussion contain $\mathbb{N}$, they are all infinite by Corollary 6.6.6. The question is then determining which number systems are countable and which are uncountable.

We saw in Example 6.5.3 (2) that the set $\mathbb{Z}$ is countably infinite. If we think of the set of real numbers as forming the "number line," we then view the integers as sitting discretely in $\mathbb{R}$, that is, there are gaps between the integers. The rational numbers, by contrast, are "dense" in $\mathbb{R}$, in that between any two real numbers, no matter how close, we can always find a rational number. A proof of this fact is beyond the scope of this book; see [Blo11, Theorem 2.6.13] for details. It therefore might appear that there are "more" rational numbers than integers. The following theorem shows that our intuition here is deceiving.

Theorem 6.7.1. *The set $\mathbb{Q}$ is countably infinite.*

Proof. We have just remarked that the set $\mathbb{Z}$ is countably infinite, and hence it is countable. Let $\mathbb{Z}^* = \mathbb{Z} - \{0\}$. It follows from Exercise 6.5.8 (1) that $\mathbb{Z}^*$ is also countable. By Theorem 6.6.10 we know that $\mathbb{Z} \times \mathbb{Z}^*$ is countable, and it follows from Theorem 6.6.8 that there is a surjective function $g \colon \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}^*$. Let $f \colon \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}$ be defined by $f((m,n)) = \frac{m}{n}$ for all $(m,n) \in \mathbb{Z} \times \mathbb{Z}^*$. Given that $\mathbb{Q}$ consists of all fractions, it is evident that f is surjective. By Lemma 4.4.4 (2) we see that $f \circ g$ is a surjective function $\mathbb{N} \to \mathbb{Q}$. Hence $\mathbb{Q}$ is countable by Theorem 6.6.8. Because $\mathbb{Q}$ is infinite, as previously remarked, it is therefore countably infinite. $\square$

Theorem 6.7.1 tells us that in principle the elements of $\mathbb{Q}$ can be "lined up" in some order, so that $\mathbb{Q}$ has a first element, a second element and so on, in the same way that the elements of $\mathbb{N}$ are lined up, although this lining up of the elements of $\mathbb{Q}$ will not necessarily be according to increasing size. However, the proof of the theorem does not tell us explicitly how to line up the elements of $\mathbb{Q}$. In Figure 6.7.1 we see a diagram, due to Cantor, that summarizes a well-known way of lining up the positive rational numbers: follow the path indicated by the arrows, and drop every

fraction that is equal to one that has already been encountered. (An alternative way to line up the positive rational numbers is given in Exercise 6.7.9; this approach is a bit trickier than Cantor's method, but it has the aesthetic appeal of never encountering any number twice, and therefore avoiding the need to drop repeated numbers as in Cantor's method.)

Fig. 6.7.1.

Another set of numbers that is countable, and which is even larger than $\mathbb{Q}$, is the set of algebraic numbers, which is the set of all roots of polynomials with rational coefficients. (We are referring to real roots here, so that the set of algebraic numbers is a subset of $\mathbb{R}$.) Every rational number is algebraic, but there are also many irrational numbers that are algebraic, for example $\sqrt{2}$, which is a solution of the equation $x^2 - 2 = 0$. There are also many non-algebraic numbers (called transcendental numbers), for example π and e, though it is not trivial to prove that these numbers are not algebraic; see [Her75, Section 5.2] for details.

Theorem 6.7.2. *The set of algebraic numbers is countably infinite.*

Proof. Left to the reader in Exercise 6.7.3.   □

We now turn to the set of all real numbers, which is our first concrete example of an uncountable set. (We already saw an uncountable set in Corollary 6.5.8, but that set is not as familiar as $\mathbb{R}$.) The proof that $\mathbb{R}$ is uncountable was a major breakthrough due to Cantor. We follow his proof, often referred to as "Cantor's diagonal argument." For this proof we will need to use the fact that every real number can be expressed as an infinite decimal, and that this decimal expansion is unique if decimal expansions that eventually become the number 9 repeating are not allowed. The proof of this fact is beyond the scope of this book; see [Blo11, Section 2.8] for details. The rational numbers can be shown to be precisely those real numbers with decimal expansions that are either repeating, or are zero beyond some point.

Theorem 6.7.3. *The set $\mathbb{R}$ is uncountable.*

Proof. Suppose to the contrary that $\mathbb{R}$ is countable. Because $\mathbb{R}$ is infinite, as already observed, it must be countably infinite. From Example 6.5.3 (4) we know that $(0,1) \sim \mathbb{R}$, and hence $(0,1)$ must be countably infinite. Let $f \colon \mathbb{N} \to (0,1)$ be a bijective function. For each $n \in \mathbb{N}$, we can write $f(n)$ as an infinite decimal $f(n) = 0.a_n^1 a_n^2 a_n^3 \ldots$, where the numbers $a_n^1, a_n^2, a_n^3, \ldots$ are integers in $\{0, 1, \ldots, 9\}$, and where the expansion does not eventually become the number 9 repeating.

For each $k \in \mathbb{N}$, let

$$b_k = \begin{cases} 1, & \text{if } a_k^k \neq 1 \\ 2, & \text{if } a_k^k = 1. \end{cases}$$

Observe that $b_k \neq a_k^k$ for all $k \in \mathbb{N}$. Let b be the number represented by the decimal expansion $b = 0.b_1 b_2 b_3 \ldots$. Because $b_k \neq 9$ for all $k \in \mathbb{N}$, then this decimal expansion corresponds to a unique number in $(0,1)$. We claim that $b \neq f(n)$ for all $n \in \mathbb{N}$. The decimal expansion of any real number is unique if it does not become the number 9 repeating, and therefore if two numbers have different such decimal expansions (even if the difference is by only one digit) then the two numbers are not equal. For each $n \in \mathbb{N}$, the n-th digit in the decimal expansion of $f(n)$ is a_n^n, whereas the n-th digit in the decimal expansion of b is b_n. Hence $b \neq f(n)$ for all $n \in \mathbb{N}$. We have therefore reached a contradiction to the surjectivity of f, and we deduce that $\mathbb{R}$ is not countable. $\qquad\square$

The proof of Theorem 6.7.3 is referred to as "Cantor's diagonal argument" because of the shaded line in Figure 6.7.2, which is the set of numbers that are modified in order to define the number $b = 0.b_1 b_2 b_3 \ldots$.

$$
\begin{aligned}
f(1) &= 0.\ a_1^1\ a_1^2\ a_1^3\ a_1^4\ \cdots \\
f(2) &= 0.\ a_2^1\ a_2^2\ a_2^3\ a_2^4\ \cdots \\
f(3) &= 0.\ a_3^1\ a_3^2\ a_3^3\ a_3^4\ \cdots \\
f(4) &= 0.\ a_4^1\ a_4^2\ a_4^3\ a_4^4\ \cdots \\
&\ \ \vdots \qquad\qquad \vdots
\end{aligned}
$$

Fig. 6.7.2.
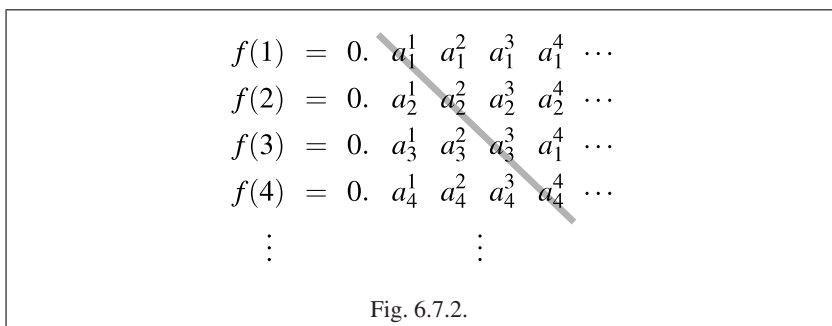
Although Cantor's diagonal argument is a very nice proof, it is not quite as simple as it might at first appear, because to put in all the details, it would be necessary to prove that every real number can be represented by an infinite decimal, and that this decimal representation is unique if decimal representations that eventually become the number 9 repeating are not allowed; unfortunately, such a proof is more difficult than might be expected, in part because it relies upon the Least Upper Bound

Property of the real numbers. This property of the real numbers is discussed very briefly in Example 7.4.11 (2), though a full discussion awaits the reader in a course on real analysis; see, for example, [Blo11, Section 2.6]. This reliance upon the decimal representation of real numbers not only makes the Cantor diagonal argument more difficult than it at first appears, but it is also somewhat bothersome in that the decimal representation of real numbers, while extremely useful from a computational perspective, is not conceptually at the heart of the real numbers. Hence, it would be nice to have a proof of the uncountability of the set of real numbers that is more directly related to the fundamental properties of these numbers. Such a proof, also due to Cantor (in fact prior to his diagonal argument), can be found in [Blo11, Theorem 8.4.8]; this proof, which makes use of sequences, is a special case of a more general theorem in topology, seen in [Mun00, pp. 176–177].

Theorem 6.7.3 tells us that $\mathbb{R} \not\sim \mathbb{N}$. There is, in fact, a much more precise relation between the cardinalities of $\mathbb{R}$ and $\mathbb{N}$, which is that $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$. A proof of this fact, making use of the Schroeder–Bernstein Theorem (Theorem 6.5.10), is given in Exercise 6.7.8.

The set of irrational numbers is defined to be the set of all real numbers that are not rational, that is, the set $\mathbb{R} - \mathbb{Q}$. There does not seem to be standard notation for the set of irrational numbers; we will use $\mathbb{IRR}$. The set $\mathbb{IRR}$ is uncountable, for if not, then the real numbers would have to be a countable set as well by Theorem 6.7.1 and Theorem 6.6.9 (2), because $\mathbb{R} = \mathbb{Q} \cup \mathbb{IRR}$. The following theorem shows that in fact $\mathbb{IRR} \sim \mathbb{R}$, which should not be taken as obvious, because not every uncountable set has the same cardinality as $\mathbb{R}$; for example $\mathcal{P}(\mathbb{R}) \not\sim \mathbb{R}$ by Theorem 6.5.7.

Theorem 6.7.4. *The set of irrational numbers has the same cardinality as $\mathbb{R}$.*

Proof. We follow [Ham82]. Let $P = \{\sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \ldots\}$. We know that $\sqrt{2} \in \mathbb{IRR}$ by Theorem 2.3.5. Using Exercise 2.3.4 it follows that all other members of P are also in $\mathbb{IRR}$, and therefore $P \subseteq \mathbb{IRR}$. It is straightforward to verify that P is countably infinite; we omit the details. By Theorem 6.7.1 and Theorem 6.6.9 (2) we see that $\mathbb{Q} \cup P$ is countable, and by Lemma 6.5.5 (2) and Corollary 6.6.6 we see that $\mathbb{Q} \cup P$ is countably infinite. Hence $\mathbb{Q} \cup P \sim P$. We now use Exercise 6.5.6 (2) to see that

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{IRR} = \mathbb{Q} \cup [P \cup (\mathbb{IRR} - P)] = (\mathbb{Q} \cup P) \cup (\mathbb{IRR} - P)$$
$$\sim P \cup (\mathbb{IRR} - P) = \mathbb{IRR}. \qquad \square$$

The following theorem is, once again, slightly counterintuitive.

Theorem 6.7.5. *Let $n \in \mathbb{N}$. Then $\mathbb{R}^n \sim \mathbb{R}$.*

Proof. The fact that $\mathbb{R}^2 \sim \mathbb{R}$ follows immediately from Exercise 6.7.4 (2). The proof that $\mathbb{R}^n \sim \mathbb{R}$ for arbitrary n is by induction on n; the details are left to the reader. $\quad \square$

In Exercise 6.7.5 it is seen that the set of complex numbers $\mathbb{C}$ also has the same cardinality as $\mathbb{R}$.

We now turn to a rather curious issue concerning the cardinalities of sets of numbers. Using the notation defined in Section 6.5, we know that $\mathbb{N} \preccurlyeq \mathbb{R}$, because the

inclusion function $i \colon \mathbb{N} \to \mathbb{R}$ is injective. From Theorem 6.7.3 we know that $\mathbb{N} \prec \mathbb{R}$. Is there a set X such that $\mathbb{N} \prec X \prec \mathbb{R}$? Cantor conjectured that there was no such set, and this conjecture is known as the Continuum Hypothesis. You might be tempted to try to look for such a set yourself, but you will not succeed. Nor, amazingly enough, will you succeed in proving that no such set exists. Due to the remarkable work of Kurt Gödel in 1938 and Paul Cohen in 1963, it turns out that the Continuum Hypothesis is independent of the Zermelo–Fraenkel Axioms for set theory (see Section 3.5 for a discussion of these axioms). In other words, the Continuum Hypothesis can neither be proved nor disproved from the Zermelo–Fraenkel Axioms. See [Mal79, Section 1.12] or [Vau95, Section 7.7] for further discussion (though the proof of Cohen's result is to be found only in more advanced texts). It follows that we either need to be satisfied with not being able to resolve the Continuum Hypothesis, or we need to find new axioms for set theory. Mathematicians have stuck to the standard axioms, because they have worked well so far, and therefore have decided to live with the odd situation regarding the Continuum Hypothesis.

We conclude this section with an application of cardinality to computer science.

Example 6.7.6. There are many general-purpose computer programming languages, such as Pascal, C++, Java, Haskell and Prolog, each with its particular features and conceptual approach. See [Set96] for a discussion of programming languages. Common to all these programming languages is that a program consists of a list of instructions, written using various code words and symbols that the programmer can understand, and which is then translated by the computer into machine operations. For example, a very short program in Haskell is

```
binom:: Integer -> Integer -> Integer
binom n 0 = 1
binom n k = if k == n then 1
            else binom (n - 1) k + binom (n - 1) (k - 1)
```

(This program calculates binomial coefficients recursively; see Section 6.4 for a discussion of Definition by Recursion, and Section 7.7 for a discussion of binomial coefficients. See [Hud00] for details about Haskell.)

What do computer programs do? Fundamentally, they cause the computer to take various input data (which could be the empty set), and for each possible input, produce some output data. Is there a programming language in which we could write sufficiently many different programs so that we could make the computer do any possible thing we might wish it to do? If not, then there would be a limitation on what we could do with computers. It might appear that this question would depend upon the type of computer (its memory, speed, etc.) and the choice of programming language. Somewhat surprisingly, it turns out that the answer to this question is the same for all computers and all computer languages: It is not possible to program any computer to do all possible things we might wish it to do. The key is the cardinality of sets.

As seen in the above example of a computer program, any computer program is a finite string of symbols, constructed out of an allowed list of symbols. In Haskell, for

example, the allowed symbols include the letters of the English alphabet (uppercase and lowercase versions of the same letter are considered to be different symbols), the digits $0, \ldots, 9$, various symbols such as $=$, $:$, $[$, $]$ and so on, and a blank space (which we also think of as a symbol). Repeated blank spaces and new lines are ignored by the computer (though they make it easier for human beings to read the code), so we can ignore them too. For a given computer programming language, let Σ denote the set of all possible symbols used, including the blank space symbol. The set Σ is always finite. Using the symbols in Σ, we can then write computer programs, which are simply certain finite strings of symbols in Σ, though of course not all strings will be valid programs. Let $S(\Sigma)$ denote the set of all finite strings with symbols in Σ, and let $C(\Sigma)$ denote the set of all valid programs using symbols in Σ. Then $C(\Sigma) \subseteq S(\Sigma)$.

As stated above, a computer program causes the computer to take various input data, and for each possible input, produce some output data. For a computer program written with the symbols Σ, both the input and the output are finite strings of symbols in Σ. Therefore each computer program in Σ causes the computer to act as a function $S(\Sigma) \to S(\Sigma)$. The collection of all such functions is denoted $\mathcal{F}(S(\Sigma), S(\Sigma))$, using the notation of Section 4.5. Putting these observations together, we see that each programming language using symbols in Σ gives rise to a function $\Phi \colon C(\Sigma) \to \mathcal{F}(S(\Sigma), S(\Sigma))$, where for each computer program p written with symbols in Σ, we obtain the function $\Phi(p) \colon S(\Sigma) \to S(\Sigma)$.

Our question stated above asking whether there is a computer programming language with which we could make the computer do anything we might wish it to do can now be expressed by asking whether there is some programming language such that the corresponding function Φ is surjective. If Φ were surjective, then every possible function $S(\Sigma) \to S(\Sigma)$ could be obtained from at least one computer program. On the other hand, if Φ were not surjective, then there would be at least one function $S(\Sigma) \to S(\Sigma)$ that we might want the programming language to do that could not be achieved.

The answer to our question is that regardless of the programming language and the set of symbols Σ used, and regardless of the computer used, the function Φ is never surjective. The reason is that $C(\Sigma)$ is always countable, and $\mathcal{F}(S(\Sigma), S(\Sigma))$ is always uncountable. The fact that there cannot be a surjective function from a countable set to an uncountable one follows from Theorem 6.6.8; the details are left to the reader.

To see that $C(\Sigma)$ is countable, we will show that $S(\Sigma)$ is countable, and then use Theorem 6.6.7. The set $S(\Sigma)$ is the collection of finite strings of elements of Σ. For each $n \in \mathbb{N}$, let $S_n(\Sigma)$ denote the set of strings of length n. Hence $S(\Sigma) = \bigcup_{n=1}^{\infty} S_n(\Sigma)$. It can be seen that $S_n(\Sigma)$ is a finite set for each $n \in \mathbb{N}$; this fact is intuitively clear, and can be seen rigorously using the ideas of Section 7.7. It follows that each set $S_n(\Sigma)$ is countable, and hence $S(\Sigma) = \bigcup_{n=1}^{\infty} S_n(\Sigma)$ is countable by Theorem 6.6.9 (2).

To see that $\mathcal{F}(S(\Sigma), S(\Sigma))$ is uncountable, we start by observing that because $S(\Sigma)$ is countable, and is clearly infinite, it must be countably infinite. Hence $S(\Sigma) \sim \mathbb{N}$. By Lemma 4.5.3 we see that $\mathcal{F}(S(\Sigma), S(\Sigma)) \sim \mathcal{F}(\mathbb{N}, \mathbb{N})$. Exercise 6.7.7 says that $\mathcal{F}(\mathbb{N}, \mathbb{N})$ is uncountable, and hence so is $\mathcal{F}(S(\Sigma), S(\Sigma))$.

We therefore see that cardinality considerations imply that there is a theoretical limitation to what can be accomplished by computer programming. See [Har96] for further discussion.   ◊

<div align="center">

Exercises

</div>

Exercise 6.7.1. Which of the following sets is countable, and which has the same cardinality as $\mathbb{R}$? Informal justification is acceptable.

(1) $\{\sqrt[n]{2} \mid n \in \mathbb{N}\}$.
(2) $\{q \in \mathbb{Q} \mid q$ has denominator a multiple of 3 when q is expressed in lowest terms$\}$.
(3) $\mathbb{Q} \cap [2,3)$.
(4) $[3,4] \cup [5,6]$.
(5) $\text{GL}_3(\mathbb{Z})$, which is the set of invertible 3×3 matrices with integer entries.
(6) $[0,1] \times [0,1]$.
(7) $\{9^x \mid x \in \mathbb{R}\}$.
(8) $\{S \subseteq \mathbb{N} \mid S$ has 7 elements$\}$.
(9) The set with elements that are the closed bounded intervals in $\mathbb{R}$ having rational endpoints.

[Use Exercise 6.5.6.]

Exercise 6.7.2. Prove that the set

$$S = \{x \in (0,1) \mid \text{the decimal expansion of } x \text{ has only odd digits}\}$$

is uncountable.

Exercise 6.7.3. [Used in Theorem 6.7.2.]

(1) Let $n \in \mathbb{N}$. Let A_n be the set of all roots of polynomials of degree n with rational coefficients. Prove that A_n is countable. You may assume the fact that a polynomial of degree n has at most n roots.
(2) Prove that the set of algebraic numbers is countably infinite.

Exercise 6.7.4. [Used in Theorem 6.7.5.]

(1) Prove that $(0,1) \times (0,1) \sim (0,1)$. Use the fact that every real number can be expressed uniquely as an infinite decimal, if decimal expansions that eventually become the number 9 repeating are not allowed.
(2) Let A and B be sets. Suppose that $A \sim \mathbb{R}$ and $B \sim \mathbb{R}$. Prove that $A \times B \sim \mathbb{R}$.

Exercise 6.7.5. [Used in Section 6.7.] This exercise is for the reader who is familiar with the complex numbers. Prove that the set of complex numbers $\mathbb{C}$ has the same cardinality as $\mathbb{R}$.

Exercise 6.7.6. Let $\mathcal{D}$ be a partition of $\mathbb{R}$ such that each element of $\mathcal{D}$ is an interval of some sort, other than an interval with only one element. Prove that $\mathcal{D}$ is countable. (Use the "density" of $\mathbb{Q}$ in $\mathbb{R}$, as mentioned in the text.)

Exercise 6.7.7. [Used in Section 6.6 and Example 6.7.6.] Prove that $\mathcal{F}(\mathbb{N}, \{0,1\})$ and $\mathcal{F}(\mathbb{N},\mathbb{N})$ are uncountable.   [Use Exercise 6.6.7.]

Exercise 6.7.8. [Used in Section 6.7.] The purpose of this exercise is to prove that $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$. As in the proof of Theorem 6.7.3, it will suffice to prove that $\mathcal{P}(\mathbb{N}) \sim (0,1)$. We will use the facts about decimal expansions of real numbers that were used in the proof of Theorem 6.7.3, as well as the analogous facts about binary expansions, according to which every number in the interval $(0,1)$ can be written uniquely in the form $0.b_1 b_2 b_3 \ldots$, where the numbers $b_1, b_2, b_3, \ldots$ are in the set $\{0,1\}$, and where the expansion does not eventually become the number 1 repeating. See [Blo11, Section 2.8] for a detailed proof of these facts about decimal and binary expansions.

By the Schroeder–Bernstein Theorem (Theorem 6.5.10), it will suffice to prove that $\mathcal{P}(\mathbb{N}) \preccurlyeq (0,1)$ and that $(0,1) \preccurlyeq \mathcal{P}(\mathbb{N})$.

    (1) Use the decimal expansion of numbers in $(0,1)$ to define an injective function $g\colon \mathcal{P}(\mathbb{N}) \to (0,1)$.
    (2) Use the binary expansion of numbers in $(0,1)$ to define an injective function $f\colon (0,1) \to \mathcal{P}(\mathbb{N})$.

Exercise 6.7.9. [Used in Section 6.7.] In Theorem 6.7.1 we saw that the set $\mathbb{Q}$ is countably infinite, which told us that in principle the elements of $\mathbb{Q}$ could be "lined up" in some order just like the elements of $\mathbb{N}$. Of course, it is nicer to see a concrete way of lining up the rational rational numbers, rather than just knowing that it is possible to do so in principle. In Figure 6.7.1 we saw a well-known way of lining up the positive rational numbers, due to Cantor. In that figure, the positive rational numbers were lined up by following the arrows, and dropping every fraction that is equal to one that had already been encountered. In this exercise we discuss an alternative way of lining up the positive rational numbers, having the aesthetic appeal of never encountering any number twice, and therefore avoiding the need to drop repeated numbers as in Cantor's procedure. (This alternative method is discussed in [CW00], where it is attributed to [Ste58].)

The alternative way of lining up the positive rational numbers is represented by the following diagram.
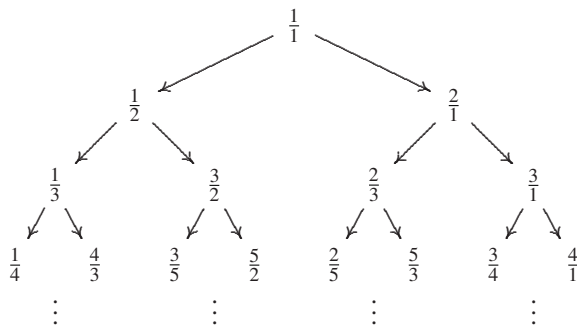
This diagram is constructed using Definition by Recursion, starting with $\frac{1}{1}$, and then adding one row at a time, where the fractions in each row are obtained from

those in the previous row by taking every fraction $\frac{a}{b}$ in the previous row and writing $\frac{a}{a+b}$ and $\frac{a+b}{b}$. We will prove below that every positive rational number, expressed as a fraction in lowest terms, is obtained precisely once by this procedure. We can therefore line up the positive rational numbers by stringing together the successive rows in the diagram, yielding

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, \frac{3}{1}, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, \frac{4}{1}, \dots .$$

To prove that this procedure works, it is easier if we replace each fraction of the form $\frac{a}{b}$ with the ordered pair (a,b). Observe that the fraction $\frac{a}{b}$ is in lowest terms if and only if the two numbers a and b are relatively prime, as defined in Exercise 2.4.3.

As in Exercise 4.4.8, let $\mathbb{L}$ be the set defined by

$$\mathbb{L} = \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ and } b \text{ are relatively prime}\},$$

and let $U, D \colon \mathbb{L} \to \mathbb{L}$ be defined by $U((a,b)) = (a+b,b)$ and $D((a,b)) = (a,a+b)$ for all $(a,b) \in \mathbb{L}$ (these functions are well-defined by Exercise 2.4.3).

We now define subsets $A_1, A_2, A_3, \dots \subseteq \mathbb{L}$ as follows. For each $n \in \mathbb{N}$, the set A_n will have 2^{n-1} elements, labeled as

$$A_n = \{c_n^1, c_n^2, \dots, c_n^{2^{n-1}}\}.$$

We define these elements using Definition by Recursion as follows. Let $c_1^1 = (1,1)$. Now suppose that the set A_n has been defined for some $n \in \mathbb{N}$. Then define the elements of A_{n+1} by $c_{n+1}^{2k-1} = D(c_n^k)$ and $c_{n+1}^{2k} = U(c_n^k)$ for all $k \in \{1, \dots, 2^{n-1}\}$. It is seen that this definition captures the procedure given in the above diagram.

To prove our desired result, we will show that $\bigcup_{i=1}^{\infty} A_i = \mathbb{L}$, and that there are no redundancies among the elements of the form c_i^x. More precisely, for each $n \in \mathbb{N}$, let $S_n = \bigcup_{i=1}^{n} A_i$. It will suffice to show that the following two claims hold for all $n \in \mathbb{N}$.

(1) The set S_n contains all $(a,b) \in \mathbb{L}$ such that $1 \le a \le n$ and $1 \le b \le n$. (There may also be other elements of $\mathbb{L}$ in S_n, but that does not matter.)
(2) All the elements in S_n are distinct, which means that $c_i^x = c_j^y$ if and only if $i = j$ and $x = y$, for all $i, j, x, y \in \mathbb{N}$ such that $0 \le i \le n$, and $0 \le j \le n$, and $1 \le x \le 2^i$, and $1 \le y \le 2^j$.

Prove both these claims. Use Exercise 2.4.3 and Exercise 4.4.8.

Part III
EXTRAS

Having completed the basics, we now turn to a number of additional topics. These topics were chosen because they contain accessible ideas from important areas of modern mathematics, and because they make use of the concepts we have learned so far. Due to space limitations, we will be a bit more terse in this part of the text than previously. Each section of Chapter 7 gives a very brief introduction to a particular topic; further details await courses in those areas. Section 7.1 treats binary operations, Sections 7.2 and 7.3 treat groups, Sections 7.4 and 7.5 treat partially ordered sets and lattices, Sections 7.6 and 7.7 treat enumeration, and Section 7.8 treats limits of sequences. In Chapter 8 we let the reader take over. In each of Sections 8.2–8.7 we briefly introduce a topic, which the reader is then urged to explore on her own; in Section 8.8 the reader has the opportunity to assume the role of a mathematics professor and critique some attempted proofs taken from actual homework exercises submitted by students.

7

Selected Topics

Don't just read it; fight it! Ask your own questions, look for your own examples, discover your own proofs.

– Paul Halmos (1916–2006)

7.1 Binary Operations

Among the most basic topics taught in elementary school mathematics are operations such as addition and multiplication of numbers. Each such operation takes two numbers, and produces a single resulting number. Another type of operation is negation of numbers, which takes a single number and produces another number. We can formalize both these types of operations using sets and functions.

Definition 7.1.1. Let A be a set. A **binary operation** on A is a function $A \times A \to A$. A **unary operation** on A is a function $A \to A$. $\triangle$

Let A be a set, and let $*\colon A \times A \to A$ be a binary operation. If $a, b \in A$, then it would be proper to denote the result of doing the operation $*$ to the pair (a, b) by writing $*((a, b))$. Such notation is quite cumbersome, however, and would not look like familiar binary operations such as addition of numbers. Hence, we will write $a * b$ instead of $*((a, b))$.

Binary operations are used throughout mathematics. We will prove only one very easy theorem about binary operations in this section, because it is hard to say much of interest about binary operations in general. Rather, we will look at various examples, and define certain important properties that binary relations may satisfy. An important use of binary operations and the properties will be seen in Sections 7.2 and 7.3.

Example 7.1.2.

(1) The sum of any two natural numbers is a natural number, and hence we can think of addition on $\mathbb{N}$ as a function $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, which means that addition is a

binary operation on $\mathbb{N}$. Subtraction is not a binary operation on $\mathbb{N}$, because the difference of two natural numbers is not always a natural number. However, subtraction is a binary operation on $\mathbb{Z}$.

(2) This example involves 2×2 matrices. See any introductory text on linear algebra, for example [AR05, Chapters 1 and 2], for the relevant information about matrices. Let $\mathrm{GL}_2(\mathbb{R})$ denote the set of invertible 2×2 matrices with real number entries. (The notion of an inverse matrix was discussed very briefly just before Theorem 2.5.2, and is discussed in detail in any introductory text on linear algebra.) Such matrices are precisely those with non-zero determinant.

Let $\cdot$ denote matrix multiplication (again, see any introductory text on linear algebra for details). Then $\cdot$ is a binary operation on $\mathrm{GL}_2(\mathbb{R})$, because the product of two matrices with non-zero determinant also has non-zero determinant. On the other hand, matrix addition is not a binary operation on $\mathrm{GL}_2(\mathbb{R})$, because two matrices with non-zero determinant could add up to a matrix with zero determinant (the reader should supply an example).

(3) Just as multiplication of numbers is often taught by using multiplication tables, we can define binary operations on finite sets by using operation tables. For example, let $Z = \{p, q, r\}$. We define a binary operation $\star$ on Z by the operation table

$$
\begin{array}{c|ccc}
\star & p & q & r \\
\hline
p & r & p & q \\
q & p & q & r \\
r & r & r & p
\end{array}.
$$

To compute $r \star p$, for example, we look in the row containing r and the column containing p, which yields $r \star p = r$. It is important not to reverse the role of rows and columns when we use operation tables; for example, the entry in the column containing r and the row containing p is q. Any table using the elements of Z as entries would define a binary operation on Z.   ◇

There are a number of useful properties that a binary operation might or might not satisfy. The first of these properties generalizes the fact that $x + y = y + x$ for all $x, y \in \mathbb{R}$.

Definition 7.1.3. Let A be a set, and let $*$ be a binary operation on A. The binary operation $*$ satisfies the **Commutative Law** (an alternative expression is that $*$ is **commutative**) if $a * b = b * a$ for all $a, b \in A$.   △

Example 7.1.4.

(1) The binary operations addition and multiplication on $\mathbb{Z}$ are both commutative. The binary operation subtraction on $\mathbb{Z}$ is not commutative; for example, we see that $5 - 2 \neq 2 - 5$.

(2) The binary operation $\cdot$ defined in Example 7.1.2 (2) is not commutative. The reader should supply an example of two matrices $A, B \in \mathrm{GL}_2(\mathbb{R})$ such that $A \cdot B \neq B \cdot A$. Some pairs of matrices in $\mathrm{GL}_2(\mathbb{R})$ can be multiplied in either order without changing the result, for example $\left(\begin{smallmatrix} 3 & 0 \\ 0 & 4 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 5 & 0 \\ 0 & 2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 2 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 3 & 0 \\ 0 & 4 \end{smallmatrix}\right)$; however, because it is not the case that all pairs can be multiplied in either order without changing the

result, the binary operation $\cdot$ is not commutative. (Even if the commutative property fails for only a single pair of elements, then the binary operation is not commutative.)

(3) The binary operation $\star$ defined in Example 7.1.2 (3) is not commutative, because $p \star r = q$ and $r \star p = r$. This non-commutativity can be seen easily by observing that the entries of the operation table for $\star$ are not symmetric with respect to the downward sloping diagonal. $\Diamond$

The next property of binary operations generalizes the fact that $(x + y) + z = x + (y + z)$ for all $x, y, z \in \mathbb{R}$.

Definition 7.1.5. Let A be a set, and let $*$ be a binary operation on A. The binary operation $*$ satisfies the **Associative Law** (an alternative expression is that $*$ is **associative**) if $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$. $\triangle$

Example 7.1.6.

(1) The binary operations addition and multiplication on $\mathbb{Z}$ are both associative. The binary operation subtraction on $\mathbb{Z}$ is not associative; for example, we see that $(5 - 2) - 1 \neq 5 - (2 - 1)$.

(2) The binary operation $\cdot$ defined in Example 7.1.2 (2) is associative. This fact can be proved directly by a tedious computation, or indirectly by using more advanced facts from linear algebra; see [AR05, Chapter 1] for details.

(3) The binary operation $\star$ defined in Example 7.1.2 (3) is not associative, because $(r \star p) \star p = r \star p = r$, whereas $r \star (p \star p) = r \star r = p$. In contrast to commutativity, which can be verified quite easily for a binary operation given by an operation table via symmetry with respect to the downward sloping diagonal, there is no correspondingly simple way to verify associativity. The direct way to verify associativity for a binary operation given by an operation table is simply to check all the possible ways of combining three elements at a time; such verification is extremely tedious when the set has more than a few elements. $\Diamond$

As we discussed at the start of Section 3.4, it is the associativity of addition on $\mathbb{R}$ that allows us to write expressions such as $3 + 8 + 5$ without fear of ambiguity, given that the binary operation $+$ applies to only two elements at a time. If you asked two people to calculate the sum $3 + 8 + 5$ in their heads, one person might first add 3 and 8, obtaining 11, and then add 5 to that, obtaining 16, and the other person might first add 8 and 5, obtaining 13, and then add 3 to that, obtaining 16. In other words, one person might do $(3 + 8) + 5$, whereas the other might do $3 + (8 + 5)$. Of course, the same result would be obtained by either method, precisely because addition on $\mathbb{R}$ is associative. The same idea holds for any other associative binary operation. That is, if we are given an associative binary operation $*$ on a set G, and three elements $a, b, c \in G$, we can write $a * b * c$ unambiguously, because it could be calculated as either $(a * b) * c$ or $a * (b * c)$, and the same result would be obtained by either method. This idea can be extended by recursion to allow us to combine any finite number of elements of G unambiguously using $*$, though we cannot use this method to combine infinitely many elements at once.

The next property of binary operations generalizes the unique role of the number 0 in relation to addition of numbers, which is that $x + 0 = x = 0 + x$ for all $x \in \mathbb{R}$.

Definition 7.1.7. Let A be a set, and let $*$ be a binary operation on A. An element $e \in A$ is an **identity element** for $*$ if $a * e = a = e * a$ for all $a \in A$. If $*$ has an identity element, the binary operation $*$ satisfies the **Identity Law**.   △

Observe that we need to specify both $a * e = a$ and $e * a = a$ for all $a \in A$ in Definition 7.1.7, because it cannot be assumed that $*$ is commutative, and so knowing only one of these equalities does not necessarily imply the other.

Example 7.1.8.

(1) The binary operation multiplication on $\mathbb{N}$ has an identity element, the number 1, because $n \cdot 1 = n = 1 \cdot n$ for all $n \in \mathbb{N}$. The binary operation addition on $\mathbb{N}$ does not have an identity element, because $0 \notin \mathbb{N}$. On the other hand, addition on $\mathbb{Z}$ does have an identity element, the number 0. The binary operation subtraction on $\mathbb{Z}$ does not have an identity element. Even though $n - 0 = n$ for all $n \in \mathbb{N}$, we observe that $0 - n \neq n$ when $n \neq 0$.

(2) The binary operation $\cdot$ defined in Example 7.1.2 (2) has an identity element, namely, the identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)$, as the reader can verify.

(3) The binary operation $\star$ defined in Example 7.1.2 (3) has an identity element, which is q. This fact can be verified directly by checking all possibilities, for example $p \star q = p$ and $q \star p = p$, and so on. The fact that q is an identity element can be seen easily by observing in the operation table for $\star$ that the column below q is identical to the column below $\star$, and the row to the right of q is identical to the row to the right of $\star$.

(4) Let $T = \{k, m, n\}$, and let $\diamond$ be the binary operation on T defined by the operation table

$\diamond$	k	m	n
k	k	m	m
m	m	n	k
n	n	k	m

We see that $\diamond$ has no identity element. It is true that $m \diamond k = m$ and $k \diamond m = m$, that $k \diamond k = k$ (only one equality is needed here) and that $n \diamond k = n$, but we observe that $k \diamond n \neq n$, and that last fact is sufficient to rule out k as an identity element. It is easily seen that no element other than k could be the identity element with respect to $\diamond$; we omit the details.   ◇

Observe that in Definition 7.1.7, it is not stated that an identity element, if it exists, is unique. The following lemma shows, however, that uniqueness holds automatically.

Lemma 7.1.9. *Let A be a set, and let $*$ be a binary operation on A. If $*$ has an identity element, the identity element is unique.*

Proof. Let $e, \hat{e} \in A$. Suppose that e and $\hat{e}$ are both identity elements for $*$. Then $e = e * \hat{e} = \hat{e}$, where in the first equality we are thinking of $\hat{e}$ as an identity element, and in the second equality we are thinking of e as an identity element. Therefore the identity element is unique.   □

Because of Lemma 7.1.9, if a binary operation has an identity element, we can refer to it as "the identity element."

The last property of binary operations we discuss generalizes the idea of the negation of a real number. The relevant property of negation is that it allows us to "cancel out" the original number. More precisely, we know that $x + (-x) = 0$ and $(-x) + x = 0$ for all $x \in \mathbb{R}$. In general, canceling out means obtaining the identity element for the binary operation under consideration. Of course, it is only possible to define this property for a binary operation that has an identity element.

Definition 7.1.10. Let A be a set, and let $*$ be a binary operation of A. Let $e \in A$. Suppose that e is an identity element for $*$. If $a \in A$, an **inverse** for a is an element $a' \in A$ such that $a * a' = e$ and $a' * a = e$. If every element in A has an inverse, the binary operation $*$ satisfies the **Inverses Law**.   △

As in the definition of identity elements, we need to specify both $a * a' = e$ and $a' * a = e$ for all $a \in A$, because we cannot assume that $*$ is commutative.

Example 7.1.11.

(1) Every element of $\mathbb{Z}$ has an inverse with respect to addition, namely, its negative. On the other hand, not every element of $\mathbb{Z}$ has an inverse with respect to multiplication, because the reciprocal of most integers is not an integer. Every element of $\mathbb{Q} - \{0\}$ has an inverse with respect to multiplication, namely, its reciprocal.

