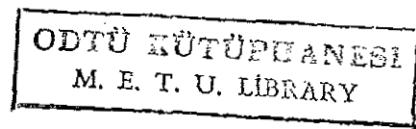


Ethan D. Bloch

Proofs and Fundamentals

A First Course in Abstract Mathematics

Birkhäuser
Boston • Basel • Berlin



QA9.54
B57
c.2

Ethan D. Bloch
Department of Mathematics
and Computer Science
Bard College
Annandale-on-Hudson, NY 12504

QA9.54 B57

METU LIBRARY

c.2

Proofs and fundamentals : a first



0020160561

311089

Library of Congress Cataloging-in-Publication Data

Bloch, Ethan D., 1956-

Proofs and fundamentals: a first course in abstract mathematics / Ethan D. Bloch.

p. cm.

Includes bibliographical references and indexes.

ISBN 0-8176-4111-4 (alk. paper) — ISBN 3-7643-4111-4 (alk. paper)

1. Proof theory. 2. Set theory. I. Title.

QA9.54.B57 2000

511.3—dc21

00-023309

CIP

Math Subject Classifications 2000: Primary 00A35; Secondary 00-01.

Printed on acid-free paper
©2000 Birkhäuser Boston

Birkhäuser ®

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Birkhäuser Boston, c/o Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

ISBN 0-8176-4111-4 SPIN 10741129
ISBN 3-7643-4111-4

Reformatted from the author's files by TE_Xniques, Inc, Cambridge, MA.
Figures recreated by Marty Stock, Watertown, MA.

Cover design by Jeff Cosloy, Newton, MA.

Printed and bound by Hamilton Printing, Rensselaer, NY.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

Contents

Introduction	ix
To the Student	xiii
To the Instructor	xix
Part I PROOFS	1
1 Informal Logic	3
1.1 Introduction	3
1.2 Statements	4
1.3 Relations Between Statements	18
1.4 Valid Arguments	31
1.5 Quantifiers	41
2 Strategies for Proofs	55
2.1 Mathematical Proofs — What They Are and Why We Need Them	55
2.2 Direct Proofs	63
2.3 Proofs by Contrapositive and Contradiction	67
2.4 Cases, and If and Only If	74

2.5 Quantifiers in Theorems	81
2.6 Writing Mathematics	93
Part II FUNDAMENTALS	105
3 Sets	107
3.1 Introduction	107
3.2 Sets — Basic Definitions	109
3.3 Set Operations	119
3.4 Indexed Families of Sets	129
4 Functions	135
4.1 Functions	135
4.2 Image and Inverse Image	145
4.3 Composition and Inverse Functions	152
4.4 Injectivity, Surjectivity and Bijectivity	161
4.5 Sets of Functions	170
5 Relations	177
5.1 Relations	177
5.2 Congruence	184
5.3 Equivalence Relations	191
6 Infinite and Finite Sets	203
6.1 Cardinality of Sets	203
6.2 Cardinality of the Number Systems	218
6.3 Mathematical Induction	226
6.4 Recursion	236
Part III EXTRAS	249
7 Selected Topics	251
7.1 Binary Operations	251
7.2 Groups	258
7.3 Homomorphisms and Isomorphisms	267
7.4 Partially Ordered Sets	273
7.5 Lattices	284
7.6 Counting: Products and Sums	294
7.7 Counting: Permutations and Combinations	304

8 Number Systems	323
8.1 Back to the Beginning	323
8.2 The Natural Numbers	324
8.3 Further Properties of the Natural Numbers	333
8.4 The Integers	338
8.5 The Rational Numbers	348
8.6 The Real Numbers and the Complex Numbers	352
8.7 Appendix: Proof of Theorem 8.2.1	361
9 Explorations	363
9.1 Introduction	363
9.2 Greatest Common Divisors	364
9.3 Divisibility Tests	366
9.4 Real-Valued Functions	367
9.5 Iterations of Functions	368
9.6 Fibonacci Numbers and Lucas Numbers	369
9.7 Fuzzy Sets	371
Appendix: Properties of Numbers	375
Hints for Selected Exercises	379
References	405
Index	413

Introduction

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 I believe 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 to distractions.

Some of 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, since 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. I believe 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, respectively. At the end of the book is a brief appendix summarizing a few basic properties of the standard number systems (integers, rational numbers, real numbers) that we use, a section of hints for selected exercises, 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 1–2, covering informal logic and proof techniques, respectively. These two chapters discuss the “how” of modern mathematics, namely 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. This material is basic to all of modern mathemat-

ics. 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 7–9, and has brief treatments of a variety of topics, including groups, homomorphisms, partially ordered sets, lattices and combinatorics, has a lengthier axiomatic treatment of some of the standard number systems, and concludes with topics for exploration by the reader.

Some instructors might choose to skip Sections 4.5 and 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, I would urge instructors not to do so. Section 4.5 is intended to help students prepare for dealing with sets of linear maps in linear algebra. Section 6.4 is a topic that is often skipped over in the mathematical education of many undergraduates, and that is unfortunate, since 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, Jesse Ross in Math 231 in the spring of 1995. Much of the inspiration (and work) for Sections 8.2–8.4 comes from the 1993 senior project at Bard of Neal Brofee.

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, Amy Cara 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: [Dea66], [Fra94], [GG88], [Blo87]; texts on posets and lattices: [Bir48], [Bog90], [CD73], [LP98]; texts 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 1974-78: 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), the former being a source for parts of Chapter 8, and the latter being the most abstract linear algebra text I have seen.

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 my 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 (contrary to a popular misconception) is 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, etc. 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 subjects in mathematics, it will be even harder to be sure whether certain ideas that seem right intuitively are indeed correct. Thus 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 and syntax, 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 you are certainly familiar. See the Appendix for a brief list of some of the standard properties of real numbers that we use. On very few occasions we give an example with matrices, though they can easily be skipped.

Exercises

Like 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, and to see what you understand and what needs further study. Exercises range from routine examples to rather tricky proofs. Some of the exercises have hints in the back of the book. Try doing the exercises by yourself prior to consulting the hints. 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 appropriately 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, etc. You 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 high school geometry classes, are not used in advanced mathematics (except for some 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 about 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. It is, for example, 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. Keep in mind at all times what the symbols and terms mean. It is the meaning in which we are ultimately interested.

Most of the symbols used in this text are completely standard. There is one case, namely the inverse image under a function of a set (as discussed in Section 4.2), where the standard notation causes a great deal of confusion, and so we provide an alternative. We have also added a few symbols that are not standard, but are analogs of the very useful (and widely used)

end-of-proof symbol, which is a \square . 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 Δ for the end of a definition, the symbol \Diamond for the end of an example, and the symbol $/\!/\!$ for the end of scratch work or other nonproofs. 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 keep in mind concerning mathematical terminology is that whereas some names are invented specifically for mathematical use (for example, “injective”), other mathematical terms are borrowed from colloquial English. For example, the words “group,” “orbit” and “relation” all have technical meanings in mathematics. 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], [Str48] 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, philo-

sophical 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 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 book we take the mainstream approach, and 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 maintain high standards in content, rigor and in writing, by both the instructor and by the students, while 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, detailed, feedback by the instructor on the homework assignments. Students can only learn from their mistakes if mistakes are not only pointed out, but if better approaches are suggested. Having students present their proofs to the class is an ad-

ditional forum for helpful feedback. Many mathematicians of my generation never had a transition course, and simply picked up the techniques of writing proofs, and fundamentals such as sets and functions, along the way when taking courses such as linear algebra and abstract algebra. What worked for many mathematicians 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.

One place where too much indulgence is given, however, even in more advanced mathematics courses, and where such indulgence is, I believe, 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. I urge 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). I have heard the argument that students in an introductory course are simply not ready for an emphasis on the proper writing of mathematics. My experience tells me otherwise: not only are students ready and able to write carefully no matter what their mathematical sophistication, but they gain much from the experience since 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.

Proofs and Fundamentals

A First Course in Abstract Mathematics

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 (especially in geometry), and do others computationally (especially in algebra); some things at the high school level are concrete and applied, whereas others are abstract. 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 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.

Herman 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, since logical ideas are at the basis of some aspects of computer science. For references to traditional logic, see [Cop68], which is very readable, and [KMM80], which is more formal. For mathematical logic, see [End72], [Mal79] or [EFT94], for example. 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 19–20]. 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. Since we only start discussing what a mathematical proof consists of 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 standard number systems will be treated more rigorously in Chapter 8. See the Appendix for a brief list of some of the standard properties of real numbers that we use.

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 thus 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, which can be either true or false. For example, the expression “Fred’s hair is brown” is a statement, since it is either true or false. We do not know

whether this statement is actually true or not, since we would need to see a picture of Fred, or another representation. For something to be a statement, it has to be either true or false in principle; that something is a statement does not depend on whether we personally can verify its truth or falsity. By contrast, the expression “Eat a pineapple” is not a statement, since 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’s hair is brown,” we could just as well have written “Fred has brown hair.” These two English expressions concerning Fred are not identical since 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’s hair is brown” 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 in this book we will not hesitate to use it. 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 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 found). 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.

Let P and Q be statements. We define the **conjunction** of P and Q , denoted $P \wedge Q$, to be 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.”

There are a few ways in which 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 $3x < 6$, so that $x < 2$.” Such a use of “and” is virtually never necessary, and since it can lead to possible confusion, it is best avoided.

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 conclude from this statement that each of Fred and Susan is married, possibly to different people. In colloquial usage, this statement would almost always be interpreted as meaning that Fred and Susan are married to each other. In literary writing, some measure of ambiguity is often valuable. In mathematics, by contrast, precision is key, and ambiguity is to be avoided at all cost. When using a mathematical term, always stick to the precise mathematical definition, regardless of any other colloquial usage.

For our next definition, once again let P and Q be statements. We define the **disjunction** of P and Q , denoted $P \vee Q$, to be 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 mathematical use of the word “or” from the colloquial use of the same 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, since it is virtually never necessary, and can lead to confusion.

For our third definition, let P be a statement. We define the **negation** of P , denoted $\neg P$, to be the statement that, intuitively, is true if P is false, and is false if P is true. We read $\neg P$ as “it is not the case that P ,” or, more simply, “not P .” The precise definition of $\neg P$ is given in the truth table

P	$\neg P$
T	F
F	T

Let $P =$ “Susan likes mushy bananas.” Then the most straightforward way of negating this statement 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.” In general, we will try to use statements that read well in English, as well as being logically correct.

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 only means 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, since 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 compo-

nent parts, 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. Thus, since 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 our approach as follows.

Let P and Q be statements. We define the **conditional** from P to Q , denoted $P \rightarrow Q$, to be the statement that, intuitively, is true if it is never the case that P is true and Q is false. We read $P \rightarrow Q$ as “if P then Q .” The precise definition of $P \rightarrow Q$ is given in the truth table

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

The first two rows of the truth table are fairly reasonable intuitively. If P is true and Q is true, then certainly $P \rightarrow Q$ should be true; if P is true and Q is false, then $P \rightarrow Q$ should be false. The third and fourth rows of the truth table, which say that the statement $P \rightarrow Q$ 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 we are primarily concerned with is that we do not want P to be true and Q to be false. Moreover, if we made the value of $P \rightarrow Q$ 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 $P \rightarrow Q$ redundant. This truth table, 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, since we will always use $P \rightarrow Q$ 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 $P \rightarrow Q$, 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 go see a movie this evening. It only says what will happen if it rains today, namely 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 $P \rightarrow Q$, it is not the order of writing that counts, but the logical relationship. It would be identical to write $Q \leftarrow P$ instead of $P \rightarrow Q$. Either way, each of P and Q have specified roles. We call P the “antecedent” of $P \rightarrow Q$, and Q the “consequent.” By contrast, if we write $Q \rightarrow P$, then we have Q as the antecedent, and P as the consequent; this statement is not equivalent to $P \rightarrow Q$, as 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.

For our final definition, let P and Q be statements. We define the biconditional from P to Q , denoted $P \leftrightarrow Q$, to be 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 $Q \leftrightarrow P$.

We can now form more complicated compound statements using our five basic operations. For example, we can form $P \vee (Q \rightarrow \neg R)$ 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. We can form the truth table for the statement $P \vee (Q \rightarrow \neg R)$, doing one operation at a time, as follows:

P	Q	R	$\neg R$	$Q \rightarrow \neg R$	$P \vee (Q \rightarrow \neg R)$
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 above truth table, 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. The final result (in column 5) refers to the compound statement in which we are interested. It is, of course, the same as in the previous truth table.

P	Q	R	$P \vee (Q \rightarrow \neg R)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	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 our original sentence can be written in symbols as $(A \vee B) \wedge C$. On the other hand, suppose 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, and thus are of no use for mathematical purposes. The ambiguity in the first statement results from the lack of necessary punctuation, and in the second statement 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 in symbols.

We end this section with a brief mention of two important concepts. A **tautology** is a statement that is necessarily true, regardless of whether anything else (such as component statements) are true or false, and regardless of what we happen to see around us in the real world. A **contradiction** is a statement that is necessarily false. 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, since 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.

A tautology is a statement that is true by virtue of logic. For example, the statement “Irene has red hair or she does not have red hair” is a tautology, which seems intuitively clear. We can use truth tables to verify this fact more formally. Let $P = \text{“Irene has red hair.”}$ Then our purported tautology is the statements $P \vee \neg P$. The truth table for this statement is

P	P	\vee	$\neg P$
T	T	T	F
F	F	T	T

1 3 2 .

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 it is always true, regardless of whether its component statements are true or false, as can be verified using a truth table.

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

P	P	\wedge	$\neg P$
T	T	F	F
F	F	F	T

1 3 2 .

In this case, the statement under consideration is always false, regardless of whether P is true or false. In general, a statement is a contradiction if it is always false, regardless of whether its component statements are true or false.

That the first of the above two statements about Irene is a tautology, and the second a contradiction, seems quite intuitively reasonable. It is possible, however, to have more complicated (and unintuitive) 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	$((P \wedge Q) \rightarrow R)$	\rightarrow	$(P \rightarrow (Q \rightarrow R))$	
T	T	T	T	T	T	.
T	T	F	T	T	F	
T	F	T	T	F	T	
T	F	F	F	T	T	
F	T	T	F	T	F	
F	T	F	F	T	T	
F	F	T	F	F	F	
F	F	F	F	T	T	
			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 are true or false. Thus the statement is a tautology. Suppose we let 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

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.

1.2.2. Which of the following expressions are statements?

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

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) $P \wedge Q$. | (5) $\neg P \vee \neg Q$. |
| (2) $Q \vee R$. | (6) $\neg P \vee Q$. |
| (3) $\neg R$. | (7) $(R \wedge P) \vee Q$. |
| (4) $\neg(P \vee Q)$. | (8) $R \wedge (P \vee Q)$. |

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) $Z \rightarrow X$. | (4) $Y \vee (Z \rightarrow X)$. |
| (2) $X \leftrightarrow Y$. | (5) $(Y \rightarrow \neg X) \wedge (Z \rightarrow \neg X)$. |
| (3) $(Y \vee Z) \rightarrow X$. | (6) $(X \wedge \neg Y) \leftrightarrow (Y \vee Z)$. |

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.

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.

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 is true, and which is false?

(1) $A \vee C$.

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

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

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

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

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

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 is true, and which is false?

(1) $Z \rightarrow Y$.

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

(2) $X \leftrightarrow Z$.

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

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

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

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

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 is true, and which is 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.

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

- | | |
|----------------------------------|--------------------------------------------|
| (1) $P \wedge \neg Q$. | (4) $(A \vee B) \wedge (A \vee C)$. |
| (2) $(R \vee S) \wedge \neg R$. | (5) $(P \wedge R) \vee \neg(Q \wedge S)$. |
| (3) $X \vee (\neg Y \vee Z)$. | |

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

- | | |
|---------------------------------------------|-----------------------------------------------------------------|
| (1) $X \rightarrow \neg Y$. | (4) $(E \leftrightarrow F) \rightarrow (E \leftrightarrow G)$. |
| (2) $(R \rightarrow S) \leftrightarrow R$. | (5) $(P \rightarrow R) \vee \neg(Q \leftrightarrow S)$. |
| (3) $\neg M \rightarrow (N \wedge L)$. | |

1.2.13. Which of the following statements is a tautology, which is a contradiction and which is 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) $((P \leftrightarrow \neg Q) \wedge P) \wedge Q$.

1.2.14. Which of the following statements is a tautology, which is a contradiction and which is 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, iff the goat is blue and the goat is not blue.

1.2.15. Let P be a statement, let TA be a tautology, and let CO be a contradiction.

- (1) Show that $P \vee TA$ is a tautology.
- (2) Show that $P \wedge CO$ 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 it implies that 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 approaches to these concepts are, intuitively the above two sentences seem right. (It might be objected to that our 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.)

Our two examples given above of relations between statements represent the two types of such relations we will study, namely implication and equivalence, which are the meta-statement analogs of conditionals and bi-conditionals. 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, since 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 $P \rightarrow Q$ is true), since 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,” since 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 theory happen, we do not say that

“the sky is blue” implies “grass is green.” In general, even though $P \rightarrow Q$ happens to be true now, given that it might be false under other circumstances, we cannot say that P implies Q . To have P implies Q , we need $P \rightarrow Q$ 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” (recall that we are, as always, using inclusive “or”). Whether or not each of these statements are 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 statement is true or false.

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

P	Q	$\neg(P \rightarrow Q)$	$P \vee Q$
T	T	F	T
T	F	T	F
F	T	F	T
F	F	F	F
		4 1 3 2 ,	1 3 2 .

The column numbered 4 in the first truth table has the truth values for $\neg(P \rightarrow Q)$, 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 $\neg(P \rightarrow Q)$, 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 $\neg(P \rightarrow Q)$ has truth value F . Thus $\neg(P \rightarrow Q)$ logically implies $P \vee Q$.

Alternately, 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 $(P \rightarrow Q) \rightarrow (\neg Q \rightarrow \neg P)$ will always be true, regardless of the truth or falsity of P and Q . In other words, the statement $(\neg(P \rightarrow Q)) \rightarrow (P \vee Q)$ will be a tautology (also in Section 1.2), as can be seen in the

truth table

P	Q	$(\neg(P \rightarrow Q))$	$\rightarrow(P \vee Q)$
T	T	F	T
T	F	T	F
F	T	F	T
F	F	F	F
		4	1 3 2 8 5 7 6

Column 8 has the truth values for the whole statement $(\neg(P \rightarrow Q)) \rightarrow (P \vee Q)$, and since it has all trues in it, the statement 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 $P \rightarrow Q$ is a tautology. We abbreviate the English sentence “ P implies Q ” by the notation “ $P \Rightarrow Q$.”

It is important to note the difference between the notations “ $P \Rightarrow Q$ ” and “ $P \rightarrow Q$.” The notation “ $P \rightarrow Q$ ” 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 in this case is simply a shorthand way of writing the English sentence “ P implies Q ,” and it means that $P \rightarrow Q$ is not just true in some particular instances, but is a tautology. It might appear as if we are not introducing anything new here, given that we are defining implication in terms of conditional statements, but we will see in Section 1.4 that our reformulation in terms of meta-statements will be extremely useful in constructing valid arguments. In particular, the following implications will be used extensively in the next section.

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

- (i) $(P \rightarrow Q) \wedge P \Rightarrow Q$ (Modus Ponens).
- (ii) $(P \rightarrow Q) \wedge \neg Q \Rightarrow \neg P$ (Modus Tollens).
- (iii) $P \wedge Q \Rightarrow P$ (Simplification).
- (iv) $P \wedge Q \Rightarrow Q$ (Simplification).
- (v) $P \Rightarrow P \vee Q$ (Addition).
- (vi) $Q \Rightarrow P \vee Q$ (Addition).
- (vii) $(P \vee Q) \wedge \neg P \Rightarrow Q$ (Modus Tollendo Ponens).
- (viii) $(P \vee Q) \wedge \neg Q \Rightarrow P$ (Modus Tollendo Ponens).

- (ix) $P \leftrightarrow Q \Rightarrow P \rightarrow Q$ (*Biconditional-Conditional*).
- (x) $P \leftrightarrow Q \Rightarrow Q \rightarrow P$ (*Biconditional-Conditional*).
- (xi) $(P \rightarrow Q) \wedge (Q \rightarrow P) \Rightarrow P \leftrightarrow Q$ (*Conditional-Biconditional*).
- (xii) $(P \rightarrow Q) \wedge (Q \rightarrow R) \Rightarrow P \rightarrow R$ (*Hypothetical Syllogism*).
- (xiii) $\underbrace{(P \rightarrow Q)}_{\text{and}} \wedge \underbrace{(R \rightarrow S)}_{\text{and}} \wedge \underbrace{(P \vee R)}_{\text{implies}} \Rightarrow \underbrace{Q \vee S}_{\text{or}} \text{ (*Constructive Dilemma*)}$.

Demonstration. We will show that part (i) holds, leaving parts (ii) – (xiii) to the reader in Exercise 1.3.6.

Part (i) asserts that $(P \rightarrow Q) \wedge P \Rightarrow Q$. To demonstrate this assertion, we need to show that the statement $((P \rightarrow Q) \wedge P) \rightarrow Q$ is a tautology, which we do with the truth table

P	Q	$((P \rightarrow Q) \wedge P) \rightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	F
		1 3 2 5 4 7 6 .

Column 7 has the truth values for the statement $((P \rightarrow Q) \wedge P) \rightarrow Q$, and since it has all trues in it, the statement 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 (vii). 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. Since the implications stated in Fact 1.3.1 will be used in the next section, 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 $\neg(P \rightarrow Q) \Rightarrow P \vee Q$. On the other hand, the same truth tables used to establish this implication also show that $P \vee Q$ does not imply $\neg(P \rightarrow Q)$. For example, when P and Q are both true, then $P \vee Q$

is true, but $\neg(P \rightarrow Q)$ is false. Alternately, it can be seen by a truth table that $(P \vee Q) \rightarrow (\neg(P \rightarrow Q))$ 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 are reversible, which is very convenient, and is precisely 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 $P \rightarrow Q$, 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 are in fact logically equivalent, since that will allow us to find alternative, but equivalent, forms of the statements of 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 iff 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.” These statements can be seen to be equivalent, in that if one of them is true, then so is the other one, regardless of truth or falsity of the component statements “Fred has good taste in food” and “Fred likes to eat liver.” Let us denote these last two statements by P and Q respectively. Then we want to show the equivalence of $P \rightarrow Q$ and $\neg Q \rightarrow \neg P$. 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 have

P	Q	$P \rightarrow Q$		P	Q	$\neg Q$	\rightarrow	$\neg P$
T	T	T	T	T		F	T	F
T	F	T	F	F		T	F	F
F	T	F	T	T		F	T	T
F	F	F	T	F		F	T	T
		1	3	2	,		1	3

The columns numbered 3 in the truth tables have the truth values for $P \rightarrow Q$ and $\neg Q \rightarrow \neg P$ respectively. These columns are identical, which says that $P \rightarrow Q$ is true if and only if $\neg Q \rightarrow \neg P$ 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 above two truth tables is the same as saying that the single statement $(P \rightarrow Q) \leftrightarrow (\neg Q \rightarrow \neg P)$ is a tautology, as can be seen in the truth table

P	Q	$(P \rightarrow Q)$	\leftrightarrow	$(\neg Q \rightarrow \neg P)$
T	T	T	T	T
T	F	T	F	T
F	T	F	T	F
F	F	F	T	T
		1	3	2
			7	4
				6
				5

Column 7 has the truth values for the statement $(P \rightarrow Q) \leftrightarrow (\neg Q \rightarrow \neg P)$, and since it has all trues in it, the statement is indeed a tautology.

To be precise, 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 sentence “ P and Q are equivalent” by the notation “ $P \iff Q$.”

It can be seen that $P \iff Q$ is true if and only if $P \Rightarrow Q$ and $Q \Rightarrow P$ are both true. Also, it is important to note the difference between the notations “ $P \iff Q$ ” 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 sentence “ P is equivalent to Q .”

Listed below are some equivalences of statements that will be particularly useful. Part (ix) of the result is the example we just saw. We will discuss some of these equivalences after stating them.

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

- (i) $\neg(\neg P) \iff P$ (*Double Negation*).
- (ii) $P \vee Q \iff Q \vee P$ (*Commutative Law*).

- (iii) $P \wedge Q \iff Q \wedge P$ (*Commutative Law*).
- (iv) $(P \vee Q) \vee R \iff P \vee (Q \vee R)$ (*Associative Law*).
- (v) $(P \wedge Q) \wedge R \iff P \wedge (Q \wedge R)$ (*Associative Law*).
- (vi) $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$ (*Distributive Law*).
- (vii) $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$ (*Distributive Law*).
- (viii) $P \rightarrow Q \iff \neg P \vee Q$.
- (ix) $P \rightarrow Q \iff \neg Q \rightarrow \neg P$ (*Contrapositive*).
- (x) $P \leftrightarrow Q \iff Q \leftrightarrow P$.
- (xi) $P \leftrightarrow Q \iff (P \rightarrow Q) \wedge (Q \rightarrow P)$.
- (xii) $\neg(P \wedge Q) \iff \neg P \vee \neg Q$ (*De Morgan's Law*).
- (xiii) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$ (*De Morgan's Law*).
- (xiv) $\neg(P \rightarrow Q) \iff P \wedge \neg Q$.
- (xv) $\neg(P \leftrightarrow Q) \iff (P \wedge \neg Q) \vee (\neg P \wedge Q)$.

Demonstration. Part (ix) was discussed previously. We will show here that part (vii) holds, leaving parts (i) – (vi), (viii), (x) – (xv) to the reader in Exercise 1.3.7. The demonstration here is very similar to the demonstration of Fact 1.3.1 (i).

Part (vii) of the present fact asserts that $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$, which we demonstrate 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	$(P \vee (Q \wedge R))$	\leftrightarrow	$((P \vee Q) \wedge (P \vee R))$	\wedge	$(P \vee Q)$	\wedge	$(P \vee R)$
T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	F	F	T	T	T
T	F	T	T	F	F	T	T	F	T
T	F	F	T	F	F	F	T	F	F
F	T	T	F	T	T	T	F	T	F
F	T	F	F	T	F	T	F	T	T
F	F	T	F	F	F	T	F	F	T
F	F	F	F	F	F	T	F	F	F
			4	5	1	3	2	13	6
							8	7	12
								9	11
									10

Column 13 has the truth values for the statement $(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R))$, and since it has all trues in it, the statement is a tautology.

///

Part (i) of the above fact 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 we want to show that a statement P is true. One method to prove this claim 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. Since $\neg(\neg P)$ 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 complete discussion of this method of proof is in Section 2.3.

Parts (viii), (ix) and (xi) of Fact 1.3.2 are also useful equivalences that will allow us to restate theorems in ways that are sometimes easier to prove; more on this in Chapter 2. Part (viii), for example, gives a characterization of a conditional statement in terms of disjunction and negation. Using this equivalence, we deduce that the statement “if it snows today I will eat a cake” is equivalent to “it will not snow today or I will eat a cake” (let P = “it snows today” and Q = “I will eat a cake”). These two statements may not appear equivalent at first glance, but that is probably due to the fact that in colloquial English the word “or” is often interpreted as the exclusive “or,” rather than the inclusive “or” we are using. Suppose that the statement “it snows today” is false. Then “if it snows today I will eat a cake” is true regardless of whether “I will eat a cake” is true or not. Also, “it will not snow today” is true, and hence “it will not snow today or I will eat a cake” is true regardless of whether “I will eat a cake” is true or not. Next, suppose that “it snows today” is true. Then “if it snows today I will eat a cake” is true precisely if “I will eat a cake” is true. Also, “it will not snow today” is false, and hence “it will not snow today or I will eat a cake” will be true precisely if “I will eat a cake” is true. We thus see that “if it snows today I will eat a cake” and “it will not snow today or I will eat a cake” behave exactly the same way.

Part (xi) 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 suffices to prove $(P \rightarrow Q) \wedge (Q \rightarrow P)$; it thus 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 (ix) 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.” The equivalence of these statements does make sense intuitively. Suppose 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, since 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, since perhaps it rained, and she washed her clothes in that case too (and she might even wash her clothes on a sunny day). Thus “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 wear tan pants I will wear brown shoes” is “if I do not wear brown shoes I will not wear tan pants.” Fact 1.3.2 (ix) says that a statement and its contrapositive are always equivalent.

While we are at it, we also give names to two other variants to 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 wear tan pants I will wear brown shoes” is “if I wear brown shoes I will wear tan pants”; the inverse of the original statement is “if I do not wear tan pants I will not wear brown shoes.” It is important to recognize that neither the converse nor the inverse are equivalent to the original statement (you can verify this by constructing the appropriate truth tables). However, the converse and the inverse are equivalent to one another, as can be seen by applying Fact 1.3.2 (ix) to the statement $Q \rightarrow P$.

One valuable use of equivalences of statements is to find convenient formulas for the negations of statements. Such formulas are found in parts

(xii) – (xv) 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.” Note 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. Thus, 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 (xii) and (xiii).

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 thus 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 observations is given in Fact 1.3.2 (xiv).

Exercises

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

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

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

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

1.3.3. Let P be a statement, let TA be a tautology, and let CO be a contradiction.

- (1) Show that $P \wedge TA \iff P$.
- (2) Show that $P \vee CO \iff P$.

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.”

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 iff 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.”

1.3.6. [Used in Section 1.3.] Prove Fact 1.3.1 (ii) – (xiii).

1.3.7. [Used in Section 1.3.] Prove Fact 1.3.2 (i) – (vi), (viii), (x) – (xv).

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, give him a hug.

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.”

1.3.10. Negate each of the following statements.

(1) $e^5 > 0$.

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

- (3) $\sin(\pi/2) < 0$ and $\tan(0) \geq 0$.
- (4) If $y = 3$ then $y^2 = 7$.
- (5) $w - 3 > 0$ implies $w^2 + 9 > 6w$.
- (6) $a - b = c$ iff $a = b + c$.

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.

1.3.12. Simplify the following statements (making use of any equivalences of statements given so far in the text or exercises).

- | | |
|------------------------------------|--------------------------------------|
| (1) $\neg(P \rightarrow \neg Q)$. | (4) $\neg(M \vee L) \wedge L$. |
| (2) $A \rightarrow (A \wedge B)$. | (5) $(P \rightarrow Q) \vee Q$. |
| (3) $(X \wedge Y) \rightarrow X$. | (6) $\neg(X \rightarrow Y) \vee Y$. |

1.3.13. [Used in Section 6.3.] 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 $\bar{\wedge}$ be the binary logical operation, often referred to as **nand**, defined by the truth table

P	Q	$P \bar{\wedge} Q$
T	T	F
T	F	T
F	T	T
F	F	T

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

1.4 Valid Arguments

In the previous two sections 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 allow 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 statements, does not appear to resemble the way mathematicians prove theorems, which is by writing sequences of statements, starting with the hypotheses, and leading step by step to the conclusion. In this section we look at the analogous construction in logic, and will mention the relation of this process to our discussion in the previous two sections.

When we turn to the construction of proofs in the next chapter, we will be focusing on the mathematical content of our proofs, and will not be explicitly referring to the logical rules of argumentation to be discussed here (since that would be a distraction from the mathematical issues involved). We will also not be using the logical notation we use at present. Nonetheless, we will be using these logical rules of 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.

Let us look at a very simple logical argument.

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.

Note, first of all, that logicians use the word “argument” differently from the colloquial use of the word. In the latter usage, the word could mean a heated discussion, or it could mean the reasons given for thinking that something is true. Logicians, by contrast, use the term “argument” to mean 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. 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. (We note that 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,” M = “the poodle-o-matic makes money for the manufacturer,” and let R = “the poodle-o-matic is painted red.” The argument then becomes

$$\begin{array}{c} (C \vee E) \rightarrow \neg M \\ R \rightarrow M \\ \hline C \\ \hline \neg R, \end{array}$$

where the horizontal line separates the premises from the conclusion. Alternately, we could write it as $((C \vee E) \rightarrow \neg M) \wedge (R \rightarrow M) \wedge C \Rightarrow \neg R$, which is in keeping with our notation from Section 1.3.

Thinking of the last way we wrote our argument, we could attempt to show that it is true just as we showed that certain logical implications were true in Section 1.3, namely by showing that the statement $((C \vee E) \rightarrow \neg M) \wedge (R \rightarrow M) \wedge C \rightarrow \neg R$ is a tautology, which we could accomplish by using a truth table. This method would 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. In even more complicated cases, the truth tables would have to be even larger. Second, using a truth table gives no intuitive insight into why the argument is true. 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 truth tables, we will make 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 — we proved them in Fact 1.3.1, although we are stating them in a different format here, to conform to the notation used for logical arguments.

$\frac{P \rightarrow Q}{Q}$	Modus Ponens	$\frac{P \vee Q}{\neg P}$	Modus Tollendo Ponens
$\frac{P \rightarrow Q}{\neg Q}$	Modus Tollens	$\frac{P \vee Q}{\neg Q}$	Modus Tollendo Ponens
$\frac{\neg\neg P}{P}$	Double Negation	$\frac{P \leftrightarrow Q}{P \rightarrow Q}$	Biconditional-Conditional
$\frac{P}{\neg\neg P}$	Double Negation	$\frac{P \leftrightarrow Q}{Q \rightarrow P}$	Biconditional-Conditional
$\frac{P}{P}$	Repetition	$\frac{P \rightarrow Q}{Q \rightarrow P}$	Conditional-Biconditional
$\frac{P \wedge Q}{P}$	Simplification	$\frac{P \rightarrow Q}{Q \rightarrow R}$	Hypothetical Syllogism
$\frac{P \wedge Q}{Q}$	Simplification	$\frac{P \rightarrow Q}{P \rightarrow R}$	Constructive Dilemma
$\frac{P}{P \wedge Q}$	Adjunction	$\frac{P \rightarrow Q}{R \rightarrow S}$	
$\frac{P}{P \vee Q}$	Addition	$\frac{P \vee R}{Q \vee S}$	
$\frac{Q}{P \vee Q}$	Addition		

The names for some of the above rules of inference, such as modus ponens, are quite standard; a few 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 (since $P \rightarrow P$ is a tautology), but is still worth mentioning. Adjunction is just a glorified version of repetition, since if we stated it in the format of Fact 1.3.1, it would look like $P \wedge Q \Rightarrow P \wedge Q$.

We now return to our argument concerning the poodle-o-matic. Using the above listed rules of inference, 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; 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 proof is

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

This sort of proof, 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**. Note that the derivability of an argument is one thing, and the truth of the statements involved is another. We can have a derivable argument with statements that happen to be true, or happen to be false, and we can have a non-derivable argument with 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 same argument, this time making use of the equivalences of statements given in Fact 1.3.2. In general, it is acceptable in a derivation to replace one statement with another that is equivalent to it. The alternate derivation is

(1) $(C \vee E) \rightarrow \neg M$	
(2) $R \rightarrow M$	
(3) <u>C</u>	
(4) $C \vee E$	(3), Addition
(5) $\neg M \rightarrow \neg R$	(2), Contrapositive

- | | |
|-----------------------------------------------------|--------------------------------------------------------------|
| $(6) (C \vee E) \rightarrow \neg R$
$(7) \neg R$ | $(1), (5)$, Hypothetical Syl.
$(4), (6)$, Modus Ponens. |
|-----------------------------------------------------|--------------------------------------------------------------|

This alternate 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, namely that it is or is not valid, and that it is or is not derivable. The former notion involves checking truth values (which we have been doing using 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 4-5] for more details. (Different treatments of this subject might use different collections of rules of inference, but the basic ideas are the same.)

We see from the above 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, since we would need to show that no derivation could possibly be found. It would not suffice to say that you cannot find a derivation, since you cannot be sure that you have not simply overlooked a derivation that works. Rather, we use the definition of validity directly, and we show that an argument is invalid by finding some truth values for the component statements used in the argument for which the premises are all true but the conclusion is 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,” S = “Earth receives signals from outer space,” and let H = “all people grow long hair.” The argument then becomes

$$\begin{array}{c} A \rightarrow R \\ S \rightarrow H \\ \hline \underline{A \wedge H} \\ R \wedge S. \end{array}$$

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. Thus the premises are all true, but the conclusion is false. Hence the argument is invalid. For some other combinations of A , R , S and H being true or false, it does work 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. (That the argument was invalid may have been evident intuitively even without all this effort, but this method works in more complicated cases as well, where our intuition might not be such a reliable guide.)

We now look at a particular type of argument for which special care is needed.

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. Then Ferdinand plays the accordion.

This argument seems absurd, since 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,” 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 Toll. Pon.
(9) F	(5), (8), Modus Toll. Pon.

This is genuinely a valid derivation, 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 Toll. Pon.
(9) $\neg F$	(5), (8), Modus Toll. Pon.

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 it can be seen that this statement is a contradiction by using a truth table. 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 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, since 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. It was eventually shown that non-Euclidean is no less consistent than Euclidean geometry, and so no one could claim that non-Euclidean geometry was less worthwhile mathematically than Euclidean geometry. See [Tru87, Chapter 7] for more 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 discussion of a few common logical errors, often referred to as fallacies, that are regularly found in attempted mathematical proofs.

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. Thus, 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 (also known as the fallacy of affirming the consequent).

For our next type of fallacy, we examine 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 sleazebucket.

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. Thus, 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 (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 arguments. 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

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

$$(1) \frac{\begin{array}{c} P \wedge Q \\ (P \vee Q) \rightarrow R \end{array}}{R}$$

$$(2) \frac{\begin{array}{c} \top \\ \neg X \rightarrow Y \\ \neg X \rightarrow Z \end{array}}{\frac{\begin{array}{c} \top \\ \neg Z \rightarrow \neg Y \\ \top \end{array}}{\vdash}}$$

$$(3) \frac{\begin{array}{c} E \rightarrow F \\ \neg G \rightarrow \neg F \\ H \rightarrow I \\ E \vee H \end{array}}{G \vee I}$$

$$(4) \frac{\begin{array}{c} L \rightarrow M \\ (M \vee N) \rightarrow (L \rightarrow K) \\ \neg P \wedge L \end{array}}{K}$$

$$\begin{array}{l}
 (5) \quad P \rightarrow Q \\
 \quad \neg R \rightarrow (S \rightarrow T) \\
 \quad R \vee (P \vee T) \\
 \quad \underline{\neg R} \\
 \quad Q \vee S
 \end{array}$$

$$\begin{array}{l}
 (6) \quad \neg A \rightarrow (B \rightarrow \neg C) \\
 \quad C \rightarrow \neg A \\
 \quad (\neg D \vee A) \rightarrow \neg\neg C \\
 \quad \underline{\neg D} \\
 \quad \neg B
 \end{array}$$

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.

1.4.3. Write a derivation for each of the following valid arguments. 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.

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 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 given is not precise, however, since 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 type of logic that involves quantifiers is often referred to as “first order” (or “predicate”) logic; the type of logic we looked at previously is often called “sentential” (or “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 thus 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, since 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 all cats x , and all mice y , the cat x likes to eat the mouse y .” The statement “every person has a mother” combines two different types of quantifiers, since it could be rephrased as “for each person A , there is a woman B such that B is the mother of A .” Similarly to any other 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, consider the expression $P = "x + y > 0."$ Note that x and y have the same roles in the statement P . Using P we can form a new expression $Q = \text{“for all positive real numbers } x, \text{ we have } x + y > 0\text{.”}$ There is a substantial difference between the roles of x and y in Q . We call x a **bound variable** in Q , in that we have no ability

to choose which values of x we want to consider. By contrast, we call y a **free variable** in Q , since its possible values are not limited. Since y is a free variable in Q , it is often useful to write $Q(y)$ instead of Q to indicate that y is free.

Another aspect of the difference between a bound variable and a free one is 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 , we have $w + y > 0$.” 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 this expression would be completely unaffected by replacing Q with \hat{Q} . By contrast, suppose we change every occurrence of y to z in Q , obtaining \tilde{Q} = “for all positive real numbers x , we have $x + z > 0$.” 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 .

Finally, note that an expression with a free variable is not a statement. Our expression Q in the previous paragraph, for example, is not a statement, since 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 , we have $x + y > 0$,” has no free variables, and is indeed a statement (which happens to be false).

We now turn to a closer look at the two main types of quantifiers. Let $P(x)$ be an expression with free variable x (the statement could have other free variables as well). Let U denote some collection of possible values of x . A **universal quantifier** applied to $P(x)$ is a 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 $(\forall x)P(x)$.

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 $P(\alpha)$ = “the person α has red hair,” and let W be the collection of all people in the world. Then 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.”

Changing the set U in a statement of the form $(\forall x \text{ in } U)P(x)$ might change the truth or falsity of the statement, so that the choice of set 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 other type of quantifier we are interested in, once again let $P(x)$ be a statement with free variable x (as before, the statement could have other free variables as well); let U denote some collection of possible values of x . An **existential quantifier** applied to $P(x)$ is a 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 $(\exists x)P(x)$. 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 certainly true – with a lot of overkill.

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

For some value of x in U , we have $P(x)$ is true;

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

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

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

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

Let $Q(r)$ = “the person r has brown hair,” and let W be the collection of all people in the world. Then the statement $(\exists r \text{ in } W)Q(r)$ would mean that “some people have brown hair” (which is true). 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. We can express the statement “some integers are even and prime” 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, since 2 is both even and prime.)

We can form statements with more than one quantifier, as long as different quantifiers involve different bound variables. Suppose $P(x, y) = “x + y^2 = 3”$, 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 $x + y^2 = 3$.” This statement is true, since we can always solve for x in terms of y for any real number 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 , we have $x + y^2 = 3$.” This statement is clearly false, since for any given x , there can be at most two values of y such that $x + y^2 = 3$. The order of the quantifiers thus 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 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 whose statements involve 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 [Pow94, Chapter 3] for example.

A non-mathematical example of clarifying a statement in English by writing it symbolically 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 times that are precisely on the hour and that $C(x, t) = “\text{person } x \text{ is hit by a car at time } t”$. 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 two bound 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 fruit and that $L(x, y) = \text{"person } x \text{ likes to eat fruit } y\text{"}$. Our eight ways of applying two quantifiers to $L(x, y)$ are the following:

(1) $(\forall x)(\forall y)L(x, y)$. We could write this statement in English as “for each person x , for each type of fruit y , person x likes to eat y .” This statement can be restated more simply as “every person likes every type of fruit.” To verify whether this statement is true, we would have to ask every 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) $(\forall y)(\forall x)L(x, y)$. We could write this statement as “for each type of fruit y , for each person x , we know x likes to eat y .” This statement can be restated more simply as “every type of fruit is liked by every person.” This statement is equivalent to statement (1).

(3) $(\forall x)(\exists y)L(x, y)$. We could write this statement as “for each person x , there is a type of fruit y such that x likes to eat y .” This statement can be restated more simply as “every person likes at least one type of fruit.” To verify whether this statement is true, we would have to ask every 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) $(\exists x)(\forall y)L(x, y)$. We could write this statement as “there is a person x such that for all types of fruit y , person x likes to eat y .” This statement can be restated more simply as “there is a person who likes every type of fruit.” To verify whether this statement is true, we would have to 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.

(5) $(\forall y)(\exists x)L(x, y)$. We could write this statement as “for each type of fruit y , there is a person x such that x likes to eat y .” This statement can be restated 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. For the statement to be true, we would have to

find at least one person per fruit, though it would be acceptable if for more than one fruit we found the same person.

(6) $(\exists y)(\forall x)L(x, y)$. We could write this statement as “there is a type of fruit y such that for all persons x , we know that x likes to eat y .” This statement can be restated 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 every 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) $(\exists x)(\exists y)L(x, y)$. We could write this statement as “there is a person x such that there is a type of fruit y such that x likes to eat y .” This statement can be restated 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) $(\exists y)(\exists x)L(x, y)$. We could write this statement as “there is a type of fruit y such that there is a person x such that x likes to eat y .” This statement can be restated 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, since there were two bound variables. When there are more bound variables, then the number of cases will be even larger. Also, we note 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 are equal).

Some statements with quantifiers imply others. With one variable, we see that $(\forall x)P(x)$ implies $(\exists x)P(x)$. With two quantifiers, it is straightforward to see that $(\forall x)(\forall y)P(x, y)$ is equivalent to $(\forall y)(\forall x)P(x, y)$. These two statements each imply both of $(\exists x)(\forall y)P(x, y)$ and $(\exists y)(\forall x)P(x, y)$. The first of these implies $(\forall y)(\exists x)P(x, y)$, and the second of these implies $(\forall x)(\exists y)P(x, y)$. Each of these last two imply the two equivalent statements $(\exists x)(\exists y)P(x, y)$ and $(\exists y)(\exists x)P(x, y)$. See Figure 1.5.1 for a summary of these implications.

Lastly, we turn to relations between statements with quantifiers (compare Section 1.3), and rules of inference with quantifiers (compare Section 1.4). We start with the former, where our concern is to negate statements containing quantifiers. Consider the statement $Q =$ “all people have red hair.” The negation of this statement can, most directly, be written as

$$\begin{array}{ccc}
 (\forall x)(\forall y)P(x, y) & \iff & (\forall y)(\forall x)P(x, y) \\
 \swarrow & & \searrow \\
 (\exists x)(\forall y)P(x, y) & & (\exists y)(\forall x)P(x, y) \\
 \downarrow & & \downarrow \\
 (\forall y)(\exists x)P(x, y) & & (\forall x)(\exists y)P(x, y) \\
 \searrow & & \swarrow \\
 (\exists x)(\exists y)P(x, y) & \iff & (\exists y)(\exists x)P(x, y)
 \end{array}$$

Figure 1.5.1.

$\neg Q =$ “it is not the case that all people have red hair.” This last statement means that at least one person does not have red hair, so we could rewrite $\neg Q$ as “there are some people who do not have red hair.” We could rewrite Q and $\neg Q$ as follows, using quantifiers. If we 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.

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 we can rewrite it 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, since we are not using a quantifier that corresponds directly to “no pigs.”) If we let $W(x) =$ “pig x has wings,” then $R = (\exists x)W(x)$, and $\neg R = (\forall x)(\neg W(x))$. Note 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 here are completely typical. Let $P(x)$ be a statement with free variable x , taking values in some collection U . Then

$$\begin{aligned}
 \neg[(\forall x \text{ in } U)P(x)] &\iff (\exists x \text{ in } U)(\neg P(x)) & (1.5.1) \\
 \neg[(\exists x \text{ in } U)P(x)] &\iff (\forall x \text{ in } U)(\neg P(x)).
 \end{aligned}$$

Unlike the equivalences discussed in Section 1.3, we cannot use truth tables to show that these equivalences with quantifiers are true, though they are true nonetheless, based on the meanings of the quantifiers.

We can use the above rules to negate statements with more than one quantifier. For example, suppose 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

$$\begin{aligned}\neg Q &\iff \neg[(\forall w)(\exists y)P(w, y)] \iff (\exists w)\neg[(\exists y)P(w, y)] \\ &\iff (\exists w)(\forall y)(\neg P(w, y)).\end{aligned}$$

Rephrasing this last expression in English yields $\neg Q$ = “there exists a real number w such that for all real numbers y we have $f(y) \neq w.$ ” 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.

There are four rules of inference involving quantifiers.

$$\frac{(\forall x \text{ in } U)P(x)}{P(a)} \quad \text{Universal Instantiation}$$

where a is any member of $U.$

$$\frac{(\exists x \text{ in } U)P(x)}{P(b)} \quad \text{Existential Instantiation}$$

where b is some member of $U,$ and where the symbol “ b ” does not already have any other meaning in the given argument.

$$\frac{P(c)}{(\forall x \text{ in } U)P(x)} \quad \text{Universal Generalization}$$

where c is an arbitrary member of $U.$

$$\frac{P(d)}{(\exists x \text{ in } U)P(x)} \quad \text{Existential Generalization}$$

where d is a member of $U.$

Note 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 $N(x) = \text{“cat } x \text{ is nice,”}$ let $S(x) = \text{“cat } x \text{ is smart,”}$ let $C(x) = \text{“cat } x \text{ likes chopped liver,”}$ and let $T(x) = \text{“cat } x \text{ is Siamese.”}$

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

- | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> (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) $\neg(\exists x \text{ in } U)[T(x) \wedge \neg C(x)]$ |  |
| <hr/> <ul style="list-style-type: none"> (4) $T(a) \wedge \neg C(a)$ (5) $\neg C(a)$ (6) $T(a)$ (7) $T(a) \rightarrow N(a)$ (8) $\neg N(a)$ (9) $\neg\neg N(a)$ (10) $(N(a) \wedge S(a)) \rightarrow C(a)$ (11) $\neg(N(a) \wedge S(a))$ (12) $\neg N(a) \vee \neg S(a)$ | <ul style="list-style-type: none"> (3), Existential Instantiation (4), Simplification (4), Simplification (2), Universal Instantiation (7), (6), Modus Ponens (8), Double Negation (1), Universal Instantiation (10), (5), Modus Tollens (11), De Morgan’s Law |

- (13) $\neg S(a)$ (12), (9), Modus Toll. Pon.
 (14) $(\exists x \text{ in } U)[\neg S(x)]$ (13), Existential Gen.

Note that in line (4) we chose some letter “ a ” that was not in use prior to this line, since we are using Existential Instantiation. We needed to use this rule of inference at that point in the derivation in order to remove the quantifier in line (3) of the premises, thus allowing 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), since Universal Instantiation allows us to choose anything in U that we want.

Exercises

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

- (1) $(\forall x)Y(x).$ (4) $(\exists x)[Y(x) \rightarrow W(x)].$
 (2) $(\exists x)Z(x).$ (5) $(\forall x)[W(x) \leftrightarrow \neg Z(x)].$
 (3) $(\forall x)[W(x) \wedge Z(x)].$

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

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

1.5.3. Suppose that the possible values of x are all cows. Let $P(y) = “y \text{ is brown,”}$ let $Q(y) = “y \text{ is four years old”}$ and $R(y) = “y \text{ has white spots.”}$ 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.

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 $C(p, q) = "p$ 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.

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.

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)).

- (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 every one 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.

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.)

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

1.5.9. Let x be a real number. We say that 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.)

1.5.10. Someone claims that the argument

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

$$(\exists x \text{ in } U)[M(x) \wedge Q(x)]$$

is valid, using the alleged derivation

- | | |
|---------------------------------------------------|----------------------------------|
| (1) $(\exists x \text{ in } U)[P(x) \wedge Q(x)]$ | |
| (2) $(\exists x \text{ in } U)[M(x)]$ | |
| <hr/> | |
| (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.

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

(1)

$$\frac{(\forall x \text{ in } U)[(R(x) \rightarrow C(x)]}{(\forall x \text{ in } U)[T(x) \rightarrow R(x)]}$$

$$(\forall x \text{ in } U)[\neg C(x) \rightarrow \neg T(x)].$$

(2)

$$\frac{(\forall a \text{ in } V)[(N(a) \rightarrow B(a)]}{(\exists b \text{ in } V)[N(b) \wedge D(b)]}$$

$$(\exists c \text{ in } V)[B(c) \wedge D(c)].$$

$$(3) \quad \begin{array}{l} (\forall x \text{ in } Z)[(A(x) \rightarrow R(x)) \vee T(x)] \\ (\exists x \text{ in } Z)[T(x) \rightarrow P(x)] \\ (\forall x \text{ in } Z)[A(x) \wedge \neg P(x)] \\ \hline (\exists x \text{ in } Z)[R(x)]. \end{array}$$

$$(4) \quad \begin{array}{l} (\forall x \text{ in } W)(\exists y \text{ in } W)[E(x) \rightarrow (M(x) \vee N(y))] \\ \neg(\forall x \text{ in } W)[M(y)] \\ (\forall x \text{ in } W)[E(x)] \\ \hline (\exists x \text{ in } W)[N(x)]. \end{array}$$

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 that eats will make a mess and drool. Every baby that 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 and 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 what we learned in grade school is true. 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 more details on 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 mathe-

matics 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 elementary algebra (that is familiar from high school) in a rigorous, axiomatic fashion. (A lot of applied mathematics today also has rigorous foundations, though the work of applied mathematicians, while very challenging, 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, since 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 some 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, and so forth.

Why mathematics has moved over time in the direction of ever greater rigor 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 is to be sure that something is true. Contrary to a 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 (or both) 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 proofs 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 (as in Section 1.4), for a number of reasons: proofs are often much too long and complicated to be broken down into the two-column (statement-justification) approach; the mathematics is the major issue, so we don’t even mention the logical rules of inference used, but rather mention the mathematical justification of each step; we often have to refer to previous theorems, which would need to be brought into the proper logical format; many mathematical proofs are so complicated, and involve so many definitions and symbols, that bringing everything into the logicians’ format would be extremely cumbersome; we want proofs to focus on the conceptual difficulties, not the logical ones; non-logicians, which means most mathematicians, find long strings of logical symbols at minimum unpleasant, not to mention confusing. (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 result proved 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 you why mathematicians do things as they do.)

To some extent mathematicians relate to proofs the same way that 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). Learning to recognize and construct rigorous mathematical proofs is accomplished, similarly to classical art, 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 proofs, see [Die92, Section 3.2] or [EC89, Chapter 5], and for more general discussion about mathematical activity see, for example, [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 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 to write proofs. 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 “theorems” 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 ΔABC 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 is, I have often heard students say “ $a^2 + b^2 = c^2$.” This expression alone is not the statement of the theorem (indeed, it is not even a statement). 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 $a^2 + b^2 = c^2$ (this formula is not true for the sides of a non-right triangle). It is crucial to state theorems with all their hypotheses.

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 thus 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 definitions, and theorems that have already been proved. If we don’t 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 a 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, but we will want 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 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 real numbers that we use. We will discuss these numbers more rigorously in Chapter 8. We have to start somewhere, and these assumptions are safe to make. Our proofs in Section 8.4 will not use anything we do here, so there will be no circular reasoning.

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, since it really 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 proof is concerned with integers, namely the numbers

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

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. The following definition precisely captures a concept with which you are most likely familiar.

Definition: Let n be an integer. We say that n is **even** if there is some integer k such that $n = 2k$. We say that n is **odd** if there is some integer j such that $n = 2j + 1$. Δ

It can be proved that every integer is either even or odd, but not both; the proof uses some tools we have not learned yet, and is given in Exercise 8.4.15. We can now state and prove our theorem. This result may seem rather trivial, but our point here is to see a properly done proof, not learn an exciting new result about numbers.

Theorem 2.1.2. *Let n and m be integers.*

- (i) *If n and m are both even, then $n + m$ is even.*
- (ii) *If n and m are both odd, then $n + m$ is even.*
- (iii) *If n is even and m is odd, then $n + m$ is odd.*

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

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

Since k and j are integers so is $k + j$. Thus $n + m$ is even.

(ii) & (iii). These are proved similarly to part (i). \square

There is a fourth possible case we did not state in the theorem, namely n is odd and m is even, because that case 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 (i) of the theorem is quite simple, but there are a few features worth mentioning, since 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, notice that the proof is written in grammatically correct English. Complete sentences are used, with full 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 are often used in high school geometry, should be left behind at this point. Mathematics texts and research papers are all written in the style we are using. See Section 2.6 for more details on writing mathematics.

An important consideration when writing a proof is recognizing what needs to be proved and what doesn't. There is no formula for such a determination; it completely depends upon the context. 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, since 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 reason to prove facts that we already know is two-fold: 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, note that in the above proof we did not use the logical symbols we discussed in Chapter 1. We will generally not be using logical symbols when we write our proofs. Logical symbols were used 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, we did make use in the above proof of some of the rules of inference discussed in Section 1.4, though as will always be the case, they are not mentioned explicitly to avoid unnecessary length and clutter. For instance, the hypothesis in part (i) has the form $P \wedge Q$, where $P = “n$ is even” and $Q = “m$ is even.” The proof starts by assuming that $P \wedge Q$ is true. We then used the Simplification rule of inference to deduce that each of P and Q are true, so that we could apply the definition of even numbers to each, to deduce that each of the statements “ $n = 2k$ ” and “ $m = 2j$ ” hold, for appropriate k and j . We then applied the Adjunction rule of inference to deduce that the statement “ $n = 2k$ and $m = 2j$ ” holds, so that we could do the calculation involving $n + m$. Finally, we need repeated use of the Hypothetical Syllogism rule of inference to put all the pieces of the proof together. Mathematicians do not generally mention the logical rules of inference used in their proofs, but focus instead on the mathematical ideas. Of course, the rules of inference must be used correctly, even when not stated.