(2) Let $GL_2(\mathbb{R})$ and $\cdot$ be as in Example 7.1.2 (2). Every element of $GL_2(\mathbb{R})$ has an inverse, because $GL_2(\mathbb{R})$ is the set of invertible 2×2 matrices with real entries; recall that a 2×2 matrix A is invertible precisely if there is a 2×2 matrix B such that $A \cdot B = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $B \cdot A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

(3) Let $H = \{a, b, c, d, e\}$, and let $*$ be the binary operation on H defined by the operation table

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	e	d	e
b	b	e	c	e	a
c	c	d	e	a	c
d	d	b	a	c	b

It is seen that e is the identity element. We see that $a * b = e = b * a$, so b is an inverse of a, and a is an inverse of b. We observe that $c * b = e = b * c$, so b is an inverse of c, and c is an inverse of b. Therefore b has more than one inverse. We see that $e * e = e$, so e is its own inverse. Finally, we see that d has no inverse, because there is no $x \in H$ such that $d * x = e$ (it is the case that $a * d = e$, but for a to be the inverse of d it would also have to be the case that $d * a = e$, and that is not true).   ◇

Exercises

Exercise 7.1.1. Which of the following formulas defines a binary operation on the given set?

(1) Let $*$ be defined by $x*y = xy$ for all $x,y \in \{-1,-2,-3,\dots\}$.
(2) Let $\diamond$ be defined by $x \diamond y = \sqrt{xy}$ for all $x,y \in [2,\infty)$.
(3) Let $\oplus$ be defined by $x \oplus y = x - y$ for all $x,y \in \mathbb{Q}$.
(4) Let $\circ$ be defined by $(x,y) \circ (z,w) = (x+z, y+w)$ for all $(x,y),(z,w) \in \mathbb{R}^2 - \{(0,0)\}$.
(5) Let $\odot$ be defined by $x \odot y = |x+y|$ for all $x,y \in \mathbb{N}$.
(6) Let $\otimes$ be defined by $x \otimes y = \ln(|xy| - e)$ for all $x,y \in \mathbb{N}$.

Exercise 7.1.2. For each of the following binary operations, state whether the binary operation is associative, whether it is commutative, whether there is an identity element and, if there is an identity element, which elements have inverses.

(1) The binary operation $\oplus$ on $\mathbb{Z}$ defined by $x \oplus y = -xy$ for all $x,y \in \mathbb{Z}$.
(2) The binary operation $\star$ on $\mathbb{R}$ defined by $x \star y = x + 2y$ for all $x,y \in \mathbb{R}$.
(3) The binary operation $\otimes$ on $\mathbb{R}$ defined by $x \otimes y = x + y - 7$ for all $x,y \in \mathbb{R}$.
(4) The binary operation $*$ on $\mathbb{Q}$ defined by $x * y = 3(x+y)$ for all $x,y \in \mathbb{Q}$.
(5) The binary operation $\circ$ on $\mathbb{R}$ defined by $x \circ y = x$ for all $x,y \in \mathbb{R}$.
(6) The binary operation $\diamond$ on $\mathbb{Q}$ defined by $x \diamond y = x + y + xy$ for all $x,y \in \mathbb{Q}$.
(7) The binary operation $\odot$ on $\mathbb{R}^2$ defined by $(x,y) \odot (z,w) = (4xz, y+w)$ for all $(x,y),(z,w) \in \mathbb{R}^2$.

Exercise 7.1.3. For each of the following binary operations given by operation tables, state whether the binary operation is commutative, whether there is an identity element and, if there is an identity element, which elements have inverses. (Do not check for associativity.)

(1)

$\otimes$	1	2	3
1	1	2	1
2	2	3	2
3	1	2	3 .

(2)

$\odot$	j	k	l	m
j	k	j	m	j
k	j	k	l	m
l	k	l	j	l
m	j	m	l	m .

(3)

$*$	x	y	z	w
x	x	z	w	y
y	z	w	y	x
z	w	y	x	z
w	y	x	z	w .

(4)

$\star$	a	b	c	d	e
a	d	e	a	b	b
b	e	a	b	a	d
c	a	b	c	d	e
d	b	a	d	e	c
e	b	d	e	c	a .

(5)

$\diamond$	i	r	s	a	b	c
i	i	r	s	a	b	c
r	r	s	i	c	a	b
s	s	i	r	b	c	a
a	a	b	c	i	s	r
b	b	c	a	r	i	s
c	c	a	b	s	r	i .

Exercise 7.1.4. [**Used in Section 7.2.**] Find an example of a set and a binary operation on the set such that the binary operation satisfies the Identity Law and Inverses Law, but not the Associative Law, and for which at least one element of the set has more than one inverse. The simplest way to solve this problem is by constructing an appropriate operation table.

Exercise 7.1.5. Let $n \in \mathbb{N}$. Recall the definition of the set $\mathbb{Z}_n$ and the binary operation $\cdot$ on $\mathbb{Z}_n$ given in Section 5.2. Observe that $[1]$ is the identity element for $\mathbb{Z}_n$ with respect to multiplication. Let $a \in \mathbb{Z}$. Prove that the following are equivalent.

    a. The element $[a] \in \mathbb{Z}_n$ has an inverse with respect to multiplication.
    b. The equation $ax \equiv 1 \pmod{n}$ has a solution.
    c. There exist $p, q \in \mathbb{Z}$ such that $ap + nq = 1$.

(It turns out that the three conditions listed above are equivalent to the fact that a and n are relatively prime, as defined in Exercise 2.4.3; a proof of that fact uses Theorem 8.2.6, though the reader need not be concerned with that proof.)

Exercise 7.1.6. Let A be a set. A **ternary operation** on A is a function $A \times A \times A \to A$. A ternary operation $\star \colon A \times A \times A \to A$ is **left-induced** by a binary operation $\diamond \colon A \times A \to A$ if $\star((a,b,c)) = (a \diamond b) \diamond c$ for all $a, b, c \in A$.

    Is every ternary operation on a set left-induced by a binary operation? Give a proof or a counterexample.

7.2 Groups

As discussed in Section 7.1, some binary operations satisfy various nice properties, such as associativity and commutativity, whereas others do not. Certain combinations of these properties have been found, in retrospect, to be particularly widespread and useful. The most important such combination of properties is given in the following definition.

Definition 7.2.1. Let G be a non-empty set, and let $*$ be a binary operation on G. The pair $(G, *)$ is a **group** if $*$ satisfies the Associative Law, the Identity Law and the Inverses Law. $\triangle$

    Logically, it would have been possible to drop the non-emptiness requirement in Definition 7.2.1, because the empty set satisfies all three properties (even the Identity Law, because the identity element is only needed for use with existing elements, of which the empty set has none). However, the empty set is quite uninteresting as a group, and so to avoid special cases, we will assume that all groups have at least one element.

    Observe that Definition 7.2.1 does not require the Commutative Law. Though associativity may appear at first to be more obscure than commutativity, there turn out to be a number of important examples of binary operations where the former holds but the latter does not. One such example will be seen in Example 7.2.10 below. It is in order to include such examples that the definition of groups does not include the Commutative Law. On the other hand, groups that do satisfy the commutative property are particularly nice to work with, and merit a special name.

Definition 7.2.2. Let $(G, *)$ be a group. We say that $(G, *)$ is an **abelian group** if $*$ satisfies the Commutative Law. $\triangle$

Among many other uses, Definition 7.2.2 gives rise to the following well-known mathematical joke. Question: What is purple and commutative? Answer: An abelian grape. (Mathematical jokes are rather scarce, so one cannot be overly picky about their quality.)

Groups are relatively recent by mathematical standards, having arisen in the nineteenth century, but they are now important in a wide variety of areas of both pure and applied mathematics, including geometry, algebraic topology, quantum mechanics and crystallography, to name just a few. Crystallography makes use of the centrality of groups in the rigorous study of symmetry. See [Fra03] or [Rot73], among many possible texts, for a more detailed treatment of group theory; see [Arm88] or [Bur85] for the connection between group theory and symmetry; and see [LP98, Chapter 6] for some applications of group theory. Our brief discussion of groups, in this section and the next, cannot even begin to hint at the many fascinating aspects of this topic.

The term "group" is one of those words that has a standard colloquial meaning, and to which mathematicians have given a technical meaning that has little to do with the colloquial usage. The term "abelian" is in honor of the mathematician Niels Abel (1802–1829), who did important work in algebra.

Formally, a group is a pair $(G, *)$. However, when the binary operation $*$ is understood from the context, or it is not important to designate the symbol for the binary operation, we will simply say "Let G be a group." If we are discussing more than one group, we will write things such as "e_G" if we need to specify to which group an identity element belongs.

Example 7.2.3.

(1) The pair $(\mathbb{Z}, +)$ is an abelian group, which is seen by combining Example 7.1.6 (1), Example 7.1.8 (1), Example 7.1.11 (1) and Example 7.1.4 (1). Similarly, it is seen that $(\mathbb{Q}, +)$, and $(\mathbb{Q} - \{0\}, \cdot)$ and $(\mathbb{R}, +)$, and $(\mathbb{R} - \{0\}, \cdot)$ are abelian groups.

(2) Let $\{e\}$ be a single element set, and let $*$ be the only possible binary operation on $\{e\}$, which is $e * e = e$. It is simple to verify that $(\{e\}, *)$ is an abelian group. This group is called the **trivial group**. Any two trivial groups, while perhaps labeled differently, are essentially identical, as will be discussed more precisely in Example 7.3.9 (2).

(3) Let $\mathrm{GL}_2(\mathbb{R})$ and $\cdot$ be as in Example 7.1.2 (2). Then $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ is a group, but not an abelian group, which is seen by combining Example 7.1.6 (2), Example 7.1.8 (2), Example 7.1.11 (2) and Example 7.1.4 (2).

(4) Let $V = \{e, a, b, c\}$, and let $\circ$ be a binary operation on V be defined by

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

The pair $(V, \circ)$ is an abelian group. To verify that the Associative Law holds is tedious, and simply requires checking all possible sets of three elements in V; we will

omit the details, though the ambitious reader is invited to check all 64 cases. It is easy to verify that e is the identity element, by observing in the operation table for $\circ$ that the column below e is identical to the column below $\circ$, and similarly for the row to the right of e. The elements e and b are their own inverses, and a and c are inverses of each other. Hence $(V, \circ)$ is a group. It is easy to verify that $\circ$ is commutative, because the operation table is symmetric along the downward sloping diagonal. Hence $(V, \circ)$ is an abelian group.

(5) The pair $(Z, \star)$ given in Example 7.1.2 (3) is not a group. Although $\star$ does have an identity element, which is q, this binary operation is not associative, as discussed in Example 7.1.6 (3), and the element p does not have an inverse. $\diamond$

The axioms for a group turn out to be surprisingly powerful, as can be seen from a full treatment of group theory (for which, of course, we do not have room in this book). We will discuss here only a few of the properties of groups that follow relatively straightforwardly from the axioms. We start with the observation that in the definition of a group, it is not stated that the identity element is unique, nor that each element has a unique inverse. However, we saw in Lemma 7.1.9 that if any binary operation has an identity element, then the identity element is unique, and so in particular that holds for groups. The following lemma shows that the inverse elements in groups are unique, though we remark that the uniqueness does not follow solely from the definition of inverses, but also requires the Associative Law, as seen by Exercise 7.1.4.

Lemma 7.2.4. *Let $(G, *)$ be a group. If $g \in G$, then g has a unique inverse.*

Proof. Left to the reader in Exercise 7.2.5.   □

Because of Lemma 7.2.4, we can now refer to "the inverse" of a given element of the group. Another way of viewing this lemma is that if $(G, *)$ is a group, and if $a, b \in G$ are such that $a * b = e$ and $b * a = e$, then $b = a'$. We will use this idea in the proof of Theorem 7.2.5 (4).

The following theorem generalizes some familiar properties of $(\mathbb{R}, +)$, for example that $-(x + y) = (-x) + (-y)$ for all $x, y \in \mathbb{R}$.

Theorem 7.2.5. *Let $(G, *)$ be a group, and let $a, b, c \in G$.*

1. *If $a * c = b * c$, then $a = b$ (Cancellation Law).*
2. *If $c * a = c * b$, then $a = b$ (Cancellation Law).*
3. *$(a')' = a$.*
4. *$(a * b)' = b' * a'$.*

Proof. We prove Part (4), leaving the rest to the reader in Exercise 7.2.6.

(4). By Lemma 7.2.4 we know that $a * b$ has a unique inverse. If we can show that $(a * b) * (b' * a') = e$ and $(b' * a') * (a * b) = e$, then it will follow that $a' * b'$ is the unique inverse for $a * b$, which means that $(a * b)' = b' * a'$. Using the definition of a group we see that

$$(a * b) * (b' * a') = [(a * b) * b'] * a' = [a * (b * b')] * a'$$

$$= [a * e] * a' = a * a' = e.$$

A similar computation shows that $(b' * a') * (a * b) = e$. □

Observe that Theorem 7.2.5 (4) is the generalization to arbitrary groups of the fact that $-(x + y) = (-x) + (-y)$ for all $x, y \in \mathbb{R}$. Observe, however, that in the statement of Theorem 7.2.5 (4) the order of a and b are reversed in the right-hand side of the equation $(a * b)' = b' * a'$. For an arbitrary group $(G, *)$, which does not necessarily satisfy the Commutative Law, it is not always true that $(a * b)' = a' * b'$ for all $a, b \in G$. The reader is asked to provide such an example in Exercise 7.2.7. However, in the special case where $(G, *)$ is $(\mathbb{R}, +)$, and where a' is given by $-a$ for all $a \in \mathbb{R}$, then Theorem 7.2.5 (4) does indeed say exactly that $-(x + y) = (-x) + (-y)$ for all $x, y \in \mathbb{R}$. The fact that arbitrary groups do not necessarily satisfy the Commutative Law is also the reason why both Parts (1) and (2) of Theorem 7.2.5 are needed.

A useful consequence of Theorem 7.2.5 (1) (2) is that if the binary operation of a group with finitely many elements is given by an operation table, then each element of the group appears once and only once in each row of the operation table and once and only once in each column (consider what would happen otherwise). We can therefore see instantly that $(T, \diamond)$ in Example 7.1.8 (4) is not a group, even if we had not known from our discussion in that example that there is no identity element, because the leftmost column does not have the element n. On the other hand, just because an operation table does have each element once and only once in each row and once and only once in each column does not guarantee that the operation yields a group; the reader is asked in Exercise 7.2.3 to find such an operation table.

We now turn to the notion of a group inside another group. For example, the set $\mathbb{Z}$ sits inside the set $\mathbb{Q}$, and both $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are groups. We formalize this notion as follows.

Definition 7.2.6. Let $(G, *)$ be a group, and let $H \subseteq G$ be a subset. The subset H is a **subgroup** of G if the following two conditions hold.

    (a) If $a, b \in H$, then $a * b \in H$.
    (b) $(H, *)$ is a group. △

Observe in Definition 7.2.6 that because $(H, *)$ is itself a group, it must be non-empty, because all groups are assumed to be non-empty. Part (a) of the definition says that $*$ is a binary operation on H. The following theorem allows for easy verification that a subset of a group is in fact a subgroup. The crucial issue is the notion of "closure" under the binary operation $*$ and the unary operation $'$.

Theorem 7.2.7. Let $(G, *)$ be a group, and let $H \subseteq G$ be a non-empty subset. Then H is a subgroup of G if and only if the following two conditions hold.

    (i) If $a, b \in H$, then $a * b \in H$.
    (ii) If $a \in H$, then $a' \in H$.

Proof. First suppose that H is a subgroup. Then Property (i) holds by the definition of a subgroup. Let e be the identity element of G. Because $(H, *)$ is a group, it has

an identity element, say $\hat{e}$. (We cannot assume, until we prove it, that $\hat{e}$ is the same as e.) Then $\hat{e} * \hat{e} = \hat{e}$ thinking of $\hat{e}$ as being in H, and $e * \hat{e} = \hat{e}$ thinking of $\hat{e}$ as being in G. Hence $\hat{e} * \hat{e} = e * \hat{e}$. Because both $\hat{e}$ and e are in G, we can use Theorem 7.2.5 (1) to deduce that $\hat{e} = e$.

Now let $a \in H$. Because $(G, *)$ is a group, the element a has an inverse $a' \in G$. We will show that $a' \in H$. Because $(H, *)$ is a group, then a has an inverse $\hat{a} \in H$. (Again, we cannot assume, until we prove it, that $\hat{a}$ is the same as a'.) Using the definition of inverses, and what we saw in the previous paragraph, we know that $a' * a = e$ and $\hat{a} * a = e$. Hence $\hat{a} * a = a' * a$. Using Theorem 7.2.5 (1) again, we deduce that $a' = \hat{a}$. Because $\hat{a} \in H$, it follows that $a' \in H$. Therefore Property (ii) of the theorem holds.

Now suppose that Properties (i) and (ii) hold. To show that H is a subgroup, we need to show that $(H, *)$ is a group. We know that $*$ is associative with respect to all the elements of G, so it certainly is associative with respect to the elements of H. Let $b \in H$. By Property (ii) we know that $b' \in H$. By Property (i) we deduce that $b' * b \in H$, and hence $e \in H$. Because e is the identity element for all the elements of G, it is certainly the identity element for all the elements of H. By Property (ii) we now know that every element of H has an inverse in H. Hence H is a group. $\qquad\square$

The following corollary can be deduced immediately from the proof of Theorem 7.2.7.

Corollary 7.2.8. *Let G be a group, and let $H \subset G$ be a subgroup. Then the identity element of G is in H, and it is the identity element of H. The inverse operation in H is the same as the inverse operation in G.*

Example 7.2.9.

(1) The set $\mathbb{Q}$ is a subgroup of $(\mathbb{R}, +)$, and the set $\mathbb{Z}$ is a subgroup of each of $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$.

(2) Let $(G, *)$ be a group. Let e be the identity element of G. Then $\{e\}$ and G are both subgroups of G. The subgroup $\{e\}$ is often called the **trivial subgroup** of G.

(3) Let $(V, \circ)$ be as in Example 7.2.3 (4). By checking all possibilities, it is seen that the only subgroups of V are $\{e\}$, $\{e, b\}$ and V. $\qquad\qquad\diamond$

We conclude this section with a very brief example of the relation between groups and symmetry.

Example 7.2.10. We wish to list all possible symmetries of an equilateral triangle, as shown in Figure 7.2.1 (i). The letters A, B and C are not part of the triangle, but are added for our convenience. Mathematically, a symmetry of an object in the plane is an isometry of the plane (that is, a motion that does not change lengths between points) that take the object onto itself. In other words, a symmetry of an object in the plane is an isometry of the plane that leaves the appearance of the object unchanged. See [Rya86] for more about isometries. Because the letters A, B and C in Figure 7.2.1 (i) are not part of the triangle, a symmetry of the triangle may interchange these letters; we use the letters to keep track of what the isometry did. There are only two types of isometries that will leave the triangle looking unchanged: reflections (that is, flips) of the plane in certain lines, and rotations of the plane by

certain angles about the center of the triangle. In Figure 7.2.1 (ii) we see the three possible lines in which the plane can be reflected without changing the appearance of the triangle. Let M_1, M_2 and M_3 denote the reflections of the planes in these lines. For example, if we apply reflection M_2 to the plane, we see that the vertex labeled C is unmoved, and that the vertices labeled A and B are interchanged, as seen in Figure 7.2.1 (iii). The only two possible rotations of the plane about the center of the triangle that leave the appearance of the triangle unchanged are rotation by $120°$ clockwise and rotation by $240°$ clockwise, denoted R_{120} and R_{240}. We do not need rotation by $120°$ counterclockwise and rotation by $240°$ counterclockwise, even though they also leave the appearance of the triangle unchanged, because they have the same net effect as rotation by $240°$ clockwise and rotation by $120°$ clockwise, respectively, and it is only the net effect of isometries that is relevant to the study of symmetry. Let I denote the isometry of the plane that does not move anything, that is, rotation by $0°$.
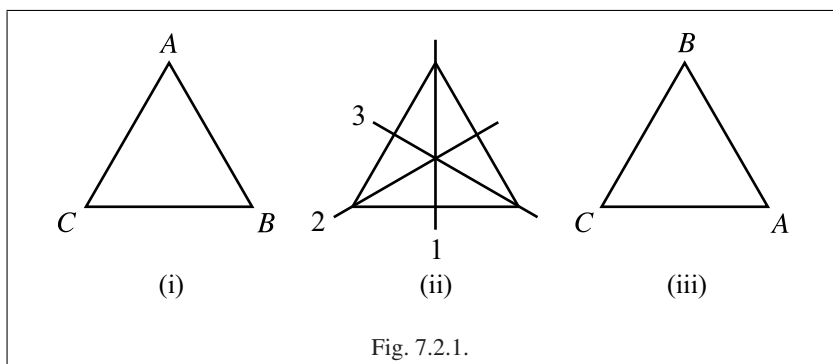
Fig. 7.2.1.

The set $G = \{I, R_{120}, R_{240}, M_1, M_2, M_3\}$ is the collection of all isometries of the plane that take the equilateral triangle onto itself. Each of these isometries can be thought of as a function $\mathbb{R}^2 \to \mathbb{R}^2$, and as such we can combine these isometries by composition of functions. It can be proved that the composition of isometries is an isometry, and therefore composition becomes a binary operation on the set G; we omit the details. (Alternatively, it would be possible to use brute force to check all 36 possible ways of forming compositions of pairs of these six isometries, and it would be seen that the composition of any two of these six isometries is also one of these six isometries, again showing that composition is a binary operation on G.) We can then form the operation table

∘	I	R_{120}	R_{240}	M_1	M_2	M_3
I	I	R_{120}	R_{240}	M_1	M_2	M_3
R_{120}	R_{120}	R_{240}	I	M_2	M_3	M_1
R_{240}	R_{240}	I	R_{120}	M_3	M_1	M_2
M_1	M_1	M_3	M_2	I	R_{240}	R_{120}
M_2	M_2	M_1	M_3	R_{120}	I	R_{240}
M_3	M_3	M_2	M_1	R_{240}	R_{120}	I

Composition of functions is associative, as proved in Lemma 4.3.5 (1), and hence this binary operation on G is associative. Observe that I is an identity element. It is seen that I, M_1, M_2 and M_3 are their own inverses, and that R_{120} and R_{240} are inverses of each other. Therefore $(G, \circ)$ is a group. This group is not abelian, however. For example, we see that $R_{120} \circ M_1 \neq M_1 \circ R_{120}$. The subgroups of G are $\{I, R_{120}, R_{240}\}$, $\{I, M_1\}$, $\{I, M_2\}$ and $\{I, M_3\}$.

The group G is called the symmetry group of the equilateral triangle.   ◇

Similarly to the equilateral triangle in Example 7.2.10, every object in Euclidean space has a corresponding symmetry group, though such groups are often much more complicated than the symmetry group of the equilateral triangle. Because groups have been widely studied by mathematicians, it turns out that quite a lot can be proved about symmetry groups. For example, group theory has been used to obtain rather surprising results about the symmetries of ornamental patterns such as frieze patterns and wallpaper patterns. See [Arm88] or [Bur85] for more about symmetry groups.

$$\boxed{\textbf{Exercises}}$$

Exercise 7.2.1. Which of the following sets and binary operations are groups? Which of the groups are abelian?

(1) The set $(0, 1]$, and the binary operation multiplication.
(2) The set of positive rational numbers, and the binary operation multiplication.
(3) The set of even integers, and the binary operation addition.
(4) The set of even integers, and the binary operation multiplication.
(5) The set $\mathbb{Z}$, and the binary operation $*$ on $\mathbb{Z}$ defined by $a * b = a - b$ for all $a, b \in \mathbb{Z}$.
(6) The set $\mathbb{Z}$, and the binary operation $\star$ on $\mathbb{Z}$ defined by $a \star b = ab + a$ for all $a, b \in \mathbb{Z}$.
(7) The set $\mathbb{Z}$, and the binary operation $\diamond$ on $\mathbb{Z}$ defined by $a \diamond b = a + b + 1$ for all $a, b \in \mathbb{Z}$.
(8) The set $\mathbb{R} - \{-1\}$, and the binary operation $\odot$ on $\mathbb{R} - \{-1\}$ defined by $a \odot b = a + b + ab$ for all $a, b \in \mathbb{R} - \{-1\}$.

Exercise 7.2.2. Let $P = \{a, b, c, d, e\}$. Find a binary operation $*$ on P given by an operation table such that $(P, *)$ is a group.

Exercise 7.2.3. **[Used in Section 7.2.]** Find an example of a set and a binary operation on the set given by an operation table such that each element of the set appears once and only once in each row of the operation table and once and only once in each column, but the set together with this binary operation is not a group.

Exercise 7.2.4. Let A be a set. Define the binary operation $\triangle$ on $\mathcal{P}(A)$ by $X \triangle Y = (X - Y) \cup (Y - X)$ for all $X, Y \in \mathcal{P}(A)$. (This binary operation is called symmetric difference; some properties of symmetric difference are proved in Exercise 3.3.14.) Prove that $(\mathcal{P}(A), \triangle)$ is an abelian group.

Exercise 7.2.5. **[Used in Lemma 7.2.4.]** Prove Lemma 7.2.4.

Exercise 7.2.6. **[Used in Theorem 7.2.5.]** Prove Theorem 7.2.5 (1) (2) (3).

Exercise 7.2.7. **[Used in Section 7.2.]** Find an example of a group $(G, *)$, and elements $a, b \in G$, such that $(a * b)' \neq a' * b'$.

Exercise 7.2.8. Let A be a non-empty set, and let $*$ be a binary operation on A. Suppose that $*$ satisfies the Associative Law and the Identity Law, and that it also satisfies the **Right Inverses Law**, which states that for each $a \in A$ there is an element $b \in A$ such that $a * b = e$, where e is the identity element for $*$.

    (1) Prove that $(A, *)$ satisfies Theorem 7.2.5 (1).
    (2) Prove that $*$ satisfies the Inverses Law, and hence $(A, *)$ is a group.

Exercise 7.2.9. Let $(G, *)$ be a group. Prove that the following are equivalent.

    a. G is abelian.
    b. $aba'b' = e$ for all $a, b \in G$.
    c. $(ab)^2 = a^2 b^2$ for all $a, b \in G$.

Exercise 7.2.10. Let $(G, *)$ be a group. Suppose that $K \subseteq H \subseteq G$. Prove that if K is a subgroup of H, and H is a subgroup of G, then K is a subgroup of G.

Exercise 7.2.11. Let $\mathrm{GL}_2(\mathbb{R})$ and $\cdot$ be as in Example 7.1.2 (2). Let $\mathrm{SL}_2(\mathbb{R})$ denote the set of all 2×2 matrices with real entries that have determinant 1. Prove that $\mathrm{SL}_2(\mathbb{R})$ is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. (This exercise requires familiarity with basic properties of determinants.)

Exercise 7.2.12. Let $n \in \mathbb{N}$. Recall the definition of the set $\mathbb{Z}_n$ and the operations $+$ and $\cdot$ on $\mathbb{Z}_n$ given in Section 5.2.

    (1) **[Used in Example 7.3.2 and Exercise 7.3.3.]** Prove that $(\mathbb{Z}_n, +)$ is an abelian group.
    (2) Suppose that n is not a prime number. Then $n = ab$ for some $a, b \in \mathbb{N}$ such that $1 < a < n$ and $1 < b < n$. Prove that the set $\{[0], [a], [2a], \ldots, [(b-1)a]\}$ is a subgroup of $\mathbb{Z}_n$.
    (3) Is $(\mathbb{Z}_n - \{[0]\}, \cdot)$ a group for all n? If not, can you find any conditions on n that would guarantee that $(\mathbb{Z}_n - \{[0]\}, \cdot)$ is a group?

Exercise 7.2.13. Let $(G, *)$ be a group. Prove that if $x' = x$ for all $x \in G$, then G is abelian. Is the converse to this statement true?

Exercise 7.2.14. Describe the symmetry group of a square, similarly to our description of the symmetry group of an equilateral triangle in Example 7.2.10. Find all the subgroups of the symmetry group of the square.

7.3 Homomorphisms and Isomorphisms

What does it mean for two groups to be "the same"? Consider the group $(V, \circ)$ in Example 7.2.3 (4). We then form a new group $(W, \diamond)$, where $W = \{I, F, G, H\}$, and where $\diamond$ is defined by the same operation table as for $\circ$, with I replacing e, with F replacing a, with G replacing b and with H replacing c. Formally, the group $(W, \diamond)$ is not identical to the group $(V, \circ)$, and yet we would certainly like to consider them essentially the same. This concept is formalized by the use of functions between groups. Such functions need to be bijective, and must "preserve the group operation." This latter notion is meaningful even for non-bijective functions, and we start by making it precise in the following definition.

Definition 7.3.1. Let $(G, *)$ and $(H, \diamond)$ be groups, and let $f \colon G \to H$ be a function. The function f is a **homomorphism** (sometimes called a **group homomorphism**) if $f(a * b) = f(a) \diamond f(b)$ for all $a, b \in G$. △

Example 7.3.2.

(1) We consider two examples of functions from $(\mathbb{Z}, +)$ to $(\mathbb{Q}, +)$. Let $f \colon \mathbb{Z} \to \mathbb{Q}$ be defined by $f(n) = \frac{n}{3}$ for all $n \in \mathbb{Z}$. If $n, m \in \mathbb{Z}$, then $f(n + m) = \frac{(n+m)}{3} = \frac{n}{3} + \frac{m}{3} = f(n) + f(m)$. Hence f is a homomorphism. Let $g \colon \mathbb{Z} \to \mathbb{Q}$ be defined by $g(n) = n^2$ for all $n \in \mathbb{Z}$. If $n, m \in \mathbb{Z}$, then $g(n + m) = (n + m)^2 = n^2 + 2nm + m^2$, whereas $g(n) + g(m) = n^2 + m^2$, and so $g(n + m)$ is not always equal to $g(n) + g(m)$, which means that g is not a homomorphism.

(2) It is straightforward to verify that $((0, \infty), \cdot)$ is a group. Let $h \colon \mathbb{R} \to (0, \infty)$ be defined by $h(x) = e^x$ for all $x \in \mathbb{R}$. Then h is a homomorphism from $(\mathbb{R}, +)$ to $((0, \infty), \cdot)$, because $h(x + y) = e^{x+y} = e^x \cdot e^y = h(x) \cdot h(y)$ for all $x, y \in \mathbb{R}$.

(3) Let $(V, \circ)$ be as in Example 7.2.3 (4). Let $k \colon V \to V$ be defined by $k(e) = e$, and $k(a) = b$, and $k(b) = e$, and $k(c) = b$. Then k is a homomorphism. Rather than verifying that $k(x \circ y) = k(x) \circ k(y)$ for all $x, y \in V$ by checking all possibilities directly, we consider the following four cases. First, suppose that $x, y \in \{e, b\}$. Then $x \circ y \in \{e, b\}$, and hence $k(x) = e$, and $k(y) = e$, and $k(x \circ y) = e$. It follows that $k(x \circ y) = e = e \circ e = k(x) \circ k(y)$. Second, suppose that $x \in \{e, b\}$ and $y \in \{a, c\}$. Then $x \circ y \in \{a, c\}$, and hence $k(x) = e$, and $k(y) = b$, and $k(x \circ y) = b$. It follows that $k(x \circ y) = b = e \circ b = k(x) \circ k(y)$. The other two cases, which are $x \in \{a, c\}$ and $y \in \{e, b\}$, or $x, y \in \{a, c\}$, are similar, and we leave the details to the reader.

(4) Let $n \in \mathbb{N}$. Recall the definition of the set $\mathbb{Z}_n$ and the operations $+$ and $\cdot$ on $\mathbb{Z}_n$ given in Section 5.2. We know from Exercise 7.2.12 (1) that $(\mathbb{Z}_n, +)$ is an abelian group. Recall the definition of the canonical map $\gamma \colon \mathbb{Z} \to \mathbb{Z}_n$ given in Definition 5.2.13. We know from Lemma 5.2.15 that $\gamma(a + b) = \gamma(a) + \gamma(b)$ and $\gamma(ab) = \gamma(a) \cdot \gamma(b)$ for all $a, b \in \mathbb{Z}$. The first of these two properties, involving addition, states that γ is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_n, +)$; more precisely, the

first property states that γ is group homomorphism. It turns out that $\mathbb{Z}$ and $\mathbb{Z}_n$ both have the structure of a "ring," which involves two binary operations (in this case addition and multiplication) that satisfy certain properties. The two properties of γ, which involve both addition and multiplication, together state that γ is in fact a "ring homomorphism." We will not discuss rings in this text; the reader can find this topic in any introductory abstract algebra text, for example [Fra03]. $\diamond$

Homomorphisms of groups preserve the basic group structure, that is, the group operation. The following theorem shows that a group homomorphism also preserves some of the other features of groups.

Theorem 7.3.3. *Let G, H be groups, and let $f : G \to H$ be a homomorphism. Let e_G and e_H be the identity elements of G and H, respectively.*

1. *$f(e_G) = e_H$.*
2. *If $a \in G$, then $f(a') = [f(a)]'$, where the first inverse is in G, and the second is in H.*
3. *If $A \subseteq G$ is a subgroup of G, then $f(A)$ is a subgroup of H.*
4. *If $B \subseteq H$ is a subgroup of H, then $f^{-1}(B)$ is a subgroup of G.*

Proof. We will prove Parts (2) and (3), leaving the rest to the reader in Exercise 7.3.6. Let $*$ and $\diamond$ be the binary operations of G and H, respectively.

(2). Let $a \in G$. Then $f(a) \diamond f(a') = f(a * a') = f(e_G) = e_H$, where the last equality uses Part (1) of this theorem, and the other two equalities use the fact that f is a homomorphism and that G is a group. A similar calculation shows that $f(a') \diamond f(a) = e_H$. By Lemma 7.2.4, it follows that $[f(a)]' = f(a')$.

(3). By Corollary 7.2.8 we know that $e_G \in A$, and by Part (1) of this theorem we know that $e_H = f(e_G) \in f(A)$. Hence $f(A)$ is non-empty. We can therefore use Theorem 7.2.7 to show that $f(A)$ is a subgroup of H. Let $x, y \in f(A)$. Then there are $a, b \in A$ such that $x = f(a)$ and $y = f(b)$. Hence $x \diamond y = f(a) \diamond f(b) = f(a * b)$, because f is a homomorphism. Because A is a subgroup of G we know that $a * b \in A$, and hence $x \diamond y \in f(A)$. Using Part (2) of this theorem, we see that $x' = [f(a)]' = f(a')$. Because A is a subgroup of G, it follows from Theorem 7.2.7 (ii) that $a' \in A$. We now use Theorem 7.2.7 to deduce that $f(A)$ is a subgroup of H. $\square$

The most important method of combining functions is by composition. The following lemma shows that composition works nicely with respect to homomorphisms.

Theorem 7.3.4. *Let G, H and K be groups, and let $f : G \to H$ and $j : H \to K$ be homomorphisms. Then $j \circ f$ is a homomorphism.*

Proof. Left to the reader in Exercise 7.3.7. $\square$

Our next goal is to give a useful criterion by which it can be verified whether a given homomorphism is injective. We start with the following definition.

Definition 7.3.5. Let G and H be groups, and let $f: G \to H$ be a homomorphism. Let e_H be the identity element of H. The **kernel** of f, denoted $\ker f$, is the set $\ker f = f^{-1}(\{e_H\})$.   △

Observe that if $f: G \to H$ is a homomorphism, then by Theorem 7.3.3 (4) we know that $\ker f$ is always a subgroup of G, because $\{e_H\}$ is a subgroup of H.

Example 7.3.6.

(1) Let g be as in Example 7.3.2 (2). The identity element of the group $((0,\infty), \cdot)$ is 1. Then $\ker g = g^{-1}(\{1\}) = \{0\}$. Observe that the function g is injective.

(2) Let k be as in Example 7.3.2 (3). Then $\ker k = k^{-1}(\{e\}) = \{e, b\}$. This kernel is indeed a subgroup of V. We also compute that $k^{-1}(\{a\}) = \emptyset$, that $k^{-1}(\{c\}) = \emptyset$ and that $k^{-1}(\{b\}) = \{a, c\}$; none of these three inverse images are subgroups of V. Observe that the function k is not injective.   ◇

In Example 7.3.6 (1) we had an injective function, and the kernel was the trivial subgroup; in Part (2) of the example we had a non-injective function, and the kernel was non-trivial. The following theorem shows that this correlation between injectivity of homomorphisms and triviality of kernels always holds.

Theorem 7.3.7. *Let G and H be groups, and let $f: G \to H$ be a homomorphism. Let e_G be the identity element of G. The function f is injective if and only if $\ker f = \{e_G\}$.*

Proof. Suppose that f is injective. Because $f(e_G) = e_H$ by Theorem 7.3.3 (1), it follows from the injectivity of f that $\ker f = f^{-1}(\{e_H\}) = \{e_G\}$.

Now suppose that $\ker f = \{e_G\}$. Let $a, b \in G$, and suppose that $f(a) = f(b)$. By Theorem 7.3.3 (2) and the definition of homomorphisms we see that

$$f(b * a') = f(b) \diamond f(a') = f(a) \diamond [f(a)]' = e_H.$$

It follows that $b * a' \in f^{-1}(\{e_H\}) = \ker f$. Because $\ker f = \{e_G\}$, we deduce that $b * a' = e_G$. A similar calculation shows that $a' * b = e_G$. By Lemma 7.2.4 we deduce that $(a')' = b$, and therefore by Theorem 7.2.5 (3) we see that $b = a$. Hence f is injective.   □

Theorem 7.3.7 tells us that the kernel provides us an easy way to tell whether or not a homomorphism is injective. To tell whether an arbitrary function $f: A \to B$ of sets is injective, it would be both necessary and sufficient to verify that $f^{-1}(\{b\})$ is either the empty set or a single element set for all $b \in B$. For homomorphisms, by contrast, it is necessary to check only one such set, namely, the kernel.

We now define what we mean by saying that two groups are "essentially the same."

Definition 7.3.8. Let G and H be groups.

1. Let $f: G \to H$ be a function. The function f is an **isomorphism** (sometimes called a **group isomorphism**) if it is a homomorphism and it is bijective.
2. The groups G and H are **isomorphic** if there is an isomorphism $G \to H$.   △

If two groups are isomorphic, there may be more than one isomorphism between the groups, as we will see in Example 7.3.9 (1); to prove that two groups are isomorphic, it is sufficient to find only one isomorphism between them.

Example 7.3.9.

(1) Let $\mathbb{E}$ denote the set of even integers. It is straightforward to verify that $(\mathbb{E}, +)$ is a group; we omit the details. We claim that $(\mathbb{E}, +)$ and $(\mathbb{Z}, +)$ are isomorphic. Let $f \colon \mathbb{Z} \to \mathbb{E}$ be defined by $f(n) = 2n$ for all $n \in \mathbb{Z}$. It is left to the reader to verify that f is bijective. To see that f is a homomorphism, observe that $f(n + m) = 2(n + m) = 2n + 2m = f(n) + f(m)$ for all $n, m \in \mathbb{Z}$. Hence f is an isomorphism, and therefore $(\mathbb{E}, +)$ and $(\mathbb{Z}, +)$ are isomorphic. The function f is not the only possible isomorphism $\mathbb{Z} \to \mathbb{E}$. The reader can verify that the function $g \colon \mathbb{Z} \to \mathbb{E}$ defined by $g(n) = -2n$ for all $n \in \mathbb{Z}$ is also an isomorphism.

(2) Any two trivial groups, as discussed in Example 7.2.3 (2), are isomorphic. Let $(\{e\}, *)$ and $(\{u\}, \circ)$ be trivial groups. Let $g \colon \{e\} \to \{u\}$ be defined by $g(e) = u$. Then $g(e * e) = g(e) = u = u \circ u = g(e) \circ g(e)$. Hence g is a homomorphism. Clearly g is bijective, and hence it is an isomorphism.

(3) Because isomorphisms are bijective functions, we see that if two groups are isomorphic, then they have the same cardinality. Hence, two finite groups with different numbers of elements cannot possibly be isomorphic. However, just because two finite groups have the same number of elements does not automatically guarantee that they are isomorphic. For example, let $Q = \{1, x, y, z\}$, and let $\diamond$ be the binary operation on Q defined by the operation table

$$
\begin{array}{c|cccc}
\diamond & 1 & x & y & z \\
\hline
1 & 1 & x & y & z \\
x & x & 1 & z & y \\
y & y & z & 1 & x \\
z & z & y & x & 1
\end{array}.
$$

It can be verified that $(Q, \diamond)$ is a group; we omit the details. The group $(V, \circ)$ in Example 7.2.3 (4) also has four elements, but it is shown in Exercise 7.3.9 that $(Q, \diamond)$ and $(V, \circ)$ are not isomorphic. Intuitively, these groups are different in that all four elements of Q are their own inverses, whereas in V only two elements (the elements e and b) are their own inverses. $\diamond$

In Example 7.3.9 (3) we saw that there are at least two non-isomorphic groups with four elements. As seen in Exercise 7.3.10, it turns out that every group with four elements is isomorphic to one of these two groups. In general, it is quite difficult to take a natural number, and to describe all possible non-isomorphic groups with that number of elements, or even to say how many such groups there are; simply checking all possible operation tables (as is done in Exercise 7.3.10) is neither feasible nor satisfying with more than a few elements. The results are known for sufficiently small groups (up to 100 elements, for example), but there is no formula for the number of non-isomorphic groups with n elements for arbitrary n. See [Dea66, Section 9.3] or [Rot96, p. 85] for details.

We conclude this section with the following theorem, which gives some basic properties of isomorphisms. In the statement of Part (2) of the theorem, the function f^{-1} is simply defined to be the inverse of the function f, because any bijective function has an inverse by Theorem 4.4.5 (3); hence f^{-1} is defined without any regard to the fact that f is a homomorphism.

Theorem 7.3.10. *Let G, H and K be groups, and let $f\colon G \to H$ and $j\colon H \to K$ be isomorphisms.*

   1. *The identity map $1_G\colon G \to G$ is an isomorphism.*
   2. *The function f^{-1} is an isomorphism.*
   3. *The function $j \circ f$ is an isomorphism.*

Proof. Left to the reader in Exercise 7.3.8.   □

Exercises

Exercise 7.3.1. Which of the following functions are homomorphisms? Which of the homomorphisms are isomorphisms? The groups under consideration are $(\mathbb{R},+)$, and $(\mathbb{Q},+)$, and $((0,\infty),\cdot)$.

   (1) Let $f\colon \mathbb{Q} \to (0,\infty)$ be defined by $f(x) = 5^x$ for all $x \in \mathbb{Q}$.
   (2) Let $k\colon (0,\infty) \to (0,\infty)$ be defined by $k(x) = x^{-7}$ for all $x \in (0,\infty)$.
   (3) Let $m\colon \mathbb{R} \to \mathbb{R}$ be defined by $m(x) = x + 3$ for all $x \in \mathbb{R}$.
   (4) Let $g\colon (0,\infty) \to \mathbb{R}$ be defined by $g(x) = \ln x$ for all $x \in (0,\infty)$.
   (5) Let $h\colon \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = |x|$ for all $x \in \mathbb{R}$.

Exercise 7.3.2. Let $(\mathrm{GL}_2(\mathbb{R}),\cdot)$ be the group described in Example 7.1.2 (2). We know from Example 7.2.3 (1) that $(\mathbb{R} - \{0\},\cdot)$ is a group. Prove that the function $\det\colon \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R} - \{0\}$ is a homomorphism. What is the kernel of this function? (This exercise requires familiarity with basic properties of determinants.)

Exercise 7.3.3. In this exercise we use the fact that $(\mathbb{Z}_n,+)$ is a group for all $n \in \mathbb{N}$, as was proved in Exercise 7.2.12 (1).

   (1) Let $j\colon \mathbb{Z}_4 \to \mathbb{Z}_3$ be defined by $j([x]) = [x]$ for all $[x] \in \mathbb{Z}_4$, where the two appearances of "$[x]$" in the definition of j refer to elements in different groups. Is this function well-defined? If it is well-defined, is it a homomorphism? If it is a homomorphism, find the kernel.
   (2) Let $k\colon \mathbb{Z}_6 \to \mathbb{Z}_3$ be defined by $k([x]) = [x]$ for all $[x] \in \mathbb{Z}_6$. Is this function well-defined? If it is well-defined, is it a homomorphism? If it is a homomorphism, find the kernel.
   (3) Can you find criteria on $n,m \in \mathbb{N}$ that will determine when the function $r\colon \mathbb{Z}_n \to \mathbb{Z}_m$ defined by $r([x]) = [x]$ for all $[x] \in \mathbb{Z}_n$ is well-defined and is a homomorphism? Prove your claim. Find the kernels for those functions that are well-defined and are homomorphisms.

Exercise 7.3.4. Let G and H be groups. Prove that the projection maps $\pi_1 \colon G \times H \to G$ and $\pi_2 \colon G \times H \to H$ are homomorphisms (see Section 4.1 for the definition of projection maps). What is the kernel of each of these functions?

Exercise 7.3.5. Prove that the two groups in each of the following pairs are isomorphic to each other.

(1) $(\mathbb{Z}, +)$ and $(5\mathbb{Z}, +)$, where $5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\}$.
(2) $(\mathbb{R} - \{0\}, \cdot)$ and $(\mathbb{R} - \{-1\}, *)$, where $x * y = x + y + xy$ for all $x, y \in \mathbb{R} - \{-1\}$.
(3) $(\mathbb{R}^4, +)$ and $(M_{2 \times 2}(\mathbb{R}), +)$, where $M_{2 \times 2}(\mathbb{R})$ is the set of all 2×2 matrices with real entries.

Exercise 7.3.6. [Used in Theorem 7.3.3.] Prove Theorem 7.3.3 (1) (4).

Exercise 7.3.7. [Used in Theorem 7.3.4.] Prove Theorem 7.3.4.

Exercise 7.3.8. [Used in Theorem 7.3.10.] Prove Theorem 7.3.10.

Exercise 7.3.9. [Used in Example 7.3.9.] Prove that the groups $(V, \circ)$ in Example 7.2.3 (4) and $(Q, \diamond)$ in Example 7.3.9 (3) are not isomorphic.

Exercise 7.3.10. [Used in Section 7.3.] Prove that up to isomorphism, the only two groups with four elements are $(V, \circ)$ of Example 7.2.3 (4) and $(Q, \diamond)$ of Example 7.3.9 (3). Consider all possible operation tables for the binary operation of a group with four elements; use the fact that each element of a group appears once in each row and once in each column of the operation table for the binary operation of the group, as remarked after Theorem 7.2.5.

7.4 Partially Ordered Sets

In Sections 7.2 and 7.3 we discussed the concept of a group, which is an algebraic structure based on the notion of a binary operation. If we think of familiar number systems such as the natural numbers and real numbers, we observe that there is another type of structure on these sets, namely, the order relation $\leq$. In this section and the next we will discuss two important structures, called partially ordered sets and lattices, that are based on the notion of an order relation, rather than a binary operation.

Order relations have widespread use in many areas of both pure and applied mathematics, such as combinatorics, boolean algebras, switching circuits, computer science and others. An interesting application of order relations to the theory of voting is in [KR83a, Section 1.6], where a proof is given of the remarkable Arrow Impossibility Theorem (which says roughly that in an election with three or more candidates, no voting system satisfying certain reasonable conditions can exist). Because of the widespread appearance of order relations in many combinatorial topics, they are often treated in texts on combinatorics, for example [Bog90, Chapter 7]. A treatment of order relations in the context of computer science is [DSW94, Chapter 16].

In Section 5.1 we discussed relations in general, and in particular three properties that a relation might satisfy, which are reflexivity, symmetry and transitivity. We now turn our attention to a particular type of relation, which generalizes the order relation $\leq$ on $\mathbb{R}$. The relation $\leq$ is reflexive and transitive, but certainly not symmetric. Indeed, this relation is about as non-symmetric as can be, given the well-known property that if $x, y \in \mathbb{R}$ and both $x \leq y$ and $y \leq x$ hold, then $x = y$. In other words, if $x \neq y$, it cannot happen that both $x \leq y$ and $y \leq x$.

Now compare the relation $\leq$ on $\mathbb{R}$ with the relation $\subseteq$ on $\mathcal{P}(A)$. Observe that $\subseteq$ is also reflexive and transitive, and is similarly non-symmetric, in that if $X, Y \subseteq A$ and if $X \subseteq Y$ and $Y \subseteq X$, then $X = Y$. Both these relations involve what would intuitively be called "order" on some set, and it is this notion of order that we wish to generalize. There is, however, one substantial difference between $\leq$ and $\subseteq$. For any $x, y \in \mathbb{R}$, we know that either $x \leq y$ or $y \leq x$. On the other hand, for two arbitrary subsets $X, Y \subseteq A$, it might not be the case that either of $X \subseteq Y$ or $Y \subseteq X$ holds; for example, let $A = \{1, 2, 3, 4\}$, let $X = \{1, 2\}$ and let $Y = \{3, 4\}$. Informally, for $\leq$ every two elements are "comparable," whereas for $\subseteq$ they are not necessarily so. Given that we want the broadest possible notion of order, we will not be requiring comparability in our most general definition. These ideas are all made precise as follows.

Definition 7.4.1. Let A be a non-empty set, and let $\preccurlyeq$ be a relation on A.

1. The relation $\preccurlyeq$ is **antisymmetric** if $x \preccurlyeq y$ and $y \preccurlyeq x$ imply that $x = y$, for all $x, y \in A$.
2. The relation $\preccurlyeq$ is a **partial ordering** (also called a **partial order**) if it is reflexive, transitive and antisymmetric. If $\preccurlyeq$ is a partial ordering, the pair $(A, \preccurlyeq)$ is a **partially ordered set**, often abbreviated as **poset**.
3. The relation $\preccurlyeq$ is a **total ordering** (also called a **total order** or **linear ordering**) if it is a partial ordering, and if for every $a, b \in A$, at least one of $a \preccurlyeq b$ or $b \preccurlyeq a$ holds. If $\preccurlyeq$ is a total ordering, the pair $(A, \preccurlyeq)$ is a **totally ordered set**. $\triangle$

Formally, a poset is a pair $(A, \preccurlyeq)$. However, when the relation $\preccurlyeq$ is understood from the context, or it is not important to designate the symbol for the relation, we will simply say "let A be a poset." Similarly for totally ordered sets. We will primarily be looking at posets, rather than totally ordered sets, because the former are more prevalent orderings. Observe that posets and totally ordered sets are all assumed to be non-empty.

Example 7.4.2.

(1) The relation E in Example 5.1.6 (5) is antisymmetric and reflexive, but it is not transitive, and hence it is not a partial ordering.

(2) There are many relations that are reflexive and transitive but not antisymmetric. For instance, any equivalence relation that has non-equal elements that are related cannot be antisymmetric; the reader is asked to prove this fact in Exercise 7.4.5 (2). For example, the relation of congruence modulo n for any $n \in \mathbb{N}$ such that $n \neq 1$ is reflexive and transitive, but not antisymmetric (see Section 5.2 for the definition of this relation).

(3) Each of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ with the relation $\leq$ is a totally ordered set. The relation $<$ on these sets is not a partial ordering, because it is not reflexive.

(4) Let A be a set. Then $(\mathcal{P}(A), \subseteq)$ is a poset but not a totally ordered set, as mentioned previously.

(5) The relation "$a|b$" on $\mathbb{N}$ is given in Definition 2.2.1. (The proper name for this relation is "|," without the "variables," but that would be awkward to read.) The relation is certainly reflexive, and it was shown in Theorem 2.2.2 that this relation is transitive. Let $a, b \in \mathbb{N}$, and suppose that $a|b$ and $b|a$. Then by Theorem 2.4.3 we know that $a = b$ or $a = -b$. Because both a and b are positive, then it must be the case that $a = b$. Hence the relation is antisymmetric, and therefore it is a partial ordering. This relation is not a total ordering, however; for example, neither $2|3$ nor $3|2$ holds. Observe that the relation $a|b$ on $\mathbb{Z}$ is not antisymmetric, because $3|(-3)$ and $(-3)|3$, and yet $3 \neq -3$.

(6) Let W be the set of all words in the English language. Let $\preccurlyeq$ be the relation on W defined as follows. If w_1 and w_2 are words, then $w_1 \preccurlyeq w_2$ if for some $n \in \mathbb{N}$, the first $n - 1$ letters of w_1 and w_2 are the same, and the n-th letter of w_1 comes before the n-th letter of w_2 in the usual ordering of the letters of the alphabet (the second condition is dropped when $w_1 = w_2$). For example, we see that mandrel $\preccurlyeq$ mandrill. This relation, which is seen to be a total ordering, is called the lexicographical order (also called the dictionary order). $\diamondsuit$

A nice way to visualize finite posets is via Hasse diagrams. To construct these diagrams we need the following definition.

Definition 7.4.3. Let $(A, \preccurlyeq)$ be a poset, and let $a, b \in A$. The element b **covers** the element a if $a \preccurlyeq b$, and $a \neq b$, and there is no $x \in A$ such that $a \preccurlyeq x \preccurlyeq b$ and $a \neq x \neq b$. $\triangle$

We form the Hasse diagram of a finite poset as follows. First, put a dot on the page for each element of the poset, placed in such a way that if $x \preccurlyeq y$ then y is higher on the page than x, though not necessarily directly above it. Second, connect the dots representing elements x and y by a line segment if and only if y covers x.

Example 7.4.4.

(1) Let $A = \{2, 4, 6, 8, 10, 12\}$, and let $\preccurlyeq$ be the relation $a|b$ discussed in Example 7.4.2 (5). By the argument given in that example, we know that $(A, \preccurlyeq)$ is a poset. The Hasse diagram for this poset is given in Figure 7.4.1 (i). Observe that there is no line segment from 2 to 8, even though $2 \preccurlyeq 8$, because 8 does not cover 2. Also, observe that the placement of the dots on the page is not unique. Figure 7.4.1 (ii) shows another possible Hasse diagram for the same poset.

(2) For finite posets with small numbers of elements, Hasse diagrams allow us a convenient way to list all possible inequivalent posets of a given size; a rigorous definition of "inequivalent" needs the notion of order preserving functions defined later in this section, but we will use the term informally here. The Hasse diagrams of all inequivalent posets with 3 elements are given in Figure 7.4.2. (Of course, the Hasse diagrams are not the posets themselves, but they accurately represent the posets.) $\diamondsuit$

Fig. 7.4.1.

Fig. 7.4.2.
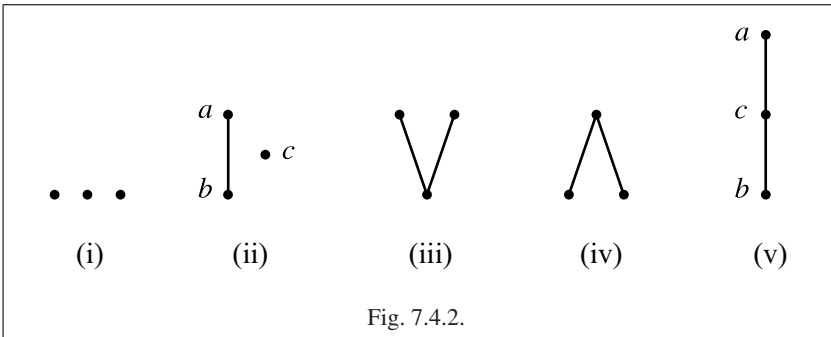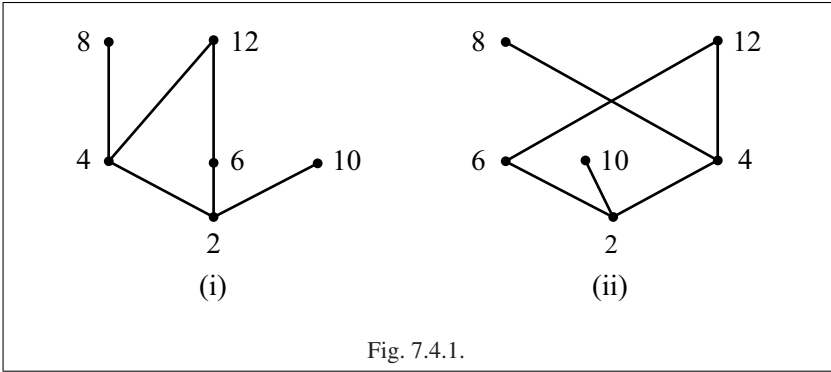
Whenever we have a notion of order on a set, it is tempting to look for largest elements and smallest elements of various types. The most basic type of largest element or smallest element is given in the following definition.

Definition 7.4.5. Let $(A, \preccurlyeq)$ be a poset, and let $a \in A$. The element a is a **greatest element** of A if $x \preccurlyeq a$ for all $x \in A$. The element a is a **least element** of A if $a \preccurlyeq x$ for all $x \in A$. △

Not every poset has a greatest element or a least element, as we now see.

Example 7.4.6. The poset $(\mathbb{Z}, \leq)$ has no greatest element or least element. Even finite posets need not have greatest elements or least elements. For example, the poset in Example 7.4.4 (1) does not have a greatest element; observe that 12 is not a greatest element with respect to the relation $a|b$, because 10 does not divide 12. The poset does have a least element, the number 2, because 2 divides all the other numbers in the set. ◇

We now turn to a definition that is slightly weaker than Definition 7.4.5. The following definition generalizes Definition 3.5.4 (1).

Definition 7.4.7. Let $(A, \preccurlyeq)$ be a poset, and let $a \in A$. The element a is a **maximal element** of A if there is no $x \in A$ such that $a \preccurlyeq x$ and $a \neq x$. The element a is a **minimal element** of A if there is no $x \in A$ such that $x \preccurlyeq a$ and $a \neq x$. △

Example 7.4.8. The poset $(\mathbb{Z}, \leq)$ has no maximal element or minimal element. Let $(A, \preccurlyeq)$ be the poset in Example 7.4.4 (1). The elements 8, 10 and 12 are all maximal elements, which shows that maximal elements need not be unique, and also that maximal elements need not be greatest elements. The element 2 is a minimal element, which also happens to be a least element.   ◇

Although not every poset has a maximal element or minimal element, the following theorem shows that such elements always exist in finite posets.

Theorem 7.4.9. *Let* $(A, \preccurlyeq)$ *be a poset. Suppose that A is finite. Then A has a maximal element and a minimal element.*

Proof. We will prove the existence of maximal elements; the existence of minimal elements is similar, and we omit the details. Let $n = |A|$. We proceed by induction on n. If $n = 1$, then the single element of A is clearly a maximal element. Now assume that $n \geq 2$. Suppose that the result is true for $n - 1$. Let $w \in A$, and let $B = A - \{w\}$. By Exercise 7.4.8 we know that $(B, \preccurlyeq)$ is a poset. Because $|B| = n - 1$, it follows from the inductive hypothesis that there is a maximal element p of B. We now define $r \in A$ as follows. If $p \preccurlyeq w$, let $r = w$; if it is not the case that $p \preccurlyeq w$, then let $r = p$. We claim that r is a maximal element of A. There are two cases. First, suppose that $p \preccurlyeq w$. Then $r = w$. Suppose that there is some $y \in A$ such that $w \preccurlyeq y$ and $w \neq y$. By transitivity it follows that $p \preccurlyeq y$, and by antisymmetry it follows that $p \neq y$. Because $y \neq w$, then $y \in B$, and we then have a contradiction to the fact that p is a maximal element of B. It follows that w is a maximal element of A. Second, suppose that it is not the case that $p \preccurlyeq w$. Then $r = p$. Because p is a maximal element of B, then there is no $x \in B$ such that $p \preccurlyeq x$ and $p \neq x$. It follows that there is no $x \in A = B \cup \{w\}$ such that $p \preccurlyeq x$ and $p \neq x$, and hence p is a maximal element of A.   □

We now look at another concept that is related to the idea of an element being larger than everything in a collection of elements, and similarly for elements that are smaller than others. This new concept turns out to be extremely useful, both in our study of lattices in Section 7.5, and, as mentioned briefly in Example 7.4.11 (2), in the field of real analysis.

Definition 7.4.10. Let $(A, \preccurlyeq)$ be a poset, let $X \subseteq A$ be a subset and let $a \in A$. The element a is an **upper bound** of X if $x \preccurlyeq a$ for all $x \in X$. The element a is a **least upper bound** of X if it is an upper bound of X, and $a \preccurlyeq z$ for any other upper bound z of X. The element a is a **lower bound** of X if $a \preccurlyeq x$ for all $x \in X$. The element a is a **greatest lower bound** for X if it is a lower bound of X, and $w \preccurlyeq a$ for any other lower bound w of X.   △

Example 7.4.11.

(1) Let A be a set. Every subset of the poset $(\mathcal{P}(A), \subseteq)$ has a greatest lower bound and a least upper bound. Let $X \subseteq \mathcal{P}(A)$. Then X is a family of subsets of A. It follows from Theorem 3.4.5 (1) (2) that $\bigcup_{D \in X} D$ is a least upper bound of X, and that $\bigcap_{D \in X} D$ is a greatest lower bound of X.

(2) We start by looking at subsets of the poset $(\mathbb{Q}, \leq)$. Let $X = \{\frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \frac{4}{2}, \frac{5}{2}, \ldots\}$. Then X has no upper bound in $\mathbb{Q}$, and hence no least upper bound. This set has many lower bounds, for example -17 and 0, and it has a greatest lower bound, which is $\frac{1}{2}$. Let $Y = \{x \in \mathbb{Q} \mid 1 < x < 3\}$. Then Y has many upper and lower bounds; it has a least upper bound, which is 3, and a greatest lower bound, which is 1. In contrast to the set X, which contains its greatest lower bound, the set Y contains neither its greatest lower bound nor its least upper bound. Let $Z = \{x \in \mathbb{Q} \mid 0 \leq x < \sqrt{2}\}$. Then Z has a greatest lower bound, which is 0. However, even though Z has many upper bounds in $\mathbb{Q}$, for example 2 and $\frac{3}{2}$, the set Z has no least upper bound in $\mathbb{Q}$, which can be seen using the fact that $\sqrt{2} \notin \mathbb{Q}$, as was proved in Theorem 2.3.5.

Now consider the poset $(\mathbb{R}, \leq)$. Let $Z' = \{x \in \mathbb{R} \mid 0 \leq x < \sqrt{2}\}$. In contrast to the subset Z of $\mathbb{Q}$, which has upper bounds in $\mathbb{Q}$ but no least upper bound, the subset Z' of $\mathbb{R}$ has a least upper bound in $\mathbb{R}$, which is $\sqrt{2}$. Indeed, what distinguishes $\mathbb{R}$ from $\mathbb{Q}$ is precisely the fact that in $\mathbb{R}$, if a subset has an upper bound then it must have a least upper bound, and similarly for lower bounds. This property of $\mathbb{R}$, known as the Least Upper Bound Property, is crucial in the field of real analysis, where the results of calculus are proved rigorously; see any introductory real analysis text, for example [Blo11, Section 2.6], for details.

(3) As shown in Example 7.4.2 (5), the set $\mathbb{N}$ with the relation "$a|b$" is a poset. Let $a_1, \ldots, a_p \in \mathbb{N}$, for some $p \in \mathbb{N}$. Then the greatest common divisor of $a_1, \ldots, a_p$ is a greatest lower bound of $\{a_1, \ldots, a_p\}$, and the least common multiple of these numbers is a least upper bound of $\{a_1, \ldots, a_p\}$. On the other hand, if $X \subseteq \mathbb{N}$ is an infinite subset, then X will have no upper bound, and hence it will not have a least upper bound, though it will have a greatest lower bound (which will still be the greatest common divisor of all the elements of X). $\diamond$

We see from Example 7.4.11 that not every subset of a poset has a least upper bound or a greatest lower bound. The following lemma shows that if a least upper bound or a greatest lower bound of a subset exists, then it is unique.

Lemma 7.4.12. *Let $(A, \preccurlyeq)$ be a poset, and let $X \subseteq A$ be a subset. If X has a least upper bound, then it is unique, and if X has a greatest lower bound, then it is unique.*

Proof. Let $p, q \in A$, and suppose that both are least upper bounds of X. By definition both p and q are upper bounds for X. Because p is a least upper bound of X, and q is an upper bound of X, then $p \preccurlyeq q$ by the definition of least upper bounds. Similarly, we see that $q \preccurlyeq p$. By antisymmetry, it follows that $p = q$. A similar argument works for greatest lower bounds; we omit the details. $\square$

Because of Lemma 7.4.12, we can refer to "the least upper bound" and "the greatest lower bound" of a subset of a poset, whenever a least upper bound and a greatest lower bound exist. It is standard to write $\operatorname{lub} X$ and $\operatorname{glb} X$ to denote the least upper bound and the greatest lower bound respectively for a subset X of a poset, though we will not need that notation in this book.

What is the relation between posets and totally ordered sets? Clearly, every totally ordered set is a poset. The converse is certainly not true, as seen in Example 7.4.2 (4).

However, the following theorem shows that every finite poset can be "expanded" into a totally ordered set.

Theorem 7.4.13. *Let $(A, \preceq)$ be a poset. Suppose that A is finite. Then there is a total ordering $\preceq'$ on A such that if $x \preceq y$ then $x \preceq' y$, for all $x, y \in A$.*

Proof. Let $n = |A|$. We proceed by induction on n. If $n = 1$ the result is trivial. Now assume that $n \geq 2$. Suppose that the result is true for $n - 1$. By Theorem 7.4.9 the poset A has a maximal element, say $r \in A$. Let $B = A - \{r\}$. By Exercise 7.4.8 we know that $(B, \preceq)$ is a poset. Because $|B| = n - 1$, it follows from the inductive hypothesis that there is a total ordering $\preceq''$ on B such that if $x \preceq y$ then $x \preceq'' y$, for all $x, y \in B$. Now define a relation $\preceq'$ on A as follows. If $x, y \in B$, let $x \preceq' y$ if and only if $x \preceq'' y$. If $x \in A$, let $x \preceq' r$. It is left to the reader in Exercise 7.4.9 to show that $\preceq'$ is a total order on A, and that if $x \preceq y$ then $x \preceq' y$, for all $x, y \in A$.   □

Theorem 7.4.13 states that any finite poset can be given a total ordering that includes the original partial ordering; such a total ordering is often referred to as a linear ordering of the original poset. A poset can have more than one linear ordering. A close look at the proof of Theorem 7.4.13 shows that we actually gave an algorithmic procedure for finding a linear ordering of a given poset. This is not the only (nor the best) such algorithm, though it is a very simple one. Such algorithms are useful in the theory of posets, and well as in applications of posets to computer science (where finding a linear ordering is known as topological sorting); see [Knu73, pp. 258–268] for discussion of the latter.

Example 7.4.14. Let $(A, \preceq)$ be the poset corresponding to the Hasse diagram in Figure 7.4.2 (ii). We will apply the algorithm in the proof of Theorem 7.4.13 to this poset. First, we need to choose a maximal element of A. There are two such elements, which are a and c. Let us choose the element a. Then let $B = A - \{a\} = \{b, c\}$. We now need a total ordering on B that includes the given partial ordering on B. Such a total ordering is quite easy to obtain, given that B has only two elements, and neither element is greater than the other in the given partial ordering. Again, there is a choice to be made, and we will choose the total ordering $\preceq''$ on B defined by $b \preceq'' c$. We now define $\preceq'$ on A by first letting $b \preceq' c$, and then, because a is the chosen maximal element of A, letting $b \preceq' a$ and $c \preceq' a$. The Hasse diagram of the totally ordered set $(A, \preceq')$ is given in Figure 7.4.2 (v).

Different choices in the above procedure would have yielded different total orderings on A. For example, if we had chosen the maximal element c instead of a, the resulting total ordering would have been $b \preceq' a \preceq' c$.   ◊

In Section 7.3 we discussed homomorphisms and isomorphisms of groups, which are functions between groups that preserved the group operation. We can similarly discuss functions between posets that preserve their basic structures. Our treatment here partially follows [Szá63, Section 20].

Definition 7.4.15. Let $(A, \preceq)$ and $(B, \preceq')$ be posets, and let $f : A \to B$ be a function. The function f is an **order homomorphism** (also called an **order preserving**

function) if $x \preccurlyeq y$ implies $f(x) \preccurlyeq' f(y)$, for all $x, y \in A$. The function f is an **order isomorphism** if it is bijective, and if both f and f^{-1} are order homomorphisms.   △

Two posets are considered essentially the same if there is an order isomorphism between them.

The following useful lemma is a direct consequence of Definition 7.4.15, and we omit the proof.

Lemma 7.4.16. *Let* $(A, \preccurlyeq)$ *and* $(B, \preccurlyeq')$ *be posets, and let* $f : A \to B$ *be a function. Then* f *is an order isomorphism if and only if* f *is a bijective function, and* $x \preccurlyeq y$ *if and only if* $f(x) \preccurlyeq' f(y)$ *for all* $x, y \in A$.

Example 7.4.17.

(1) Let $\mathcal{P}_F(\mathbb{N})$ denote the family of all finite subsets of $\mathbb{N}$. Then $(\mathcal{P}_F(\mathbb{N}), \subseteq)$ is a poset. We saw in Example 7.4.2 (3) that $(\mathbb{Z}, \leq)$ is a poset. Let $s \colon \mathcal{P}_F(\mathbb{N}) \to \mathbb{Z}$ be defined by $s(X) = |X|$ for all $X \in \mathcal{P}_F(\mathbb{N})$. It follows from Theorem 6.6.5 (3) that the function s is an order homomorphism. The function s is not bijective, however, so it is not an order isomorphism.

(2) Let $A = \{a, b\}$, let $D = \{1, 2, 3, 6\}$ and let $\preccurlyeq$ be the relation on D given by $a | b$. Then $(\mathcal{P}(A), \subseteq)$ and $(D, \preccurlyeq)$ are posets, as seen in Example 7.4.2 (4) (5). Let $f : D \to \mathcal{P}(A)$ be defined by $f(1) = \emptyset$, and $f(2) = \{a\}$, and $f(3) = \{b\}$ and $f(6) = \{a, b\}$. It is left to the reader to verify that f is an order isomorphism.

(3) Observe that $(\mathbb{N}, =)$ is a poset. We also know that $(\mathbb{N}, \leq)$ is a poset, as stated in Example 7.4.2 (3) . The identity map $1_{\mathbb{N}} \colon \mathbb{N} \to \mathbb{N}$ is then seen to be an order homomorphism from the poset $(\mathbb{N}, =)$ to the poset $(\mathbb{N}, \leq)$. The function $1_{\mathbb{N}}$ is also bijective, and clearly $(1_{\mathbb{N}})^{-1} = 1_{\mathbb{N}}$. However, if we think of the function $1_{\mathbb{N}}$ in its roles as $(1_{\mathbb{N}})^{-1}$, then we observe that this inverse function is not an order homomorphism from $(\mathbb{N}, \leq)$ to $(\mathbb{N}, =)$. For example, we observe that $5 \leq 7$, but $1_{\mathbb{N}}(5) \neq 1_{\mathbb{N}}(7)$. We therefore see that a bijective order homomorphism need not have its inverse automatically be an order homomorphism. Hence, the definition of order isomorphism is not redundant. (If the reader is familiar with group isomorphisms, as in Section 7.3, or with linear maps, then this example may seem rather strange. For both groups and vector spaces, if a function is bijective and a homomorphism, then its inverse is automatically a homomorphism as well; see Theorem 7.3.10 (2) for the group case. Homomorphisms of posets, we now see, are not as well-behaved.)   ◇

We conclude this section with a nice result about order homomorphisms. To appreciate this result, recall from Figure 7.4.2 that there are a number of distinct partial orderings on a set with 3 elements, and of course there are even larger numbers of distinct partial orderings on larger finite sets. However, only one of the partial orderings in Figure 7.4.2 is a total ordering, namely, the one corresponding to the Hasse diagram that is a single vertical line. The following theorem says, not surprisingly, that a similar result holds for all finite sets.

Theorem 7.4.18. *Let* $(A, \preccurlyeq)$ *be a totally ordered set. Suppose that* A *is finite. Let* $n = |A|$. *Then there is an order isomorphism from* $(A, \preccurlyeq)$ *to* $(\{1, 2, \ldots, n\}, \leq)$.

Proof. We follow [KR83a]. We prove the result by induction on n. When $n = 1$ the result is trivial. Now assume that $n \geq 2$. Suppose that the result holds for $n - 1$.

By Theorem 7.4.9 the poset A has a maximal element, say $r \in A$. Let $x \in A$. Because $\preccurlyeq$ is a total ordering, we know that $x \preccurlyeq r$ or $r \preccurlyeq x$. If it were the case that $r \preccurlyeq x$, then by hypothesis on r we would know that $r = x$. Hence $x \preccurlyeq r$.

Let $B = A - \{r\}$. By Exercise 7.4.8 we know that $(B, \preccurlyeq)$ is a poset. Because $|B| = n - 1$, it follows from the inductive hypothesis that there is an order iso-morphism from $(B, \preccurlyeq)$ to $(\{1, 2, \ldots, n - 1\}, \leq)$, say $f \colon B \to \{1, 2, \ldots, n - 1\}$. Let $F \colon A \to \{1, 2, \ldots, n\}$ be defined by $F(x) = f(x)$ for all $x \in B$, and $F(r) = n$.

Because f is bijective, it is straightforward to see that F is bijective as well; we omit the details. To see that F is an order isomorphism, it suffices by Lemma 7.4.16 to show that $x \preccurlyeq y$ if and only if $F(x) \leq F(y)$, for all $x, y \in A$. First, let $x, y \in B$. Then $x \preccurlyeq y$ if and only if $f(x) \leq f(y)$ because f is an order isomorphism. Because $F(x) = f(x)$ and $F(y) = f(y)$, then $x \preccurlyeq y$ if and only if $F(x) \leq F(y)$. Now let $z \in B$. We know that $z \preccurlyeq r$, and we also know that $F(z) \leq n = F(r)$, because $F(z) \in \{1, 2, \ldots, n - 1\}$. Hence $z \preccurlyeq r$ if and only if $F(z) \leq F(r)$, because both these statements are true. It follows that F is an order isomorphism. $\square$

The analog of Theorem 7.4.18 for infinite sets is not true. For example, as the reader is asked to show in Exercise 7.4.16, there is no order isomorphism from the totally ordered set $(\mathbb{N}, \leq)$ to the totally ordered $(\mathbb{N}^-, \leq)$, where $\mathbb{N}^-$ denotes the set of negative integers, even though both sets have the same cardinality.

<div align="center">

Exercises

</div>

Exercise 7.4.1. Is each of the relations given in Exercise 5.1.3 antisymmetric, a partial ordering and/or a total ordering?

Exercise 7.4.2. Is each of the following relations antisymmetric, a partial ordering and/or a total ordering?

    (1) Let F be the set of people in France, and let M be the relation on F defined by $x M y$ if and only if x eats more cheese annually than y, for all $x, y \in F$.

    (2) Let W be the set of all people who ever lived and ever will live, and let A be the relation on W defined by $x A y$ if and only if y is an ancestor of x or if $y = x$, for all $x, y \in W$.

    (3) Let T be the set of all triangles in the plane, and let L be the relation on T defined by $s L t$ if and only if s has area less than or equal to t, for all triangles $s, t \in T$.

    (4) Let U be the set of current U.S. citizens, and let Z be the relation on U defined by $x Z y$ if and only if the Social Security number of x is greater than the Social Security number of y, for all $x, y \in U$.

Exercise 7.4.3. **[Used in Exercise 7.4.4, Exercise 7.4.15 and Example 7.5.2.]** Let $A \subset \mathbb{N}$ be a subset, and let $\preccurlyeq$ be the relation on A defined by $a \preccurlyeq b$ if and only if $b = a^k$ for some $k \in \mathbb{N}$, for all $a, b \in A$. Prove that $(A, \preccurlyeq)$ is a poset. Is $(A, \preccurlyeq)$ a totally ordered set?

Exercise 7.4.4. Draw a Hasse diagram for each of the following posets.

(1) The set $A = \{1, 2, 3, \ldots, 15\}$, and the relation $a|b$.
(2) The set $B = \{1, 2, 3, 4, 6, 8, 12, 24\}$, and the relation $a|b$.
(3) The set $C = \{1, 2, 4, 8, 16, 32, 64\}$, and the relation $a|b$.
(4) The set $C = \{1, 2, 4, 8, 16, 32, 64\}$, and the relation $\preccurlyeq$ defined by $a \preccurlyeq b$ if and only if $b = a^k$ for some $k \in \mathbb{N}$, for all $a, b \in C$. (It was proved in Exercise 7.4.3 that $(C, \preccurlyeq)$ is a poset.)
(5) The set $\mathcal{P}(\{1, 2, 3\})$, and the relation $\subseteq$.

Exercise 7.4.5. [Used in Example 7.4.2.]

(1) Give an example of a relation on $\mathbb{R}$ that is transitive and antisymmetric but neither symmetric nor reflexive.
(2) Let A be a non-empty set, and let R be a relation on A. Suppose that R is both symmetric and antisymmetric. Prove that every element of A is related at most to itself.

Exercise 7.4.6.

(1) Prove that if the poset has a greatest element, then the greatest element is unique, and if a poset has a least element, then the least element is unique. unique.
(2) Find an example of a poset that has both a least element and a greatest element, an example that has a least element but not a greatest element, an example that has a greatest element but not a least element and an example that has neither.

Exercise 7.4.7. Prove that a greatest element of a poset is a maximal element, and that a least element of a poset is a minimal element.

Exercise 7.4.8. [Used in Theorem 7.4.9, Theorem 7.4.13 and Theorem 7.4.18.] Let $(A, \preccurlyeq)$ be a poset, and let $B \subseteq A$ be a subset. The relation $\preccurlyeq$ is defined by a subset $\bar{R} \subseteq A \times A$. Then $\bar{R} \cap B \times B$ defines a relation on B, which can be thought of as the restriction of $\preccurlyeq$ to B; for convenience, because no confusion arises, we will also denote this relation on B by $\preccurlyeq$. Prove that $(B, \preccurlyeq)$ is a poset.

Exercise 7.4.9. [Used in Theorem 7.4.13.] Complete the missing step in the proof of Theorem 7.4.13. That is, let $\preccurlyeq'$ be as defined in the proof of the theorem. Prove that $\preccurlyeq'$ is a total order on A, and that if $x \preccurlyeq y$ then $x \preccurlyeq' y$, for all $x, y \in A$.

Exercise 7.4.10. Let A be a non-empty set, and let R be a relation on A. The relation R is a **quasi-ordering** if it is reflexive and transitive.

Suppose that R is a quasi-ordering. Let $\sim$ be the relation on A defined by $x \sim y$ if and only if $x R y$ and $y R x$, for all $x, y \in A$.

(1) Prove that $\sim$ is an equivalence relation.
(2) Let $x, y, a, b \in A$. Prove that if $x R y$, and $x \sim a$, and $y \sim b$, then $a R b$.
(3) Form the quotient set $A/\!\sim$, as defined in Definition 5.3.6. Let S be the relation on $A/\!\sim$ defined by $[x] S [y]$ if and only if $x R y$. Prove that S is well-defined.

(4) Prove that $(A/\sim, S)$ is a poset.

Exercise 7.4.11. Let $(A, \preccurlyeq)$ be a poset. For each $X \subseteq A$, let $Prec(X)$ be the set defined by

$$Prec(X) = \{w \in A \mid w \preccurlyeq x \text{ and } w \neq x \text{ for all } x \in X\}.$$

Let $C, D \subseteq A$. Prove that $Prec(C \cup D) = Prec(C) \cap Prec(D)$.