Two final comments on writing proofs. First, neither thinking up proofs nor writing them properly is easy — especially as the material we treat becomes more and more abstract. Mathematics is not a speed activity, and you should not expect to construct proofs rapidly. Before finalizing the write-up of a proof, you will often need to do scratch work first. 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 will be true for students of mathematics.

Lastly, unlike some other texts on proofs, we will not be categorizing proofs into a very fine typology of different kinds of proofs. There are really only a few basic categories of proofs: direct proof (such as the one given above), proof by contrapositive, proof by contradiction. The way to learn to construct proofs is not to spend time classifying them into minutely differentiated categories, but rather to read a lot of well written proofs, to write a lot of proofs, and to get detailed feedback on the proofs you write.

Exercises

2.1.1. Reformulate each of the following theorems in the form $P \rightarrow Q$. (The statements of the these 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 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 2.1.2 are of the form $P \rightarrow Q$. To prove theorems, we thus 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, and which eventually lead to Q . This type of proof is called a **direct proof**. That this sort of proof deserves a name at all is because there are other approaches that can be taken, as we will see in the next section. An example of a direct proof is the proof of Theorem 2.1.2.

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 (namely P) and ends at the end (namely 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. Just as when 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 might be 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 if the chosen strategy is direct proof, there are a number of ways of proceeding. 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 under-

stand 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. Thus the proof would look something like “Suppose P (argumentation) . . . Then Q .”

The reason for writing direct proofs this way is not to cover up your tracks, 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 logically. For example, not all arguments are reversible, and an argument that worked backwards during scratch work might not always work when written forwards. Intuitive thinking that may have been useful in formulating the proof should be replaced by logical deduction in the final written proof.

In sum, there are two main steps to the process of producing a rigorous proof: formulating the proof 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, etc.

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

Definition. Let a and b be integers. We say a divides 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 . Δ

It is important to note that 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 .” Thus, for example, even though it is not sensible to write the fraction $7/0$, it is perfectly reasonable to write the expression $7|0$, since 7 does in fact divide 0 (because $7 \cdot 0 = 0$). Keep in mind that to show the truth of a statement of the form “ $a|b$,” it is necessary to find an integer q such that $aq = b$. Thus, a statement of the form “ $a|b$ ” is an existence statement.

We now have two simple results about divisibility. Read the scratch work as well as the actual proofs.

Theorem 2.2.1. *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. Since $a|b$ 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 get $(aq)r = c$. 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 $ak = a(qr) = (aq)r = br = c$. Since $ak = c$, we know that $a|c$. \square

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 2.2.2. *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 $n|0$. \square

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

Exercises

2.2.1. Outline the strategy for a direct proof of each of the following statements (do not prove them, since 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.

2.2.2. Let n and m be integers.

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

2.2.3. Let n be an integer.

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

2.2.4. [Used in Sections 2.3 and 2.4.] Let n be an integer. Show that if n is even then n^2 is even, and if n is odd then n^2 is odd.

2.2.5. Let n be an integer. We say that n is a multiple of 3 if $n = 3k$ for some integer k . Let n and m be integers.

- (1) Suppose that n and m are both multiples of 3. Show that $n + m$ is a multiple of 3.
- (2) Suppose that n is a multiple of 3. Show that nm is a multiple of 3.

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

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

2.2.8. Let a, b be integers. Show that if $a|b$, then $a^n|b^n$ for all positive integers n . (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 these more convoluted methods are easier to work with. A less than perfect analogy might be when the straightest road between two cities leads up 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. 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 logic in Section 1.3. For our first method, recall that the contrapositive of $P \rightarrow Q$, namely $\neg Q \rightarrow \neg P$, is equivalent to $P \rightarrow Q$. Thus, in order to prove $P \rightarrow Q$, we could just as well prove $\neg Q \rightarrow \neg P$, which we 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**. The following proof is a simple example of this method.

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 even. Thus there would be some integer j such that $n^2 = 2j$. It is not clear how to proceed from this point, so instead we try a proof by contrapositive. Such a proof would involve assuming that n is not odd (so that it is even), and then deducing that n^2 is not odd (so that it too is even). We start such a proof by observing that if n is even, then there is some integer k such that $n = 2k$. We can then compute n^2 in terms of k , and this will lead to the desired result. ///

Proof. Assume that n is even. Then there is some integer k such that $n = 2k$. Hence $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ 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 were using 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 $P \rightarrow Q$, which appears similar to proof by contrapositive but is actually distinct,

is **proof by contradiction**. Recall from Section 1.3 that $\neg(P \rightarrow Q) \iff P \wedge \neg Q$. Suppose we could prove that $P \wedge \neg Q$ were false; we would then conclude that $\neg(P \rightarrow Q)$ is false, and hence $\neg(\neg(P \rightarrow Q))$ is true. It then follows, using the Double Negation equivalence (Fact 1.3.2 (i)), that $P \rightarrow Q$ must be true. The method of proof by contradiction shows that $P \rightarrow Q$ is true by assuming that $P \wedge \neg Q$ is true, and then deriving a logical contradiction (which implies that $P \wedge \neg Q$ is false). Another way to think about 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 when P is true and Q is false, that is, when 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.

Proof by contradiction implicitly uses the Double Negation equivalence, 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.) Any mathematician who does not believe in the law of the excluded middle would therefore object to proof by contradiction. There are some such mathematicians, though the majority, including the author of this book, are quite comfortable with the law of the excluded middle, and with proof by contradiction. (Logicians, we should mention, tend to use the term “proof by contradiction” to mean the proof of any statement A where you proceed by assuming $\neg A$, and arrive at a contradiction. For our purposes, we are primarily interested in statements A of the form $P \rightarrow Q$.)

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 method.

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 $P \rightarrow Q$, since we could restate it 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, since 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 note 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 . Since a , b and c are not 3, 4 and 5, we know that $a \neq 3$, and since 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. Thus we have a contradiction, and the theorem is proved. \square

Our next two theorems are famous results, both of which 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 at this point. The 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 the previous section). The real numbers form what is commonly referred to as the real number line, and are the collection of all numbers that are generally used in elementary mathematics (they do not contain the complex numbers, but those numbers do not concern us). We have the operations addition, subtraction, multiplication and division on the real numbers, and these operations satisfy standard properties, for example the commutative law for addition and subtraction. See the Appendix for a brief list of some of the standard properties of real numbers that we use. (We will discuss the real numbers in more detail in Section 8.6, though it is beyond the scope of this book to give a thorough treatment of the real numbers.) We now turn to the matter at hand.

Definition. Let x be a real number. We say x is a **rational number** if there exist integers n and m such that $m \neq 0$ and $x = n/m$. If x is not a rational number, we say it is an **irrational number**. \triangle

Note that if x is a rational number, then there are many different fractions of the form n/m such that $x = n/m$. Given any fraction n/m , we can always reduce it to “lowest terms,” by which we mean that the numerator and denominator have no common factors.

Are there any irrational numbers? 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 6.2). The following theorem says that $\sqrt{2}$ is an irrational number. To us this result 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 (which were related to the mathematics). Among other things, the Pythagoreans believed in the importance of whole numbers, and held that anything meaningful in the universe could be related to either whole numbers, or 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 $\sqrt{2}$. Thus $\sqrt{2}$ would be a geometrically meaningful number to the Pythagoreans. Hence they were very disturbed to discover that this number was not expressible as a ratio of whole numbers. Legend has it that the discoverer of this fact, in despair, threw himself overboard from a ship.

Theorem 2.3.3. *The number $\sqrt{2}$ is irrational.*

Preliminary Analysis. First, we need to recall what the “square root” of a number means. Suppose b is a non-negative real number. By definition, a number x is a square root of b iff $x^2 = b$. We can now rephrase our theorem in the form $P \rightarrow Q$ as follows. Let x be a real number. If $x^2 = 2$, then x is irrational. Our proof by contradiction starts by assuming that x is a real number such that $x^2 = 2$, and that x is not irrational (and hence it is rational). ///

Proof. Let x be a real number. Assume that $x^2 = 2$, and that x is rational. We will derive a contradiction. Since x is rational, there are integers n and m such that $x = n/m$. If n/m is not in lowest terms, then we could cancel any common factors, bringing it to lowest terms. There is no loss 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 .

Since $x^2 = 2$, we have $(n/m)^2 = 2$, and thus $n^2/m^2 = 2$, 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, since it is divisible by 2. Thus n cannot be odd; hence n must be even. Therefore there is some integer k such that $n = 2k$. Thus we have $(2k)^2 = 2m^2$, so that $4k^2 = 2m^2$, and thus $2k^2 = m^2$. We now ask whether m is even or odd, and by an argument just as before, we deduce that m is even. We therefore conclude that both n and m are even. We thus have a contradiction, since 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. \square

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. Let p be a positive integer greater than 1. We say that p is a **prime number** if the only positive integers that divide it are 1 and p . A positive integer is a **composite number** if it is not a prime number. Δ

Note that a positive composite number n can always be written as $n = ab$ for some positive integers a and b such that $1 < a, b < n$. The first few prime numbers are 2, 3, 5, 7, 11, The study of prime numbers is quite old and very extensive; see almost any book on elementary number theory, for example [Ros93a], for more details. How many prime numbers are there? The following theorem answers this question. The proof we give is the one most commonly used, and goes back to Euclid; see [Rib96, Chapter 1] for discussion, and for some other nice proofs of this theorem.

Theorem 2.3.4. *There are infinitely many prime numbers.*

Preliminary Analysis. Though it may not be immediately clear that this theorem has the form $P \rightarrow Q$, the theorem can be rephrased as “if there are prime numbers, then there are infinitely many of them.” So, we will start our proof by contradiction by supposing that there are prime numbers (which in fact is true, since 2 is a prime number), and that there are only finitely many of them. The idea of the proof is to take the finite collection of prime numbers, and use these numbers to produce a new prime number that is not in this collection, which would lead to a contradiction. $///$

Proof. We know that there are prime numbers; for example, the number 2 is a prime number. Assume that there are only finitely many prime numbers. We will derive a contradiction. Suppose P_1, P_2, \dots, P_n are all the prime numbers, for some positive integer n . Let $Q = (P_1 \times P_2 \times \dots \times P_n) + 1$. We will show that Q is a prime number. Since Q is clearly larger than any of the numbers P_1, P_2, \dots, P_n , we would then have a prime number that is not in the collection P_1, P_2, \dots, P_n , thus yielding the desired contradiction.

To show that Q is a prime number, we again use proof by contradiction, and so we suppose that Q is not prime. Thus Q is a composite number. By

Theorem 6.3.10, we deduce that Q has a prime number factor. (Though this theorem comes later – since it needs some tools we have not yet developed – it does not use the result we are now proving, so it is safe to use.) The only prime numbers are P_1, P_2, \dots, P_n , and thus one of these numbers must be a factor of Q . Suppose that P_k is a factor of Q , for some positive number k such that $1 \leq k \leq n$. Thus 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 (see Theorem 8.4.5 (viii) for a rigorous proof of this fact). Since P_k is a prime number it cannot possibly equal 1 or -1 , a contradiction. Thus Q could not have been a composite number, and hence it is a prime number. \square

Though we have proved that there are infinitely many prime numbers, our proof did not produce an explicit infinite list of prime numbers, but only proved that in theory such a list exists. In fact, no one has produced such a list for far. More generally, we distinguish between a constructive proof, which proves the existence of something by actually producing it, and an existence proof (such as the above proof), which only shows that in theory something exists. Existence proofs are one of the hallmarks of modern mathematics. A important proof in ring theory by Hilbert in 1890 (see [Hil90]) helped promote acceptance of existence proofs in modern mathematics, although at first this proof was controversial, prompting the famous response “Das ist nicht Mathematik. Das ist Theologie.” by Paul Gordan. Most mathematicians today accept existence proofs, but there is a minority who do not accept their validity. See [Ang94, Chapter 39], [GG94, Section 5.6] and [EC89, Chapter 26] for a discussion of the mathematical philosophies known as “intuitionism” and “constructivism,” which differ from mainstream mathematics; see [BR87, Section 4.6] for a constructivist discussion of Hilbert’s theorem.

Exercises

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, since the terms are meaningless).

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

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

2.3.4. [Used in Section 6.2.] Show that the product of a non-zero rational number and an irrational number is irrational.

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

2.3.6. Let c be a positive integer that is not a prime number. Show that there is some positive integer b such that $b|c$ and $b \leq \sqrt{c}$.

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

2.3.8. Let q be a positive integer such that $q \geq 2$ and such that for any integers a and b , if $q|ab$ then $q|a$ or $q|b$. Show 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 (also given in Section 1.3 and its exercises) to prove theorems that have certain types of statements.

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, etc.). Formally, we use proof by cases when the premise P can be written in the form $A \vee B$. We then apply Exercise 1.3.2 (6), which states 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, we prove that both the statements $A \rightarrow Q$ and $B \rightarrow Q$ are true. The use of this proof strategy often occurs when proving a statement involving a quantifier of the form “for all x in U ,” but where no single proof can be

found for all such x . A simple example of proof by cases is the following. 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. Since 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. Let $A = "n \text{ is an even integer,"}$ let $B = "n \text{ is an odd integer,"}$ and let $Q = "n^2 + n \text{ is even.}"$ Then the theorem has the form $(A \vee B) \rightarrow Q$. We will prove the theorem by proving that $(A \rightarrow Q)$ and $(B \rightarrow Q)$ 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 2.1.2 and Exercise 2.2.4, or from scratch; since the latter is simple enough, we will do that. $\//\//$

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

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

Since k is an integer so is $2k^2 + k$. Thus $n^2 + n$ is an even integer.

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

$$\begin{aligned} n^2 + n &= (2k + 1)^2 + (2k + 1) = (4k^2 + 4k + 1) + (2k + 1) \\ &= 4k^2 + 6k + 2 = 2(2k^2 + 3k + 1). \end{aligned}$$

Since k is an integer so is $2k^2 + 3k + 1$. Thus $n^2 + n$ is an even integer. \square

It is not really necessary to define A and B explicitly as we did in the scratch work above, and we will not do so in the future, but it seems worthwhile doing it once. In the above proof 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, where we proceed similarly. 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 $P \rightarrow (A \vee B)$. Such theorems are less common than the previously discussed type, but do occur on occasion, and it is worth being familiar with the standard proof

strategies. 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 (xiii)), which together imply that $P \rightarrow (A \vee B)$ is equivalent to $(\neg A \wedge \neg B) \rightarrow \neg P$. The other would be to use Exercise 1.3.2 (5), which says that $P \rightarrow (A \vee B)$ is equivalent to $(P \wedge \neg A) \rightarrow B$. The roles of A and B could also be interchanged in this last statement. The following proof uses the second approach, in order to give an example of it, although the first approach would work quite easily in this case. (See the proof of Theorem 8.4.5 (iv) for a more substantial use of the second approach.)

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 $P \rightarrow (A \vee B)$. We will prove $(P \wedge \neg A) \rightarrow B$, which we do by assuming that xy is irrational and that x is rational, and deducing that y is irrational. //

Proof. Assume that xy is irrational and that x is rational. Hence $x = a/b$ 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 $y = m/n$ for some integers m and n such that $n \neq 0$. Hence $xy = am/bn$, where $bn \neq 0$, contradicting the irrationality of xy . Hence y is irrational. \square

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

Not only are there a variety of ways to organize proofs, but there are also variants in the logical structure of 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 (abbreviated "iff" theorems). To prove such a theorem, we make use of the fact that $P \leftrightarrow Q$ is equivalent to $(P \rightarrow Q) \wedge (Q \rightarrow P)$, as was shown in Fact 1.3.2 (xi). Thus, to prove

a single statement of the form $P \leftrightarrow Q$, it will suffice 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, the proof of which is sufficiently straightforward so that we dispense with the scratch work. Recall the definition of divisibility of integers given in Section 2.2.

Theorem 2.4.3. *Let a and b be non-zero integers. Then $a|b$ and $b|a$ iff $a = b$ or $a = -b$.*

Proof. \Rightarrow . Assume that $a|b$ and $b|a$. Since $a|b$, there is some integer m such that $am = b$, and since $b|a$, there is some integer k such that $bk = a$. Plugging this last equation into the previous one, we obtain $(bk)m = b$, and hence $b(km) = b$. Since $b \neq 0$, it follows that $km = 1$. Because k and m are integers, we know that either $k = 1 = m$ or $k = -1 = m$ (see Theorem 8.4.5 (viii) for a rigorous proof of this fact). In the former case $a = b$, and in the latter case $a = -b$.

\Leftarrow . Assume 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 $b|a$. \square

Our next example of an iff theorem uses a number of the methods we have discussed so far.

Theorem 2.4.4. *Let m and n be integers. Then mn is odd iff 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 $mn = 2p + 1$ some integer p , but it is not clear how to go from here 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. $///$

Proof. \Leftarrow . Assume that m and n are both odd. Hence there are integers j and k such that $m = 2j + 1$ and $n = 2k + 1$. Therefore

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

Since k and j are integers so is $2jk + j + k$. Thus mn is an odd integer.

\Rightarrow . Assume 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. Assume first that m is even. Thus there is an integer j such that $m = 2j$. Hence $mn = (2j)n = 2(jn)$. Since j and n are integers so is jn . Therefore mn is even. Next assume that n is even. The proof that mn is even in this case is similar to the previous case, and we omit the details. \square

A slightly more built-up version of an iff 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,” abbreviated “TFAE” in some texts. The following theorem is an example of this type of result. We first recall some notation concerning matrices. A 2×2 matrix has the form $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for some real numbers a, b, c, d . The determinant of such a matrix is given by $\det M = ad - bc$, and the trace of the matrix is given by $\text{tr } M = a + d$. An upper triangular 2×2 matrix has the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ for some real numbers a, b, d .

Theorem 2.4.5. Let $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ be an upper triangular 2×2 matrix, and suppose that a, b and d are integers. The following are equivalent.

- (1) $\det M = 1$.
- (2) $a = d = \pm 1$.
- (3) $\text{tr } M = \pm 2$ and $a = d$.

What the above theorem says is that (1) iff (2), that (1) iff (3), and that (2) iff (3). Hence, to prove these three iff statements we would in theory need to prove that (1) \Rightarrow (2), that (2) \Rightarrow (1), that (1) \Rightarrow (3), that (3) \Rightarrow (1), that (2) \Rightarrow (3) and that (3) \Rightarrow (2). 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 (xii)). For example, suppose we could prove that (1) \Rightarrow (2), that (2) \Rightarrow (3) and that (3) \Rightarrow (1); the other three implications would then hold automatically. We could just as well prove that (1) \Rightarrow (3), that (3) \Rightarrow (2) and that (2) \Rightarrow (1), if that were easier.

Alternately, it would suffice to prove that $(1) \Rightarrow (3)$, that $(3) \Rightarrow (1)$, that $(1) \Rightarrow (2)$ and that $(2) \Rightarrow (1)$. Any collection of logical implications suffices if all the other logical implications of the original six can be deduced using transitivity; the choice depends upon the particular theorem being proved. Similar reasoning holds when more than three statements are being proved equivalent.

We can now proceed to the proof of Theorem 2.4.5.

Proof. We will prove that $(1) \Rightarrow (2)$, that $(2) \Rightarrow (3)$ and that $(3) \Rightarrow (1)$.

$(1) \Rightarrow (2)$. Assume that $\det M = 1$. This condition means that $ad = 1$. Since both a and d are integers, it must be the case that either $a = 1 = d$, or $a = -1 = d$.

$(2) \Rightarrow (3)$. Assume that $a = d = \pm 1$. First, suppose that $a = d = 1$. Then $\text{tr } M = a + d = 2$. Second, suppose that $a = d = -1$. Then $\text{tr } M = a + d = -2$. Hence $\text{tr } M = \pm 2$ and $a = d$.

$(3) \Rightarrow (1)$. Assume that $\text{tr } M = \pm 2$ and $a = d$. We can rewrite $\text{tr } M = \pm 2$ as $a + d = \pm 2$. Hence $4 = (a + d)^2 = a^2 + 2ad + d^2$. Since $a = d$, we deduce that $a^2 = ad = d^2$. Therefore $4 = 4ad$. Thus $ad = 1$, and since $\det M = ad$ for an upper triangular 2×2 matrix, it follows that $\det M = 1$.

□

Exercises

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

- (1) If an integer is combustible then it is even or prime.
- (2) A 2×2 matrix is collapsible iff 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.

2.4.2. Let a, b and c be integers such that $c \neq 0$. Show that $a|b$ iff $ac|bc$.

2.4.3. [Used in Sections 4.4 and 6.4.] Let a and b be integers. We say that 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 9.2 for further discussion and references.

(1) Find two integers a and b that are relatively prime. Find two integers c and d that are not relatively prime.

(2) Suppose that a and b are positive. Show that the following are equivalent.

- (i) a and b are relatively prime.
- (ii) $a + b$ and b are relatively prime.
- (iii) a and $a + b$ are relatively prime.

2.4.4. Let n be an integer. Show that one of the two numbers n and $n + 1$ is even, and the other is odd.

2.4.5. This exercise makes use of the definition given in Exercise 2.2.5. It can be shown that if n is an integer, then precisely one of the following holds: either $n = 3k$ for some integer k , or $n = 3k + 1$ for some integer k , or $n = 3k + 2$ for some integer k . (A proof of this fact is given in Exercise 8.4.16; this proof does not make use of the present exercise.) Let n and m be integers.

(1) Suppose that n is a multiple of 3 and that m is not a multiple of 3. Show that $n + m$ is not a multiple of 3.

(2) Show that mn is a multiple of 3 iff m or n is a multiple of 3.

2.4.6. Find all triples of numbers p , $p + 2$ and $p + 4$ such that all three numbers are prime numbers. Prove that you have all such triples. (For the proof, use the discussion at the start of Exercise 2.4.5.)

2.4.7. Let n be an odd integer. Show 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 . (All you need is the fact that every integer is even or odd.)

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

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

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

Let x and y be real numbers. Prove the following statements.

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

- (2) $|x|^2 = x^2$.
- (3) $|x - y| = |y - x|$.
- (4) $|xy| = |x||y|$.

2.4.10. Let x and y be real numbers. Define $x \sim y$ and $x \curvearrowleft y$ to be

$$x \sim y = \begin{cases} x, & \text{if } x \geq y \\ y, & \text{if } x \leq y, \end{cases} \quad \text{and} \quad x \curvearrowleft y = \begin{cases} y, & \text{if } x \geq y \\ x, & \text{if } x \leq y. \end{cases}$$

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) $(a \sim b) + (a \curvearrowleft b) = a + b$.
- (2) $(a \sim b) + c = (a + c) \sim (b + c)$ and $(a \sim b) + c = (a + c) \curvearrowleft (b + c)$.
- (3) $(a \sim b) \sim c = a \sim (b \sim c)$ and $(a \sim b) \curvearrowleft c = a \curvearrowleft (b \sim c)$.
- (4) $(a \sim b) - (a \curvearrowleft b) = |a - b|$.
- (5) $a \sim b = \frac{1}{2}(a + b + |a - b|)$ and $a \curvearrowleft b = \frac{1}{2}(a + b - |a - b|)$.

2.4.11. Let x be a real number. We let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x . To clarify this definition, we note that there are unique numbers I_x and $\#x$ such that I_x is an integer, that $0 \leq \#x < 1$ and that $x = I_x + \#x$. Then $\lfloor x \rfloor = I_x$. Let x and y be real numbers. Prove the following statements.

- (1) $\lfloor x \rfloor + \lfloor -x \rfloor$ equals either 0 or -1 .
- (2) $\lfloor x + y \rfloor$ equals either $\lfloor x \rfloor + \lfloor y \rfloor$ or $\lfloor x \rfloor + \lfloor y \rfloor + 1$.
- (3) $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor \leq \lfloor x \rfloor \lfloor y \rfloor + \lfloor x \rfloor + \lfloor y \rfloor$.

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 those who are new to proof writing. 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 that section 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, since it could 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 a typical integer that we labeled n (any other symbol would do), and proved the result for this typical 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, 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 we want to prove a theorem with statement of the form $(\forall x \text{ in } U)P(x)$. The key observation is to notice 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 thus 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 such a choice of x_0 . The outline of this type of proof would thus typically have the form "Let x_0 be in U (argumentation) . . . Then $P(x_0)$ is true." The point is that we prove that $P(x)$ is true for all x in U by picking an arbitrary x_0 in U , and proving that $P(x_0)$ is true; since x_0 is arbitrary we would then have shown that $P(x)$ is true for all x in U . It is crucial that we pick an arbitrary x_0 in U , not some particularly convenient value. We stress, once again, that we cannot 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 given by the formula $f(n) = n^2 + n + 41$. If you substitute the numbers $n = 0, 1, 2, \dots, 39$ into this function, then you obtain the numbers 41, 43, 47, ..., 1601, all of which are prime numbers. It thus might appear that plugging in every positive integer into this function would result in a prime number (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 , then it does not suffice to try only some (even many) 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 instance, we can use the method of proof by contradiction to prove the statement “if x is in U , then $P(x)$ is true.” Such a proof would have the form “Let y_0 be in U , and suppose that $P(y_0)$ is false. . . . (argumentation) . . . 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.

The other common type of statement containing a single quantifier involves the existential quantifier, and has 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 $(\exists x)P(x)$, 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.” A typical outline for writing up such a proof would be “Let $z_0 = \text{blah. . . (argumentation) . . . Then } z_0 \text{ is in } U, \text{ and } P(z_0) \text{ is true.}”$

How we find the element z_0 in the above discussion 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, since, 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.

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

Scratch Work. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The condition $\det A = 4$ means that $ad - bc = 4$; the condition $\text{tr } A = 7$ 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 we obtain

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

Since 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 $A = \begin{pmatrix} 5 & 2 \\ 3 & 2 \end{pmatrix}$. Then $\det A = 5 \cdot 2 - 2 \cdot 3 = 4$, and $\text{tr } A = 5 + 2 = 7$. □

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 actually 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, since we were showing 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. Also, since we were only asked to show that A existed, and not describe how many possible values of A there were, we only needed to mention 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 they are often unnoticed, and rarely criticized — even though they

should be. While such 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 we are asked to solve the equation $7x + 6 = 21 + 4x$. A typical solution submitted by a high school student might look like

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

There is nothing wrong with the algebra here, and indeed $x = 5$ is the correct solution. For computational mathematics such a solution 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 great pedagogical interest, of course). The proposed solutions simply have to be listed, and then tested in the equation. A logically correct “forwards” solution to our original equation would be

“Let $x = 5$. Plugging $x = 5$ into the left hand side of the equation yields $7x + 6 = 7 \cdot 5 + 6 = 41$, whereas plugging it into the right hand side of the equation yields $21 + 4x = 21 + 4 \cdot 5 = 41$. Thus $x = 5$ is a solution. Since the equation is linear, it has only one solution. Hence $x = 5$ is the only solution.”

Such a write-up seems ridiculously long, given the simplicity of the original equation. 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.

Suppose 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

$$\begin{aligned}\sqrt{x^2 - 5} &= \sqrt{x + 1} \\ x^2 - 5 &= x + 1 \\ x^2 - x - 6 &= 0 \\ (x - 3)(x + 2) &= 0 \\ x = 3 \quad \text{or} \quad x &= -2.\end{aligned}\tag{2.5.2}$$

The written solution is definitely not correct, since $x = -2$ is not a solution to the original equation. It is not even possible to plug $x = -2$ into either side of the original equation. The source of the error is that not every step in the calculation is reversible (we leave it to the reader to figure out which one). In an elementary course such as high school algebra or calculus, it would suffice to write up the above computation, and then note 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 are theorems that involve existence and uniqueness, of which the following theorem is an example. Recall the definitions concerning 2×2 matrices prior to Theorem 2.4.5. Additionally, we will need the 2×2 identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. 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 $AB = I = BA$. Do all 2×2 matrices have inverses? The answer is no. For example, the matrix $\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$ has no inverse. Our 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 need 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 them separately. It makes no difference which part is proved first. To prove existence, we proceed as above, 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 objects are actually the same, but there is rarely any advantage to using this alternate strategy.)

Scratch Work. We will 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 inverses, 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 for A would be as follows. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Suppose $B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ is an inverse 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

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

in the four variables x , y , z and w . We can then solve for these variables in terms of a , b , c and d . To do so, we will have to make use of the fact that $\det A \neq 0$, which means $ad - bc \neq 0$. The solution to these four equations turns out to be $x = d/(ad - bc)$, and $y = -b/(ad - bc)$, and $z = -c/(ad - bc)$ and $w = a/(ad - bc)$. ///

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

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

Since $B = C$, 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

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

We then compute

$$\begin{aligned} AB &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \left(\frac{ad}{ad-bc} + \frac{-bc}{ad-bc}, \frac{-ab}{ad-bc} + \frac{ab}{ad-bc} \right) \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I. \end{aligned}$$

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

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. Using what we learned in Section 1.5, we see that $\neg[(\forall x \text{ in } U)Q(x)]$ is equivalent to $(\exists x \text{ in } U)(\neg Q(x))$. Thus to prove that the original statement is false, it suffices 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, namely by finding some x_0 in U such that $(\neg Q(x_0))$ is true (that is, 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 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 $Q(x) = \text{“if } x \text{ is prime, then it is odd.”}$ Using the reasoning above, it suffices to prove that $(\exists x)(\neg Q(x))$ is true. Using Fact 1.3.2 (xiv), we see that $\neg Q(x)$ is equivalent to “ x is prime, and not odd.” Hence, we need to find some integer x_0 such that x_0 is prime, and 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). 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, since you would have to examine all possible cases, and show that none of them have the desired properties. Rather we use the fact that $\neg[(\exists y)R(y)]$ is equivalent to $(\forall y)(\neg R(y))$, proving by our usual methods that $\neg R(y)$ holds for all y .

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 $(\exists a)(\forall b)Q(a, b)$, or have more quantifiers. There is no point in giving detailed instructions on how to proceed for each different combination of quantifiers, because there are many possible combinations, 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, namely $\forall a$. 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 just 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. Thus 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 can do a backwards computation to solve for b . We find that $b = \pm\sqrt{(a_0)^2 + 4}$, 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. Define $b_0 = \sqrt{(a_0)^2 + 4}$. 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. We thus need to find a single real number x_0 such that $(\forall y)((3 - x_0)(y^2 + 1) > 0)$ is true. That is, we need to find a single 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 only one value of x_0 that works, so let us randomly pick $x_0 = 2$. ///

Proof. Let $x_0 = 2$. Let y_0 be a real number. Note 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 . \square

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 our previous discussion concerning the negation of statements with quantifiers, we see 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 $(a_0)^2 - (b_0)^2 + 4 \neq 0$. Thus the negation of the original statement is true, so the original statement is false. We therefore see that the order of the quantifiers in Proposition 2.5.3 does matter. On the other hand, it can be seen that changing the order of the quantifiers in the statement of Proposition 2.5.4 does affect its truth.

Exercises

2.5.1. Convert the following statements, which do not have their quantifiers explicitly given, into statements with explicit quantifiers (do not prove them, since 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 $\text{tr } M$.

2.5.2. A problem that might be given in a high school mathematics class is “Show that the equation $e^x = 5$ has a unique solution.” We could rewrite the problem as “Show 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. Then write up a proper solution to the problem, using the ideas discussed in this section. Write up the uniqueness part of the proof 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).

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 , we have $s \geq t$.
- (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 , we have $s \geq t$.

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 , we have $a|b$.
- (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 , we have $a|b$.

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 , we have $e^x - y > 0$.
- (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 , we have $e^x - y > 0$.

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

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

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 $e^{3x} + y = y^2 - 1$.

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 $q \sin(r/5) = p$.

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 $z^2 + 2xz - y^2 = 0$.

2.5.10. Let $P(x, y)$ be a statement with free variables x and y , which are real numbers. Let a and b be real numbers. We say that the real number u is 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; 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 . Show that this least P -number is unique. (One familiar example of this situation is the least common multiple of two numbers.)

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:

$$\begin{aligned}x(x - 1) &= 2(x + 2) \\x^2 - x &= 2x + 4 \\x^2 - 3x - 4 &= 0 \\(x - 4)(x + 1) &= 0 \\x = 4 \quad \text{or} \quad x &= -1.\end{aligned}$$

Thus there are two solutions.”

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 the writer to pay attention to all the details of an argument. Often an idea that seemed to make sense in a person’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 it seemed at first.

Mathematical correctness is certainly the ultimate test of the validity of a proof. 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], [SHSD73] and [KLR89] 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 to 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. Precision is key. 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 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 (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. Since a proof should aim to convince the reader, that person is the one to judge what is obvious. 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 this 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 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 “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. As previously mentioned, the two-column approach to proofs often used in high school geometry should now be discarded.

A proof is a logical argument. A well-written proof is a logical argument that someone else can understand. Proper grammar helps the reader follow the logical flow of an argument. Connective words such as “therefore,” “hence,” and “it follows that” help guide the logical flow of an argument, 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 are both condensations of the proof of Theorem 2.3.3. Both proofs, which contain all the mathematical ideas of the original proof, are not unlike many homework assignments I have graded, and are written without regard to proper grammar and style. Compare these versions of the proof with the write-up of the proof originally given in Section 2.3.

This first version is genuinely awful, though for reasons that I do not understand, some students seem to be given the impression in high school that this sort of writing is proper mathematical style.

$$x^2 = 2 \text{ and } x \text{ rational}$$

$$\therefore x = n/m$$

n and m have no common factors

$(n/m)^2 = 2 \Rightarrow n^2/m^2 = 2 \Rightarrow n^2 = 2m^2$ 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 $x = n/m$; n and m have no common factors. $(n/m)^2 = 2$, $n^2/m^2 = 2$, $n^2 = 2m^2$. If n were odd, then n^2 would be odd by Exercise 2.2.4 — a contradiction since $2m^2$ is even since 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 since 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 beginning mathematics students both 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 a student is asked to take the derivative of the function given 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, and is therefore extremely confusing to anyone other than the writer of the statement. The second type of mistake occurs when someone writes “ $f(x) = x^2$, and so $2x$.” Here it is not clear what the writer means 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 “ $f(x) = x^2$, so $f'(x) = 2x$,” or simply “ $(x^2)' = 2x$.”

Another common type of error involving “=” signs involves lengthier calculations. Suppose we were asked to show that

$$\sqrt{x^2 + 2x} \sqrt{x^2 - 4\sqrt{x^2 - 2x}} = x^3 - 4x.$$

An incorrect way of writing the calculation, which the author has seen very regularly on homework assignments, would be

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

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.

Another incorrect way of writing this same calculation, and also one that the author has seen regularly, is

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

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 usually deduce what the writer of such a collection of formulas meant, but there is no advantage in forcing the reader to guess, so 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 “ $\sqrt{x^2 + 2x} \sqrt{x^2 - 4} \sqrt{x^2 - 2x} = x^3 - 4x$ ” is a complete sentence, with subject “ $\sqrt{x^2 + 2x} \sqrt{x^2 - 4} \sqrt{x^2 - 2x}$,” with verb “=” and with object “ $x^3 - 4x$.” To drop the = sign is to drop the verb in this sentence. It is baffling to this author why students who would never turn in papers with missing verbs in literature courses would do so in a mathematics course, except that perhaps no one has ever told them that doing so is inappropriate. Indeed, both these improper ways of writing lengthy calculations are, unfortunately, actually taught to many students in high school. These approaches should be discarded.

There are a number of correct ways of writing this calculation, for example

$$\begin{aligned}\sqrt{x^2 + 2x} \sqrt{x^2 - 4} \sqrt{x^2 - 2x} &= \sqrt{x(x+2)} \sqrt{(x+2)(x-2)} \sqrt{x(x-2)} \\&= \sqrt{x^2(x+2)^2(x-2)^2} \\&= x(x+2)(x-2) \\&= x^3 - 4x,\end{aligned}$$

or

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

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. There is no success in mathematics without attention to details. 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 Pascal or C++, 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, we cannot rely on such a convention, since 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 had the statement “for each integer n of type A , there is an integer p such that *blah*.” 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 an integer of type A , 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 like “let n be an integer of type A .”

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.

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 have 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 these points 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 (periods, commas, etc.). When a symbol follows punctuation, there might be some confusion as to whether or not the punctuation is part of the symbol. As a corollary, do not start a sentence with a symbol.

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, since $y \leq 0$, 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. Logical symbols make proofs harder for others to read (unless you are writing about logic). Of course, you may use symbols 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,” or instead of punctuation, or as a substitute for something properly expressed in words.

Bad: $n = \text{odd} = 2k + 1$.

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 by $i + 1$.

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 upper case letters for matrices and lower case 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 take 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 often bad style. 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. There is rarely need for a colon other than in a heading or at the start of a list. 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: $10^2 - 4 \cdot 1 \cdot 3 \neq 0$.

Good: The equations $x^2 + 10x + 3 = 0$ has two real solutions because $10^2 - 4 \cdot 1 \cdot 3 \neq 0$.

- (G) Capitalize names such as “Theorem 2.3” and “Lemma 17.” No capitalization is needed in phrases such as “by the previous theorem.”

Exercises

- 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 $x^2 + 6x = 16$:

$$\begin{aligned}x^2 + 6x &= 16 \\x^2 + 6x - 16 &= 0 \\(x - 2)(x + 8) &= 0\end{aligned}$$

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 thus $x = 2$, $x = -8$.

(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

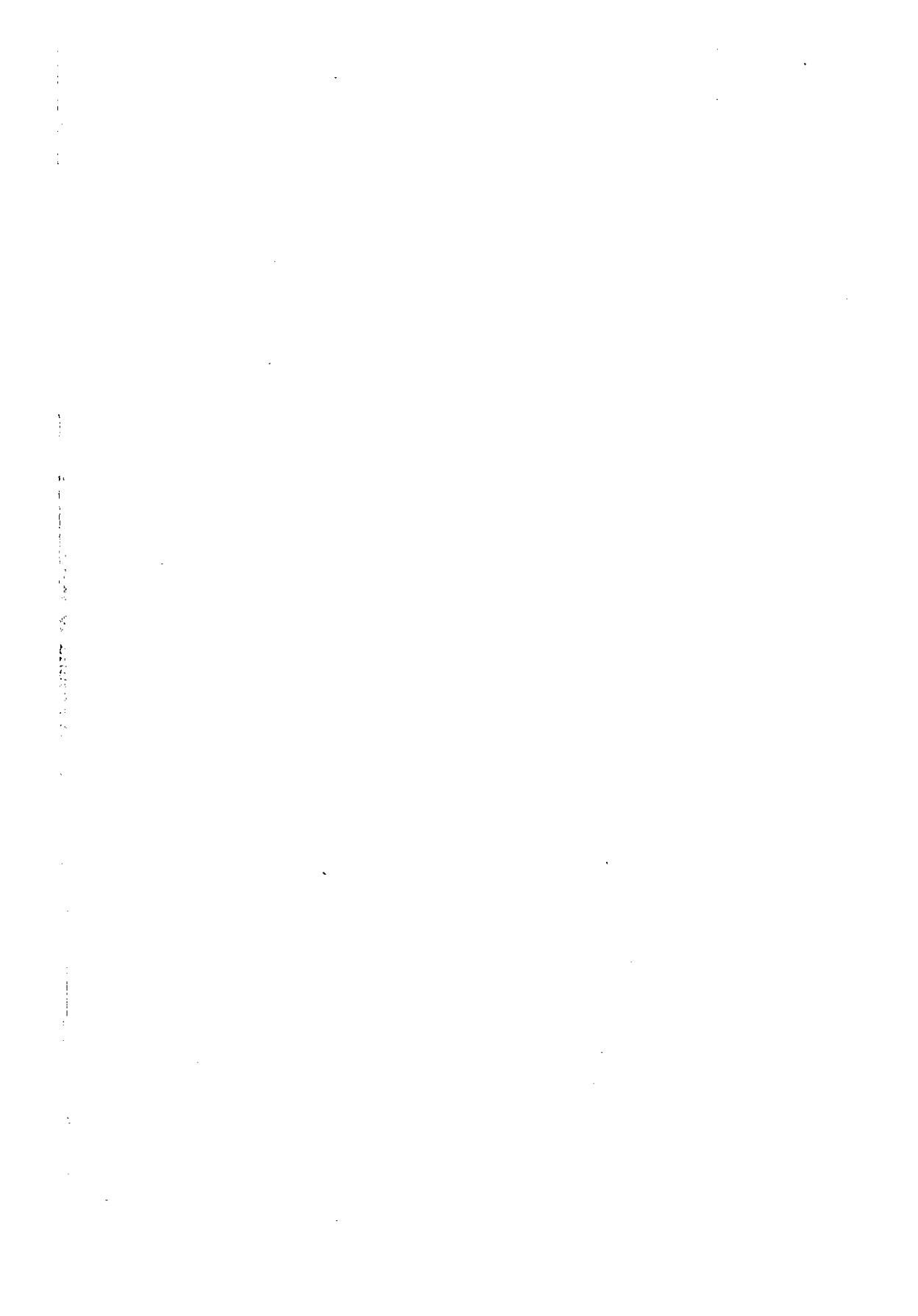
$$\begin{aligned}(7 + 2y)(y^2 + 5y - 6) \\7y^2 + 35y - 42 + 2y^3 + 10y^2 - 12y \\2y^3 + 17y^2 + 23y - 42\end{aligned}$$

the answer is $2y^3 + 17y^2 + 23y - 42$.

(6) We say that a real number x is gloppy if there is some integer n such that $x^2 - n$ is sloppy. Suppose that x is gloppy. Since 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 ,

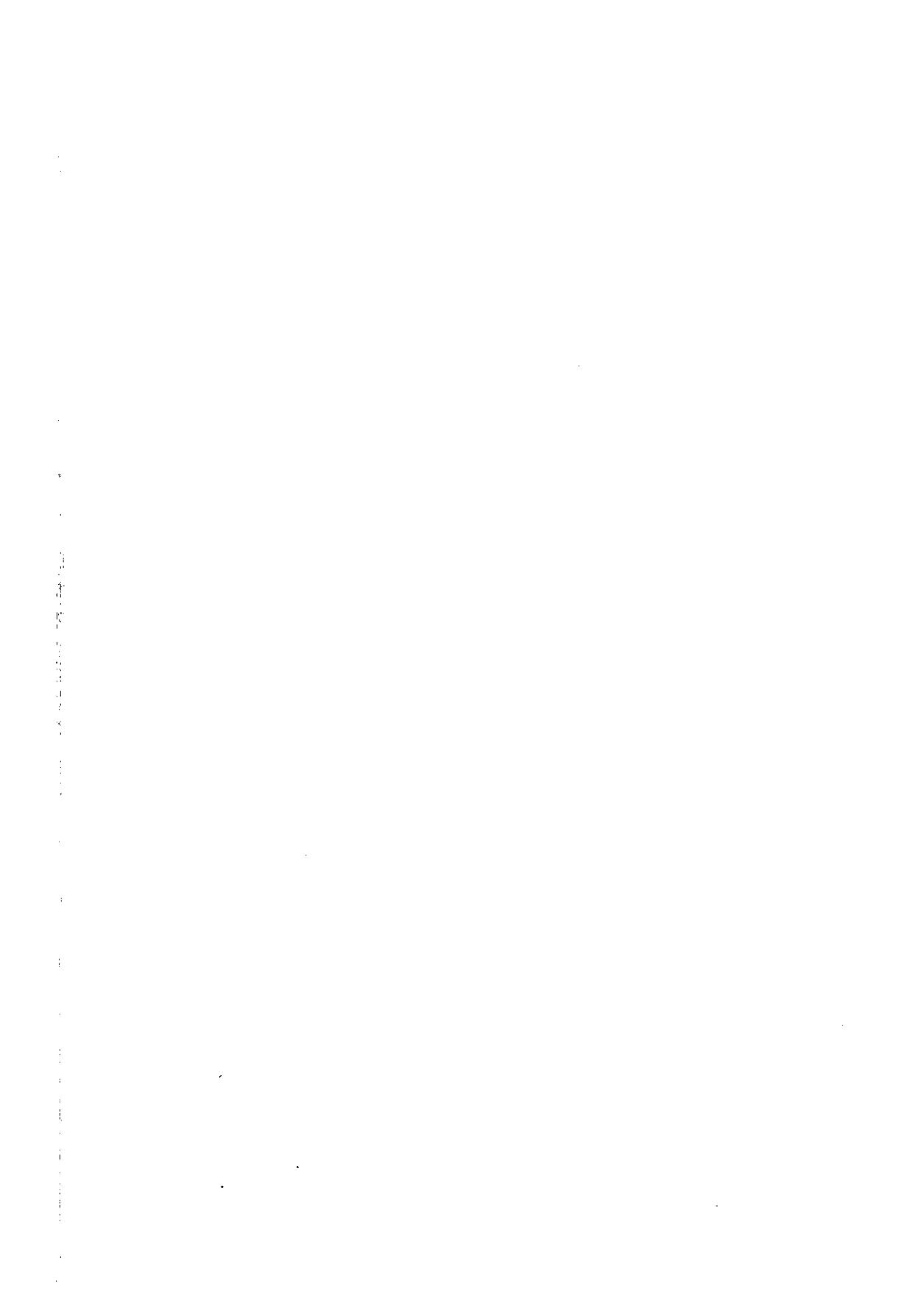
(8) It is known that $\sqrt{a} < a$ for all $a > 1$. Thus $\sqrt{a} + 3 < a + 3$. Hence $(\sqrt{a} + 3)^2 < (a + 3)^2$.



Part II

FUNDAMENTALS

We turn now from the essential “how” of mathematics, which is the methodology of proofs, to the essential “what,” which is basic ideas such as sets, functions and relations. These ideas are used in all of modern mathematics. The tone and style of writing in the text now changes corresponding to the change in content. We will have less informal discussion, and will write in the more straightforward definitiontheorem/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 have 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 more details on both these issues.)

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 utterly 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. (This critique of Euclid is in no way intended to deny the overwhelming importance of his work.)

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 is quite comfortable with undefined terms. The view is that undefined objects do not so much exist in themselves as they are determined by the axiomatic properties hypothesized for them.

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 the pure variety) is thus 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). 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, topology, were only arrived at 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. (Mathematicians do, of course, find real pleasure in doing mathematics — that is why most of us do it.)

In this text we will not focus on any particular axiomatic system (though a few will be given in Chapters 7 and 8), but rather we will discuss the common basis for all axiom systems used in contemporary mathematics,

namely 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. See [Sup60], [Ham82], [Dev93] and [Vau95] for more about axiomatic set theory. The text [Hal60] is a classic reference for naive set theory. See [EFT94, Section 7.4] for a discussion of the role of set theory as a basis for mathematics.

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 contained 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 we write 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 $\{2, 3, 1\}$. We list each element of a set 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

$$\mathbb{N} = \{1, 2, 3, \dots\};$$

the set of integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\};$$

the set of rational numbers (also called fractions), denoted \mathbb{Q} ; the set of real numbers, denoted \mathbb{R} . The symbols \mathbb{N} , \mathbb{Z} , \mathbb{Q} and \mathbb{R} are quite standard. For convenience we will let \mathbb{Z}^m denote the set of non-negative integers $\{0, 1, 2, \dots\}$, and let \mathbb{R}^+ denote the set of positive real numbers (there are no completely standard symbols for these sets).

An extremely valuable set we will regularly encounter is the **empty set**, (also known as 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 relatively late arrival, and presumably seemed strange to some at first as well; today we simply 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. We can often 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 wanted 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

$$S = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k^2\}. \quad (3.2.1)$$

The letters n and k used in this definition are “dummy variables.” We would obtain the exact same set if we wrote

$$S = \{x \in \mathbb{Z} \mid \text{there exists } r \in \mathbb{Z} \text{ such that } x = r^2\}. \quad (3.2.2)$$

A useful example of sets that are defined in the style just mentioned are intervals in the real number line, which we summarize here. Let $a, b \in \mathbb{R}$

be any two numbers. We then define the following sets.

Open interval:

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}.$$

Closed interval:

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}.$$

Half-open intervals:

$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\},$$

$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}.$$

Infinite intervals:

$$[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\},$$

$$(a, \infty) = \{x \in \mathbb{R} \mid a < x\},$$

$$(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\},$$

$$(-\infty, b) = \{x \in \mathbb{R} \mid x < b\},$$

$$(-\infty, \infty) = \mathbb{R}.$$

There are no intervals that are “closed” at ∞ or $-\infty$ (for example, there is no interval of the form $[a, \infty]$), since ∞ is not a real number, and therefore it cannot be included in an interval contained in the real numbers. We are simply using the symbol ∞ to tell us that an interval “goes on forever.”

Recall the subsection entitled “Define All Symbols and Terms You Make Up” in Section 2.6. It is important to recognize that since the letters x and r in Equation 3.2.2 are dummy variables, we cannot use them outside the “ $\{ \mid \}$ ” notation without redefinition. Thus, if we want to refer to some element of the set defined in 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 $x \geq 0$.” We could say “observe that $x \geq 0$ for all $x \in S$.” This latter formulation, though correct, has the defect that if we want to continue to discuss elements in S , we would have to define x once again, since 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.

Just as there are various relations between numbers (such as equality and less than) there are relations between sets. The following is the most important such relation.

Definition. Let A and B be sets. We say that A is a *subset* of B if $x \in A$ implies $x \in B$. If A is a subset of B we write $A \subseteq B$. If A is not a subset of B , we write $A \not\subseteq B$. Δ

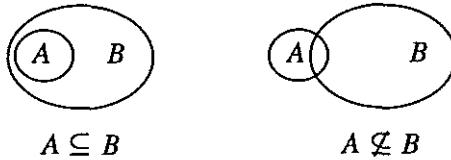


Figure 3.2.1.

Intuitively, we have $A \subseteq B$ whenever the set A is contained in the set B . The standard strategy for proving a statement of the form " $A \subseteq B$ " is to start by taking a typical element $a \in A$, and then to use the definitions of A and B to deduce that $a \in B$. Such a proof would typically look like "Let $a \in A$ (argumentation) . . . Then $a \in B$. Hence $A \subseteq B$." We will see a number of such proofs 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 $a \notin B$. (We could write what we are doing here using quantifiers as follows. We write $A \subseteq B$ 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 Equation 1.5.1 and Fact 1.3.2 (xiv).)

Example 3.2.1.

(1) Let A and B be the sets given by

$$A = \{1, 2, 3, 4\}, \quad \text{and} \quad B = \{1, 3\}.$$

Then $B \subseteq A$ and $A \not\subseteq B$.

(2) If P is the set of all people, and if M is the set of all men, then $M \subseteq P$. If T is 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

It is important to distinguish between the notion of one thing being an element of a set and the notion of one set being a subset of another set. For example, suppose $A = \{a, b, c\}$. Then $a \in A$ and $\{a\} \subseteq A$ are both true, whereas the statements " $a \subseteq A$ " and " $\{a\} \in A$ " are both false. Also, note that a set can be an element of another set. Suppose that $B = \{\{a\}, b, c\}$. Observe that B is not the same as the set A . Here $\{a\} \in B$ 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 using sets, is quite standard. In each of the three parts we show that one set is a subset of another by using the strategy mentioned just before Example 3.2.1.

Lemma 3.2.2. *Let A , B and C be sets.*

- (i) $A \subseteq A$.
- (ii) $\emptyset \subseteq A$.
- (iii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof. (i). To show that $A \subseteq A$, we start by choosing a typical 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 subset.

(ii). We give two proofs, since both are instructive, starting with a direct proof. To show that $\emptyset \subseteq A$, we need to show that if $a \in \emptyset$, then $a \in A$. Since $a \in \emptyset$ is always false, then the logical implication “if $a \in \emptyset$, then $a \in A$ ” is always true, using our precise definition of the conditional given in Section 1.2.

Next, we have a proof by contradiction. Assume $\emptyset \not\subseteq A$. Then there exists some $x \in \emptyset$ such that $x \notin A$. This statement cannot be true, however, since there is no x such that $x \in \emptyset$. Thus the desired result is true. (If this proof by contradiction does not appear to fit the standard outline for such proofs as described in Section 2.3, it can be put in the standard form by noting that the precise statement we are proving is “if A is a set, then $\emptyset \subseteq A$,” so the statement we are proving here is indeed of the form $P \rightarrow Q$. The interested reader can supply the rest of the details.)

(iii). This proof, having no logical monkey business, is extremely typical. Let $a \in A$. Since $A \subseteq B$, it follows that $a \in B$. Since $B \subseteq C$, it follows that $a \in C$. Thus 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. Let A and B be sets. We say that A equals B , denoted $A = B$, if $A \subseteq B$ and $B \subseteq A$. We say that A is a proper subset of B if $A \subseteq B$ and $A \neq B$; we write $A \subsetneq B$ to indicate that A is a proper subset of B . Δ

This definition gives rise to a standard strategy for proving the equality of two sets, namely proving that each is a subset of the other. Note that the word “subset” and the symbol “ \subseteq ” do not necessarily mean “proper subset.” There is a bit of variation in the notation used for proper subsets among different texts. Some texts use $A \subset B$ to mean A is a proper subset of B , whereas others use the notation $A \subsetneq B$ to mean what we write as $A \subseteq B$.

Example 3.2.3.

(1) Let A and B be the sets in Example 3.2.1 (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 $P = Q$, using the standard strategy, 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.

To 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 $3 < y$; since there is no number that satisfies both these inequalities, then this case cannot occur. In the other case, we have $y - 2 > 0$ and $y - 3 < 0$, and so $2 < y$ and $y < 3$. Thus $2 < y < 3$. Hence $y \in Q$.

To 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 $z - 3 < 0$. Thus $(z - 2)(z - 3) < 0$, and therefore $z^2 - 5z + 6 < 0$. Hence $z \in P$, and so $Q \subseteq P$. Combining this paragraph with the previous one, we see that $P = Q$. \diamond

The above examples may seem trivial, but the strategy used is not. Virtually every time we need to 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 thus to prove that $A \subseteq B$ and that $B \subseteq A$. Such a proof will usually have the form “Let $a \in A$ (argumentation) . . . Then $b \in B$. Thus $A \subseteq B$. Next, Let $b \in B$ (argumentation) . . . Then $a \in A$. Hence $B \subseteq A$. Therefore $A = B$.” We will

see a number of examples of the use this strategy, starting with the proof of Theorem 3.3.2 (iv) 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 3.2.4. *Let A , B and C be sets.*

- (i) $A = A$.
- (ii) *If $A = B$ then $B = A$.*
- (iii) *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 and Lemma 3.2.2. Details are left to the reader. \square

In some situations we will find it useful to look not just at one subset of a given set, but at all subsets of the set.

Definition. Let A be a set. The **power set** of A , denoted $\mathcal{P}(A)$, is the set whose elements are the subsets of A . \triangle

Example 3.2.5. 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 are listing all subsets, not only the proper ones. We thus have

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

It can be seen intuitively that if A is a finite set with n elements, then $\mathcal{P}(A)$ has 2^n elements. Try a few cases to verify this claim. A proof of this fact is given in Theorem 7.7.3. \diamond

Sets can be either finite or infinite in size. The set A in the above example 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 6.1. 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 6.1, 7.6 and 7.7.