Exercise 7.4.12. Let $(A, \preccurlyeq)$ be a poset. Let $f: A \to \mathcal{P}(A)$ be defined by $f(x) = \{y \in A \mid y \preccurlyeq x\}$ for all $x \in A$.

(1) Let $x, z \in A$. Prove that $x \preccurlyeq z$ if and only if $f(x) \subseteq f(z)$.
(2) Prove that f is injective.

Exercise 7.4.13. Let $(A, \preccurlyeq)$ be a poset, let X be a set and let $h: X \to A$ be a function. Let $\preccurlyeq'$ be the relation on X defined by $x \preccurlyeq' y$ if and only if $h(x) \preccurlyeq h(y)$, for all $x, y \in X$. Prove that $(X, \preccurlyeq')$ is a poset.

Exercise 7.4.14. Let $(A, \preccurlyeq)$ be a poset, and let X be a set. Let $\mathcal{F}(X, A)$ be as defined in Section 4.5. Let $\preccurlyeq'$ be the relation on $\mathcal{F}(X, A)$ defined by $f \preccurlyeq' g$ if and only if $f(x) \preccurlyeq g(x)$ for all $x \in X$, for all $f, g \in \mathcal{F}(X, A)$. Prove that $(\mathcal{F}(X, A), \preccurlyeq')$ is a poset.

Exercise 7.4.15. Let $\preccurlyeq$ denote the relation $a \mid b$ on $\mathbb{N}$, and let $\preccurlyeq'$ be the relation on $\mathbb{N}$ defined by $a \preccurlyeq' b$ if and only if $b = a^k$ for some $k \in \mathbb{N}$, for all $a, b \in \mathbb{N}$. (It was proved in Exercise 7.4.3 that $(\mathbb{N}, \preccurlyeq')$ is a poset.) Prove that the identity map $1_{\mathbb{N}}: \mathbb{N} \to \mathbb{N}$ is an order homomorphism from $(\mathbb{N}, \preccurlyeq')$ to $(\mathbb{N}, \preccurlyeq)$, but that it is not an order isomorphism.

Exercise 7.4.16. [Used in Section 7.4.] Let $\mathbb{N}^-$ be the set of negative integers. Prove that there is no order isomorphism from the poset $(\mathbb{N}, \leq)$ to the poset $(\mathbb{N}^-, \leq)$.

Exercise 7.4.17. Let $(A, \preccurlyeq)$ and $(B, \preccurlyeq')$ be posets, and let $f: A \to B$ be an order isomorphism. Prove that if $\preccurlyeq$ is a total order, then so is $\preccurlyeq'$.

Exercise 7.4.18. [Used in Section 3.5.] The Well-Ordering Theorem states that for any set A, there is a total ordering on the set A such that every subset of A has a least element. Prove that the Well-Ordering Theorem implies the Axiom of Choice (use the version given in Theorem 3.5.3). Recall that the Axiom of Choice is not needed when there is a specific procedure for selecting elements from sets.

7.5 Lattices

In this section we turn our attention to a special type of poset, in which certain least upper bounds and greatest lower bounds exist.

Definition 7.5.1. Let $(A, \preccurlyeq)$ be a poset.

1. Let $a, b \in A$. The **join** of a and b, denoted $a \vee b$, is the least upper bound of $\{a, b\}$, if the least upper bound exists; the join is not defined if the least upper bound does not exist. The **meet** of a and b, denoted $a \wedge b$, is the greatest lower bound of $\{a, b\}$, if the greatest lower bound exists; the meet is not defined if the greatest lower bound does not exist.

2. The poset $(A, \preccurlyeq)$ is a **lattice** if $a \wedge b$ and $a \vee b$ exist for all $a, b \in A$.   △

The symbols for meet and join are the same symbols that we used for "and" and "or" in Chapter 1. Both usages are quite standard, and no confusion should arise, because the context should be clear in every situation. The different uses of the same symbols is not entirely coincidental, however, because meet and join play roles analogous to "and" and "or," though the former do not satisfy all the properties of the latter.

Lattices are an extremely useful type of poset. A nice introduction to lattices and their applications, including a brief history of lattice theory, is [LP98, Chapters 1 and 2]; some applications mentioned include probability and boolean algebras (the latter, defined in Exercise 7.5.11, are a special type of lattice, and are of use in areas such as logic and switching circuits). A classic text on lattices is [Bir48]; another comprehensive text is [Szá63]. For a combinatorial perspective on lattices see [Bog90, Chapter 7], where some lattices related to graphs and partitions are given.

Example 7.5.2.

(1) The sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ with the relation $\leq$ are all lattices. We know from Example 7.4.2 (3) that these sets with the relation $\leq$ are all posets. Let x and y be two numbers in any one of these sets. If $x = y$ then $x \wedge y = x = y$ and $x \vee y = x = y$; if $x \neq y$, then $x \wedge y$ is the smaller of the two numbers, and $x \vee y$ is the larger. More generally, any totally ordered set is a lattice, by the same argument.

(2) Let A be a set. The poset $(\mathcal{P}(A), \subseteq)$ is a lattice. If $X, Y \in \mathcal{P}(A)$, then $X \wedge Y = X \cap Y$ and $X \vee Y = X \cup Y$.

(3) As shown in Example 7.4.2 (5), the set $\mathbb{N}$ with the relation "$a|b$" is a poset. This poset is a lattice. If $a, b \in \mathbb{N}$, then $a \wedge b$ is the greatest common divisor of a and b, and $a \vee b$ is the least common multiple.

(4) If a finite poset is represented by a Hasse diagram, we can use the Hasse diagram to check whether or not the poset is a lattice. In Figure 7.5.1 (i)(ii) we see posets that are lattices. For example, in Part (i) we see that $y \vee z = x$ and $y \wedge z = w$. On the other hand, the posets in Figure 7.5.1 (iii)(iv) are not lattices. For example, in Part (iii) of the figure the elements s and t do not have an upper bound, and hence no least upper bound, and therefore no join. In Part (iv) of the figure the elements y and z have two upper bounds, but no least upper bound, and therefore no join. A very thorough discussion of Hasse diagrams of lattices is given in [Dub64, pp. 9–19].

(5) Let $\preccurlyeq$ be the relation on $\mathbb{N}$ defined by $a \preccurlyeq b$ if and only if $b = a^k$ for some $k \in \mathbb{N}$, for all $a, b \in \mathbb{N}$. It was proved in Exercise 7.4.3 that $(\mathbb{N}, \preccurlyeq)$ is a poset. This poset is not a lattice, however, because meets and joins do not always exist. For example, the numbers 2 and 3 have neither a lower bound nor an upper bound, and hence neither a greatest lower bound nor a least upper bound. Suppose to the contrary that c is an upper bound of $\{2, 3\}$. It follows that $2 \preccurlyeq c$ and $3 \preccurlyeq c$, and therefore there are $k, j \in \mathbb{N}$ such that $c = 2^k$ and $c = 3^j$. Hence $2^k = 3^j$, which cannot be the case. Now suppose that d is a lower bound of $\{2, 3\}$. Then $d \preccurlyeq 2$ and $d \preccurlyeq 3$, and therefore there are $p, q \in \mathbb{N}$ such that $2 = d^p$ and $3 = d^q$, which again cannot happen, because p and q are natural numbers. Some meets and joints do exist in this poset, for example $4 \wedge 8 = 2$ and $4 \vee 8 = 64$.   ◇

Fig. 7.5.1.
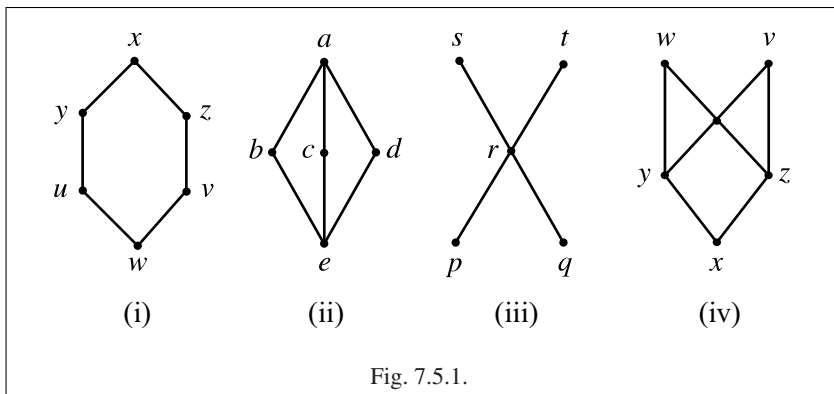
From Example 7.5.2 (1) and Example 7.4.11 (2), we see that whereas the least upper bound and the greatest lower bound of any pair of elements in a lattice must exist, the least upper bound and the greatest lower bound of an arbitrary subset of a lattice need not exist (though in some cases they do). Exercise 7.5.5 shows that for finite lattices there are no such problems.

The following theorem gives various standard properties of meet and join in lattices. See [LP98, Section 1.1] for more such properties.

Theorem 7.5.3. *Let $(L, \preccurlyeq)$ be a lattice, and let $x, y, z \in L$.*

1. $x \wedge y \preccurlyeq x$ and $x \wedge y \preccurlyeq y$ and $x \preccurlyeq x \vee y$ and $y \preccurlyeq x \vee y$.
2. $x \wedge x = x$ and $x \vee x = x$ *(Idempotent Laws).*
3. $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ *(Commutative Laws).*
4. $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$ *(Associative Laws).*
5. $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$ *(Absorption Laws).*
6. $x \preccurlyeq y$ if and only if $x \wedge y = x$ if and only if $x \vee y = y$.
7. *If* $x \preccurlyeq y$, *then* $x \wedge z \preccurlyeq y \wedge z$ and $x \vee z \preccurlyeq y \vee z$.

Proof. We will prove Parts (4) and (5), leaving the rest to the reader in Exercise 7.5.3.

(4). We will prove that $x \wedge (y \wedge z) = (x \wedge y) \wedge z$; the proof that $x \vee (y \vee z) = (x \vee y) \vee z$ is similar, and we omit the details. Let $d = x \wedge (y \wedge z)$. By Part (1) of this theorem we know that $d \preccurlyeq x$ and $d \preccurlyeq y \wedge z$. Applying Part (1) again, we see that $d \preccurlyeq y$ and $d \preccurlyeq z$. Because d is a lower bound of x and y, it follows from the definition of meet as greatest lower bound that $d \preccurlyeq x \wedge y$. Similarly, because d is a lower bound of $x \wedge y$ and z, it follows that $d \preccurlyeq (x \wedge y) \wedge z$. Hence $x \wedge (y \wedge z) \preccurlyeq (x \wedge y) \wedge z$. A similar argument shows that $(x \wedge y) \wedge z \preccurlyeq x \wedge (y \wedge z)$; we omit the details. By the antisymmetry of $\preccurlyeq$, we deduce that $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.

(5). We will prove that $x \vee (x \wedge y) = x$; the proof that $x \wedge (x \vee y) = x$ is similar, and we omit the details. By the reflexivity of $\preccurlyeq$ we know that $x \preccurlyeq x$, and by Part (1) of this theorem we know that $x \wedge y \preccurlyeq x$. Therefore x is an upper bound of x and $x \wedge y$, and by the definition of join as least upper bound, we deduce that $x \vee (x \wedge y) \preccurlyeq x$. On

the other hand, by Part (1) we know that $x \preccurlyeq x \vee (x \wedge y)$. By the antisymmetry of $\preccurlyeq$, we deduce that $x \vee (x \wedge y) = x$.   □

We see in Theorem 7.5.3 that some of the standard algebraic properties of addition and multiplication of numbers also hold for lattices. However, not all familiar properties of addition and multiplication of numbers hold for every lattice, for example the Distributive Law. This law does hold for the lattice in Example 7.5.2 (2), as seen from Theorem 3.3.3 (5), but it does not hold in the lattice represented by the Hasse diagram in Figure 7.5.1 (ii). In that Hasse diagram, we see that $b \wedge (c \vee d) = b \wedge a = b$, whereas $(b \wedge c) \vee (b \wedge d) = e \vee e = e$. Exercise 7.5.7 gives two inequalities related to the Distributive Law that hold in all lattices.

We started our discussion of posets and lattices in Section 7.4 by stating that we are interested in algebraic structures involving order relations rather than binary operations (which are discussed in Section 7.1). Though posets truly involve only an order relation, in lattices there are two binary operations, namely, meet and join. (Indeed, it is because meet and join are binary operations that we prefer the notation $a \wedge b$ and $a \vee b$ rather than the notation glb$\{a,b\}$ and lub$\{a,b\}$, respectively.) The binary operations meet and join satisfy certain properties, some of which were given in Theorem 7.5.3. As shown in the following theorem, we can in fact reformulate the definition of lattices as sets with two binary operations that satisfy certain properties, which in turn give rise to the appropriate type of order relation. The basic idea for this theorem is Theorem 7.5.3 (6), which expresses the partial ordering relation in terms of meet and join.

Theorem 7.5.4. *Let A be a set, and let $\sqcap \colon A \times A \to A$ and $\sqcup \colon A \times A \to A$ be binary operations on A. Suppose that $\sqcap$ and $\sqcup$ satisfy the following properties. Let $x, y, z \in A$.*

  a. $x \sqcap y = y \sqcap x$ and $x \sqcup y = y \sqcup x$.
  b. $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$ and $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$.
  c. $x \sqcap (x \sqcup y) = x$ and $x \sqcup (x \sqcap y) = x$.

Let $\preccurlyeq$ be the relation on A defined by $x \preccurlyeq y$ if and only if $x \sqcap y = x$, for all $x, y \in A$. Then $(A, \preccurlyeq)$ is a lattice, with $\sqcap$ and $\sqcup$ the meet and join of the lattice, respectively.

Proof. We follow [Bir48] and [LP98] in part. As a preliminary, we prove the following two facts: (1) $x \sqcap x = x$ for all $x \in A$; and (2) $x \sqcap y = x$ if and only if $x \sqcup y = y$, for all $x, y \in A$. Let $x, y, z \in A$. Using both parts of Property (c), we see that $x \sqcap x = x \sqcap (x \sqcup (x \sqcap x)) = x$, which proves Fact (1). Suppose that $x \sqcap y = x$. Then by Properties (a) and (c) we see that $x \sqcup y = (x \sqcap y) \sqcup y = y \sqcup (y \sqcap x) = y$, which proves one of the implications in Fact (2); a similar argument proves the other implication, and we omit the details.

We now show that $(A, \preccurlyeq)$ is a poset. Because $x \sqcap x = x$ by Fact (1), it follows from the definition of $\preccurlyeq$ that $x \preccurlyeq x$. Hence $\preccurlyeq$ is reflexive. Now suppose that $x \preccurlyeq y$ and $y \preccurlyeq z$. Then $x \sqcap y = x$ and $y \sqcap z = y$. By Property (b) we see that $x \sqcap z = (x \sqcap y) \sqcap z = x \sqcap (y \sqcap z) = x \sqcap y = x$. It follows that $x \preccurlyeq z$. Therefore $\preccurlyeq$ is transitive. Next, suppose

that $x \preccurlyeq y$ and $y \preccurlyeq x$. Then $x \sqcap y = x$ and $y \sqcap x = y$. It follows from Property (a) that $x = y$. Therefore $\preccurlyeq$ is antisymmetric. We conclude that $(A, \preccurlyeq)$ is a poset.

Finally, we show that $\sqcap$ and $\sqcup$ are the meet and join of $(A, \preccurlyeq)$, respectively. It will then follow from this fact that meet and join always exist for any two elements of A, and hence $(A, \preccurlyeq)$ is a lattice. We start with $\sqcap$. Using Property (b) and Fact (1) we see that $(x \sqcap y) \sqcap y = x \sqcap (y \sqcap y) = x \sqcap y$. Hence $x \sqcap y \preccurlyeq y$. Because $x \sqcap y = y \sqcap x$ by Property (a), a similar argument shows that $x \sqcap y \preccurlyeq x$. Therefore $x \sqcap y$ is a lower bound of $\{x, y\}$. Now suppose that $z \in A$ is a lower bound of $\{x, y\}$. Then $z \preccurlyeq x$ and $z \preccurlyeq y$, and therefore $z \sqcap x = z$ and $z \sqcap y = z$. By Property (b) we see that $z \sqcap (x \sqcap y) = (z \sqcap x) \sqcap y = z \sqcap y = z$. Hence $z \preccurlyeq (x \sqcap y)$. It follows that $x \sqcap y$ is the greatest lower bound of $\{x, y\}$, which means that $x \sqcap y$ is the meet of x and y.

We now turn to $\sqcup$. By Property (c) we know that $x \sqcap (x \sqcup y) = x$. Hence $x \preccurlyeq x \sqcup y$. Because $x \sqcup y = y \sqcup x$ by Property (a), a similar argument shows that $y \preccurlyeq x \sqcup y$. Hence $x \sqcup y$ is an upper bound of $\{x, y\}$. Now suppose that $w \in A$ is an upper bound of $\{x, y\}$. Then $x \preccurlyeq w$ and $y \preccurlyeq w$, and therefore $x \sqcap w = x$ and $y \sqcap w = y$. By Fact (2) we deduce that $x \sqcup w = w$ and $y \sqcup w = w$. Property (b) then implies that $(x \sqcup y) \sqcup w = x \sqcup (y \sqcup w) = x \sqcup w = w$. Hence $(x \sqcup y) \sqcap w = x \sqcup y$ by Fact (2). Therefore $x \sqcup y \preccurlyeq w$. It follows that $x \sqcup y$ is the least upper bound of $\{x, y\}$, which means that $x \sqcup y$ is the join of x and y. $\square$

Whereas Theorem 7.5.4 says that it is possible to view lattices as being defined by binary operations, which is useful in some approaches to the subject, it is nonetheless often useful to view lattices as we did originally, based upon partial orderings.

In Section 7.4 we discussed order homomorphisms and order isomorphisms of posets. Because lattices are posets, we can apply such functions to lattices. Additionally, there are two other types of functions that are suited to lattices, though not to arbitrary posets.

Definition 7.5.5. Let $(L, \preccurlyeq)$ and $(M, \preccurlyeq')$ be lattices, and let $f \colon L \to M$ be a function. Let $\wedge$ and $\vee$ be the meet and join for L, and let $\wedge'$ and $\vee'$ be the meet and join for M. The function f is a **meet homomorphism** if $f(x \wedge y) = f(x) \wedge' f(y)$ for all $x, y \in L$. The function f is a **join homomorphism** if $f(x \vee y) = f(x) \vee' f(y)$ for all $x, y \in L$. $\triangle$

Example 7.5.6.

(1) The function $f \colon D \to \mathcal{P}(A)$ in Example 7.4.17 (2) is both a meet homomorphism and a join homomorphism, as the reader can verify.

(2) Let $(L, \preccurlyeq)$ and $(M, \preccurlyeq')$ be the lattices represented by the Hasse diagrams in Figure 7.5.1 (i)(ii). Let $f \colon L \to M$ be defined by

$$f(s) = \begin{cases} a, & \text{if } s = x \\ e, & \text{otherwise.} \end{cases}$$

The function f is a meet homomorphism. If $s, t \in L$ are not both x, then $s \wedge t \neq x$, and hence $f(s \wedge t) = e = e \wedge e = f(s) \wedge f(t)$; also, we observe that $f(x \wedge x) = f(x) = a = a \wedge a = f(x) \wedge f(x)$. The function f is not a join homomorphism, because $f(y \vee z) =$

$f(x) = a$, but $f(y) \vee f(z) = e \vee e = e$. A similar construction yields a function $L \to M$ that is a join homomorphism but not a meet homomorphism.

(3) The function $s \colon \mathcal{P}_F(\mathbb{N}) \to \mathbb{Z}$ in Example 7.4.17 (1) is an order homomorphism, as was stated in that example. However, this function is neither a meet homomorphism nor a join homomorphism. For example, let $X = \{5, 7\}$, and let $Y = \{7, 9\}$. Then, as in Example 7.5.2 (2), we see that $X \wedge Y = X \cap Y = \{7\}$, and $X \vee Y = X \cup Y = \{5, 7, 9\}$. Hence $s(X \wedge Y) = 1$ and $s(X \vee Y) = 3$. However, as discussed in Example 7.5.2 (1), we see that $s(X) \wedge s(Y) = 2 \wedge 2 = 2$, and $s(X) \vee s(Y) = 2 \vee 2 = 2$. Hence $s(X \wedge Y) \neq s(X) \wedge s(Y)$ and $s(X \vee Y) \neq s(X) \vee s(Y)$. $\diamond$

We now have four types of functions that we can use with lattices, namely, order homomorphisms, order isomorphisms, meet homomorphisms and join homomorphisms. How are these different types of functions related? We saw in Example 7.4.17 (1) that a function can be an order homomorphism without being an order isomorphism. We saw in Example 7.5.6 (2) that a function can be a meet homomorphism without being a join homomorphism, and vice versa. Parts (1) and (3) of the following theorem clarify the relations between the four types of functions.

Theorem 7.5.7. *Let $(L, \preccurlyeq)$ and $(M, \preccurlyeq')$ be lattices, and let $f \colon L \to M$ be a function.*

1. *If f is a meet homomorphism or a join homomorphism, then it is an order homomorphism.*
2. *If f is bijective and a meet (respectively, join) homomorphism, then f^{-1} is a meet (respectively, join) homomorphism.*
3. *The function f is an order isomorphism if and only if f is bijective and a meet homomorphism if and only if f is bijective and a join homomorphism.*

Proof. We will prove Part (1), leaving the rest to the reader in Exercise 7.5.14.

(1). Suppose that f is a meet homomorphism. Let $\wedge$ and $\wedge'$ denote the meet for L and M, respectively. Let $x, y \in L$. Suppose that $x \preccurlyeq y$. Then by Theorem 7.5.3 (6) we know that $x = x \wedge y$. Then $f(x) = f(x \wedge y) = f(x) \wedge' f(y)$, because f is a meet homomorphism. Using Theorem 7.5.3 (6) again, we deduce that $f(x) \preccurlyeq' f(y)$. It follows that f is an order homomorphism. A similar argument works if f is a join homomorphism; we omit the details. $\square$

Because of Theorem 7.5.7 (3), we consider two lattices to be essentially the same if there is an order isomorphism between them, or, equivalently, if there is a bijective meet homomorphism or a bijective join homomorphism between them.

We conclude this section with a nice result that involves the notion of a fixed point of a function, that is, an element taken to itself by the function. Fixed points arise in many parts of mathematics, for example the famous Brouwer Fixed Point Theorem in topology (see [Nab80, p. 29]), as well as in applications of mathematics to economics (see [Deb] or [KR83b, pp. 38–39]). The following theorem gives a criterion that guarantees the existence of fixed points for certain functions of lattices to themselves.

Theorem 7.5.8. *Let* $(L, \preccurlyeq)$ *be a lattice, and let* $f: L \to L$ *be an order homomorphism. Suppose that the least upper bound and greatest lower bound exist for all non-empty subsets of L. Then there is some* $a \in L$ *such that* $f(a) = a$.

Proof. Let $C = \{x \in L \mid x \preccurlyeq f(x)\}$. Observe that L is non-empty because it is a poset, and all posets are assumed to be non-empty. Let m be the greatest lower bound of L, which exists by hypothesis. Then m is a lower bound of L, and therefore $m \preccurlyeq x$ for all $x \in L$. In particular, we see that $m \preccurlyeq f(m)$. It follows that $m \in C$, and so C is non-empty.

Let a be the least upper bound of C. Let $x \in C$. Then a is an upper bound of C, and therefore $x \preccurlyeq a$. Using the definition of C and the fact that f is an order homomorphism, we deduce that $x \preccurlyeq f(x) \preccurlyeq f(a)$. It follows that $f(a)$ is an upper bound for C. Because a is the least upper bound of C, we deduce that $a \preccurlyeq f(a)$. Because f is an order homomorphism, it follows that $f(a) \preccurlyeq f(f(a))$. Hence $f(a) \in C$, and therefore $f(a) \preccurlyeq a$, because a is an upper bound of C. By antisymmetry, we deduce that $f(a) = a$. $\qquad\qquad\square$

Corollary 7.5.9. *Let* $(L, \preccurlyeq)$ *be a lattice, and let* $f: L \to L$ *be an order homomorphism. If L is finite, then there is some* $a \in L$ *such that* $f(a) = a$.

Proof. This corollary follows immediately from Exercise 7.5.5 and Theorem 7.5.8. $\qquad\qquad\square$

Theorem 7.5.8 does not necessarily hold for lattices that do not satisfy the additional hypothesis concerning least upper bounds and greatest lower bounds. Consider the lattice $(\mathbb{N}, \leq)$ and the function $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x + 1$ for all $x \in \mathbb{N}$. This function is an order isomorphism, and yet there is no $a \in \mathbb{N}$ such that $f(a) = a$. Of course, arbitrary subsets of $\mathbb{N}$ do not necessarily have least upper bounds, so Theorem 7.5.8 does not apply.

Exercises

Exercise 7.5.1. Which of the posets given in Exercise 7.4.4 are lattices?

Exercise 7.5.2. Which of the posets represented by Hasse diagrams in Figure 7.5.2 are lattices?

Exercise 7.5.3. **[Used in Theorem 7.5.3.]** Prove Theorem 7.5.3 (1) (2) (3) (6) (7).

Exercise 7.5.4. Find Hasse diagrams corresponding to all possible distinct lattices with five elements.

Exercise 7.5.5. **[Used in Section 7.5 and Corollary 7.5.9.]** Let $(L, \preccurlyeq)$ be a lattice. Prove that if $X \subseteq L$ is a finite subset, then X has a least upper bound and a greatest lower bound. Deduce that if L is finite and if $X \subseteq L$ is a subset, then X has a least upper bound and a greatest lower bound.

Exercise 7.5.6. Let $(L, \preccurlyeq)$ be a lattice, and let $a, b \in L$. Prove that $a \wedge b = a \vee b$ if and only if $a = b$.
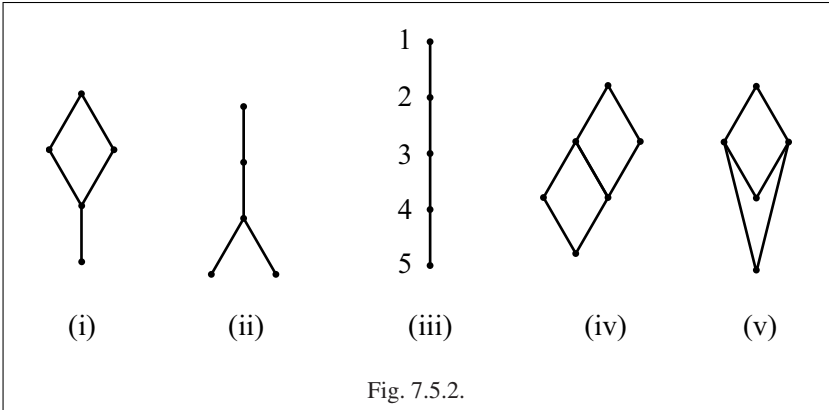
Fig. 7.5.2.

Exercise 7.5.7. **[Used in Section 7.5.]** Let $(L, \preccurlyeq)$ be a lattice, and let $a, b, c \in L$. Prove the following inequalities.

   (1) $a \wedge (b \vee c) \succcurlyeq (a \wedge b) \vee (a \wedge c)$ (Distributive Inequality).
   (2) $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$ (Distributive Inequality).
   (3) If $a \succcurlyeq c$, then $a \wedge (b \vee c) \succcurlyeq (a \wedge b) \vee c$ (Modular Inequality).
   (4) If $a \preccurlyeq c$, then $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$ (Modular Inequality).

Exercise 7.5.8. **[Used in Exercise 7.5.9, Exercise 7.5.11 and Exercise 7.5.12.]** Let $(L, \preccurlyeq)$ be a lattice. Prove that $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in A$ if and only if $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ for all $a, b, c \in A$.

   The lattice $(L, \preccurlyeq)$ is **distributive** if either (and hence both) of these conditions holds.

Exercise 7.5.9. Let $(L, \preccurlyeq)$ be a lattice, and let $a, b, c \in A$. Suppose that $(L, \preccurlyeq)$ is distributive, as defined in Exercise 7.5.8 Prove that if $a \wedge c = b \wedge c$ and $a \vee c = b \vee c$, then $a = b$.

Exercise 7.5.10. **[Used in Exercise 7.5.11 and Exercise 7.5.12.]** Let $(L, \preccurlyeq)$ be a lattice. The lattice $(L, \preccurlyeq)$ is **complemented** if it has a least element O and a greatest element I such that $O \neq I$, and if for each $a \in L$, there is an element $a' \in L$ such that $a \wedge a' = O$ and $a \vee a' = I$.

   Suppose that $(L, \preccurlyeq)$ is complemented. For each $a \in L$, is a' unique? Give a proof or a counterexample.

Exercise 7.5.11. **[Used in Section 7.5 and Exercise 7.5.12.]** Let $(L, \preccurlyeq)$ be a lattice. The lattice $(L, \preccurlyeq)$ is a **boolean algebra** if it is distributive and complemented, as defined in Exercise 7.5.8 and Exercise 7.5.10 respectively.

   Suppose that $(L, \preccurlyeq)$ is a boolean algebra. Let $a, b \in L$.

   (1) Prove that a' is unique.
   (2) Prove that $(a \wedge b)' = a' \vee b'$ and $(a \vee b)' = a' \wedge b'$.

Exercise 7.5.12. Which of the following lattices are distributive, complemented and/or boolean algebras, as defined in Exercise 7.5.8, Exercise 7.5.10 and Exercise 7.5.11, respectively?

(1) The lattice in Example 7.5.2 (2).
(2) The lattice in Example 7.5.2 (3).
(3) The lattices represented by the Hasse diagrams in Figure 7.5.3.

Fig. 7.5.3.
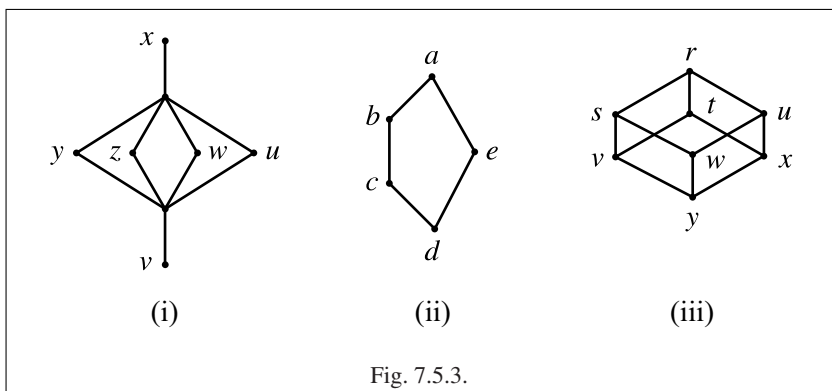
Exercise 7.5.13. Let $(L, \preccurlyeq)$ and $(M, \preccurlyeq')$ be the lattices represented by the Hasse diagrams in Figure 7.5.3 (ii) and Figure 7.5.2 (iii), respectively. Described below are various functions $L \to M$. Which of these functions is an order homomorphism, a meet homomorphism, a join homomorphism and/or an order isomorphism?

(1) $f(a) = f(b) = f(c) = f(d) = f(e) = 1$.
(2) $f(a) = f(b) = f(c) = f(d) = 1$, and $f(e) = 2$.
(3) $f(a) = f(b) = f(c) = f(e) = 1$, and $f(d) = 5$.
(4) $f(b) = f(c) = f(d) = 3$, and $f(a) = f(e) = 2$.
(5) $f(a) = 1$, and $f(b) = 2$, and $f(c) = 3$, and $f(d) = 4$, and $f(e) = 5$.

Exercise 7.5.14. **[Used in Theorem 7.5.7.]** Prove Theorem 7.5.7 (2) (3).

7.6 Counting: Products and Sums

Some very interesting, and extremely applicable, mathematical questions involve counting. Aspects of number theory, probability, graph theory and optimization, for example, all use counting arguments. A branch of contemporary mathematics, called combinatorics, deals with counting questions in very sophisticated ways. See [Bog90] for a very nice treatment of combinatorics at a level appropriate to anyone who has finished the present text; see [Rob84] for many applications of counting.

A counting problem, in the terminology we have developed so far, is the determination of the cardinality of a finite set. The difficulty arises when the elements of the set are described, possibly quite indirectly, but are not listed explicitly. Suppose, for example, that we want to find the number of integers from 1 to 20 that are not divisible by any of 3, 5 or 13. That is, we want to find the cardinality of the set

$$S = \{n \in \mathbb{N} \mid 1 \leq n \leq 20 \text{ and } n \text{ is not divisible by } 3, 5 \text{ or } 13\}.$$

This problem is trivial, of course, because we list the elements of this set explicitly as $S = \{1, 2, 4, 7, 8, 11, 14, 16, 17, 19\}$. Hence $|S| = 10$. Now suppose that we wanted to find the number of integers from 1 to 1,000,000 that are not divisible by any of 3, 5 or 13. Here it would be a very unpleasant task to list all the elements of the set explicitly. We will answer this problem without listing the elements of the set in Example 7.6.11 (2), after we have developed some useful techniques.

In this section and the next we will discuss a few of the most basic ways of figuring out the cardinalities of finite sets. Our approach is a bit different from many standard treatments of the subject—not in the statements of our results, but in our approach to proving them. In many texts, such as [Bog90, Chapter 1], the discussion of counting starts out by simply stating without proof some basic counting principles such as the Product Rule and Sum Rule (which we will discuss shortly). These rules are then used both to solve various applied problems, and to yield proofs of mathematical theorems. An example of such a theorem would be a formula for the number of injective functions from one finite set to another, the proof of which is simple if we have these basic counting principles at our disposal.

Our approach is the opposite of what was just described. We are not interested in counting problems for their own sake (though they are certainly worthwhile), but rather as an interesting and useful application of the ideas developed throughout this text. Therefore, instead of hypothesizing the Product Rule and Sum Rule, and using counting arguments in our proofs, we will formulate ideas about counting in terms of our familiar notions of sets, functions and relations. In particular, we will prove the Product Rule and Sum Rule, as well as other results, by relating these topics to concepts such as injective functions from one finite set to another, and using what we have previously learned. Some of our proofs might therefore appear more cumbersome than in other texts, and not focused on counting per se—both of which are true, but reasonable given our goals.

We start our discussion of counting, as do many texts, with the "Product Rule." A typical informal statement of this result is as follows; we use the formulation in [Rob84, Chapter 2].

Fact 7.6.1 (**Product Rule**). *If something can happen in n ways, and no matter how the first thing happens, a second thing can happen in m ways, then the two things together can happen in n · m ways.*

Some simple examples of the use of this rule are as follows.

Example 7.6.2.

(1) Fred has seven shirts and five pairs of pants. How many ways can Fred choose a shirt/pants pair (assuming that Fred does not care whether his shirt and pants match)? By the Product Rule, there are $7 \cdot 5 = 35$ ways.

(2) A committee of 6 people wants to select a chair and a vice-chair. How many ways can this happen, assuming that no person can simultaneously hold both positions? If the committee first chooses the chair, there are 6 choices. For each of these choices, there are then 5 choices for vice-chair. By the Product Rule, there are $6 \cdot 5 = 30$ choices for the two positions. If the committee chose the vice-chair first, the total number of choices for chair and vice-chair would still be 30. Observe that the collections of "second things" that can happen are not disjoint.

The Product Rule can be generalized to any finite number of things happening. For example, suppose that the above committee decided to choose not just a chair and vice-chair but also a treasurer, again stipulating that no person can hold more than one position. By reasoning as above, we deduce that there are $6 \cdot 5 \cdot 4 = 120$ choices. ◇

Although the Product Rule is often stated in term of numbers of "ways that things can happen," and for practical problem solving that way of formulating it is very useful, the expression "ways that things can happen" is not entirely rigorous, and does not directly fit into our framework of sets, functions, relations and the like. Fortunately, we can reformulate the Product Rule in terms of cardinalities of finite sets. To simplify matters we will restrict our attention to the product of two "choices," because it is all we will need later on.

Observe that in Example 7.6.2 (1), the choice of the "second thing that happens" is independent of the choice of the "first thing," whereas in Part (2) of the example the second choice is not independent of the first. The former situation is a special case of the latter, but it is convenient to deal with this special case first, as we do in the following theorem. The proof of this theorem makes use of an important fact about the integers, namely, the Division Algorithm, which is stated as Theorem A.5 in the Appendix.

Theorem 7.6.3. *Let A and B be sets. Suppose that A and B are finite. Then $A \times B$ is finite, and $|A \times B| = |A| \cdot |B|$.*

Proof. If A or B is empty, then so is $A \times B$, and the result is trivial. Now suppose that A and B are both non-empty. Let $n = |A|$ and $p = |B|$, and let $f \colon A \to \{1, \ldots, n\}$ and $g \colon B \to \{1, \ldots, p\}$ be bijective functions. Let $h \colon A \times B \to \{1, \ldots, np\}$ be defined by $h((a, b)) = (f(a) - 1)p + g(b)$ for all $(a, b) \in A \times B$.

Let $x \in \{1, \ldots, np\}$. By the Division Algorithm (Theorem A.5 in the Appendix) there are $q, r \in \mathbb{Z}$ such that $x = pq + r$ and $0 \leq r < p$. Because $1 \leq x \leq np$, it follows that $0 \leq q \leq n$. There are now two cases. First, suppose that $r \neq 0$. Then $q \neq n$. By the surjectivity of f and g, there are $a \in A$ and $b \in B$ such that $f(a) = q + 1$ and $g(b) = r$. Then $h((a, b)) = ((q + 1) - 1)p + r = pq + r = x$. Next, suppose that $r = 0$. Then $q \neq 0$. By the surjectivity of f and g, there are $m \in A$ and $n \in B$ such that

$f(m) = q$ and $g(n) = p$. Then $h((m,n)) = (q-1)p + p = pq + 0 = x$. It follows that h is surjective.

Let $(a,b),(c,d) \in A \times B$, and suppose that $h((a,b)) = h((c,d))$. Then $(f(a) - 1)p + g(b) = (f(c) - 1)p + g(d)$. Hence $[f(a) - f(c)]p + [g(b) - g(d)] = 0$. Observe that $0 \leq |g(b) - g(d)| < p$. Because $0 \cdot p + 0 = 0$, we can see the uniqueness part of the Division Algorithm to deduce that $f(a) - f(c) = 0$ and $g(b) - g(d) = 0$. Hence $f(a) = f(c)$ and $g(b) = g(d)$. By the injectivity of f and g, we see that $(a,b) = (c,d)$. It follows h is injective.

Because h is bijective, it follows that $|A \times B| = np = |A| \cdot |B|$.   □

The proof of Theorem 7.6.3 might appear to the reader to be needlessly complicated, given that the result being proved is intuitively simple. It is, in fact, possible to prove this theorem without using the Division Algorithm, as is left to the reader in Exercise 7.6.5. Avoiding the Division Algorithm yields somewhat simpler proofs than the one given above, but these simpler proofs have the disadvantage of not giving an explicit bijective function $h: A \times B \to \{1, \ldots, |A| \cdot |B|\}$.

We are now ready for the general case of the Product Rule, which allows for the second choices to depend upon the first choice.

Theorem 7.6.4 (Product Rule). *Let A be a set, and let $\{B_a\}_{a \in A}$ be a family of sets indexed by A. Suppose that A is finite, that B_a is finite for all $a \in A$ and that there is a set B such that $B \sim B_a$ for all $a \in A$. Let $X = \{(a,b) \mid a \in A \text{ and } b \in B_a\}$. Then X is finite, and $|X| = |A| \cdot |B|$.*

Proof. By hypothesis there is a bijective function $g_a: B_a \to B$ for each $a \in A$. Let $\Phi: X \to A \times B$ be defined by $\Phi((a,b)) = (a, g_a(b))$ for all $(a,b) \in X$. It is left to the reader in Exercise 7.6.6 to show that Φ is bijective. It follows that $X \sim A \times B$. We now use Theorem 7.6.3 and Corollary 6.6.3 to deduce that X is finite, and that $|X| = |A \times B| = |A| \cdot |B|$.   □

The other standard counting rule given in introductory treatments of combinatorics is the "Sum Rule." A typical informal statement of this result, also from [Rob84, Chapter 2], is as follows.

Fact 7.6.5 (Sum Rule). *If one event can occur in n ways and a second event in m (different) ways, then there are $n + m$ ways in which either the first event or the second event can occur (but not both).*

Observe that the Product Rule, which is about multiplication, involves "and" situations, whereas the Sum Rule, which is about addition, involves "or" situations, though the meaning here is exclusive "or," rather than the inclusive "or" regularly used by mathematicians (we will discuss the inclusive case shortly). Some simple examples of the use of the Sum Rule are as follows.

Example 7.6.6.

(1) Murkstown High School has 120 juniors and 95 seniors. The principal has to pick one junior or one senior to represent the school at a conference. How many

choices are there? Because we may assume that no student is simultaneously a junior and a senior, by the Sum Rule there are $120 + 95 = 215$ choices.

(2) Every resident on planet Blort has either just a first name, or both a first name and a last name. These names must be chosen from a list of 17 acceptable choices. How many differently named Blortians can there be? For those Blortians with only one name, there are 17 possibilities. For those with two names, by the Product Rule there are $17 \cdot 17 = 289$ possibilities. By the Sum Rule, there can be a total of $17 + 289 = 306$ differently named Blortians. ◇

Similarly to the Product Rule, the Sum Rule can also be stated in terms of cardinalities of finite sets, as we do in Part (2) of the following theorem. Part (3) of the theorem deals with the inclusive "or" situation; the intuitive idea is that we should not double count the elements in the intersection of the two given sets.

Theorem 7.6.7 (Sum Rule). *Let A and B be sets. Suppose that A and B are finite.*

    1. The sets $A \cup B$ and $A \cap B$ are finite.
    2. If A and B are disjoint, then $|A \cup B| = |A| + |B|$.
    3. $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof.

    (1). The fact that $A \cap B$ is finite follows immediately from Theorem 6.6.5 (1), because $A \cap B \subseteq A$. The fact that $A \cup B$ is finite is shown in Exercise 6.6.1.

    (2). This part is a special case of Part (3) of the theorem, which is proved below.

    (3). Viewing $A \cap B$ as a subset of B, it follows from Theorem 6.6.5 (2) that $|B| = |A \cap B| + |B - (A \cap B)|$. Viewing A as a subset of $A \cup B$, we see that $|A \cup B| = |A| + |(A \cup B) - A|$. Also, we know by Exercise 3.3.9 that $(A \cup B) - A = B - (A \cap B)$. Then

$$|A \cup B| = |A| + |(A \cup B) - A| = |A| + |B - (A \cap B)| = |A| + |B| - |A \cap B|. \qquad \square$$

Example 7.6.8. Hicksville has two radio stations, which are WSNF that plays non-stop disco, and WRNG that plays only Wagner's operas. The stations poll 20 people, and find that 15 listen to WSNF, 11 listen to WRNG, and 9 listen to both stations. From these data we can figure out how many people listen to at least one station, and how many listen to neither. Let A be the set of those people surveyed who listen to WSNF, and let B denote those who listen to WRNG. Then $|A| = 15$, and $|B| = 11$, and $|A \cap B| = 9$. By Theorem 7.6.7 (3) we see that $|A \cup B| = |A| + |B| - |A \cap B| = 15 + 11 - 9 = 17$. Therefore 17 people listen to at least one station, and hence 3 listen to neither. ◇

Theorem 7.6.7 can be generalized to the union of finitely many finite sets, rather than just two sets, as seen in the following theorem. Recall the definition of a family of sets being pairwise disjoint, given in Definition 3.5.1. Part (3) of this theorem is often called the "principle of inclusion-exclusion," and it has many applications in combinatorics. See [Rob84, Chapter 6] for various applications, and [Bog90, Section 3.1] for an interesting reformulation of the statement of this principle.

Theorem 7.6.9. *Let $A_1,\ldots,A_n$ be sets for some $n \in \mathbb{N}$. Suppose that $A_1,\ldots,A_n$ are finite.*

1. *The set $A_1 \cup \ldots \cup A_n$ is finite, and if $\{r_1,\ldots,r_k\} \subseteq \{1,\ldots,n\}$, then $A_{r_1} \cap \cdots \cap A_{r_k}$ is finite.*
2. *If $A_1,\ldots,A_n$ are pairwise disjoint, then $|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$.*
3.
$$|A_1 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k|$$
$$- \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|$$
$$= \sum_{p=1}^{n} (-1)^{p+1} \sum_{1 \le i_1 < \cdots < i_p \le n} |A_{i_1} \cap \cdots \cap A_{i_p}|.$$

Proof.

   (1). The fact that $A_1 \cup \ldots \cup A_n$ is finite is proved by induction on n, using Theorem 7.6.7 (1); the details are left to the reader. If $\{r_1,\ldots,r_k\} \subseteq \{1,\ldots,n\}$, then $A_{r_1} \cap \cdots \cap A_{r_k} \subseteq A_{r_1}$, and hence $A_{r_1} \cap \cdots \cap A_{r_k}$ is finite by Theorem 6.6.5 (1).

   (2). This part is a special case of Part (3) of the theorem, which is proved below.

   (3). We prove this result by induction on n. If $n = 1$, both sides of the equation we need to prove are just $|A_1|$, so the result is true. Now suppose that the result is true for $n - 1$. Making use of Theorem 7.6.7 (3), Theorem 3.4.5 (3) and the inductive hypothesis we see that

$$|A_1 \cup \cdots \cup A_n| = |(A_1 \cup \cdots \cup A_{n-1}) \cup A_n|$$
$$= |A_1 \cup \cdots \cup A_{n-1}| + |A_n| - |(A_1 \cup \cdots \cup A_{n-1}) \cap A_n|$$
$$= |A_n| + |A_1 \cup \cdots \cup A_{n-1}| - |(A_1 \cap A_n) \cup \cdots \cup (A_{n-1} \cap A_n)|$$
$$= |A_n| + \left\{ \sum_{i=1}^{n-1} |A_i| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n-1} |A_i \cap A_j \cap A_k| \right.$$
$$\left. - \cdots + (-1)^{(n-1)+1} |A_1 \cap \cdots \cap A_{n-1}| \right\}$$
$$- \left\{ \sum_{i=1}^{n-1} |(A_i \cap A_n)| - \sum_{1 \le i < j \le n-1} |(A_i \cap A_n) \cap (A_j \cap A_n)| \right.$$
$$\left. + \cdots + (-1)^{(n-1)+1} |(A_1 \cap A_n) \cap \cdots \cap (A_{n-1} \cap A_n)| \right\}$$
$$= |A_n| + \sum_{i=1}^{n-1} |A_i| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n-1} |A_i \cap A_j \cap A_k|$$
$$- \cdots + (-1)^{(n-1)+1} |A_1 \cap \cdots \cap A_{n-1}|$$

$$-\sum_{i=1}^{n-1}|A_i \cap A_n| + \sum_{1 \le i < j \le n-1}|A_i \cap A_j \cap A_n|$$

$$-\cdots + (-1)^{n+1}|A_1 \cap \cdots \cap A_{n-1} \cap A_n|$$

$$=\sum_{i=1}^{n}|A_i| - \sum_{1 \le i < j \le n}|A_i \cap A_j| + \sum_{1 \le i < j < k \le n}|A_i \cap A_j \cap A_k|$$

$$-\cdots + (-1)^{n+1}|A_1 \cap \cdots \cap A_n|. \qquad \square$$

Corollary 7.6.10. *Let X be a set, and let $A_1,\ldots,A_n \subseteq X$ for some $n \in \mathbb{N}$. Suppose that A is finite. Then*

$$|X - (A_1 \cup \cdots \cup A_n)| = |X| - \sum_{i=1}^{n}|A_i| + \sum_{1 \le i < j \le n}|A_i \cap A_j|$$

$$- \sum_{1 \le i < j < k \le n}|A_i \cap A_j \cap A_k| + \cdots + (-1)^n|A_1 \cap \cdots \cap A_n|.$$

Proof. This corollary follows from Theorem 6.6.5 (2) and Theorem 7.6.9 (3). $\square$

Example 7.6.11.

(1) A class of 30 students was surveyed to find out how many students liked bananas, pickles and/or ice cream. The survey showed that 11 liked bananas, 16 liked pickles, 17 liked ice cream, 5 liked both bananas and pickles, 4 liked both bananas and ice cream, 8 liked both pickles and ice cream, and everyone in the class liked at least one of these foods. The survey forgot to ask how many students liked all three of the foods, but we can figure that out from the given data. Let B, P and I denote the sets of students who like bananas, pickles and ice cream, respectively. The survey then says that $|B| = 11$, and $|P| = 16$, and $|I| = 17$, and $|B \cap P| = 5$, and $|B \cap I| = 4$, and $|P \cap I| = 8$, and $|B \cup P \cup I| = 30$. By Theorem 7.6.9 (3) we see that

$$|B \cup P \cup I| = (|B| + |P| + |I|) - (|B \cap P| + |B \cap I| + |P \cap I|) + |B \cap P \cap I|,$$

which yields
$$30 = (11 + 16 + 17) - (5 + 4 + 8) + |B \cap P \cap I|.$$

Hence $|B \cap P \cap I| = 3$, which is the number of students who like all three foods.

(2) We can now solve a problem stated at the beginning of this section, which is to find the number of integers from 1 to 1,000,000 that are not divisible by any of 3, 5 or 13. Let

$$X = \{n \in \mathbb{N} \mid 1 \le n \le 1{,}000{,}000\},$$
$$B_3 = \{n \in X \mid n \text{ is divisible by 3}\},$$
$$B_5 = \{n \in X \mid n \text{ is divisible by 5}\},$$
$$B_{13} = \{n \in X \mid n \text{ is divisible by 13}\}.$$

We wish to find $|X - (B_3 \cup B_5 \cup B_{13})|$, which we will do by Corollary 7.6.10. To find $|B_3|$, we observe that every third integer is divisible by 3, so that the number of integers from 1 to 1,000,000 that are divisible by 3 will be the greatest integer less than or equal to $\frac{1,000,000}{3}$. Hence $|B_3| = 333{,}333$. Similarly we can see that $|B_5| = 200{,}000$ and $|B_{13}| = 76{,}923$. Next, an integer will be in $B_3 \cap B_5$ if and only if it is divisible by both 3 and 5, which is equivalent to being divisible by 15. Therefore $|B_3 \cap B_5|$ will be the greatest integer less than or equal to $\frac{1,000,000}{15}$, which is 66,666. Similarly we can see that $|B_3 \cap B_{13}| = 25{,}641$, that $|B_5 \cap B_{13}| = 15{,}384$ and that $|B_3 \cap B_5 \cap B_{13}| = 5{,}128$. By Corollary 7.6.10 we see that

$$\begin{aligned}
&|X - (B_3 \cup B_5 \cup B_{13})| \\
&\quad = |X| - (|B_3| + |B_5| + |B_{13}|) \\
&\qquad + (|B_3 \cap B_5| + |B_3 \cap B_{13}| + |B_5 \cap B_{13}|) - |B_3 \cap B_5 \cap B_{13}| \\
&\quad = 1{,}000{,}000 - (333{,}333 + 200{,}000 + 76{,}923) \\
&\qquad + (66{,}666 + 25{,}641 + 15{,}384) - 5{,}128 \\
&\quad = 492{,}307.
\end{aligned}$$
◊

Another consequence of Theorem 7.6.9 is the following result, the statement of which may seem obvious, but is worth proving, because we will use it in the next section.

Corollary 7.6.12. *Let A be a set, and let $\sim$ be an equivalence relation on A. Suppose that A is finite, and that all the equivalence classes of A with respect to $\sim$ have the same cardinality. If N is the number of equivalence classes, and S is the number of elements in each equivalence class, then $|A| = N \cdot S$.*

Proof. Let $A_1, \ldots, A_N$ be the equivalence classes of A with respect to $\sim$. Then $|A_i| = S$ for all $i \in \{1, \ldots, N\}$. By Theorem 5.3.4 we know that $A_1, \ldots, A_N$ are pairwise disjoint, and that $A = A_1 \cup \cdots \cup A_N$. It now follows from Theorem 7.6.9 (2) that $|A| = |A_1| + \cdots + |A_N| = N \cdot S$.   □

Exercises

Exercise 7.6.1. Murray has 231 compact disks. He wants to lend one disk to his father and one to his mother. How many ways can he do this?

Exercise 7.6.2. Bonesville has 1000 residents. Explain why at least two of them must have the same initials, if they use only their first names and last names, and if they use letters only from the English alphabet. If they use middle initials as well, must it be the case that two residents have the same initials? (Assume that every resident has precisely one middle name.)

Exercise 7.6.3. A cheese factory labels each of its product with a code that has two letters and one single-digit number. The codes must start with either the letter G or B. How many possible codes are there?

Exercise 7.6.4. The first grade and second grade students at the Blabbertown Elementary School decide to send a delegation to the school principal to complain about the school lunches. The delegation is to have either two second graders, or one second grader and one first grader. There are 23 first graders and 27 second graders. How many possible delegations are there?

Exercise 7.6.5. **[Used in Section 7.6.]** The goal of this exercise is to give proofs of Theorem 7.6.3 that do not use the Division Algorithm.

    (1) Prove Theorem 7.6.3 using induction on $|A|$ and Theorem 7.6.7 (2).
    (2) Prove Theorem 7.6.3 using Theorem 7.6.9 (2); note that the proof of that theorem uses induction, and it is therefore not surprising that induction is not needed in this part of the exercise.

Exercise 7.6.6. **[Used in Theorem 7.6.4.]** Prove that the function Φ defined in the proof of Theorem 7.6.4 is bijective.

Exercise 7.6.7. A pair of new parents decide to test 10 different brands of diapers on their newborn baby. They find that 7 brands leak, 5 brands do not stay on properly, and 4 brands both leak and do not stay on properly.

    (1) How many brands have at least one of the problems?
    (2) How many brands have neither problem?

Exercise 7.6.8. A laboratory study of 50 rabbits showed that 29 liked carrots, 18 liked lettuce, 27 liked bratwurst, 9 liked both carrots and lettuce, 16 liked both carrots and bratwurst, 8 liked both lettuce and bratwurst, and 47 liked at least one of the three foods.

    (1) How many rabbits liked none of the three foods?
    (2) How many rabbits liked all three of the foods?

Exercise 7.6.9. A new drug was tested on 40 people to see if it cured any or all of dandruff, ingrown toenails and halitosis. The result of the test showed that 13 people were cured of dandruff, 27 were cured of ingrown toenails, 23 were cured of halitosis, 10 were cured of dandruff and ingrown toenails, 8 were cured of dandruff and halitosis, 16 were cured of ingrown toenails and halitosis, and 7 were cured of all three problems. How many people were not cured of anything?

Exercise 7.6.10. A newspaper report claims that a survey of 100 computer hackers showed that 36 read Geek Magazine, 56 read Nerd Newsletter, 38 read Wonk Weekly, 11 read Geek and Nerd, 10 read Geek and Wonk, 18 read Nerd and Wonk, 5 read all three, and 7 read none. A hacker who read the newspaper article doubted that the purported survey was actually taken. Was she right?

Exercise 7.6.11. Find the number of integers from 1 to 100,000 that are not divisible by any of 2, 5, 11 or 67.

Exercise 7.6.12. **[Used in Theorem 7.7.12.]** Let I be a non-empty set, and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I. Suppose that I is finite, and that A_i is finite for all $i \in I$. Show that Theorem 7.6.9 (3) can be rewritten as

$$\left|\bigcup_{i\in I} A_i\right| = \sum_{r=1}^{|I|}(-1)^{r+1} \sum_{K\in \mathscr{P}_r(I)} \left|\bigcap_{k\in K} A_k\right|.$$

7.7 Counting: Permutations and Combinations

In this section we are concerned with problems involving the choice of some objects out of a larger collection of objects, for example choosing cards out of a deck, or people out of a classroom. In some problems the order of choosing matters, for example in choosing a president, vice-president and secretary for a three-person committee, while in other problems order does not matter, for example choosing a five-card poker hand out of a deck of cards. As in the previous section, the material here is quite standard, but our approach is a bit less so. For a standard discussion of these topics see [Bog90] and [Rob84].

We start with choosing where the order of choosing matters; we have three types of problems of this sort. First, we saw in Example 7.6.2 (2) an example of choosing 2 people out of 6 where order matters. Second, suppose that the same six-person committee decides to select someone to stuff envelopes and someone to make coffee; the same person could fill both of these new positions. How many ways could these two positions be filled? Once again by the Product Rule there are $6 \cdot 6 = 36$ choices for the two positions. Finally, suppose that the members of the committee decide to line up for a group photograph. How many ways can this happen? Here we would have to use the Product Rule repeatedly, which seems correct informally, though it would take proof by induction to be rigorous. There are 6 choices for the person on the left, then 5 choices for the person next to her, then 4 choices after that and so on. All told, there are $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$ possibilities.

The general formulas for solving the above three types of problems are as follows. In two of the following formulas we make use of factorials, which were discussed in Example 6.4.4 (1). That example defined $n!$ for all $n \in \mathbb{N}$, though it did not apply to $n = 0$. For convenience we define $0! = 1$, which might seem strange to the reader who has not encountered it previously, but it works out very nicely, and it allows us to avoid some special cases in the statements of theorems. Recall also the formula $(n+1)! = (n+1)n!$ for all $n \in \mathbb{N}$.

Fact 7.7.1 (Counting Rules—Permutations). *Let $k, n \in \mathbb{N} \cup \{0\}$. Suppose that $0 \le k \le n$.*

1. *The number of ways of choosing k objects out of n objects, where order matters and where each object can be chosen more than once, is n^k.*
2. *The number of ways of choosing k objects out of n objects, where order matters and where each object can be chosen only once, is $\frac{n!}{(n-k)!}$.*
3. *The number of ways of arranging n objects, where order matters, is $n!$.*

Part (2) of Counting Rules—Permutations leads us to the following definition.

Definition 7.7.2. Let $k, n \in \mathbb{N} \cup \{0\}$. Suppose that $0 \leq k \leq n$. The number of **permutations** of n elements taken k at a time, denoted $P(n,k)$, is defined by $P(n,k) = \frac{n!}{(n-k)!}$.   △

There are other common notations for the number of permutations of n elements taken k at a time, for example $_nP_k$.

Example 7.7.3.

(1) The license plates in a certain state have 7 letters. How many different license plates can be made if all letters are allowed? We need to choose 7 letters out of 26, where the order of selection matters and where each letter can be chosen more than once. Because there are 26 letters, by Part (1) of Counting Rules—Permutations we know that there are $26^7 = 8{,}031{,}810{,}176$ possible license plates.

(2) A 10-person board wishes to select an executive committee consisting of a chair, a vice-chair and a secretary; no person may fill more than one of these positions. How many possible executive committees are there? We need to choose 3 people out of 10, where the order of selection matters and where each person can be chosen only once. By Part (2) of Counting Rules—Permutations there are $P(10,3) = \frac{10!}{(10-3)!} = 720$ possibilities.

(3) Four women and three men go to the theater together, and all sit in a row. How many ways can they be seated if the three men want to sit together in the three seats closest to the aisle? Here we need to use the Product Rule from the previous section as well as Part (3) of Counting Rules—Permutations. By the latter, there are 4! ways for the women to be seated, and there are 3! ways for the men to be seated. By the Product Rule, there are a total of $4! \cdot 3! = 24 \cdot 6 = 144$ possible seatings.   ◇

Counting Rules—Permutations are usually justified by repeated application of the Product Rule (via an often unstated use of proof by induction), but, as was the case with "ways that things can happen," the notion of "choosing objects" is not entirely rigorous, and does not directly fit into our framework of sets, functions, relations and the like. We can reformulate the concept of choosing objects, where order matters, in terms of sets of functions. Recall the notation $\mathcal{F}(A,B)$, $I(A,B)$ and $\mathcal{B}(A,B)$ from Section 4.5.

Let $k, n \in \mathbb{N} \cup \{0\}$. Suppose that we want to find the number of ways of choosing k things out of n where order matters, and where each object can be chosen more than once. Let B be a finite set such that $|B| = n$. Then we want to identify an element of B as the first chosen element, and an element of B as the second chosen element and so on ending with an element of B as the k-th chosen element. We could express such a collection of choices as a function $f: \{1, \ldots, k\} \to B$. Hence, the collection of all possible ways of choosing k things out of n where order matters, and where each object can be chosen more than once, would be $\mathcal{F}(\{1, \ldots, k\}, B)$, and the number of ways of choosing is $|\mathcal{F}(\{1, \ldots, k\}, B)|$. Now let A be a finite set such that $|A| = k$. Then $A \sim \{1, \ldots, k\}$ by Corollary 6.6.3, and therefore by Lemma 4.5.3 we see that $\mathcal{F}(\{1, \ldots, k\}, B) \sim \mathcal{F}(A, B)$, which in turn implies that $|\mathcal{F}(\{1, \ldots, k\}, B)| = |\mathcal{F}(A, B)|$. This last number is what we need to compute to solve our original counting problem. Similarly, to find the number of ways of choosing k things out of n where order

matters, and where each object can be chosen only once, we need to find $|I(A,B)|$; to find the number of ways of arranging n things, where order matters, we need to find $|\mathcal{B}(A,B)|$ for the special case where $|A| = |B|$. The values of $|\mathcal{F}(A,B)|$, $|I(A,B)|$ and $|\mathcal{B}(A,B)|$ depend only upon $k = |A|$ and $n = |B|$, and not on the particular choice of the sets A and B, as can be seen by using Lemma 4.5.3 and Exercise 4.5.9. The following theorem gives formulas for $|\mathcal{F}(A,B)|$, $|I(A,B)|$ and $|\mathcal{B}(A,B)|$ in terms of $|A|$ and $|B|$.

Theorem 7.7.4 (**Counting Rules—Permutations**). *Let A and B be sets. Suppose that A and B are finite.*

1. *The set $\mathcal{F}(A,B)$ is finite. If $A = \emptyset$ and $B = \emptyset$, then $|\mathcal{F}(A,B)| = 1$. If $A \neq \emptyset$ or $B \neq \emptyset$, then $|\mathcal{F}(A,B)| = |B|^{|A|}$.*
2. *The set $I(A,B)$ is finite. If $|A| > |B|$, then $|I(A,B)| = 0$. If $|A| \leq |B|$, then $|I(A,B)| = \frac{|B|!}{(|B|-|A|)!}$.*
3. *The set $\mathcal{B}(A,B)$ is finite. If $|A| \neq |B|$, then $|\mathcal{B}(A,B)| = 0$. If $|A| = |B|$, then $|\mathcal{B}(A,B)| = |B|!$.*

Proof.

(1). First, suppose that $A = \emptyset$ and $B = \emptyset$. Then $\mathcal{F}(A,B) = \{\emptyset\}$, as remarked in Example 4.5.2 (1), and hence $\mathcal{F}(A,B)$ is finite, and $|\mathcal{F}(A,B)| = 1$.

Second, $A = \emptyset$ or $B = \emptyset$. If $A = \emptyset$, then once again $\mathcal{F}(A,B) = \{\emptyset\}$, and therefore $\mathcal{F}(A,B)$ is finite, and $|\mathcal{F}(A,B)| = 1 = |B|^0 = |B|^{|A|}$. Now suppose that $A \neq \emptyset$. Then $|A| \geq 1$. For convenience, let $k = |A|$ and $n = |B|$. We proceed by induction on k. Suppose first that $k = 1$, and that $n \in \mathbb{N}$ is any number. It follows from Exercise 4.5.2 that $\mathcal{F}(A,B) \sim B$, and therefore by Corollary 6.6.3 we see that $|\mathcal{F}(A,B)| = |B| = n = n^1 = n^k$.

Now assume that the result holds for some $k \in \mathbb{N}$, and for all $n \in \mathbb{N} \cup \{0\}$. Let $m \in \mathbb{N} \cup \{0\}$. We will show the result for $k+1$ and m. If $m = 0$, then $B = \emptyset$, and because $A \neq \emptyset$, then $\mathcal{F}(A,B) = \emptyset$ by Example 4.5.2 (1), and so $\mathcal{F}(A,B)$ is finite, and $|\mathcal{F}(A,B)| = 0 = m^{k+1}$. Now suppose that $m \geq 1$. Let $a \in A$ and $b \in B$, and let $F_{a,b} = \{f \in \mathcal{F}(A,B) \mid f(a) = b\}$. By Exercise 4.5.10 (1) we see that $F_{a,b} \sim \mathcal{F}(A - \{a\}, B)$, and therefore $|F_{a,b}| = |\mathcal{F}(A - \{a\}, B)|$. Because $|A - \{a\}| = k$, it follows from the inductive hypothesis that $|\mathcal{F}(A - \{a\}, B)| = m^k$. Therefore $|F_{a,b}| = m^k$. Observe that $\mathcal{F}(A,B) = \bigcup_{c \in B} F_{a,c}$ and that the family of sets $\{F_{a,c}\}_{c \in B}$ is pairwise disjoint. It then follows from Theorem 7.6.9 (2) that

$$|\mathcal{F}(A,B)| = \sum_{c \in B} |F_{a,c}| = \sum_{c \in B} m^k = m \cdot m^k = m^{k+1}.$$

(2). Left to the reader in Exercise 7.7.19.

(3). First suppose that $|A| \neq |B|$. Then by Corollary 6.6.3 we see that $A \nsim B$. Hence there is no bijective function $A \to B$, and therefore $\mathcal{B}(A,B) = \emptyset$, which implies that $|\mathcal{B}(A,B)| = 0$. Now suppose that $|A| = |B|$. It follows from Exercise 6.6.4 that $\mathcal{B}(A,B) = I(A,B)$. By Part (2) of this theorem we deduce that $|\mathcal{B}(A,B)| = |I(A,B)| = \frac{|B|}{(|B|-|A|)!} = \frac{|B|}{0!} = |B|!$. $\qquad\square$

We now turn to problems where the order of the chosen objects does not matter. We have two types of problems. First, you choose five cards out of a deck of cards. How many ways can this happen? Second, suppose that you go to a shoe store, and they have six pairs in your size. You might buy anywhere from none of the pairs to all six of them. How many choices can you make? We cannot solve these problems by direct application of the Sum Rule and Product Rule (though it is possible to do so indirectly); instead, we use the following formulas.

Fact 7.7.5 (Counting Rules—Combinations). *Let $n \in \mathbb{N} \cup \{0\}$.*

1. *Let $k \in \mathbb{N} \cup \{0\}$. Suppose that $0 \leq k \leq n$. The number of ways of choosing k objects out of n objects, where order does not matter and where each object can be chosen only once, is $\frac{n!}{k!(n-k)!}$.*
2. *The number of ways of choosing an unspecified number of objects out of n objects, where order does not matter and where each object can be chosen only once, is 2^n.*

The formula given in Part (1) of Counting Rules—Combinations turns out to be useful in many parts of mathematics, not only in simple counting problems.

Definition 7.7.6. Let $n \in \mathbb{N} \cup \{0\}$, and let $k \in \mathbb{Z}$. The number of **combinations** of n elements taken k at a time, denoted $\binom{n}{k}$, is defined by

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!}, & \text{if } 0 \leq k \leq n \\ 0, & \text{if } k < 0 \text{ or } k > n. \end{cases}$$

The number $\binom{n}{k}$ is called the **binomial coefficient** of n and k.   △

Other common notations for $\binom{n}{k}$ are $C(n,k)$ and $_nC_k$. Observe that if $k, n \in \mathbb{N} \cup \{0\}$ and $0 \leq k \leq n$, then $\binom{n}{k} = \frac{P(n,k)}{k!}$. Although the formula for $\binom{n}{k}$ contains a fraction in its definition, it will always be the case that $\binom{n}{k}$ is an integer, because by Theorem 7.7.10 it is equal to the number of elements of a certain set. We will shortly see why the term "binomial coefficient" is used.

Example 7.7.7.

(1) The Portland Society annual meeting has 11 people from Portland, Maine, and 9 people from Portland, Oregon. The meeting needs to elect a five-person steering committee. One faction at the meeting wants to allow any five people to be elected, while the other faction wants to have either 3 Mainers and 2 Oregonians, or vice versa. How many possible committees could be elected by each of these methods?

For the first method, because there are a total of 20 people at the meeting, and because the order of the members of the committee does not matter, by Part (1) of the Combinations Rule there are $\binom{20}{5} = 15,504$ possible committees.

The second method has two exclusive cases, and by the Sum Rule we will add the number of possibilities for the two cases. First, suppose that the committee has 3 Mainers and 2 Oregonians. Then there are $\binom{11}{3}$ possible choices of the Maine members of the committee, and for each of these choices, there are $\binom{9}{2}$ possible choices

for the Oregon members. By the Product Rule there are $\binom{11}{3} \cdot \binom{9}{2}$ possible steering committees with 3 Mainers and 2 Oregonians. Similarly, there are $\binom{11}{2} \cdot \binom{9}{3}$ possible steering committees with 2 Mainers and 3 Oregonians. Combining the two cases implies that there are $\binom{11}{3} \cdot \binom{9}{2} + \binom{11}{2} \cdot \binom{9}{3} = 165 \cdot 36 + 55 \cdot 84 = 10,560$ possible committees.

(2) You pass by a pizza shop that advertises that it has over 1000 varieties of pizza, and you want to determine whether this is false advertising. All pizzas in this shop have cheese, and they may have any combination of up to 10 toppings, for example pepperoni, broccoli, mushrooms, etc. Any type of pizza corresponds to a choice of toppings, which is a choice of anywhere from 0 to 10 of the 10 toppings (choosing 0 toppings corresponds to a plain cheese pizza). By Part (2) of the Combinations Rule we see that the power set of a 10-element set has $2^{10} = 1024$ elements. Therefore there are indeed over 1000 varieties of pizza (that some of them might be unpalatable is another matter).

(3) An important use of counting techniques is to compute probabilities. Although the computation of probabilities can be quite complicated, and is the subject of its own branch of mathematics (see [Pit93] or [Ros10] for introductory probability), it is possible to compute probabilities in some elementary cases by using binomial coefficients. When a number of distinct events can occur with equal likelihood, then the probability of an event is the ratio of the number of ways the event can occur to the number of ways all possibilities can occur. For example, we will calculate the probability for a flush in five-card poker, which means that a player draws five cards from a deck of cards, and all the cards turn out to be from the same suit. Because the order of cards does not matter, the total number of different five-card hands is $\binom{52}{5} = 2,598,960$. To compute the number of possible flushes, we observe that there are four suits in a deck of cards, and for each suit we need to choose 5 cards out of the 13 cards in the suit. Using the Product Rule, the number of flushes is therefore $4 \cdot \binom{13}{5} = 5148$. The probability of a flush is therefore $\frac{5148}{2,598,960} \approx 0.00198$. The probabilities of other poker hands can be computed similarly.

(4) Probability calculations sometimes yield rather counterintuitive results; we discuss here a well-known example of such a result. Suppose that we choose n random people, and then ask them their birthdays. What is the probability that at least two of the people have the same birthday? The probability depends upon the number n, and clearly the probability is larger for larger values of n. To guarantee that the probability is 1, which means that the desired outcome will definitely happen, we would need to have $n \geq 366$ (for simplicity, we will ignore leap years). What is the smallest value of n such that the probability of at least two people having the same birthday is 0.5, which means that it is a one in two likelihood?

Suppose that $1 \leq n \leq 365$. We then think of having n people, and we assign to each of these people a birthday. Such an assignment is the same as choosing n numbers from the set $\{1, \ldots, 365\}$, where order matters and where each number can be chosen more than once. We want to count how many such choices there are, and then out of those we want to see how many choices have at least two chosen numbers the same. By Part (1) of Counting Rules—Permutations there are 365^n ways of assigning birthdays to n people. Of these 365^n possibilities, we know by Part (2)

of Counting Rules—Permutations that there are $\frac{365!}{(365-n)!}$ possible way of assigning birthdays to the n people such that no two people have the same birthday. It follows that there are $365^n - \frac{365!}{(365-n)!}$ possible ways of assigning birthdays to the n people such that at least two people have the same birthday. Hence, the probability of having at least two people out of n people with the same birthday, denoted P_n, is

$$P_n = \frac{365^n - \frac{365!}{(365-n)!}}{365^n} = 1 - \frac{365!}{365^n(365-n)!}.$$

We can compute these probabilities using a calculator, obtaining for example that $P_2 \approx 0.0027$ and $P_3 \approx 0.0082$. There is no direct way of solving the inequality $P_n \geq 0.5$, but we can solve the problem by brute force by computing P_4, P_5, and so on until we first find a value that is greater than or equal to 0.5. Such a calculation, which is easy with a computer, yields $P_{22} = 0.476$ and $P_{23} \approx 0.507$, which says that if 23 people are randomly chosen, there is roughly a 50% chance that two people will have the same birthday, and that 23 is the minimum number of people needed. The number 23 is somewhat counterintuitive, given how much smaller it is than 365.   ◇

To give a rigorous treatment of Counting Rules—Combinations, we look at the number of subsets of a given finite set, either subsets of a fixed size or of arbitrary size. We start with the following definition.

Definition 7.7.8. Let A be a set, and let $k \in \mathbb{Z}$. Let $\mathcal{P}_k(A)$ denote the family of all subsets of A with k elements, that is, the family

$$\mathcal{P}_k(A) = \{S \in \mathcal{P}(A) \mid |S| = k\}.$$ △

Example 7.7.9. Let $A = \{a,b,c\}$. We saw in Example 3.2.9 (2) that the subsets of A are $\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{a,b\}$, $\{a,c\}$, $\{b,c\}$ and $\{a,b,c\}$. Then $|\mathcal{P}_0(A)| = 1$, and $|\mathcal{P}_1(A)| = 3$, and $|\mathcal{P}_2(A)| = 3$, and $|\mathcal{P}_3(A)| = 1$, and $|\mathcal{P}_k(A)| = 0$ if $k < 0$ or $k > 3$.   ◇

The first part of the following theorem gives a formula for $|\mathcal{P}_k(A)|$ when A is finite, and the second part of the theorem gives a formula for $|\mathcal{P}(A)|$ when A is finite, formalizing a fact that was stated without proof in Section 3.2. The proof of the second part of the theorem is much shorter than the first, because we can make use of something we proved about sets of functions in Section 4.5; the intuitive idea of the proof is that each subset of a given set can be specified by assigning each element of the set either 1 or 0, depending upon whether or not it is in the subset.

Theorem 7.7.10 (Counting Rules—Combinations). *Let A be a set. Suppose that A is finite.*

1. *Let $k \in \mathbb{Z}$. The set $\mathcal{P}_k(A)$ is finite. If $k < 0$ or $k > |A|$, then $|\mathcal{P}_k(A)| = 0$. If $0 \leq k \leq |A|$, then*

$$|\mathcal{P}_k(A)| = \frac{|A|!}{k!(|A|-k)!}.$$

2. *The set $\mathcal{P}(A)$ is finite, and $|\mathcal{P}(A)| = 2^{|A|}$.*

Proof. We prove the two parts of the theorem in reverse order.

(2). We saw in Theorem 4.5.4 that $\mathcal{P}(A) \sim \mathcal{F}(A, \{0,1\})$, and it follows from Theorem 7.7.4 (1) that $\mathcal{P}(A)$ is finite. By Corollary 6.6.3 we see that $|\mathcal{P}(A)| = |\mathcal{F}(A, \{0,1\})|$, and Theorem 7.7.4 (1) then implies that $|\mathcal{F}(A, \{0,1\})| = 2^{|A|}$.

(1). Regardless of the value of k, observe that $\mathcal{P}_k(A) \subseteq \mathcal{P}(A)$, and it then follows from Part (2) of this theorem and Theorem 6.6.5 (1) that $\mathcal{P}_k(A)$ is finite. To compute $|\mathcal{P}_k(A)|$, we examine a number of cases.

First, suppose that $A = \emptyset$. Then $\mathcal{P}_0(A) = \{\emptyset\}$ and $\mathcal{P}_k(A) = \emptyset$ when $k \neq 0$. Hence $|\mathcal{P}_0(A)| = 1 = \frac{0!}{0!0!} = \frac{|A|!}{0!(|A|-0)!}$, and $|\mathcal{P}_k(A)| = 0$ when $k \neq 0$. Now assume that $A \neq \emptyset$.

If $k < 0$, then it is clear that there are no subsets of A of order k, and hence $\mathcal{P}_k(A) = \emptyset$. Therefore $|\mathcal{P}_k(A)| = 0$. If $k > |A|$, then it follows from Theorem 6.6.5 (3) that $\mathcal{P}_k(A) = \emptyset$, and hence $|\mathcal{P}_k(A)| = 0$. If $k = 0$, then $\mathcal{P}_k(A) = \{\emptyset\}$, and so $|\mathcal{P}_k(A)| = 1 = \frac{|A|!}{0!(|A|-0)!}$. Now assume that $1 \leq k \leq |A|$.

Let E be a set with k elements. Let $\sim$ be the relation on $I(E,A)$ defined by $f \sim g$ if and only if $f(E) = g(E)$, for all $f, g \in I(E,A)$. It is straightforward to verify that $\sim$ is an equivalence relation; the details are left to the reader. We will prove the following two facts: (1) Each equivalence class of $I(E,A)$ with respect to $\sim$ has $|E|!$ elements; and (2) the number of equivalence classes equals $|\mathcal{P}_k(A)|$. Once we prove these two claims, it will then follow from Corollary 7.6.12 that $|I(E,A)| = |\mathcal{P}_k(A)||E|!$. By Theorem 7.7.4 (2) we know that $|I(E,A)| = \frac{|A|!}{(|A|-|E|)!}$, and it will follow that $|\mathcal{P}_k(A)| = \frac{|A|!}{|E|!(|A|-|E|)!} = \frac{|A|!}{k!(|A|-k)!}$.

For each $h \in I(E,A)$, let $\hat{h} \colon E \to h(E)$ be defined by $\hat{h}(x) = h(x)$ for all $x \in E$; because h is injective, then $\hat{h}$ is bijective. Let $f \in I(E,A)$. Let $\Psi \colon [f] \to \mathcal{B}(f(E), f(E))$ be defined by $\Psi(g) = \hat{g} \circ \hat{f}^{-1}$ for all $g \in [f]$. To see that the definition of Ψ makes sense, let $g \in [f]$. Because $g(E) = f(E)$, then $\Psi(g)$ is indeed a function $f(E) \to f(E)$. It follows from Exercise 4.4.13 (3) and Lemma 4.4.4 (3) that $g \circ \hat{f}^{-1}$ is bijective. Hence $\Psi(g) \in \mathcal{B}(f(E), f(E))$, and we deduce that Ψ is well-defined. It is left to the reader in Exercise 7.7.20 to show that the function Ψ is bijective. It follows that $[f] \sim \mathcal{B}(f(E), f(E))$, and therefore by Corollary 6.6.3 we then deduce that $|[f]| = |\mathcal{B}(f(E), f(E))|$. By Exercise 6.5.4 we see that $|f(E)| = |E|$, and hence by Theorem 7.7.4 (3) we know that $|[f]| = |\mathcal{B}(f(E), f(E))| = |E|!$, which proves Fact (1).