We conclude this section by briefly mentioning that whereas set theory is used as the basis for modern mathematics, it does not work quite as nicely

as we might have made it appear. Early in the development of set theory, a number of “paradoxes” were discovered, the most well-known of which is Russell’s Paradox. Suppose we could form the set of all sets; let S denote this set. Note 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, it turns out, is that we are quantifying over sets. (See [GG94, Section 5.3] for further comments on the paradoxes of set theory.)

In our use of sets, 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 constructs. To treat set theory rigorously, however, some subtlety is needed. Various axiom systems for set theory have been developed that avoided any paradoxes, the most common being the Zermelo-Fraenkel axioms. See [Vau95, Introduction] for a succinct discussion of the history of set theory and its axiomatization.

One particular axiom of set theory worth mentioning is the famous Axiom of Choice. Intuitively, this axiom states that if we have a collection of sets, we can simultaneously choose one element from each of the sets in the collection. For a finite collection of sets, this axiom may seem rather unremarkable, but it is less clear that the Axiom of Choice makes sense intuitively when choosing out of an infinite collection of sets (particularly an uncountable collection — uncountability will be defined in Section 6.1). We single out this axiom of set theory because there are mathematicians who do not accept its use. It turns out that the Axiom of Choice is independent of other axioms for set theory (see [Mal79, p. 57]), and hence it can either be accepted or not without having to change the other axioms. The author (and the majority of mathematicians) have no qualms about using the Axiom of Choice, but since some mathematicians do have reservations about it, this axiom should always be mentioned when it is used. (We will use this axiom in the proof of Theorem 4.4.3). See [Moo82] and [Dev93, Section 2.7] for further discussion of the Axiom of Choice.

Exercises

3.2.1. Which of the following are true and which are false?

- | | |
|----------------------------------------|------------------------------------------------------|
| (1) $3 \in (3, 5]$. | (6) $[1, 2] \subseteq \{0, 1, 2, 3\}$. |
| (2) $10 \notin (-\infty, \pi^2]$. | (7) $\{-1, 0, 1\} \subseteq [-1, 1]$. |
| (3) $7 \in \{2, 3, \dots, 11\}$. | (8) $[5, 7] \subseteq (4, \infty)$. |
| (4) $\pi \in (2, \infty)$. | (9) $\{2, 4, 8, 16, \dots\} \subseteq [2, \infty)$. |
| (5) $-1.3 \in \{\dots, -3, -2, -1\}$. | |

3.2.2. 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) $\{x \in \mathbb{R} \mid \text{there exist } a, b \in \mathbb{Z} \text{ such that } b \neq 0 \text{ and } x = a/b\}$.

3.2.3. 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) $\{x \in P \mid \text{there exist } n \in M \text{ such that } x \text{ is the child of } n, \text{ and } x \text{ is older than } n\}$.

3.2.4. 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 $\{1, 5, 9, 13, 17, 21, \dots\}$.

3.2.5. We assume for this problem that functions are intuitively familiar to the reader (a more 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?

3.2.6. Among the following sets, which is a subset of which?

$$M = \{\text{the set of all men}\};$$

$$W = \{\text{the set of all women}\};$$

$$P = \{\text{the set of all parents}\};$$

$$O = \{\text{the set of all mothers}\};$$

$$F = \{\text{the set of all fathers}\};$$

$$U = \{\text{the set of all uncles}\};$$

$$A = \{\text{the set of all aunts}\};$$

$$C = \{\text{the set of all people who are children of other people}\}.$$

3.2.7. Among the following sets, which is a subset of which?

$$C = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k^4\};$$

$$E = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = 2k\};$$

$$P = \{n \in \mathbb{Z} \mid n \text{ is prime}\};$$

$$N = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k^8\};$$

$$S = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = 6k\};$$

$$D = \{n \in \mathbb{Z} \mid \text{there exists } k \in \mathbb{Z} \text{ such that } n = k - 5\};$$

$$B = \{n \in \mathbb{Z} \mid n \text{ is non-negative}\}.$$

3.2.8. 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 3.2.1; the solution, however, is the “exception that proves the rule.”)

3.2.9. How many elements does the set $A = \{a, b, \{a, b\}\}$ have?

3.2.10. Let A , B and C be sets. Suppose that $A \subseteq B$ and $B \subseteq C$ and $C \subseteq A$. Show that $A = B = C$.

3.2.11. 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.

3.2.12. Let $A = \{x, y, z, w\}$. List all the elements in $\mathcal{P}(A)$?

3.2.13. Let A and B be sets. Suppose that $A \subseteq B$. Show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

3.2.14. List all elements of each of the following sets.

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

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

3.2.15. Which of the following are true and which are false?

- (1) $\{\emptyset\} \subseteq G$ for all sets G ;
- (2) $\emptyset \subseteq G$ for all sets G ;
- (3) $\emptyset \subseteq \mathcal{P}(G)$ for all sets G ;
- (4) $\{\emptyset\} \subseteq \mathcal{P}(G)$ for all sets G ;
- (5) $\emptyset \in G$ for all sets G ;
- (6) $\emptyset \in \mathcal{P}(G)$ for all sets G ;
- (7) $\{\{\emptyset\}\} \subseteq \mathcal{P}(\emptyset)$;
- (8) $\{\emptyset\} \subseteq \{\{\emptyset\}, \{\{\emptyset\}\}\}$;
- (9) $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

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. 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

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}. \quad \Delta$$

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 3.3.1. Let A and B be the sets

$$A = \{x, y, z, p\} \quad \text{and} \quad B = \{x, q\}.$$

Then

$$A \cup B = \{x, y, z, p, q\} \quad \text{and} \quad A \cap B = \{x\}. \quad \diamond$$

To help visualize unions and intersections of sets (as well as other constructions we will define later on), 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 called A and B . In Figure 3.3.1 (ii) we shade the region representing $A \cup B$, and in Figure 3.3.1 (iii) we shade the region representing $A \cap B$.

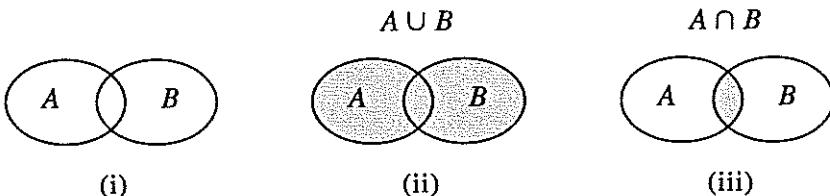


Figure 3.3.1.

Venn diagrams can be useful for convincing ourselves of the intuitive truth of various propositions concerning sets. For instance, we will prove in Theorem 3.3.2 (v) 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 region shaded in Figure 3.3.2. Although Venn diagrams seem much easier to use than regular 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.

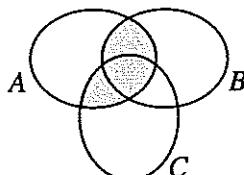


Figure 3.3.2.

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 3.3.2. *Let A , B and C be sets.*

- (i) $A \cap B \subseteq A$ and $A \cap B \subseteq B$. If X is a set such that $X \subseteq A$ and $X \subseteq B$, then $X \subseteq A \cap B$.
- (ii) $A \subseteq A \cup B$ and $B \subseteq A \cup B$. If Y is a set such that $A \subseteq Y$ and $B \subseteq Y$, then $A \cup B \subseteq Y$.
- (iii) $A \cup B = B \cup A$ and $A \cap B = B \cap A$ (*Commutative Laws*).
- (iv) $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$ (*Associative Laws*).
- (v) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*Distributive Laws*).
- (vi) $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$ (*Identity Laws*).
- (vii) $A \cup A = A$ and $A \cap A = A$ (*Idempotent Laws*).
- (viii) $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$ (*Absorption Laws*).
- (ix) 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 (iv) and (v), leaving the rest to the reader in Exercise 3.3.6.

(iv). We will show that $(A \cup B) \cup C = A \cup (B \cup C)$; the other equation can be proved similarly. The equality of the two sets under consideration is demonstrated by showing that each is a subset of the other. First, suppose that $x \in (A \cup B) \cup C$. Then $x \in A \cup B$ or $x \in C$. In the latter case it follows from part (ii) of this theorem that $x \in B \cup C$, and hence $x \in A \cup (B \cup C)$. In the former case, either $x \in A$ or $x \in B$. If $x \in A$ then $x \in A \cup (B \cup C)$ by part (ii), and if $x \in B$ then $x \in B \cup C$, 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 inclusion in the other direction is proved similarly, simply changing the roles of A and C .

(v). 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 $x \in C$. In the former case we deduce that $x \in A \cap B$, and in the latter case we deduce that $x \in A \cap C$. In either case we have $x \in (A \cap B) \cup (A \cap C)$, using part (ii) of this theorem. Thus $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Now let $x \in (A \cap B) \cup (A \cap C)$. Then $x \in A \cap B$ or $x \in A \cap C$. In the former case $x \in A$ and $x \in B$. It follows that $x \in B \cup C$ by

part (ii) of the theorem, and hence $x \in A \cap (B \cup C)$. A similar argument works in the second case, and combining the two cases we deduce that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Combining this last result with the result of the previous paragraph, we see that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. \square

In part (v) of the above theorem, we see 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 captures the intuitive notion of two sets having no elements in common.

Definition. Let A and B be sets. We say that A and B are **disjoint** if $A \cap B = \emptyset$. Δ

Example 3.3.3. 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 P and O are not disjoint. \diamond

Another useful set operation is given in the following definition.

Definition. Let A and B be sets. The **difference** (also known as **set difference**) of A and B , denoted $A - B$, is the set defined by

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}.$$

Δ

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 $B \subseteq A$. Some books use the notation $A \setminus B$ instead of $A - B$. See Figure 3.3.3 for a Venn diagram of the $A - B$.

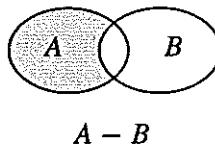


Figure 3.3.3.

Example 3.3.4. Using the sets A and B in Example 3.3.1, we have

$$A - B = \{y, z, p\}.$$

\diamond

The following theorem gives some standard properties of set difference.

Theorem 3.3.5. Let A , B and C be sets.

- (i) $A - B \subseteq A$.
- (ii) $(A - B) \cap B = \emptyset$.
- (iii) $A - B = \emptyset$ iff $A \subseteq B$.
- (iv) $B - (B - A) = A$ iff $A \subseteq B$.
- (v) If $A \subseteq B$, then $A - C = A \cap (B - C)$.
- (vi) If $A \subseteq B$, then $C - A \supseteq C - B$.
- (vii) $C - (A \cup B) = (C - A) \cap (C - B)$ and $C - (A \cap B) = (C - A) \cup (C - B)$
(De Morgan's Laws).

Proof. We will prove part (vii), leaving the rest to the reader in Exercise 3.3.7.

(vii). We will show that $C - (A \cup B) = (C - A) \cap (C - B)$; the other equation can be proved similarly. Let $x \in C - (A \cup B)$. Then $x \in C$ and $x \notin A \cup B$. It follows that $x \notin A$ and $x \notin B$ (since either $x \in A$ or $x \in B$ would imply that $x \in A \cup B$). Since $x \in C$ and $x \notin A$, then $x \in C - A$. Since $x \in C$ 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 $x \in (C - A) \cap (C - B)$. Hence $x \in C - A$ and $x \in C - B$. Since $x \in C - A$ it follows that $x \in C$ and $x \notin A$. Since $x \in C - B$ it follows that $x \in C$ and $x \notin B$. Because $x \notin A$ and $x \notin B$ it follows that $x \notin A \cup B$. Therefore $x \in C - (A \cup B)$. Thus $(C - A) \cap (C - B) \subseteq C - (A \cup B)$. Hence $C - (A \cup B) = (C - A) \cap (C - B)$. \square

There is one additional fundamental way of forming new sets out of old that we will be using regularly. Think of how the plane is coordinatized by 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) iff $a = c$ 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 interval of real numbers, as defined in Section 3.2. Both uses of this notation are widespread, so we are stuck with them. In practice the meaning of “ (a, b) ” is usually clear from context.)

Definition. Let A and B be sets. The product (also known as 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. Δ

Example 3.3.6. (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 often listed in the table

1	2	(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	(1, 6)
3	4	(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	(2, 6)
5	6	(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	(3, 6)
7	8	(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	(4, 6)
9	10	(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	(5, 6)
11	12	(6, 1)	(6, 2)	(6, 3)	(6, 4)	(6, 5)	(6, 6).

This table is the product of the set $\{1, \dots, 6\}$ with itself.

(3) If A and B are finite sets, then $A \times B$ is finite, and $|A \times B| = |A| \cdot |B|$. (This fact, which is intuitively clear, is proved in Proposition 7.6.3.) \diamond

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, for example, 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, namely $(A \times B) \times C$ or $A \times (B \times C)$. Strictly speaking, these two triple products are not the same, since 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 thus gloss over this whole 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 $A \times (B \times C)$ can be expressed using the concepts developed in Section 4.4; see Exercise 4.4.6.)

Example 3.3.7. 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

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ times}}. \quad \diamond$$

The following theorem gives some standard properties of products of sets.

Theorem 3.3.8. Let A, B, C and D be sets.

- (i) If $A \subseteq B$ and $C \subseteq D$, then $A \times C \subseteq B \times D$.
- (ii) $A \times (B \cup C) = (A \times B) \cup (A \times C)$ and $(B \cup C) \times A = (B \times A) \cup (C \times A)$ (Distributive Laws).
- (iii) $A \times (B \cap C) = (A \times B) \cap (A \times C)$ and $(B \cap C) \times A = (B \times A) \cap (C \times A)$ (Distributive Laws).
- (iv) $A \times \emptyset = \emptyset$ and $\emptyset \times A = \emptyset$.
- (v) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

Proof. We will prove part (iii), leaving the rest to the reader in Exercise 3.3.8.

(iii). We will prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$; the second equation is similar. 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) , since $(A \times B) \cap (A \times C)$ is not of the form $X \times Y$ for 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 $b \in B$. Since $y \in A \times C$, we thus have $(a, b) \in A \times C$. It follows that $b \in C$. Hence $b \in B \cap C$. Hence $y = (a, b) \in A \times (B \cap C)$. Therefore $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

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 3.2.2 (i) we know that $A \subseteq A$. Using the first sentence in Theorem 3.3.2 (i) we know that $B \cap C \subseteq B$ and $B \cap C \subseteq C$. By part (i) of the present theorem we deduce that $A \times (B \cap C) \subseteq A \times B$ and $A \times (B \cap C) \subseteq A \times C$. It follows from the second sentence in Theorem 3.3.2 (i) that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$. Thus $A \times (B \cap C) = (A \times B) \cap (A \times C)$. \square

Note 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 (v) of the above theorem, but with \cup instead of \cap , is not true.

Example 3.3.9. 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 3.3.8 (v) holds for these sets. We have $A \cap B = \{2\}$ and $C \cap D = \{y\}$, and so $(A \cap B) \times (C \cap D) = \{(2, y)\}$. On the other hand, we have $A \times C = \{(1, x), (1, y), (2, x), (2, y)\}$ and $B \times D = \{(2, y), (2, z), (3, y), (3, z)\}$, and so $(A \times C) \cap (B \times D) = \{(2, y)\}$. Thus $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.

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 have $(A \times C) \cup (B \times D) = \{(1, x), (1, y), (2, x), (2, y), (2, z), (3, y), (3, z)\}$. Thus $(A \cup B) \times (C \cup D) \neq (A \times C) \cup (B \times D)$. 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). \diamond

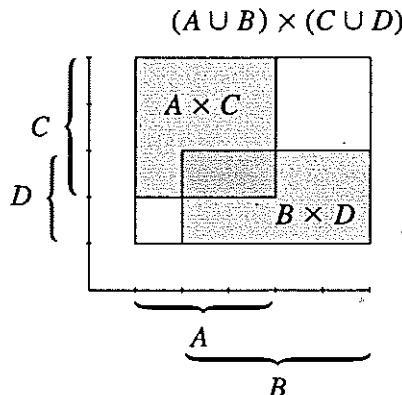


Figure 3.3.4.

Exercises

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) $A \times B$. | |

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) $(C - D) \cup (F \cap E)$. |

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) $X - (Z \cup W)$. |

3.3.4. Let

$$\begin{aligned} G &= \{n \in \mathbb{Z} \mid n = 2m \text{ for some } m \in \mathbb{Z}\} \\ H &= \{n \in \mathbb{Z} \mid n = 3k \text{ for some } k \in \mathbb{Z}\} \\ I &= \{n \in \mathbb{Z} \mid n^2 \text{ is odd}\} \\ J &= \{n \in \mathbb{Z} \mid 0 \leq n \leq 10\}. \end{aligned}$$

Find each of the following sets.

- | | |
|------------------|------------------------|
| (1) $G \cup I$. | (4) $J - G$. |
| (2) $G \cap I$. | (5) $I - H$. |
| (3) $G \cap H$. | (6) $J \cap (G - H)$. |

3.3.5. Given two sets A and B , consider the sets $A - B$ and $B - A$. Are they necessarily disjoint? Give a proof or a counterexample.

3.3.6. [Used in Section 3.3.] Prove Theorem 3.3.2 parts (i) – (iii) and (vi) – (ix).

3.3.7. [Used in Section 3.3.] Prove Theorem 3.3.5 parts (i) – (vi).

3.3.8. [Used in Section 3.3.] Prove Theorem 3.3.8 parts (i), (ii), (iv), (v).

3.3.9. Let X be a set, and let $A, B, C \subseteq X$. Suppose that $A \cap B = A \cap C$, and that $(X - A) \cap B = (X - A) \cap C$. Show that $B = C$.

3.3.10. Let A, B and C be sets. Show that $(A - B) \cap C = (A \cap C) - B = (A \cap C) - (B \cap C)$.

3.3.11. For real numbers a, b and c we know that $a - (b - c) = (a - b) + c$. Discover and prove a formula for $A - (B - C)$, where A, B and C are sets.

3.3.12. Let A and B be sets. The **symmetric difference** of A and B , denoted $A \Delta B$, is the set $A \Delta B = (A - B) \cup (B - A)$.

Let X , Y and Z be sets. Prove the following statements.

- (1) $X \Delta \emptyset = X$.
- (2) $X \Delta X = \emptyset$.
- (3) $X \Delta Y = Y \Delta X$.
- (4) $X \Delta (Y \Delta Z) = (X \Delta Y) \Delta Z$.
- (5) $X \cap (Y \Delta Z) = (X \cap Y) \Delta (X \cap Z)$.
- (6) $X \Delta Y = \underline{(X \cup Y)} - \underline{(X \cap Y)}$.

3.3.13. Prove or find a counterexample to the following statement: Let A , B , and C be sets. Then $(A - B) \cup C = (A \cup B \cup C) - (A \cap B)$.

3.3.14. Prove or find a counterexample to the following statement: Let A , B , and C be sets. Then $(A \cup C) - B = (A - B) \cup (C - B)$.

3.3.15. Prove or find a counterexample to the following statement: Let A , B , and C be sets. Then $(A \cup B) - (A \cap B \cap C) = [A - (B \cap C)] \cup [B - (A \cap C)]$.

3.3.16. Let A , B , and C be sets. Prove that $A \subseteq C$ iff $A \cup (B \cap C) = (A \cup B) \cap C$.

3.3.17. 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 $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

3.3.18. Let A , B and C be sets. Show that $A \times (B - C) = (A \times B) - (A \times C)$.

3.3.19. Let A and B be sets such that $B \subseteq A$. Prove that $A \times A - B \times B = [(A - B) \times A] \cup [A \times (A - B)]$.

3.3.20. Let A , B and E be sets such that $E \neq \emptyset$. Show that if $A \times E = B \times E$, then $A \subseteq B$.

3.3.21. Let A and B be sets such that $A \neq B$. Suppose that E is a set such that $A \times E = B \times E$. Prove that $E = \emptyset$.

3.3.22. Let X be a finite set. 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 Indexed Families of Sets

So far we have dealt only with unions and intersections of two sets at a time. Now we want to apply these operations to more than two sets. For finitely many sets we can use the definitions we already have, making use of the associative law for unions and intersections (Theorem 3.3.2 (iv)). Suppose, for example, we had three sets A , B and C , and we wanted to form the union of all three of them. Since our original definition works only for two sets at a time, we could form the union of all three sets in one of two possible ways, namely $(A \cup B) \cup C$ and $A \cup (B \cup C)$. Theorem 3.3.2 (iv) says that these two expressions are equal, and so it makes sense to define the expression $A \cup B \cup C$ as simply equaling either $(A \cup B) \cup C$ or $A \cup (B \cup C)$. If we are willing to change the order of the three sets, there are an additional ten other ways of forming the desired union, though by Theorem 3.3.2 (iii) all ways still yield the same result. The same idea holds for the intersection of three sets, and for unions and intersections of any finite collection of sets A_1, A_2, \dots, A_n (where the word "finite" refers only to the number of sets, not the sizes of the individual sets, which could be infinitely large). For ease of notation, we will use an analog of the summation notation and write

$$\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n,$$

$$\bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n.$$

We would like to construct the analog of the above two equations when we have infinitely many sets. In the simplest case, suppose we have an infinite sequence of sets A_1, A_2, A_3, \dots . Such infinite collections of sets occur quite frequently. For example, for each natural number n , we form the set D_n of all natural numbers that divide n ; thus $D_1 = \{1\}$, and $D_2 = \{1, 2\}$, and $D_3 = \{1, 3\}$, and $D_4 = \{1, 2, 4\}$, etc. In general, we would like to define the infinite union and intersection $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$. It might be tempting to form $\bigcup_{i=1}^{\infty} A_i$ analogously to the way infinite series of numbers are constructed out of partial sums. That is, we might try to form $A_1 \cup A_2$, then $A_1 \cup A_2 \cup A_3$, then $A_1 \cup A_2 \cup A_3 \cup A_4$, etc., and then take the "limit." However, as you will see if you study real analysis, limits can be a tricky business, and it is simpler in the present case to avoid them entirely. Instead, we form the desired union and intersection directly,

modeled on the definitions of $A \cup B$ and $A \cap B$, by letting

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \dots = \{x \mid x \in A_n \text{ for some } n \in \mathbb{N}\},$$

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \dots = \{x \mid x \in A_n \text{ for all } n \in \mathbb{N}\}.$$

It is possible (and in fact quite standard) to write $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$ as $\bigcup_{i \in \mathbb{N}} A_i$ and $\bigcap_{i \in \mathbb{N}} A_i$ respectively.

Example 3.4.1.

(1) For each $i \in \mathbb{N}$, let B_i be the set $B_i = \{1, 2, \dots, 3i\}$. Then $\bigcup_{i=1}^{\infty} B_i = \{1, 2, \dots\}$ and $\bigcap_{i=1}^{\infty} B_i = \{1, 2, 3\}$.

(2) Recall the notation for intervals in \mathbb{R} in Section 3.2. 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 $\bigcap_{k=1}^{\infty} F_k = (1, 8]$. \diamond

We will need unions and intersections for more general situations than just discussed. Suppose, for example, that for each real number x we define the set Q_x to be all real numbers less than x , so that $Q_x = (-\infty, x)$. Though it is not obvious, and will only be proved in Section 6.2, 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, \dots . We are therefore not in precisely the same situation as described previously. If we look carefully at the definitions of $\bigcup_{i=1}^{\infty} A_i$ and $\bigcap_{i=1}^{\infty} A_i$, however, we see that we do not need to think of the sets A_1, A_2, A_3, \dots as written in order. Rather, we can think of this collection of sets as having one set for each number in \mathbb{N} . We now generalize this observation as follows.

Definition. Let I be a non-empty set. Suppose there is a set denoted A_i for each element $i \in I$. Such a collection is called a **family of sets indexed by I** ; the set I is called the **indexing set** for this family of sets. We denote the family of sets by

$$\{A_i\}_{i \in I}.$$

The **union** and **intersection** of all the sets in the family of sets are defined by

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for some } i \in I\},$$

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for all } i \in I\}. \quad \Delta$$

The set I in the above definition could be any set. 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 . Note the crucial role that our two standard quantifiers play in the above definition of union and intersection.

Example 3.4.2. For each $x \in \mathbb{R}$, let C_x be the interval of real numbers $C_x = [-x/3, x/2]$. Then $\bigcup_{x \in \mathbb{R}} C_x = \mathbb{R}$ and $\bigcap_{x \in \mathbb{R}} C_x = \{0\}$. \diamond

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 (i) of the theorem says that $\bigcup_{i \in I} A_i$ is the smallest set containing all the sets A_k , and part (ii) of the theorem says that $\bigcap_{i \in I} A_i$ is the largest set contained in all the sets A_k .

Theorem 3.4.3. 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.

- (i) $\bigcap_{i \in I} A_i \subseteq A_k$ for all $k \in I$. If $B \subseteq A_k$ for all $k \in I$, then $B \subseteq \bigcap_{i \in I} A_i$.
- (ii) $A_k \subseteq \bigcup_{i \in I} A_i$ for all $k \in I$. If $A_k \subseteq B$ for all $k \in I$, then $\bigcup_{i \in I} A_i \subseteq B$.
- (iii) $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$ (Distributive Law).
- (iv) $B \cup (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \cup A_i)$ (Distributive Law).
- (v) $B - (\bigcup_{i \in I} A_i) = \bigcap_{i \in I} (B - A_i)$ (De Morgan's Law).
- (vi) $B - (\bigcap_{i \in I} A_i) = \bigcup_{i \in I} (B - A_i)$ (De Morgan's Law).

Proof. We will prove part (iii), leaving the rest to the reader in Exercise 3.4.3.

(iii). Let $x \in B \cap (\bigcup_{i \in I} A_i)$. Then $x \in B$ and $x \in \bigcup_{i \in I} A_i$. Thus $x \in A_k$ 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 (i) of this theorem. Hence $B \cap (\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} (B \cap A_i)$.

Now let $x \in \bigcup_{i \in I} (B \cap A_i)$. Hence $x \in B \cap A_k$ for some $k \in I$. Thus $x \in B$ and $x \in A_k$. Therefore $x \in \bigcup_{i \in I} A_i$ by part (i) of this theorem. Thus $x \in B \cap (\bigcup_{i \in I} A_i)$. Hence $\bigcup_{i \in I} (B \cap A_i) \subseteq B \cap (\bigcup_{i \in I} A_i)$. We conclude that $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$. \square

It is interesting to compare the above proof with the proof of Theorem 3.3.2 (v). Though Theorem 3.4.3 (iii) is a generalization of Theorem 3.3.2 (v), the proof of the generalized statement is slightly more concise than the proof of the simpler statement. The proof of Theorem 3.4.3 (iii) is more concise precisely because it is phrased explicitly in terms of quantifiers, thus avoiding the need for cases as in the proof of Theorem 3.3.2 (v).

It is also possible to form infinite products of sets, though to do so requires the use of functions, to be defined in the next chapter. See the end of Section 4.5 for a brief mention of products of indexed families of sets.

Exercises

3.4.1. In each of the following cases, suppose we are given sets 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) $B_k = \{0, 1, 2, 3, \dots, 2k\}.$ | (4) $B_k = [-1, 3 + \frac{1}{k}] \cup [5, \frac{5k+1}{k}).$ |
| (2) $B_k = \{k - 1, k, k + 1\}.$ | (5) $B_k = (-\frac{1}{k}, 1] \cup (2, \frac{3k-1}{k}).$ |
| (3) $B_k = [\frac{3}{k}, \frac{5k+2}{k}) \cup \{10 + k\}.$ | (6) $B_k = [0, \frac{k+1}{k+2}] \cup [7, \frac{7k+1}{k}).$ |

3.4.2. In each of the following cases, define a family of sets $\{E_k\}_{k \in \mathbb{N}}$, where $E_k \subseteq \mathbb{R}$ for each $k \in \mathbb{N}$, where no two sets E_k are equal to each other, and such 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) $\bigcup_{k \in \mathbb{N}} E_k = \mathbb{N}$ and $\bigcap_{k \in \mathbb{N}} E_k = \{\dots, -2, 0, 2, 4, 6, \dots\}.$
- (7) $\bigcup_{k \in \mathbb{N}} E_k = \mathbb{R}$ and $\bigcap_{k \in \mathbb{N}} E_k = \mathbb{N}.$

3.4.3. [Used in Section 3.4.] Prove Theorem 3.4.3 parts (i), (ii), (iv) – (vi).

3.4.4. Let I and J be sets such that $J \subseteq I$, and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I .

- (1) Show that $\bigcup_{j \in J} A_j \subseteq \bigcup_{i \in I} A_i.$
- (2) Show that $\bigcap_{i \in I} A_i \subseteq \bigcap_{j \in J} A_j.$

3.4.5. Let I be a set, let $\{A_i\}_{i \in I}$ be a family of sets indexed by I , and let B be a set.

- (1) Show that $(\bigcup_{i \in I} A_i) - B = \bigcup_{i \in I} (A_i - B)$.
- (2) Show that $(\bigcap_{i \in I} A_i) - B = \bigcap_{i \in I} (A_i - B)$.

3.4.6. 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.

Show that $B \times (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \times A_i)$.

Show that $B \times (\bigcap_{i \in I} A_i) = \bigcap_{i \in I} (B \times A_i)$.

3.4.7. 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 $\{X_i\}_{i \in I}$ be a collection of co- \mathcal{W} subsets of \mathbb{R} , where I is some indexing set. For each of the properties \mathcal{W} listed below, either prove that $\bigcup_{i \in I} X_i$ is co- \mathcal{W} , or give a counterexample. Try to figure out a general rule for deciding when $\bigcup_{i \in I} X_i$ is co- \mathcal{W} for a given property \mathcal{W} .

- (1) A subset of \mathbb{R} has property \mathcal{W} iff it is finite.
- (2) A subset of \mathbb{R} has property \mathcal{W} iff it has at most 7 elements.
- (3) A subset of \mathbb{R} has property \mathcal{W} iff it has precisely 7 elements.
- (4) A subset of \mathbb{R} has property \mathcal{W} iff it contains only integers.
- (5) A subset of \mathbb{R} has property \mathcal{W} iff it is finite, and has an even number of elements.

4

Functions

A function is the abstract image of the dependence of one magnitude on another.

A. D. Aleksandrov (1912–1999)

4.1 Functions

You have encountered functions repeatedly in your previous mathematics courses. In high school you learned about polynomial, exponential, logarithmic and trigonometric functions, among others. Though logarithms and trigonometry are often first learned about without thinking about functions (for example, sines and cosines can be thought of in terms of solving right triangles), in many pre-calculus courses, and certainly in calculus, the focus shifts to functions (for example, thinking of sine and cosine as functions defined on the entire real number line). In calculus, the operation of taking a derivative is something that takes functions, and gives us new functions (namely the derivatives of the original ones). In applications of calculus, such as in physics or chemistry, thinking of exponentials, sines, cosines, etc. as functions is crucial. For example, we use sine and cosine functions 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. When we want to com-

pare two sets (for example, to see if they have the same size, as discussed in Section 6.1), we use functions between the sets. In topology, when we want to show that two spaces are essentially the same, we use functions between the spaces. Similarly in group theory and 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 deal with numbers, nor need it be given by a formula. For example, we can form the function that assigns to each person his or her biological mother. We can think of a function informally as a little machine, where the input objects are put into a hopper on the top, and for each input object, the machine spits out one output object. See Figure 4.1.1. For example, if a function is given by the formula $f(x) = x^2$, then the machine takes real numbers as input, and if we put $a = 5$ into the machine, then it will spit out $f(a) = 25$.

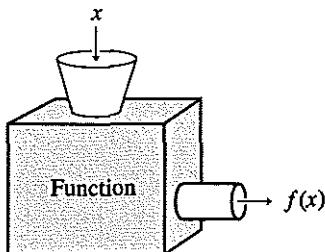


Figure 4.1.1.

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’s 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, since 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 his or her biological mother. There is no simple formula that describes this function. That is, if we denote this function by $f(\text{person})$, we cannot say $f(\text{person}) = \text{person}^2$, or the like. We can, however, specify this function 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	Martha Smith
Susan Levy	Louise Cohen
:	:

Even for functions that have nice formulas, we can also think of them as given by lists. Consider, once again, the function given by $f(x) = x^2$. To make a list for this function, we need to know which numbers can be "plugged into" it, so that they can be included in the left-hand column of the list. We can in fact plug all real numbers into the function given by $f(x) = x^2$. (By contrast, the function given by $g(x) = \sqrt{x}$ cannot have all numbers plugged into it.) We can thus make a list for the function $f(x) = x^2$, part of which would be

x	x^2
0	0
1	1
-1	1
2	4
2.5	6.25
π	π^2
:	:

Of course, the list for $f(x) = x^2$ is infinite, so we cannot 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 a list consisting of two columns, we use ordered pairs, where each ordered pair represents one row in our list. So, for the function $f(x) = x^2$ we have an infinite list of pairs, containing $(2, 4)$, $(-2, 4)$, $(\sqrt{5}, 5)$, (π, π^2) , etc. Note that for any given real number 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, namely (c, c^2) and $(-c, c^2)$, unless $c = 0$, so we cannot be as specific about how often each number appears in the right hand slot of an ordered pair in the list.

This idea of representing a function as a collection of ordered pairs is the broadest possible way to think of functions, and we take it as our definition.

Definition. Let A and B be sets. A **function** (also known as a **map**) f from A to B , denoted $f: A \rightarrow B$, is a subset $F \subseteq A \times B$ such that for each $a \in A$, there is one and only one pair of the form (a, b) in F . The set A is called the **domain** of the function and the set B is called the **codomain** of the function. \triangle

Let us look closely at the above definition, which is stated entirely in terms of sets. 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 we change even one of these three things we obtain a different function. For example, the function $f: \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x^2 + 1$ for all $x \in \mathbb{R}$ is not the same function as $g: \mathbb{R} \rightarrow \mathbb{R}^+$ given by $g(x) = x^2 + 1$ for all $x \in \mathbb{R}$, even though they both have the same formula and the same domain. The term “codomain” should not be confused with the term “range,” which we will define in Section 4.2.

Example 4.1.1.

(1) Consider the sets $A = \{a, b, c, d\}$ and $B = \{1, 2, 3, 4\}$. We construct two “rules of assignment” from A to B using diagrams with arrows, as given in Figure 4.1.2. The rule of assignment in part (i) of the figure corresponds to the set $\{(a, 2), (b, 1), (c, 4), (d, 4)\} \subseteq A \times B$, and it 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.

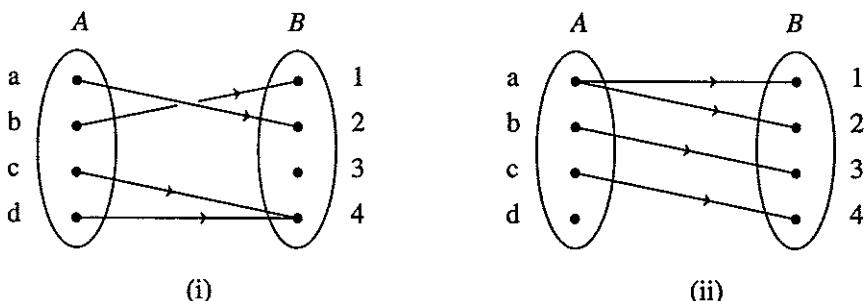


Figure 4.1.2.

(2) A “rule of assignment” is given by assigning to each person his or 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, since not everyone has a sister. Even if we restrict the domain to all people with sisters there is a problem, since some people have more than one sister, and we do not know which sister is being assigned. Thus we need to restrict the domain even further to all people with precisely one sister. As for the codomain, whatever it is chosen to be, it needs to contain at least all those women who have siblings.

(3) Consider the formula $f(x) = \sqrt{x^2 - 5x + 6}$. On its own, this formula does not really define a function, since we are not given a domain and codomain. It is standard 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 we take $(-\infty, 2] \cup [3, \infty)$ 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 $[-17, \infty)$. \diamond

We are defining functions in terms of sets, but we can recover the intuitive “rule of assignment” approach to functions. Let $f : A \rightarrow B$ be a function. Then for each $a \in A$ there is one and only one pair of the form (a, b) in the subset $F \subseteq A \times B$. 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. Thus our definition of function leads to the more usual notation for functions, and so we can use the notation we are used to.

The use of the “ $f(x)$ ” notation, though legitimate when used properly, often leads to a very common mistake. It is common in elementary courses (such as calculus) to write phrases such as “let $f(x)$ be a function.” Such a phrase, however, is technically incorrect. If $f : A \rightarrow B$ is a function, then the name of the function is “ f ,” not “ $f(x)$.” The symbol “ $f(x)$ ” means the value of the function f at the element x in the domain; thus $f(x)$ is an element of the codomain (namely B), rather than being 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 an element of the domain.

In reality, there is no such thing as a variable in a function. It would be commonly understood that the notation “ $f(a)$ ” denotes the value of the function f at the element $a \in A$, and so $f(a)$ is an element of the codomain. Why should “ $f(x)$ ” mean anything different than “ $f(a)$,” except that a 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 will always use the symbol f to denote the name of the function, and $f(x)$ to denote an element of the codomain. This distinction between f and $f(x)$ might seem at first like 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.

It might appear that we are not following our own guidelines when we define a function by writing “let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = \cos x$ for all $x \in \mathbb{R}$,” but there is no mistake here. We are defining the function named “ f ” by stating what the value of $f(x)$ is for each possible x in the domain of f . 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 on 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. Thus the entire statement of the definition at the start of this paragraph 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 is 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 4.1.1 (3), and take $(-\infty, 2] \cup [3, \infty)$ as the domain, and \mathbb{R} as the codomain. Because we now wish to attain a higher level of rigor, however, it is usually best to avoid all such informal conventions concerning the definition of functions, and give truly proper definitions, as discussed in the previous paragraph.

On the topic of giving functions by numerical formulas, whereas in courses such as calculus, the functions encountered are often given by simple formulas such as $f(x) = x^2$, sometimes a function cannot be given by a single formula, but can be given in cases. Consider, for example, the function $f : \mathbb{R} \rightarrow \mathbb{R}$ given 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 a number of disjoint pieces, and defining the function on each of the pieces. So far there is nothing problematic. However, it is sometimes more convenient to break up the domain into pieces that are not disjoint, and to define the function on each piece. For example, we might define a function $g: \mathbb{R} \rightarrow \mathbb{R}$ by

$$g(x) = \begin{cases} x^2, & \text{if } x \geq 1 \\ x, & \text{if } x \leq 1. \end{cases}$$

Unlike the case in which the domain is broken up into disjoint pieces, where there is nothing to check, in this case we must verify whether the formulas for the two pieces agree when evaluated at the point common to both pieces (namely $x = 1$). In the present example everything works out fine, and so the way we presented g makes sense. We say the function g is **well-defined**. On the other hand, if a function is presented by overlapping cases, and if the formulas do not agree on the overlap, then we don't have a function at all.

A look at functions $\mathbb{R} \rightarrow \mathbb{R}$, which are familiar from algebra and calculus, can help us gain some insight into functions generally. We know that such a map 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 $x \in \mathbb{R}$. The function f has the property that for each $x \in \mathbb{R}$, there is one and only one 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 we are given a curve in \mathbb{R}^2 . Is this curve necessarily the graph of some function $f: \mathbb{R} \rightarrow \mathbb{R}$? 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 $f: \mathbb{R} \rightarrow \mathbb{R}$; if this property does not hold, then the curve will not be the graph of a function of the form $f: \mathbb{R} \rightarrow \mathbb{R}$.

It is important to recognize what it means for two functions to be equal. According to the definition of functions, each 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 we change even one of these three things we obtain a different function.

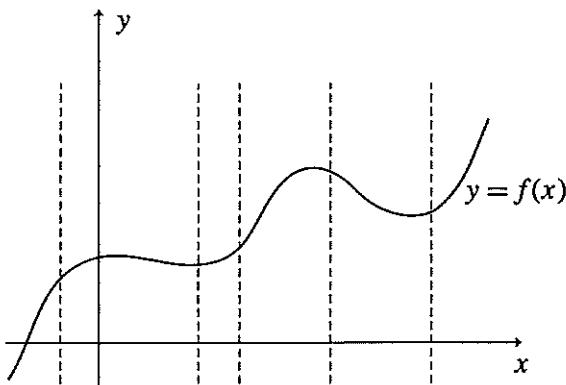


Figure 4.1.3.

For example, the function $f: \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x^2 + 1$ for all $x \in \mathbb{R}$ is not the same function as $g: \mathbb{R} \rightarrow \mathbb{R}^+$ given by $g(x) = x^2 + 1$ for all $x \in \mathbb{R}$, even though they both have the same formula and the same domain.

If f and g are functions, to say that " $f = g$ " means that the two functions have the same domain, say A , the same codomain, say B , and correspond to the same subset of $A \times B$. This last statement can be rephrased by saying that $f(x) = g(x)$ for all $x \in A$. Note that the statement " $f(x) = g(x)$ for all x in the domain" is not a statement about equivalent formulas for f and g , since the functions f and g might not be given by formulas, but rather is a statement about the equality of various elements in the codomain. Thus, a single statement about functions, namely $f = g$, 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). To prove that two functions f and g are equal, a typical proof would look like "(Argumentation) ... Thus the domain of f is the same as the domain of g (Argumentation) ... Thus the codomain of f is the same as the codomain of g . Let a be in the domain of f and g (Argumentation) ... Then $f(a) = g(a)$. Hence $f = g$."

We conclude this section with some particularly useful functions.

Definition. Let A and B be sets, and let $S \subseteq A$. A **constant map** $f: A \rightarrow B$ is any function of the form $f(x) = b$ for all $x \in A$, where $b \in B$ is some fixed element. The **identity map** on A is the function $1_A: A \rightarrow A$ defined by $1_A(x) = x$ for all $x \in A$. The **inclusion map** from S to A is the function $j: S \rightarrow A$ defined by $j(x) = x$ for all $x \in S$. If $f: A$

→ B is a map, the **restriction** of f to S , denoted $f|_S$, is the map $f|_S: S \rightarrow B$ defined by $f|_S(x) = f(x)$ for all $x \in S$. If $g: S \rightarrow B$ is a map, an **extension** of g to A is any map $G: A \rightarrow B$ such that $G|_S = g$. The **projection maps** from $A \times B$ are the functions $\pi_1: A \times B \rightarrow A$ and $\pi_2: A \times B \rightarrow B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ for all $(a, b) \in A \times B$. Projection maps

$$\pi_i: A_1 \times \cdots \times A_p \rightarrow A_i$$

for any finite collection of sets A_1, \dots, A_p can be defined similarly. △

Example 4.1.2.

(1) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $f(x) = \sin x$ for all $x \in \mathbb{R}$. Then the restriction of f to \mathbb{Q} is the map $f|_{\mathbb{Q}}: \mathbb{Q} \rightarrow \mathbb{R}$ defined by $f|_{\mathbb{Q}}(x) = \sin x$ for all $x \in \mathbb{Q}$.

(2) Let $X = \{a, b, c, d\}$, let $Y = \{a, b\}$ and let $Z = \{1, 2, 3\}$. Let $f: Y \rightarrow Z$ be defined by $f(a) = 3$ and $f(b) = 2$. We now define two maps $g, h: X \rightarrow Z$ as follows. Let $g(a) = 3$, let $g(b) = 2$, let $g(c) = 1$ and let $g(d) = 3$. Let $h(a) = 3$, let $h(b) = 1$, let $h(c) = 2$ and let $h(d) = 3$. Then the map g is an extension of f , since $g|_Y = f$, but the map 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 $\pi_1: \mathbb{R}^2 \rightarrow \mathbb{R}$ and $\pi_2: \mathbb{R}^2 \rightarrow \mathbb{R}$ that are defined by $\pi_1((x, y)) = x$ and $\pi_2((x, y)) = y$ for all $(x, y) \in \mathbb{R}^2$. ◇

Exercises

4.1.1. Let $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$. Which of the following subsets of $A \times B$ are functions $A \rightarrow B$?

- | | |
|------------------------------------|--------------------------------------------|
| (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) $\{(a, 3), (c, 3), (b, 3)\}$. |

4.1.2. Let X denote the set of all people. Which of the following descriptions define functions $X \rightarrow X$?

- (1) $f(a)$ is a 's mother.
- (2) $g(a)$ is a 's brother.
- (3) $h(a)$ is a 's best friend.
- (4) $k(a)$ is a 's first born child if he or she is a parent, and his or her father otherwise.

- (5) $j(a)$ is a 's sibling if he or she has siblings, and himself or herself otherwise.

4.1.3. Which of the diagrams in Figure 4.1.4 represent functions?

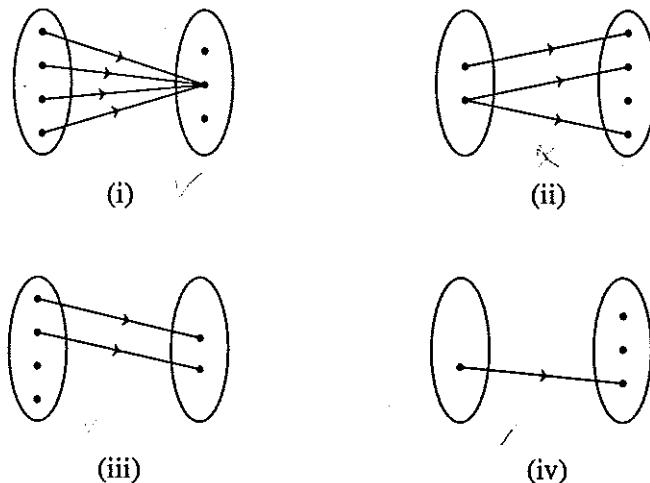


Figure 4.1.4.

4.1.4. Which of the following phrases completely (and strictly) describe functions?

- (1) Let $f(x) = \cos x$.
- (2) To every person a , let $g(a)$ be a 's height in inches.
- (3) For every real number, assign the real number that is the logarithm of the original number.
- (4) Let $g: \mathbb{R} \rightarrow \mathbb{R}$ be given by $g(x) = e^x$.

4.1.5. Which of the following formulas define functions $\mathbb{R} \rightarrow \mathbb{R}$?

- (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) $s(x) = \begin{cases} x^2, & \text{if } x \geq 1 \\ x^3, & \text{if } x \leq 0. \end{cases}$

$$(6) t(x) = \begin{cases} x^3 - 2, & \text{if } x \geq 1 \\ |x|, & \text{if } x \leq 1. \end{cases}$$

$$(7) g(x) = \begin{cases} \sin x, & \text{if } x \geq \pi \\ x, & \text{if } x < \pi. \end{cases}$$

4.1.6. For each of the following formulas, find the largest subset $X \subseteq \mathbb{R}$ such that $g: X \rightarrow \mathbb{R}$ is a function.

$$(1) g(x) = \frac{1}{x^4 - 3} \text{ for all } x \in X.$$

$$(2) g(x) = \sqrt{1 - x^2} \text{ for all } x \in X.$$

$$(3) g(x) = 3 \ln(\sin x) \text{ for all } x \in X.$$

$$(4) g(x) = \begin{cases} \sqrt{x}, & \text{if } x \in X \text{ and } x \geq 0 \\ x + 1, & \text{if } x \in X \text{ and } x \leq 0. \end{cases}$$

$$(5) g(x) = \begin{cases} \tan \pi x + 4, & \text{if } x \in X \text{ and } x \geq 1 \\ 3x^2 + 1, & \text{if } x \in X \text{ and } x \leq 1. \end{cases}$$

4.1.7. Let A and B be sets, let $S \subseteq A$ be a subset, and let $f: A \rightarrow B$ be a map. Let $g: A \rightarrow B$ be an extension of $f|_S$ to A . Does $g = f$?

4.1.8. Let X be a set. For each subset $A \subseteq X$, define the characteristic function $\chi_A^X: X \rightarrow \{0, 1\}$ by

$$\chi_A^X(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \in X - A. \end{cases}$$

It is common to write χ_A rather than χ_A^X , since the set X is usually understood from the context. (Also, it is often useful to take \mathbb{R} rather than $\{0, 1\}$ as the codomain of characteristic functions.)

Let $A, B \subseteq X$. Show that $\chi_A = \chi_B$ iff $A = B$.

4.2 Image and Inverse Image

Suppose we let A denote the set of all adults on earth (defined to be people 18 years and older), and we define a function $h: A \rightarrow \mathbb{R}$ by letting $h(x)$ be person x 's height in inches. There are a number of things we might wish to do with this function. For example, we might want to know the various heights found among all adults living in France. This set of heights would be written in our set notation as $\{h(x) \mid x \text{ lives in France}\}$. Alternatively, and more useful to us, we could write this set as $\{r \in \mathbb{R} \mid r =$

$h(x)$ for some x that 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 know all the adults whose heights are between, or equal to 6 ft. and 6 ft. 3 in. Since we are working in inches, we want to find all people whose heights are in the interval $[72, 75]$. Thus, we want to find 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 of the desired type.

The following definition generalizes the above process. Given a map $f: A \rightarrow B$, 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 (giving us a subset of A).

Definition. Let $f: A \rightarrow B$ be a function.

(1) For each $P \subseteq A$, let $f_*(P)$ be defined by

$$\begin{aligned} f_*(P) &= \{b \in B \mid b = f(p) \text{ for some } p \in P\} \\ &= \{f(p) \mid p \in P\}. \end{aligned}$$

For each $P \subseteq A$, the set $f_*(P)$ is called the **image** of P under f . The **range** of the function f is the set $f_*(A)$. The range is also known as the **image** of f .

(2) For each $Q \subseteq B$, let $f^*(Q)$ be defined by

$$\begin{aligned} f^*(Q) &= \{a \in A \mid f(a) = q \text{ for some } q \in Q\} \\ &= \{a \in A \mid f(a) \in Q\}. \end{aligned}$$

For each $Q \subseteq B$, the set $f^*(Q)$ is called the **inverse image** of Q under f . Δ

Example 4.2.1. Let $f: (-\infty, 2] \cup [3, \infty) \rightarrow \mathbb{R}$ be defined by $f(x) = \sqrt{x^2 - 5x + 6}$ for all $x \in (-\infty, 2] \cup [3, \infty)$. It is straightforward to compute that $f_*([4, 5]) = [\sqrt{2}, \sqrt{6}]$, that $f^*([\sqrt{12}, \infty)) = (-\infty, -1] \cup [6, \infty)$, and that $f^*([\sqrt{-8}, \sqrt{-7}]) = \emptyset$. It can be seen (for example by graphing the function) that the range of the function is $[0, \infty)$. \diamond

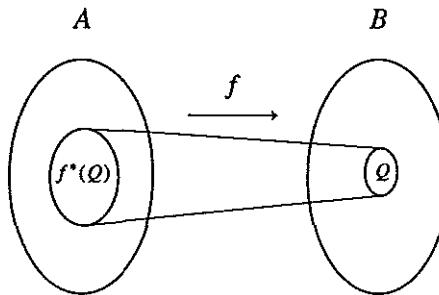


Figure 4.2.1.

The terms range and codomain are often confused, so precise use of language is needed. We should mention that the notations $f_*(P)$ and $f^*(Q)$ are not the standard ones used for the image of the set P under the map f and the inverse image of the set Q under f respectively. (By contrast, the notations f_* and f^* are commonly used for the maps of power sets induced by f .) It is most common to write $f_*(P)$ simply as $f(P)$, which is not formally meaningful, since only elements of the domain (not subsets of it) can be plugged into f . The notation $f(P)$ is an example of what mathematicians refer to as an “abuse of notation,” which is a technically incorrect way of writing something that everyone understands what it means anyway, and tends not to cause problems. It is also very common to write $f^*(Q)$ as $f^{-1}(Q)$. This latter notation, though widespread, causes a lot of problems for students learning to write proofs. Later in this chapter we will discuss the notion of an inverse function; when such functions exist, we will denote them by f^{-1} . Even though this latter notation is very similar to the notation $f^{-1}(Q)$, these two concepts are quite different, and should not be confused. Let $f: A \rightarrow B$ be a function, and let $Q \subseteq B$. The inverse image $f^{-1}(Q)$ of the set Q under a map f is a subset of the set A , 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 $B \rightarrow A$, not a subset of A . Writing the notation $f^{-1}(Q)$ does not necessarily imply that the map f^{-1} exists. To avoid all this confusion, and to avoid abuse of notation, we will stick with the technically correct $f_*(P)$ and $f^*(Q)$ instead of the more common $f(P)$ and $f^{-1}(Q)$.

The following example should further demonstrate that the notation $f^{-1}(D)$ is misleading, since f_* and f^* do not “cancel each other out,” as is sometimes mistakenly assumed when using the more common notation.

~ 2

Example 4.2.2. Let $h: \mathbb{R} \rightarrow \mathbb{R}$ be given by $h(x) = x^2$ for all $x \in \mathbb{R}$. It is straightforward to compute that $h_*([0, 3]) = [0, 9]$ and $h_*([-2, 2]) = [0, 4]$. Hence $h^*(h_*([0, 3])) = h^*([0, 9]) = [-3, 3]$. We thus see that $h^*(h_*([0, 3])) \neq [0, 3]$. Similarly, we compute that $h^*([-4, 4]) = [-2, 2]$, and hence $h_*(h^*([-4, 4])) = h_*([-2, 2]) = [0, 4]$. Thus we also see that $h_*(h^*([-4, 4])) \neq [-4, 4]$. \diamond

We make two observations about strategies for proving statements involving expressions of the form $f_*(P)$ or $f^*(Q)$. First, suppose we wish to prove that either of these types of expressions is equal to some other set (as in the following proposition, for example). Though we are dealing with functions, objects of the form $f_*(P)$ or $f^*(Q)$ 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, namely showing that each set is a subset of the other.

Second, suppose we start with a statement of the form " $x \in f_*(P)$." A helpful strategy is often to go back to the definition of $f_*(P)$, and to rewrite the original statement as " $x = f(a)$ for some $a \in P$." Conversely, if we are given a statement of the form " $x = f(a)$ for some $a \in P$," it is often useful to rewrite this statement as " $x \in f_*(P)$." Similarly, suppose we start with a statement of the form " $z \in f^*(Q)$." Then by going back to the definition of $f^*(Q)$, we can rewrite the original statement as " $f(z) \in Q$." Conversely, if we have a statement of the form " $f(z) \in Q$," then it is often useful to rewrite it as " $z \in f^*(Q)$." 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, whose proof uses the above mentioned strategies, gives some of the most basic properties of images and inverse images. Observe in part (viii) of the theorem that images are not quite as well behaved as inverse images.

Theorem 4.2.3. Let $f: A \rightarrow B$ be a function. Let $C, D \subseteq A$, and let $S, T \subseteq B$. Let I and J be non-empty sets, let $\{U_i\}_{i \in I}$ be a family of sets indexed by I such that $U_i \subseteq A$ for all $i \in I$, and let $\{V_j\}_{j \in J}$ be a family of sets indexed by J such that $V_j \subseteq B$ for all $j \in J$.

$$(i) \quad f_*(\emptyset) = \emptyset \text{ and } f^*(\emptyset) = \emptyset.$$

$$(ii) \quad f^*(B) = A.$$

$$(iii) \quad f_*(C) \subseteq S \text{ iff } C \subseteq f^*(S).$$

(iv) If $C \subseteq D$, then $f_*(C) \subseteq f_*(D)$.

(v) If $S \subseteq T$, then $f^*(S) \subseteq f^*(T)$.

$$(vi) f_* \left(\bigcup_{i \in I} U_i \right) = \bigcup_{i \in I} f_*(U_i).$$

$$(vii) f_* \left(\bigcap_{i \in I} U_i \right) \subseteq \bigcap_{i \in I} f_*(U_i).$$

$$(viii) f^* \left(\bigcup_{j \in J} V_j \right) = \bigcup_{j \in J} f^*(V_j).$$

$$(ix) f^* \left(\bigcap_{j \in J} V_j \right) = \bigcap_{j \in J} f^*(V_j).$$

Proof. We will prove parts (v) and (vi); the other parts are left to the reader in Exercise 4.2.6.

(v). Suppose that $S \subseteq T$. Let $x \in f^*(S)$. Then by definition we have $f(x) \in S$. Since $S \subseteq T$, it follows that $f(x) \in T$. Hence $x \in f^*(T)$. We deduce that $f^*(S) \subseteq f^*(T)$.

(vi). First, let $b \in f_* \left(\bigcup_{i \in I} U_i \right)$. Thus $b = f(u)$ for some $u \in \bigcup_{i \in I} U_i$. Then $u \in U_j$ for some $j \in I$. Hence $b \in f_*(U_j) \subseteq \bigcup_{i \in I} f_*(U_i)$. Hence $f_* \left(\bigcup_{i \in I} U_i \right) \subseteq \bigcup_{i \in I} f_*(U_i)$. Next, let $a \in \bigcup_{i \in I} f_*(U_i)$. Thus $a \in f_*(U_k)$ for some $k \in I$. Thus $a = f(v)$ for some $v \in U_k$. Since $v \in \bigcup_{i \in I} U_i$, it follows that $a \in f_* \left(\bigcup_{i \in I} U_i \right)$. Hence $\bigcup_{i \in I} f_*(U_i) \subseteq f_* \left(\bigcup_{i \in I} U_i \right)$. Therefore $f_* \left(\bigcup_{i \in I} U_i \right) = \bigcup_{i \in I} f_*(U_i)$. \square

Finally, we note that from a slightly more abstract point of view, the definition of images and inverse images can be thought of as taking a given map $f: A \rightarrow B$, and inducing a map $f_*: \mathcal{P}(A) \rightarrow \mathcal{P}(B)$, and a map $f^*: \mathcal{P}(B) \rightarrow \mathcal{P}(A)$. We will not be using this more abstract approach (except in a few exercises).

Exercises

4.2.1. Find the range of each of the following functions $\mathbb{R} \rightarrow \mathbb{R}$.

$$(1) f(x) = x^6 - 5 \text{ for all } x \in \mathbb{R}.$$

$$(2) g(x) = x^3 - x^2 \text{ for all } x \in \mathbb{R}.$$

- (3) $h(x) = e^{x-1} + 3$ for all $x \in \mathbb{R}$.
 (4) $p(x) = \sqrt{x^4 + 5}$ for all $x \in \mathbb{R}$.
 (5) $q(x) = \sin x + \cos x$ for all $x \in \mathbb{R}$.

4.2.2. Let C be the set of all cows in the world. Let $m: C \rightarrow \mathbb{R}$ 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) $m_*(\{\text{Bessie, Bossie}\})$.
 (2) $m_*(F)$, where F denotes all the cows in India.
 (3) $m^*([1, 3])$.
 (4) $m^*([-5, 3])$.
 (5) $m^*(\{0\})$.

$$C \rightarrow m(C)$$

4.2.3. For each of the following functions $f: \mathbb{R} \rightarrow \mathbb{R}$ and each set $T \subset \mathbb{R}$, find $f_*(T)$, $f^*(T)$, $f_*(f^*(T))$ and $f^*(f_*(T))$.

- (1) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = (x+1)^2$ for all $x \in \mathbb{R}$, and let $T = [-1, 1]$.
 (2) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = (x+1)^2$ for all $x \in \mathbb{R}$, and let $T = [-5, 2]$.
 (3) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = [x]$ for all $x \in \mathbb{R}$, where $[x]$ is the smallest integer greater than or equal to x , and let $T = (1, 3)$.
 (4) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = [x]$ for all $x \in \mathbb{R}$, where $[x]$ is the greatest integer less than or equal to x , and let $T = [0, 2] \cup (5, 7)$.

4.2.4. Let $g: \mathbb{R}^2 \rightarrow \mathbb{R}$ be given by $g((x, y)) = xy$ for all $(x, y) \in \mathbb{R}$. Sketch each of the following sets.

- (1) $g^*([3])$.
 (2) $g^*([-1, 1])$.

4.2.5. Let X and Y be sets, let $A \subseteq X$ and $B \subseteq Y$, and let $\pi_1: X \times Y \rightarrow X$ and $\pi_2: X \times Y \rightarrow Y$ be projection maps, as defined in Section 4.1.

- (1) Show that $(\pi_1)^*(A) = A \times Y$ and $(\pi_2)^*(B) = X \times B$.
 (2) Show that $A \times B = (\pi_1)^*(A) \cap (\pi_2)^*(B)$.
 (3) Let $P \subseteq X \times Y$. Does $P = \pi_1(P) \times \pi_2(P)$? Give a proof or a counterexample.

4.2.6. [Used in Section 4.2.] Prove Theorem 4.2.3 parts (i)–(iv), (vii)–(ix).

4.2.7. Find the flaw(s) in the following alleged proof of part (viii) of Theorem 4.2.3, assuming that parts (i)–(vii) have already been proved: “Applying f_* to $f^*(\bigcup_{j \in J} V_j)$ we obtain $f_*(f^*(\bigcup_{j \in J} V_j)) = \bigcup_{j \in J} V_j$. Applying f_* to $\bigcup_{j \in J} f^*(V_j)$, and using part (vi) of the theorem, we obtain $f_*(\bigcup_{j \in J} f^*(V_j)) = \bigcup_{j \in J} f_*(f^*(V_j)) = \bigcup_{j \in J} V_j$. Since applying f_* to both sides of the equation in part (viii) yields the same result, we deduce that the equation in part (viii) is true.”

4.2.8. In this exercise we show that it is not possible to strengthen the statement of Theorem 4.2.3 (iii).

- (1) Find an example of a function $f: A \rightarrow B$ together with sets $X \subseteq A$ and $Y \subseteq B$ such that $f_*(X) = Y$ and $X \neq f^*(Y)$.
- (2) Find an example of a function $g: J \rightarrow K$ together with sets $Z \subseteq J$ and $W \subseteq K$ such that $f^*(W) = Z$ and $f_*(Z) \neq W$.

4.2.9. Find an example to show that the “ \subseteq ” in Theorem 4.2.3 (vii) cannot be replaced with “ $=$.” (It suffices to use the intersection of two sets.)

- (1) Find an example of a map $f: A \rightarrow B$ and subsets $P, Q \subseteq A$ such that $P \subsetneq Q$, but that $f_*(P) = f_*(Q)$.
- (2) Find an example of a map $g: C \rightarrow D$ and subsets $S, T \subseteq D$ such that $S \subsetneq T$, but that $g^*(S) = g^*(T)$.

4.2.11. Let $f: A \rightarrow B$ be a map and let $P, Q \subseteq A$. Show that $f_*(P) - f_*(Q) \subseteq f_*(P - Q)$. Is it necessarily the case that $f_*(P - Q) \subseteq f_*(P) - f_*(Q)$? Give a proof or a counterexample.

4.2.12. Let $f: A \rightarrow B$ be a map and let $C, D \subseteq B$. Show that $f^*(D - C) = f^*(D) - f^*(C)$.

4.2.13. Let $f: A \rightarrow B$ be a map. Let $X \subseteq A$ and $Y \subseteq B$.

- (1) Show that $X \subseteq f^*(f_*(X))$.
- (2) Show that $f_*(f^*(Y)) \subseteq Y$.
- (3) Show that $X = f^*(f_*(X))$ iff $X = f^*(Z)$ for some $Z \subseteq B$.
- (4) Show that $Y = f_*(f^*(Y))$ iff $Y = f_*(W)$ for some $W \subseteq A$.
- (5) Show that $f_*(f^*(f_*(X))) = f_*(X)$.
- (6) Show that $f^*(f_*(f^*(Y))) = f^*(Y)$.

4.2.14. Let $f, g: A \rightarrow B$ be maps. Think of these maps as inducing maps $f_*, g_*: \mathcal{P}(A) \rightarrow \mathcal{P}(B)$, and maps $f^*, g^*: \mathcal{P}(B) \rightarrow \mathcal{P}(A)$. Show that $f_* = g_*$ iff $f^* = g^*$ iff $f = g$.

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 we see in courses such as calculus is to add or multiply functions $\mathbb{R} \rightarrow \mathbb{R}$. Though very useful, this method of combining functions is not applicable to all sets, since we are able to add or multiply functions $\mathbb{R} \rightarrow \mathbb{R}$ by using the addition or multiplication of the real numbers, whereas not all sets have operations such as addition or multiplication defined on them. A more broadly applicable way of combining functions, also encountered in calculus, is when we use the chain rule for taking derivatives. This rule is used with functions such as $f: \mathbb{R} \rightarrow \mathbb{R}$ given 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. Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be functions. The **composition** of f and g is the function $g \circ f: A \rightarrow C$ defined by

$$(g \circ f)(x) = g(f(x))$$

for all $x \in A$.

△

Note that $g \circ f$ in the above definition is the name of a single function $A \rightarrow C$, which we constructed out of the two functions f and g . By contrast, the quantity $(g \circ f)(x)$ used in the definition of $g \circ f$ is a single value in the set C . It would not be correct to write “ $g \circ f(x)$,” since \circ is an operation that combines two functions, whereas “ $f(x)$ ” is not a function but a single element in the set B . Note also that for the composition of two functions to be defined, the codomain of the first function has to equal the domain of the second function.

If this is your first time using the notation $g \circ f$, it is necessary to get used to the fact that it is “backwards” from what you might expect, since $g \circ f$ means doing f first and then g (even though we generally read from left to right in English). Think of “ \circ ” as meaning “following.” The “ \circ ” notation is extremely widespread, and so we will stick to it even though it is awkward at first.

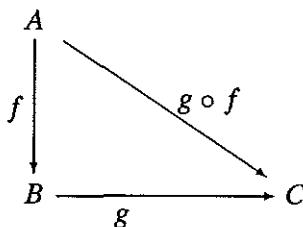
Example 4.3.1.

- (1) Define the function $m: \{\text{all people}\} \rightarrow \{\text{all people}\}$ to be the function that assigns to each person his or her mother. Then $m \circ m$ is the function that assigns to each person his or her maternal grandmother.

(2) Let $f, g: \mathbb{R} \rightarrow \mathbb{R}$ be given 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 $k: \mathbb{R} \rightarrow \mathbb{R}$ be given by $k(x) = \sin x$ for all $x \in \mathbb{R}$, and let $h: \mathbb{R}^+ \rightarrow \mathbb{R}$ be given by $h(x) = \ln x$ for all $x \in \mathbb{R}^+$. Then $k \circ h$ is defined, and is given by $(k \circ h)(x) = \sin(\ln x)$ for all $x \in \mathbb{R}^+$. On the other hand, we cannot form the composition $h \circ k$, since 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 $x \in \mathbb{R}$. \diamond

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 maps in the following diagram.



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 that go 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, we obtain $(g \circ f)(x)$.

An example of the use of composition of maps is coordinate functions. In multivariable calculus it is standard to write maps into \mathbb{R}^n in terms of coordinate functions, and we can now generalize this notion to arbitrary sets.

Definition. Let A, A_1, \dots, A_n be sets, for some positive integer n , and let $f: A \rightarrow A_1 \times \dots \times A_n$ be a function. For each $i \in \{1, \dots, n\}$, let $f_i: A \rightarrow A_i$ be defined by $f_i = \pi_i \circ f$, where $\pi_i: A_1 \times \dots \times A_n \rightarrow A_i$ is the projection map. The functions f_1, \dots, f_n are the **coordinate functions** of f . Δ

In the above definition, we see that $f(x) = (f_1(x), \dots, f_n(x)) \in A_1 \times \dots \times A_n$ for all $x \in A$. It is thus standard to write the abbreviation $f = (f_1, \dots, f_n)$, with some books writing $f = f_1 \times \dots \times f_n$ to mean the

same thing. Both these notations for writing f in terms of its coordinate functions are convenient, but they should not be taken to be more than handy abbreviations. Whereas the notation $f(x) = (f_1(x), \dots, f_n(x))$ is perfectly sensible, the two sides of the equation being different expressions for the same element of a certain set, the map f is neither an element of the product of n sets, as the notation (f_1, \dots, f_n) might mistakenly suggest, nor the product of n sets, as the notation $f_1 \times \dots \times f_n$ might mistakenly suggest. We can form a picture of coordinate functions by using the following commutative diagram. Each triangle of maps in the diagram is commutative in the sense described above.

$$\begin{array}{ccccc} & & A & & \\ & f_1 \swarrow & \downarrow f & \searrow f_2 & \\ A_1 & \xleftarrow{\pi_1} & A_1 \times A_2 & \xrightarrow{\pi_2} & A_2 \end{array}$$

Example 4.3.2. Let $f: \mathbb{R}^2 \rightarrow \mathbb{R}^3$ be given by

$$\underline{f((x, y)) = (xy, \sin x^2, x + y^3)}$$

for all $(x, y) \in \mathbb{R}^2$. The three coordinate functions of f are $f_1, f_2, f_3: \mathbb{R}^2 \rightarrow \mathbb{R}$ given by

$$\underline{f_1((x, y)) = xy}, \quad \underline{f_2((x, y)) = \sin x^2}, \quad \text{and} \quad \underline{f_3((x, y)) = x + y^3}$$

for all $(x, y) \in \mathbb{R}^2$. ◊

Which of the familiar properties of operations (for example commutativity and associativity) hold for composition of functions? The commutative law, which for numbers and addition says that $a + b = b + a$ for any numbers a and b , does not hold for functions and composition on two counts. First, suppose we have functions $f: A \rightarrow B$ and $g: B \rightarrow C$, so that we can form $g \circ f$. Unless it happens 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 4.3.1 (2). The following lemma shows that some nice properties do hold for composition.

Lemma 4.3.3. *Let $f: A \rightarrow B$, let $g: B \rightarrow C$ and let $h: C \rightarrow D$ be functions.*

(i) $(h \circ g) \circ f = h \circ (g \circ f)$ (*Associative Law*).

(ii) $f \circ 1_A = f$ and $1_B \circ f = f$ (*Identity Law*).

Proof. (i). 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 and codomain, so we only need to see what both functions do to the elements of A . If $a \in A$, then

$$\begin{aligned} ((h \circ g) \circ f)(a) &= (h \circ g)(f(a)) = h(g(f(a))) \\ &= h((g \circ f)(a)) = (h \circ (g \circ f))(a), \end{aligned}$$

which proves that the two functions are equal.

(ii). This is straightforward, and is left to the reader. \square

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, thus yielding 0. For functions, the roles of the operation addition and the number 0 are replaced by composition of maps 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. Let $f: A \rightarrow B$ and $g: B \rightarrow A$ 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. Δ

Observe that $f \circ g = 1_B$ means that $f(g(x)) = x$ for all $x \in B$, and that $g \circ f = 1_A$ means that $g(f(x)) = x$ for all $x \in A$. We used the term “an inverse” in the above definition, but the following result shows that we could actually have written “the inverse.”

Lemma 4.3.4. *Let $f: A \rightarrow B$ be a function.*

- (i) *If f has an inverse, then the inverse is unique.*
- (ii) *If f has a right inverse g and a left inverse h , then $g = h$; hence f has an inverse.*
- (iii) *If f has an inverse g , then g has an inverse, which is f .*

Proof. (i). Suppose that $g, h: B \rightarrow A$ 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 4.3.3 repeatedly we have

$$g = 1_A \circ g = (h \circ f) \circ g = h \circ (f \circ g) = h \circ 1_B = h.$$

(ii). The proof is virtually the same as in part (i).

(iii). Since $g: B \rightarrow A$ 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 . By part (i) of this lemma, we know that f is the unique inverse of g . \square

Observe that the proof of part (i) of the above theorem 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 the proof of Theorem 7.2.2 (ii).

If a function $f: A \rightarrow B$ has an inverse function, then it is unique by the above lemma. It is standard to denote this unique inverse function by $f^{-1}: B \rightarrow A$. (For those who use the notation $f^{-1}(Q)$ to denote the inverse image of the subset $Q \subseteq B$ under the map f (in contrast to the notation $f^*(Q)$ we used starting in Section 4.2), it is important to note the contrast between this use of the symbol $f^{-1}(Q)$ and the notation f^{-1} used for the inverse function. The quantity $f^{-1}(Q)$ denotes a set, not a function, and it exists even if the function f^{-1} does not exist. If the inverse function f^{-1} does exist, then the notation $f^{-1}(Q)$ could mean either the inverse image of the set Q under the map f , or the image of the set Q under the map f^{-1} . Fortunately, it can be verified that both these options refer to the same subset of A .)

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, the right or left inverse need not be unique.

Example 4.3.5.

(1) Let $k: (0, 1) \rightarrow (3, 5)$ given by $k(x) = 2x + 3$ for all $x \in (0, 1)$. We claim that k has an inverse, namely $j: (3, 5) \rightarrow (0, 1)$ given by $j(x) = (x - 3)/2$ for all $x \in (3, 5)$. We compute $j(k(x)) = ((2x + 3) - 3)/2 = x$ for all $x \in (0, 1)$, and hence $j \circ k = 1_{(0,1)}$. Similarly, we compute $k(j(x)) = 2 \cdot (x - 3)/2 + 3 = x$ for all $x \in (3, 5)$, and hence $k \circ j = 1_{(3,5)}$. Thus j is both a right inverse and a left inverse for k , and hence it is an inverse for k . Thus $j = k^{-1}$.

(2) Let $f: \mathbb{R} \rightarrow [0, \infty)$ be given by $f(x) = x^2$ for all $x \in \mathbb{R}$. This function has no left inverse, but many right inverses, of which we show two. Let $g, h: [0, \infty) \rightarrow \mathbb{R}$ be given 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 , since $(f \circ g)(x) = f(g(x)) = (\sqrt{x})^2 = x$ 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 $m: [0, \infty) \rightarrow \mathbb{R}$. How should we define $m(9)$? (We could have chosen any other positive number instead of 9.) Since m is a left inverse for f , we know that $m \circ f = 1_{\mathbb{R}}$. Hence $m(f(x)) = x$ for all $x \in \mathbb{R}$. On the one hand, we would then need to have $m(9) = m(3^2) = (m \circ f)(3) = 3$, and on the other hand, we would similarly need to have $m(9) = m((-3)^2) = (m \circ f)(-3) = -3$. Thus there is no possible way to define $m(9)$. Hence f has no left inverse.

(3) Let $p: [0, \infty) \rightarrow \mathbb{R}$ be given by $p(x) = x^2$ for all $x \in [0, \infty)$. Then p has no right inverse, but many left inverses, of which we show two. Let $q, r: \mathbb{R} \rightarrow [0, \infty)$ be given by

$$q(x) = \begin{cases} \sqrt{x}, & \text{if } x \geq 0 \\ 1, & \text{if } x < 0, \end{cases} \quad r(x) = \begin{cases} \sqrt{x}, & \text{if } x \geq 0 \\ \sin x, & \text{if } x < 0. \end{cases}$$

Both q and r are left inverses for p , since $(q \circ p)(x) = q(p(x)) = \sqrt{x^2} = x$ 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 $u: \mathbb{R} \rightarrow [0, \infty)$. How should we define $u(-4)$? Since u is a right inverse for p , we know that $p \circ u = 1_{\mathbb{R}}$. Hence $p(u(x)) = x$ for all $x \in \mathbb{R}$. Thus $(u(x))^2 = x$ for all $x \in \mathbb{R}$. Hence we would need to have $(u(-4))^2 = -4$, which is impossible, since $u(-4)$ is a real number, and no real number squared is negative. Thus there is no possible way to define $u(-4)$. Hence p has no right inverse.

(4) We claim that the function $s: \mathbb{R} \rightarrow \mathbb{R}$ given by $s(x) = x^2$ for all $x \in \mathbb{R}$ has neither a right inverse nor a left inverse. That s has no left inverse follows from the same argument used to show that the map f in part (2) of this example has no left inverse, and that s has no right inverse follows the same argument used to show that the map p in part (3) of this example has no right inverse. \diamond

Exercises

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 $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = e^x$ for all $x \in \mathbb{R}$, and let $g: \mathbb{R} \rightarrow \mathbb{R}$ be given by $g(x) = \sin x$ for all $x \in \mathbb{R}$.
- (2) Let $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ be given by $f(x) = x^7$ for all $x \in \mathbb{R}$, and let $g: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ be given by $g(x) = x^{-3}$ for all $x \in \mathbb{R}^+$.
- (3) Let $f: \mathbb{R} \rightarrow [0, \infty)$ be given by $f(x) = x^6$ for all $x \in \mathbb{R}$, and let $g: [0, \infty) \rightarrow \mathbb{R}$ be given by $g(x) = \sqrt[5]{x}$ for all $x \in [0, \infty)$.
- (4) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = \lfloor x \rfloor$ for all $x \in \mathbb{R}$, and let $g: \mathbb{R} \rightarrow \mathbb{R}$ be given 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 . (See Exercise 2.4.11 for more about the former of these.)

4.3.2. For each of the following functions $f: \mathbb{R} \rightarrow \mathbb{R}$, find non-identity functions $g, h: \mathbb{R} \rightarrow \mathbb{R}$ such that $f = h \circ g$.

- (1) $f(x) = \sqrt{x+7}$ for all $x \in \mathbb{R}$.
- (2) $f(x) = \sqrt[3]{x+7}$ for all $x \in \mathbb{R}$.
- (3) $f(x) = \begin{cases} x^6, & \text{if } 0 \leq x \\ x^4, & \text{if } x < 0. \end{cases}$
- (4) $f(x) = \begin{cases} x^3, & \text{if } 0 \leq x \\ x, & \text{if } x < 0. \end{cases}$

4.3.3. Let $f, g: \mathbb{R} \rightarrow \mathbb{R}$ be given by

$$f(x) = \begin{cases} 1 - 2x, & \text{if } x \geq 0 \\ |x|, & \text{if } x < 0, \end{cases} \quad g(x) = \begin{cases} 3x, & \text{if } x \geq 0 \\ x - 1, & \text{if } x < 0. \end{cases}$$

Find $f \circ g$ and $g \circ f$.

- 4.3.4.** (1) Find two functions $h, k: \mathbb{R} \rightarrow \mathbb{R}$ such that neither h nor k is a constant map, but $k \circ h$ is a constant map.
 (2) Find two functions $s, t: \mathbb{R} \rightarrow \mathbb{R}$ such that neither $s \neq 1_{\mathbb{R}}$ and $t \neq 1_{\mathbb{R}}$, but $t \circ s = 1_{\mathbb{R}}$.

4.3.5. [Used in Section 6.1.] Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be functions, and let $U \subseteq A$ and $V \subseteq C$ be subsets. Show that

$$(g \circ f)_*(U) = g_*(f_*(U)) \quad \text{and} \quad (g \circ f)^*(V) = f^*(g^*(V)).$$

4.3.6. Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be functions that both have inverse functions. Show that $g \circ f$ has an inverse function, and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

4.3.7. Find two right inverses for each of the following functions.

(1) Let $h: \mathbb{R} \rightarrow [0, \infty)$ be given by $f(x) = |x|$ for all $x \in \mathbb{R}$.

(2) Let $k: \mathbb{R} \rightarrow [1, \infty)$ be given by $h(x) = e^{x^2}$ for all $x \in \mathbb{R}$.

4.3.8. Find two left inverses for each of the following functions.

(1) Let $f: [0, \infty) \rightarrow \mathbb{R}$ be given by $f(x) = x^3 + 4$ for all $x \in [0, \infty)$.

(2) Let $g: \mathbb{R} \rightarrow \mathbb{R}$ be given by $g(x) = e^x$ for all $x \in \mathbb{R}$.

4.3.9. Define maps $h, k: \mathbb{R} \rightarrow \mathbb{R}$ by

$$h(x) = \begin{cases} 4x + 1, & \text{if } x \geq 0 \\ x, & \text{if } x < 0, \end{cases} \quad k(x) = \begin{cases} 3x, & \text{if } x \geq 0 \\ x + 3, & \text{if } x < 0. \end{cases}$$

Find an inverse for $k \circ h$.

4.3.10. Let $f: A \rightarrow B$ be a map. Show that if f has two distinct left inverses, then it has no right inverse. Show that if f has two distinct right inverses, then it has no left inverse.

4.3.11. Let A, A_1, \dots, A_k be sets, for some positive integer k , let $f: A \rightarrow A_1 \times \dots \times A_k$ be a function and let $U_i \subseteq A_i$ for each $i \in \{1, \dots, k\}$. Show that

$$f^*(U_1 \times \dots \times U_k) = \bigcap_{i=1}^k (f_i)^*(U_i),$$

where the f_i are the coordinate functions of f .

4.3.12. Let A, A_1, \dots, A_k be sets, for some positive integer k , and let $h_i: A \rightarrow A_i$ be a function for each $i \in \{1, \dots, k\}$. Show that there is a unique function $g: A \rightarrow A_1 \times \dots \times A_k$ such that $\pi_i \circ g = h_i$ for all $i \in \{1, \dots, k\}$, where $\pi_i: A_1 \times \dots \times A_k \rightarrow A_i$ is the projection map. This exercise can be represented by the following commutative diagram.

$$\begin{array}{ccc} A & \xrightarrow{g} & A_1 \times \dots \times A_k \\ & \searrow h_i & \downarrow \pi_i \\ & & A_i \end{array}$$

4.3.13. This exercise and the next give examples of definitions of functions by universal property. Rather than defining what certain functions are, we state how they should behave, and then prove that such things exist. 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 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 $f, g: A \rightarrow B$ be maps. Show that there exists a set E and a map $e: E \rightarrow A$ such that $f \circ e = g \circ e$, and that for any set C and map $h: C \rightarrow A$ such that $f \circ h = g \circ h$, there is a unique map $t: C \rightarrow E$ such that $h = e \circ t$. The last condition is expressed by saying that the following diagram commutes. The map e is called an **equalizer** of f and g .

$$\begin{array}{ccccc} & & C & & \\ & \downarrow t & & \searrow h & \\ & E & \xrightarrow{e} & A & \xrightleftharpoons[f]{g} B \end{array}$$

4.3.14. This exercise is similar to the previous one. Let A, B and C be sets, and let $f: A \rightarrow C$ and $g: B \rightarrow C$ be maps. Show that there exists a set P and maps $h: P \rightarrow A$ and $k: P \rightarrow B$ such that $f \circ h = g \circ k$, and that for any set X and maps $s: X \rightarrow A$ and $t: X \rightarrow B$ such that $f \circ s = g \circ t$, there is a unique map $u: X \rightarrow P$ such that $s = h \circ u$ and $t = k \circ u$. These conditions are expressed by saying that the following diagram commutes. The maps h and k are a **pullback** of f and g .

$$\begin{array}{ccccc} & & X & & \\ & \swarrow u & & \searrow t & \\ & & P & \xrightarrow{k} & B \\ & \downarrow s & \downarrow h & & \downarrow g \\ A & \xrightarrow{f} & C & & \end{array}$$

4.4 Injectivity, Surjectivity and Bijectivity

As we saw in Example 4.3.5, there exist functions with neither right nor left inverse, others with a right inverse but not a left inverse, or vice versa, and others with both a right and a left inverse (and hence an inverse by Lemma 4.3.4 (ii)). Are there any convenient criteria by which to check whether a function in principle has a left inverse, right inverse or both before attempting to find an inverse function of the appropriate type? Remarkably, there are such criteria, as seen in Theorem 4.4.3 below.

Let P denote the set of all people, and let $f: P \rightarrow P$ be the function such that $f(x)$ is x 's mother. Does this function have a right inverse or a left inverse? Suppose first that $g: P \rightarrow P$ is a right inverse for f . This would mean that $f \circ g = 1_P$, and thus $f(g(x)) = x$ for every person x . Suppose m is some man. Then it would follow that $f(g(m)) = m$, which would mean that m is $g(m)$'s mother. This is impossible, since men cannot be mothers. Thus f has no right inverse. The obstacle to finding a right inverse for f is that there are objects in the codomain (namely men, and some women) who are not in the range of f (namely the set of mothers).

Now suppose that $h: P \rightarrow P$ is a left inverse for f . That would mean that $h \circ f = 1_P$, and thus $h(f(x)) = x$ for every person x . Here we will encounter a different problem than with the proposed right inverse. Suppose a and b are siblings. Then $f(a) = f(b)$, since a and b have the same mother. It would then follow that $h(f(a)) = h(f(b))$. Since $h(f(x)) = x$ for every person x , it would follow that $a = b$, which is a contradiction. Thus f 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 will turn out that the two problems just identified are the only obstacles to finding right and left inverses. We now give names to maps that do not have these problems.

Definition. Let $f: A \rightarrow B$ be a function.

- (1) The map f is **injective** (also known as **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 map f is **surjective** (also known as **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 map f is **bijective** if it is both injective and surjective. △

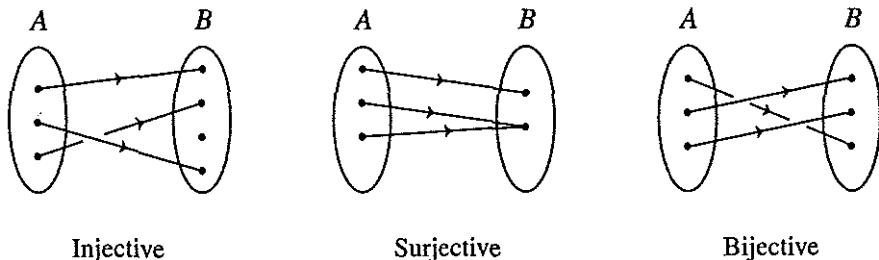


Figure 4.4.1.

Example 4.4.1. 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.

(1) A function that is both injective and surjective (and hence bijective) is $k: [0, \infty) \rightarrow [0, \infty)$ given by $k(x) = x^2$ for all $x \in [0, \infty)$. To see 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. To see that k is injective, let $x, y \in [0, \infty)$, and suppose that $k(x) = k(y)$. Thus $x^2 = y^2$. It follows that $\sqrt{x^2} = \sqrt{y^2}$, and since $x, y \geq 0$, we see that $x = \sqrt{x^2} = \sqrt{y^2} = y$. Hence k is injective.

(2) A function that is surjective but not injective is $h: \mathbb{R} \rightarrow [0, \infty)$ given by $h(x) = x^2$ for all $x \in \mathbb{R}$. The proof of the surjectivity of h is like that of k . The reason h is not injective is, for example, that $h(-3) = 9 = h(3)$ even though $-3 \neq 3$.

(3) A function that is injective but not surjective is $g: [0, \infty) \rightarrow \mathbb{R}$ given by $g(x) = x^2$ for all $x \in [0, \infty)$. The proof of the injectivity of g is just like that of k . The reason that g is not surjective is, for example, that $g(a) \neq -2$ for any $a \in [0, \infty)$, though -2 is in the codomain of g .

(4) A function that is neither injective nor surjective is $f: \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = x^2$ for all $x \in \mathbb{R}$. The reason that f is neither injective nor surjective is like the arguments for h and g . Observe from these examples that injectivity and surjectivity very much depend upon the choice of domain and codomain of a function. ◇

The terminology “one-to-one” and “onto” are fairly prevalent, especially in books at the elementary level, but these words are unfortunate. 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 does not seem parallel to “one-to-one.” The two adjectives “injective” and “surjective” are clearly parallel. Moreover, some texts use the word “onto” as if it were

an adjective, leading to phrases such as “the function f is a one-to-one and onto function,” which are grammatically problematic; 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. We will stick to the terms injective and surjective. (If you really want to use prepositions rather than adjectives to describe functions, the author’s proposed scheme would be that an arbitrary function $f: A \rightarrow B$ be described as a function from A to B ; an injective function be described as from A into B ; a surjective function be described as from A onto B ; and a bijective function be described as from A unto B . The author would not necessarily recommend the use of this scheme, but it is consistent.)

We note that a function is surjective iff its range equals its codomain. One way of thinking about injectivity, surjectivity and bijectivity is as follows. Let $f: A \rightarrow B$ be a map. The map f is injective iff for each element of $b \in B$, there is at most one element in the inverse image $f^*(\{b\})$; the map f is surjective iff for each element of $b \in B$, there is at least one element in the inverse image $f^*(\{b\})$; the map f is bijective iff for each element of $b \in B$, there is precisely one element in the inverse image $f^*(\{b\})$. Consider now the special case of a map $f: \mathbb{R} \rightarrow \mathbb{R}$. Then the function f is injective iff each horizontal line in the plane intersects its graph at most once. See Figure 4.4.2 part (i). The function f is surjective iff each horizontal line intersects its graph at least once. See Figure 4.4.2 part (ii). The function f is bijective iff each horizontal line intersects its graph once and only once.

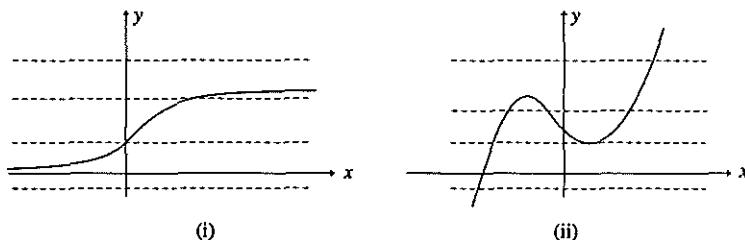


Figure 4.4.2.

There is a standard strategy for proving that a function is injective or surjective. Let $f: A \rightarrow B$ be a map. 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 would typically look like “Let $x, y \in A$. Suppose that $f(x) = f(y)$ (argumentation) . . . 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 typically look like “Let $b \in B$ We define a by $a = \text{blah}$ (argumentation) . . . Then $b = f(a)$. Hence f is surjective.”

We will use the above strategies in the proof of the following lemma, which shows that composition of maps behaves nicely with respect to injectivity, surjectivity and bijectivity.

Lemma 4.4.2. *Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be functions.*

(i) *If f and g are both injective, then so is $g \circ f$.*

(ii) *If f and g are both surjective, then so is $g \circ f$.*

(iii) *If f and g are both bijective, then so is $g \circ f$.*

Proof. (i) Suppose that f and g are both injective. We wish to show that $g \circ f: A \rightarrow C$ is injective. Let $x, y \in A$. We will show that $(g \circ f)(x) = (g \circ f)(y)$ implies $x = y$. Assume that $(g \circ f)(x) = (g \circ f)(y)$. Thus $g(f(x)) = g(f(y))$. Since g is injective, we deduce that $f(x) = f(y)$. Since f is injective, we then deduce that $x = y$.

(ii) Suppose that f and g are both surjective. We wish to show that $g \circ f: A \rightarrow C$ is surjective. Let $p \in C$. We will show that there exists some element $a \in A$ such that $(g \circ f)(a) = p$. Since $p \in C$ and g is surjective, we know that there is some $w \in B$ such that $g(w) = p$. Since f is surjective, we know that there is some $a \in A$ such that $f(a) = w$. It follows that $(g \circ f)(a) = g(f(a)) = g(w) = p$.

(iii) This is derived easily from parts (i) and (ii). □

The converse to each of the parts of the above lemma is not true. Exercise 4.4.13 discusses the best possible results that can be proved.

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 4.4.3. *Let A and B be non-empty sets, and let $f: A \rightarrow B$ be a function.*

(i) *The function f has a right inverse iff f is surjective.*

(ii) *The function f has a left inverse iff f is injective.*

(iii) *The function f has an inverse iff f is bijective.*

Proof. (i). Suppose f has a right inverse g . Hence $f \circ g = 1_B$. 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 would be a map $h : B \rightarrow A$ such that $f \circ h = 1_B$. We define h as follows. For each $b \in B$, there is by surjectivity 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). That is, let $h(b)$ be any choice of element in the set $f^*(\{b\})$. It is now true by definition that $f(h(b)) = b$ for all $b \in B$. Hence $f \circ h = 1_B$.

(ii). Left to the reader in Exercise 4.4.9.

(iii). This follows from parts (i) and (ii), and Lemma 4.3.4 (ii). \square

An important comment is needed about the seemingly innocent proof of part (i) of the above theorem. In the second paragraph of the proof we chose — simultaneously — one element from each set of the form $f^*(\{b\})$, for all $b \in B$. Though it seems intuitively reasonable that we can simultaneously choose an element from each of these sets, if set theory is dealt with axiomatically, then this ability to choose requires the Axiom of Choice, one of the axioms commonly assumed (though not universally accepted) for set theory. See Section 3.2 for a few comments about this axiom, and for references.

The following result concerning “cancelation” of functions is a typical application of Theorem 4.4.3.

Theorem 4.4.4. *Let A and B be non-empty sets, and let $f : A \rightarrow B$ be a function.*

(i) *The function f is surjective iff $g \circ f = h \circ f$ implies $g = h$ for all functions $g, h : B \rightarrow X$, for all sets X .*

(ii) *The function f is injective iff $f \circ g = f \circ h$ implies $g = h$ for all functions $g, h : Y \rightarrow A$, for all sets Y .*

Proof. We will prove part (i), leaving part (ii) to the reader in Exercise 4.4.14.

(i) First assume that f is surjective. Let $g, h: B \rightarrow X$ be functions such that $g \circ f = h \circ f$, for some set X . By Theorem 4.4.3 (i), the function f has a right inverse $q: B \rightarrow A$. It now follows from the hypothesis on g and h that $(g \circ f) \circ q = (h \circ f) \circ q$. Using Lemma 4.3.3 and the definition of right inverses, we see that $g \circ (f \circ q) = h \circ (f \circ q)$, and thus $g \circ 1_B = h \circ 1_B$, and so $g = h$.

Now assume f is not surjective. Let $b \in B$ be a point that is not in the image of f . Let $X = \{1, 2\}$. Define $g, h: B \rightarrow X$ 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

4.4.1. Is each of the following functions injective, surjective, both or neither. Prove your answers.

- (1) Let $t: (1, \infty) \rightarrow \mathbb{R}$ be defined by $t(x) = \ln x$ for all $x \in (1, \infty)$.
- (2) Let $s: \mathbb{R} \rightarrow \mathbb{R}$ be defined by $s(x) = x^4 - 5$ for all $x \in \mathbb{R}$.
- (3) Let $g: [0, \infty) \rightarrow [0, 1)$ be defined by $g(x) = \frac{x}{1+x}$ for all $x \in [0, \infty)$.
- (4) Let $k: \mathbb{R}^2 \rightarrow \mathbb{R}$ be defined by $k((x, y)) = x^2 + y^2$ for all $(x, y) \in \mathbb{R}^2$.
- (5) Let $Q: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$ be defined by $Q(n) = \{1, 2, \dots, n\}$ for all $n \in \mathbb{N}$.

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) $f: \mathbb{Z} \rightarrow \mathbb{Z}$. | (3) $f: \mathbb{Q} \rightarrow \mathbb{R}$. |
| (2) $f: \mathbb{Q} \rightarrow \mathbb{Q}$. | (4) $f: \mathbb{R} \rightarrow \mathbb{R}$. |

4.4.3. Let A and B be sets and let $S \subseteq A$. We will be using various definitions from Section 4.1.

- (1) Show that the identity map $1_A: A \rightarrow A$ is bijective.
- (2) Show that inclusion map $j: S \rightarrow A$ is injective.
- (3) Suppose that $f: A \rightarrow B$ is an injective map. Is the restriction $f|_S$ necessarily injective? Give a proof or a counterexample.
- (4) Suppose that $g: A \rightarrow B$ is a surjective map. Is the restriction $g|_S$ necessarily surjective? Give a proof or a counterexample.

(5) Suppose that $h: S \rightarrow B$ is an injective map, and let $\hat{h}: A \rightarrow B$ be an extension of h . Is \hat{h} necessarily injective? Give a proof or a counterexample.

(6) Suppose that $k: S \rightarrow B$ is a surjective map, and let $\hat{k}: A \rightarrow B$ be an extension of k . Is \hat{k} necessarily surjective? Give a proof or a counterexample.

(7) Show that the projection maps $\pi_1: A \times B \rightarrow A$ and $\pi_2: A \times B \rightarrow B$ are surjective. Are the projection maps injective?

4.4.4. Let h and k be as in Exercise 4.3.9. Is $h \circ k$ bijective, injective, surjective or neither?

4.4.5. Let A and B be sets. Show that there is a bijective map $f: A \times B \rightarrow B \times A$.

4.4.6. [Used in Section 3.3.] Let A , B and C be sets. Show that there is a bijective map $g: (A \times B) \times C \rightarrow A \times (B \times C)$.

4.4.7. Let A be a set. Let $\phi: \mathcal{P}(A) \rightarrow \mathcal{P}(A)$ be defined by $\phi(X) = A - X$ for all $X \in \mathcal{P}(A)$. Show that ϕ is bijective.

4.4.8. [Used in Section 6.4.] Define the set \mathbb{L} to be

$$\mathbb{L} = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ and } b \text{ are relatively prime}\},$$

where relatively prime is defined in Exercise 2.4.3. Define two functions $U, D: \mathbb{L} \rightarrow \mathbb{L}$ 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) Show that $(1, 1) \notin U(\mathbb{L})$ and $(1, 1) \notin D(\mathbb{L})$.

(2) Show that $U((a, b)) \neq (a, b)$ and $D((a, b)) \neq (a, b)$ for all $(a, b) \in \mathbb{L}$.

(3) Show that U and D are both injective.

(4) Show that $U(\mathbb{L}) \cap D(\mathbb{L}) = \emptyset$.

4.4.9. [Used in Section 4.4.] Prove Theorem 4.4.3 (ii).

4.4.10. [Used in Section 6.1] Let $f: A \rightarrow B$ be an injective map, and let $P, Q \subseteq A$ be any sets. Show that $f_*(P - Q) = f_*(P) - f_*(Q)$. (Use Exercise 4.2.11 for part of the proof.)

4.4.11. Let $f: A \rightarrow B$ be a function.

(1) Show that f is injective iff $E = f^*(f_*(E))$ for all subsets $E \subseteq A$.

(2) Show that f is surjective iff $F = f_*(f^*(F))$ for all subsets $F \subseteq B$.

4.4.12. [Used in Sections 4.5 and 6.1.] Let $f: A \rightarrow B$ and $g: B \rightarrow A$ be functions.

- (1) Suppose that f is surjective, and that g is a right inverse of f . Show that g is injective.
- (2) Suppose that f is injective, and that g is a left inverse of f . Show that g is surjective.
- (3) Suppose that f is bijective, and that g is the inverse of f . Show that g is bijective.

4.4.13. [Used in Section 4.4.] Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be functions.

- $\begin{array}{c} f(a) = b \\ g(b) = c \end{array}$
- (1) Show that if $g \circ f$ is injective, then f must be injective.
 - (2) Show that if $g \circ f$ is surjective, then g must be surjective.
 - (3) Show that if $g \circ f$ is bijective, then f must be injective, and g must be surjective.
 - (4) Find an example of maps $f: A \rightarrow B$ and $g: B \rightarrow C$ such that $g \circ f$ is bijective, but f is not surjective, and g is not injective. Thus parts (1) – (3) of this exercise are the best possible results.

4.4.14. [Used in Section 4.4.] Prove Theorem 4.4.4 (ii).

4.4.15. Let $f: A \rightarrow B$ be a map. Show that f is surjective iff $B - f_*(X) \subseteq f_*(A - X)$ for all $X \subseteq A$.

4.4.16. Let $h: X \rightarrow Y$ be a function. Show that h is injective iff $h_*(A \cap B) = h_*(A) \cap h_*(B)$ for all $A, B \subseteq X$.

4.4.17. Let $f: A \rightarrow B$ be a map. Think of this map as inducing a map $f_*: \mathcal{P}(A) \rightarrow \mathcal{P}(B)$, and a map $f^*: \mathcal{P}(B) \rightarrow \mathcal{P}(A)$.

- (1) Show that f_* is surjective iff f is surjective.
- (2) Show that f_* is injective iff f is injective.
- (3) Show that f^* is surjective iff f is injective.
- (4) Show that f^* is injective iff f is surjective.
- (5) Show that f_* is bijective iff f^* is bijective iff f is bijective.
- (6) Suppose that f is bijective. Show that f_* and f^* are inverses of each other.

4.4.18. Let A be a non-empty set, and let $f: A \rightarrow A$ be a bijective map. For any positive integer n , let f^n denote the map $A \rightarrow A$ given by

$$f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

We refer to f^n as the **n -fold iteration** of f . Define $f^0 = 1_A$. Since f is bijective, then its inverse f^{-1} exists. Define f^{-n} for any positive integer n to be $(f^{-1})^n$. It can be seen that $f^a \circ f^b = f^{a+b}$ and that $(f^a)^b = f^{ab}$ for all $a, b \in \mathbb{Z}$.

(1) Let $x, y, z \in A$. Show 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 $z = f^u(x)$ for some $u \in \mathbb{Z}$.

(In Section 5.3 we will see that these three properties are particularly important.)

(2) Let $x \in A$. The **orbit** of x under f is defined to be the set $\mathcal{O}_{f,x} = \{f^n(x) \mid n \in \mathbb{Z}\}$. Let $y \in A$. Show that the following four properties hold.

- (A) If $y = f^m(x)$ for some $m \in \mathbb{Z}$, then $\mathcal{O}_{f,x} = \mathcal{O}_{f,y}$.
- (B) If $y \neq f^n(x)$ for any $n \in \mathbb{Z}$, then $\mathcal{O}_{f,x} \cap \mathcal{O}_{f,y} = \emptyset$.
- (C) $x \in \mathcal{O}_{f,y}$ iff $y \in \mathcal{O}_{f,x}$.
- (D) $A = \bigcup_{x \in A} \mathcal{O}_{f,x}$.

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 form a partition of A .)

(3) Give an example of a bijective map $\mathbb{Z} \rightarrow \mathbb{Z}$ with infinitely many orbits. Let r be a positive integer. Give an example of a bijective map $\mathbb{Z} \rightarrow \mathbb{Z}$ with precisely r orbits.

4.4.19. This exercise assumes Exercise 4.4.18. Let A be a non-empty finite set. The results in this exercise are valid only for finite sets. Let $f: A \rightarrow A$ be a bijective map. Let $x \in A$.

(1) Show that $f^m = 1_A$ for some positive integer m . Let r be the smallest positive integer such that $f^r = 1_A$.

- (2) Suppose that $y = f^i(x)$ for some $i \in \mathbb{Z}$. Show that there is some non-negative integer s such that $y = f^s(x)$.
- (3) Let the orbit of x under f be as defined in Exercise 4.4.18 (2). Show that if $f^k(x) = x$ for some $k \in \mathbb{Z}$, then $f^k(y) = y$ for all $y \in \mathcal{O}_{f,x}$.
- (4) Show that there is some positive integer v such that $f^v(x) = x$. Let q be the smallest positive integer such that $f^q(x) = x$. We call q the **order** of x with respect to f .
- (5) Suppose $y \in \mathcal{O}_{f,x}$. Show that the order of y with respect to f equals q .
- (6) Show that $\mathcal{O}_{f,x} = \{x, f(x), f^2(x), \dots, f^{q-1}(x)\}$. (Using the notation that $f^0(x) = x$, then $\mathcal{O}_{f,x} = \{f^0(x), \dots, f^{q-1}(x)\}$.)
- (7) Show that $q|r$.
- (8) The **stabilizer** of x with respect to f is defined to be the set $f_x = \{m \in \mathbb{Z} \mid f^m(x) = x \text{ and } 0 \leq m < r\}$. Suppose that $y \in \mathcal{O}_{f,x}$. Show that $|f_y| = |f_x|$.
- (9) Show that $r = |\mathcal{O}_{f,x}| \cdot |f_x|$.
- (10) Since A is finite, there are finitely many distinct orbits in A . Let B denote the number of distinct orbits of f . Show that $r \cdot B = \sum_{y \in A} |f_y|$.
- (11) For any $m \in \{0, \dots, r-1\}$, define the **fixed set** of m to be $A_m = \{z \in A \mid f^m(z) = z\}$. Show that $r \cdot B = \sum_{i=0}^{r-1} |A_i|$. This result is a special case of Burnside's Formula; see [Fra94, Section 3.7] for more details.

4.5 Sets of Functions

We now go to one level higher of abstraction than we have seen so far. Up till 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 quite useful in everything from linear algebra to functional analysis, and hence are well worth studying. We will use sets of functions briefly at the end of Section 6.2, and more extensively in Section 7.7. The material in this section is among the most conceptually difficult in this book. We start with the following definition.

Definition. Let A and B be sets. The set $\mathcal{F}(A, B)$ is defined to be the set of all functions $f: A \rightarrow B$. Δ

If A and B are any sets, we observe that $\mathcal{F}(A, B)$ is also a set; each element of the set $\mathcal{F}(A, B)$ is a function $A \rightarrow B$. There is no theoretical

problem with having a set whose elements are functions, though sometimes it is hard to get an intuitive picture of what is going on. We prove results about sets of functions no differently than we prove things about sets containing simpler objects (such as numbers). Observe that if neither A nor B is empty, then $\mathcal{F}(A, B)$ is also not empty; if either of A or B is the empty set, then so is $\mathcal{F}(A, B)$.

Example 4.5.1.

(1) Let $A = \{1, 2\}$ and $B = \{x, y\}$. Then $\mathcal{F}(A, B) = \{f, g, h, k\}$, where $f, g, h, k: A \rightarrow B$ are the maps such that $f(1) = x$ and $f(2) = x$, such that $g(1) = x$ and $g(2) = y$, such that $h(1) = y$ and $h(2) = x$, and such that $k(1) = y$ and $k(2) = y$.

(2) 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 $\mathbb{R} \rightarrow \mathbb{R}$, and the set $D(\mathbb{R}, \mathbb{R})$ of all differentiable functions $\mathbb{R} \rightarrow \mathbb{R}$. Observe that $D(\mathbb{R}, \mathbb{R}) \subsetneq C(\mathbb{R}, \mathbb{R}) \subsetneq \mathcal{F}(\mathbb{R}, \mathbb{R})$. We can define a number of useful maps between these three sets, for example $K: D(\mathbb{R}, \mathbb{R}) \rightarrow \mathcal{F}(\mathbb{R}, \mathbb{R})$ given 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 $f(x) = x^2 + 5$ for all $x \in \mathbb{R}$ and $g(x) = x^2 + 7$ for all $x \in \mathbb{R}$. Then $K(f) = K(g)$, even though $f \neq g$.

(3) 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 $f(1), f(2), f(3), \dots$. Conversely, given a sequence of real numbers a_1, a_2, a_3, \dots , we can define an element $g \in \mathcal{F}(\mathbb{N}, \mathbb{R})$ by setting $g(1) = a_1, g(2) = a_2$, etc. Thus 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 we could give concerning sets of functions; we give two typical results. We start with a relatively simple lemma, which will be of use later on.

Lemma 4.5.2. *Let A, B, C and D be sets. Suppose that there are bijective maps $f: A \rightarrow C$ and $g: B \rightarrow D$. Then there is a bijective map from $\mathcal{F}(A, B)$ to $\mathcal{F}(C, D)$.*

Proof. Since f and g are both bijective, they have inverse maps f^{-1} and g^{-1} respectively. Define $\Phi: \mathcal{F}(A, B) \rightarrow \mathcal{F}(C, D)$ by $\Phi(h) = g \circ h \circ f^{-1}$ for all $h \in \mathcal{F}(A, B)$. (See the commutative diagram following the 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 $h, k \in \mathcal{F}(A, B)$,

and 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 it follows that $h = k$. Thus Φ is injective. Now let $r \in \mathcal{F}(C, D)$. Then define $t = g^{-1} \circ r \circ f$. 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. \square

$$\begin{array}{ccc} A & \xrightarrow{h} & B \\ f \downarrow & & \downarrow g \\ C & \xrightarrow{\Phi(h)} & D \end{array}$$

Our next result is a bit more complicated. This proposition says that we can use sets of functions to study power sets.

Proposition 4.5.3. *Let A be a non-empty set. Then there is a bijective map from $\mathcal{F}(A, \{0, 1\})$ to $\mathcal{P}(A)$.*

Scratch Work. We will construct a bijective map $\mathcal{P}(A)$ to $\mathcal{F}(A, \{0, 1\})$. Using Exercise 4.4.12), it will then follow that there is bijective map from $\mathcal{F}(A, \{0, 1\})$ to $\mathcal{P}(A)$. Intuitively, what is the connection 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 map $A \rightarrow \{0, 1\}$? Suppose $S \in \mathcal{P}(A)$, so that $S \subseteq A$. We want to associate with this set S a map $A \rightarrow \{0, 1\}$. To do so, notice that we can divide A into two disjoint pieces, namely S and $A - S$. We then define a map from A to $\{0, 1\}$ by assigning the value of 1 to every point in S , and 0 to every point in $A - S$. For different choices of S , we will obtain different maps $A \rightarrow \{0, 1\}$. $\//\//$

Proof. Let $\Phi: \mathcal{P}(A) \rightarrow \mathcal{F}(A, \{0, 1\})$ be defined as follows. Let $S \in \mathcal{P}(A)$. Hence $S \subseteq A$. Define $\Phi(S)$ to be the function $A \rightarrow \{0, 1\}$ given by

$$[\Phi(S)](x) = \begin{cases} 1, & \text{if } x \in S \\ 0, & \text{if } x \in A - S. \end{cases} \quad (4.5.1)$$

We give two proofs that Φ is bijective, since each is instructive.

(1) We will show that Φ is bijective by showing that it is injective and surjective, starting with the former. Let $S, T \in \mathcal{P}(A)$, and suppose that

$\Phi(S) = \Phi(T)$. We need to show that $S = T$. Let $y \in S$. By Equation 4.5.1 we have $[\Phi(S)](y) = 1$. Since $\Phi(S)$ and $\Phi(T)$ are the same functions $A \rightarrow \{0, 1\}$, we know that $[\Phi(S)](y) = [\Phi(T)](y)$. Hence $[\Phi(T)](y) = 1$. It follows from Equation 4.5.1 that $y \in T$. Hence $S \subseteq T$. A similar argument shows that $T \subseteq S$. Thus $S = T$, and therefore Φ is injective.

We now show that Φ is surjective. Let $f \in \mathcal{F}(A, \{0, 1\})$. Define $S \in \mathcal{P}(A)$ to be $S = f^*(\{1\})$. We will show that $\Phi(S) = f$. Since both $\Phi(S)$ and f are functions $A \rightarrow \{0, 1\}$, it will suffice to show that $[\Phi(S)](x) = f(x)$ for all $x \in A$. We have two cases.

First, let $x \in S$. Then we see that $[\Phi(S)](x) = 1$ by Equation 4.5.1. On the other hand, since $S = f^*(\{1\})$, we deduce immediately that $f(x) = 1$. Thus $[\Phi(S)](x) = f(x)$. Now let $x \in A - S$. By Equation 4.5.1 we see that $[\Phi(S)](x) = 0$. Since $S = f^*(\{1\})$, we deduce that $f(x) = 0$. Thus $[\Phi(S)](x) = f(x)$. Putting these two cases together, we see that $[\Phi(S)](x) = f(x)$ for all $x \in A$. Hence $\Phi(S) = f$. It follows that Φ is surjective.

(2) We will show that Φ is bijective by producing an inverse for it. Let $\Psi: \mathcal{F}(A, \{0, 1\}) \rightarrow \mathcal{P}(A)$ be defined by $\Psi(f) = f^*(\{1\})$ for all $f \in \mathcal{F}(A, \{0, 1\})$. We will show that Ψ is an inverse for Φ by showing that

$$\Psi \circ \Phi = 1_{\mathcal{P}(A)} \quad \text{and} \quad \Phi \circ \Psi = 1_{\mathcal{F}(A, \{0, 1\})}.$$

We start by showing that $\Psi \circ \Phi = 1_{\mathcal{P}(A)}$. Let $S \in \mathcal{P}(A)$. Then

$$(\Psi \circ \Phi)(S) = \Psi(\Phi(S)) = [\Phi(S)]^*(\{1\}).$$

Using Equation 4.5.1 we see that $[\Phi(S)]^*(\{1\}) = S$. Hence $(\Psi \circ \Phi)(S) = S$. It follows that $\Psi \circ \Phi = 1_{\mathcal{P}(A)}$.