Let $I(E,A)/\sim$ denote the set of equivalence classes of $I(E,A)$ with respect to $\sim$, as discussed in Section 5.3. Let $\Phi \colon I(E,A)/\sim \to \mathcal{P}_k(A)$ be defined by $\Phi([f]) = f(E)$ for all $f \in I(E,A)$. We leave it to the reader in Exercise 7.7.20 to show that the function Φ is well-defined and bijective, which implies Fact (2). $\qquad \square$

The reader might find the proof of Theorem 7.7.10 unsatisfying due to its reliance on some heavy machinery involving sets of functions. Alternative proofs of the two parts of the theorem, using proof by induction (and for the first part of the theorem some of the properties of binomial coefficients given below), but without sets of functions and equivalence relations, are left to the reader in Exercise 7.7.22 and Exercise 7.7.23.

Some texts use the notation 2^A to denote $\mathcal{P}(A)$, whether or not A is finite. This alternative notation might seem strange, but it does allow for the nice formula $|2^A| = 2^{|A|}$ when A is a finite set.

We have seen a number of problems involving counting in Section 7.6 and the present section. Given that most of these problems were not very tricky, the reader might have been led to think, mistakenly, that counting problems can usually be solved in a simple intuitive fashion, and that we have made a big deal out of nothing. As evidence that counting problems are not all straightforward, we present one final counting problem, known as the "hat check problem," which is somewhat trickier than the problems we have seen until now, and which makes use of a number of the ideas we have learned.

Example 7.7.11. Suppose that n people check their hats at a theater. The hat check attendant accidentally loses all the stubs for the hats, and returns the hats at random. What is the probability that no one gets her own hat back? As discussed in Example 7.7.7 (3), this probability is the ratio of the number of ways that the hats can be returned so that no one gets her own hat back, denoted $S(n)$, to the total number of ways that the hats can be randomly returned, denoted $T(n)$. It is easy to compute $T(n)$, because this is just the number of ways of arranging n things, where order matters. Therefore $T(n) = n!$ by Theorem 7.7.4 (3).

Computing $S(n)$ is a bit trickier; it is the number of ways of arranging n things, where order matters, and where nothing stays where it started. Such a rearrangement is called a derangement in the combinatorics literature. We can reformulate our problem in terms of functions, as follows. Let A be a set with n elements, where $n \in \mathbb{N}$. Then each derangement of n objects corresponds to a bijective function $f: A \to A$ such that $f(a) \neq a$ for all $a \in A$. To use standard terminology, a fixed point of a function $f: A \to A$ is an element $x \in A$ such that $f(x) = x$. We are therefore interested in counting the number of bijective functions $A \to A$ with no fixed points, which we do in Theorem 7.7.12 following this example. The hard work for the hat check problem is in the proof of the theorem. From that theorem we see that

$$S(n) = n! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^n \frac{1}{n!} \right).$$

It follows that the probability that no one gets her own hat back is

$$\frac{S(n)}{T(n)} = \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^n \frac{1}{n!}.$$

For example, with six people the probability is approximately 0.36667. It is interesting to observe that as $n \to \infty$, the probability goes to $\frac{1}{e}$, as can be seen using the power series for e^x (consult any standard calculus text for this power series). $\diamond$

Theorem 7.7.12. *Let A be a set. Suppose that A is finite and non-empty. Let $F = \{f \in \mathcal{B}(A,A) \mid f(a) \neq a \text{ for all } a \in A\}$. Then*

$$|F| = |A|! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^{|A|} \frac{1}{|A|!} \right).$$

Proof. Let $a \in A$, and let $G_a = \{f \in \mathcal{B}(A,A) \mid f(a) = a\}$. Observe that if $f \in G_a$, it might also be the case that $f(b) = b$ for some $b \in A$ such that $b \neq a$. Let $B \in \mathcal{P}_p(A)$, for some $p \in \{1, \ldots, n\}$. Then

$$\bigcap_{b \in B} G_b = \{f \in \mathcal{B}(A,A) \mid f(b) = b \text{ for all } b \in B\}.$$

It can be verified, similarly to Exercise 4.5.10 (3), that there is a bijective function from $\bigcap_{b \in B} G_b$ to $\mathcal{B}(A - B, A - B)$. Using Theorem 7.7.4 (3) and Theorem 6.6.5 (2) we deduce that $|\bigcap_{b \in B} G_b| = |A - B|! = (|A| - |B|)! = (|A| - p)!$.

Observe that $F = \mathcal{B}(A,A) - \bigcup_{c \in A} G_c$. By Theorem 7.7.4 (3) we know that $|\mathcal{B}(A,A)| = |A|!$. Using Theorem 6.6.5 (2), Exercise 7.6.12 and Theorem 7.7.10 (1) we then compute

$$|F| = \left| \mathcal{B}(A,A) - \bigcup_{c \in A} G_c \right| = |\mathcal{B}(A,A)| - \left| \bigcup_{c \in A} G_c \right|$$

$$= |\mathcal{B}(A,A)| + \sum_{r=1}^{|A|} (-1)^r \sum_{K \in \mathcal{P}_r(A)} \left| \bigcap_{k \in K} G_k \right|$$

$$= |A|! + \sum_{r=1}^{|A|} (-1)^r \sum_{K \in \mathcal{P}_r(A)} (|A| - r)!$$

$$= |A|! + \sum_{r=1}^{|A|} (-1)^r (|A| - r)! \sum_{K \in \mathcal{P}_r(A)} 1$$

$$= |A|! + \sum_{r=1}^{|A|} (-1)^r (|A| - r)! |\mathcal{P}_r(A)|$$

$$= |A|! + \sum_{r=1}^{|A|} (-1)^r (|A| - r)! \frac{|A|!}{r!(|A| - r)!}$$

$$= |A|! + \sum_{r=1}^{|A|} (-1)^r \frac{|A|!}{r!}$$

$$= |A|! - \frac{|A|!}{1!} + \frac{|A|!}{2!} - \cdots + (-1)^{|A|} \frac{|A|!}{|A|!}$$

$$= |A|! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^{|A|} \frac{1}{|A|!} \right). \qquad \square$$

Having defined the binomial coefficients in Definition 7.7.6, and having seen a few applications of them, we conclude this section by proving a few basic properties of these numbers. Some additional properties of the binomial coefficients can be found in the exercises for this section, and more properties than you ever wanted to know about the binomial coefficients (as well as some very clever arguments) are found in [GKP94, Chapter 5].

Theorem 7.7.13. *Let $n \in \mathbb{N} \cup \{0\}$, and let $k \in \mathbb{Z}$.*

1. *$\binom{n}{0} = 1$, and $\binom{n}{n} = 1$, and $\binom{n}{1} = n$, and $\binom{n}{n-1} = n$.*
2. *$\binom{n}{n-k} = \binom{n}{k}$.*

3. $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$.

Proof. We will prove Part (3), leaving the rest to the reader in Exercise 7.7.14.

(3). There are a number of cases, depending upon the value of k. If $k < 0$, then $\binom{n-1}{k} + \binom{n-1}{k-1} = 0 + 0 = 0 = \binom{n}{k}$. If $k = 0$, then by Part (1) of this proposition we see that $\binom{n-1}{k} + \binom{n-1}{k-1} = 1 + 0 = 1 = \binom{n}{k}$. Similar calculations show that the equation holds if $k = n$ or $k > n$. If $1 \le k \le n - 1$, then

$$
\begin{aligned}
\binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} \\
&= \frac{(n-1)!}{k(k-1)!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)(n-k-1)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k-1)!} \left\{ \frac{1}{k} + \frac{1}{n-k} \right\} \\
&= \frac{(n-1)!}{(k-1)!(n-k-1)!} \frac{n}{k(n-k)} \\
&= \frac{n!}{k!(n-k)!} = \binom{n}{k}. \qquad \square
\end{aligned}
$$

Part (3) of the above proposition leads to a convenient way of displaying and computing the binomial coefficients. Consider the following arrangement of the binomial coefficients.

$$
\begin{array}{ccccccccc}
& & & & \binom{0}{0} & & & & \\
& & & \binom{1}{0} & & \binom{1}{1} & & & \\
& & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
& \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}
$$

$$\vdots$$

Replacing the binomial coefficients with their numerical values, we obtain the following triangle.

$$
\begin{array}{ccccccccc}
& & & & 1 & & & & \\
& & & 1 & & 1 & & & \\
& & 1 & & 2 & & 1 & & \\
& 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
1 & 5 & & 10 & & 10 & & 5 & 1
\end{array}
$$

$$\vdots$$

Observe that each entry in the triangle can be computed by adding the two entries above it in the previous row, which is equivalent to Theorem 7.7.13 (3). This fact allows for easy computation of binomial coefficients with small numbers. The left-right symmetry of the triangle is equivalent to Theorem 7.7.13 (2). This triangle of binomial coefficients is called Pascal's triangle, though it was known in China earlier than Pascal's time; see [Ifr85, p. 396] for the history of Pascal's triangle, and see [HHP97, Chapter 6] for an interesting mathematical discussion of Pascal's triangle and its extensions.

The term "binomial coefficient" comes from the following very important theorem.

Theorem 7.7.14 (Binomial Theorem). *Let $n \in \mathbb{N}$, and let $x, y \in \mathbb{R}$. Then*

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n$$

$$= \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

Proof. The proof is by induction on n. When $n = 1$, then

$$(x+y)^1 = x + y = \binom{1}{0}x^1 y^0 + \binom{1}{1}x^0 y^1 = \sum_{i=0}^{1} \binom{1}{i} x^{1-i} y^i.$$

Now suppose that the result is true for some $n \in \mathbb{N}$. Making use of Theorem 7.7.13 (1) (3) we compute

$$(x+y)^{n+1} = (x+y)(x+y)^n = (x+y)\sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

$$= \sum_{i=0}^{n} \binom{n}{i} x^{n-i+1} y^i + \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^{i+1}$$

$$= \sum_{i=0}^{n} \binom{n}{i} x^{(n+1)-i} y^i + \sum_{i=1}^{n+1} \binom{n}{i-1} x^{n-(i-1)} y^{(i-1)+1}$$

$$= \binom{n}{0}x^{n+1} + \sum_{i=1}^{n} \left[\binom{n}{i} + \binom{n}{i-1} \right] x^{(n+1)-i} y^i + \binom{n}{n}y^{n+1}$$

$$= \binom{n+1}{0}x^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} x^{(n+1)-i} y^i + \binom{n+1}{n+1}y^{n+1}$$

$$= \sum_{i=0}^{n+1} \binom{n+1}{i} x^{(n+1)-i} y^i. \qquad \square$$

Combining the Binomial Theorem with Pascal's triangle, we see, for example, that $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$.

There are various formulas for sums of binomial coefficients, the simplest of which is given in the following proposition. Other sums may be found in Exercise 7.7.16 and Exercise 7.7.17, and even more complicated ones in [GKP94, Chapter 5]. We give three proofs of this proposition, in order of increasing pleasantness, to demonstrate a variety of the techniques we have learned.

Theorem 7.7.15. *Let $n \in \mathbb{N} \cup \{0\}$. Then*

$$\sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Proof. First Proof: This proof is by induction on n. If $n = 0$ then $\binom{0}{0} = 1 = 2^0$, and if $n = 1$ then $\binom{1}{0} + \binom{1}{1} = 1 + 1 = 2 = 2^1$. Now suppose that the result holds for $n \in \mathbb{N}$. We then use Theorem 7.7.13 (3) and the inductive hypothesis to compute

$$\sum_{k=0}^{n+1} \binom{n+1}{k} = \sum_{k=0}^{n+1} \left\{ \binom{n}{k} + \binom{n}{k-1} \right\} = \sum_{k=0}^{n+1} \binom{n}{k} + \sum_{k=0}^{n+1} \binom{n}{k-1}$$

$$= \sum_{k=0}^{n} \binom{n}{k} + \binom{n}{n+1} + \binom{n}{-1} + \sum_{k=1}^{n+1} \binom{n}{k-1}$$

$$= \sum_{k=0}^{n} \binom{n}{k} + \binom{n}{n+1} + \binom{n}{-1} + \sum_{k=0}^{n} \binom{n}{k}$$

$$= 2^n + 0 + 0 + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

Second Proof: This proof uses Theorem 7.7.10, which interprets the binomial coefficient as the numbers of subsets of appropriate size of a given set. Let A be a set with n elements. Then

$$\mathcal{P}(A) = \mathcal{P}_0(A) \cup \mathcal{P}_1(A) \cup \cdots \cup \mathcal{P}_n(A).$$

Moreover, the family of sets $\{\mathcal{P}_i(A)\}_{i=0}^{n}$ is pairwise disjoint. Using Theorem 7.6.9 (2) we see that

$$|\mathcal{P}(A)| = |\mathcal{P}_0(A)| + |\mathcal{P}_1(A)| + \cdots + |\mathcal{P}_n(A)|,$$

and therefore by Theorem 7.7.10 we deduce that

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}.$$

Third Proof: This proof makes use of the Binomial Theorem (Theorem 7.7.14). Because that theorem holds for all values of x and y, it holds in particular when $x = 1$ and $y = 1$. Substituting these values into the Binomial Theorem yields

$$2^n = (1+1)^n = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} 1^i = \sum_{i=0}^{n} \binom{n}{i}. \qquad \square$$

Exercises

Exercise 7.7.1. The alphabet on planet Blort has 11 letters, which are divided into two types; there are 8 letters of type one, and 3 letters of type two.

(1) How many different words can be made with these letters?
(2) How many different words can be made with these letters if the words all have to start with a letter of type one?
(3) How many different words can be made with these letters if the words are required to have all letters of the same type?

Exercise 7.7.2. The license plates in a certain state have three letters followed by three numbers.

(1) How many different license plates can be made?
(2) How many different license plates can be made if the license plates all have to start with one of PU, FE or GA?

Exercise 7.7.3. A group of eight brothers and sisters line up to get food at a family gathering.

(1) How many different ways can they line up?
(2) How many different ways can they line up if the oldest is at the head of the line and the youngest is at the end of the line?
(3) How many different ways can they line up if the oldest and the youngest always stand together, with the oldest always ahead of the youngest?

Exercise 7.7.4. You have five books in Esperanto and five books in Ugaritic, which you want to line up on a shelf.

(1) How many different ways can you line the books up?
(2) How many different ways can you line the books up if you put all the Esperanto books on the left, and all the Ugaritic books on the right?
(3) How many different ways can you line the books up if you alternate Esperanto and Ugaritic books?

Exercise 7.7.5. A horse race has eight horses, and the first three places are announced. Assume there are no ties.

(1) How many possible outcomes are there for a single running of the race?
(2) How many possible outcomes are there for two runnings of the race?

Exercise 7.7.6. We want to select five distinct letters out of the word MUSHBRAIN and write them in a row.

(1) How many different ways can this selection be done?
(2) How many different ways can this selection be done if we write three consonants followed by two vowels?
(3) How many different ways can this selection be done if we write four consonants followed by one vowel, or five consonants and no vowels?

Exercise 7.7.7. A company that solicits magazine subscriptions by phone sells 13 different magazines. Given that any person they call might subscribe to anything from no magazines to all 13 of them, how many different possible responses could the company receive?

Exercise 7.7.8. Susan has 15 shirts, from which she might or might not take any on an upcoming trip.

- **(1)** How many possible collections of shirts might she take?
- **(2)** How many possible collections of shirts might she take if she is definitely going to take at least two shirts?

Exercise 7.7.9. Let $X = \{1,2,3,4\}$. Explicitly list the elements of each of the sets $\mathcal{P}_0(X)$, $\mathcal{P}_1(X)$, $\mathcal{P}_2(X)$, $\mathcal{P}_3(X)$ and $\mathcal{P}_4(X)$.

Exercise 7.7.10. Xavier has six pairs of cotton pants and four pairs of wool pants. He needs to take five pairs of pants on a trip.

- **(1)** How many possible choices can Xavier make?
- **(2)** How many possible choices can Xavier make if he is to take three pairs of cotton pants and two pairs of wool pants?

Exercise 7.7.11. The Al Jolson fan club of Flugletown has eight men and five women, including Mr. and Ms. Atiyah-Singer. The club want to pick a steering committee.

- **(1)** How many possible five-person committees can be formed?
- **(2)** How many possible four- or five-person committees can be formed?
- **(3)** How many possible four-person committees can be formed if there must be two men and two women on the committee?
- **(4)** How many possible four-person committees can be formed if there must be two men and two women on the committee, and not both Mr. and Ms. Atiyah-Singer are allowed to be on the committee at the same time?

Exercise 7.7.12. You choose three cards from a deck of cards. Find the probability of drawing each of the following options.

- **(1)** Three red cards.
- **(2)** A face card.
- **(3)** Three Aces.
- **(4)** Two Queens and one Jack.
- **(5)** Three cards of the same suit.
- **(6)** Three Aces or Three Kings.

Exercise 7.7.13. Expand the following expressions.

- **(1)** $(a+3b)^6$.
- **(2)** $(2x + \frac{1}{x})^7$.

Exercise 7.7.14. **[Used in Proposition 7.7.13.]** Prove Theorem 7.7.13 (1) (2).

Exercise 7.7.15. Let $n,s \in \mathbb{N} \cup \{0\}$, and let $k,s \in \mathbb{Z}$. Prove that the following formulas hold.

(1) $\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$, when $k \neq 0$.

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

(2) $\binom{n}{s}\binom{s}{k} = \binom{n}{k}\binom{n-k}{s-k}$, when $k \leq n$.

(4) $\binom{n+2}{3} - \binom{n}{3} = n^2$.

Exercise 7.7.16. [Used in Section 7.7.] Let $n, s \in \mathbb{N} \cup \{0\}$. Prove that the following formulas hold.

(1) $\sum_{k=0}^{n} \binom{s+k}{k} = \binom{s+n+1}{n}$.

(2) $\sum_{k=0}^{n} \binom{k}{s} = \binom{n+1}{s+1}$.

Exercise 7.7.17. [Used in Section 7.7.] Let $n \in \mathbb{N}$.

(1) Prove that $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$.

(2) Prove that

$$\sum_{\substack{k \text{ even} \\ 0 \leq k \leq n}} \binom{n}{k} = \sum_{\substack{k \text{ odd} \\ 0 \leq k \leq n}} \binom{n}{k}.$$

(3) Let A be a non-empty set. Suppose that A is finite. Let $\mathcal{P}_E(A)$, respectively $\mathcal{P}_O(A)$, denote the family of all subsets of A with an even, respectively odd, number of elements. Prove that $|\mathcal{P}_E(A)| = |\mathcal{P}_O(A)|$.

Exercise 7.7.18. Certain diagonals in Pascal's triangle are indicated in Figure 7.7.1. Make a conjecture for a formula for the sums of the entries along these diagonals; state your formula in terms of binomial coefficients. Prove your conjecture. Recall the Fibonacci numbers discussed in Section 6.4.

Fig. 7.7.1.

Exercise 7.7.19. [Used in Theorem 7.7.4.] Prove Theorem 7.7.4 (2).

Exercise 7.7.20. [Used in Theorem 7.7.10.] Let Ψ and Φ be the functions defined in the proof of Theorem 7.7.10. Prove that function Φ is well-defined, and that both Φ and Ψ are bijective.
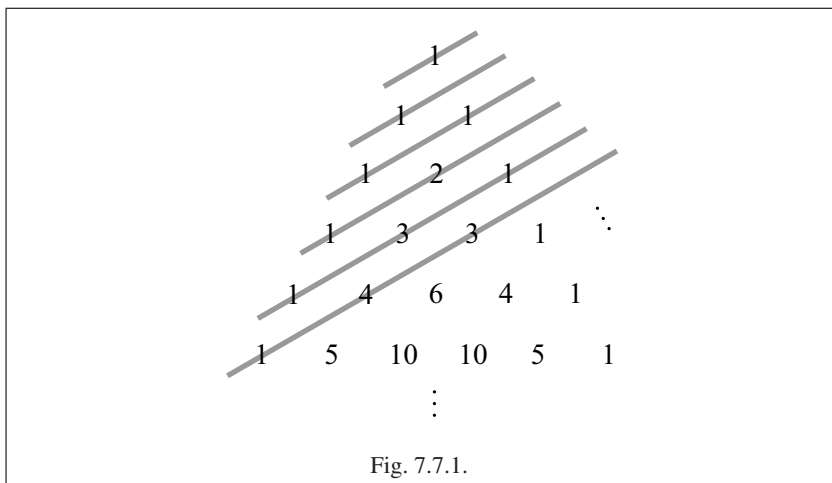
Exercise 7.7.21. Let A and B be sets. Prove that $A \sim B$ implies that $\mathcal{P}_k(A) \sim \mathcal{P}_k(B)$, for all $k \in \mathbb{N} \cup \{0\}$. Observe that Theorem 7.7.10 cannot be used here, because A and B are not required to be finite.

Exercise 7.7.22. **[Used in Section 7.7.]** Prove Theorem 7.7.10 (1) directly by induction on $|A|$, without using sets of functions. Only the case $0 \le k \le |A|$ needs to be treated. Use Exercise 7.7.21.

Exercise 7.7.23. **[Used in Section 7.7.]** Prove Theorem 7.7.10 (2) directly by induction on $|A|$, without making use of Theorem 4.5.4.

Exercise 7.7.24. Let A and B be sets, and let $f \colon A \to B$ be a function. Suppose that f that has a left inverse but not a right inverse. Suppose that A and $B - f(A)$ are both finite sets. How many left inverse does f have? Prove your answer.

7.8 Limits of Sequences

In the previous sections of this chapter we saw various topics that had an algebraic flavor. In the present section, by contrast, where we discuss limits of sequences, the material is from analysis. See any introductory real analysis text, for example [Blo11, Chapter 8], for a detailed treatment of limits of sequences.

  The proofs in this section, while not longer than those in the previous sections of this chapter, are very different from what we have seen so far, and are often considered a bit trickier upon first encounter. The source of this trickiness is the double quantifier in the definition of limits of sequences, as we will soon see. Careful attention to quantifiers is important in the formulation of all proofs, and is even more important here.

  Before proceeding to the topic of this section, we note that in addition to all the basic algebraic properties of the real numbers that we have used throughout this text, we need for the present section two additional properties, which are stated as Theorem A.2 and Theorem A.3 in the Appendix. The reader, who should review these two theorems before proceeding, is most likely familiar with these facts informally, but we need to be quite explicit in their use if we want rigorous proofs about sequences.

  In our discussion of limits of sequences we will use the following phraseology. We will regularly need to select an arbitrary positive real number, often denoted ε. Formally, we should write "let $\varepsilon \in \mathbb{R}$, and suppose that $\varepsilon > 0$." However, in order to avoid that cumbersome formulation, we will stick with the standard, albeit not quite precise, phrase "let $\varepsilon > 0$."

  We have already seen sequences in a few places in this text. In Example 4.5.2 (4) we defined a sequence of real numbers formally as a function $f \colon \mathbb{N} \to \mathbb{R}$. Informally, we write a sequence as $c_1, c_2, c_3, \ldots$, where we could convert this informal notation to the formal approach by defining a function $g \colon \mathbb{N} \to \mathbb{R}$ by letting $g(1) = c_1$, and $g(2) = c_2$, and so on. For convenience, we summarize this definition of sequences as follows.

Definition 7.8.1. A **sequence** of real numbers (also called a **sequence in** $\mathbb{R}$) is a function $f \colon \mathbb{N} \to \mathbb{R}$. If $f \colon \mathbb{N} \to \mathbb{R}$ is a sequence, and if $c_i = f(i)$ for all $i \in \mathbb{N}$, then we will write either $c_1, c_2, c_3, \ldots$ or $\{c_n\}_{n=1}^{\infty}$ to denote the sequence. Each number c_n, for $n \in \mathbb{N}$, is called a **term** of the sequence $\{c_n\}_{n=1}^{\infty}$. $\triangle$

It is important to distinguish between the concept of a "sequence" and the related, but not identical, concept of a "series." In non-mathematical usage these two words are often used interchangeably, but not in mathematical terminology. Intuitively, a sequence of real numbers is a collection of numbers of which there is a first, a second, a third and so on, with one real number for each element of $\mathbb{N}$. For example,

$$\frac{1}{1^2}, \frac{1}{2^2}, \frac{1}{3^2}, \frac{1}{4^2}, \ldots$$

is a sequence. By contrast, a series is a "sum" of the terms in a sequence, for example

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots.$$

The word "sum" is in quotes because, although we can write such an infinite sum, it is not clear whether such a sum actually adds up to a finite amount (this particular example does). We will not discuss series here, though we note that they are a very important topic in real analysis and in applications of mathematics; see [Blo11, Chapter 9] for basic information about series.

In addition to seeing the formal definition of sequences in Section 4.5, we also saw the use of Definition by Recursion to define sequences in Section 6.4. For example, we used Definition by Recursion to define the Fibonacci sequence, which starts

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 \ldots.$$

What concerns us at present is not how sequences are defined, but what happens to the terms of a sequence $\{c_n\}_{n=1}^{\infty}$ as n gets larger and larger. Rather than repeatedly saying the cumbersome phrase "n gets larger and larger," we will use the slightly shorter, and very standard, phrase "n goes to ∞," which we write with the notation "$n \to \infty$." Keep in mind that there is no real number "∞," and that this symbol is simply shorthand for allowing us to take larger and larger numbers without bound.

For example, if we look at the terms of the Fibonacci sequence, they clearly grow without bound as n goes to ∞. On the other hand, in Exercise 6.4.14 we looked at the sequence of the successive ratios of Fibonacci numbers, that is, the numbers

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \ldots.$$

In that exercise, it was noted that as n goes to ∞, the terms in this sequence get closer and closer to the number $1.618\ldots$. The reader is urged to check the plausibility of this claim by calculating the values of the first few terms of this sequence in decimals; a proof of the claim, which is not important to us here, is discussed in Exercise 6.4.14.

What concerns us in this section is the general notion of the terms of a sequence getting closer and closer to a number as n goes to ∞. Given a sequence of real numbers $\{c_n\}_{n=1}^{\infty}$, we want to verify whether or not there is a real number L such that the

value of c_n gets closer and closer to L as the value of n goes to ∞. If such a number exists, we call it the limit of $\{c_n\}_{n=1}^{\infty}$. Not every sequence has a limit, for example the Fibonacci sequence.

The intuitive idea of the limit of a sequence is not hard to understand. For example, it seems clear intuitively that the sequence $\left\{\frac{1}{n}\right\}_{n=1}^{\infty}$ has a limit, which is 0. However, it is not at all trivial to formulate this intuitive notion in a rigorous way that allows us to formulate proofs of properties of limits of sequences.

If we look at the formulation "the value of c_n gets closer and closer to a number L as the value of n goes to ∞," we see that there are two parts that need to be made precise, namely, the part about c_n getting closer and closer to L, and the part about n going to ∞. The key idea is to reformulate the notion of getting closer and closer to something by using a numerical measure of closeness, which is done by a number often denoted ε. We then say that the limit of $\{c_n\}_{n=1}^{\infty}$ is L if, for every possible choice of $\varepsilon > 0$, no matter how small, the value of c_n will eventually stay within distance ε of L as n goes to ∞. In other words, the limit of $\{c_n\}_{n=1}^{\infty}$ is L if for every $\varepsilon > 0$ we can show that for all sufficiently large values of n, the value of c_n will be within distance ε of L. We will use $N \in \mathbb{N}$ to denote the measure of largeness of n. We then say that the limit of $\{c_n\}_{n=1}^{\infty}$ is L if for every $\varepsilon > 0$ we can show that there is some $N \in \mathbb{N}$ such that for all n at least as large as N, the number c_n will be within ε distance of L. To say that c_n is within distance ε of L is to say that $|c_n - L| < \varepsilon$. We then see that the rigorous way to say "the value of c_n gets closer and closer to a number L as the value of n goes to ∞" is to say that for every $\varepsilon > 0$, there is some $N \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ such that $n \geq N$, it is the case that $|c_n - L| < \varepsilon$.

Definition 7.8.2. Let $\{c_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$, and let $L \in \mathbb{R}$. The sequence $\{c_n\}_{n=1}^{\infty}$ **converges** to L if for each $\varepsilon > 0$, there is some $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $|c_n - L| < \varepsilon$. If the sequence $\{c_n\}_{n=1}^{\infty}$ converges to L, then L is the **limit** of $\{c_n\}_{n=1}^{\infty}$, and we write

$$\lim_{n \to \infty} c_n = L.$$

If $\{c_n\}_{n=1}^{\infty}$ converges to some real number, the sequence $\{c_n\}_{n=1}^{\infty}$ is **convergent**; otherwise the sequence $\{c_n\}_{n=1}^{\infty}$ is **divergent**. $\triangle$

If the reader finds Definition 7.8.2 a bit hard to follow upon first, or second, encounter, the reader is in good company. This definition is indeed trickier than any definition we have seen in this text, and it often takes some practice to attain a reasonble level of comfort with this definition. Moreover, we are just skimming the surface in our discussion of the limits of sequences in this section, and substantial practice with this, and similar, concepts awaits the reader who takes a course in real analysis.

The use of quantifiers in general was discussed in Section 1.5, and the use of quantifiers in proofs was discussed in Section 2.5. In both those sections it was mentioned that when a statement has more than one quantifier, the order of the quantifiers matters. A classic example of the importance of the order of quantifiers can be seen in Definition 7.8.2. This definition could be written in logical symbols as

$$(\forall \varepsilon > 0)(\exists N \in \mathbb{N})[(n \in \mathbb{N} \wedge n \geq N) \to |c_n - L| < \varepsilon].$$

The order of the quantifiers in this statement cannot be changed, as the reader may verify by thinking about what the statement would mean if the order of the quantifiers were reversed.

As we saw in our discussion of proofs involving quantifiers in Section 2.5, when we want to prove a statement with more than one quantifier, we take one quantifier at a time, in the given order, from the outside in. Suppose that we want to prove that $\lim_{n \to \infty} c_n = L$, for some sequence $\{c_n\}_{n=1}^{\infty}$ and some $L \in \mathbb{R}$. The first quantifier that we need to deal with is $\forall \varepsilon > 0$, which is an abbreviated way of writing $\forall \varepsilon \in (0, \infty)$. To prove a statement with the universal quantifier $\forall \varepsilon > 0$, we must choose an arbitrary $\varepsilon > 0$, and then prove the result for that ε. From this point on in the proof, the arbitrary ε is fixed, and cannot be changed. Next, we need to deal with the quantifier $\exists N \in \mathbb{N}$. To prove a statement with this existential quantifier, we simply need to produce a value of N, and then show that it works. How we find the value of N is part of our scratch work, but is not part of the actual proof. The value of N may depend upon ε and upon the sequence $\{c_n\}_{n=1}^{\infty}$. Once N has been found, we then need to prove $(n \in \mathbb{N} \wedge n \geq N) \to |c_n - L| < \varepsilon$. To prove such an implication, we assume $n \in \mathbb{N} \wedge n \geq N$, and we need to deduce that $|c_n - L| < \varepsilon$. Hence, we proceed by choosing an arbitrary $n \in \mathbb{N}$ such that $n \geq N$. We then use whatever argumentation is needed to deduce that $|c_n - L| < \varepsilon$. It is important in such a proof that the arbitrary choices of ε and n are indeed arbitrary. Putting the above ideas together, we see that this type of proof typically has the following form.

Proof. Let $\varepsilon > 0$.

    ⋮

(argumentation)

    ⋮

Choose $N = \ldots$.

    ⋮

(argumentation)

    ⋮

Let $n \in \mathbb{N}$, and suppose that $n \geq N$.

    ⋮

(argumentation)

    ⋮

Therefore $|c_n - L| < \varepsilon$.   □

The above type of proof that $\lim_{n \to \infty} c_n = L$ is often called an "ε-N" proof.

For our first proof involving limits of sequences, observe that in Definition 7.8.2 it is not stated that the number "L" in the definition is unique. Of course, if the limit of a sequence were not unique, we could not properly speak of "the limit" but rather only of "a limit," and such a situation would be quite contrary to our intuitive notion of limits. Fortunately, as we see in the following lemma, it is indeed the case that

if a sequence has a limit, then there is a single number L that c_n is getting closer and closer to as n goes to ∞. In Section 2.5, we discussed proofs of existence and uniqueness. In the following lemma we prove only uniqueness but not existence, because not every sequence has a limit, though if a limit exists, then it is unique.

Lemma 7.8.3. *Let $\{c_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$. Then there is at most one $L \in \mathbb{R}$ such that $\lim\limits_{n \to \infty} c_n = L$.*

Proof. If there is no $L \in \mathbb{R}$ such that $\lim\limits_{n \to \infty} c_n = L$, then there is nothing to prove. Now suppose that there are $L_1, L_2 \in \mathbb{R}$ such that $L_1 \neq L_2$, and that $\lim\limits_{n \to \infty} c_n = L_1$ and $\lim\limits_{n \to \infty} c_n = L_2$. Let $\varepsilon = \frac{|L_1 - L_2|}{2}$. Then $\varepsilon > 0$. Hence by Definition 7.8.2 there is some $N_1 \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N_1$ imply $|c_n - L_1| < \varepsilon$, and there is some $N_2 \in \mathbb{N}$ that $n \in \mathbb{N}$ and $n \geq N_2$ imply $|c_n - L_2| < \varepsilon$. Let $N = \max\{N_1, N_2\}$. Then $N \geq N_1$ and $N \geq N_2$. We now use the Triangle Inequality (Theorem A.2 (1)) to compute

$$|L_1 - L_2| = |L_1 - c_N + c_N - L_2| \leq |L_1 - c_N| + |c_N - L_2|$$

$$= |c_N - L_1| + |c_N - L_2| < \varepsilon + \varepsilon = 2\varepsilon = 2\frac{|L_1 - L_2|}{2} = |L_1 - L_2|.$$

We have reached a contradiction, and it follows that there is at most one $L \in \mathbb{R}$ such that $\lim\limits_{n \to \infty} c_n = L$. $\square$

Because of Lemma 7.8.3, we can refer to "the" limit of a sequence, if the limit exists.

Now that we have established the uniqueness of limits of sequences when they exist, we turn to a few examples. In the first three parts of this example we will do scratch work prior to the actual proof. As the reader will observe, particularly in Part (3) of the example, it can happen that the scratch work and the actual proof look quite different from each other.

Example 7.8.4.

(1) Let $k \in \mathbb{R}$. We will prove that the constant sequence $k, k, k, k, \ldots$ is convergent, and that its limit is k. We can write this constant sequence as $\{c_n\}_{n=1}^{\infty}$, where $c_n = k$ for all $n \in \mathbb{N}$. We will prove that $\lim\limits_{n \to \infty} c_n = k$, which could also be written as $\lim\limits_{n \to \infty} k = k$.

Scratch Work. We will work backwards for our scratch work. We want to find $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $|c_n - k| < \varepsilon$, which is the same as $0 < \varepsilon$, and that is always true. Hence any $N \in \mathbb{N}$ will work, and we will arbitrarily choose $N = 1$.

Actual Proof. Let $\varepsilon > 0$. Let $N = 1$. Let $n \in \mathbb{N}$, and suppose that $n \geq N$. Then $|c_n - k| = |k - k| = 0 < \varepsilon$. Hence $\lim\limits_{n \to \infty} c_n = k$.

(2) We will prove that $\lim\limits_{n \to \infty} \frac{1}{n} = 0$.

Scratch Work. Again, we will work backwards for our scratch work. We want to find $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $\left|\frac{1}{n} - 0\right| < \varepsilon$, which is the same as $\frac{1}{n} < \varepsilon$.

Hence, we need some $N \in \mathbb{N}$ such that $\frac{1}{N} < \varepsilon$, which means that we need to choose some $N \in \mathbb{N}$ such that $N > \frac{1}{\varepsilon}$. It is intuitively evident that such N can always be found, and formally we can find such N by Theorem A.3.

Actual Proof. Let $\varepsilon > 0$. By Theorem A.3 there is some $N \in \mathbb{N}$ such that $\frac{1}{\varepsilon} < N$. Then $\frac{1}{N} < \varepsilon$. Let $n \in \mathbb{N}$, and suppose that $n \geq N$. Then

$$\left| \frac{1}{n} - 0 \right| = \left| \frac{1}{n} \right| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon.$$

Therefore $\lim\limits_{n \to \infty} \frac{1}{n} = 0$.

(**3**) We will prove that $\lim\limits_{n \to \infty} \frac{2n^2}{n^2+3} = 2$.

Scratch Work. This example is trickier than the previous one. We want to find $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply

$$\left| \frac{2n^2}{n^2+3} - 2 \right| < \varepsilon,$$

which is the same as

$$\left| \frac{-6}{n^2+3} \right| < \varepsilon,$$

which is equivalent to

$$\frac{6}{n^2+3} < \varepsilon,$$

which in turn is the same as

$$\frac{6}{\varepsilon} < n^2 + 3.$$

Solving for n we obtain

$$n > \sqrt{\frac{6}{\varepsilon} - 3}.$$

Unfortunately, this last inequality has a problem when the expression inside the square root is negative, and we will therefore need to consider two cases. First, suppose that $\frac{6}{\varepsilon} \geq 3$. Then $\varepsilon \leq 2$. In this case case we can use any choice of N such that

$$N > \sqrt{\frac{6}{\varepsilon} - 3}.$$

Second, suppose that $\frac{6}{\varepsilon} < 3$. Then $\varepsilon > 2$. In this case we cannot use $\sqrt{\frac{6}{\varepsilon} - 3}$, but fortunately it turns out that we do not need to. Instead, we observe that if $n \in \mathbb{N}$, then

$$\frac{6}{n^2+3} < \frac{6}{0^2+3} = 2 < \varepsilon.$$

Hence, in this case any choice of N will work, so we choose $N = 1$.

Actual Proof. Let $\varepsilon > 0$. There are two cases. First, suppose that $\varepsilon > 2$. Let $N = 1$. Let $n \in \mathbb{N}$, and suppose that $n \geq N$. Then

$$\left| \frac{2n^2}{n^2+3} - 2 \right| = \left| \frac{-6}{n^2+3} \right| = \frac{6}{n^2+3} < 2 < \varepsilon.$$

Second, suppose that $\varepsilon \leq 2$. Then $\frac{6}{\varepsilon} - 3 \geq 0$. By Theorem A.3 there is some $N \in \mathbb{N}$ such that

$$N > \sqrt{\frac{6}{\varepsilon} - 3}.$$

Let $n \in \mathbb{N}$, and suppose that $n \geq N$. Then

$$n > \sqrt{\frac{6}{\varepsilon} - 3}.$$

Some rearranging yields

$$\frac{6}{n^2+3} < \varepsilon,$$

and therefore

$$\left| \frac{2n^2}{n^2+3} - 2 \right| = \frac{6}{n^2+3} < \varepsilon.$$

Putting the two cases together proves that $\lim_{n\to\infty} \frac{2n^2}{n^2+3} = 2$.