We now show that $\Phi \circ \Psi = 1_{\mathcal{F}(A, \{0, 1\})}$. Let $f \in \mathcal{F}(A, \{0, 1\})$. Our goal is to show that $(\Phi \circ \Psi)(f) = f$. Since both $(\Phi \circ \Psi)(f)$ and f are functions $A \rightarrow \{0, 1\}$, it will suffice to show that $[(\Phi \circ \Psi)(f)](x) = f(x)$ for all $x \in A$. We observe that

$$(\Phi \circ \Psi)(f) = \Phi(\Psi(f)) = \Phi(f^*(\{1\})).$$

It will thus suffice to show that $[\Phi(f^*(\{1\}))](x) = f(x)$ for all $x \in A$. We have two cases.

First, let $x \in f^*(\{1\})$. Then we see that $[\Phi(f^*(\{1\}))](x) = 1$ by Equation 4.5.1. On the other hand, the fact that $x \in f^*(\{1\})$ immediately implies that $f(x) = 1$. Thus $[\Phi(f^*(\{1\}))](x) = f(x)$. Now let $x \in A - f^*(\{1\})$. By Equation 4.5.1 we see that $[\Phi(f^*(\{1\}))](x) = 0$. Since f is a map A

$\rightarrow \{0, 1\}$, we can deduce from $x \in A - f^*(\{1\})$ that $x \in f^*(\{0\})$. Thus $f(x) = 0$. Therefore $[\Phi(f^*(\{1\}))](x) = f(x)$.

Putting these two cases together, we see that $[\Phi(f^*(\{1\}))](x) = f(x)$ for all $x \in A$, and the proof is complete. \square

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.

Definition. Let A and B be sets. The set $\mathcal{I}(A, B)$ is defined to be the set of all injective functions $f: A \rightarrow B$. The set $\mathcal{B}(A, B)$ is defined to be the set of all bijective functions $f: A \rightarrow B$. Δ

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 have $\mathcal{B}(A, B) \subseteq \mathcal{I}(A, B) \subseteq \mathcal{F}(A, B)$. 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 and infinite sets in Section 6.1). Similarly, the set $\mathcal{I}(A, B)$ will be empty whenever A is “larger” than B (same comment as in the previous sentence).

Example 4.5.4.

(1) Continuing Example 4.5.1 (1), it is seen that $\mathcal{B}(A, B) = \mathcal{I}(A, B) = \{g, h\}$.

(2) Let $A = \{1, 2\}$ and $C = \{x, y, z\}$. Then $\mathcal{I}(A, C) = \{p, q, r, s, t, u\}$, where $p, q, r, s, t, u: A \rightarrow B$ are the maps such that $p(1) = x$ and $p(2) = y$, such that $q(1) = y$ and $q(2) = x$, such that $r(1) = x$ and $r(2) = z$, such that $s(1) = z$ and $s(2) = x$, such that $t(1) = y$ and $t(2) = z$, and such that $u(1) = z$ and $u(2) = y$. Also, we see that $\mathcal{B}(A, C) = \emptyset$. \diamond

More details about sets of the form $\mathcal{I}(A, B)$ and $\mathcal{B}(A, B)$ will be given in Section 7.7.

Finally, we can use sets of functions to resolve an issue that was left outstanding from 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 indexed families of sets, rather than just two sets at a time. We did not state how to form the product of an indexed family of sets in Section 3.4, 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 “sec-

ond" one. Functions are the tool we need to pick things out of sets more rigorously. 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 map $f: \{1, 2\} \rightarrow A \cup B$ 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

$$\{f \in \mathcal{F}(\{1, 2\}, A \cup B) \mid f(1) \in A \text{ and } f(2) \in B\}.$$

The above reformulation of the definition of $A \times B$ can be generalized to arbitrary indexed families of sets.

Definition. 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 all the sets in the family of sets is 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 , then we denote $\prod_{i \in I} A_i$ by A^I . Δ

It is not hard to verify that if I is a non-empty set, and if A is a set, then $A^I = \mathcal{F}(I, A)$. Thus, for example, we have $\mathbb{R}^{\mathbb{N}} = \mathcal{F}(\mathbb{N}, \mathbb{R})$. Given our discussion in Example 4.5.1 (3), we therefore see that $\mathbb{R}^{\mathbb{N}}$ is the set of sequences of real numbers.

Exercises

4.5.1. Let $X = \{l, m, n\}$ and $Y = \{\alpha, \beta\}$. Describe all the elements of $\mathcal{F}(X, Y)$.

4.5.2. Let A be a non-empty set, and let x be an element (not necessarily in A).

- (1) Show that there is a bijective map from $\mathcal{F}(A, \{x\})$ to $\{x\}$.
- (2) Show that there is a bijective map from $\mathcal{F}(\{x\}, A)$ to A .

4.5.3. Let A, B be non-empty sets. Let $\Phi: \mathcal{F}(A, B) \rightarrow \mathcal{F}(\mathcal{P}(A), \mathcal{P}(B))$ be the map defined by $\Phi(f) = f_*$ for all $f \in \mathcal{F}(A, B)$, where $f_*: \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ is defined in Section 4.2. Is Φ bijective, injective, surjective or neither?

4.5.4. Let A, B, C be sets such that $A \subseteq B$.

- (1) Show that $\mathcal{F}(C, A) \subseteq \mathcal{F}(C, B)$.
- (2) Show that there is an injective map $\mathcal{F}(A, C) \rightarrow \mathcal{F}(B, C)$.

4.5.5. Let A, B, C be sets. Show that there is a bijective map from $\mathcal{F}(C, A \times B)$ to $\mathcal{F}(C, A) \times \mathcal{F}(C, B)$.

4.5.6. Let A, B, C be sets. Show that there is a bijective map from $\mathcal{F}(A, \mathcal{F}(B, C))$ to $\mathcal{F}(B, \mathcal{F}(A, C))$.

4.5.7. Let $g: A \rightarrow A$ be a bijective map.

(1) Define a map $\Omega_g: \mathcal{F}(A, A) \rightarrow \mathcal{F}(A, A)$ by $\Omega_g(f) = g \circ f$ for all $f \in \mathcal{F}(A, A)$. Show that Ω_g is bijective.

(2) Define a map $\Lambda_g: \mathcal{F}(A, A) \rightarrow \mathcal{F}(A, A)$ by $\Lambda_g(f) = g \circ f \circ g^{-1}$ for all $f \in \mathcal{F}(A, A)$. Show that Λ_g is bijective. Also, show that $\Lambda_g(h \circ k) = \Lambda_g(h) \circ \Lambda_g(k)$ for all $h, k \in \mathcal{F}(A, A)$.

4.5.8. [Used in Section 7.7.] Let A, B, C and D be sets. Suppose that there are bijective maps $f: A \rightarrow C$ and $g: B \rightarrow D$.

(1) Show that there is a bijective map from $\mathcal{I}(A, B)$ to $\mathcal{I}(C, D)$.

(2) Show that there is a bijective map from $\mathcal{B}(A, B)$ to $\mathcal{B}(C, D)$.

4.5.9. [Used in Section 7.7.] Let A and B be sets. Let $a \in A$ and $b \in B$.

(1) Show that there is a bijective map from $\{f \in \mathcal{F}(A, B) \mid f(a) = b\}$ to $\mathcal{F}(A - \{a\}, B)$.

(2) Show that there is a bijective map from $\{f \in \mathcal{I}(A, B) \mid f(a) = b\}$ to $\mathcal{I}(A - \{a\}, B - \{b\})$.

(3) Show that there is a bijective map from $\{f \in \mathcal{B}(A, B) \mid f(a) = b\}$ to $\mathcal{B}(A - \{a\}, B - \{b\})$.

4.5.10. Let A a set. Define a map $\Phi: \mathcal{B}(A, A) \rightarrow \mathcal{B}(A, A)$ by $\Phi(f) = f^{-1}$ for all $f \in \mathcal{B}(A)$. Show that Φ is bijective.

4.5.11. Let A a set. Suppose we have a map $\Gamma: \mathbb{Z} \rightarrow \mathcal{B}(A, A)$ that satisfies the following two properties: (1) $\Gamma(0) = 1_A$; (2) $\Gamma(a + b) = \Gamma(a) \circ \Gamma(b)$ for all $a, b \in \mathbb{Z}$. We call such a map Γ a \mathbb{Z} -action on A . For convenience, we will write $a_* = \Gamma(a)$. Thus $0_* = 1_A$ and $(a+b)_* = a_* \circ b_*$ for all $a, b \in \mathbb{Z}$.

Let $a, b, c \in \mathbb{Z}$.

(1) Let $a \in \mathbb{Z}$. Show that $(-a)_* = (a_*)^{-1}$.

(2) Suppose that $e_* = 1_A$ for some $e \in \mathbb{Z}$. Show that $(ne)_* = 1_A$ 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. For example, one relation between people is that of having the same color hair, while another is that of being the same height. 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 \leq between real numbers. We have already seen some relations in previous chapters, without having used the term “relation.” For example, we can define a relation on the set of integers by saying that two integers a and b are related iff $a|b$. Relations (and especially equivalence relations, as discussed in Section 5.3), are used in crucial ways in abstract algebra, number theory, topology, geometry, and other areas of modern mathematics.

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 distinguish 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 once and for all list all pairs of people (X, Y) , where X is a parent of Y . We could then simply check any two given people against this list to verify whether they are a parent-child pair.

Similar to our formal definition of functions in Sections 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. Let A and B be sets. A **relation** R from A to B is a subset $R \subseteq A \times B$. If $a \in A$ and $b \in B$, we write aRb if $(a, b) \in R$, and $a \not R b$ if $(a, b) \notin R$. A relation from A to A is called a **relation on A** . Δ

Example 5.1.1.

(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 S defined by $S = \{(1, y), (1, z), (2, y)\}$. Then $1Sy$, and $1Sz$, and $2Sy$.

(2) Let P be the set of all people, and let R be the relation on P defined by having person x related to person y iff x and y have at least one parent in common.

(3) The symbols $<$ and \leq 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 T from P to B by having person x related to book b iff x has read b .

(5) Let A be a set. Define a relation on $\mathcal{P}(A)$ by saying that $P, Q \in \mathcal{P}(A)$ are related iff $P \subseteq Q$.

(6) A function $f: A \rightarrow B$ is a subset of $A \times B$ satisfying a certain condition. Hence functions $A \rightarrow B$ are also relations from A to B . The concept of a relation is thus more general than the concept of a function. In theory, 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. Functions thus deserve their own treatment independent of the study of relations. \diamond

Just as a person might wish to find out who all his/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. Let A and B be non-empty sets, and let R be a relation from A to B . For each $x \in A$, define the **relation class** of x with respect to R , denoted $R[x]$, to be the set

$$R[x] = \{y \in B \mid xRy\}.$$

If the relation R is understood from the context, we will often write $[x]$ instead of $R[x]$. Δ

Example 5.1.2. We continue Example 5.1.1 parts (1) – (3).

(1) For this relation we have $[1] = \{y, z\}$, we have $[2] = \{y\}$, and we have $[3] = \emptyset$.

(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 $[x] = \{x\}$, since 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 have no other siblings or half-siblings, then $[a] = \{a, b, c\}$, and $[b] = \{a, b\}$, and $[c] = \{a, c\}$.

(3) For the relation $<$, we have $[x] = (x, \infty)$ for all $x \in \mathbb{R}$, and for the relation \leq , we have $[x] = [x, \infty)$ for all $x \in \mathbb{R}$. \diamond

In Example 5.1.2 we see various possible behaviors of relation classes. The relation class of an element may be empty, such as $[3]$ in part (1) of the example. The relation class $[x]$ need not contain x , for example the relation classes with respect to $<$ in part (3) of the example. Different elements may have overlapping relation classes, such as $[b]$ and $[c]$ in part (2) of the example. If we think of the collection of all relation classes determined by a given relation, then some relation classes might arise from more than one element of the set, 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 nice 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. Let A be a non-empty set and let R be a relation on A .

- (1) The relation R is **reflexive** if xRx for all $x \in A$.
- (2) The relation R is **symmetric** if xRy implies yRx for all $x, y \in A$.
- (3) The relation R is **transitive** if xRy and yRz imply xRz for all $x, y, z \in A$. Δ

As seen in the following example, a relation can have any combination of the above three properties. In most of the cases we leave it to the reader to verify that the given relation has the stated properties.

Example 5.1.3.

- (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. To see that transitivity does not hold, suppose persons A , B and C 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, since any person is within 0 lbs. of her own weight, and symmetric, since if A and B weigh within 5 lbs. of each other, then B and A 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 $P = \{(2, 2), (3, 3), (2, 3), (3, 2)\}$. Then P is symmetric and transitive, but not reflexive.
- (5) Let $B = \{x, y, z\}$, and let $T = \{(x, x), (y, y), (z, z), (x, y), (y, z)\}$. Then T is reflexive, but neither symmetric nor transitive. The relation is reflexive, since (x, x) , (y, y) and (z, z) are all in T , and thus xTx , yTy and zTz . The relation is not symmetric, because xTy , but yTx . The relation is not transitive, because xTy and yTz , but xTz .
- (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 symmetric nor reflexive. Let $x, y, z \in \mathbb{R}$. If $x < y$ and $y < z$, then $x < z$, and so the relation is transitive. If $x < y$, it is never the case that $y < x$, so the relation is not symmetric. It is never the case that $x < x$, so the relation is not reflexive.
- (8) The relation of one person being the daughter of another person is neither reflexive, symmetric nor transitive. \diamond

There are standard proof strategies for proving that a relation is reflexive, symmetric or transitive. Suppose we have a non-empty set A and a relation R on A .

If we wish to prove that R is reflexive, we need to show that for every $x \in A$, the condition xRx is true. Hence, a proof of the reflexivity of R would typically look like “Let $x \in A$ (argumentation) . . . Then xRx . Hence R is reflexive.”

If we wish to prove that R is symmetric, we need to show that xRy implies yRx for every $x, y \in A$. Hence, a proof of the symmetry of R would typically look like “Let $x, y \in A$. Suppose that xRy (argumentation) . . . Then yRx . Hence R is symmetric.”

If we wish to prove that R is transitive, we need to show that xRy and yRz together imply xRz for every $x, y, z \in A$. Hence, a proof of the transitivity of R would typically look like “Let $x, y, z \in A$. Suppose that xRy and yRz (argumentation) . . . Then xRz . Hence R is transitive.”

We will see proofs using these strategies later on.

Exercises

5.1.1. For each of the following relations on \mathbb{Z} , find [3] and [-3] and [6].

- (1) Let R be the relation given by aRb iff $a = |b|$, for all $a, b \in \mathbb{Z}$.
- (2) Let S be the relation given by aSb iff $a|b$, for all $a, b \in \mathbb{Z}$.
- (3) Let T be the relation given by aTb iff $b|a$, for all $a, b \in \mathbb{Z}$.
- (4) Let Q be the relation given by aQb iff $a + b = 7$, for all $a, b \in \mathbb{Z}$.

5.1.2. For each of the following relations on \mathbb{R}^2 , give a geometric description of $[(0, 0)]$ and $[(3, 4)]$.

- (1) Let S be the relation given by $(x, y)S(z, w)$ iff $y = 3w$, for all $(x, y), (z, w) \in \mathbb{R}^2$.
- (2) Let T be the relation given by $(x, y)T(z, w)$ iff $x^2 + 3y^2 = 7z^2 + w^2$, for all $(x, y), (z, w) \in \mathbb{R}^2$.
- (3) Let Z be the relation given by $(x, y)Z(z, w)$ iff $x = z$ or $y = w$, for all $(x, y), (z, w) \in \mathbb{R}^2$.

5.1.3. Let $A = \{1, 2, 3\}$. Is each of the following relations on A reflexive, symmetric and/or transitive?

- (1) $M = \{(3, 3), (2, 2), (1, 2), (2, 1)\}$.
- (2) $N = \{(1, 1), (2, 2), (3, 3), (1, 2)\}$.
- (3) $O = \{(1, 1), (2, 2), (1, 2)\}$.

- (4) $P = \{(1, 1), (2, 2), (3, 3)\}$.
 (5) $Q = \{(1, 2), (2, 1), (1, 3), (3, 1), (1, 1)\}$.
 (6) $R = \{(1, 2), (2, 3), (3, 1)\}$.
 (7) $T = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3), (1, 3)\}$.

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 xSy iff $y = |x|$, for all $x, y \in \mathbb{R}$.
 (2) Let P be the set of all people, and let R be the relation on P given by xRy iff x and y were not born in the same city, for all people x and y .
 (3) Let T be the set of all triangles in the plane, and let G be the relation on T given by sGt iff 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 given by xMy iff x and y have the same mother, for all people x and y .
 (5) Let P be the set of all people, and let N be the relation on P given by xNy iff x and y have the same color hair or the same color eyes, for all people x and y .
 (6) Let D be the relation on \mathbb{N} defined by aDb iff $a|b$, for all $a, b \in \mathbb{N}$.
 (7) Let T be the relation on $\mathbb{Z} \times \mathbb{Z}$ defined by $(x, y)T(z, w)$ iff (x, y) and (z, w) are both on a line in \mathbb{R}^2 with slope an integer, for all $(x, y), (z, w) \in \mathbb{Z} \times \mathbb{Z}$.

5.1.5. Let A be a set, and let R be a relation on A . Define the relation R' on A by $R' = (A \times A) - R$.

- (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?

5.1.6. Let A be a set, and let R be a symmetric and transitive relation on A . Find the flaw in the following alleged proof that this relation is necessarily reflexive (which is false by Example 5.1.3 (4)): “Let $x \in A$. Choose $y \in A$ such that xRy . By symmetry we have yRx , and then by transitivity we have xRx . Hence R is reflexive.”

5.1.7. Let A be a set. Is the relation on $\mathcal{P}(A)$ defined in Example 5.1.1 (5) reflexive, symmetric and/or transitive?

5.1.8. Let A be a set. Let I be a non-empty set and let $\{R_i\}_{i \in I}$ be a family of relations on A indexed by I .

- (1) Show that if each R_i is respectively a reflexive, symmetric or transitive relation, then $\bigcap_{i \in I} R_i$ is respectively a reflexive, symmetric or transitive relation on A .
- (2) If each R_i is respectively a reflexive, symmetric or transitive relation, is $\bigcup_{i \in I} R_i$ respectively a reflexive, symmetric or transitive relation on A ? Give proofs or counterexamples.

5.1.9. Let A be a set, and let R be a relation on A . Define respectively the minimal reflexive, symmetric or transitive relation on A containing R to be the intersection respectively of all reflexive, symmetric or transitive relations on A that contain R . Show that the minimal reflexive, symmetric or transitive relation on A containing R satisfies the following two properties:

- (1) It is respectively a reflexive, symmetric or transitive relation on A that contains R ;
- (2) it is minimal in the sense that if T is respectively any reflexive, symmetric or transitive relation on A that contains R , then it contains the minimal reflexive, symmetric or transitive relation on A containing R .

5.1.10. Using the terminology of Exercise 5.1.9, find the minimal reflexive, symmetric and transitive relations respectively containing each of the relations given below.

- (1) Let $B = \{y, z\}$, and let R be the relation on B given by the set of pairs $R = \{(y, y), (y, z)\}$.
- (2) Let $D = \{a, b, c\}$, and let Z be the relation on D given by $Z = \{(a, b), (b, c)\}$.
- (3) Let W be the set of all women, and let M be the relation on W given by xMy iff x is the mother of y , for all women x and y .
- (4) The relation $<$ on \mathbb{R} .
- (5) Let L be the set of all lines in the plane, and let W be the relation on L given by $\alpha W \beta$ iff α and β are not parallel, for all $\alpha, \beta \in L$.

5.1.11. Let A be a set, and let R be a relation on A .

- (1) Suppose R is reflexive. Show that $\bigcup_{x \in A} [x] = A$.
- (2) Suppose R is symmetric. Let $x, y \in A$. Show that $x \in [y]$ iff $y \in [x]$.
- (3) Suppose R is transitive. Let $x, y \in A$. Show that if xRy , then $[y] \subseteq [x]$.

5.1.12. Let A, B be sets, and let R be a relation on A . Let $f: A \rightarrow B$ be a map. We say that f respects the relation R if xRy implies $f(x) = f(y)$, for all $x, y \in A$. Which of the following maps respects the given relation?

- (1) Let R be the relation on \mathbb{R} given by xRy iff $|x| = |y|$, for all $x, y \in \mathbb{R}$; let $f: \mathbb{R} \rightarrow \mathbb{R}$ be given by $f(x) = x^6$ for all $x \in \mathbb{R}$.
- (2) Let W be the relation on \mathbb{R} given by xWy iff $x - y = \pi k/2$ for some $k \in \mathbb{Z}$, for all $x, y \in \mathbb{R}$; let $g: \mathbb{R} \rightarrow \mathbb{R}$ be given by $g(x) = \cos x$ for all $x \in \mathbb{R}$.
- (3) Let T be the relation on \mathbb{R} given by xTy iff $|x - y| < 1$, for all $x, y \in \mathbb{R}$; let $h: \mathbb{R} \rightarrow \mathbb{R}$ be given by $h(x) = \lfloor x \rfloor$ for all $x \in \mathbb{R}$, where $\lfloor x \rfloor$ is defined in Exercise 2.4.11.
- (4) Let M be the relation on \mathbb{R}^2 given by $(x, y)M(z, w)$ iff $x + y = z + w$, for all $(x, y), (z, w) \in \mathbb{R}^2$; let $k: \mathbb{R}^2 \rightarrow \mathbb{R}$ be given by $k((x, y)) = 3x^2 + 6xy + 3y^2$ for all $(x, y) \in \mathbb{R}^2$.

5.1.13. Let A, B be sets, let R be a relation on A . Suppose that there is an injective map $f: A \rightarrow B$ that respects the relation R , as defined in Exercise 5.1.12. What can you say about the relation R ?

5.1.14. Let A, B be sets, and let R, S be relations on A and B respectively. Let $f: A \rightarrow B$ be a map. We say that f is **relation preserving** if xRy iff $f(x)Sf(y)$, for all $x, y \in A$.

- (1) Suppose that $f: A \rightarrow B$ is a bijective relation preserving map. Show that f^{-1} is relation preserving.
- (2) Suppose that $f: A \rightarrow B$ is a surjective relation preserving map. Show that R is respectively reflexive, symmetric or transitive iff S is respectively reflexive, symmetric or transitive.

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 valuable as a tool in various parts of mathematics and its applications, for example in number theory, cryptography and calendars. See [Ros93a, Chapters 3–4] for further discussion of congruences and their applications, and see [Kob87] for a treatment of congruences and cryptography. The method is based on the idea of “clock arithmetic” (if you have not seen this, it will be sufficient that you 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 the U.S. military).

Suppose 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 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 as many 12's as possible from 41. 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 add numbers that took us outside of the 1 to 12 range. To resolve the problem, we took any number that was outside the desired range, and reduced it by 12's until we were back where we wanted to be. For example, we reduced 41 to 5 by subtracting 3 times 12. We are considering 41 and 5 as essentially equivalent from the point of view of clocks. Two integers are equivalent in this approach if they differ by some integer 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 we can repeat the whole procedure with any positive integer replacing 12. The following definition makes this notion precise.

Definition. Let $n \in \mathbb{N}$. If $a, b \in \mathbb{Z}$, we say that a is **congruent to b modulo n** , denoted $a \equiv b \pmod{n}$, if $a - b = kn$ for some $k \in \mathbb{Z}$. Δ

Example 5.2.1. By the above definition, we have $19 \equiv -5 \pmod{4}$, because $19 - (-5) = 24 = 6 \cdot 4$, we have $7 \equiv 7 \pmod{3}$, because $7 - 7 = 0 = 0 \cdot 3$, and we have $13 \not\equiv 2 \pmod{9}$, because $13 - 2 = 11$, which is not a multiple of 9. \diamond

For each fixed $n \in \mathbb{N}$, 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 5.2.2. Let $n \in \mathbb{N}$ and let $a, b, c \in \mathbb{Z}$. Then

- (i) $a \equiv a \pmod{n}$;
- (ii) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
- (iii) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof. (i). Observe that $a - a = 0 \cdot n$.

(ii). Suppose that $a \equiv b \pmod{n}$. Then $a - b = kn$ for some $k \in \mathbb{Z}$. Hence $b - a = (-k)n$. Since $-k \in \mathbb{Z}$, it follows that $b \equiv a \pmod{n}$.

(iii). 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 $a - c = (k + j)n$. Since $k + j \in \mathbb{Z}$, it follows that $a \equiv c \pmod{n}$. \square

For each given $n \in \mathbb{N}$, we can form the relation classes with respect to congruence modulo n . Let us examine the case $n = 5$, where we list a few of the relation classes:

$$\begin{aligned} & \vdots \\ [0] &= \{\dots, -10, -5, 0, 5, 10, \dots\} \\ [1] &= \{\dots, -9, -4, 1, 6, 11, \dots\} \\ [2] &= \{\dots, -8, -3, 2, 7, 12, \dots\} \\ [3] &= \{\dots, -7, -2, 3, 8, 13, \dots\} \\ [4] &= \{\dots, -6, -1, 4, 9, 14, \dots\} \\ [5] &= \{\dots, -5, 0, 5, 10, 15, \dots\}. \\ & \vdots \end{aligned}$$

We see that the relation classes repeat themselves every five integers. Hence

$$\begin{aligned} [0] &= [5] = [10] = \dots \\ [1] &= [6] = [11] = \dots \\ [2] &= [7] = [12] = \dots \\ [3] &= [8] = [13] = \dots \\ [4] &= [9] = [14] = \dots. \end{aligned}$$

Thus, 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 proposition. For the proof of this proposition we need an important fact about the integers known as the Division Algorithm, which is actually not an algorithm, but a theorem that states that if $a, b \in \mathbb{Z}$, and $b \neq 0$, then there are unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$. See Section 8.4 for more details. (Even though the Division Algorithm is proved later, we will not use anything from the present section in our proof of the Division Algorithm, so there is no circular reasoning here.)

Theorem 5.2.3. Let $n \in \mathbb{N}$.

- (i) Let $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{n}$, then $[a] = [b]$. If $a \not\equiv b \pmod{n}$, then $[a] \cap [b] = \emptyset$.
- (ii) $[0] \cup [1] \cup \dots \cup [n-1] = \mathbb{Z}$.

Proof. (i). Suppose $a \equiv b \pmod{n}$. Let $x \in [a]$. Then by the definition of relation classes we know that $a \equiv x \pmod{n}$. By Lemma 5.2.2 (ii) we know that $b \equiv a \pmod{n}$, and hence by Lemma 5.2.2 (iii) we have $b \equiv x \pmod{n}$. Thus $x \in [b]$. It follows that $[a] \subseteq [b]$. A similar argument shows that $[b] \subseteq [a]$. Hence $[a] = [b]$.

Now assume that $a \not\equiv b \pmod{n}$. Suppose that $[a] \cap [b] \neq \emptyset$; we will arrive at a contradiction. By hypothesis there exists some $y \in [a] \cap [b]$. Thus $y \in [a]$ and $y \in [b]$, so that $a \equiv y \pmod{n}$ and $b \equiv y \pmod{n}$. By Lemma 5.2.2 (ii) we have $y \equiv b \pmod{n}$, and by Lemma 5.2.2 (iii) we then have $a \equiv b \pmod{n}$, a contradiction. Thus $[a] \cap [b] = \emptyset$.

(ii). By definition $[a] \subseteq \mathbb{Z}$ for all $a \in \mathbb{Z}$, and thus $[0] \cup \dots \cup [n-1] \subseteq \mathbb{Z}$. Now let $x \in \mathbb{Z}$. By the Division Algorithm (described above), we know that there are unique $q, r \in \mathbb{Z}$ such that $x = nq + r$ and $0 \leq r < n$. Hence $r - x = (-q)n$, and thus $r \equiv x \pmod{n}$. Hence $x \in [r]$. Since $r \in \{0, \dots, n-1\}$, it follows that $x \in [0] \cup \dots \cup [n-1]$. Hence $\mathbb{Z} \subseteq [0] \cup \dots \cup [n-1]$, and thus $[0] \cup \dots \cup [n-1] = \mathbb{Z}$. \square

The above proposition shows that relation classes for congruence modulo n are much better behaved than for arbitrary relations (as was seen in Example 5.1.2). We are now ready for the following definition.

Definition. Let $n \in \mathbb{N}$. The set of integers modulo n is the set $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$, where the relation classes are for congruence modulo n . Δ

The set \mathbb{Z}_n is also denoted $\mathbb{Z}/n\mathbb{Z}$ in some texts (for reasons that will become apparent if you learn about group theory).

Example 5.2.4. We have $\mathbb{Z}_3 = \{[0], [1], [2]\}$. Observe that this set has 3 elements. Each of these elements is itself a set, namely a relation class, but here we are viewing it as a single element in another set. These relation classes could each be described differently. For example, we also have $\mathbb{Z}_3 = \{[6], [4], [-1]\}$. \diamond

For any $n \in \mathbb{N}$, the set \mathbb{Z}_n has n elements. The following definition allows us to form analogs of addition and multiplication for each set \mathbb{Z}_n .

Definition. Let $n \in \mathbb{N}$. Define operations $+$ and \cdot on \mathbb{Z}_n by letting $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$ for all $[a], [b] \in \mathbb{Z}_n$. Δ

As reasonable as the above definition seems, there is a potential problem. Let $n \in \mathbb{N}$, and let $[a], [b], [c], [d] \in \mathbb{Z}_n$. Suppose $[a] = [c]$ and $[b] = [d]$. Do $[a + b] = [c + d]$ and $[ab] = [cd]$ necessarily hold? Otherwise, 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 operations on \mathbb{Z}_n , since $[a] + [b]$ 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 we define something for relation classes (or particularly equivalence classes, to be defined in the next section) by using representative elements of the classes. Neglecting such verification is a common error.

Fortunately, everything works as desired in the present case. We start with the following lemma.

Lemma 5.2.5. *Let $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$. Suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then $a + b \equiv c + d \pmod{n}$ and $ab \equiv cd \pmod{n}$.*

Proof. By hypothesis there exist $k, j \in \mathbb{Z}$ such that $a - c = kn$ and $b - d = jn$. Thus $a = c + kn$ and $b = d + jn$. Then

$$\begin{aligned} a + b &= (c + kn) + (d + jn) = c + d + (k + j)n, \\ ab &= (c + kn)(d + jn) = cd + (cj + dk + kjn)n. \end{aligned}$$

The desired result now follows. \square

From the above lemma, together with Theorem 5.2.3 (i), we can deduce the following corollary, which we state without proof. This result tells us that $+$ and \cdot are indeed well-defined for \mathbb{Z}_n .

Corollary 5.2.6. *Let $n \in \mathbb{N}$, and let $[a], [b], [c], [d] \in \mathbb{Z}_n$. Suppose $[a] = [c]$ and $[b] = [d]$. Then $[a + b] = [c + d]$ and $[ab] = [cd]$.*

It is important to note that the operations $+$ and \cdot are different in each set \mathbb{Z}_n . For example, in \mathbb{Z}_7 we have $[6] + [4] = [10] = [3]$, whereas in \mathbb{Z}_9 we have $[6] + [4] = [10] = [1]$.

One nice way of working with these operations 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]	\cdot	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[5]	[0]	[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[2]	[3]	[4]	[5]	[0]	[1]	[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[3]	[4]	[5]	[0]	[1]	[2]	[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[4]	[5]	[0]	[1]	[2]	[3]	[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[5]	[0]	[1]	[2]	[3]	[4]	[5]	[0]	[5]	[4]	[3]	[2]	[1]

The table for $+$ has a very nice pattern following the upward sloping diagonals. 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. Not all tables for \cdot for different sets \mathbb{Z}_n 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 [Fra94, Section 5.3] for more details.

A related question is whether we can solve equations of the form $[a] \cdot x = [b]$ in any \mathbb{Z}_n . An 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 $x = [9]$, 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} . Moreover, the equation $[3] \cdot x = [0]$ has three solutions in \mathbb{Z}_6 , namely $x = [0], [2], [4]$, as can be seen in the operation table for \cdot for \mathbb{Z}_6 . Note that in \mathbb{Z}_6 we can have two non-zero elements whose product is [0], in contrast to the situation for multiplication of real numbers. See [Fra94, Section 5.3] for further discussion of this type of equation in \mathbb{Z}_n .

One final note concerning the sets \mathbb{Z}_n . For any given $n \in \mathbb{N}$, we can define a map $\gamma : \mathbb{Z} \rightarrow \mathbb{Z}_n$ by letting $\gamma(a) = [a]$ for all $a \in \mathbb{Z}$. This map is called the **canonical map**, and is a special case of a more general type of canonical map defined in Exercise 5.3.17. Some important properties of the canonical map $\mathbb{Z} \rightarrow \mathbb{Z}_n$ are given in Exercise 5.2.10. These properties are discussed in more detail in Section 7.3.

Exercises

5.2.1. Which of the following are true and which are false?

- (1) $13 \equiv 5 \pmod{2}$. (4) $3 \equiv 28 \pmod{5}$.
 (2) $21 \equiv 7 \pmod{5}$. (5) $23 \equiv 23 \pmod{7}$.
 (3) $7 \equiv 0 \pmod{2}$.

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 . (4) $x \cdot [6] = [2]$ in \mathbb{Z}_{10} .
 (2) $[2] \cdot x = [7]$ in \mathbb{Z}_{11} . (5) $[3] \cdot x + [4] = [1]$ in \mathbb{Z}_5 .
 (3) $x \cdot [6] = [4]$ in \mathbb{Z}_{15} .

5.2.3. Find $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ such that $a^2 \equiv b^2 \pmod{n}$ but $a \not\equiv b \pmod{n}$.

5.2.4. Let $a, b \in \mathbb{Z}$, and let $n \in \mathbb{N}$. Suppose that $a \equiv b \pmod{n}$. Let $q \in \mathbb{N}$ be such that $q|n$. Show that $a \equiv b \pmod{q}$.

5.2.5. Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Suppose that $a \equiv b \pmod{n}$. Show that $n|a$ iff $n|b$.

5.2.6. Prove or give a counterexample for each of the following proposed cancelation laws.

- (1) Let $a, b, c \in \mathbb{Z}$, and let $n \in \mathbb{N}$. Then $a + c \equiv b + c \pmod{n}$ implies $a \equiv b \pmod{n}$.
 (2) Let $a, b, c \in \mathbb{Z}$, and let $n \in \mathbb{N}$. Then $ac \equiv bc \pmod{n}$ implies $a \equiv b \pmod{n}$.

5.2.7. Let $n \in \mathbb{N}$. Suppose that $(n - 1)! \equiv -1 \pmod{n}$. Prove that n is a prime number. (Recall that for any positive $m \in \mathbb{N}$, the notation $m!$ means $m(m - 1)(m - 2) \cdots 3 \cdot 2 \cdot 1$.) 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 [Ros93a, Section 5.1] for details.

5.2.8. Let $n \in \mathbb{Z}$. Show that $n^3 \equiv n \pmod{6}$.

5.2.9. Let $n \in \mathbb{Z}$. Show that precisely one of the following is true: $n^2 \equiv 0 \pmod{16}$ or $n^2 \equiv 1 \pmod{8}$ or $n^2 \equiv 4 \pmod{8}$.

5.2.10. Let $n \in \mathbb{N}$, and let $\gamma: \mathbb{Z} \rightarrow \mathbb{Z}_n$ be the canonical map defined at the end of this section. Let $a, b \in \mathbb{Z}$. Show that $\gamma(a + b) = \gamma(a) + \gamma(b)$ and that $\gamma(ab) = \gamma(a) \cdot \gamma(b)$.

5.2.11. What is the relation between a positive integer and the sum of its digits? We now have the tools to answer this question. Let x be a positive integer. We could then write x in decimal notation as $a_m a_{m-1} \cdots a_2 a_1$, where a_i is an integer such that $0 \leq a_i \leq 9$ for all $i \in \{1, \dots, m\}$. That is,

we have $x = \sum_{i=1}^m a_i 10^i$. 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 5.2.5 can be extended to sums and products of any finite number of integers.

5.2.12. This exercise continues Exercise 5.2.11. 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 $\Sigma(\Sigma(\dots \Sigma(a) \dots))$, with Σ repeated m times. Let $\Sigma^0(a) = a$. Show that there is some $r \in \mathbb{Z}^{mn}$ 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 (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 $\bar{\Sigma}(a)$ is the result of repeatedly adding the digits of a number until a single digit remains. (This process is used in *gematria*, a method employed in Jewish mysticism, as well as in similar constructions used in Greek and Arab traditions; see [Ifri85, Chapter 21].) 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) Show that $\bar{\Sigma}(a + b) = \bar{\Sigma}(\bar{\Sigma}(a) + \bar{\Sigma}(b))$ and $\bar{\Sigma}(ab) = \bar{\Sigma}(\bar{\Sigma}(a) \cdot \bar{\Sigma}(b))$ always hold.

5.3 Equivalence Relations

In Lemma 5.2.2 we saw that congruence modulo n satisfied the three properties of reflexivity, symmetry and transitivity. It turns out that many important relations found throughout mathematics satisfy these properties.

Definition. 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. Δ

Example 5.3.1. Some examples of equivalence relations are the following: 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

Since we can form relation classes for arbitrary relations, we can in particular form them for equivalence relations. Since relation classes for equivalence relations will turn out to behave especially nicely, and are of great importance, we give them a special name.

Definition. 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**. The **quotient set** of A and \sim is the set of all equivalence classes of A with respect to \sim , that is, the set $\{[x] \mid x \in A\}$. The quotient set of A and \sim is denoted A/\sim . Δ

Example 5.3.2. Let P be the set of all people, and let \sim be the relation on P given by $x \sim y$ iff 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. The quotient set P/\sim has elements each of which is itself a set, one such set consisting of all one-year olds, another consisting of all two-year olds, etc. \diamond

We will return to quotient sets shortly. 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 5.2.3, and which shows that equivalence classes are much better behaved than arbitrary relation classes (as seen in Example 5.1.2). The proof of part (i) of the following proposition, which is left to the reader as an exercise, is a rewriting of the proof of Theorem 5.2.3 (i) in our more general setting.

Theorem 5.3.3. *Let A be a non-empty set, and let \sim be an equivalence relation on A .*

(i) *Let $x, y \in A$. If $x \sim y$, then $[x] = [y]$. If $x \not\sim y$, then $[x] \cap [y] = \emptyset$.*

$$(ii) \quad \bigcup_{x \in A} [x] = A.$$

Proof. We will prove part (ii), leaving part (i) to the reader in Exercise 5.3.6 (ii). By definition $[x] \subseteq A$ for all $x \in A$, and thus $\bigcup_{x \in A} [x] \subseteq A$. Now let $q \in A$. By reflexivity we have $q \sim q$, and thus $q \in [q] \subseteq \bigcup_{x \in A} [x]$. Thus $A \subseteq \bigcup_{x \in A} [x]$, and hence $\bigcup_{x \in A} [x] = A$. \square

If you go through the proofs of both parts of the above theorem in detail, you will see that the proof of part (i) uses the symmetry and transitivity of the relation, and the proof of part (ii) uses reflexivity; we thus 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 part (ii) of the theorem, since some of the sets $[x]$ might be equal to one another. In Theorem 5.2.3 (ii), by contrast, we have the much stronger statement that $[0] \cup [1] \cup \dots \cup [n - 1] = \mathbb{Z}$, which does not have any redundancy. The statement of part (ii) of the above theorem in the particular case of congruence modulo n (for any $n \in \mathbb{N}$) would be that $\dots \cup [-1] \cup [0] \cup [1] \cup [2] \cup \dots = \mathbb{Z}$, which is not nearly as nice as the statement in Theorem 5.2.3 (ii). The reason that the statement in Theorem 5.2.3 (ii) is stronger is that in the particular case of congruence modulo n we have tools for studying the integers, such as the Division Algorithm (Theorem 8.4.9), that are not available for arbitrary equivalence relations.

The following corollary is derived immediately from Theorem 5.3.3 (i).

Corollary 5.3.4. *Let A be a non-empty set, and let \sim be an equivalence relation on A . Let $x, y \in A$. Then $[x] = [y]$ iff $x \sim y$.*

Suppose that we have an equivalence relation \sim on a set A . Form the quotient set A / \sim . We see from Theorem 5.3.3 that any two distinct equivalence classes are disjoint, and that the union of all equivalence classes is the original set A . We can thus think A / \sim as breaking up the set A into disjoint subsets. The following definition generalizes this notion of breaking a set into disjoint subsets.

Definition. Let A be a non-empty set. A **partition** of A is a collection \mathcal{D} of non-empty subsets of A such that

(1) $P \cap Q = \emptyset$ when $P, Q \in \mathcal{D}$ and $P \neq Q$;

(2) $\bigcup_{P \in \mathcal{D}} P = A$. △

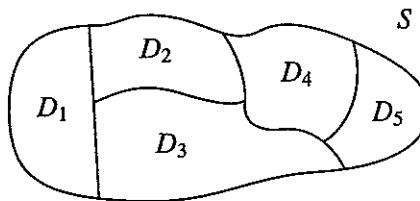


Figure 5.3.1.

Example 5.3.5.

- (1) Let E denote the even integers, and let O denote the odd integers. Then the collection $\mathcal{D} = \{E, O\}$ is a partition of \mathbb{Z} .
- (2) Let $\mathcal{C} = \{[n, n + 1) \mid n \in \mathbb{Z}\}$. Then \mathcal{C} is a partition of \mathbb{R} .

(3) Let $\mathcal{G} = \{(n - 1, n + 1) \mid n \in \mathbb{Z}\}$. Then \mathcal{G} is not a partition of \mathbb{R} , since not all elements of \mathcal{G} are disjoint. For example, we have $(1 - 1, 1 + 1) \cap (2 - 1, 2 + 1) = (0, 2) \cap (1, 3) = (1, 2)$. \diamond

With the above definition, we can now state the following immediate corollary to Theorem 5.3.3.

Corollary 5.3.6. *Let A be a non-empty set, and let \sim be an equivalence relation on A . Then A/\sim is a partition of A .*

The above corollary shows 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 maps. To state our result, we will need the following definition, which takes us to one higher level of abstraction than before.

Definition. 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 . Δ

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 collection of subsets of A that satisfy certain conditions.

Example 5.3.7. Let $A = \{1, 2, 3\}$. Then $\mathcal{T}_A = \{\mathcal{D}_1, \mathcal{D}_2, \dots, \mathcal{D}_5\}$, where the sets \mathcal{D}_i are

$$\begin{aligned}\mathcal{D}_1 &= \{\{1\}, \{2\}, \{3\}\}, & \mathcal{D}_4 &= \{\{2, 3\}, \{1\}\}, \\ \mathcal{D}_2 &= \{\{1, 2\}, \{3\}\}, & \mathcal{D}_5 &= \{\{1, 2, 3\}\}, \\ \mathcal{D}_3 &= \{\{1, 3\}, \{2\}\},\end{aligned}$$

Also, we see that $\mathcal{E}(A) = \{R_1, R_2, \dots, R_5\}$, where the relations R_i are

$$\begin{aligned}R_1 &= \{(1, 1), (2, 2), (3, 3)\}, \\ R_2 &= \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}, \\ R_3 &= \{(1, 1), (2, 2), (3, 3), (1, 3), (3, 1)\}, \\ R_4 &= \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}, \\ R_5 &= \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2)\}.\end{aligned}$$

It is straightforward to verify that each of the relations R_i listed above is an equivalence relation on A , and that we have all the equivalence relations on A . \diamond

Is it a coincidence that the sets \mathcal{T}_A and $\mathcal{E}(A)$ in the above example have the same number of elements? It is, in fact, no coincidence. We will see shortly that for any set A , whether finite or infinite, there is a correspondence between the partitions of A and equivalence relations on A . We start by defining a map from $\mathcal{E}(A)$ to \mathcal{T}_A , and a map in the other direction, for each non-empty set A . It is not entirely obvious that these definitions make sense, but they do indeed work, as noted in the lemma following the definition.

Definition. Let A be a non-empty set. Define a map $\Phi: \mathcal{E}(A) \rightarrow \mathcal{T}_A$ as follows. If \sim is an equivalence relation on A , let $\Phi(\sim)$ be the collection of sets A / \sim . Define a map $\Psi: \mathcal{T}_A \rightarrow \mathcal{E}(A)$ as follows. If \mathcal{D} is a partition of A , let $\Psi(\mathcal{D})$ be the relation on A given by $x \Psi(\mathcal{D}) y$ iff there is some $P \in \mathcal{D}$ such that $x, y \in P$, for all $x, y \in A$. Δ

Lemma 5.3.8. *Let A be a non-empty set. The maps Φ and Ψ in the above definition 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 collection of sets $\Phi(\sim)$ is a partition of A ; (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 5.3.6. The second claim is straightforward, and is left to the reader. \square

Note that there is a distinct map Φ and a distinct map Ψ for each non-empty set A , but to avoid cumbersome notation, we will assume that the set A is always known in any given situation.

Example 5.3.9.

(1) Let \sim be the relation on \mathbb{R}^2 given by $(x, y) \sim (z, w)$ iff $y - x = w - z$, 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 $[(x, y)] = \{(z, w) \in \mathbb{R}^2 \mid w - z = y - x\}$. If $c = y - x$, 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 . It is thus seen that $\Phi(\sim)$ 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 5.3.5 (2). We want to describe the equivalence relation $\Psi(\mathcal{C})$. For convenience let $\approx = \Psi(\mathcal{C})$. Suppose $x, y \in \mathbb{R}$. Then $x \approx y$ iff there is some $n \in \mathbb{Z}$ such that $x, y \in [n, n+1]$. Using the notation $[x]$ to denote the greatest integer less than or

equal to x (discussed in more detail in Exercise 2.4.11), we see that $x \approx y$ iff $[x] = [y]$.

(3) We continue Example 5.3.7. It can be verified that $\Phi(R_i) = \mathcal{D}_i$ and $\Psi(\mathcal{D}_i) = R_i$ for all $i \in \{1, \dots, 5\}$; details are left to the reader. \diamond

In part (3) of the above example, we see that Φ and Ψ are inverse maps to 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: equivalence relations and partitions are in bijective correspondence, which means that to each equivalence relation on a set, there corresponds a unique partition of the set, and vice versa; moreover, we have an explicit bijective map between the set of equivalence relations on the set and the set of partitions of the set.

Theorem 5.3.10. *Let A be a non-empty set. Then the maps Φ and Ψ are inverses of each other, and hence both are bijective.*

Proof. We need to show that

$$\Psi \circ \Phi = 1_{\mathcal{E}(A)} \quad \text{and} \quad \Phi \circ \Psi = 1_{T_A}.$$

To 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 $\approx = \sim$. It would then follow that $\Psi \circ \Phi = 1_{\mathcal{E}(A)}$. For convenience let $\mathcal{D} = \Phi(\sim)$, so that $\approx = \Psi(\mathcal{D})$. Now suppose we have $x, y \in A$. Suppose $x \approx y$. Then by the definition of Ψ we know that 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 , say $D = [q]$ 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 $x \sim y$. Then $y \in [x]$. By the reflexivity of \sim , we also know that $x \in [x]$. By the definition of Φ , we know that $[x] \in \mathcal{D}$. Hence, by the definition of Ψ , it follows that $x \approx y$. Thus $x \approx y$ iff $x \sim y$. We conclude that $\approx = \sim$.

To prove $\Phi \circ \Psi = 1_{T_A}$, let $\mathcal{D} \in T_A$ be a partition of A . Let $\mathcal{F} = \Phi(\Psi(\mathcal{D}))$. We will show that $\mathcal{F} = \mathcal{D}$. It would follow that $\Phi \circ \Psi = 1_{T_A}$. For convenience let $\sim = \Psi(\mathcal{D})$, so that $\mathcal{F} = \Phi(\sim)$. Now, let $B \subseteq A$. Then by the definition of Φ we know that $B \in \mathcal{F}$ iff B is an equivalence class of \sim . We claim that the definition of Ψ implies that B is an equivalence class of \sim iff $B \in \mathcal{D}$; this claim is left to the reader in Exercise 5.3.11. It then follows that $B \in \mathcal{F}$ iff $B \in \mathcal{D}$. Hence $\mathcal{F} = \mathcal{D}$. \square

Exercises

5.3.1. Which of the following relations is an equivalence relation?

- (1) Let M be the relation on \mathbb{R} given by xMy iff $x - y$ is an integer, for all $x, y \in \mathbb{R}$.
- (2) Let S be the relation on \mathbb{R} given by xSy iff $x = |y|$, for all $x, y \in \mathbb{R}$.
- (3) Let T be the relation on \mathbb{R} given by xTy iff $\sin x = \sin y$, for all $x, y \in \mathbb{R}$.
- (4) Let P be the set of all people, and let Z be the relation on P given by xZy iff x and y are first cousins, for all people x and y .
- (5) Let P be the set of all people, and let R be the relation on P given by xRy iff x and y have the same maternal grandmother, for all people x and y .
- (6) Let L be the set of all lines in the plane, and let W be the relation on L given by $\alpha W \beta$ iff α and β are parallel, for all $\alpha, \beta \in L$.

5.3.2. For each of the following equivalence relations on \mathbb{R} , find $[0]$ and $[3]$.

- (1) Let R be the relation given by aRb iff $|a| = |b|$, for all $a, b \in \mathbb{R}$.
- (2) Let S be the relation given by aSb iff $\sin a = \sin b$, for all $a, b \in \mathbb{R}$.
- (3) Let T be the relation given by aTb iff there is some $n \in \mathbb{Z}$ such that $a = 2^n b$, for all $a, b \in \mathbb{N}$.

5.3.3. For each of the following equivalence relations on \mathbb{R}^2 , give a geometric description of $[(0, 0)]$ and $[(3, 4)]$.

- (1) Let Q be the relation given by $(x, y)Q(z, w)$ iff $x^2 + y^2 = z^2 + w^2$, for all $(x, y), (z, w) \in \mathbb{R}^2$.
- (2) Let U be the relation given by $(x, y)U(z, w)$ iff $|x| + |y| = |z| + |w|$, for all $(x, y), (z, w) \in \mathbb{R}^2$.
- (3) Let V be the relation given by $(x, y)V(z, w)$ iff $\max\{|x|, |y|\} = \max\{|z|, |w|\}$, for all $(x, y), (z, w) \in \mathbb{R}^2$.

5.3.4. Let $f : A \rightarrow B$ be a map. Define a relation \sim on A by letting $x \sim y$ iff $f(x) = f(y)$, for all $x, y \in A$.

- (1) Show that \sim is an equivalence relation.
- (2) What can be said about the equivalence classes of \sim , depending upon whether f is injective but not surjective, surjective but not injective, neither or both?

5.3.5. Let A be a set, and let \asymp be a relation on A . Prove that \asymp is an equivalence relation iff 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 $x, y, z \in A$.

5.3.6. [Used in Section 5.3.] Prove Theorem 5.3.3 (i).

5.3.7. Let A be a non-empty set. Let I be a non-empty set and let $\{E_i\}_{i \in I}$ be a family of equivalence relations on A indexed by I .

- (1) Show that $\bigcap_{i \in I} E_i$ is an equivalence relation on A .
- (2) Is $\bigcup_{i \in I} E_i$ an equivalence relation on A ? Give a proof or a counter-example.

5.3.8. Let A be a non-empty set, and let R be a relation on A . Define the **minimal** equivalence relation on A containing R to be the intersection of all equivalence relations on A that contain R . Show that the minimal equivalence relation on A containing R satisfies the following two properties: (1) It is an equivalence relation on A that contains R ; (2) it is minimal in the sense that if \sim is any equivalence relation on A that contains R , then it contains the minimal equivalence relation on A containing R .

5.3.9. Using the terminology of Exercise 5.3.8, find the minimal equivalence relation containing each of the relations given below.

- (1) Let S be the relation on \mathbb{R} given by xSy iff $x = 2y$, for all $x, y \in \mathbb{R}$.
- (2) Let P be the set of all people, and let R be the relation on P given by xRy iff x likes y , for all people x and y .
- (3) The relation $<$ on \mathbb{R} .

5.3.10. Which of the following collections of subsets of \mathbb{R} are partitions of $[0, \infty)$?

- | | |
|----------------------------------------------------------|---------------------------------------------------------------------|
| (1) $\mathcal{H} = \{[n - 1, n)\}_{n \in \mathbb{N}}$. | (4) $\mathcal{I} = \{[n - 1, n + 1)\}_{n \in \mathbb{N}}$. |
| (2) $\mathcal{G} = \{[x - 1, x)\}_{x \in [0, \infty)}$. | (5) $\mathcal{J} = \{[0, n)\}_{n \in \mathbb{N}}$. |
| (3) $\mathcal{F} = \{\{x\}\}_{x \in [0, \infty)}$. | (6) $\mathcal{K} = \{[2^{n-1} - 1, 2^n - 1)\}_{n \in \mathbb{N}}$. |

5.3.11. [Used in Section 5.3.] Prove the claim made in the second part of the proof of Theorem 5.3.10. More precisely, let A be a non-empty set, and let \mathcal{D} be a partition of A . Let $\sim = \Psi(\mathcal{D})$. Show that the equivalence classes of \sim are precisely the elements of \mathcal{D} ; that is, show that $A/\sim = \mathcal{D}$.

5.3.12. For each of the following equivalence relations, describe the corresponding partition.

- (1) Let P be the set of all people, and let R be the relation on P given by xRy iff x and y have the same mother, for all people x and y .
- (2) Let \sim be the relation on $\mathbb{R} - \{0\}$ given by $x \sim y$ iff $xy > 0$, for all $x, y \in \mathbb{R} - \{0\}$.
- (3) Let T be the relation on \mathbb{R}^2 given by $(x, y)T(z, w)$ iff $(x - 1)^2 + y^2 = (z - 1)^2 + w^2$, 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 S be the relation on L given by l_1Sl_2 iff l_1 is parallel to l_2 or is equal to l_2 , for all $l_1, l_2 \in L$.

5.3.13. For each of the following partitions, describe the corresponding equivalence relation.

- (1) Let \mathcal{E} be the partition of $A = \{1, 2, 3, 4, 5\}$ given by $\mathcal{E} = \{\{1, 5\}, \{2, 3, 4\}\}$.
- (2) Let \mathcal{Z} be the partition of \mathbb{R} given 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} given by $\mathcal{W} = \{[n, n+2) \mid n \text{ is an even integer}\}$.

5.3.14. Let A be a non-empty set, and let E_1 and E_2 be equivalence relations on A . Let \mathcal{D}_1 and \mathcal{D}_2 denote the partitions of A that correspond to E_1 and E_2 respectively. Let $E = E_1 \cap E_2$. Then E is an equivalence relation on A by Exercise 5.3.7 (i). Let \mathcal{D} denote the partition of A that correspond to E . What is the relation between \mathcal{D}_1 , \mathcal{D}_2 and \mathcal{D} ? Prove your result.

5.3.15. Let A be a non-empty set. Let $\mathcal{R}(A)$ denote the set of all relations on A . Let \mathcal{S}_A denote the set of all collections 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 power sets.
- (3) Let $A = \{1, 2\}$. What are $\mathcal{R}(A)$ and \mathcal{S}_A ?
- (4) Suppose that A is a finite set with $|A| = n$. What are $|\mathcal{R}(A)|$ and $|\mathcal{S}_A|$? Do $\mathcal{R}(A)$ and \mathcal{S}_A have the same number of elements?

5.3.16. This exercise makes use of the definitions given in Exercise 5.3.15. We can generalize the maps Φ and Ψ defined in this section as follows. Let A be a non-empty set. Define a map $\tilde{\Phi}: \mathcal{R}(A) \rightarrow \mathcal{S}_A$ as follows. If R is a relation on A , let $\Phi(R)$ be the collection of all relation classes of A with respect to R . Define a map $\tilde{\Psi}: \mathcal{S}_A \rightarrow \mathcal{R}(A)$ as follows. If \mathcal{D} is a collection of subsets of A , let $\Psi(\mathcal{D})$ be the relation on A given by $x \Psi(\mathcal{D}) y$ iff there

is some $D \in \mathcal{D}$ such that $x, y \in D$, for all $x, y \in A$. (There is a distinct map $\tilde{\Phi}$ and a distinct map $\tilde{\Psi}$ for each non-empty set A , but, as with Φ and Ψ , to avoid cumbersome notation, we will assume that the set A is always known in any given situation.)