(4) We will prove that the sequence $1, 0, 1, 0, \ldots$ is divergent. We can write this sequence as $\{c_n\}_{n=1}^{\infty}$, where

$$c_n = \begin{cases} 1, & \text{if } n \text{ is odd} \\ 0, & \text{if } n \text{ is even.} \end{cases}$$

(It is possible to avoid the two cases in the above equation by writing $c_n = \frac{1+(-1)^{n+1}}{2}$ for all $n \in \mathbb{N}$, but doing so, while shorter, makes the proof less clear, and brevity is never worthwhile at the expense of clarity.) Suppose to the contrary that $\lim_{n\to\infty} c_n = L$ for some $L \in \mathbb{R}$. Let $\varepsilon = \frac{1}{2}$. Then there is some $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $|c_n - L| < \frac{1}{2}$. Let $n_1, n_2 \in \mathbb{N}$, and suppose that $n_1 \geq N$ and n_1 is odd, and that $n_2 \geq N$ and n_2 is even. Using the Triangle Inequality (Theorem A.2 (1)) we compute

$$1 = |1 - 0| = |c_{n_1} - c_{n_2}| = |c_{n_1} - L + L - c_{n_2}|$$
$$\leq |c_{n_1} - L| + |L - c_{n_2}| < \frac{1}{2} + \frac{1}{2} = 1.$$

We have reached a contradiction, and it follows that $\{c_n\}_{n=1}^{\infty}$ is divergent.   ◊

Limits of sequences involve what happens to the terms of the sequence as n goes to ∞. It therefore makes sense intuitively that if finitely many terms of a sequence are changed, it does not affect whether or not the sequence is convergent, and if the

sequence is convergent, it does not change what the limit of the sequence is. A proof of this fact is given in Exercise 7.8.3.

We now prove three typical, and useful, theorems about sequences. There are, of course, many more such theorems that can be proved about sequences, but we have space only for these three.

Our first theorem, which will be used in the proof of the following theorem, states that if a sequence is convergent, then the terms of the sequence cannot become too large in absolute value.

Theorem 7.8.5. *Let $\{c_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$. If $\{c_n\}_{n=1}^{\infty}$ is convergent, then there is some $B \in \mathbb{R}$ such that $|c_n| \leq B$ for all $n \in \mathbb{N}$.*

Proof. Suppose that $\{c_n\}_{n=1}^{\infty}$ is convergent. Then there is some $L \in \mathbb{R}$ such that $\lim_{n \to \infty} c_n = L$. Hence there is some $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $|c_n - L| < 1$. It follows from Theorem A.2 (2) that $n \in \mathbb{N}$ and $n \geq N$ imply $|c_n| - |L| < 1$, and therefore $|c_n| < |L| + 1$. Let

$$B = \max\{|c_1|, |c_2|, \ldots, |c_{N-1}|, |L| + 1\}.$$

We then see that $|c_k| \leq B$ for all $k \in \mathbb{N}$. □

The converse of Theorem 7.8.5 is not true. For example, the sequence $1, 0, 1, 0, \ldots$ satisfies the conclusion of the theorem, but we saw in Example 7.8.4 (4) that it is divergent. If a sequence satisfies the conclusion of Theorem 7.8.5, it is customary to say that the sequence is "bounded," though we will not need that terminology here.

Observe that in Theorem 7.8.5, it is always possible to choose the number B so that $B > 0$.

Our next theorem shows that limits of sequences behave nicely with respect to term-by-term addition, subtraction, multiplication and division of sequences.

Theorem 7.8.6. *Let $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ be sequences in $\mathbb{R}$, and let $k \in \mathbb{R}$. Suppose that $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ are convergent.*

1. *The sequence $\{c_n + d_n\}_{n=1}^{\infty}$ is convergent, and $\lim_{n \to \infty} [c_n + d_n] = \lim_{n \to \infty} c_n + \lim_{n \to \infty} d_n$.*

2. *The sequence $\{c_n - d_n\}_{n=1}^{\infty}$ is convergent, and $\lim_{n \to \infty} [c_n - d_n] = \lim_{n \to \infty} c_n - \lim_{n \to \infty} d_n$.*

3. *The sequence $\{kc_n\}_{n=1}^{\infty}$ is convergent, and $\lim_{n \to \infty} kc_n = k \lim_{n \to \infty} c_n$.*

4. *The sequence $\{c_n d_n\}_{n=1}^{\infty}$ is convergent, and $\lim_{n \to \infty} c_n d_n = \left[\lim_{n \to \infty} c_n\right] \cdot \left[\lim_{n \to \infty} d_n\right]$.*

5. *If $\lim_{n \to \infty} d_n \neq 0$, then the sequence $\left\{\frac{c_n}{d_n}\right\}_{n=1}^{\infty}$ is convergent, and $\lim_{n \to \infty} \frac{c_n}{d_n} = \dfrac{\lim_{n \to \infty} c_n}{\lim_{n \to \infty} d_n}$.*

Proof. We will prove Parts (1) and (4), leaving the rest to the reader in Exercise 7.8.13.

Let $L = \lim_{n \to \infty} c_n$ and $M = \lim_{n \to \infty} d_n$.

(1). Let $\varepsilon > 0$. Then there is some $N_1 \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N_1$ imply $|c_n - L| < \frac{\varepsilon}{2}$, and there is some $N_2 \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N_2$ imply $|d_n - M| < \frac{\varepsilon}{2}$. Let $N = \max\{N_1, N_2\}$. Let $n \in \mathbb{N}$, and suppose that $n \geq N$. The Triangle Inequality (Theorem A.2 (1)) now implies

$$|(c_n + d_n) - (L + M)| = |(c_n - L) + (d_n - M)| \leq |c_n - L| + |d_n - M| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

(4). Let $\varepsilon > 0$. By Theorem 7.8.5 there is some $B \in \mathbb{R}$ such that $|d_n| \leq B$ for all $n \in \mathbb{N}$. We may assume that $B > 0$. Therefore $B + |L| > 0$. Then there is some $N_1 \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N_1$ imply $|c_n - L| < \frac{\varepsilon}{B + |L|}$, and there is some $N_2 \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N_2$ imply $|d_n - M| < \frac{\varepsilon}{B + |L|}$. Let $N = \max\{N_1, N_2\}$. Let $n \in \mathbb{N}$, and suppose that $n \geq N$. Using the Triangle Inequality and Exercise 2.4.9 (4) we see that

$$|c_n d_n - LM| = |c_n d_n - d_n L + d_n L - LM| \leq |d_n(c_n - L)| + |L(d_n - M)|$$
$$= |d_n| \cdot |c_n - L| + |L| \cdot |d_n - M| < B \cdot \frac{\varepsilon}{B + |L|} + |L| \cdot \frac{\varepsilon}{B + |L|} = \varepsilon. \quad \square$$

It is important to recognize that in Theorem 7.8.6, it is necessary to assume that $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ are convergent. If the sequences are not convergent, then $\lim_{n \to \infty} c_n$ and $\lim_{n \to \infty} d_n$ do not exist, and so it would make no sense to write expressions such as "$\lim_{n \to \infty} c_n + \lim_{n \to \infty} d_n$." Moreover, it can happen that $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ are divergent, and yet $\{c_n + d_n\}_{n=1}^{\infty}$ is convergent, in which case it would not be plausible to expect to express $\lim_{n \to \infty}(c_n + d_n)$ in terms of the non-existent limits of $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$; the reader is asked to supply an example of such sequences in Exercise 7.8.6.

A simple use of Theorem 7.8.6 is seen in the following example.

Example 7.8.7. We saw in Example 7.8.4 (3) that $\lim_{n \to \infty} \frac{2n^2}{n^2 + 3} = 2$. The proof in that example used the definition of limits of sequences directly. Now that we have Theorem 7.8.6, we can give a much easier proof that this limit holds.

We know by Example 7.8.4 (2) that $\lim_{n \to \infty} \frac{1}{n} = 0$; that ε-N proof was much simpler than the ε-N proof in Example 7.8.4 (3). It now follows from Theorem 7.8.6 (4) that

$$\lim_{n \to \infty} \frac{1}{n^2} = \lim_{n \to \infty} \frac{1}{n} \cdot \frac{1}{n} = \left[\lim_{n \to \infty} \frac{1}{n} \right] \cdot \left[\lim_{n \to \infty} \frac{1}{n} \right] = 0 \cdot 0 = 0.$$

We then use Theorem 7.8.6 (1) (3) (5) to compute

$$\lim_{n \to \infty} \frac{2n^2}{n^2 + 3} = \lim_{n \to \infty} \frac{2}{1 + 3 \cdot \frac{1}{n^2}} = \frac{2}{1 + 3 \cdot 0} = 2. \qquad \diamond$$

Our last theorem shows that limits of sequences behave nicely with respect to the relation $\leq$.

Theorem 7.8.8. *Let $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ be sequences in $\mathbb{R}$. Suppose that there is some $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $c_n \leq d_n$. If $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ are convergent, then $\lim_{n \to \infty} c_n \leq \lim_{n \to \infty} d_n$.*

Proof. Suppose that $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ are convergent. Let $L = \lim_{n\to\infty} c_n$ and $M = \lim_{n\to\infty} d_n$. Suppose that $M < L$. Let $\varepsilon = \frac{L-M}{2}$. Then $\varepsilon > 0$. Hence there is some $N_1 \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N_1$ imply $|c_n - L| < \varepsilon$, and there is some $N_2 \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N_2$ imply $|d_n - M| < \varepsilon$. Let $P = \max\{N, N_1, N_2\}$. Then $|c_P - L| < \varepsilon$ and $|d_P - M| < \varepsilon$. It follows that $L - \varepsilon < c_P < L + \varepsilon$ and $M - \varepsilon < d_P < M + \varepsilon$, and hence

$$d_P < M + \varepsilon = M + \frac{L-M}{2} = \frac{L+M}{2} = L - \frac{L-M}{2} = L - \varepsilon < c_P.$$

This last inequality contradicts the fact that $c_n \leq d_n$ for all $n \in \mathbb{N}$ such that $n \geq N$. Therefore $L \leq M$. $\square$

We note that that it is not possible to replace $\leq$ with $<$ throughout the statement of Theorem 7.8.8; the reader is asked to supply an example to show why in Exercise 7.8.7.

<div align="center">

Exercises

</div>

Exercise 7.8.1. Using only the definition of limits of sequences, prove that each of the following statements is true.

(1) $\lim_{n\to\infty} \frac{1}{5n-2} = 0$.

(2) $\lim_{n\to\infty} \frac{1}{\sqrt[3]{n}} = 0$.

(3) $\lim_{n\to\infty} \frac{n+1}{n+2} = 1$.

(4) $\lim_{n\to\infty} \frac{1}{n^2+1} = 0$.

(5) $\{n\}_{n=1}^{\infty}$ is divergent.

Exercise 7.8.2. Prove that $\{2n\}_{n=1}^{\infty}$ is divergent, in each of the following two ways.

(1) Use only the definition of limits of sequences.

(2) Use Theorem 7.8.5.

Exercise 7.8.3. [Used in Section 7.8.] Let $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ be sequences in $\mathbb{R}$. Suppose that there is some $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $c_n = d_n$. Prove that $\{c_n\}_{n=1}^{\infty}$ is convergent if and only if $\{d_n\}_{n=1}^{\infty}$ is convergent, and if they are convergent then $\lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n$.

Exercise 7.8.4. Let $\{c_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$, and let $r \in \mathbb{N}$. Let $\{d_n\}_{n=1}^{\infty}$ be the sequence defined by $d_n = c_{n+r}$ for all $n \in \mathbb{R}$. Prove that $\{c_n\}_{n=1}^{\infty}$ is convergent if and only if $\{d_n\}_{n=1}^{\infty}$ is convergent, and if they are convergent then $\lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n$.

Exercise 7.8.5. Let $\{c_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$, and let $L \in \mathbb{R}$. Prove that $\lim_{n\to\infty} c_n = L$ if and only if $\lim_{n\to\infty} [c_n - L] = 0$.

Exercise 7.8.6. [Used in Section 7.8.] Find an example of sequences $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ in $\mathbb{R}$ such that $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ are divergent, but $\{c_n + d_n\}_{n=1}^{\infty}$ is convergent.

Exercise 7.8.7. [Used in Section 7.8.] Find an example of sequences $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ in $\mathbb{R}$ such that $c_n < d_n$ for all $n \in \mathbb{N}$, and that $\lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n$.

Exercise 7.8.8. Find an example of sequences $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ in $\mathbb{R}$ such that $\lim_{n\to\infty} c_n = 0$, but $\{c_n d_n\}_{n=1}^{\infty}$ is divergent.

Exercise 7.8.9. Let $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ be sequences in $\mathbb{R}$. Suppose that $\lim_{n\to\infty} c_n = 0$, and that there is some $D \in \mathbb{R}$ such that $|d_n| \leq D$ for all $n \in \mathbb{N}$. Prove that $\lim_{n\to\infty} c_n d_n = 0$.

Exercise 7.8.10. Let $\{c_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$. Suppose that $\{c_n\}_{n=1}^{\infty}$ is convergent, and that $\lim_{n\to\infty} c_n > 0$. Prove that there is some $D > 0$ and some $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $c_n > D$.

Exercise 7.8.11. Let $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ be sequences in $\mathbb{R}$. Suppose that $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ are convergent, and that $\lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n$. Prove that $\{\min\{c_n, d_n\}\}_{n=1}^{\infty}$ is convergent and $\lim_{n\to\infty} \min\{c_n, d_n\} = \lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n$.

Exercise 7.8.12. Let $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ be sequences in $\mathbb{R}$, and let $L \in \mathbb{R}$. Suppose that $\lim_{n\to\infty} d_n = 0$, and that there is some $N \in \mathbb{N}$ such that $n \in \mathbb{N}$ and $n \geq N$ imply $|c_n - L| \leq d_n$. Prove that $\lim_{n\to\infty} c_n = L$.

Exercise 7.8.13. [Used in Theorem 7.8.6.] Prove Theorem 7.8.6 (2) (3) (5).

Exercise 7.8.14. Let $\{c_n\}_{n=1}^{\infty}$ and $\{d_n\}_{n=1}^{\infty}$ be sequences in $\mathbb{R}$, and let $k \in \mathbb{R}$. Suppose that $\{c_n\}_{n=1}^{\infty}$ is divergent and $\{d_n\}_{n=1}^{\infty}$ is convergent.

    (1) Prove that $\{c_n + d_n\}_{n=1}^{\infty}$ is divergent.
    (2) Prove that $\{c_n - d_n\}_{n=1}^{\infty}$ is divergent.
    (3) Prove that $\{kc_n\}_{n=1}^{\infty}$ is divergent.

Exercise 7.8.15. Let $\{c_n\}_{n=1}^{\infty}$ be a sequence in $\mathbb{R}$.

    (1) Let $L \in \mathbb{R}$. Prove that if $\lim_{n\to\infty} c_n = L$, then $\lim_{n\to\infty} |c_n| = |L|$.
    (2) Prove that $\lim_{n\to\infty} c_n = 0$ if and only if $\lim_{n\to\infty} |c_n| = 0$.
    (3) Give an example of a sequence $\{d_n\}_{n=1}^{\infty}$ in $\mathbb{R}$ such that $\{|d_n|\}_{n=1}^{\infty}$ is convergent, but $\{d_n\}_{n=1}^{\infty}$ is divergent.

8

Explorations

The imagination in a mathematician who creates makes no less difference than in a poet who invents.

– Jean d'Alembert (1717–1783)

8.1 Introduction

We now turn things over to the reader. The goal of this book is for the student to learn how to do mathematics as mathematicians currently do it. The ideas we have covered, such as proofs, sets, functions and relations, are in the tool bag of any working mathematician. There is, however, one aspect of mathematics that we have not seen until now. So far the reader has been learning the material from the text, using exercises as practice. The material in the text is presented in a straight path, going one step forward at a time. The exercises, as the reader may assume, can all be solved using the material that was discussed until that point. Mathematical research, by contrast, is not so straightforward.

Research in mathematics involves discovering—and then proving —new theorems. Contrary to popular misconception, mathematics has not been "all figured out." Indeed, more new mathematics is being discovered today than at any other period in history. What makes research so exciting is precisely that there is no text, and no clear path, to follow. The researcher has to try examples, develop an intuitive feeling for what is going on, formulate proposed definitions, try to prove theorems using these definitions, go back to the drawing board if things do not work out and so on. This process can be tiring and frustrating, and often involves attempts that turn out to lead nowhere, but for the sake of those times when the ideas do come together in the proof of a new theorem, it is well worth it.

At the level of this text, it is not possible to do any research in the sense of being at the cutting edge of some branch of mathematics. Nonetheless, we can attempt to create the feeling of mathematics research for the reader by providing some open-ended topics to be explored. These topics are all known to mathematicians, but we

assume that the reader has not seen them. For each of these topics, we give a few definitions, and raise a few questions, and leave the rest to the reader's imagination.

The reader should pick a topic, and then play with it. Formulate conjectures, make whatever extra definitions are necessary, try to come up with theorems and proofs and write up the results of this exploration as if they were meant to be an additional section for this book. The writing should include definitions, examples, lemmas, theorems, proofs and informal discussion. The target audience for this exposition should be the other students who have seen the material from this book, but nothing beyond it (and in particular, have not looked at the topic under consideration). The reader should not look the topic up in other books until her own exploration and writing is complete—the point is not to see what else is known, but to explore as much as possible on one's own.

Rather than choosing one of the topics suggested below, the reader could try to come up with a topic of her own to explore. Doing so is a good way to ensure that the topic will be enjoyable, but it is also risky, because some proposed avenues of exploration may not lead anywhere, and others may be too difficult. Consult with the instructor of the course about any such ideas.

8.2 Greatest Common Divisors

A standard construction that is taught in elementary school is to find the greatest common divisor of two integers. For example, the greatest common divisor of 12 and 16 is 4. Greatest common divisors are useful not only in school mathematics, but also in advanced topics such as number theory. Recall the definition of an integer a dividing an integer b, denoted $a|b$, given in Definition 2.2.1.

Definition 8.2.1. Let $a, b \in \mathbb{Z}$. If at least one of a or b is not zero, the **greatest common divisor** of a and b, denoted (a, b), is the largest integer that divides both a and b. If $a = 0$ and $b = 0$, let $(0, 0) = 0$.   △

For example, we see that $(27, 36) = 9$. The notation (a, b) for the greatest common divisor of a and b is somewhat unfortunate, because the same notation can also mean an ordered pair or an open bounded interval in the real numbers, but it is quite standard, and rarely causes confusion when read in context.

Before proceeding, we need the following lemma.

Lemma 8.2.2. *Let $a, b \in \mathbb{Z}$. Then (a, b) exists, and $(a, b) \geq 0$.*

Proof. If $a = 0$ and $b = 0$ then (a, b) exists by definition, and $(a, b) \geq 0$. Now suppose that at least one of a or b is not zero. Let

$$S = \{d \in \mathbb{N} \mid d|a \text{ and } d|b, \text{ and } d > 0\}.$$

Observe that the set S is non-empty, because it contains 1, and that if $x \in S$, then x is less than or equal to the smaller of a and b. It follows from Exercise 6.6.2 that S is finite. By Exercise 6.6.5 there exists some $k \in S$ such that $p \leq k$ for all $p \in S$. Because

any divisor of a and b that is not in S is negative, and is therefore less than k, then k is the greatest common divisor of a and b. Hence (a,b) exists, and $(a,b) \geq 0$.   □

The following related definition is useful in the study of greatest common divisors.

Definition 8.2.3. Let $a, b \in \mathbb{Z}$. The numbers a and b are **relatively prime** if $(a,b) = 1$.   △

For example, the numbers 15 and 28 are relatively prime.

It is possible to prove many results about greatest common divisors, some simple and some more substantial. A typical simple result is the following proposition. It might appear at first glance that the proposition is entirely trivial, if one thinks about greatest common divisors in terms of factoring all the relevant integers into unique prime factors. This fact, known as the Fundamental Theorem of Arithmetic, is a substantial result that we have not proved, and so it should not be used here. All results about greatest common divisors that the reader considers should be proved using only what we have proved in this book.

Proposition 8.2.4. Let $a, b \in \mathbb{Z}$. If $d = (a,b)$ is not zero, then $(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof. Observe that $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Let $r \in \mathbb{Z}$. Suppose that $r|\frac{a}{d}$ and $r|\frac{b}{d}$. Then there are $m, n \in \mathbb{Z}$ such that $rm = \frac{a}{d}$ and $rn = \frac{b}{d}$. Then $a = rmd$ and $b = rnd$. Hence $(rd)|a$ and $(rd)|b$. Because d is the largest integer that divides a and b, it follows that $rd \leq d$. Using the fact that $d > 0$, we deduce that $r \leq 1$. Because 1 divides both $\frac{a}{d}$ and $\frac{b}{d}$, we see that $(\frac{a}{d}, \frac{b}{d}) = 1$.   □

A look at some examples of greatest common divisors shows that the greatest common divisor of any two integers a and b is not only greater than all other integers that divide a and b, but in fact is divisible by every integer that divides a and b. This fact is stated in the following theorem.

Theorem 8.2.5. Let $a, b, p \in \mathbb{Z}$. If $p|a$ and $p|b$, then $p|(a,b)$.

Theorem 8.2.5 follows from the next result.

Theorem 8.2.6. Let $a, b \in \mathbb{Z}$. Then there are $m, n \in \mathbb{Z}$ such that $(a,b) = ma + nb$.

Theorem 8.2.6 is proved by using the Well-Ordering Principle (Theorem 6.2.5) applied to the set of all natural numbers of the form $ma + nb$, and then using the Division Algorithm (Theorem A.5 in the Appendix). It is left to the reader to work out the details of the proofs of Theorem 8.2.6 and Theorem 8.2.5.

The reader's task is to conjecture and prove as many results as possible about greatest common divisors, using only what is stated above.

Greatest common divisors are discussed in many texts on number theory, for example [Ros05, Section 3.3].

8.3 Divisibility Tests

There are a number of known methods for determining whether one integer is divisible by another integer. For example, an integer is divisible by 9 if and only if the sum of its digits is divisible by 9. Therefore, it is easily seen that 107523 is divisible by 9, because $1+0+7+5+2+3 = 18$, and we know that 18 is divisible by 9. A proof of the validity of this method relies on the notion of congruence modulo 9, as discussed in Section 5.2. More precisely, it is shown in Exercise 5.2.12 that if $a_m a_{m-1} \cdots a_2 a_1$ is a natural number written in decimal notation, then

$$\sum_{i=1}^{m} a_i 10^{i-1} \equiv \sum_{i=1}^{m} a_i \pmod{9}.$$

The left-hand side of this congruence is the value of the integer written $a_m a_{m-1} \cdots a_2 a_1$ in decimal notation, and the right-hand side is the sum of the digits. Our method for verifying divisibility by 9 follows immediately from this congruence. We could also take this process one step further, using the notation of Exercise 5.2.13. If $x \in \mathbb{N}$, we let $\bar{\Sigma}(x)$ denote the result of repeatedly adding the digits of x until a single digit remains. It follows that a positive integer x is divisible by 9 if and only if $\bar{\Sigma}(x) = 9$.

The reader's task is to try to find, and prove, similar methods for determining divisibility by other numbers. A good place to start is with divisibility by each of 2, 3 and 5. It is also possible to use different bases for writing integers, instead of only decimal notation.

A reference for this topic is [Ros05, Section 5.1].

8.4 Real-Valued Functions

In Section 4.3 we discussed the most broadly applicable way of combining functions, namely, composition. In some specific situation, however, there are other ways to combine functions. In calculus courses, for example, we regularly deal with sums, differences, products and quotients of functions $\mathbb{R} \to \mathbb{R}$. From the point of view of adding, subtracting, multiplying and dividing functions, it turns out to be irrelevant that the domain of these functions is $\mathbb{R}$ (though of course the domain being $\mathbb{R}$ is very important for taking derivatives and integrals). The addition, subtraction, multiplication and division of functions take place in the codomain, and hence these four operations can be applied to any functions with codomain $\mathbb{R}$ (or certain other sets such as the complex numbers, but we will not deal with that here).

For convenience we use the following terminology.

Definition 8.4.1. A **real-valued** function is a function of the form $f \colon X \to \mathbb{R}$, where X is a set. △

Your task is to explore the properties of real-valued functions. For example, we can define addition of real-valued functions as follows.

Definition 8.4.2. Let X be a set, and let $f, g \colon X \to \mathbb{R}$ be functions. The **sum** of f and g, denoted $f + g$, is the function $f + g \colon X \to \mathbb{R}$ defined by

$$(f + g)(x) = f(x) + g(x)$$

for all $x \in X$.   △

Observe that we can add two real-valued functions only if they have the same domains. Definition 8.4.2 is often referred to as "pointwise addition," because it is done separately for each element in the domain. It is possible to define other pointwise operations, for example subtraction, multiplication and division.

The following lemma is a typical simple result about addition of real-valued functions. For those familiar with the term, this lemma says that addition of real-valued functions is commutative.

Lemma 8.4.3. *Let X be a set, and let $f, g \colon X \to \mathbb{R}$ be functions. Then $f + g = g + f$.*

Proof. Clearly $f + g$ and $g + f$ have the same domain, the set X, and the same codomain, the set $\mathbb{R}$. Let $x \in X$. Then

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x),$$

where the middle equality holds because we know that $a + b = b + a$ for all $a, b \in \mathbb{R}$, and we know that $f(x)$ and $g(x)$ are real numbers. (Recall that $f(x)$ and $g(x)$ are values in the codomain, which in this case is $\mathbb{R}$, and are not the names of the functions—which are simply f and g.) Hence $f + g = g + f$.   □

The reader should try to conjecture and prove other results about addition of real-valued functions, and should define other operations (such as multiplication), and also relations (such as less than), for real-valued functions, and then prove results about those definitions.

8.5 Iterations of Functions

The idea of iterations of functions was used in Exercise 4.4.20 and Exercise 4.4.21. Those two exercises are rather lengthy and difficult. Here we wish to look at some simpler properties of iterations of functions. For convenience, we repeat the basic definition. (As mentioned in Exercise 4.4.20, this definition, while intuitively reasonable, is not entirely rigorous, because the use of $\cdots$ is not rigorous; a completely rigorous definition was given in Example 6.4.2 (2).)

Definition 8.5.1. Let A be a non-empty set, and let $f \colon A \to A$ be a function. Suppose that f is bijective. For each $n \in \mathbb{N}$, let f^n denote the function $A \to A$ given by

$$f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

The function f^n is the n-**fold iteration** of f.   △

As simple as this definition might appear, iterations of functions are of great importance in many branches of mathematics, and have been the focus of particular attention in the field of dynamical systems, which deals, among many other things, with the much talked about fractals and "chaos."

Your task is to explore various properties of iterations of functions. Some possible questions to look at involve the following concepts.

Definition 8.5.2. Let A be a non-empty set, and let $f : A \to A$ be a function. The function f is **nilpotent** if $f^n = 1_A$ for some $n \in \mathbb{N}$. The function f is **hidempotent** if $f^n = f$ for some $n \in \mathbb{N}$ such that $n \geq 2$. The function f is **constantive** if f^n is a constant function for some $n \in \mathbb{N}$.   △

The term "nilpotent" is quite standard, whereas the other two terms in Definition 8.5.2 are not (though "hidempotent" is meant to suggest the standard term "idempotent," which means that $f^2 = f$.)

There are many questions to be asked about these concepts. Is there a constantive function that is not constant? For any $r \in \mathbb{N}$ such that $r \geq 2$, is there a function $f : A \to A$ for some set A such that f^r is a constant function, but f^{r-1} is not a constant function? Is there a nilpotent function that is not the identity function? For any given $r \in \mathbb{N}$ such that $r \geq 2$, is there a function $g : A \to A$ for some set A such that $g^r = 1_A$ but $g^{r-1} \neq 1_A$. If a function is nilpotent or hidempotent, is it necessarily bijective? If a function is hidempotent and bijective, is it necessarily nilpotent? If a function is nilpotent, is it necessarily hidempotent? Do stronger conclusions hold when the set A is finite?

The reader is asked to consider the above questions, and to try to think up other definitions and questions about iterations of functions, and to try to solve as many of those questions as possible.

See [HW91, Chapter 5] or [ASY97] for details about iterations of functions in connection with dynamical systems and chaos.

8.6 Fibonacci Numbers and Lucas Numbers

In Section 6.4 we briefly discussed the Fibonacci numbers. There is much more that can be said about these remarkable numbers. We suggest four possible avenues for exploration.

A) More Fibonacci Formulas

We gave a number of nice formulas for the Fibonacci numbers in Proposition 6.4.6, Equation 6.4.1 and Exercises 6.4.7–6.4.9. The reader should play with the Fibonacci numbers, and try to find and prove other formulas for these numbers.

B) Lucas Numbers

The Fibonacci numbers are not the only sequence of numbers that obey the Fibonacci recursion relation. If we change the initial two numbers, we obtain a different sequence. One such sequence that is often studied in conjunction with the Fibonacci numbers is the Lucas sequence, which starts

$$1, 3, 4, 7, 11, 18, 29, 47, 76, 123 \ldots.$$

The numbers in this sequence are referred to as Lucas numbers. Let $L_1, L_2, L_3, \ldots$ denote the terms of the Lucas sequence. This sequence is formally defined using Definition by Recursion as the sequence specified by $L_1 = 1$, and $L_2 = 3$, and $L_{n+2} = L_{n+1} + L_n$ for all $n \in \mathbb{N}$. We use Theorem 6.4.5 to verify that such a sequence exists. The Lucas numbers turn out to be of use in primality testing; see [Rib96, Sections 2.4 and 2.5] for details.

The reader's task is to conjecture and prove formulas for the Lucas numbers. Start by considering the analogs of the various formulas we have seen for the Fibonacci numbers. For example, do the analogs of the three parts of Proposition 6.4.6 hold for the Lucas numbers? Is there an explicit formula for the Lucas numbers similar to Binet's formula (Equation 6.4.1)?

C) Relations between Fibonacci and Lucas Numbers

There are some formulas relating the Fibonacci numbers and the Lucas numbers. One such formula is $L_n = F_n + 2F_{n-1}$ for all $n \in \mathbb{N}$ such that $n \geq 2$. The reader should prove this formula, and try to find and prove other such formulas.

D) Fibonacci Numbers Modulo k

Let $k \in \mathbb{N}$. We can then look at the Fibonacci sequence modulo k, which we obtain by taking the Fibonacci sequence, and replacing each Fibonacci number with the unique integer in $\{0, 1, \ldots, k-1\}$ that is congruent to it modulo k. For example, if we use $k = 3$, we obtain the modulo 3 Fibonacci sequence, which starts

$$1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0 \ldots.$$

Let $F_1^{(3)}, F_2^{(3)}, \ldots$ denote the terms of this sequence. Observe that $F_{n+2}^{(3)} \equiv F_{n+1}^{(3)} + F_n^{(3)}$ (mod 3) for all $n \in \mathbb{N}$, as can be proved using Lemma 5.2.11. Observe also that this sequence repeats itself. What can we deduce about the original Fibonacci sequence from this repetition? The reader should play around with these ideas using various values for k, and try to formulate and prove results about either the original Fibonacci sequence, or the modulo k Fibonacci sequence for specific values of k.

Some sources with many results about the Fibonacci numbers are [Knu73, Section 1.2.8 and exercises], [GKP94, Section 6.6] and [HHP97, Chapter 3].

8.7 Fuzzy Sets

A fundamental feature of sets is that any element either is in a given set or is not. There is no concept of something "probably" being in a set, nor of one element having a higher probability of being in a set than another. Unfortunately, the real world does not always give us black-and-white information, and so a more flexible notion of a "set" is helpful in dealing with some real-world problems. In response to this need, a theory of "fuzzy sets," "fuzzy logic" and other related "fuzzy" things was developed in the 1960s. These ideas have applications in data analysis, pattern recognition, database management and other areas. Here we will just introduce the most basic definition concerning fuzzy sets.

The method of introducing uncertainty into the definition of sets is to use the notion of characteristic maps (as discussed in Exercise 4.1.8, but which we will repeat here). For the entirety of our discussions, we will need to think of all sets under consideration as being subsets of some large set X, which in practice is not a problem in any given situation.

Definition 8.7.1. Let X be a non-empty set, and let $S \subseteq X$ be a subset. The **characteristic map** for S in X, denoted χ_S, is the function $\chi_S \colon X \to \{0,1\}$ defined by

$$\chi_S(y) = \begin{cases} 1, & \text{if } y \in S \\ 0, & \text{if } y \in X - S. \end{cases} \qquad \triangle$$

The characteristic map χ_S maps everything in the set S to 1, and everything else to 0, and it is therefore useful for identifying the subset S. In Exercise 4.1.8, it was proved that if $A, B \subseteq X$ are subsets, then $\chi_A = \chi_B$ if and only if $A = B$ (the former equality is of functions, the latter of sets).

To allow fuzziness, we use characteristic maps that have values anywhere in the interval $[0,1]$, rather than in the two-element set $\{0,1\}$. However, rather than defining the notion of a "fuzzy set" directly, and then defining characteristic maps for such sets, we simply let our broader type of characteristic maps be our new kind of sets.

Definition 8.7.2. Let X be a non-empty set. A **fuzzy subset** A of X is a function $\mu_A \colon X \to [0,1]$. $\qquad \triangle$

The idea is that if A is a fuzzy subset of X, then $x \in X$ is definitely in A if $\mu_A(x) = 1$, is definitely not in A if $\mu_A(x) = 0$ and is somewhere in between if $0 < \mu_A(x) < 1$. Observe that a function $\mu_A \colon X \to [0,1]$ is not the name of the fuzzy subset of X, but rather A is the name of the fuzzy subset; the function μ_A defines the fuzzy subset A. Observe also that the functions μ_A need not be particularly nice (for example, they do not need to be continuous). It is important to recognize that we only have fuzzy subsets of a given set X, but not fuzzy sets on their own.

Once we have fuzzy subsets, we can also discuss unions, intersections and the like. Some sample definitions are as follows.

Definition 8.7.3. Let X be a non-empty set, and let A and B be fuzzy subsets of X.

1. The **empty fuzzy subset** in X, denoted $\emptyset$, is defined by $\mu_\emptyset(x) = 0$ for all $x \in X$.
2. The fuzzy subset A is a **subset** of the fuzzy subset B if $\mu_A(x) \leq \mu_B(x)$ for all $x \in X$.
3. The **complement** of A, denoted A', is the fuzzy subset C of X defined by $\mu_C(x) = 1 - \mu_A(x)$ for all $x \in X$.
4. The **union** of A and B, denoted $A \cup B$, is the fuzzy subset D of X defined by $\mu_D(x) = \max\{\mu_A(x), \mu_B(x)\}$ for all $x \in X$.
5. The **intersection** of A and B, denoted $A \cap B$, is the fuzzy subset E of X defined by $\mu_E(x) = \min\{\mu_A(x), \mu_B(x)\}$ for all $x \in X$.
6. The **algebraic product** of A and B, denoted $A \bullet B$, is the fuzzy subset F of X defined by $\mu_F(x) = \mu_A(x) \cdot \mu_B(x)$ for all $x \in X$.
7. The **algebraic sum** of A and B, denoted $A \oplus B$, is the fuzzy subset G of X defined by $\mu_G(x) = \mu_A(x) + \mu_B(x) - \mu_A(x) \cdot \mu_B(x)$ for all $x \in X$. $\triangle$

It is left to the reader to verify that the algebraic sum of two fuzzy subsets is indeed a fuzzy subset (the issue is that the characteristic map must have codomain $[0, 1]$). We are using some of the same notation for fuzzy subsets as for regular sets (sometimes referred to as "crisp" sets in fuzzy set literature); this notation is standard, and there is usually no confusion in a given context.

Just as we proved various properties of operations on regular sets in Section 3.3, we can prove similar properties for operations on fuzzy subsets. For example, we have the following Distributive Law.

Lemma 8.7.4. *Let X be a non-empty set, and let A, B and C be fuzzy subsets of X. Then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

Proof. Let $x \in X$. We need to show that

$$\min\{\mu_A(x), \max\{\mu_B(x), \mu_C(x)\}\}$$
$$= \max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\}.$$

There are a number of cases. If $\mu_A(x) \leq \mu_B(x)$ and $\mu_A(x) \leq \mu_C(x)$, then

$$\min\{\mu_A(x), \max\{\mu_B(x), \mu_C(x)\}\} = \mu_A(x)$$

and

$$\max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\} = \max\{\mu_A(x), \mu_A(x)\} = \mu_A(x).$$

If $\mu_C(x) \leq \mu_A(x) \leq \mu_B(x)$, then

$$\min\{\mu_A(x), \max\{\mu_B(x), \mu_C(x)\}\} = \min\{\mu_A(x), \mu_B(x)\} = \mu_A(x)$$

and

$$\max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\} = \max\{\mu_A(x), \mu_C(x)\} = \mu_A(x).$$

The case when $\mu_B(x) \leq \mu_A(x) \leq \mu_C(x)$ is similar to the previous case, and we omit the details. If $\mu_B(x) \leq \mu_C(x) \leq \mu_A(x)$, then

$$\min\{\mu_A(x), \max\{\mu_B(x), \mu_C(x)\}\} = \min\{\mu_A(x), \mu_C(x)\} = \mu_C(x)$$

and

$$\max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\} = \max\{\mu_B(x), \mu_C(x)\} = \mu_C(x).$$

The case when $\mu_C(x) \leq \mu_B(x) \leq \mu_A(x)$ is similar to the previous case, and we omit the details. Putting all the cases together proves the desired result. $\square$

The reader's task is to conjecture and prove as many results as possible about the operations on fuzzy subsets. Which of the results in Lemma 3.2.4 and Theorem 3.3.3 have analogs for the union and intersection of fuzzy subsets, or for the algebraic sum and algebraic product of fuzzy subsets? Can similar operations be defined for indexed families of fuzzy subsets, analogously to what we saw in Section 3.4?

See [BG95] and [Zim96] for further discussion of fuzzy sets and their applications.

8.8 You Are the Professor

One of the best ways to learn something is to try to explain it to someone else. Now that you have had the opportunity to formulate and write many proofs, you are invited to take on the role of the professor in a class that teaches proofs. At the end of this section are a number of attempted proofs, all of which are actual homework exercises submitted by students. Every one of these proofs has problems, some large and some small, and your role as professor will be to critique these proofs.

In order to help you keep in mind what you need to look for as you examine these proofs, we have provided a summary of some of the common mistakes that students make in writing proofs. Try to spot as many of these mistakes as possible in the proofs provided below. And, of course, try to avoid these mistakes in your own proofs.

1. Incomplete Sentences, Undefined Symbols and Other Writing Problems

Everyone, including the most experienced mathematician, makes honest mathematical errors, but there is no excuse for careless writing. The ideas in mathematics are sometimes difficult, and there is no reason to make matters worse by taking already challenging mathematical concepts and making them even harder to follow by phrasing them with incomplete sentences and other grammatical mistakes, by using undefined symbols for variables or by engaging in other forms of sloppy writing. Mathematics must be written carefully, and in proper English (or whatever language you use), no differently from any other writing. See Section 2.6 for more about writing mathematics.

2. Quantifier Problems

The importance of using quantifiers correctly in proofs was discussed in detail in Section 2.5. It is not possible to pay too much attention to the proper use of quantifiers.

3. Failure to Strategize

In contrast to the exercises in an introductory course such as calculus, where it is possible for a good student to write the correct solutions by simply starting with the hypothesis and working things out along the way, for more advanced material such as in this text, it is crucial to strategize the outline of the proposed proof before working out the details. Before going on a long road trip to an unfamiliar place, one first gets directions and looks at a map before commencing to drive; one would not start driving in whatever direction the car happened to be parked, and then start worrying about the directions after driving for a few hours. The same is true for mathematical proofs—first one needs to know the strategy, and only then does one work on the details. Figuring out a good strategy for a particular proof often takes no less effort than figuring out the details of the proof.

4. Incorrect Strategy

The only way to prove something is to do whatever is required to achieve the goal of the proof. For example, suppose that we need to prove that a function $f: A \to B$ is injective. Then the definition of injectivity needs to be used precisely as stated, and doing so leads to the proper strategy for such proofs, which is to let $x, y \in A$ and to assume $f(x) = f(y)$, and then to deduce that $x = y$. Whatever hypotheses might be assumed about the function f (and something must be assumed, because not every function is injective), the overall strategy for the proof must be the one just mentioned for proving that a function is injective. In general, the strategy for a proof is determined by what is being proved—and not by what is being assumed. Somewhere in the proof the hypotheses are going to be used (and if not then the hypotheses are not necessary), but the nature of the proof is guided not by the hypotheses, but by the goal of the proof.