(1) Find a set A and an element $\mathcal{D} \in \mathcal{S}_A$ such that $\tilde{\Psi}(\mathcal{D})$ is not reflexive. Find a set B and an element $\mathcal{E} \in \mathcal{S}_B$ such that $\tilde{\Psi}(\mathcal{E})$ is not transitive.

(2) Let A be a finite set with at least two elements. Show that $\tilde{\Phi}$ and $\tilde{\Psi}$ are neither injective nor surjective. Is it necessary to restrict our attention to sets with at least two elements?

(3) Let A be any set with at least two elements. Describe the images of the maps $\tilde{\Phi}$ and $\tilde{\Psi}$, and prove your results. For $\tilde{\Phi}$ restrict your attention to A with finitely many elements.

5.3.17. Let A be a non-empty set, and let \sim be an equivalence relation on A . The **canonical map** $\gamma: A \rightarrow A/\sim$ is defined by $\gamma(x) = [x]$ for all $x \in A$.

Now suppose we are given a map $f: A \rightarrow B$, and that this map respects \sim , as defined in Exercise 5.1.12. Show that there exists a unique map $g: A/\sim \rightarrow B$ such that $f = g \circ \gamma$. This last condition can be expressed by saying that the following diagram is commutative (as discussed in Section 4.3).

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \gamma & & \nearrow g \\ A/\sim & & \end{array}$$

5.3.18. This exercise makes use of the definition given at the start of Exercise 5.3.17. Let $h: X \rightarrow Y$ be a map. Define a relation \asymp on X by letting $s \asymp t$ iff $h(s) = h(t)$, for all $s, t \in X$.

(1) Show that \asymp is an equivalence relation on X .

(2) Let $\gamma: X \rightarrow X/\asymp$ be the canonical map defined in Exercise 5.3.17. Let $j: h_*(X) \rightarrow Y$ be the inclusion map; that is, we have $j(w) = w$ for all $w \in h_*(X)$. Show that there is a unique bijective map $\hat{h}: X/\asymp \rightarrow h_*(X)$ such that $h = j \circ \hat{h} \circ \gamma$. This last condition can be expressed by saying that

the following diagram is commutative (as discussed in Section 4.3).

$$\begin{array}{ccc}
 X & \xrightarrow{f} & Y \\
 \downarrow \gamma & & \uparrow j \\
 X/\asymp & \xrightarrow{\hat{h}} & h(X)
 \end{array}$$

Note that γ is surjective, that \hat{h} is bijective and that j is injective. Thus any map can be written as a composition of a surjective map, a bijective map and an injective map.

6

Infinite and Finite 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 Cardinality of Sets

Infinite sets can behave more strangely than finite ones, at least from the perspective of 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, but this topic is beyond the scope of this text.

The issue we tackle here concerns the sizes of sets. Finite sets certainly come in different sizes, but what about infinite sets? Galileo, writing in the early 17th 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 this section and the next we will see a number of important arguments by Cantor; these ideas helped propel set theory into its prominent role in modern mathematics.

This chapter contains a seemingly disparate selection of topics, but they are loosely bound together by the notion of sets having the same size. This section and the next discuss the sizes of sets directly; Sections 6.3 and 6.4 discuss issues related to countably infinite sets. Further topics pertaining to finite sets may be found in Sections 7.6 and 7.7. As in previous chapters, we will make use of standard definitions and properties of the integers, rational numbers and real numbers (see the Appendix for a brief list of some of these properties.)

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 set before we compare different sets. The notion of the size of a finite set is intuitively clear, but for infinite sets the notion of “size” is less intuitively obvious. It turns out, and this is a great insight, that we can discuss whether two sets have the “same size” without first figuring out the size of each set.

We start with a simple example. Suppose a group of people want to stay at a hotel, with each person in a separate room. The hotel manager only wants to take the group 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.

We will determine whether two sets have the same size not by “counting” how many elements each set has, but by trying to pair up the elements of the two sets. Our tool for “pairing up” is bijective maps, as in the following definition.

Definition. Let A, B be sets. We say that A and B have the **same cardinality**, written $A \sim B$, if there is a bijective map $f: A \rightarrow B$. \triangle

If two sets have the same cardinality, there will be many bijective maps between them (unless each set has only one or zero elements). It is important to remember that when formally proving that two sets have the same cardinality, we do so by finding a bijective map from one set to the other, not by counting elements of sets. The following lemma gives the basic properties of \sim , which should look familiar.

Lemma 6.1.1. *Let A, B and C be sets.*

- (i) $A \sim A$.
- (ii) *If $A \sim B$, then $B \sim A$.*
- (iii) *If $A \sim B$ and $B \sim C$, then $A \sim C$.*

Proof. see Exercise 6.1.3. \square

We start with some examples of sets that have the same cardinality.

Example 6.1.2.

(1) Though he made one major mistake concerning infinite sets (to be discussed shortly), Galileo understood the idea of using bijective maps (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, since 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 $\mathbb{N} = \{1, 2, 3, \dots\}$ and the set of squares $S = \{1, 4, 9, 16, \dots\}$ have the same cardinality. Galileo's argument is precisely the same as our modern one, namely that the map $h: \mathbb{N} \rightarrow S$ given by $h(n) = n^2$ for all $n \in \mathbb{N}$ is a bijective map. That h is bijective follows from the fact that $k: S \rightarrow \mathbb{N}$ given by $k(n) = \sqrt{n}$ for all $n \in S$ is an inverse map for h .

(2) A very useful fact is that the set of natural numbers \mathbb{N} and the set of integers \mathbb{Z} have the same cardinality. One choice of a bijective map $f: \mathbb{N} \rightarrow \mathbb{Z}$ is given 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 map is bijective.

(3) Let $[a, b]$ and $[c, d]$ be closed intervals in \mathbb{R} with $a < b$ and $c < d$. Then $[a, b] \sim [c, d]$. Let $g: [a, b] \rightarrow [c, d]$ 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 map g is bijective. A similar argument shows that any two open intervals of the form (a, b) and (c, d) have the same cardinality, and similarly for half-open intervals. What is less obvious, but nonetheless true, is that any two intervals of real numbers, possibly of different types (including infinite intervals), have the same cardinality. More precisely, let $a, b \in \mathbb{R}$ be numbers such that $a < b$. Then 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 $(-\infty, \infty)$. See Exercise 6.1.4. \diamond

For a better analysis of the cardinality of sets, we need to define various useful categories, such as finite sets vs. infinite sets. We have used the notion of finiteness intuitively up till now; 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 $\{1, \dots, n\}$. Since the concept of “...” is not a rigorous one, we prefer to use the following definition (discussed in more detail in Section 8.3).

Definition. Let $n \in \mathbb{N}$. We let $\llbracket 1, n \rrbracket$ denote the set $\llbracket 1, n \rrbracket = \{x \in \mathbb{N} \mid 1 \leq x \leq n\}$. Δ

We can now define the different types of cardinalities we will be dealing with.

Definition. (1) A set is **finite** if it is either the empty set or it has the same cardinality as $\llbracket 1, n \rrbracket$ 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 known as **denumerable**) if it is finite or countably infinite.

(5) A set is **uncountable** if it is not countable. Δ

Are there infinite sets? Are there uncountable sets? We will answer these questions after some preliminaries. Shortly after the quote from Galileo given above, Galileo continues

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

Galileo was essentially saying that all infinite sets have the same cardinality, which would make them all countably infinite in our terminology. We shall see that Galileo was wrong, via an abstract proof in Corollary 6.1.14, and then with regard to the points in a line in Theorem 6.2.3.

We start with some remarks about finite sets. First, we make the rather trivial observation that finite sets exist, since the set $\llbracket 1, n \rrbracket$ is finite for each $n \in \mathbb{N}$. 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, using the following definition.

Definition. Let A be a finite set. We define the **cardinality** of A , denoted $|A|$, as follows. If $A = \emptyset$, we let $|A| = 0$. If $A \neq \emptyset$, we let $|A| = n$, where $A \sim [\![1, n]\!]$. \triangle

There is a potential cause for worry with this definition. It uses the fact that a finite set is either empty or has the same cardinality as some set $[\![1, n]\!]$. Could it happen that a set has the same cardinality as both $[\![1, n]\!]$ and $[\![1, m]\!]$ for some different positive integers n and m ? If so, the above definition would not make sense. Our intuition tells us that this problem cannot occur; the following lemma shows that our intuition here is correct. The proof of this lemma, as well as the parts of the proofs of Theorems 6.1.6, 6.1.8 and 6.1.9 make use of some facts about \mathbb{N} that are stated in Section 8.3. You can either simply accept these quoted facts (they are all statements that fit with our intuitive understanding of the natural numbers), or you can read their proofs when we get to them. The proofs of these facts in Section 8.3 make use of some ideas we have not yet developed, but they do not make any use of the present chapter, so there is no circular reasoning involved. Given that the set of natural numbers is used in our definitions of finite sets and countable sets, it is unavoidable that some properties of the natural numbers are needed in our discussion of such sets.

Lemma 6.1.3. *Let $n, m \in \mathbb{N}$. Then $[\![1, n]\!] \sim [\![1, m]\!]$ iff $n = m$.*

Proof. This follows immediately from Exercise 8.3.8 (1). \square

We leave it to the reader to deduce the following corollary to Lemma 6.1.3.

Corollary 6.1.4. *Let A, B be finite sets. Then $A \sim B$ iff $|A| = |B|$.*

The above corollary, though it seems rather obvious, 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 are comparing different things, namely sets in the first approach and numbers in the second. The above corollary tells us that we will always obtain the same result by either method.

Example 6.1.5. Let $B = \{1, 4, 9, 16\}$. We can formally show that $|B| = 4$ by showing that $B \sim [\![1, 4]\!] = \{1, 2, 3, 4\}$. To prove this last claim, we define the map $h: B \rightarrow [\![1, 4]\!]$ given by $h(x) = \sqrt{x}$ for all $x \in B$. It is easy to verify that the map h is bijective. Needless to say, the use of a formal proof to demonstrate that $|B| = 4$ is a bit of overkill, and we will not feel the need to give any more such proofs concerning the cardinalities of particular finite sets. It is nice to know, however, that such proofs can be constructed. \diamond

We now prove a few properties of the cardinalities of finite sets. These properties involve ideas that you have probably used many times without having had a second thought. More properties regarding the cardinalities of finite sets may be found in Sections 7.6 and 7.7, particularly Theorem 7.6.5.

Theorem 6.1.6. *Let A, B be finite sets.*

- (i) *If $X \subseteq A$, then X is finite.*
- (ii) *If $X \subseteq A$, then $|A| = |X| + |(A - X)|$.*
- (iii) *If $X \subsetneq A$, then $|X| < |A|$.*
- (iv) *If $X \subsetneq A$, then $X \not\sim A$.*

Proof. (i). This follows immediately from Exercise 8.3.7.

(ii). If $A - X = \emptyset$, then the result is trivial, so assume otherwise. Suppose $|A| = n$. Let $f: A \rightarrow [\![1, n]\!]$ be a bijective map. We can then apply Exercises 8.3.7 to the subset $f_*(X)$ of $[\![1, n]\!]$ to find a bijective map $g: [\![1, n]\!] \rightarrow [\![1, n]\!]$, and some $k \in \mathbb{N}$ with $k \leq n$, such that $g_*(f_*(X)) = [\![1, k]\!]$. We deduce that $|X| = k$. Using Exercises 4.3.5 and 4.4.10, and the bijectivity of f and g , we deduce

$$\begin{aligned} (g \circ f)_*(A - X) &= g_*(f_*(A - X)) = g_*(f_*(A) - f_*(X)) \\ &= g_*(f_*(A)) - g_*(f_*(X)) = g_*([\![1, n]\!]) - g_*(f_*(X)) \\ &= [\![1, n]\!] - [\![1, k]\!] = [\![k+1, n]\!]. \end{aligned}$$

Hence $(g \circ f)|_{A-X}$ is a bijective map between $A - X$ and $[\![k+1, n]\!]$. By Exercise 8.3.9, we know that there is a bijective map from $[\![k+1, n]\!]$ to $[\![1, n-k]\!]$. Putting everything together we deduce that $|A - X| = n - k$. The result now follows.

- (iii). This follows from part (ii).
- (iv). This follows from part (iii) and Corollary 6.1.4. \square

Part (iv) of this lemma might seem trivial, but it should not be taken for granted, since 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 6.1.2 (2) that $\mathbb{N} \sim \mathbb{Z}$. In fact, it can be shown that Theorem 6.1.6 (iv) completely characterizes finite sets. That is, a set is finite iff it has no proper subset with the same cardinality as itself. See [Sup60, Section 4.2] for more details. The proof of this characterization uses the Axiom of Choice (mentioned briefly at the end of Section 3.2). This characterization of finite sets is quite nice, since 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 alternate way of stating this characterization of finiteness is that if A is a finite set, then a map $f: A \rightarrow A$ is bijective iff it is injective iff it is surjective. For an infinite set B , by contrast, a surjective or injective map $g: B \rightarrow B$ need not be bijective; the reader should supply examples.

We now turn to infinite sets. Our first result is a simple corollary to Theorem 6.1.6 (i); details are left to the reader.

Corollary 6.1.7. *Let A be a set. Then A is infinite iff it contains an infinite subset.*

To prove more about infinite sets, we narrow our focus first to countable sets, and then to uncountable ones. (See [Sup60, Section 5.3] for a more extensive discussion of countable sets.) Certainly \mathbb{N} is countably infinite, so countably infinite sets exist. Intuitively, 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. We will see later on that not every set can be so ordered. As an example of how to line up the elements of a countably infinite set, recall Example 6.1.2 (2), in which we have a bijective map $f: \mathbb{N} \rightarrow \mathbb{Z}$, which shows that \mathbb{Z} is countably infinite. If we think of the integers written in increasing order, that is $\dots, -2, -1, 0, 1, 2, \dots$, then there is no obvious “first integer”, “second integer”, etc. However, we can use the bijective map f to line up the integers in an alternate way. Since the map f is bijective, we know that the sequence $f(1), f(2), f(3), f(4), \dots$ contains each integer once and only once. Using the definition of the map f , we see that $f(1), f(2), f(3), f(4), \dots$ equals $0, 1, -1, 2, -2, \dots$, and we thus have the entire set of integers nicely arranged in a line. (This arrangement of the integers is not in order of increasing size, but that would be asking too much.)

We need to clear up one matter before going any further. The term “countably infinite” would seem to suggest that such a set is infinite. However, the definitions of “countably infinite” and “infinite” were made separately, and so we have to prove that countably infinite sets are indeed infinite (otherwise our choice of terminology would be rather misleading).

Theorem 6.1.8.

- (i) The set \mathbb{N} is infinite,
- (ii) A countably infinite set is infinite.

Proof. (i). Suppose to the contrary that \mathbb{N} is finite. Then there is some $n \in \mathbb{N}$ such that $\mathbb{N} \sim [\![1, n]\!]$. Let $f: [\![1, n]\!] \rightarrow \mathbb{N}$ be a bijective map. Then it is shown in Exercise 8.3.5 that there is some $k \in [\![1, n]\!]$ such that $f(k) \geq f(i)$ for any $i \in [\![1, n]\!]$. It follows that $f(k) + 1 > f(i)$ for all $i \in [\![1, n]\!]$. Thus $f(k) + 1 \notin f([\![1, n]\!])$. Since $f(k) + 1 \in \mathbb{N}$, we deduce that f is not surjective, a contradiction. Hence $\mathbb{N} \not\sim [\![1, n]\!]$.

(ii). Let B be a countably infinite set. Then $B \sim \mathbb{N}$. Suppose that B is finite. Then $B \sim [\![1, n]\!]$ for some $n \in \mathbb{N}$. By Lemma 6.1.1 we deduce that $\mathbb{N} \sim [\![1, n]\!]$, a contradiction to part (i) of this theorem. Thus B is infinite. \square

From part (i) of the above theorem we see that there are infinite sets. From part (ii) of the theorem and Corollary 6.1.7 we deduce that if a set A contains a countably infinite subset, then A is infinite; if a countable set B contains a countably infinite subset, then B is countably infinite. It also turns out that, conversely, any infinite set contains a countably infinite subset. The proof of this fact depends upon the Axiom of Choice. See [Sup60, Section 8.1] for details.

The following theorem, which gives some basic properties of countable sets, indicates why it is often useful to work with the broader concept of countability, rather than countably infinite, since the theorem would not be true if we replaced the word “countable” with “countably infinite.”

Theorem 6.1.9. *Let A be a non-empty set. The following are equivalent.*

- (1) The set A is countable.
- (2) The set A is a subset of a countable set.
- (3) There is an injective map $f: A \rightarrow \mathbb{N}$.
- (4) There is a surjective map $g: \mathbb{N} \rightarrow A$.

Proof. (1) \Rightarrow (2). This is trivial.

(2) \Rightarrow (3). Let X be a countable set such that $A \subseteq X$. Let $j: A \rightarrow X$ be the inclusion map. The map j is injective. We have two cases, depending upon whether X is finite or countably infinite. If X is finite, there is a bijective map $k: X \rightarrow [\![1, n]\!]$ for some $n \in \mathbb{N}$, and hence there is an injective map $\hat{k}: X \rightarrow \mathbb{N}$, because $[\![1, n]\!] \subseteq \mathbb{N}$. The map $\hat{k} \circ j: A \rightarrow \mathbb{N}$ is injective by Lemma 4.4.2 (i). If X is countably infinite, there is a bijective map $h: X \rightarrow \mathbb{N}$. Then $h \circ j: A \rightarrow \mathbb{N}$ is an injective map.

(3) \Rightarrow (1). Since A is non-empty, so is $f_*(A)$. Since $f_*(A) \subseteq \mathbb{N}$, we can apply Theorem 8.3.2 to find some $x_1 \in A$ such that $f(x_1) \leq f(x)$ for all $x \in A$. Since f is injective, it follows that $f(x_1) < f(x)$ for all $x \in A - \{x_1\}$. Let $A_2 = A - \{x_1\}$. If $A_2 = \emptyset$, then stop here. Otherwise, we can apply the same argument to the set $f_*(A_2)$, to obtain some $x_2 \in A_2$ such that $f(x_2) < f(x)$ for all $x \in A_2 - \{x_2\} = A - \{x_1, x_2\}$. Let $A_3 = A - \{x_1, x_2\}$. We can continue this process as long as $A_i \neq \emptyset$.

There are now two cases.

Case 1: Suppose that $A_n = \emptyset$ for some $n \in \mathbb{N}$. Then $A = \{x_1, \dots, x_{n-1}\}$, and so $A \sim [\![1, n-1]\!]$. Hence A is finite, and thus countable.

Case 2: Suppose $A_n \neq \emptyset$ for all $n \in \mathbb{N}$. Then we have defined an element $x_n \in A$ for all $n \in \mathbb{N}$. Let $h: \mathbb{N} \rightarrow A$ be defined by $h(n) = x_n$ for all $n \in \mathbb{N}$. We claim that h is bijective. By our construction, it is seen that $x_i \neq x_j$ for $i \neq j$. It follows that h is injective. To show that h is surjective, let $y \in A$, and suppose that $y \neq h(n)$ for any $n \in \mathbb{N}$. We know that $f(y) \in \mathbb{N}$, so $f(y) = m$ for some $m \in \mathbb{N}$. We know that $f(x_1) < f(x_2) < f(x_3) < \dots$, and it follows that $f(x_n) \geq n$ for each $n \in \mathbb{N}$. Hence $f(y) \leq f(x_m)$. On the other hand, by the definition of x_m we know that $f(x_m) < f(z)$ for any $z \in A - \{x_1, \dots, x_m\}$. Since $y \neq x_i$ for any $i \in \mathbb{N}$, we see that $y \in A - \{x_1, \dots, x_m\}$. Hence $f(x_m) < f(y)$, a contradiction. Thus h must be surjective. It follows that $A \sim \mathbb{N}$, and so A is countably infinite, and hence countable.

(3) \Leftrightarrow (4). Suppose (3) holds, so that there is an injective map $f: A \rightarrow \mathbb{N}$. By Theorem 4.4.3 (ii) we know that f has a left inverse, say $g: \mathbb{N} \rightarrow A$. By Exercise 4.4.12 (2) we see that g is surjective. A similar argument shows that (4) implies (3). \square

Are unions, intersections and products of countable sets also countable? The answer, proved in the following two theorems, is yes, with two caveats. When a union of countable sets is taken, we can use only countably many sets if we want to guarantee countability. To form an intuitive picture of

why the union of countably many countable sets is itself countable, consider the union of two countable sets A and B . We can line up each of their elements as $A = \{a_1, a_2, \dots\}$ and $B = \{b_1, b_2, \dots\}$. We can then line up the elements of $A \cup B$ as $\{a_1, b_1, a_2, b_2, \dots\}$, where we drop any element that is the same as an element previously listed in this order (which could happen, since A and B might have elements in common). A picture for the union of countably many countable sets is seen in Figure 6.1.1. When a product of countable sets is taken, we can use only finitely many sets if we want to guarantee countability.

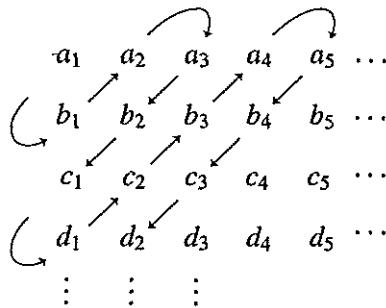


Figure 6.1.1.

Theorem 6.1.10. Let I be a non-empty set and let $\{A_i\}_{i \in I}$ be a family of sets indexed by I , where A_i is countable for each $i \in I$.

- (i) $\bigcap_{i \in I} A_i$ is countable.
- (ii) If I is countable, then $\bigcup_{i \in I} A_i$ is countable.

Proof. (i). Choose some $k \in I$. Then $\bigcap_{i \in I} A_i \subseteq A_k$, and thus $\bigcap_{i \in I} A_i$ is countable by Theorem 6.1.9.

(ii). 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 6.1.16. Since we are assuming that I is countably infinite, we can without loss of generality assume that $I = \mathbb{N}$.

Since A_i is countable for all $i \in I$, there is a surjective map $f_i : \mathbb{N} \rightarrow A_i$ for each $i \in I$ by Theorem 6.1.9. (It is pointed out in [Vau95, p. 56] that simultaneously choosing such maps for all $i \in I$ requires the Axiom of Choice, and that all proofs of this part of the lemma require this axiom.) We now define a map $g : \mathbb{N} \rightarrow \bigcup_{i \in I} A_i$ as follows. Let $r \in \mathbb{N}$. We now apply Exercise 6.3.13 to the function $f : \mathbb{N} \rightarrow \mathbb{N}$ given by $f(n) = (n - 1)n/2$ for all $n \in \mathbb{N}$, and deduce that there are unique $n, p \in \mathbb{N}$ such

that $(n-1)n/2 < r \leq n(n+1)/2$ and $r = (n-1)n/2 + p$. Define $g(r)$ to be $g(r) = f_{n-p+1}(p)$.

To prove the desired result, it will suffice by Theorem 6.1.9 to show that g is surjective. Let $x \in \bigcup_{i \in I} A_i$. Then $x \in A_k$ for some $k \in I$. Since f_k is surjective, there is some $w \in \mathbb{N}$ such that $x = f_k(w)$. Let $t = k + w - 1$. Then it is straightforward to verify that $g((t-1)t/2 + w) = f_{t-w+1}(w) = f_k(w) = x$. Thus g is surjective. \square

Theorem 6.1.11. *Let A_1, \dots, A_n be countable sets, for some $n \in \mathbb{N}$. Then $A_1 \times \dots \times A_n$ is countable.*

Proof. The result is trivial when $n = 1$. In Exercise 6.1.13 there is a proof of this result for the case $n = 2$. The general result follows from the case $n = 2$ and mathematical induction, as discussed in Section 6.3; the reader should fill in the details after reading that section. \square

We now turn briefly to uncountable sets. To show easily that there exist such sets, we need to consider the cardinality of the power set of a set. We start with an example.

Example 6.1.12. Let $A = \{1, 2\}$. Then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Thus we have $A \not\sim \mathcal{P}(A)$. \diamond

The following theorem shows that the above example is typical.

Theorem 6.1.13. *Let A be a set. Then $A \not\sim \mathcal{P}(A)$.*

Proof. There are two cases. First, suppose $A = \emptyset$. Then $\mathcal{P}(A) = \{\emptyset\}$. Thus $|A| = 0$ and $|\mathcal{P}(A)| = 1$, so $A \not\sim \mathcal{P}(A)$ by Corollary 6.1.4.

Next, suppose that $A \neq \emptyset$. Suppose further that $A \sim \mathcal{P}(A)$. Hence there is a bijective map $f: A \rightarrow \mathcal{P}(A)$. Let $D = \{a \in A \mid a \notin f(a)\}$. Note that $D \subseteq A$, and so $D \in \mathcal{P}(A)$. Since 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 have $d \notin f(d) = D$. Suppose that $d \notin D$. Then $d \in f(d) = D$. Thus we have a contradiction, and so $A \not\sim \mathcal{P}(A)$. \square

Corollary 6.1.14. *The set $\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof. By Theorem 6.1.13 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 $T = \{\{n\} \mid n \in \mathbb{N}\} \subseteq \mathcal{P}(\mathbb{N})$. By Theorem 6.1.6 (i) it follows that T is

finite. However, it is evident that $T \sim \mathbb{N}$, and this would imply that \mathbb{N} is finite, a contradiction to Theorem 6.1.8 (i). Hence $\mathcal{P}(\mathbb{N})$ is uncountable. \square

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.

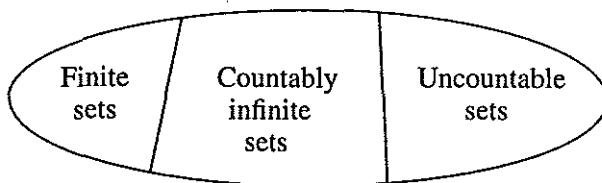


Figure 6.1.2.

We conclude this section by stating without proof two important results concerning cardinalities of sets. We start with the following definition, which gives a convenient relation between sets.

Definition. Let A and B be sets. We say that $A \preccurlyeq B$ if there is an injective map $f: A \rightarrow B$; we say that $A \prec B$ if $A \preccurlyeq B$ and $A \not\sim B$. (We assume that there is an injective map from the empty set to any set.) \triangle

Some basic properties of the relation \preccurlyeq are given in Exercise 6.1.18. It is simple to see that for any set A , there is an injective map $A \rightarrow \mathcal{P}(A)$. Using Theorem 6.1.13 we see that $A \prec \mathcal{P}(A)$. Applying this fact to the set \mathbb{N} , we deduce that

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \dots$$

Since all the sets in this sequence other than the first are uncountable, there are infinitely many different cardinalities among the uncountable sets. A commonly used notation due to Cantor is the symbol \aleph_0 , which denotes the cardinality of \mathbb{N} . Note that \aleph_0 is not a real number, though it is referred to as a “cardinal number.” Motivated by an observation made in Example 3.2.5, it is common to denote the cardinality of $\mathcal{P}(\mathbb{N})$ by 2^{\aleph_0} . (It is also possible to define \aleph_1, \aleph_2 , and beyond. See [Vau95, Section 7.5] for more details.)

The following two theorems about cardinality of sets are conveniently expressed using \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.

Theorem 6.1.15. *Let A and B be sets. Then $A \preccurlyeq B$ or $B \preccurlyeq A$.*

See [Mal79, Section 1.9] for a proof of this theorem. The proof relies on the Axiom of Choice.

Theorem 6.1.16. (Schroeder–Bernstein Theorem) *Let A and B be sets. Suppose that $A \preccurlyeq B$ and $B \preccurlyeq A$. Then $A \sim B$.*

See [Dev93, Section 3.6] for a quick (though technical) proof of this theorem using the Axiom of Choice, or [Vau95, Section 4.1] for a more concrete proof without the Axiom of Choice. The Schroeder–Bernstein Theorem (also referred to as the Cantor–Bernstein Theorem), not only has aesthetic appeal (by showing that the relation \preccurlyeq behaves analogously, at least in this respect, to the relation \leq on \mathbb{R}), but it is quite useful as well. There are cases where it is easier to find two injective maps (one $A \rightarrow B$ and the other $B \rightarrow A$) than a single bijective one. See Exercises 6.1.19 and 6.2.8 for examples.

Exercises

6.1.1. Show that the set of all integers that are multiples of 5 has the same cardinality as the set of all integers.

6.1.2. Show 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.

6.1.3. [Used in Section 6.1.] Prove Lemma 6.1.1

6.1.4. [Used in Section 6.1.] Let $a, b \in \mathbb{R}$ be numbers such that $a < b$. Using only the definition of two sets having the same cardinality, 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 $(-\infty, \infty)$. There is no need to show that every possible interval has the same cardinality as any other, since some of the cases are very similar to others. This exercise is rather tricky.

6.1.5. [Used in Section 7.6.] Let A and B be finite sets. Show that $A \cup B$ is finite.

6.1.6. [Used in Section 7.7.] Let A and B be finite sets such that $|A| = |B|$. Let $f: A \rightarrow B$. Show that f is bijective iff it is injective iff it is surjective.

6.1.7. [Used in Section 6.2.] (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 $A \cap C = \emptyset = B \cap C$. Show 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 $A \cap C = \emptyset = B \cap C$. Is it necessarily the case that $A \sim B$? Give a proof or a counterexample.

6.1.8. Let A and B be sets. Show that $A \sim B$ implies that $\mathcal{P}(A) \sim \mathcal{P}(B)$.

6.1.9. Let A be a set. Show that A is uncountable iff it contains an uncountable subset.

6.1.10. Let A be respectively a finite, infinite, countably infinite, countable or uncountable set, and let F be a finite set.

(1) Show that $A - F$ is respectively finite, infinite, countably infinite, countable or uncountable.

(2) Show that $A \cup F$ is respectively finite, infinite, countably infinite, countable or uncountable.

6.1.11. Let A be a set, and let x be an element (not necessarily in A). Show that $A \times \{x\} \sim A$.

6.1.12. Let A , B , C and D be sets. Suppose that $A \sim B$ and $C \sim D$. Show that $A \times C \sim B \times D$.

6.1.13. [Used in Section 6.1.] Let A and B be countable sets. Show that $A \times B$ is countable.

6.1.14. Let A be a countably infinite set, and let F be a non-empty finite set. Show that $A \times F$ is countably infinite.

6.1.15. Let A be an uncountable set, and let T be any non-empty set. Show that $A \times T$ is uncountable.

6.1.16. [Used in Section 6.1.] Prove Theorem 6.1.10 (ii) in the case that I is finite. Without loss of generality we may assume that $I = [\![1, s]\!]$ for some $s \in \mathbb{N}$.

6.1.17. (1) Let $f: A \rightarrow B$ be a map that has a left inverse but no right inverse. Show that if A is infinite, or if $B - f_*(A)$ is infinite and A has at least 2 elements, then f has infinitely many left inverses.

(2) Let $k: A \rightarrow B$ be a map that has a right inverse but no left inverse. Let

$$S = \{b \in B \mid k^*(\{b\}) \text{ has more than one element}\}.$$

Show that if S is infinite, or if $k^*(\{t\})$ is infinite for some $t \in S$, then k has infinitely many right inverses.

6.1.18. [Used in Section 6.1.] Let A, B, C be sets.

- (1) Show that $A \preccurlyeq A$.
- (2) Show that if $A \preccurlyeq B$ and $B \preccurlyeq C$, then $A \preccurlyeq C$.

6.1.19. [Used in Section 6.1.] Let $a, b, c, d \in \mathbb{R}$ be numbers such that $a < b$ and $c < d$. Use the Schroeder–Bernstein Theorem (Theorem 6.1.16) to give proofs of the following statements. (More concrete proofs of parts (1) and (2) were given in Exercise 6.1.4.)

- (1) $(a, b) \sim [a, b]$.
- (2) $(a, b) \sim \mathbb{R}$.
- (3) Let $X, Y \subseteq \mathbb{R}$ be sets such that $(a, b) \subseteq X$ and $(c, d) \subseteq Y$. Then $X \sim Y$.

6.2 Cardinality of the Number Systems

In this section we use the results of the previous section to discuss the cardinality of the standard number systems, namely the natural numbers, the integers, the rational numbers, the real numbers and the complex numbers. As mentioned in Section 6.1, the set of natural numbers \mathbb{N} is countably infinite. Since all the number systems under discussion contain \mathbb{N} , they are all infinite by Corollary 6.1.7. Which number systems are countable and which are uncountable?

The simplest case is the set of integers \mathbb{Z} , which we know is countably infinite by Example 6.1.2 (2). If we think of the real number line, we view the integers as sitting “discretely” in \mathbb{R} , that is, there are “gaps” between the integers. By contrast, the rational numbers are “dense” in \mathbb{R} , in that between any two real numbers, no matter how close, we can always find a rational number (see [Pow94, p. 128] for more details). It thus might appear that there are “more” rational numbers than integers. The following theorem shows that our intuition here is deceiving.

Theorem 6.2.1. *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. It is easy to see that the set $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ is also countable. By Theorem 6.1.11 we know that $\mathbb{Z} \times \mathbb{Z}^*$ is countable. It follows from Theorem 6.1.9 that there is a surjective map $g: \mathbb{N} \rightarrow \mathbb{Z} \times \mathbb{Z}^*$. Define a map $f: \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$ by $f((m, n)) = m/n$ 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 4.4.2 (ii) we see that $f \circ g$ is a surjective map $\mathbb{N} \rightarrow \mathbb{Q}$. Hence \mathbb{Q} is countable by Theorem 6.1.9. Since \mathbb{Q} is infinite, as previously remarked, it is therefore countably infinite. \square

The above theorem tells us that in theory the elements of \mathbb{Q} can be “lined up” in order just like the elements of \mathbb{N} (although this lining up of the elements of \mathbb{Q} will not necessarily be according to increasing size). It does not tell us how to line up the elements of \mathbb{Q} . The following picture, due to Cantor, summarizes a well known way of doing so for 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 6.4.15, having the aesthetic appeal of never encountering any number twice, and thus avoiding the need to drop repeated numbers as in Cantor’s procedure.)

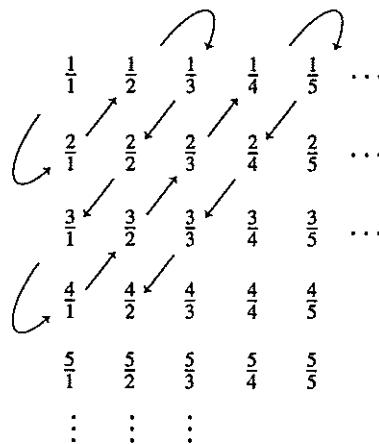


Figure 6.2.1.

Another set of numbers that is countable, and which is even larger than \mathbb{Q} , is the set of algebraic numbers, defined to be the set of all roots of polynomials with rational coefficients. Every rational number is contained in this set, but so are irrationals such as $\sqrt{2}$ (which is a solution to $x^2 - 2 = 0$). Many numbers are not algebraic, for example π and e , though it is not trivial to prove this; see [Her75, Section 5.2] for more details.

Theorem 6.2.2. *The set of all algebraic numbers is countably infinite.*

Proof. Left to the reader in Exercise 6.2.3 \square

We now turn to the set of all real numbers, our first concrete example of an uncountable set. (We already saw an uncountable set in Corollary 6.1.14, but that set was 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 we do not allow decimal expansions that eventually become repeating 9’s. We won’t prove this fact; see [BS82, pp. 60-63] or [Ros68, pp. 26-28] for more 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 6.2.3. *The set \mathbb{R} is uncountable.*

Proof. Suppose to the contrary that \mathbb{R} is countable. Since \mathbb{R} is infinite, as already noted, it must be countably infinite. From Example 6.1.2 (3) we know that $(0, 1) \sim \mathbb{R}$, and hence $(0, 1)$ must be countably infinite. Let $f: \mathbb{N} \rightarrow (0, 1)$ be a bijective map. For each $n \in \mathbb{N}$, we can write $f(n)$ as an infinite decimal $f(n) = 0.a_n^1 a_n^2 a_n^3 \dots$, where the numbers $a_n^1, a_n^2, a_n^3, \dots$ are integers in $\{0, 1, \dots, 9\}$, and where the expansion does not eventually become repeating 9’s.

We now define a number $b \in (0, 1)$ as follows. For $k \in \mathbb{N}$, define

$$b_k = \begin{cases} 1, & \text{if } a_k^k \neq 1 \\ 2, & \text{if } a_k^k = 1. \end{cases}$$

Note that $b_k \neq a_k^k$ for all $k \in \mathbb{N}$. Let b be the number represented by the decimal expansion $b = 0.b_1 b_2 b_3 \dots$. Since none of the numbers b_k are 9’s, 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, and thus if two numbers have different decimal expansions (even in only one digit) then they are different numbers. 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 . Thus $b \neq f(n)$ for any $n \in \mathbb{N}$, a contradiction to the surjectivity of f . We deduce that \mathbb{R} is not countable. \square

The above theorem 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 6.1.16), is given in Exercise 6.2.8.

$$\begin{aligned}
 f(1) &= 0.a_1^1 a_1^2 a_1^3 a_1^4 \dots \\
 f(2) &= 0.a_2^1 a_2^2 a_2^3 a_2^4 \dots \\
 f(3) &= 0.a_3^1 a_3^2 a_3^3 a_3^4 \dots \\
 f(4) &= 0.a_4^1 a_4^2 a_4^3 a_4^4 \dots \\
 &\vdots \quad \vdots
 \end{aligned}$$

Figure 6.2.2.

The set of irrational numbers is defined to be the set of all real numbers that are not rational, that is $\mathbb{R} - \mathbb{Q}$. There does not seem to be standard notation for the set of irrational numbers; we will use IRR . The set IRR is uncountable, for if not, then the real numbers would have to be a countable set as well, because $\mathbb{R} = \mathbb{Q} \cup \text{IRR}$, and using Theorems 6.2.1 and 6.1.10 (ii). The following theorem shows that in fact $\text{IRR} \sim \mathbb{R}$, which should not be taken as obvious, since not every uncountable set has the same cardinality as \mathbb{R} . (For example, we have $\mathcal{P}(\mathbb{R}) \not\sim \mathbb{R}$ by Theorem 6.1.13.)

Theorem 6.2.4. *The set of irrational numbers has the same cardinality as \mathbb{R} .*

Proof. We follow [Ham82]. Let IRR denote the set of irrational numbers. Define the set P to be $P = \{\sqrt{2}, 2\sqrt{2}, 3\sqrt{2}, \dots\}$. We know that $\sqrt{2} \in \text{IRR}$ by Theorem 2.3.3. Using Exercise 2.3.4 it follows that all other members of P are also in IRR . Hence $P \subseteq \text{IRR}$. It is straightforward to verify that P is countably infinite. By Theorems 6.2.1 and 6.1.10 (ii) we see that $\mathbb{Q} \cup P$ is countable. By Theorem 6.1.8 (ii) and Corollary 6.1.7 we deduce that this set is countably infinite. Hence $\mathbb{Q} \cup P \sim P$. We now have

$$\begin{aligned}
 \mathbb{R} &= \mathbb{Q} \cup \text{IRR} = \mathbb{Q} \cup [P \cup (\text{IRR} - P)] = (\mathbb{Q} \cup P) \cup (\text{IRR} - P) \\
 &\sim P \cup (\text{IRR} - P) = \text{IRR},
 \end{aligned}$$

using Exercise 6.1.7 (2) and the fact that $\mathbb{Q} \cup P \sim P$. □

The following theorem is, once again, slightly counterintuitive.

Theorem 6.2.5. *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 6.2.4. The proof that $\mathbb{R}^n \sim \mathbb{R}$ for arbitrary n is similar, using induction on n (as discussed in Section 6.3); the details are left to the reader. \square

In Exercise 6.2.5 we see 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 at the end of the previous section, we know that $\mathbb{N} \preccurlyeq \mathbb{R}$, since the inclusion map $i : \mathbb{N} \rightarrow \mathbb{R}$ is injective. From Theorem 6.2.3 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. 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. This remarkable situation is due to the work of Paul Cohen, who in 1963 proved that the Continuum Hypothesis is independent of the standard axioms for set theory. In other words, the Continuum Hypothesis can neither be proved nor disproved from these axioms. See [Mal79, Section 1.12] or [Vau95, Section 7.7] for further discussion (though the proof of Cohen's result is only to be found 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, living with the odd situation.