5. Missing or Disorganized Ideas

A proof is not simply a collection of arguments, it is a collection of arguments in the correct logical order, starting with the hypotheses and proceeding in a logical step-by-step fashion to the conclusion. If a proof is missing steps it will not be complete, and even if one has all the right ideas for a proof, these ideas will not add up to a valid proof if they are not presented in the correct logical order.

6. Scratch Work Substituted for the Actual Proof

Scratch work for a proof can be backwards, forwards or any combination thereof, and it is often not written in proper sentences and with correct grammar. The actual proof should be written properly, and must start with the hypotheses and end with the conclusion. It is therefore important to distinguish between the scratch work and the actual proof, which might have little resemblance to each other. Ultimately, what counts in a proof is whether the final draft stands on its own; what one does during scratch work is important to the person who does it, but it is not part of the actual proof.

7. Failure to Check the Final Draft

The last stage of writing a proof is to read over the proposed final draft *as if it were written by someone else*, to see if it works as written. Does every step follow from the previous step? Are all symbols appropriately defined? Is a valid strategy being followed? Are the definitions being used correctly? Is the grammar correct? Is the proof clearly written? If the answer to any of these questions is "no," then the proof needs revision.

Read and comment upon the following attempted proofs as if you are the professor in a class that teaches proofs. Your comments should indicate what is wrong, and give suggestions for improvement. Some of these proofs are wildly incorrect, and others are mostly correct, though with small errors of content or writing style. Photocopy the proofs or download them at `http://math.bard.edu/bloch/you_are_the_prof.pdf`, take a red pen and go at them mercilessly.

Exercise 8.8.1. [Same as Exercise 2.5.5 (1)] Prove or give a counterexample to the following statement: For each real number x, there exists a real number y such that $e^x - y > 0$.

> **Proof (A).** The statement is true. For any x we can choose $y = 0$. Since $0 < e^x$ for all x, we have that for all x we can choose a y such that $e^x - y > 0$.

> **Proof (B).** The statement is true. Let $y = 0$. Since $x \in \mathbb{R}$, therefore $e^x - y > 0$ for each x.

> **Proof (C).** The statement is true. Let $x \in \mathbb{R}$. For all x, $e^x > 0$. Let $y = 0$. For all x, $e^x - y > 0$.

Exercise 8.8.2. [Same as Exercise 5.3.4 (1)] Let A and B be sets, and let $f : A \to B$ be a function. Let $\sim$ be the relation on A defined by $x \sim y$ if and only if $f(x) = f(y)$, for all $x, y \in A$. Prove that $\sim$ is an equivalence relation.

> **Proof (A).** We will prove that $\sim$ is reflexive. Suppose that $x \sim x$. Then $f(x) = f(x)$, for $x \in A$. Suppose that $f(x) = f(x)$, then $x \sim x$. Hence $\sim$ is reflexive.

> **Proof (B).** We will prove that $\sim$ is symmetric. Suppose that $f(x) = f(y)$. Then $f(y) = f(x)$. So $x \sim y$ and $y \sim x$. Now suppose that $f(x) \neq f(y)$. Then $f(y) \neq f(x)$. So $x \nsim y$ and $y \nsim x$. So $x \sim y$ if and only if $y \sim x$; that is, $\sim$ is symmetric.

> **Proof (C).** We will prove that $\sim$ is transitive. Since $f(x) = f(x)$, $x \sim x$ so $\sim$ is reflexive. If $z \in A$ and $f(x) = f(y) = f(z)$ then $x \sim y$ and $y \sim z$ implies $x \sim z$, so $\sim$ is transitive.

Exercise 8.8.3. [Same as Exercise 3.3.11] Let X be a set, and let $A, B, C \subseteq X$ be subsets. Suppose that $A \cap B = A \cap C$, and that $(X - A) \cap B = (X - A) \cap C$. Prove that $B = C$.

Proof (A). First, we show that $B \subseteq C$. Let $p \in A \cap B$. This means that $p \in A$ and $p \in B$. Since $A \cap B = A \cap C$, $A \cap B \subseteq A \cap C$ and $A \cap C \subseteq A \cap B$. That means that $p \in A \cap B$ implies $p \in A \cap C$. Since $p \in A \cap C$, it follows that $p \in C$. Because $p \in A \cap B$ means that $p \in B$, $p \in B$ implies $p \in C$. Therefore $B \subseteq C$.

Second, we show that $C \subseteq B$. Let $p \in (X - A) \cap C$. This means that $p \in C$. Since $(X - A) \cap C = (X - A) \cap B$, we know that $(X - A) \cap C \subseteq (X - A) \cap B$. This means that $p \in (X - A) \cap C$ implies $p \in (X - A) \cap B$. Since $p \in (X - A) \cap B$, it can be said that $p \in B$. Since $p \in (X - A) \cap C$ means $p \in C$, $p \in C$ implies $p \in B$. Therefore $C \subseteq B$.

We have shown both that $B \subseteq C$ and $C \subseteq B$. Therefore, $B = C$.

Proof (B). First, I will show that $B \subseteq C$. Let $x \in B$.

Considering $A \cap B = A \cap C$, $x \in A \cap B$ implies that $x \in A \cap C$. According to Theorem 3.3.3 (1), $A \cap B \subseteq B$ and $A \cap C \subseteq C$. Since $A \cap B = A \cap C$, it can be said that $A \cap B \subseteq C$. Since $x \in A \cap B$ and therefore $x \in B$, and $A \cap B \subseteq C$, x is therefore also an element of C in the case that $A \cap B = A \cap C$.

Likewise, $(X - A) \cap B = (X - A) \cap C$ implies that a given element x exists in $(X - A) \cap B$ and $(X - A) \cap C$. Therefore $x \notin A$ and $x \in B$. Also, according to Theorem 3.3.3, $(X - A) \cap C \subseteq C$. Since $(X - A) \cap C = (X - A) \cap B$, then $(X - A) \cap B \subseteq C$. This implies that there is an element $x \in (X - A) \cap B$ and $x \in C$. The phrase $x \in (X - A) \cap B$ can be further broken down to $x \notin A$ and $x \in B$. Therefore $B \subseteq C$, regardless of whether $x \in A$ or $x \notin A$.

To prove that $C \subseteq B$, it suffices to show that element $y \in C$ implies $y \in B$. Take $(X - A) \cap B = (X - A) \cap C$. Then $y \in (X - A) \cap B$, and thus $y \in B$ and $y \notin A$. According to Theorem 3.3.3, $(X - A) \cap B \subseteq B$. Since $(X - A) \cap B = (X - A) \cap C$, then $(X - A) \cap C \subseteq B$. This implies that $y \notin A$ and $y \in C$. Also $y \in B$. Therefore, $C \subseteq B$. If $B \subseteq C$ and $C \subseteq B$, then $B = C$.

Proof (C). Let $x \in A \cap B$. Then $x \in A$ and $x \in B$. Also let $x \in A \cap C$, then $x \in A$ and $x \in C$. This shows that $x \in A$, B and C. Since $(X - A) \cap B = (X - A) \cap C$, then $x \in X$ and $x \notin A$ and $x \in B$ and $x \in X$ and $x \notin A$ and $x \in C$ are equivalent. Therefore $x \in X$, B, and C and $x \notin A$. By Theorem 3.3.3, $A \cap B \subseteq A$ and $A \cap B \subseteq B$, and $A \cap C \subseteq A$ and $A \cap C \subseteq C$. However, since $x \notin A$, then $B = C$.

Exercise 8.8.4. [Same as Exercise 4.2.11] Let A and B be sets, let $P, Q \subseteq A$ be subsets and let $f \colon A \to B$ be a function.

(1) Prove that $f(P) - f(Q) \subseteq f(P - Q)$.
(2) Is it necessarily the case that $f(P - Q) \subseteq f(P) - f(Q)$? Give a proof or a counterexample.

Proof (A).

(1). Let $b \in B$. By Definition 4.2.1, there is some $x \in f(P) - f(Q)$ such that $b \in B$ is also $b \in f(P) - f(Q)$. By definition of $f(P)$, there is some $p \in P$ and $q \in Q$ such that $b \in f(p)$ and $b \notin f(q)$. This means that there is $a \in A$ such that $a \in p$ and $a \notin q$. Thus $a \in p - q$, and therefore $b \in f(p - q)$. Thus, $x \in f(P - Q)$. Thus $f(P) - f(Q) \subseteq f(P - Q)$.

(2). It is also the case that $f(P - Q) \subseteq f(P) - f(Q)$. Let $b \in B$. By Definition 4.2.1, there exists x such that $x \in f(P - Q)$ in which there exist elements $p \in P$ and $q \in Q$ such that $b \in f(p - q)$. Therefore $b \in f(p)$ and $b \notin f(q)$. Therefore $x \in f(P)$ and $x \notin f(Q)$, and thus $x \in f(P) - f(Q)$.
  Therefore $x \in f(P - Q)$ implies that $x \in f(P) - f(Q)$. Thus $f(P - Q) \subseteq f(P) - f(Q)$.

Proof (B).

(1). Let $f(x) \in f(P) - f(Q)$. This implies that $f(x) \in f(P)$ and $f(x) \notin f(Q)$, and thus that $x \in P$ and $x \notin Q$. It follows that $x \in P - Q$ and that $f(x) \in f(P - Q)$.

(2). Let $f(y) \in f(P - Q)$. This implies that $y \in P - Q$ and thus that $y \in P$ and $y \notin Q$. Hence, $f(y) \in f(P)$ and $f(y) \notin f(Q)$, and $f(y) \in f(P) - f(Q)$.

Proof (C).

(1). Let $f \colon A \to B$ be a function, and let $x \in f(P) - f(Q)$. So, by the definition of the image, it follows that $f(x) \in P$ and $f(x) \notin Q$. Therefore by definition of the image, $f(x) \in P - Q$, and $x \in f(P - Q)$. So $f(P) - f(Q) \subseteq f(P - Q)$.

(2). Now let $x \in f(P - Q)$. So, by the definition of the image, $f(x) \in P - Q$. This means that $f(x) \in P$ and $f(x) \notin Q$. This implies that $x \in f(P)$ and $x \notin f(Q)$. Therefore $x \in f(P) - f(Q)$. It follows that $f(P - Q) \subseteq f(P) - f(Q)$.

Proof (D).

(1). Let $k \in f(P) - f(Q)$. This means that $k \in f(P)$ and $k \notin f(Q)$. By Definition 4.2.1 this means that $k = f(p)$ for all $p \in P$ and that $k \neq f(q)$ for any $q \in Q$. Since $k = f(p)$ for all $p \in P$ and $k \neq f(q)$ for all $q \in Q$, it follows that $f(p) \neq f(q)$. Because of Definition 4.2.1, which states that in a function $f: A \to B$ each $a \in A$ maps to only one $b \in B$ and each $b \in B$ has only one $a \in A$ that maps to it, the fact that $f(p) \neq f(q)$ implies that $p \neq q$. Because $p \neq q$ for all $q \in Q$, it follows that $p \notin Q$. Since $p \in P$ and $p \notin Q$, we can derive that $p \in P - Q$. This means that $f(p) \in f(P - Q)$, which means that $k \in f(P - Q)$. Since $k \in f(P) - f(Q)$ implies $k \in f(P - Q)$, it follows that $f(P) - f(Q) \subseteq f(P - Q)$.

(2). Let $b \in f(P - Q)$. By Definition 4.2.1, there is some $r \in P - Q$ such that $b = f(r)$. Also, $r \in P$ and $r \notin Q$ by Definition 3.3.6. Because $b \in B$, $b = f(r)$, and $r \in P$, we know from Definition 4.2.1 (1) that $b \in f(P)$. Similarly, since $b \in B$, $b = f(r)$, and $r \notin Q$, we know that $b \notin f(Q)$. Since $r \in f(P)$ and $r \notin f(Q)$, then $r \in f(P) - f(Q)$ from Definition 3.3.6. Therefore $f(P - Q) \subseteq f(P) - f(Q)$.

Proof (E).

(1). Let $x \in f(P) - f(Q)$. Then $x \in f(P)$ but $x \notin f(Q)$. By the definition of image, $x \in B$, and $x = f(p)$ for all $p \in P$. But $x \neq f(q)$ for any $q \in Q$.
   For convenience, we assign $P - Q = Z$. If $x \in f(Z)$, then $x = f(z)$ for $z \in Z$. We know that for $p \in P$, $p \notin Q$ because that would make $x = f(q)$ true, which we have shown is a false statement. Therefore, $x = f(p)$ for $p \in P - Q$. It follows that $x \in f(P - Q)$. We have shown that $x \in f(P) - f(Q)$ and $x \in f(P - Q)$. Hence, $f(P) - f(Q) \subseteq f(P - Q)$.

(2). First, we prove that if $x = f(a)$ for some $a \in P$ and $a \notin Q$ then $x \neq f(b)$ for any $b \in Q$. This is a proof by contradiction. Suppose $x = f(a)$ for some $a \in P$ and $a \notin Q$, and that $x = f(b)$ for some $b \in Q$. We have reached our contradiction since $x = f(a)$ for some $a \in P$ and $a \notin Q$. This contradicts the fact that $x = f(b)$ for some $b \in Q$. Therefore $x \neq f(b)$ for any $b \in Q$.
   We now prove that $f(P - Q) \subseteq f(P) - f(Q)$. Let $x \in f(P - Q)$. We will show that $x \in f(P) - f(Q)$. Hence, $x = f(a)$ for some $a \in P - Q$, by definition of image. It follows that $x = f(a)$ for some $a \in P$ and $a \notin Q$ from the definition of set difference. Hence, $x \neq f(b)$ for any $b \in Q$ by the previous paragraph. Notice that $x = f(a)$ for some $a \in P$ and $x \neq f(b)$ for any $b \in Q$. Thus, $x \in f(P)$ and $x \notin f(q)$ by the definition of image. It follows that $x \in f(P) - f(Q)$ from the definition of set difference. Therefore, we conclude that $f(P - Q) \subseteq f(P) - f(Q)$.

Exercise 8.8.5. [Same as Exercise 5.1.11 (1)] Let A and B be sets, let R and S be relations on A and B, respectively, and let $f: A \rightarrow B$ be a function. The function f is **relation preserving** if $x R y$ if and only if $f(x) S f(y)$, for all $x, y \in A$.

Suppose that f is bijective and relation preserving. Prove that f^{-1} is relation preserving.

Proof (A). Let $p, q \in B$ such that $p S q$. Let $m, n \in A$ such that $f^{-1}(p) = m$ and $f^{-1}(q) = n$. Note that $f(m) = p$ and $f(n) = q$. Hence $f(m) S f(n)$. Since f is relation preserving, thus $f(m) S f(n)$ implies $m S n$ for all $m, n \in A$. Thus $f^{-1}(p) R f^{-1}(q)$. Therefore, if $x S y$, then $f^{-1}(x) R f^{-1}(y)$ for all $x, y \in B$.

Suppose $f^{-1}(p) R f^{-1}(q)$ for some $p, q \in B$. Let $m, n \in A$ such that $f^{-1}(p) = m$ and $f^{-1}(q) = n$. Thus $m R n$. Since f is relation preserving, thus $m R n$ implies $f(m) S f(n)$ for all $m, n \in A$. Observe that $f(m) = p$ and $f(n) = q$, hence $p S q$. Therefore if $f^{-1}(x) R f^{-1}(y)$, then $x S y$ for all $x, y \in B$.

Therefore f^{-1} is relation preserving.

Proof (B). Since f is relationship preserving, we know that $x R y$ if and only if $f(x) S f(y)$. So $f(x) S f(y)$ if and only if $x R y$, for all $x, y \in A$ and all $f(x), f(y) \in B$. So f^1 is relationship preserving.

Proof (C). Define f^{-1} as the function $g: B \rightarrow A$. Let $w, z \in B$. Because g is the inverse of f, then let $w = f(x)$ and let $z = f(y)$. Thus $w = f(x)$ and $z = f(y)$. Because $f(x) S f(y)$, then $w S z$. Then $f(w) = f^{-1}(f(x)) = x$ and $f(z) = f^{-1}(f(y)) = y$. Because $x R y$, then $f(w) R f(z)$. Therefore if $w S z$ if and only if $f(w) R f(z)$. Therefore f^{-1} is relation preserving.

Proof (D). Suppose $f^{-1}: B \rightarrow A$. Let $m, n \in B$. Suppose $m S n$. Because f is both injective and relation preserving for all $x, y \in A$, $f(x) S f(y)$. Hence, $f(x)$ and $f(y)$ both correspond to elements in B, namely, some $m, n \in B$. Therefore, because $f(x) S f(y)$ implies $x R y$, $m S n$ implies $f(m) R f(n)$ for all $m, n \in B$. Suppose $f(m) R f(n)$. Hence, $f(m)$ and $f(n)$ both correspond to elements in A namely, some $x, y \in A$. Therefore, because $x R y$ implies $f(x) S f(y)$, $f(m) R f(n)$ implies $m S n$. Therefore f^{-1} is relation preserving.

Proof (E). We begin by assuming that $f: A \to B$ is a bijective relation preserving function. Since f is bijective, we know there exists a bijective inverse function $f^{-1}: B \to A$ by Theorem 4.4.5. Since f^{-1} is bijective, by definition we know it is both injective and surjective. Let $p, q \in B$ and suppose that $f^{-1}(p) = f^{-1}(q)$. Since f^{-1} is injective, then $f^{-1}(p) = f^{-1}(q)$ implies that $p = q$ for all $p, q \in B$. Hence $f^{-1}(p) R f^{-1}(q)$ implies $p S q$ for all $p, q \in B$. Let $c \in A$. Let $a = b$ for all $a, b \in B$. Since f^{-1} is surjective there exists some a, b such that $f(a) = c = f(b)$. Therefore, $f(a) = f(b)$. Hence $a S b$ implies $f^{-1}(a) R f^{-1}(b)$ for all $a, b \in B$. Hence $x S y$ if and only if $f^{-1}(x) R f^{-1}(y)$ for all $x, y \in B$. Thus f^{-1} is relation preserving.

Appendix

Properties of Numbers

Throughout this book we have assumed an informal familiarity with the standard number systems used in high school mathematics. In this appendix we briefly summarize some of the commonly used properties of these number systems. A rigorous treatment of these number systems, including proofs of everything stated in this appendix, can be found in [Blo11, Chapters 1 and 2].

All the numbers we deal with in this book are real numbers. In particular, we do not make use of complex numbers. We standardly think of the real numbers as forming the real number line, which extends infinitely in both positive and negative directions. The real numbers have the operations addition, multiplication, negation and reciprocal, and the relations $<$ and $\leq$. (The real numbers also have the operations subtraction and division, but we do not focus on them in this appendix because they can be defined in terms of addition and multiplication, respectively.) Among the most important properties of the real numbers are the following.

Theorem A.1. *Let x, y and z be real numbers.*

1. $(x+y)+z = x+(y+z)$ *and* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(Associative Laws).*
2. $x+y = y+x$ *and* $x \cdot y = y \cdot x$ *(Commutative Laws).*
3. $x+0 = x$ *and* $x \cdot 1 = x$ *(Identity Laws).*
4. $x+(-x) = 0$ *(Inverses Law).*
5. *If* $x \neq 0$*, then* $x \cdot x^{-1} = 1$ *(Inverses Law).*
6. *If* $x+z = y+z$*, then* $x = y$ *(Cancellation Law).*
7. *If* $z \neq 0$*, then* $x \cdot z = y \cdot z$ *if and only if* $x = y$ *(Cancellation Law).*
8. $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$ *(Distributive Law).*
9. $-(-x) = x$ *(Double negation).*
10. $-(x+y) = (-x) + (-y)$.
11. $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$.
12. *If* $x < y$ *and* $y < z$*, then* $x < z$ *(Transitive Law).*
13. *Precisely one of the following holds: either* $x < y$*, or* $x = y$*, or* $x > y$ *(Trichotomy Law).*

14. *If $x \leq y$ and $y \leq x$, then $x = y$ (Antisymmetry Law).*
15. *$x < y$ if and only if $x + z < y + z$.*
16. *If $z > 0$, then $x < y$ if and only if $x \cdot z < y \cdot z$.*

We mention here two additional facts about the real numbers, which we will need in Section 7.8, though nowhere else. These facts involve the absolute value of real numbers, which was defined in Exercise 2.4.9. A proof of the first of these facts may be found in [Blo11, Lemma 2.3.9]; the second fact can be deduced from the first without too much difficulty.

Theorem A.2. *Let $x, y \in \mathbb{R}$.*

1. *$|x + y| \leq |x| + |y|$ (Triangle Inequality).*
2. *$|x| - |y| \leq |x + y|$ and $|x| - |y| \leq |x - y|$.*

There are three particularly useful subsets of the real numbers, namely, the natural numbers, the integers and the rational numbers.

The set of natural numbers is the set

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}.$$

The sum and product of any two natural numbers is also a natural number, though the difference and quotient of two natural numbers need not be a natural number. Being real numbers, the natural numbers satisfy all the properties of real numbers listed above. The natural numbers also satisfy a number of special properties not satisfied by the entire set of real numbers, for example the ability to do proof by induction; see Section 6.2 for more about the natural numbers.

We mention here one additional property of the natural numbers, which we will need in Section 7.8, though again nowhere else. This property, rather than being about the natural numbers themselves, refers to the way that the natural numbers sit inside the real number.

Theorem A.3. *Let $x \in \mathbb{R}$. Then there is some $n \in \mathbb{N}$ such that $x < n$.*

This theorem may seem intuitively obvious, but it is not trivial to prove, because its proof relies upon the Least Upper Bound Property of the real numbers. It would take us too far afield to discuss the Least Upper Bound Property, but we will mention that it is the property of the set of real numbers that distinguish that set from the set of rational numbers; there is no difference between these two sets in terms of algebraic properties of addition, subtraction, multiplication and division. See [Blo11, Section 2.6] for a discussion of the Least Upper Bound Property in general, and a proof of Theorem A.3 in particular.

The set of integers is the set

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

The sum, difference and product of any two integers is also an integer, though the quotient of two integers need not be an integer. Being real numbers, the integers satisfy all the properties of real numbers listed above.

We will need two additional properties of the integers; these properties do not hold for all real numbers. Our first property, given in the following theorem, is very evident intuitively, though it requires a proof; see [Blo11, Exercise 2.4.4] for details.

Theorem A.4. *Let $a, b \in \mathbb{Z}$. If $ab = 1$, then $a = 1$ and $b = 1$, or $a = -1$ and $b = -1$.*

Our second property of the integers, which is much less obviously true than the previous property, is known as the Division Algorithm, though it is not an algorithm (the name is simply historical). See [Ros05, Section 1.5] for a proof.

Theorem A.5 (**Division Algorithm**). *Let $a, b \in \mathbb{Z}$. Suppose that $b \neq 0$. Then there are unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.*

The set of rational numbers, denoted $\mathbb{Q}$, is the set of all real numbers that can be expressed as fractions. That is, a real number x is rational if $x = \frac{a}{b}$ for some integers a and b, where $b \neq 0$. Clearly, a rational number can be represented in more than one way as a fraction, for example $\frac{1}{2} = \frac{3}{6}$. However, as we now state, there is always a particularly convenient representation of each rational number, namely, writing it in "lowest terms." This latter concept is phrased using the notion of integers being relatively prime, as defined in Exercise 2.4.3. The following theorem can be proved using the Fundamental Theorem of Arithmetic, which is found in [Ros05, Section 3.5]; a proof of the following theorem is also found in [Olm62, Section 402 and Section 404].

Theorem A.6. *Let $x \in \mathbb{Q}$. Suppose that $x \neq 0$. There are $a, b \in \mathbb{Z}$ such that $x = \frac{a}{b}$ and a and b are relatively prime. The integers a and b are unique up to negation.*

It can be shown that the rational numbers are precisely those real numbers that have decimal expansions that are either repeating, or are zero beyond some point; see [Blo11, Section 2.8] for a proof. The sum, difference, product and quotient of any two rational numbers is also a rational number, except that we cannot divide by zero. The rational numbers are not all the real numbers; for example, the number $\sqrt{2}$ is not rational, as is proved in Theorem 2.3.5. Again, being real numbers, the rational numbers satisfy all the properties of real numbers listed above.

The rational numbers also satisfy some additional nice properties, for example, they are "dense" in the real number line, which means that between any two real numbers, no matter how close, we can always find a rational number; see [Blo11, Theorem 2.6.13] for a proof. We will rarely make use of such facts.

References

[AR89] R. B. J. T. Allenby and E. J. Redfern, *Introduction to Number Theory with Computing*, Edward Arnold, London, 1989.

[ASY97] Kathleen Alligood, Tim Sauer, and James Yorke, *Chaos: An Introduction to Dynamical Systems*, Springer-Verlag, New York, 1997.

[Ang94] W. S. Anglin, *Mathematics: A Concise History and Philosophy*, Springer-Verlag, New York, 1994.

[AR05] Howard Anton and Chris Rorres, *Elementary Linear Algebra, Applications Version*, 9th ed., John Wiley & Sons, New York, 2005.

[AM75] Michael Arbib and Ernst Manes, *Arrows, Structures and Functors: The Categorical Imperative*, Academic Press, New York, 1975.

[Arm88] M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, New York, 1988.

[Ave90] Carol Avelsgaard, *Foundations for Advanced Mathematics*, Scott, Foresman, Glenview, IL, 1990.

[BG95] Hans Bandemer and Siegfried Gottwald, *Fuzzy Sets, Fuzzy Logic, Fuzzy Methods*, John Wiley & Sons, New York, 1995.

[Bir48] Garrett Birkhoff, *Lattice Theory*, AMS Colloquium Publications, vol. 25, American Mathematical Society, New York, 1948.

[Blo11] Ethan D. Bloch, *The Real Numbers and Real Analysis*, Springer-Verlag, New York, 2011.

[Blo87] Norman J. Bloch, *Abstract Algebra with Applications*, Prentice Hall, Englewood Cliffs, NJ, 1987.

[Bog90] Kenneth Bogart, *Introductory Combinatorics*, 2nd ed., Harcourt, Brace, Jovanovich, San Diego, 1990.

[Boy91] Carl Boyer, *A History of Mathematics*, 2nd ed., John Wiley & Sons, New York, 1991.

[Bur85] R. P. Burns, *Groups: A Path to Geometry*, Cambridge University Press, Cambridge, 1985.

[CW00] Neil Calkin and Herbert S. Wilf, *Recounting the rationals*, Amer. Math. Monthly **107** (2000), no. 4, 360–363.

[Cop68]   Irving Copi, *Introduction to Logic*, 3rd ed., Macmillan, New York, 1968.

[Cox61]   H. S. M. Coxeter, *Introduction to Geometry*, John Wiley & Sons, New York, 1961.

[CD73]   Peter Crawley and Robert Dilworth, *Algebraic Theory of Lattices*, Prentice Hall, Englewood Cliffs, NJ, 1973.

[DSW94]   Martin Davis, Ron Sigal, and Elaine Weyuker, *Computability, Complexity, and Languages*, 2nd ed., Academic Press, San Diego, 1994.

[DHM95]   Phillip Davis, Reuben Hersh, and E. A. Marchisotto, *The Mathematical Experience*, Birkhäuser, Boston, 1995.

[Dea66]   Richard Dean, *Elements of Abstract Algebra*, John Wiley & Sons, New York, 1966.

[Deb]   Gerard Debreu, *Four aspects of the mathematical theory of economic equilibrium*, Studies in Mathematical Economics (Stanley Reiter, ed.), Mathematical Association of America, Washington, DC, 1986.

[Dev93]   Keith Devlin, *The Joy of Sets*, 2nd ed., Springer-Verlag, New York, 1993.

[Die92]   Jean Dieudonné, *Mathematics—the Music of Reason*, Springer-Verlag, Berlin, 1992.

[Dub64]   Roy Dubisch, *Lattices to Logic*, Blaisdell, New York, 1964.

[EFT94]   H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical Logic*, 2nd ed., Springer-Verlag, New York, 1994.

[End72]   Herbert Enderton, *A Mathematical Introduction to Logic*, Academic Press, New York, 1972.

[End77]   Herbert B. Enderton, *Elements of Set Theory*, Academic Press, New York, 1977.

[Epp90]   Susanna Epp, *Discrete Mathematics with Applications*, Wadsworth, Belmont, CA, 1990.

[EC89]   Richard Epstein and Walter Carnielli, *Computability: Computable Functions, Logic, and the Foundations of Mathematics*, Wadsworth & Brooks/Cole, Pacific Grove, CA, 1989.

[Fab92]   Eugene D. Fabricus, *Modern Digital Design and Switching Theory*, CRC Press, Boca Raton, FL, 1992.

[FR90]   Daniel Fendel and Diane Resek, *Foundations of Higher Mathematics*, Addison-Wesley, Reading, MA, 1990.

[FP92]   Peter Fletcher and C. Wayne Patty, *Foundations of Higher Mathematics*, PWS-Kent, Boston, 1992.

[Fra03]   John Fraleigh, *A First Course in Abstract Algebra*, 7th ed., Addison-Wesley, Reading, MA, 2003.

[Gal74]   Galileo Galilei, *Two New Sciences*, University of Wisconsin Press, Madison, 1974.

[Gar87]   Trudi Garland, *Fascinating Fibonaccis*, Dale Seymour, Palo Alto, 1987.

[Ger96]   Larry Gerstein, *Introduction to Mathematical Structures and Proofs*, Springer-Verlag, New York, 1996.

[GG88]   Jimmie Gilbert and Linda Gilbert, *Elements of Modern Algebra*, 2nd ed., PWS-Kent, Boston, 1988.

[Gil87]   Leonard Gillman, *Writing Mathematics Well*, Mathematical Association of America, Washington, DC, 1987.

[GKP94]   Ronald Graham, Donald Knuth, and Oren Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, Reading, MA, 1994.

[GG94]   I. Grattan-Guinness (ed.), *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, Vol. 1, Routledge, London, 1994.

[Hal60]   Paul Halmos, *Naive Set Theory*, Van Nostrand, Princeton, NJ, 1960.

[Ham82]   A. G. Hamilton, *Numbers, Sets and Axioms*, Cambridge University Press, Cambridge, 1982.

[Har96]   Leon Harkleroad, *How mathematicians know what computers can't do*, College Math. J. **27** (1996), 37–42.

[Hea21]   Thomas Heath, *A History of Greek Mathematics, Vols. I and II*, Dover, New York, 1921.

[Her97]   Reuben Hersh, *What is Mathematics, Really?*, Oxford University Press, New York, 1997.

[Her75]   I. N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley & Sons, New York, 1975.

[Hig98]   Nicholas J. Higham, *Handbook of Writing for the Mathematical Sciences*, 2nd ed., Society for Industrial and Applied Mathematics (SIAM), Philadelphia, 1998.

[HHP97]   Peter Hilton, Derek Holton, and Jean Pedersen, *Mathematical Reflections*, Springer-Verlag, New York, 1997.

[HJ99]   Karel Hrbacek and Thomas Jech, *Introduction to Set Theory*, 3rd ed., Monographs and Textbooks in Pure and Applied Mathematics, vol. 220, Marcel Dekker, New York, 1999.

[HW91]   John H. Hubbard and Beverly H. West, *Differential Equations: A Dynamical Systems Approach*, Part I: Ordinary Differential Equations, Springer-Verlag, New York, 1991.

[Hud00]   Paul Hudak, *The Haskell School of Expression: Learning Functional Programming through Multimedia*, Cambridge University Press, Cambridge, 2000.

[Hun70]   H. E. Huntley, *The Divine Proportion*, Dover, New York, 1970.

[Ifr85]   Georges Ifrah, *From One to Zero: A Universal History of Numbers*, Viking, New York, 1985.

[KMM80]   Donald Kalish, Richard Montague, and Gary Mar, *Logic: Techniques of Formal Reasoning*, 2nd ed., Harcourt, Brace, Jovanovich, New York, 1980.

[KR83a]   Ki Hang Kim and Fred Roush, *Applied Abstract Algebra*, Ellis Horwood, Chichester, 1983.

[KR83b]   K. H. Kim and F. W. Roush, *Competitive Economics: Equilibrium and Arbitration*, North-Holland, Amsterdam, 1983.

[Knu73]   Donald E. Knuth, *The Art of Computer Programming, Volume 1: Fundamental Algorithms*, 2nd ed., Addison-Wesley, Reading, MA, 1973.

[KLR89]   Donald Knuth, Tracy Larrabee, and Paul Roberts, *Mathematical Writing*, Mathematical Association of America, Washington, DC, 1989.

[Kob87]   Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.

[Kri81]   V. Sankrithi Krishnan, *An Introduction to Category Theory*, North-Holland, New York, 1981.

[Lev02]   Azriel Levy, *Basic Set Theory*, Dover, New York, 2002.

[LP98]   Rudolf Lidl and Günter Pilz, *Applied Abstract Algebra*, 2nd ed., Springer-Verlag, New York, 1998.

[Loo40]   Elisha Loomis, *The Pythagorean Proposition*, Edwards Brothers, Ann Arbor, 1940.

[Mac96]   Moshé Machover, *Set Theory, Logic and Their Limitations*, Cambridge University Press, Cambridge, 1996.

[Mal79]   Jerome Malitz, *Introduction to Mathematical Logic*, Springer-Verlag, New York, 1979.

[Moo82]   Gregory H. Moore, *Zermelo's Axiom of Choice*, Springer-Verlag, New York, 1982.

[Mor87]   Ronald P. Morash, *Bridge to Abstract Mathematics*, Random House, New York, 1987.

[Mos06]   Yiannis Moschovakis, *Notes on Set Theory*, 2nd ed., Springer-Verlag, New York, 2006.

[Mun00]   J. R. Munkres, *Topology*, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 2000.

[Myc06]   Jan Mycielski, *A system of axioms of set theory for the rationalists*, Notices Amer. Math. Soc. **53** (2006), no. 2, 206–213.

[Nab80]   Gregory Naber, *Topological Methods in Euclidean Spaces*, Cambridge University Press, Cambridge, 1980.

[Olm62]   John M. H. Olmsted, *The Real Number System*, Appleton-Century-Crofts, New York, 1962.

[OZ96]   Arnold Ostebee and Paul Zorn, *Instructor's Resource Manual for Calculus from Graphical, Numerical, and Symbolic Points of View*, Vol. 1, Saunders, Fort Worth, 1996.

[Pie91]   Benjamin Pierce, *Basic Category Theory for Computer Scientists*, MIT Press, Cambridge, MA, 1991.

[Pit93]   Jim Pitman, *Probability*, Springer-Verlag, New York, 1993.

[Pot04]   Michael D. Potter, *Set Theory and its Philosophy: A Critical Introduction*, Oxford University Press, Oxford, 2004.

[Pou99]   Bruce Pourciau, *The education of a pure mathematician*, Amer. Math. Monthly **106** (1999), 720–732.

[Rib96]   Paulo Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, New York, 1996.

[Rob86]   Eric Roberts, *Thinking Recursively*, John Wiley & Sons, New York, 1986.

[Rob84]   Fred Roberts, *Applied Combinatorics*, Prentice Hall, Englewood Cliffs, NJ, 1984.

[Ros05]   Kenneth H. Rosen, *Elementary Number Theory*, 5th ed., Addison-Wesley, Reading, MA, 2005.

[Ros10]   Sheldon Ross, *A First Course in Probability*, 8th ed., Prentice Hall, Upper Saddle River, NJ, 2010.

[Rot73]   Joseph J. Rotman, *Theory of Groups*, 2nd ed., Allyn & Bacon, Boston, 1973.

[Rot96]   ———, *An Introduction to the Theory of Groups*, 4th ed., Springer-Verlag, New York, 1996.

[RR85]   Herman Rubin and Jean E. Rubin, *Equivalents of the Axiom of Choice. II*, Studies in Logic and the Foundations of Mathematics, vol. 116, North-Holland, Amsterdam, 1985.

[Rus19]   Bertrand Russell, *Introduction to Mathematical Philosophy*, Allen & Unwin, London, 1919.

[Rya86]   Patrick J. Ryan, *Euclidean and Non-Euclidean Geometry*, Cambridge University Press, New York, 1986.

[Sch]   Eric Schechter, *A Home Page for the Axiom of Choice*, `http://www.math.vanderbilt.edu/~schectex/ccc/choice.html`.

[Set96]   Ravi Sethi, *Programming Languages: Concepts and Constructs*, 2nd ed., Addison-Wesley, Reading, MA, 1996.

[SHSD73] N. E. Steenrod, P. R. Halmos, M. M. Schiffer, and J. A. Dieudonné, *How to Write Mathematics*, Amer. Math. Soc., Providence, 1973.

[Ste58]   M. A. Stern, *Über eine zahlentheoretische Funktion*, J. Reine Angew. Math. **55** (1858), 193–220.

[Sto79]   Robert R. Stoll, *Set Theory and Logic*, Dover, New York, 1979. Corrected reprint of the 1963 edition.

[Str87]   Dirk J. Struik, *A Concise History of Mathematics*, 4th ed., Dover, New York, 1987.

[Sup60]   Patrick Suppes, *Axiomatic Set Theory*, Van Nostrand, Princeton, 1960.

[Szá63]   Gábor Szász, *Introduction to Lattice Theory*, Academic Press, New York, 1963.

[Tho59]   D'Arcy Wentworth Thompson, *On Growth and Form*, 2nd ed., Vol. 2, Cambridge University Press, Cambridge, 1959.

[Tru87]   Richard Trudeau, *The Non-Euclidean Revolution*, Birkhäuser, Boston, 1987.

[Vau95]   Robert Vaught, *Set Theory*, 2nd ed., Birkhäuser, Boston, 1995.

[WW98]   Edward Wallace and Stephen West, *Roads to Geometry*, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 1998.

[Wea38]   Warren Weaver, *Lewis Carroll and a geometrical paradox*, Amer. Math. Monthly **45** (1938), 234–236.

[Wil65]   Raymond Wilder, *An Introduction to the Foundations of Mathematics*, John Wiley & Sons, New York, 1965.

[Zim96]   H.-J. Zimmermann, *Fuzzy Set Theory and its Applications*, 3rd ed., Kluwer Academic Publishers, Boston, 1996.

Index

△
△ △
Ethan
Bloch was
born in 1956,
and spent part of
his childhood in Con-
necticut and part in Is-
rael. He received a B.A. in
mathematics in 1978 from Reed
College, where he developed a firm
belief in the value of a liberal arts edu-
cation, and a Ph.D. in mathematics in 1983
from Cornell University, under the supervision
of Prof. David Henderson. He was an Instructor
at the University of Utah for three years, and arrived
at Bard College in 1986, where he has, very fortunately,
been ever since. He is married and has two children; his
family, his work and travel to Israel more than fill his time.

This text was written using TEXShop on a Mac. The style file is
svmono from Springer Verlag, and the fonts are mathptmx (a
free version of Times Roman with mathematical symbols)
and pzc (Zapf Chancery). Commutative diagrams were
made using the DCpic package. Most figures were
drawn with Adobe Illustrator, exported as encapsu-
lated postscript files, and converted to portable
document format by Preview; a few fig-
ures were drawn using Mathematica,
and then modified with Adobe Il-
lustrator. The labels for the fig-
ures were typeset in LATEXiT,
and exported as encapsu-
lated postscript files.
This colophon was
made with the
shapepar
package.
▽ ▽
▽