We conclude this section with an application of cardinality to computer science. There are many useful general purpose computer programming languages, such as Pascal, C++, Java, Standard ML 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 Standard ML is:

```
fun binom(n,k) =
  if k=0 orelse 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 more details about recursive definition, and 7.7 for discussion of the binomial coefficients.)

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 C++, for example, the allowed symbols include the letters of the English alphabet, the digits 0, . . . , 9, various symbols such as =, :, {, }, etc., and a blank space (which we can also think of as a symbol). Repeated blank spaces and carriage returns 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 not all strings will be valid programs. Let us denote the set of all finite strings in Σ by $S(\Sigma)$, and the set of all valid programs using these symbols by $C(\Sigma)$. 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 should be finite strings of symbols in Σ . Thus each computer program in Σ causes the computer to act as a function $S(\Sigma) \rightarrow S(\Sigma)$. 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 Σ gives rise to a map $\Phi: C(\Sigma) \rightarrow \mathcal{F}(S(\Sigma), S(\Sigma))$, where for each computer program p written with symbols Σ , we obtain the function $\Phi(p): S(\Sigma) \rightarrow S(\Sigma)$.

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 map Φ is surjective. If Φ were surjective, then every possible function $S(\Sigma) \rightarrow S(\Sigma)$ 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 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, regardless of the computer used, the map 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 map from a countable set to an uncountable one follows from Theorem 6.1.9.

To see that $C(\Sigma)$ is countable, we will show that $S(\Sigma)$ is countable, and then use Theorem 6.1.9. 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. Thus each set $S_n(\Sigma)$ is countable, and hence $S(\Sigma) = \bigcup_{n=1}^{\infty} S_n(\Sigma)$ is countable by Theorem 6.1.10 (ii).

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 4.5.2 it follows that $\mathcal{F}(S(\Sigma), S(\Sigma)) \sim \mathcal{F}(\mathbb{N}, \mathbb{N})$. It follows from Exercise 6.2.7 that $\mathcal{F}(\mathbb{N}, \mathbb{N})$ is uncountable, and hence so is $\mathcal{F}(S(\Sigma), S(\Sigma))$.

We thus see that cardinality considerations imply that there is a theoretical limitation to what can be accomplished by computer programming. See [Har96] for further discussion.

Exercises

6.2.1. Which of the following sets is countable, and which has the same cardinality as \mathbb{R} ? Prove your claims.

- (1) $\{\sqrt[n]{2} \mid n \in \mathbb{N}\}$.
- (2) $\{q \in \mathbb{Q} \mid q \text{ has denominator a multiple of } 3 \text{ when } q \text{ is expressed in lowest terms}\}$.
- (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) $\{S \subseteq \mathbb{N} \mid S \text{ has 7 elements}\}$.

(9) The set whose elements are the closed intervals in \mathbb{R} that have rational endpoints.

6.2.2. Show that the set

$$S = \{x \in (0, 1) \mid \text{the decimal expansion of } x \text{ has only odd digits}\}$$

is uncountable.

6.2.3. [Used in Section 6.2.] Prove Theorem 6.2.2.

6.2.4. [Used in Section 6.2.] Let A and B be sets, and suppose that $A \sim \mathbb{R}$ and $B \sim \mathbb{R}$. Show that $A \times B \sim \mathbb{R}$.

6.2.5. [Used in Section 6.2.] For those familiar with the complex numbers, show that the set of complex numbers \mathbb{C} has the same cardinality as \mathbb{R} .

6.2.6. 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 point. Show that \mathcal{D} is countable. (Use the “density” of \mathbb{Q} in \mathbb{R} , as mentioned in the text.)

6.2.7. [Used in Section 6.2.] Show that $\mathcal{F}(\mathbb{N}, \{0, 1\})$ and $\mathcal{F}(\mathbb{N}, \mathbb{N})$ are uncountable, using the notation of Section 4.5.

6.2.8. [Used in Section 6.1.] In this exercise we prove that $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$. We follow the proof in [Mor87, p. 286-287]. As in the proof of Theorem 6.2.3, it will suffice to prove that $(0, 1) \sim \mathcal{P}(\mathbb{N})$, and we will use the fact that every element of the interval $(0, 1)$ can be expressed uniquely as a decimal of the form $0.a_1 a_2 a_3 \dots$, where the numbers a_1, a_2, a_3, \dots are integers in $\{0, 1, \dots, 9\}$, and where the expansion does not eventually become repeating 9's. We will also use binary expansions, where every element of the interval $(0, 1)$ can be expressed uniquely as a decimal of the form $0.b_1 b_2 b_3 \dots$, where the numbers b_1, b_2, b_3, \dots are each either 0 or 1, and where the expansion does not eventually become repeating 1's.

By the Schroeder–Bernstein Theorem (Theorem 6.1.16), it will suffice to prove that $(0, 1) \preccurlyeq \mathcal{P}(\mathbb{N})$ and that $\mathcal{P}(\mathbb{N}) \preccurlyeq (0, 1)$. Thus we need to find an injective map $f: (0, 1) \rightarrow \mathcal{P}(\mathbb{N})$ and an injective map $g: \mathcal{P}(\mathbb{N}) \rightarrow (0, 1)$.

(1) Use the binary expansion of numbers in $(0, 1)$ mentioned above to define an injective map $f: (0, 1) \rightarrow \mathcal{P}(\mathbb{N})$.

- (2) Use the decimal expansion of numbers in $(0, 1)$ mentioned above to define an injective map $g: \mathcal{P}(\mathbb{N}) \rightarrow (0, 1)$.

6.3 Mathematical Induction

Mathematical induction is a very useful method of proving certain types of statements that involve 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 is not restricted to mathematics. 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 some statement involving n . 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 might have originally thought of trying to prove such a statement could occur 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 mathematical 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 mathematical 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 suffices 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 suffices to prove 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. We state this theorem without proof, since it is essentially one of the axiomatic properties that are assumed for the natural numbers. If you read Section 8.2, you will notice that PMI is just a restatement of part (3) of the Peano Postulates given in that section. PMI is essentially what distinguishes the natural numbers from the other systems of numbers such as the integers and the rational numbers. A more thorough understanding of the natural numbers can be obtained by studying them axiomatically, as in Sections 8.2 and 8.3, though it is possible to read the present section without having read either

of those sections. (There are a few proofs in the present section that rely on results from Chapter 8, but these proofs can be skipped over for now, or the results from Chapter 8 can be assumed without proof.) Formally, the statement of PMI gives criteria that guarantee that a subset of \mathbb{N} is in fact all of \mathbb{N} . We will see how to use these criteria shortly.

Theorem 6.3.1 (Principle of Mathematical Induction). *Let $G \subseteq \mathbb{N}$. Suppose that*

- (1) $1 \in G$;
- (2) if $n \in G$, then $n + 1 \in G$.

Then $G = \mathbb{N}$.

It is important to make use of part (2) of the statement of PMI precisely as it is written. This part has the form $P \rightarrow Q$. To show that part (2) is true in some given situation, we do not show that either P or Q is true, but only that the conditional statement $P \rightarrow Q$. In other words, we will not need to show directly that $n \in G$, nor that $n + 1 \in G$, but only that $n \in G$ implies $n + 1 \in G$.

Example 6.3.2. We will show that $8^n - 3^n$ is divisible by 5 for all $n \in \mathbb{N}$. We start by defining a set G by

$$G = \{n \in \mathbb{N} \mid 8^n - 3^n \text{ is divisible by } 5\}.$$

If we could show that $G = \mathbb{N}$, then it would indeed follow that $8^n - 3^n$ is divisible by 5 for all $n \in \mathbb{N}$. We will use PMI to show that $G = \mathbb{N}$. First, we note that $G \subseteq \mathbb{N}$ by definition. To use PMI, we need to show two things, namely that $1 \in G$, and that if $n \in G$ then $n + 1 \in G$. We start with the first of these. We observe that $8^1 - 3^1 = 5$, and thus $8^1 - 3^1$ is indeed divisible by 5. Hence $1 \in G$, which is part (1) of the statement of PMI.

To show part (2) of the statement of PMI, we assume that $n \in G$. We then need to deduce that $n + 1 \in G$. Since $n \in G$ 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

$$\begin{aligned} 8^{n+1} - 3^{n+1} &= 8 \cdot 8^n - 3 \cdot 3^n = (5 \cdot 8^n + 3 \cdot 8^n) - 3 \cdot 3^n \\ &= 5 \cdot 8^n + 3 \cdot (8^n - 3^n) \\ &= 5 \cdot 8^n + 3(5k) \\ &= 5(8^n + 3k). \end{aligned}$$

Hence we see that $8^{n+1} - 3^{n+1} = 5(8^n + 3k)$, which implies that $8^{n+1} - 3^{n+1}$ is divisible by 5. Hence $n + 1 \in G$. Thus we have proved that part (2) of the statement of PMI holds. PMI now implies that $G = \mathbb{N}$, and the result is proved. \diamond

The strategy used in the above example is quite typical. We first defined the set G . We then showed separately that parts (1) and (2) of the statement of PMI each holds. We often make a proof by mathematical induction less cumbersome by avoiding mentioning the set G explicitly. Suppose we are trying to show that the statement $P(n)$ holds for all $n \in \mathbb{N}$. The most formal way to proceed would be to define the set G as 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 statement $P(n)$ 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 variants on the inductive step, such as showing that if $P(n - 1)$ holds then so does $P(n)$ for all $n \in \mathbb{N}$ such that $n \geq 2$, or other similar variants.

The following example of a proof by mathematical induction, which we write in the less cumbersome style, is quite standard.

Proposition 6.3.3. *Let $n \in \mathbb{N}$. Then*

$$1 + 2 + \cdots + n = \frac{n(n + 1)}{2}. \quad (6.3.1)$$

Proof. We prove the result by induction on n . First, suppose that $n = 1$. Then $1 + 2 + \cdots + n = 1$, and $\frac{n(n + 1)}{2} = \frac{1(1 + 1)}{2} = 1$. Thus Equation 6.3.1 holds for the case $n = 1$. Now suppose that Equation 6.3.1 holds for n , that is

$$1 + 2 + \cdots + n = \frac{n(n + 1)}{2}.$$

Using this equation, we compute

$$\begin{aligned}
 1 + 2 + \cdots + (n+1) &= \{1 + 2 + \cdots + n\} + (n+1) \\
 &= \frac{n(n+1)}{2} + (n+1) \\
 &= (n+1)\left(\frac{n}{2} + 1\right) \\
 &= \frac{(n+1)(n+2)}{2} \\
 &= \frac{(n+1)[(n+1)+1]}{2}.
 \end{aligned}$$

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. This completes the proof that Equation 6.3.1 holds for all $n \in \mathbb{N}$. \square

It is important to note that a proof by mathematical induction can only show 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 mathematical 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, and so PMI does not apply to it.

Proof by mathematical 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 “in any collection of n horses, all the horses have the same color,” is true for all $n \in \mathbb{N}$. Since 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 in any collection of one horse, all the horses have the same color. Now suppose the result is true for n , so that in any collection of n horses, all the horses have the same color. We need to show that the result is true for $n+1$. Let $\{H_1, \dots, H_{n+1}\}$ be a collection of $n+1$ horses. The set $\{H_1, \dots, H_n\}$ has n horses, so by hypothesis all the horses in this set have the same color. On the other hand, the set $\{H_2, \dots, H_{n+1}\}$ also has n horses, so all horses in this set have the same color. It thus follows that H_n and H_{n+1} have the same color. Combining this fact with the previous observation that horses H_1, \dots, H_n all have the same color, it follows that H_1, \dots, H_{n+1} all have the same color. Thus we have proved the inductive step, and so the proof is complete. Hence all horses have the same color.

The reader is asked in Exercise 6.3.4 to find the flaw in the above argument. \diamond

The following example gives an application of mathematical induction to switching circuits, and thus to computers (which are built out of such circuits). See [LP98, Sections 2.7-2.8] or [Fab92] for more details about switching 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). We often represent these two states as 1 or 0 respectively. At its simplest, a switching circuit is a device with some number of inputs, say x_1, \dots, x_n , and one output, say y ; the device takes each collection of values (0 or 1) of the inputs, and produces a specific value for the output. A switching circuit is thus similar to a function, except that it can have any number of inputs, rather than just one, and the inputs and output can have only one of two values each. A switching circuit is defined by specifying its output value for each collection of input values. We can represent such a circuit schematically by the type of diagram in Figure 6.3.1.

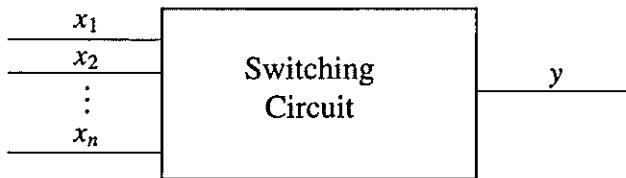


Figure 6.3.1.

For each $n \in \mathbb{N}$, it can be shown that there are 2^{2^n} possible switching circuits with n inputs (we leave it to the reader to derive this number). It would be unfortunate if each possible switching circuit with n inputs would have to be manufactured separately, and it turns out that doing so is unnecessary. We will show that all switching circuits can be built up out of 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 $\bar{\wedge}$. 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 $\bar{\wedge}$ with schematic symbols, such as those shown in Figure 6.3.2.

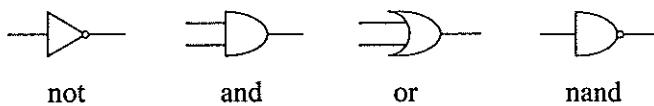


Figure 6.3.2.

We now prove by mathematical 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 the result is true for all switching circuits with n inputs. Let C be a switching circuit with $n + 1$ inputs, labeled x_1, \dots, 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, \dots, x_n , and such that the output of C_0 for a given collection of values of x_1, \dots, x_n equals the output of C for the same values of x_1, \dots, 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, \dots, x_{n+1} . Because C_0 and C_1 both have n inputs, it follows from our 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 mathematical induction, it follows that every switching circuit can be made out of our three building blocks. Even better, we can use Exercise 1.3.13 (3) to deduce that every switching circuit can be built out of $\bar{\wedge}$ circuits. \diamond

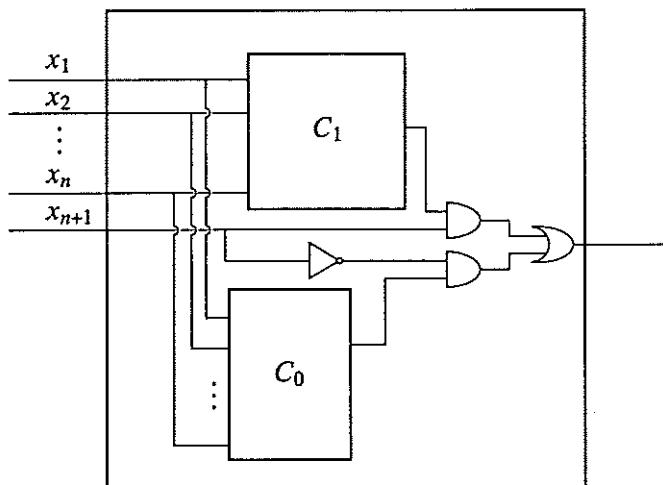


Figure 6.3.3.

There are various alternate versions of PMI, each of which is useful in certain situations where PMI might not be directly applicable. The three variants we mention are all derived from PMI, and are just restatements of Theorems 8.3.3, 8.3.4 and 8.3.5, so we will not prove them here. 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 an inductive step.

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*

- (1) $k_0 \in G$;
- (2) *if $n \in \mathbb{N}$ is such that $n \geq k_0$ and $n \in G$, then $n + 1 \in G$.*

Then $\{n \in \mathbb{N} \mid n \geq k_0\} \subseteq G$.

Note that in PMI-V1 we do not deduce that $G = \mathbb{N}$, only that $\{n \in \mathbb{N} \mid n \geq k_0\} \subseteq G$. 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 $n \geq 5$, then $4^n > n^4$.*

Scratch Work. For the case $n = 5$, it is easy to verify that $4^5 > 5^4$. Now suppose we know the result for n , so that $4^n > n^4$. We want to deduce that $4^{n+1} > (n+1)^4$. Using the binomial formula (Theorem 7.7.9), or by brute force multiplication, we know that $(n+1)^4 = n^4 + 4n^3 + 6n^2 + 4n + 1$. Since this expression has a number of pieces, it might be helpful to write $4^{n+1} = 4 \cdot 4^n = 4^n + 4^n + 4^n + 4^n$. Since 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 $4^n > 4n + 1$. To show these inequalities, we can make use of the fact that $n \geq 5$, as well as the fact that $4^n > n^4$. First, we notice that $4n^3 < 5n^3 \leq n \cdot n^3 = n^4 < 4^n$. Next, we observe that $6n^2 < 5^2 n^2 \leq n^2 n^2 = n^4 < 4^n$.

Finally, we have $4n + 1 < 4n + n = 5n \leq n \cdot n < n^4 < 4^n$. Putting all these observations together will do the trick. $\//\!$

Proof. We prove the result by induction on n , making use of PMI-V1 with $k_0 = 5$. First, suppose that $n = 5$. Then $4^5 = 1024 > 625 = 5^4$. Thus the desired result holds for the case $n = 5$. Now suppose that the result holds for n , so that $4^n > n^4$. We assume that $n \geq 5$. We will prove that the result holds for $n + 1$. We start with three preliminary calculations, all of which make use of our hypotheses that $4^n > n^4$ and $n \geq 5$. First, we have

$$4^n > n^4 > n^2 \geq 5n = 4n + n > 4n + 1.$$

Second, we have

$$4^n > n^4 \geq 5^2 n^2 > 6n^2.$$

Finally, we have

$$4^n > n^4 > 4n^3.$$

Combining all three inequalities we obtain

$$4^{n+1} = 4 \cdot 4^n = 4^n + 4^n + 4^n + 4^n > n^4 + 4n^3 + 6n^2 + (4n + 1) = (n + 1)^4.$$

This last inequality shows that the desired result holds for $n + 1$ whenever it holds for n , assuming that $n \geq 5$. This completes the proof. \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*

- (1) $1 \in G$;
- (2) if $n \in \mathbb{N}$ and $\{i \in \mathbb{N} \mid 1 \leq i \leq n\} \subseteq G$, then $n + 1 \in G$.

Then $G = \mathbb{N}$.

When using PMI-V2, the inductive step involves showing that if the desired statement is assumed to hold for all values in $\{1, \dots, n\}$, 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, by allowing a larger hypothesis in order to derive the same conclusion, but

PMI-V2 can be derived rigorously from PMI, and so we are free to use it whenever we need to.

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*

$$(1) \ k_0 \in G;$$

$$(2) \text{ if } n \in \mathbb{N} \text{ is such that } n \geq k_0 \text{ and } \{i \in \mathbb{N} \mid k_0 \leq i \leq n\} \subseteq G, \text{ then } n+1 \in G.$$

Then $\{n \in \mathbb{N} \mid n \geq k_0\} \subseteq G$.

The following theorem, which is a basic tool in number theory, is proved using PMI-V3. An examination of the proof reveals why PMI-V3 is preferable in this case to PMI-V1. Recall the definition of prime numbers in Section 2.3.

Theorem 6.3.10. *Let $n \in \mathbb{N}$ be such that $n \geq 2$. Then either n is prime, or it is the product of finitely many prime numbers.*

Proof. We will use PMI-V3 with $k_0 = 2$. First, suppose that $n = 2$. Since 2 is a prime number, we see that the desired result is true for $n = 2$. Now let $n \in \mathbb{N}$ be such that $n \geq 2$, and suppose that the desired result holds for all natural numbers in the set $\{2, 3, \dots, n\}$; that is, we assume that each of the numbers in $\{2, 3, \dots, n\}$ 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. We have two cases: either $n + 1$ is a prime number or it is not. If $n + 1$ is a prime number, then there is nothing to prove. Now assume that $n + 1$ is not a prime number. That means that $n + 1 = ab$, where a and b are natural numbers such that $1 < a, b < n + 1$. Thus $a, b \in \{2, 3, \dots, n\}$. Hence 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. This completes the proof. \square

The above result can be proved for all integers, and it can be proved that the decomposition into prime numbers is unique. The version of the theorem that includes both existence and uniqueness is known as the Fundamental Theorem of Arithmetic. See [Ros93a, 2.3] or [AR89, Section 1.4] for more details.

Exercises

6.3.1. Show that each of the following formulas holds for all $n \in \mathbb{N}$.

$$(1) 1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

$$(2) 1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

$$(3) 1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

$$(4) 1^3 + 3^3 + \cdots + (2n - 1)^3 = n^2(2n^2 - 1).$$

$$(5) 1 \cdot 2 + 2 \cdot 3 + \cdots + n(n + 1) = \frac{n(n+1)(n+2)}{3}.$$

$$(6) \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

$$(7) \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}.$$

6.3.2. Show that $1 + 2n < 3^n$ for all $n \in \mathbb{N}$.

6.3.3. Let $a, b \in \mathbb{N}$. Show that $a^n - b^n$ is divisible by $a - b$ for all $n \in \mathbb{N}$.

6.3.4. [Used in Section 6.3.] Find the flaw in Example 6.3.4.

6.3.5. For which positive values of $n \in \mathbb{N}$ does the inequality $n^2 - 9n + 19 > 0$ hold? Prove your answer by mathematical induction.

6.3.6. Prove that $(1 + \frac{1}{n})^n < n$ for all $n \in \mathbb{N}$ such that $n \geq 3$.

6.3.7. Prove that $n^3 + 1 > n^2 + n$ for all $n \in \mathbb{N}$ such that $n \geq 2$.

6.3.8. Prove that $7n < 2^n$ for all $n \in \mathbb{N}$ such that $n \geq 6$.

6.3.9. Prove $3^n > n^3$ for all $n \in \mathbb{N}$ such that $n \geq 4$.

6.3.10. Show that

$$\sum_{i=1}^n \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$$

for all $n \in \mathbb{N}$.

6.3.11. Show that

$$\prod_{i=2}^n \left(1 - \frac{i}{i^2}\right) = \frac{n+1}{2n}$$

for all $n \in \mathbb{N}$ such that $n \geq 2$. (The symbol \prod denotes the product of all the terms.)

6.3.12. Show that

$$\sum_{i=1}^n \frac{1}{\sqrt{i}} > \sqrt{n}$$

for all $n \in \mathbb{N}$ such that $n \geq 2$.

6.3.13. [Used in Section 6.1.] Let $f: \mathbb{N} \rightarrow \mathbb{Z}^{nn}$ be a map such that $f(1) = 0$, and that if $n < m$, then $f(n) < f(m)$, for any $n, m \in \mathbb{N}$. Show 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 use the function $f(n) = (n-1)b$ for all $n \in \mathbb{N}$, where $b \in \mathbb{N}$ is some fixed integer, then we obtain a variant of the Division Algorithm, which is stated formally in Theorem 8.4.9.)

6.4 Recursion

Consider the familiar sequence $1, 2, 4, 8, 16, \dots$. If we let a_n denote the n -th term of the sequence, then $a_n = 2^{n-1}$. Such a formula describes each term of the sequence explicitly, 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 is important not only in mathematics, but also in logic, and the applications of logic to computer science; see [Rob86] or [DSW94, Chapter 3] for more details. See [End72, Section 1.2] for a more general look at the mathematical approach to recursion. 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 alone, 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 definition, but no explicit formula? For example, suppose 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, \dots satisfying such a description? That is, does this description actually define a sequence? It does appear intuitively as if there is such a sequence; all we have to do is 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 $c_3 = 3 + 2c_2 = 3 + 2 \cdot 11 = 25$. We could continue indefinitely in this way, and so it would seem that the sequence c_1, c_2, c_3, \dots is defined for all $n \in \mathbb{N}$. Our intuition will turn out to be correct here, and the sequence is indeed well-defined for all $n \in \mathbb{N}$. (In fact, we will give an explicit formula for this sequence in Example 6.4.2.)

The method of recursive definition of sequences can be made completely rigorous, although it is not at all trivial to do so. Simply saying something like “just continue inductively” is not satisfactory. Proof by mathematical

induction, as discussed in Section 6.3, works for something that is already defined; here we need to prove that our definition actually produces something. Unfortunately, in some texts that discuss mathematical induction, not only is no proof given of the validity of definition by recursion, but no mention is even made of the need for such a proof. It's fine to skip a difficult proof, but mention should always be made that this is being done.

The hard part of the proof that recursive definition works will be done in Section 8.2, where we will have more tools at our disposal. To make use now of what we will prove there, we need to state more precisely what we mean by recursive definition. The simplest form of recursive definition works as follows. Suppose we are given a number $b \in \mathbb{R}$, and a function $h: \mathbb{R} \rightarrow \mathbb{R}$. We then want to define a sequence a_1, a_2, \dots such that $a_1 = b$ and that $a_{n+1} = h(a_n)$ for all $n \in \mathbb{N}$.

To be more precise, recall the formal definition of sequences in Example 4.5.1 (3). Although we informally write a sequence as a_1, a_2, \dots , the formal definition of a sequence of real numbers is a map $f: \mathbb{N} \rightarrow \mathbb{R}$, where we think of $f(1)$ as the first element of the sequence, of $f(2)$ as the second element of the sequence, etc. That is, we have $a_n = f(n)$ for all $n \in \mathbb{N}$.

Our recursive definition problem now becomes the following. Given a number $b \in \mathbb{R}$ and a function $h: \mathbb{R} \rightarrow \mathbb{R}$, can we find a function $f: \mathbb{N} \rightarrow \mathbb{R}$ such that $f(1) = b$ and $f(n+1) = h(f(n))$ for all $n \in \mathbb{N}$. The following theorem says that recursive definition always works out as expected. The proof of this theorem should be skipped until you read Section 8.2.

Theorem 6.4.1. *Let $b \in \mathbb{R}$ and $h: \mathbb{R} \rightarrow \mathbb{R}$ be given. Then there is a unique function $f: \mathbb{N} \rightarrow \mathbb{R}$ such that $f(1) = b$ and that $f(n+1) = h(f(n))$ for all $n \in \mathbb{N}$.*

Proof. Using the function s discussed in Sections 8.2, we can rewrite the second criterion in our theorem as $f(s(n)) = h(f(n))$ for all $n \in \mathbb{N}$. This last formulation is equivalent to the condition $f \circ s = h \circ s$. Our result now follows immediately from Theorem 8.2.1. \square

Example 6.4.2. We previously mentioned the recursive definition of a sequence given by $c_1 = 4$ and $c_{n+1} = 3 + 2c_n$ for all $n \in \mathbb{N}$. We can now treat this sequence more rigorously. If we let $b = 4$ and let $h: \mathbb{R} \rightarrow \mathbb{R}$ be given by $h(x) = 3 + 2x$ for all $x \in \mathbb{R}$, then Theorem 6.4.1 tells us that there is a unique function $f: \mathbb{N} \rightarrow \mathbb{R}$ such that $f(1) = 4$ and $f(n+1) = 3 + 2f(n)$ for all $n \in \mathbb{N}$. If we let $c_n = f(n)$ for all $n \in \mathbb{N}$, then we deduce that this

sequence c_1, c_2, c_3, \dots satisfies the conditions $c_1 = 2$ and $c_{n+1} = 3 + 2c_n$ for all $n \in \mathbb{N}$. Moreover, there can be no other sequence satisfying the original recursive definition, by the uniqueness property of Theorem 6.4.1.

Theorem 6.4.1 tells us only that a sequence c_1, c_2, c_3, \dots 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 recursively, 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 $n = 1$. This is seen by computing $7 \cdot 2^{1-1} - 3 = 4$, which is precisely the value of c_1 . Next, suppose that the result holds for some $n \in \mathbb{N}$. Thus $c_n = 7 \cdot 2^{n-1} - 3$. We then show that the result holds for $n + 1$, which we accomplish by computing

$$c_{n+1} = 3 + 2c_n = 3 + 2\{7 \cdot 2^{n-1} - 3\} = 7 \cdot 2^{(n+1)-1} - 3.$$

Hence the explicit formula for c_n satisfies the recursive definition. By uniqueness this formula is the only possible one for c_n (other than writing the same formula in a different way, which does not lead to a genuinely different formula). \diamond

In the above formulation of recursive definition, we had a_{n+1} be a function of a_n alone, given by the formula $a_{n+1} = h(a_n)$ for all $n \in \mathbb{N}$. Sometimes we might need a more complicated formula for a_{n+1} . For example, suppose we want to define a sequence by setting $a_1 = 1$ and $a_{n+1} = n + a_n$ for all $n \in \mathbb{N}$. Such a recursive definition is not covered by Theorem 6.4.1, though it does turn out to produce a well-defined sequence, which starts $1, 2, 4, 7, 11, \dots$. The following result, a strengthened version of Theorem 6.4.1, shows that everything works out here as well. Once again, the proof uses Section 8.2.

Theorem 6.4.3. *Let $b \in \mathbb{R}$ and $t: \mathbb{R} \times \mathbb{N} \rightarrow \mathbb{R}$ be given. Then there is a unique function $g: \mathbb{N} \rightarrow \mathbb{R}$ such that $g(1) = b$ and that $g(n + 1) = t((g(n), n))$ for all $n \in \mathbb{N}$.*

Proof. This follows immediately from Exercise 8.2.2 (which uses Theorem 8.2.1). \square

Example 6.4.4. We want to define a sequence by setting $a_1 = 1$ and $a_{n+1} = (n + 1)a_n$ for all $n \in \mathbb{N}$. Using Theorem 6.4.3 with $b = 1$

and $t(x, m) = (m + 1)x$ for all $(x, m) \in \mathbb{R} \times \mathbb{N}$, we know that there is a sequence satisfying these conditions. This sequence starts 1, 2, 6, 24, 120, ..., and consists of the familiar factorial numbers. We use the symbol $n!$ to denote a_n . You might think that we could have dispensed with the recursive definition entirely, and just have explicitly defined $a_n = n!$ for all $n \in \mathbb{N}$, but that would be putting the cart before the horse. The symbol $n!$ is informally defined by $n! = n(n - 1)(n - 2) \cdots 2 \cdot 1$, but this is not a rigorous definition, since "..." is not a rigorous concept. The formal way to define $n!$ is to say that it is the value of a_n for the sequence we have defined by our recursive formula. From our definition, we deduce immediately that $(n + 1)! = (n + 1)n!$ for all $n \in \mathbb{N}$, since that is the result of plugging the function given by $g(n) = n!$ for all $n \in \mathbb{N}$ into the recursive definition we started with. ◇

We have mentioned two types of recursive definitions so far; there are other variants as well. We present one more here, since it is used in a particularly interesting sequence that is defined recursively. This sequence, the well-known Fibonacci sequence, starts

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 \dots$$

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 more details.

The Fibonacci numbers arise in strange places, such as in phyllo-taxis, the study of various numbers that arise in plants (for example, the numbers of petals in flowers, the numbers of spirals in pine cones, etc.). 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 lengthy 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; decide for yourself 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.”)

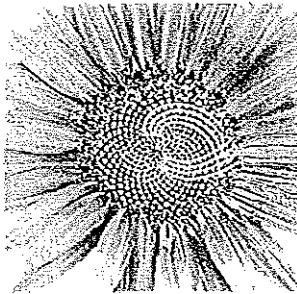


Figure 6.4.1.

What concerns us here is not biology but the mathematical properties of the Fibonacci numbers. Some mathematically serious treatments of the Fibonacci numbers appear 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, \dots . An examination of the sequence reveals its pattern, namely $F_{n+2} = F_{n+1} + F_n$. We formally define the Fibonacci sequence as the sequence satisfying the recursive definition given by $F_1 = 1$, and $F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \in \mathbb{N}$. To make sure that there is a sequence satisfying these criteria, we need the following variant on Theorem 6.4.1, the proof of which relies, yet again, on Section 8.2.

Theorem 6.4.5. *Let $a, b \in \mathbb{R}$ and $p: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ be given. Then there is a unique function $f: \mathbb{N} \rightarrow \mathbb{R}$ 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 follows immediately from Exercise 8.2.1. □

The Fibonacci sequence is defined using Theorem 6.4.5 with $a = 1$, $b = 1$ and $p((x, y)) = x + y$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is there an explicit formula for F_n ? We will answer that question shortly, but first we give 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 $n \in \mathbb{N}$. Then*

$$(i) \quad F_1 + F_2 + \cdots + F_n = F_{n+2} - 1;$$

- (ii) $F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}$;
- (iii) $(F_n)^2 - F_{n+1} \cdot F_{n-1} = (-1)^{n+1}$ when $n \geq 2$.

Proof. We will prove part (iii), leaving the rest to the reader in Exercise 6.4.4.

(iii). We use mathematical induction, using PMI-V3 with $k_0 = 2$. It is easy to check 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 suppose that the equation holds for all values in $\{2, \dots, n\}$. We calculate

$$\begin{aligned}(F_{n+1})^2 - F_{n+2} F_n &= (F_n + F_{n-1})^2 - (F_{n+1} + F_n) F_n \\&= (F_n)^2 + 2F_n F_{n-1} + (F_{n-1})^2 - F_{n+1} F_n - (F_n)^2 \\&= (F_{n-1})^2 + F_n(2F_{n-1} - F_{n+1}) \\&= (F_{n-1})^2 + F_n(2F_{n-1} - (F_n + F_{n-1})) \\&= (F_{n-1})^2 + F_n(F_{n-1} - F_n) \\&= (F_{n-1})^2 - F_n F_{n-2} = (-1)^n = (-1)^{(n+1)+1},\end{aligned}$$

where the last line follows by the inductive hypothesis. \square

To obtain an explicit formula for F_n in terms of n , we start by proving a more general result, which takes virtually no more effort than the particular case in which we are interested.

Proposition 6.4.7. *Let $c, d \in \mathbb{R}$ be non-zero. Suppose that A_1, A_2, A_3, \dots is a sequence satisfying the relation $A_{n+2} = cA_{n+1} + dA_n$ for all $n \in \mathbb{N}$.*

- (i) *If the equation $x^2 - cx - d = 0$ has two distinct real solutions r_1 and r_2 , then*

$$A_n = P(r_1)^n + Q(r_2)^n$$

for all $n \in \mathbb{N}$, where

$$P = \frac{r_2 A_1 - A_2}{r_1(r_2 - r_1)} \quad \text{and} \quad Q = \frac{r_1 A_1 - A_2}{r_2(r_1 - r_2)}.$$

- (ii) *If the equation $x^2 - cx - d = 0$ has one real solution r , then*

$$A_n = S r^n + T n r^n$$

for all $n \in \mathbb{N}$, where

$$S = \frac{2r A_1 - A_2}{r^2} \quad \text{and} \quad T = \frac{A_2 - r A_1}{r^2}.$$

Proof. We will prove part (i), leaving part (ii) to the reader in Exercise 6.4.11.

(i). We start by observing that $(r_1)^2 = cr_1 + d$ and $(r_2)^2 = cr_2 + d$. Define a sequence D_1, D_2, D_3, \dots by the explicit formula $D_n = P(r_1)^n + Q(r_2)^n$ for all n , where P and Q are given in the statement of the proposition. Suppose we could show that $D_1 = A_1$, that $D_2 = A_2$ and that $D_{n+2} = cD_{n+1} + dD_n$ for all $n \in \mathbb{N}$. It would then follow from the uniqueness in Theorem 6.4.5 that $D_n = A_n$ for all $n \in \mathbb{N}$, and the desired result would be proved.

We leave it to the reader to plug the given values of P and Q into the definition of D_1 and D_2 , and then verifying that $D_1 = A_1$, that $D_2 = A_2$. Now let $n \in \mathbb{N}$. We compute

$$\begin{aligned} cD_{n+1} + dD_n &= c(P(r_1)^{n+1} + Q(r_2)^{n+1}) + d(P(r_1)^n + Q(r_2)^n) \\ &= P(r_1)^n(cr_1 + d) + Q(r_2)^n(cr_2 + d) \\ &= P(r_1)^n(r_1)^2 + Q(r_2)^n(r_2)^2 \\ &= P(r_1)^{n+2} + Q(r_2)^{n+2} = D_{n+2}. \end{aligned}$$

This completes the proof. □

The following result about the Fibonacci numbers is a consequence of the above proposition, using $c = 1 = d$ and $F_1 = 1 = F_2$, and a bit of manipulation.

Corollary 6.4.8. *Let $n \in \mathbb{N}$. Then*

$$F_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right\}.$$

This explicit formula for the Fibonacci numbers 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 $(1 + \sqrt{5})/2$ and is often denoted ϕ , observe that Binet’s formula is $F_n = (1/\sqrt{5})\{\phi^n - (-1/\phi)^n\}$ for all $n \in \mathbb{N}$. See Exercise 6.4.13 for another relation between the Fibonacci numbers and the golden ratio. See [Hun70] for more on the golden ratio.

Exercises

6.4.1. Define a sequence by setting $r_1 = 1$ and $r_{n+1} = 4r_n + 7$ for all $n \in \mathbb{N}$. Prove that $r_n = \frac{1}{3}(10 \cdot 4^{n-1} - 7)$ for all $n \in \mathbb{N}$.

6.4.2. Define a sequence by setting $b_1 = b_2 = 1$ 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 $n \in \mathbb{N}$.

6.4.3. Define a sequence by setting $d_1 = 2$ 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.

6.4.4. [Used in Section 6.4.] Prove Proposition 6.4.6 (i) and (ii).

6.4.5. Let $n \in \mathbb{N}$.

- (1) Show that $2|F_n$ iff $3|n$.
- (2) Show that $3|F_n$ iff $4|n$.
- (3) Show that $4|F_n$ iff $6|n$.

6.4.6. Let $n \in \mathbb{N}$ be such that $n > 5$. Show that $F_n = 5F_{n-4} + 3F_{n-5}$.

6.4.7. Show that the integer $5(F_n)^2 + 4(-1)^n$ is a perfect square for all $n \in \mathbb{N}$.

6.4.8. Let $n, k \in \mathbb{N}$ be such that $k \geq 2$. Show that each of the following hold.

- (1) $F_{n+k} = F_k F_{n+1} + F_{k-1} F_n$.
- (2) $F_n | F_{kn}$.

6.4.9. Define a sequence by setting $G_1 = G_2 = 1$ and $G_{n+2} = G_{n+1} + G_n + G_{n+1}G_n$ for all $n \in \mathbb{N}$. Prove that $G_n = 2^{F_n} - 1$ for all $n \in \mathbb{N}$.

6.4.10. Let $\phi = (1 + \sqrt{5})/2$ and $\phi' = (1 - \sqrt{5})/2 = -1/\phi$. Show that $\phi^n + \phi'^n$ is an integer for all $n \in \mathbb{N}$.

6.4.11. Prove Proposition 6.4.7 (ii).

6.4.12. We discuss a curious geometric puzzle; see [Wea38] for more details of the history of this puzzle. Start with a square whose sides are 13 units long. 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?

(1) Explain the puzzle by showing that there is a slight overlap among the pieces.

(2) Let us 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

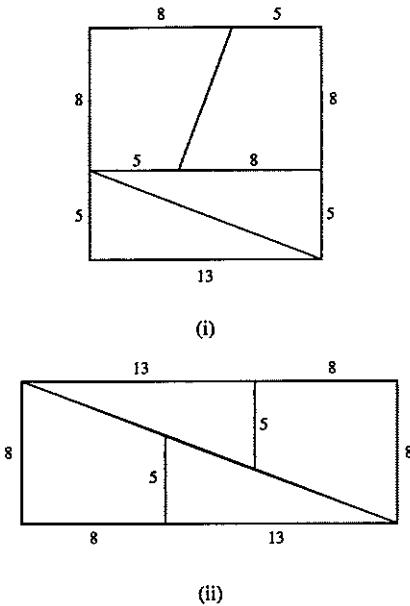


Figure 6.4.2.

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). Suppose we want a puzzle with a and b both positive integers (as is the case in the original puzzle). Since the areas of both the square and rectangle will be integers, so will the difference of these areas, which is the amount of overlap or underlap. Thus with a and b both positive integers, 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. Show that if a and b are consecutive Fibonacci numbers, then the overlap or underlap is minimal. Note that the original puzzle did have consecutive Fibonacci numbers. (It can be shown that no numbers other than two consecutive Fibonacci numbers have minimal overlap or underlap, but that is harder.)

6.4.13. This exercise is for the reader who is familiar with limits. We saw in Corollary 6.4.8 that the Fibonacci numbers can be computed using the number $\phi = (1 + \sqrt{5})/2 = 1.618\dots$. 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

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \dots$$

A calculation of some of the terms in this sequence shows that they approach the number $1.618\dots$, which looks suspiciously like ϕ , at least up to a few decimal places. Stated precisely, our result is indeed

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \phi.$$

Show that this equation holds. There are two separate parts to this problem: (1) to show that the limit exists; (2) that the limit equals ϕ . Try to prove the latter part (which is simpler) assuming that the former part is true, even if you have not proved the former part. (To show that the limit exists is more advanced, requiring a knowledge of Cauchy sequences, and the completeness of the real numbers.)

6.4.14. This exercise concerns “figurative” numbers, which are various sequences of natural numbers that correspond to certain geometric patterns of points in the plane. These numbers were of interest to the ancient Greeks; see [Fle83] for more details. A typical example are the triangular numbers, which are $1, 3, 6, 10, 15, \dots$, and correspond to the points in the triangles shown in Figure 6.4.3. Sequences of figurative numbers can be given for various shapes. Though such numbers have pictorial meaning, the more rigorous way to define them is recursively, as we do below; the pictures corresponding to a few of these definition are shown in Figure 6.4.3.

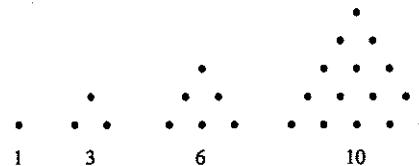
- (a) Linear Numbers: the sequence L_1, L_2, L_3, \dots given by $L_1 = 1$ and $L_{n+1} = L_n + 1$ for all $n \in \mathbb{N}$.
- (b) Triangular Numbers: the sequence T_1, T_2, T_3, \dots given by $T_1 = 1$ and $T_{n+1} = T_n + (n + 1)$ for all $n \in \mathbb{N}$.
- (c) Square Numbers: the sequence S_1, S_2, S_3, \dots given by $S_1 = 1$ and $S_{n+1} = S_n + (2n + 1)$ for all $n \in \mathbb{N}$.
- (d) Pentagonal Numbers: the sequence P_1, P_2, P_3, \dots given by $P_1 = 1$ and $P_{n+1} = P_n + (3n + 1)$ for all $n \in \mathbb{N}$.
- (e) Rectangular Numbers: the sequence R_1, R_2, R_3, \dots given by $R_1 = 2$ and $R_{n+1} = R_n + (2n + 2)$ for all $n \in \mathbb{N}$.
- (f) Cubical Numbers: the sequence C_1, C_2, C_3, \dots given by $C_1 = 1$ and $C_{n+1} = C_n + (3n^2 + 3n + 1)$ for all $n \in \mathbb{N}$.

There are now two parts to this exercise.

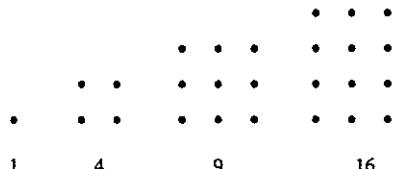
(1) Without finding explicit formulas for the above sequences, prove that the following equations hold for all $n \in \mathbb{N}$.

$$\begin{array}{ll} \text{(i)} P_n = 3T_n - 2L_n. & \text{(iii)} S_{n+1} = T_{n+1} + T_n. \\ \text{(ii)} 8T_n + 1 = (2n + 1)^2. & \text{(iv)} S_n + C_n = nR_n. \end{array}$$

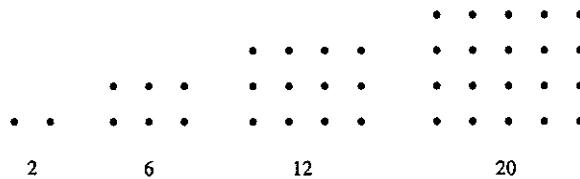
(2) Find an explicit formula for each of the sequences (a) – (f), and prove that these formulas are correct using only the definitions in (a) – (f).



Triangular Numbers



Square Numbers

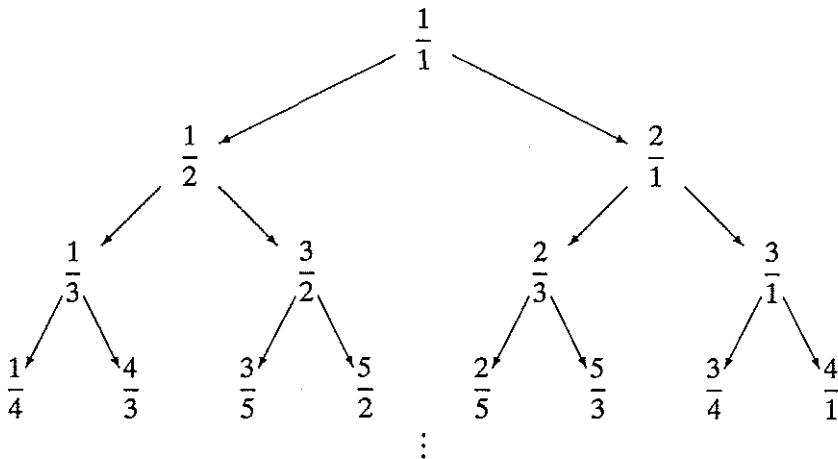


Rectangular Numbers

Figure 6.4.3.

6.4.15. [Used in Section 6.2.] In Theorem 6.2.1 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} . The picture after the proof of the theorem showed the well-known way of lining up the positive rational numbers, due to Cantor. In this picture, we lined up the positive rational numbers by following the arrows, and by 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 thus avoiding the need to drop repeated numbers as in Cantor's procedure. (This method is due to Jim Reid, and is also touched upon in [Alp99].) A picture for the new approach is as follows.



The diagram is constructed recursively by starting with $1/1$, 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 a/b in the previous row and obtaining $a/(a+b)$ and $(a+b)/b$. We will prove below that each possible 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

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, \frac{3}{1}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, \frac{4}{1}, \dots$$

To prove that this procedure works, it is easier to use ordered pairs of positive integers of the form (a, b) , rather than fractions of the form a/b . We note that the fraction a/b is in lowest terms iff 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

$$\mathbb{L} = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ and } b \text{ are relatively prime}\},$$

and let $U, D: \mathbb{L} \rightarrow \mathbb{L}$ 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 $A_0, A_1, A_2, \dots \subseteq \mathbb{L}$ as follows. For each $n \in \mathbb{Z}^{nn}$, the set A_n will have 2^n elements, labeled as

$$A_n = \{a_n^1, a_n^2, \dots, a_n^{2^n}\}.$$

We define these elements recursively as follows. Let $a_0^1 = (1, 1)$. 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 $a_{n+1}^{2k-1} = D(a_n^k)$ and $a_{n+1}^{2k} = U(a_n^k)$ for all $k \in \{1, \dots, 2^n\}$. It is seen that this recursive definition captures the procedure given in the above picture.

To prove our desired result, we will show that

$$\bigcup_{i=0}^{\infty} A_i = \mathbb{L},$$

and that there are no redundancies among the elements of the form a_i^x . More precisely, for each $n \in \mathbb{Z}^{nn}$, let $S_n = \bigcup_{i=0}^n A_i$. It will suffice to show that the following two claims hold for all $n \in \mathbb{Z}^{nn}$.

- (1) The set S_n contains all $(a, b) \in \mathbb{L}$ such that $1 \leq a, b \leq n$.
- (2) All the elements in S_n are distinct. That is, we have $a_i^x = a_j^y$ iff $i = j$ and $x = y$, for all $i, j, x, y \in \mathbb{Z}^{nn}$, such that $0 \leq i, j \leq n$, that $1 \leq x \leq 2^i$ and that $1 \leq y \leq 2^j$.

Prove both these claims. (Make use of 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 are from important areas of modern mathematics, and because they make use of the concepts we have learned so far. Due to space limitations, we are a bit more terse in this part of the text than previously. In each section of Chapter 7 we give a very brief introduction to a particular topic, touching only the tip of the iceberg in each case. Sections 7.1–7.3 deal with subjects from abstract algebra, Sections 7.4–7.5 deal with order, and Sections 7.6–7.7 deal with combinatorics. In Chapter 8 we have a more extended discussion, in which we give an axiomatic treatment of some of the standard number systems (the natural numbers, the integers and the rational numbers). The material in this chapter is, in part, rather abstract (and sometimes dry), but is extremely worthwhile. Not only should every student of mathematics be aware of how our standard number systems are constructed, but these constructions involve a good bit of the material treated in this book. As such, it is an appropriate finale for the material we present. In Chapter 9 we let the reader take over. In each section of that chapter, we briefly introduce a topic, which the reader is then urged to explore on his or her own.

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 –)

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. Let A be a set. A **binary operation** on A is a map $A \times A \rightarrow A$. A **unary operation** on A is a map $A \rightarrow A$. Δ

Let A be a set, and let $* : A \times A \rightarrow A$ 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 not be proving any theorems about binary operations in this section, since 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. Binary operations, and the properties we define, will be used throughout this chapter and the next.

Example 7.1.1.

(1) Addition is a binary operation on \mathbb{N} . Because the sum of any two natural numbers is a natural number, we can think of addition on \mathbb{N} as a map $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$. Subtraction is not a binary operation on \mathbb{N} , since the difference of two natural numbers is not always a natural number. However, subtraction is a binary operation on \mathbb{Z} .

(2) Let $GL_2(\mathbb{R})$ denote the set of invertible 2×2 matrices with real number entries. Such matrices are precisely those with non-zero determinant. Let \cdot denote matrix multiplication. Then \cdot is a binary operation on $GL_2(\mathbb{R})$, since 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 $GL_2(\mathbb{R})$, since two matrices with non-zero determinant could add up to a matrix with zero determinant (the reader should supply an example). See [AR94, Chapter 1] for more information about matrix operations.

(3) Just as multiplication of integers 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 using the operation table

\star	p	q	r
p	r	p	q
q	p	q	r
r	r	r	p

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). The binary operation \star is only one of many possible binary operations on Z . Any table using the elements of Z as entries will define a binary operation on Z . \diamond

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 any $x, y \in \mathbb{R}$.

Definition. Let A be a set and let $*$ be a binary operation on A . The binary operation $*$ satisfies the **commutative law** (or is **commutative**) if $a * b = b * a$ for all $a, b \in A$. Δ

Example 7.1.2.

(1) The binary operations addition and multiplication on \mathbb{Z} are both commutative. The binary operation subtraction on \mathbb{Z} is not commutative, since for example $5 - 2 \neq 2 - 5$.

(2) Let $GL_2(\mathbb{R})$ and \cdot be as in Example 7.1.1 (2). The binary operation \cdot is not commutative. The reader should supply an example of two matrices $A, B \in GL_2(\mathbb{R})$ such that $A \cdot B \neq B \cdot A$. Some pairs of matrices in $GL_2(\mathbb{R})$ can be multiplied in either order without changing the result, for example $\begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 4 \end{pmatrix}$; however, since it is not the case that all pairs can be multiplied in either order without changing the result, we cannot say that \cdot is 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 7.1.1 (3) is not commutative, since $p \star r = q$ 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. (Conversely, an operation table that is symmetric with respect to the downward sloping diagonal always implies commutativity.) \diamond

The next property of binary operations generalizes the fact that $(x + y) + z = x + (y + z)$ for any $x, y, z \in \mathbb{R}$.

Definition. Let A be a set and let $*$ be a binary operation of A . The binary operation $*$ satisfies the **associative law** (or is **associative**) if $(a * b) * c = a * (b * c)$ for all $a, b, c \in A$. Δ

Example 7.1.3.

(1) The binary operations addition and multiplication on \mathbb{Z} are both associative. The binary operation subtraction on \mathbb{Z} is not associative, since for example $(5 - 2) - 1 \neq 5 - (2 - 1)$.

(2) The binary operation \star defined in Example 7.1.1 (3) is not associative, since $(r \star p) \star p = r \star p = r$, 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 various possible ways of combining three elements at a time simply need to be checked. \diamond

A very important use of associativity is that it allows us to combine three or more elements by a binary operation (which by definition only applies to two elements at a time). Suppose you had to calculate the sum $3 + 8 + 5$ in your head. Some people would mentally add 3 and 8, to obtain 11, and then add 5 to that, obtaining 16. Other people might first add 8 and 5, obtaining 13, and then add 3, obtaining 16. In other words, some people might do $(3 + 8) + 5$, whereas others might do $3 + (8 + 5)$. Of course, we obtained the same result by either method, since addition on \mathbb{Z} is associative. Given this associativity, it makes sense to write $3 + 8 + 5$, without fear of ambiguity. In general, 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, since it could be calculated as either $(a * b) * c$ or $a * (b * c)$. The same idea shows that we could combine any finite number of elements of G unambiguously using $*$. (This procedure does not necessarily allow us to combine infinitely many elements at once, however.)

Our next property of binary operations generalizes the unique role of the number 0 in relation to addition of numbers, namely that $x + 0 = x = 0 + x$ for all $x \in \mathbb{R}$.

Definition. Let A be a set and let $*$ be a binary operation of A . An element $e \in A$ is an **identity element** for $*$ if $a * e = a = e * a$ for all $a \in A$. If there is an identity element for $*$, we say that $*$ satisfies the **identity law**.

 Δ

Note that we need to specify both $a * e = a$ and $e * a = a$ for all $a \in A$ in the above definition, since we cannot assume that $*$ is commutative, and so knowing only one of these equations does not necessarily imply the other.

Example 7.1.4.

(1) The binary operation multiplication on \mathbb{N} has an identity element, namely 1, since $n \cdot 1 = n = 1 \cdot n$ for all $n \in \mathbb{N}$. The binary operation addition on \mathbb{N} does not have an identity element, since $0 \notin \mathbb{N}$. On the other hand, addition on \mathbb{Z} does have an identity element, namely 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 have $0 - n \neq n$ for all $n \in \mathbb{N}$ other than $n = 0$.

(2) Let $GL_2(\mathbb{R})$ and \cdot be as in Example 7.1.1 (2). The binary operation \cdot does have an identity element, namely the identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(3) The binary operation \star defined in Example 7.1.1 (3) has an identity element, namely q . This fact can be verified directly by checking all possibilities, for example $p \star q = p$ and $q \star p = p$, etc. 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 similarly for the row to the left of q .

(4) Let $T = \{k, m, n\}$ and let \diamond be the binary operation given 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. Although it is true that $n \diamond k = n$, we see that $k \diamond n \neq n$, and both of these equalities would have to hold if k were the identity element. It is easily seen that no element other than k could be the identity element with respect to \diamond . \diamond

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 “cancels out” the original number. That is, we have $x + (-x) = 0 = (-x) + x$ for any $x \in \mathbb{R}$. 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. Let A be a set and let $*$ be a binary operation of A . Let e be an identity element for $*$. If $a \in A$, then an **inverse** for a is an element $a' \in A$ such that $a * a' = e = a' * a$. If every element in A has an inverse, we say that $*$ satisfies the **inverses law**. Δ

As in the definition of identity elements, we need to specify both $a * a' = e$ and $a' * a = e$ for all $a \in A$, since we cannot assume that $*$ is commutative.

Example 7.1.5.

(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, since 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 7.1.1 (2). Every element of $GL_2(\mathbb{R})$ has an inverse, since $GL_2(\mathbb{R})$ 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 $A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = B \cdot A$.)

(3) Let $H = \{a, b, c, d, e\}$ and let $*$ be the binary operation given 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 . Also, we have $c * b = e = b * c$, so b is an inverse of c , and c is an inverse of b . Thus 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. Although $a * d = e$, we have $d * a \neq e$, and both equalities would have to hold for a to be the inverse of d . \diamond

Exercises

7.1.1. Which of the following formulas defines a binary operation on the given set?

- (1) Let $*$ be given by $x * y = xy$ for all $x, y \in \{-1, -2, -3, \dots\}$.
- (2) Let \diamond be given by $x \diamond y = \sqrt{xy}$ for all $x, y \in [2, \infty)$.
- (3) Let \oplus be given by $x \oplus y = x - y$ for all $x, y \in \mathbb{Q}$.
- (4) Let \circ be given 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 given by $x \odot y = |x + y|$ for all $x, y \in \mathbb{N}$.
- (6) Let \otimes be given by $x \otimes y = \ln(|xy| - e)$ for all $x, y \in \mathbb{N}$.

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} given by $x \oplus y = -xy$ for all $x, y \in \mathbb{Z}$.

- (2) The binary operation \star on \mathbb{R} given by $x \star y = x + 2y$ for all $x, y \in \mathbb{R}$.
 (3) The binary operation \otimes on \mathbb{R} given by $x \otimes y = x + y - 7$ for all $x, y \in \mathbb{R}$.
 (4) The binary operation $*$ on \mathbb{Q} given by $x * y = 3(x + y)$ for all $x, y \in \mathbb{Q}$.
 (5) The binary operation \circ on \mathbb{R} given by $x \circ y = x$ for all $x, y \in \mathbb{R}$.
 (6) The binary operation \diamond on \mathbb{Q} given by $x \diamond y = x + y + xy$ for all $x, y \in \mathbb{Q}$.
 (7) The binary operation \odot on \mathbb{R}^2 given by $(x, y) \odot (z, w) = (4xz, y + w)$ for all $(x, y), (z, w) \in \mathbb{R}^2$.

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.)

\otimes		1	2	3
1	1	2	1	
2	2	3	2	
3	1	2	3	

\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

\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	

\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

$*$		x	y	z	w
x	x	z	w	y	
y	z	w	y	x	
z	w	y	x	z	
w	y	x	z	w	

7.1.4. Let $n \in \mathbb{N}$. Recall the definition of the set \mathbb{Z}_n and the binary operation multiplication (denoted \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 $a \in \mathbb{Z}$. Show that the following are equivalent.

- (1) The element $[a] \in \mathbb{Z}_n$ has an inverse element with respect to multiplication.
- (2) The equation $ax \equiv 1 \pmod{n}$ has a solution.
- (3) There exist $p, q \in \mathbb{Z}$ such that $ap + nq = 1$.

(Although it is not trivial to prove, it turns out that the three conditions listed above are equivalent to the fact that a and n are relatively prime, that is, they have no common factors other than 1 and -1 .)

7.1.5. Let A be a set. A **ternary operation** on A is a map $A \times A \times A \rightarrow A$. A ternary operation $\star: A \times A \times A \rightarrow A$ is **left-induced** by a binary operation $\diamond: A \times A \rightarrow A$ 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. 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 the above definition, since the empty set satisfies all three properties (even the identity law, since 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 all groups have at least one element.

The associative law is often quite tedious to check (simply involving trying each possibility), and in all the examples and exercises concerning groups that we give, the reader may assume that associativity holds. Notice the lack of a requirement of commutativity in the definition of a group. Though associativity may appear at first to be more obscure than commutativity, there turn out to be a number of important examples where the

former holds but the latter does not. See for instance Example 7.2.1 (3). Groups that do satisfy the commutative property are particularly nice to work with, and merit a special name.

Definition. Let $(G, *)$ be a group. We say that $(G, *)$ is an **abelian group** if $*$ satisfies the commutative law. \triangle

Groups are relatively recent by mathematical standards (having arisen in the 19th century), but they are now important in a wide variety of areas of both pure and applied mathematics, having applications in such diverse areas as geometry, algebraic topology, quantum mechanics and crystallography. The latter makes use of the centrality of groups in the rigorous study of symmetry. See [Fra94] 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 [LP98, Chapter 6] for some applications of group theory. Our discussion of groups, in this section and the next, is only the smallest tip of the iceberg.

The term “group” is one of those words that has a standard colloquial meaning, and that mathematicians have also given a technical meaning that has little to do with the colloquial usage. The term “abelian” is in honor of the Norwegian 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 often simply say “Let G be a group.” If we are discussing more than one group, we will write things like “ e_G ” if we need to specify to which group an identity element belongs.

Example 7.2.1.

(1) The pair $(\mathbb{Z}, +)$ is an abelian group. That the four necessary properties hold can be seen by combining Examples 7.1.3 (1), 7.1.4 (1), 7.1.5 (1) and 7.1.2 (1). Similarly, it is seen that $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are abelian groups, as are $(\mathbb{Q} - \{0\}, \cdot)$ and $(\mathbb{R} - \{0\}, \cdot)$.

(2) Let $\{e\}$ be a single element set, and let $*$ be the only possible binary operation on $\{e\}$, namely $e * e = e$. It is simple to verify that $(\{e\}, *)$ is an abelian group. We call this group the **trivial group**. Any two single element groups, while perhaps labeled differently, are essentially identical (as discussed more precisely in Example 7.3.6 (2)).

(3) Let $GL_2(\mathbb{R})$ and \cdot be as in Example 7.1.1 (2). Then $(GL_2(\mathbb{R}), \cdot)$ is a group, but not an abelian group. The associativity of \cdot is a well known property of matrix multiplication (see [AR94, Section 1.4]). That the Iden-

tity Law and Inverses Law hold is discussed in Examples 7.1.4 (2) and 7.1.5 (2). The non-commutativity of \cdot is discussed in Example 7.1.2 (2).

(4) One way of presenting a group with finitely many elements is to give its binary operation by an operation table, as discussed in Example 7.1.1 (3). For example, 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 leave that to the ambitious reader. It is seen that e is the identity element. Further, the elements e and b are each their own inverses, and a and c are inverses to each other. Hence (V, \circ) is a group. It is easy to verify that \circ is commutative, since the operation table for this binary operation is symmetric along the downward sloping diagonal. Hence (V, \circ) is an abelian group.

(5) The pair $(Z, *)$ given in Example 7.1.1 (3) is not a group. Although $*$ does have an identity element (namely q), this binary operation is not associative, as discussed in Example 7.1.3 (2), 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 (which we do not have room for at present). We will discuss 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 required that the identity element be unique, and that each element have a unique inverse. The following theorem shows, however, that uniqueness in both these cases holds automatically.

Theorem 7.2.2. *Let $(G, *)$ be a group.*

- (i) *The group G has a unique identity element.*
- (ii) *If $g \in G$, then g has a unique inverse.*

Proof. We prove part (i), leaving part (ii) to the reader in Exercise 7.2.6.

(i). Suppose that e and \hat{e} are both identity elements of G . 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. Thus the identity element is unique. \square

By the above theorem, we can now refer to “the identity element” of a group, and “the inverse” of a given element of the group. Part (ii) of the lemma says that if $(G, *)$ is a group, and if $a, b \in G$ are such that $a * b = e = b * a$, then $b = a'$. We will use this idea in the proof of Theorem 7.2.3 (iv).

We now prove some standard properties of groups. These properties generalize some familiar properties of groups such as $(\mathbb{Z}, +)$.

Theorem 7.2.3. *Let $(G, *)$ be a group and let $a, b, c \in G$.*

(i) *If $a * c = b * c$, then $a = b$.*

(ii) *If $c * a = c * b$, then $a = b$.*

(iii) *$(a')' = a$.*

(iv) *$(a * b)' = b' * a'$.*

Proof. We prove part (iv), leaving the other parts to the reader in Exercise 7.2.7.

(iv). By Theorem 7.2.2 (ii) we know that $a * b$ has a unique inverse. If we can show that $(a * b) * (b' * a') = e = (b' * a') * (a * b)$, then it will follow that $a' * b'$ is the unique inverse for $a * b$, which implies that $(a * b)' = b' * a'$. To prove our result, we make repeated use of the properties in the definition of a group by computing

$$\begin{aligned}(a * b) * (b' * a') &= [(a * b) * b'] * a' = [a * (b * b')] * a' \\ &= [a * e] * a' = a * a' = e.\end{aligned}$$

A similar computation shows that $(b' * a') * (a * b) = e$. \square

Parts (i) and (ii) of the above theorem are the familiar cancellation property. We need both parts of the proposition, since not all groups are abelian. Using the cancellation property, it can be shown that if a 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 and once and only once in each column (consider what would happen otherwise). We could thus spot instantly that (T, \diamond) in Example 7.1.4 (4) is not

a group (even had we not known from our discussion of this example that there is no identity element), since 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 in each column does not guarantee that the operation yields a group. The reader is asked in Exercise 7.2.5 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. Let $(G, *)$ be a group, and let $A \subseteq G$. We say that A is a subgroup of G if the following two conditions hold.

(1) If $a, b \in A$, then $a * b \in A$.

(2) $(A, *)$ is a group. △

In the above definition, note that since $(A, *)$ is itself a group, it must be non-empty, since we are assuming all groups are non-empty. Part (1) of the definition says that $*$ is a binary operation on A . 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 7.2.4. *Let $(G, *)$ be a group and let $A \subseteq G$ be a non-empty set. Then A is a subgroup of G iff the following two conditions hold.*

(1) *If $a, b \in A$ then $a * b \in A$.*

(2) *If $a \in A$ then $a' \in A$.*

Proof. First suppose that A is a subgroup. Then property (1) holds by the definition of a subgroup. We will show that property (2) holds. Let e be the identity element of G . Since $(A, *)$ is a group, it has an identity element, say \hat{e} . (Until we prove it, we cannot assume a priori that \hat{e} is the same as e .) Choose some $b \in A$. Then $\hat{e} * b = b = e * b$, first thinking of b as being in A , and then thinking of it as being in G . Since both \hat{e} and e are in G , we can use Theorem 7.2.3 (i) to deduce that $\hat{e} = e$.

Now let $a \in A$. Since $(G, *)$ is a group, the element a has an inverse $a' \in G$. We will show that $a' \in A$. Since $(A, *)$ is a group, then a has an inverse $\hat{a} \in A$. (Until we prove it, we cannot assume a priori that \hat{a} is the same as a' .) Using the definition of inverses, and what we saw in the previous paragraph, we know that $a * a' = e = a' * a$ and $a * \hat{a} = e = \hat{a} * a$.

Hence $\hat{a} * a = a' * a$. Again using Theorem 7.2.3 (i), we deduce that $a' = \hat{a}$. Since $\hat{a} \in A$, it follows that $a' \in A$. Thus property (2) of the theorem holds.

Now suppose that A satisfies properties (1) and (2). To show that A is a subgroup, we will have to show that $(A, *)$ 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 A . Since A is non-empty, choose some $b \in A$. By property (2) we know that $b' \in A$. By property (1) we deduce that $e = b' * b \in A$. Since e is the identity element for all the elements of G , it is certainly the identity element for all the elements of A . By property (2) we now know that every element of A has an inverse in A . Thus A is a group. \square

The following corollary can be deduced immediately from the proof of the above theorem.

Corollary 7.2.5. *Let G be a group, and let A be a subgroup of G . Then the identity element of G is in A , and it is the identity element of A . The inverse operation in A is the same as the inverse operation in G .*

Example 7.2.6.

- (1) The group $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$, which in turn is a subgroup of $(\mathbb{R}, +)$.
- (2) Let $(G, *)$ be any group. Let e be the identity element of G . Then $\{e\}$ and G are both subgroups of G . The subgroup $\{e\}$ is often referred to as the **trivial subgroup** of G .
- (3) Let (V, \circ) be as in Example 7.2.1 (4). By checking all possibilities, we find that the only subgroups of V are $\{e\}$, $\{e, b\}$ and V . \diamond

We conclude this section with a very brief example of the relation between group theory and the study of symmetry. 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 is an isometry of the plane (that is, a motion that does not change lengths between points) that leave the appearance of the triangle unchanged. See [Rya86] for more about isometries. It is permissible that these isometries interchange the letters used to label the triangle, since these letters are not actually part of the triangle. There are only two types of isometries that will leave the triangle looking unchanged: reflections (that is, flips) in certain lines and rotations about the center of the triangle by certain angles. In Figure 7.2.1 (ii) are indicated the three possible lines about which the triangle can be reflected

without changing its appearance. Denote the reflections through these lines by M_1 , M_2 and M_3 . For example, if we apply M_2 to the triangle as pictures in Figure 7.2.1 (i), we see that M_2 leaves the vertex labeled C unmoved, and interchanges the vertices labeled A and B ; see Figure 7.2.1 (iii). The only two possible rotations that leave the triangle looking unchanged are rotation by 120° clockwise and rotation by 240° clockwise, denoted R_{120} and R_{240} . We let I denote the isometry of the plane that does not move anything.

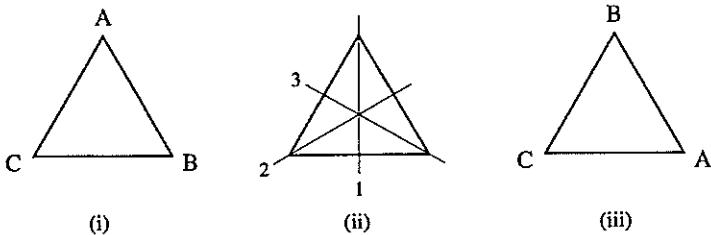


Figure 7.2.1.

The set $G = \{I, R_{120}, R_{240}, M_1, M_2, M_3\}$ is the collection of all isometries of the equilateral triangle. Each of these isometries is a function $\mathbb{R}^2 \rightarrow \mathbb{R}^2$, 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 thus composition becomes a binary operation on the set G . (We could also use brute force to check all 36 possible ways of forming compositions of pairs of these six isometries, and we would see that composition is a binary operation.) We can then form the operation table

\circ	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

The operation of composition of functions is associative in general, as proved in Lemma 4.3.3 (i), and thus this binary operation 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 each other's inverse. Thus (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 $\{I, R_{120}, R_{240}\}$, $\{I, M_1\}$, $\{I, M_2\}$, $\{I, M_3\}$.

The group G is referred to as the symmetry group of the equilateral triangle. Any object in Euclidean space has a symmetry group, though many such groups are substantially more complicated than our simple example. Since groups have been widely studied by mathematicians, it turns out that quite a lot can be proved about symmetry groups. Group theory has been used to obtain rather surprising results about the symmetries of ornamental patterns such as frieze and wallpaper patterns. See [Arm88] or [Bur85] for more about symmetry groups.

Exercises

7.2.1. Which of the following sets and binary operations form groups? Which of the groups are abelian?

- (1) The binary operation multiplication on $(0, 1]$.
- (2) The binary operation multiplication on the set of positive rational numbers.
- (3) The binary operation addition on the set of even integers.
- (4) The binary operation multiplication on the set of even integers.
- (5) The binary operation $*$ on \mathbb{Z} given by $a * b = a - b$ for all $a, b \in \mathbb{Z}$.
- (6) The binary operation \star on \mathbb{Z} given by $a \star b = ab + a$ for all $a, b \in \mathbb{Z}$.
- (7) The binary operation \diamond on \mathbb{Z} given by $a \diamond b = a + b + 1$ for all $a, b \in \mathbb{Z}$.
- (8) The binary operation \odot on $\mathbb{R} - \{-1\}$ given by $a \odot b = a + b + ab$ for all $a, b \in \mathbb{R} - \{-1\}$.

7.2.2. For each of the following binary operations given by operation tables, state whether the binary operation together with the set it acts upon forms a group. Which of the groups are abelian?

*	x	y	z
x	x	y	z
y	y	z	x
z	z	x	z

*	j	k	l	m
j	k	j	m	l
k	j	k	l	m
l	m	l	k	j
m	l	m	j	k

◊	1	2	3
1	3	1	2
2	1	2	3
3	2	3	1

7.2.3. Let A be a set. Define the binary operation Δ on $\mathcal{P}(A)$ by $X \Delta Y = (X - Y) \cup (Y - X)$ for all $X, Y \in \mathcal{P}(A)$. Show that $(\mathcal{P}(A), \Delta)$ is an abelian group.

7.2.4. Let $P = \{a, b, c, d, e\}$. Make up a binary operation $*$ on P so that $(P, *)$ is a group.

7.2.5. [Used in Section 7.2.] Find a binary operation given by an operation table such that each element of the set acted upon by the binary operation appears once and only once in each row and each column, but the set together with this binary operation is not a group.

7.2.6. [Used in Section 7.2.] Prove Theorem 7.2.2 (ii).

7.2.7. [Used in Section 7.2.] Prove Theorem 7.2.3 parts (i) – (iii).

7.2.8. [Used in Section 2.1.] 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 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 $*$ (this identity element is unique, by the same proof as for Theorem 7.2.2 (i)). Show that $*$ satisfies the inverses law, and hence $(A, *)$ is a group.

7.2.9. Let $(G, *)$ be a group. Show that the following are equivalent.

- (1) G is abelian.
- (2) $aba'b' = e$ for all $a, b \in G$.
- (3) $(ab)^2 = a^2b^2$ for all $a, b \in G$.

7.2.10. Let $(G, *)$ be a group. Suppose that $K \subseteq H \subseteq G$. Show that if K is a subgroup of H , and H is a subgroup of G , then K is a subgroup of G .

7.2.11. Let $\text{GL}_2(\mathbb{R})$ and \cdot be as in Example 7.1.1 (2). Let $\text{SL}_2(\mathbb{R})$ denote the set of all 2×2 matrices with real entries that have determinant 1. Show that $\text{SL}_2(\mathbb{R})$ is a subgroup of $\text{GL}_2(\mathbb{R})$.

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) Show that $(\mathbb{Z}_n, +)$ is an abelian group.
- (2) Suppose that n is not a prime number, and that $a, b \in \mathbb{N}$ are such that $n = ab$ and $1 < a < n$. Show that the set $\{[0], [a], [2a], \dots, [(b-1)a]\}$ is a subgroup of \mathbb{Z}_n .

(3) Is $(\mathbb{Z}_n - \{[0]\}, \cdot)$ a group? If not, can you find any conditions on n that would guarantee that $(\mathbb{Z}_n - \{[0]\}, \cdot)$ is a group?

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?

7.2.14. Describe the symmetry group of a square, similar to our description of the symmetry group of an equilateral triangle. (The symmetry group of a square has eight elements). Find all the subgroups of this symmetry group.

7.3 Homomorphisms and Isomorphisms

What does it mean for two groups to be “the same”? Consider the group (V, \circ) in Example 7.2.1 (4). We form a new group (W, \diamond) , where $W = \{I, F, G, H\}$, and where \diamond is given by the same operation table as \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 maps between groups. Such maps need to be bijective, and must “preserve the group operation.” This latter notion is meaningful even for non-bijective maps, and we start by making it precise in the following definition.

Definition. Let $(G, *)$ and (H, \diamond) be groups, and let $f: G \rightarrow H$ be a map. The map f is a **group homomorphism** (or just **homomorphism**) if $f(a * b) = f(a) \diamond f(b)$ for all $a, b \in G$. \triangle

Example 7.3.1.

(1) Let us examine maps from $(\mathbb{Z}, +)$ to $(\mathbb{Q}, +)$. Define $f: \mathbb{Z} \rightarrow \mathbb{Q}$ by $f(n) = n/3$ for all $n \in \mathbb{Z}$. If $n, m \in \mathbb{Z}$, then $f(n+m) = (n+m)/3 = n/3 + m/3 = f(n) + f(m)$. Hence f is a homomorphism. Define $g: \mathbb{Z} \rightarrow \mathbb{Q}$ 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 $g(n) + g(m) = n^2 + m^2$. Thus $g(n+m)$ is not always equal to $g(n) + g(m)$, so g is not a homomorphism.

(2) It is straightforward to verify that (\mathbb{R}^+, \cdot) is a group, where \mathbb{R}^+ denotes the set of positive real numbers. The function $g: \mathbb{R} \rightarrow \mathbb{R}^+$, defined by $h(x) = e^x$ for all $x \in \mathbb{R}$ is a homomorphism from $(\mathbb{R}, +)$ to (\mathbb{R}^+, \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 7.2.1 (4). Define $k: V \rightarrow V$ 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 $x * y \in \{e, b\}$, and hence $k(x) = e = k(y)$ and $k(x * y) = e$. It follows that $k(x * y) = e = e \circ e = k(x) \circ k(y)$. 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 $k(y) = b = k(x \circ y)$. It follows that $k(x \circ y) = b = e \circ b = k(x) \circ k(y)$. The other two cases, namely $x \in \{a, c\}$ and $y \in \{e, b\}$, or $x, y \in \{a, c\}$, are similar, and we leave the details to the reader. \diamond

Homomorphisms of groups preserve the basic group structure, namely the group operation. The following theorem shows that a group homomorphism also preserves some of the other features of groups.

Theorem 7.3.2. *Let G, H be groups, and let $f : G \rightarrow H$ be a homomorphism. Let e_G and e_H be the identity elements of G and H respectively.*

- (i) $f(e_G) = e_H$.
- (ii) If $a \in G$, then $f(a') = [f(a)]'$, where the first inverse is in G , and the second is in H .
- (iii) If $A \subseteq G$ is a subgroup of G , then $f_*(A)$ is a subgroup of H .
- (iv) If $B \subseteq H$ is a subgroup of H , then $f^*(B)$ is a subgroup of G .

Proof. We will prove parts (ii) and (iii), leaving the other parts to the reader in Exercise 7.3.6. Let $*$ and \diamond be the binary operations of G and H respectively.

(ii). Let $a \in G$. Then we compute that $f(a) \diamond f(a') = f(a * a') = f(e_G) = e_H$, where the last equality uses part (i) 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 Theorem 7.2.2 (ii), it follows that $[f(a)]' = f(a')$.

(iii). By Corollary 7.2.5 we know that $e_G \in A$, and by part (i) of the present theorem we know that $e_H \in f_*(A)$. Thus $f_*(A)$ is non-empty, and so we can use Theorem 7.2.4 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. Since A is a subgroup of G we know that $a * b \in A$. Hence $x \diamond y \in f_*(A)$. Using part (ii) of this theorem, we see that $x' = [f(a)]' = f(a')$. Since A is a subgroup of G , it follows from property (2) of Theorem 7.2.4 that $a' \in A$. Hence $x' \in f_*(A)$. Thus $f_*(A)$ is non-empty and satisfies both properties of Theorem 7.2.4, and so it 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 homomorphisms.

Theorem 7.3.3. *Let G , H and K be groups, and let $f: G \rightarrow H$ and $j: H \rightarrow K$ 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. Let G and H be groups, and let $f: G \rightarrow H$ be a homomorphism. Let e_H be the identity element of H . The **kernel** of f , denoted $\ker f$, is the set $\ker f = f^*(\{e_H\})$. Δ

Note that if $f: G \rightarrow H$ is a homomorphism, then by Theorem 7.3.2 (iv) we know that $\ker f$ is always a subgroup of G , since $\{e_H\}$ is a subgroup of H .

Example 7.3.4.

(1) Let g be as in Example 7.3.1 (2). The identity element of the group (\mathbb{R}^+, \cdot) is 1. Then $\ker g = g^*(\{1\}) = \{0\}$.

(2) Let k be as in Example 7.3.1 (3). Then $\ker k = k^*(\{e\}) = \{e, b\}$. This kernel is indeed a subgroup of V . We also compute that $k^*(\{a\}) = \emptyset = k^*(\{c\})$, and that $k^*(\{b\}) = \{a, c\}$. None of these three inverse images are subgroups of V . \diamond

In part (1) of the above example we had an injective map, and the kernel was the trivial subgroup; in part (2) of the example we had a non-injective map, and the kernel was non-trivial. The following theorem shows that this correlation between injectivity of homomorphisms and triviality of kernels always hold. The kernel thus yields an easy way to tell whether or not a homomorphism is injective. To tell whether an arbitrary map $f: A \rightarrow B$ of sets is injective, it would be both necessary and sufficient to verify that $f^*(\{b\})$ 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.

Theorem 7.3.5. *Let G and H be groups, and let $f: G \rightarrow H$ be a homomorphism. Let e_G be the identity element of G . The map f is injective iff $\ker f = \{e_G\}$.*

Proof. Suppose that f is injective. Since $f(e_G) = e_H$ by Theorem 7.3.2 (i), it follows from the injectivity of f that $\ker f = f^*(\{e_H\}) = \{e_G\}$.

Now suppose that $\ker f = \{e_G\}$. Let $a, b \in G$, and suppose that $f(a) = f(b)$. We will show that $a = b$; it will then follow that f is injective. We use Theorem 7.3.2 (ii) and the definition of homomorphisms to compute

$$f(b * a') = f(b) \diamond f(a') = f(a) \diamond [f(a)]' = e_H.$$

It follows that $b * a' \in f^*(\{e_H\}) = \ker f$. Since $\ker f = \{e_G\}$, we deduce that $b * a' = e_G$. A similar calculation shows that $a' * b = e_G$. By Theorem 7.2.2 (ii) we deduce that $(a')' = b$, and thus by Theorem 7.2.3 (iii) we see that $b = a$. \square

We can now define what we mean by saying that two groups are “essentially the same.”

Definition. Let G and H be groups, and let $f: G \rightarrow H$ be a map. We say that f is a **group isomorphism** (or just **isomorphism**) if it is a homomorphism and it is bijective. We say that G and H are **isomorphic** if there is an isomorphism $k: G \rightarrow H$. Δ

Example 7.3.6.

(1) Let $(\mathbb{E}, +)$ denote the even integers with addition. We claim that $(\mathbb{E}, +)$ and $(\mathbb{Z}, +)$ are isomorphic. Define $f: \mathbb{Z} \rightarrow \mathbb{E}$ by $f(n) = 2n$ for all $n \in \mathbb{Z}$. We leave it to the reader to verify that f is bijective. To show that f is a homomorphism, note that $f(n+m) = 2(n+m) = 2n+2m = f(n)+f(m)$ for all $n, m \in \mathbb{Z}$. Thus f is an isomorphism, and hence $(\mathbb{E}, +)$ and $(\mathbb{Z}, +)$ are isomorphic. The map f is not the only possible isomorphism $\mathbb{Z} \rightarrow \mathbb{E}$. The reader can verify that the map $g: \mathbb{Z} \rightarrow \mathbb{E}$ given by $g(n) = -2n$ for all $n \in \mathbb{Z}$ is also an isomorphism. In general, when two groups are isomorphic, there may be more than one isomorphism between the groups; to prove that two groups are isomorphic, it suffices to find one isomorphism between them.

(2) Any two trivial groups (as discussed in Example 7.2.1 (2)) are isomorphic. Let $(\{e\}, *)$ and $(\{u\}, \circ)$ be trivial groups. Define the map $g: \{e\} \rightarrow \{u\}$ by $g(e) = u$. Then $g(e * e) = g(e) = u = u \circ u = g(e) \circ g(e)$. Hence g is a homomorphism. Since g is clearly bijective, it is an isomorphism.

(3) Since there is always a bijective map between any two isomorphic groups, we deduce that two finite groups with different numbers of elements could not 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 given by the operation table

\diamond	1	x	y	z
1	1	x	y	z
x	x	1	z	y
y	y	z	1	x
z	z	y	x	1

It can be verified that (Q, \diamond) is a group. In Exercise 7.3.9 it is demonstrated that (Q, \diamond) is not isomorphic to the group (V, \circ) of Example 7.2.1 (4), even though both groups have four elements. Intuitively, these groups are different in that all four elements of Q are their own inverses, whereas in V only two elements (namely e and b) are their own inverses. \diamond

In part (3) of the above example we saw that there are at least two non-isomorphic groups with four elements. As discussed 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 any finite 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 more details. This question is beyond the scope of this brief section.

We conclude this section with the following theorem, which implies that the relation of “isomorphic” is an equivalence relation on the collection of all groups. In the statement of part (ii) of the theorem, the map f^{-1} is simply defined to be the inverse of the map f , since any bijective map has an inverse (by Theorem 4.4.3 (iii)); hence f^{-1} is defined without any regard to the fact that f is a homomorphism.

Theorem 7.3.7. *Let G , H and K be groups, and let $f: G \rightarrow H$ and $j: H \rightarrow K$ be isomorphisms.*

- (i) *The identity map $1_G: G \rightarrow G$ is an isomorphism.*
- (ii) *The map f^{-1} is an isomorphism.*
- (iii) *The map $j \circ f$ is an isomorphism.*

Proof. Left to the reader in Exercise 7.3.8. □

Exercises

7.3.1. Which of the following maps are homomorphisms? Which of the homomorphisms is an isomorphism? The groups \mathbb{R} and \mathbb{Q} in the following examples have addition as the binary operation, and \mathbb{R}^+ has multiplication as the binary operation.

- (1) Let $f: \mathbb{Q} \rightarrow \mathbb{R}^+$ be given by $f(x) = 5^x$ for all $x \in \mathbb{Q}$.
- (2) Let $k: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ be given by $k(x) = x^{-7}$ for all $x \in \mathbb{R}^+$.
- (3) Let $m: \mathbb{R} \rightarrow \mathbb{R}$ be given by $m(x) = x + 3$ for all $x \in \mathbb{R}$.
- (4) Let $g: \mathbb{R}^+ \rightarrow \mathbb{R}$ be given by $g(x) = \ln x$ for all $x \in \mathbb{R}^+$.
- (5) Let $h: \mathbb{R} \rightarrow \mathbb{R}$ be given by $h(x) = |x|$ for all $x \in \mathbb{R}$.

7.3.2. Let $(\text{GL}_2(\mathbb{R}), \cdot)$ be the group described in Example 7.1.1 (2). Show that the map $\det: \text{GL}_2(\mathbb{R}) \rightarrow \mathbb{R} - \{0\}$ is a homomorphism, where $\mathbb{R} - \{0\}$ has the binary operation multiplication. What is the kernel of this map?

7.3.3. (1) Let $j: \mathbb{Z}_4 \rightarrow \mathbb{Z}_3$ be given 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 map a homomorphism? If the map is a homomorphism, find the kernel.

(2) Let $k: \mathbb{Z}_6 \rightarrow \mathbb{Z}_3$ be given by $k([x]) = [x]$ for all $[x] \in \mathbb{Z}_6$. Is this map a homomorphism? If the map is a homomorphism, find the kernel.

(3) Can you find criteria on $n, m \in \mathbb{N}$ that will determine when the map $r: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ given by $r([x]) = [x]$ for all $[x] \in \mathbb{Z}_n$ is a homomorphism? Prove your claim. Find the kernel for those maps that are homomorphisms.

7.3.4. Let G and H be groups. Show that the projection maps $\pi_1: G \times H \rightarrow G$ and $\pi_2: G \times H \rightarrow H$ are homomorphisms (see Section 4.1 for the definition of projection maps). What is the kernel of each of these maps?

7.3.5. Show 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, and where $+$ in each case has the standard definition.

7.3.6. [Used in Section 7.3.] Prove Theorem 7.3.2 parts (i) and (iv).

7.3.7. [Used in Section 7.3.] Prove Theorem 7.3.3.

7.3.8. [Used in Section 7.3.] Prove Theorem 7.3.7.

7.3.9. [Used in Section 7.3.] Show that the group (V, \circ) of Example 7.2.1 (4) is not isomorphic to the group (Q, \diamond) of Example 7.3.6 (3).

7.3.10. [Used in Section 7.3.] Show that up to isomorphism, the only two groups with four elements are (V, \circ) of Example 7.2.1 (4) and (Q, \diamond) of Example 7.3.6 (3).

7.4 Partially Ordered Sets

In the previous two sections 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 notice 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 on sets that are based on the notion of an order relation, rather than a binary operation.

Our undertaking is not simply an exercise in playing with definitions, since in fact the types of structures we will discuss here, called partially ordered sets and lattices, have widespread use in many areas of both pure and applied mathematics, such as combinatorics, boolean algebras, switching circuits, computer science and others. See [LP98, Chapters 1–2] for example. An interesting application of order relations to the theory of voting is in [KR83b, 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 our brief discussion we will focus more on lattices than on partially ordered sets, not because the former is more important, but simply because the latter allows for a treatment more appropriate to this text.

In Section 5.1 we defined the idea of a relation on a set, and discussed various properties that a relation might satisfy, such as 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 $x \leq y$ and $y \leq x$. (See Chapter 8 for further discussion of the relation \leq on the various standard number systems.)

Now compare the relation \leq on \mathbb{R} with the relation \subseteq on the collection of all subsets of a given set A (that is, on $\mathcal{P}(A)$). Note 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 two real numbers x and y , 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. 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 $y \preccurlyeq x$ together imply that $x = y$, for all $x, y \in A$.
- (2) The relation \preccurlyeq is a **partial ordering** if it is reflexive, transitive and antisymmetric. If \preccurlyeq is a partial ordering, then the pair (A, \preccurlyeq) is a **partially ordered set**, also known as a **poset**.
- (3) The relation \preccurlyeq is a **total ordering** if it is a partial ordering, and if for every $a, b \in A$, either $a \preccurlyeq b$ or $b \preccurlyeq a$. 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 often simply say “let A be a poset.” Similarly for totally ordered sets. We will primarily be looking at posets, rather than totally ordered sets, since the former are more prevalent. Clearly any totally ordered set is also a poset. Total orderings are also called linear orderings.

Example 7.4.1.

- (1) The relation T in Example 5.1.3 (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; see Exercise 7.4.4 (2) for the reason. For example, the relation of congruence modulo n for any $n \in \mathbb{N}$ with $n \neq 1$ is reflexive and transitive, but not antisymmetric (see Section 5.2 for the definition of this relation).
- (3) Let A be a set. Then $(\mathcal{P}(A), \subseteq)$ is a poset. The relation \subseteq is not a total ordering, as mentioned previously.
- (4) The relation “ $a|b$ ” on \mathbb{N} is defined in Section 2.2. This relation is a partial ordering. To see antisymmetry, let $a, b \in \mathbb{N}$, and suppose that $a|b$ and $b|a$ are both true. Then by Theorem 2.4.3 we know that $a = b$ or $a = -b$. Since both a and b are positive, then it must be the case that $a = b$. The relation is certainly reflexive, and it was shown in Theorem 2.2.1 that this relation is transitive. Thus the relation is a partial ordering. This relation is not a total ordering, however. For example, neither $2|3$ nor $3|2$ hold. (Note that the relation $a|b$ on \mathbb{Z} is not antisymmetric, since $3|(-3)$ and $(-3)|3$.)
- (5) Each of the sets \mathbb{N} , \mathbb{Z} , \mathbb{Q} and \mathbb{R} with \leq are totally ordered sets. The relation $<$ on these sets is not a partial ordering, since it is not reflexive. The set of complex numbers \mathbb{C} , by contrast, does not have any naturally occurring total ordering (though it could be given an unnatural one).
- (6) Let W be the set of all words in the English language. We define a relation \preccurlyeq on W as follows. If w_1 and w_2 are words, we say that $w_1 \preccurlyeq w_2$ if for some $n \in \mathbb{N}$, the first $n-1$ letters of both 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 (we drop the second condition when $w_1 = w_2$). For example, we have $\text{mandrel} \preccurlyeq \text{mandrill}$. This relation, which can be seen to be a total ordering, is called the lexicographical order. \diamond

A very nice way to visualize finite posets is via Hasse diagrams. To construct these diagrams we need the following definition.

Definition. Let (A, \preccurlyeq) be a poset and let $a, b \in A$. We say that b **covers** a if $a \preccurlyeq b$, if $a \neq b$, and if there is no $x \in A$ such that $a \preccurlyeq x \preccurlyeq b$ and $a \neq x \neq b$. Δ

Given a finite poset, we form its Hasse diagram 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 iff y covers x .

Example 7.4.2.

(1) Let $A = \{2, 4, 6, 8, 10, 12\}$ and let \preccurlyeq be the relation $a|b$ discussed in Example 7.4.1 (4). 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 $2 \preccurlyeq 8$, since 8 does not cover 2. Also, note 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.

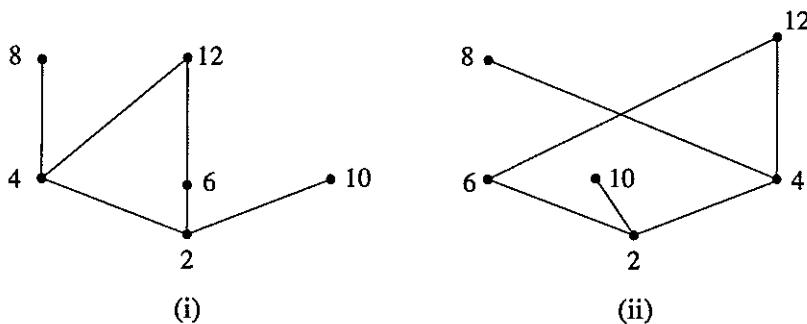


Figure 7.4.1.

(2) One interesting thing to do with Hasse diagrams is to list all possible inequivalent posets of a given size, where a rigorous definition of “inequivalent” needs the notion of order preserving maps 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. (Not that Hasse diagrams are the posets, but they accurately represent them.) \diamond

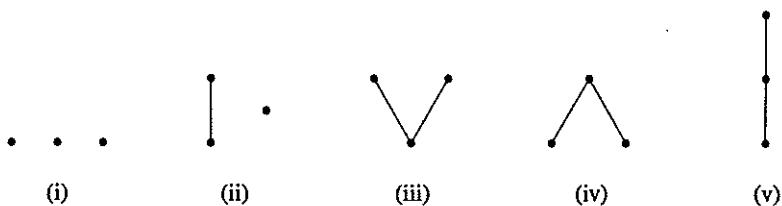


Figure 7.4.2.

Whenever we have a notion of order, it is tempting to look for a greatest element and a least element with respect to the order, where an element is

greatest if it is greater than or equal to every other element, and similarly for a least element. Unfortunately, greatest and least elements do not always exist in posets. In the poset (\mathbb{Z}, \leq) , for example, there is no greatest or least element. Even finite posets need not have greatest or least elements. The poset in Example 7.4.2 (1) does not have a greatest element; notice that 12 is not a greatest element with respect to the relation $a|b$, since 10 does not divide 12. The poset does have a least element, namely 2, since 2 divides all the other numbers in the set. The following theorem states that we can always find elements that at least are not less than anything else, and others that at least are not greater than anything else.

Theorem 7.4.3. *Let (A, \preccurlyeq) be a poset, and suppose that A is finite. Then there is an element $r \in A$ such that if $r \preccurlyeq x$ for some $x \in A$, then $r = x$. There is an element $s \in A$ such that if $x \preccurlyeq s$ for some $x \in A$, then $s = x$.*

Proof. We will prove the existence of the element r ; the existence of the element s is similar. Let $|A| = n$. We proceed by induction on n . If $n = 1$, then let r be the single element of A , and there is nothing to prove. Now assume that $n \geq 2$, and suppose that the result is true for $n - 1$. Choose any element $w \in A$, and let $A' = A - \{w\}$. Then $|A'| = n - 1$. By the inductive hypothesis, we know there is an element $p \in A'$ such that if $p \preccurlyeq x$ for some $x \in A'$, then $p = x$. We now define r as follows. If $p \preccurlyeq w$, let $r = w$; if it is not the case that $p \preccurlyeq w$, then let $r = p$. We leave it to the reader in Exercise 7.4.6 to show that if $r \preccurlyeq x$ for some $x \in A$, then $r = x$. \square

The elements r and s , whose existence is guaranteed in the above theorem, are not necessarily unique (the reader should supply examples). This theorem, while not completely satisfying, is the best we can do in general. In some posets, however, we can do better. The following definition is needed to clarify what “better” means.

Definition. Let (A, \preccurlyeq) be a poset. Let $X \subseteq A$. An **upper bound** for X is an element $p \in A$ such that $x \preccurlyeq p$ for all $x \in X$. A **least upper bound** for X is an element $p \in A$ such that p is an upper bound for X , and such that $p \preccurlyeq z$ for any other upper bound z for X . A **lower bound** for X is an element $q \in A$ such that $q \preccurlyeq x$ for all $x \in X$. A **greatest lower bound** for X is an element $q \in A$ such that q is a lower bound for X , and such that $w \preccurlyeq q$ for any other lower bound w for X . Δ

Example 7.4.4.

(1) We continue Example 7.4.1 (3). In this poset, greatest lower bounds and least upper bounds always exist. Let $X \subseteq \mathcal{P}(A)$. Thus X is a collection of subsets of A . It can be seen that $\bigcup_{D \in X} D$ is a least upper bound for X , and that $\bigcap_{D \in X} D$ is a greatest lower bound for X .

(2) We continue Example 7.4.1 (5), starting with (\mathbb{Q}, \leq) . The set $X = \{1/2, 2/2, 3/2, 4/2, 5/2, \dots\}$ has no upper bound in \mathbb{Q} , and hence no least upper bound. This set does have many lower bounds, for example -17 and 0 , and it has a greatest lower bound, namely $1/2$. Now consider $Y = \{x \in \mathbb{Q} \mid 1 < x < 3\}$. Then Y has many upper and lower bounds; it has a least upper bound, namely 3 , and a greatest lower bound, namely 1 . Unlike the set X , which contains its greatest lower bound, the Y contains neither its greatest lower bound nor its least upper bound. Next, let $Z = \{x \in \mathbb{Q} \mid 0 \leq x < \sqrt{2}\}$. Then Z has a greatest lower bound, namely 0 . However, even though Z has many upper bounds in \mathbb{Q} , for example 2 and $3/2$, 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 2.3.3). This last example is somewhat disturbing. That the set X had no least upper bound was expected, since it had no upper bounds. By contrast, the set Z does have upper bounds, but no least upper bound.

If we look at the poset (\mathbb{R}, \leq) , by contrast, then the above mentioned problem does not occur. If we let $Z' = \{x \in \mathbb{R} \mid 0 \leq x < \sqrt{2}\}$, then this set has a least upper bound in \mathbb{R} , namely $\sqrt{2}$. Indeed, what distinguishes \mathbb{R} from \mathbb{Q} is precisely the fact that every set in \mathbb{R} that has an upper bound 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 Section 8.6 for a bit more discussion, and most texts on real analysis (such as [Pow94]) for more substantial discussion.

(3) We continue Example 7.4.1 (4). Suppose we have finitely many numbers $a_1, \dots, a_p \in \mathbb{N}$, where $p \in \mathbb{N}$. Then the greatest common divisor of a_1, \dots, a_p is a greatest lower bound for $\{a_1, \dots, a_p\}$ with respect to the given partial ordering, and the least common multiple of these numbers is a least upper bound for $\{a_1, \dots, a_p\}$. On the other hand, if we have an infinite set of numbers $X \subseteq \mathbb{N}$, a least upper bound for X will not exist, though a greatest lower bound for X will exist (and it will still be the greatest common divisor of all the elements of X). \diamond

We see from the above example that least upper bounds and greatest lower bounds do not exist for all subsets of posets. The following lemma shows that if they exist, they are unique.

Lemma 7.4.5. *Let (A, \preccurlyeq) be a poset. Let $X \subseteq A$. If X has a least upper bound, then it is unique. If X has a greatest lower bound, then it is unique.*

Proof. Suppose that $p, q \in A$ are both least upper bounds for X . By definition both p and q are upper bounds for X . Since p is a least upper bound for X , and q is an upper bound for X , then $p \preccurlyeq q$ by the definition of least upper bounds. Similarly, we see that $q \preccurlyeq p$. By antisymmetry, we deduce that $p = q$. A similar argument works for greatest lower bounds. \square

Because of the above lemma, 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 $\text{lub } X$ and $\text{glb } X$ to denote the least upper bound and the greatest lower bound respectively for a subset X of a poset.)

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 7.4.1 (3). However, the following theorem shows that every finite poset can be “strengthened” into a totally ordered set.

Theorem 7.4.6. *Let (A, \preccurlyeq) be a poset, and suppose that A is finite. Then there is a total ordering \preccurlyeq' on A such that if $x \preccurlyeq y$ then $x \preccurlyeq' y$, for all $x, y \in A$.*

Proof. Let $|A| = n$. We proceed by induction on n . If $n = 1$ the result is trivial. Now assume that $n \geq 2$, and suppose that the result is true for $n - 1$. Using Theorem 7.4.3, we know that there exists $r \in A$ such that if $r \preccurlyeq x$ for some $x \in A$, then $r = x$. Let $B = A - \{r\}$. Then $|B| = n - 1$. By the inductive hypothesis, there is a total ordering \preccurlyeq'' on B such that if $x \preccurlyeq y$ then $x \preccurlyeq'' y$, for all $x, y \in B$. Now define a relation \preccurlyeq' on A as follows. For any $x, y \in B$, let $x \preccurlyeq' y$ iff $x \preccurlyeq'' y$. For any $x \in A$, let $x \preccurlyeq' r$. We leave it to the reader in Exercise 7.4.7 to show that \preccurlyeq' is a total order on A , and that if $x \preccurlyeq y$ then $x \preccurlyeq' y$, for all $x, y \in A$. \square

In the above theorem we showed 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 will have many linear orderings. A close look at the proof of the above theorem

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.

In Section 7.3 we discussed homomorphisms and isomorphisms of groups, which are maps between groups that preserved the group operation. Similarly, we can discuss maps between posets that preserve their basic structures. Our treatment here partially follows [Szá63, Section 20].

Definition. Let (A, \preccurlyeq) and (B, \preccurlyeq') be posets, and let $f: A \rightarrow B$ be a map. The map f is an **order homomorphism** if $x \preccurlyeq y$ implies $f(x) \preccurlyeq' f(y)$, for all $x, y \in A$. The map f is an **order isomorphism** if it is bijective, and if both f and f^{-1} are order homomorphisms. \triangle

The names “order homomorphism” and “order isomorphism” are slightly less standard than the very standard terms homomorphism and isomorphism for groups. For example, the term “order preserving map” is used for order homomorphisms in some texts. Two posets are considered essentially the same if there is an order isomorphism between them. The following useful lemma is a direct consequence of the above definition, and so we omit the proof.

Lemma 7.4.7. *Let (A, \preccurlyeq) and (B, \preccurlyeq') be posets, and let $f: A \rightarrow B$ be a map. Then f is an order isomorphism iff it is a bijective map, and if $x \preccurlyeq y$ iff $f(x) \preccurlyeq' f(y)$ for all $x, y \in A$.*

Example 7.4.8.

(1) Let $\mathcal{P}_F(\mathbb{N})$ denote the collection of all finite subsets of \mathbb{N} . It is straightforward to see that $(\mathcal{P}_F(\mathbb{N}), \subseteq)$ is a poset. Recall from Examples 7.4.1 (5) that (\mathbb{Z}, \leq) is a poset. Let $s: \mathcal{P}_F(\mathbb{N}) \rightarrow \mathbb{Z}$ be defined by $s(X) = |X|$ for any finite subset X of \mathbb{N} . It follows from Theorem 6.1.6 (iii) that the map s is an order homomorphism. The map 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, using Example 7.4.1 (3) and (4). Define a map $f: D \rightarrow \mathcal{P}(A)$ by $f(1) = \emptyset$, and $f(2) = \{a\}$, and $f(3) = \{b\}$ and $f(6) = \{a, b\}$. We leave it 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. The identity map $1_{\mathbb{N}}: \mathbb{N} \rightarrow \mathbb{N}$ is then seen to be an order homomorphism from the poset $(\mathbb{N}, =)$ to the poset (\mathbb{N}, \leq) . The map $1_{\mathbb{N}}$ is also bijective. However, the inverse map $(1_{\mathbb{N}})^{-1} = 1_{\mathbb{N}}$ is not an order homomorphism from (\mathbb{N}, \leq) to $(\mathbb{N}, =)$. For example, we have $5 \leq 7$, 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. Thus the definition of order isomorphism is not redundant. (If you are 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 map is bijective and a homomorphism, then its inverse is automatically a homomorphism as well; see Theorem 7.3.7 (ii) for the group case. Homomorphisms of posets, we now see, are not as well-behaved.) \diamond

We conclude this section with an example of a nice result about order homomorphisms. To appreciate this result, recall from Figure 7.4.2 that even with only 3 elements, there are a number of different partial orderings that can be given on any finite set. With more elements, the number of possible partial orderings is even larger. In the figure, however, only one of the partial orderings is a total ordering, namely the one whose Hasse diagram is a single vertical line. The following theorem says, not surprisingly, that a similar result holds for all finite sets.

Theorem 7.4.9. *Let (A, \preccurlyeq) be a totally ordered set. Suppose that A is finite, with $|A| = n$ for some $n \in \mathbb{N}$. Then there is an order isomorphism from (A, \preccurlyeq) to $(\{1, 2, \dots, n\}, \leq)$.*

Proof. We follow [KR83b]. We prove the result by induction on n . When $n = 1$ the result is evidently true. Now assume that $n \geq 2$, and suppose that the result holds for $n - 1$.

Using Theorem 7.4.3, we know that there exists $r \in A$ such that if $r \preccurlyeq x$ for some $x \in A$, then $r = x$. Let $x \in A$. Since \preccurlyeq is a total order, 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 $B = A - \{r\}$. Then $|B| = n - 1$, so we can apply the inductive hypothesis to deduce the existence of a map $f: B \rightarrow \{1, 2, \dots, n - 1\}$ that is an order isomorphism from (B, \preccurlyeq) to $(\{1, 2, \dots, n - 1\}, \leq)$. Define $F: A \rightarrow \{1, 2, \dots, n\}$ by $F(x) = f(x)$ for all $x \in B$ and $F(r) = n$. We claim that F is an order isomorphism.

Since f is bijective, it is straightforward to see that F is bijective as well. To see that F is an order isomorphism, it suffices by Lemma 7.4.7 to

show that $x \preccurlyeq y$ iff $F(x) \leq F(y)$, for all $x, y \in A$. First, let $x, y \in B$. Then $x \preccurlyeq y$ iff $f(x) \leq f(y)$ because f is an order isomorphism. Since $F(x) = f(x)$ and $F(y) = f(y)$, then $x \preccurlyeq y$ iff $F(x) \leq F(y)$. Now let $z \in B$. Then we know that $z \preccurlyeq r$, and we also know that $F(z) \leq n = F(r)$, since $F(z) \in \{1, 2, \dots, n - 1\}$. Thus $z \preccurlyeq r$ iff $F(z) \leq F(r)$. Hence F is an order isomorphism. \square

The above result is not true for infinite sets. For example, the posets (\mathbb{N}, \leq) and (\mathbb{N}^-, \leq) have no order isomorphism from one to the other, where \mathbb{N}^- denotes the set of negative integers (see Exercise 7.4.14 for details).

Exercises

7.4.1. Is each of the relations given in Exercise 5.1.3 antisymmetric, a partial ordering and/or a total ordering?

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 given by xMy iff 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 given by xAy iff 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 given by sLt iff 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 given by xZy iff x 's social security number is greater than y 's social security number, for all $x, y \in U$.

7.4.3. Draw a Hasse diagram for each of the following posets.

(1) The relation $a|b$ on the set $A = \{1, 2, 3, \dots, 15\}$.

(2) The relation $a|b$ on the set $B = \{1, 2, 3, 4, 6, 8, 12, 24\}$.

(3) The relation $a|b$ on the set $C = \{1, 2, 4, 8, 16, 32, 64\}$.

(4) The relation \preccurlyeq on the set $C = \{1, 2, 4, 8, 16, 32, 64\}$ given by $a \preccurlyeq b$ iff $b = a^k$ for some $k \in \mathbb{N}$, for all $a, b \in C$. (That this relation is a partial ordering can be verified by the reader.)

(5) The relation \subseteq on $\mathcal{P}(\{1, 2, 3\})$.

7.4.4. [Used in Section 7.4.] (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. Show that every element of A is related at most to itself.

7.4.5. Let (A, \preccurlyeq) be a poset. An element $O \in A$ is a **least element** if $O \preccurlyeq x$ for all $x \in A$. An element $I \in A$ is a **greatest element** if $x \preccurlyeq I$ for all $x \in A$.

(1) Show that if A has a least element, it is unique, and if it has a greatest element, it is 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.

7.4.6. [Used in Section 7.4.] Complete the missing step in the proof of Theorem 7.4.3. That is, let r be as defined in the proof of the theorem. Show that if $r \preccurlyeq x$ for some $x \in A$, then $r = x$.

7.4.7. [Used in Section 7.4.] Complete the missing step in the proof of Theorem 7.4.6. That is, let \preccurlyeq' be as defined in the proof of the theorem. Show that \preccurlyeq' is a total order on A , and that if $x \preccurlyeq y$ then $x \preccurlyeq' y$, for all $x, y \in A$.

7.4.8. 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 for the duration of this problem that R is a quasi-ordering.

(1) Define a new relation \sim on A by the condition $x \sim y$ iff xRy and yRx , for all $x, y \in A$. Show that \sim is an equivalence relation.

(2) Suppose that $x, y, a, b \in A$, and that xRy , that $x \sim a$ and that $y \sim b$. Show that aRb .

(3) Form the quotient set A / \sim (as defined in Section 5.3). Define a relation S on A / \sim by the condition $[x]S[y]$ iff xRy . Show that S is well-defined.

(4) Show that $(A / \sim, S)$ is a poset.

7.4.9. Let (A, \preccurlyeq) be a poset. For each $X \subseteq A$, define the set $Prec(X)$ to be

$$Prec(X) = \{w \in A \mid w \preccurlyeq x \text{ and } w \neq x \text{ for all } x \in X\}.$$

Let $C, D \subseteq A$. Show that $Prec(C \cup D) = Prec(C) \cap Prec(D)$.

7.4.10. Let (A, \preccurlyeq) be a poset. Define a map $f: A \rightarrow \mathcal{P}(A)$ by $f(x) = \{y \in A \mid y \preccurlyeq x\}$ for all $x \in A$.

(1) Let $x, z \in A$. Show that $x \preccurlyeq y$ iff $f(x) \subseteq f(y)$.

(2) Show that f is injective.

7.4.11. Let (A, \preccurlyeq) be a poset, let X be a set and let $h: X \rightarrow A$ be a map. Define a relation \preccurlyeq' on X by letting $x \preccurlyeq' y$ iff $h(x) \preccurlyeq h(y)$ for all $x, y \in X$. Show that (X, \preccurlyeq') is a poset.

7.4.12. Let (A, \preccurlyeq) be a poset and let X be a set. We let $\mathcal{F}(X, A)$ be as defined in Section 4.5. Define a relation \preccurlyeq' on $\mathcal{F}(X, A)$ as follows. If $f, g \in \mathcal{F}(X, A)$, we let $f \preccurlyeq' g$ iff $f(x) \preccurlyeq g(x)$ for all $x \in X$. Show that $(\mathcal{F}(X, A), \preccurlyeq')$ is a poset.

7.4.13. Let \preccurlyeq denote the relation $a|b$ on \mathbb{N} , and let \preccurlyeq' denote the relation on \mathbb{N} given by $a \preccurlyeq' b$ iff $b = a^k$ for some $k \in \mathbb{N}$, where $a, b \in \mathbb{N}$. (That this relation is a partial ordering can be verified by the reader.) Show that the identity map $1_{\mathbb{N}}: \mathbb{N} \rightarrow \mathbb{N}$ is an order homomorphism from $(\mathbb{N}, \preccurlyeq')$ to $(\mathbb{N}, \preccurlyeq)$, but that it is not an order isomorphism.

7.4.14. [Used in Section 7.4.] Let \mathbb{N}^- be the set of negative integers. Show that there is no order isomorphism from the poset (\mathbb{N}, \leq) to the poset (\mathbb{N}^-, \leq) .

7.4.15. Let (A, \preccurlyeq) and (B, \preccurlyeq') be posets and let $f: A \rightarrow B$ be an order isomorphism. Show that if \preccurlyeq is a total order, then so is \preccurlyeq' .

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. Let (A, \preccurlyeq) be a poset.

(1) Let $a, b \in A$. If the greatest lower bound of $\{a, b\}$ exists, we call it the **meet** of a and b , and denote it $a \wedge b$. If the least upper bound of $\{a, b\}$ exists, we call it the **join** of a and b , and denote it $a \vee b$.

(2) We call (A, \preccurlyeq) a **lattice** if $a \wedge b$ and $a \vee b$ exist for all $a, b \in A$. Δ

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, since the context should be clear in every situation.

The different uses of the same symbols is not entirely coincidental, however, since 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 1–2]; 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 7.5.1.

(1) We continue Examples 7.4.1 (5) and 7.4.4 (2). The sets \mathbb{N} , \mathbb{Z} , \mathbb{Q} and \mathbb{R} with the relation \leq are all lattices. If x and y are two numbers in any one of these sets, then $x \wedge y$ is the smaller of the two numbers, and $x \vee y$ is the larger; if $x = y$ then $x \wedge y = x = y = x \vee y$. Indeed, any totally ordered set is a lattice, a fact that we leave to the reader to verify.

(2) We continue Examples 7.4.1 (3) and 7.4.4 (1). The poset $(\mathcal{P}(A), \subseteq)$ is a lattice. For any $X, Y \in \mathcal{P}(A)$, we have $X \wedge Y = X \cap Y$ and $X \vee Y = X \cup Y$.

(3) We continue Examples 7.4.1 (4) and 7.4.4 (3). The set \mathbb{N} with the relation $a|b$ 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) Given a finite poset presented by a Hasse diagram, we can check whether or not it is a lattice. In Figure 7.5.1 (i) and (ii) we see posets that are lattices. For example, in part (i) we have $y \vee z = x$ and $y \wedge z = w$. On the other hand, the posets in Figure 7.5.1 (iii) and (iv) are not lattices. For example, in part (iii) the elements s and t do not have an upper bound, and hence no least upper bound, and thus no join. In part (iv) the elements y and z have two upper bounds, but no least upper bound, and thus 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 $a \preccurlyeq b$ iff $b = a^k$ for some $k \in \mathbb{N}$. It can be verified that $(\mathbb{N}, \preccurlyeq)$ is a poset, but it is not a lattice, 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 for $\{2, 3\}$. Then it would follow that $2 \preccurlyeq c$ and $3 \preccurlyeq c$. Thus there would be some $k, j \in \mathbb{N}$ 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 for $\{2, 3\}$. Then $d \preccurlyeq 2$ and $d \preccurlyeq 3$, and so there would be some $p, q \in \mathbb{N}$ such that $2 = d^p$ and $3 = d^q$, which again cannot happen, since p and q are natural numbers. Some meets and joints do exist in this poset, for example $4 \wedge 8 = 2$ and $4 \vee 8 = 16$. \diamond

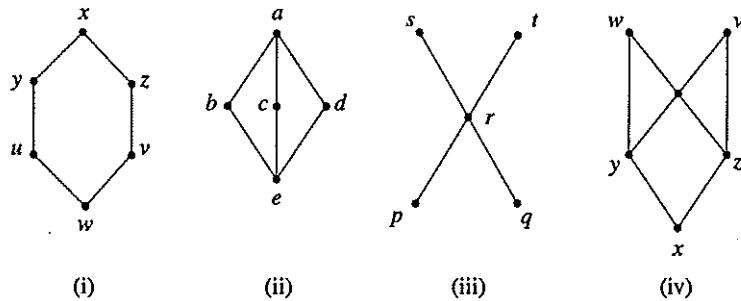


Figure 7.5.1.

From part (1) of the above example, and from Example 7.4.4 (2), we see that whereas the least upper bound and the greatest lower bound for any pair of elements in a lattice must exist, the least upper bound and the greatest lower bound for an arbitrary set of elements in 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 7.5.2. *Let (L, \preccurlyeq) be a lattice, and let $x, y, z \in L$.*

- (i) $x \wedge y \preccurlyeq x$ and $x \wedge y \preccurlyeq y$ and $x \preccurlyeq x \vee y$ and $y \preccurlyeq x \vee y$.
- (ii) $x \wedge x = x$ and $x \vee x = x$ (*Idempotent Laws*).
- (iii) $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ (*Commutative Laws*).
- (iv) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$ (*Associative Laws*).
- (v) $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$ (*Absorption Laws*).
- (vi) $x \preccurlyeq y$ iff $x \wedge y = x$ iff $x \vee y = y$.
- (vii) 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 (iv) and (v), leaving the rest to the reader in Exercise 7.5.3.

(iv). 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. Let $d = x \wedge (y \wedge z)$. By part (i) we know that $d \preccurlyeq x$ and $d \preccurlyeq y \wedge z$. Applying part (i) again, we see that $d \preccurlyeq y$ and $d \preccurlyeq z$. Since d is a lower bound for x and y , it follows from the definition of meet as a greatest lower bound that $d \preccurlyeq x \wedge y$. Similarly, since d is a lower bound for $x \wedge y$ and z , it follows that $d \preccurlyeq (x \wedge y) \wedge z$. Thus $x \wedge (y \wedge z) \preccurlyeq (x \wedge y) \wedge z$. The same sort of argument shows that $(x \wedge y) \wedge z \preccurlyeq x \wedge (y \wedge z)$. By the antisymmetry of \preccurlyeq , we deduce that $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.

(v). We will prove that $x \wedge (x \vee y) = x$; the proof that $x \vee (x \wedge y) = x$ is similar. By the reflexivity of \preccurlyeq we know that $x \preccurlyeq x$, and by part (i) of this theorem, we know that $x \wedge y \preccurlyeq x$. Thus x is an upper bound for x and $x \wedge y$, and by the definition of join as a least upper bound, we deduce that $x \vee (x \wedge y) \preccurlyeq x$. On the other hand, by part (i) of this theorem we know that $x \preccurlyeq x \vee (x \wedge y)$. By the antisymmetry of \preccurlyeq , we deduce that $x \wedge (x \vee y) = x$. \square

We see in the above theorem that a number of the standard algebraic properties we are familiar with from the addition and multiplication of numbers also hold for lattices. Not all familiar properties of addition and multiplication of numbers hold for every lattice, however. One such property is the distributive law. This law holds for the lattice in Example 7.5.1 (2), as seen from Theorem 3.3.2 (v). It does not hold in the lattice with Hasse diagram shown 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 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. These binary operations satisfy certain properties, some of which were given in Theorem 7.5.2. 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.

Theorem 7.5.3. Let A be a set. Suppose that there are two binary operations $\wedge: A \times A \rightarrow A$ and $\vee: A \times A \rightarrow A$ satisfying the following conditions for all $x, y, z \in A$:

- (1) $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$;
- (2) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ and $x \vee (y \vee z) = (x \vee y) \vee z$;
- (3) $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$.

Define a relation \preceq on A by setting $x \preceq y$ iff $x \wedge y = x$, for all $x, y \in A$. Then (A, \preceq) is a lattice, with \wedge and \vee the meet and join of the lattice respectively.

Proof. We follow [Bir48] and [LP98] in part. As a preliminary, we prove the following three facts: Let $x, y \in A$. Then (a) $x \wedge x = x$; (b) $x \vee x = x$; (c) $x \wedge y = x$ iff $x \vee y = y$. To prove fact (a), we use both parts of property (3) to deduce that $x \wedge x = x \wedge (x \vee (x \wedge x)) = x$. A similar argument yields fact (b). To prove fact (c), suppose that $x \wedge y = x$. Then by using properties (1) and (3) we compute $x \vee y = (x \wedge y) \vee y = y \vee (y \wedge x) = y$. A similar argument proves the other direction of the iff statement.

We now show that (A, \preceq) is a poset. Let $x, y, z \in A$. Since $x \wedge x = x$ by fact (a), it follows from the definition of \preceq that $x \preceq x$. Thus \preceq is reflexive. Now suppose that $x \preceq y$ and $y \preceq z$. Then $x \wedge y = x$ and $y \wedge z = y$. Using property (2) we compute $x \wedge z = (x \wedge y) \wedge z = x \wedge (y \wedge z) = x \wedge y = x$. It follows that $x \preceq z$. Thus \preceq is transitive. Next, suppose that $x \preceq y$ and $y \preceq x$. Then by definition we have $x \wedge y = x$ and $y \wedge x = y$. By property (1) we know that $x \wedge y = y \wedge x$, and so $x = y$. Thus \preceq is antisymmetric. Hence (A, \preceq) is a poset.

Finally, we show that \wedge and \vee are the meet and join of (A, \preceq) . A corollary to this fact would be that the meet and join always exists for any two elements of A . We start with \wedge . Let $x, y \in A$. Using property (2) and fact (a) we see that $(x \wedge y) \wedge y = x \wedge (y \wedge y) = x \wedge y$. Hence $x \wedge y \preceq y$. Since $x \wedge y = y \wedge x$ by property (1), a similar argument shows that $x \wedge y \preceq x$. Thus $x \wedge y$ is a lower bound for the set $\{x, y\}$. Now suppose that $z \in A$ is another lower bound for the set $\{x, y\}$. Thus $z \preceq x$ and $z \preceq y$, and hence $z \wedge x = z$ and $z \wedge y = z$. Using property (2) we see that $z \wedge (x \wedge y) = (z \wedge x) \wedge y = z \wedge y = z$. Hence $z \preceq (x \wedge y)$. It follows that $x \wedge y$ is the greatest lower bound for the set $\{x, y\}$, which means that $x \wedge y$ is the meet of x and y .

We now turn to \vee . Let $x, y \in A$. Using property (3) we see that $x \wedge (x \vee y) = x$. Hence $x \preceq x \vee y$. Since $x \vee y = y \vee x$ by property (1), a similar argument shows that $y \preceq x \vee y$. Thus $x \vee y$ is an upper bound for

the set $\{x, y\}$. Now suppose that $w \in A$ is another upper bound for the set $\{x, y\}$. Thus $x \preccurlyeq w$ and $y \preccurlyeq w$, and hence $x \wedge w = x$ and $y \wedge w = y$. By fact (c) we deduce that $x \vee w = w$ and $y \vee w = w$. Using property (2) it then follows that $(x \vee y) \vee w = x \vee (y \vee w) = x \vee w = w$. Hence $(x \vee y) \wedge w = x \vee y$ by fact (c). Thus $x \vee y \preccurlyeq w$. It follows that $x \vee y$ is the least upper bound for the set $\{x, y\}$, which means that $x \vee y$ is the join of x and y . \square

While the above theorem 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 on order.

In Section 7.4 we discussed order homomorphisms and order isomorphisms of posets. Since lattices are posets, we can apply such maps to lattices. There are two other types of maps that are more particularly suited to lattices.

Definition. Let (L, \preccurlyeq) and (M, \preccurlyeq') be lattices, and let $f: L \rightarrow M$ be a map. Let \wedge and \vee be the meet and join for L , and let \wedge' and \vee' be the meet and join for M . The map f is a **meet homomorphism** if $f(x \wedge y) = f(x) \wedge' f(y)$ for all $x, y \in L$. The map f is a **join homomorphism** if $f(x \vee y) = f(x) \vee' f(y)$ for all $x, y \in L$. Δ

Example 7.5.4.

(1) The map in Example 7.4.8 (2) is both a meet homomorphism and a join homomorphism, as the reader can verify.

(2) Let (L, \preccurlyeq) and (M, \preccurlyeq') respectively denote the lattices corresponding to the Hasse diagrams in Figure 7.5.1 (i) and (ii). Define a map $f: L \rightarrow M$ by letting $f(x) = a$, and letting f take every other element of L to e . The map f is seen to be a meet homomorphism as follows: If $\alpha, \beta \in L$ are not both x , then $\alpha \wedge \beta \neq x$, and $f(\alpha \wedge \beta) = e = e \wedge e = f(\alpha) \wedge' f(\beta)$; also, we have $f(x \wedge x) = f(x) = a = a \wedge a = f(x) \wedge f(x)$. The map f is not a join homomorphism, since $f(y \vee z) = f(x) = a$, but $f(y) \vee' f(z) = e \vee e = e$. A similar construction yields a map $L \rightarrow M$ that is a join homomorphism but not a meet homomorphism.

(3) We continue Example 7.4.8 (1). As mentioned, the map s is an order homomorphism. It is neither a meet homomorphism nor a join homomorphism, however. For example, let $X = \{5, 7\}$ and let $Y = \{7, 9\}$. Then, similar to Examples 7.5.1 (2), we have $X \wedge Y = X \cap Y = \{7\}$, and $X \vee Y = X \cup Y = \{5, 7, 9\}$. Then $s(X \wedge Y) = 1$ and $s(X \vee Y) = 3$.

However, by Example 7.5.1 (1) we know that in the lattice (\mathbb{Z}, \leq) we have $s(X) \wedge s(Y) = 2 \wedge 2 = 2$, and $s(X) \vee s(Y) = 2 \vee 2 = 2$. Thus $s(X \wedge Y) \neq s(X) \wedge s(Y)$ and $s(X \vee Y) \neq s(X) \vee s(Y)$. \diamond

We now have four types of maps that we can use with lattices, namely order homomorphisms, order isomorphisms, meet homomorphisms and join homomorphisms. How are these different types of maps related? We saw in Example 7.4.8 (1) that a map can be an order homomorphism without being an order isomorphism. We saw in Example 7.5.4 (2) that a map can be a meet homomorphism without being a join homomorphism, and vice-versa. Parts (i) and (iii) of the following theorem clarify the relations between the four types of maps.

Theorem 7.5.5. *Let (L, \preccurlyeq) and (M, \preccurlyeq') be lattices, and let $f : L \rightarrow M$ be a map.*

- (i) *If f is a meet homomorphism or a join homomorphism, then it is an order homomorphism.*
- (ii) *If f is bijective and a meet homomorphism (respectively, a join homomorphism), then f^{-1} is a meet homomorphism (respectively, a join homomorphism).*
- (iii) *The map f is an order isomorphism iff f is bijective and a meet homomorphism iff f is bijective and a join homomorphism.*

Proof. We will prove part (i), leaving parts (ii) and (iii) to the reader in Exercise 7.5.14.

(i). Suppose f is a meet homomorphism. Let \wedge and \wedge' denote the meet for L and M respectively. Let $x, y \in L$, and suppose that $x \preccurlyeq y$. Then by Theorem 7.5.2 (vi) we know that $x = x \wedge y$. Then $f(x) = f(x \wedge y) = f(x) \wedge' f(y)$, since f is a meet homomorphism. Using Theorem 7.5.2 (vi) 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. \square

Because of part (iii) of the above theorem, 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 bijective join homomorphism between them.

We conclude this section with a nice result that involves the notion of a fixed point of a map, that is, a point taken to itself by the map. 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 to economics (see [Deb86] or [KR83a, pp. 38–39]). The following theorem gives a criterion that guarantees the existence of fixed points for certain maps of lattices to themselves.

Theorem 7.5.6. *Let (L, \preccurlyeq) be a lattice, and let $f : L \rightarrow L$ be an order homomorphism. Suppose 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 $C = \{x \in L \mid x \preccurlyeq f(x)\}$. We claim that C is non-empty. Note that L is non-empty by definition (since L is a poset). Let m be the greatest lower bound for L , which exists by hypothesis. Then m is a lower bound for L , and thus $m \preccurlyeq x$ for all $x \in L$. In particular, we have $m \preccurlyeq f(m)$. Thus $m \in C$, and so C is non-empty.

Let a be the least upper bound for C , which exists by hypothesis. Now let $x \in C$. Since a is an upper bound for C , we have $x \preccurlyeq a$. 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 . Since a is the least upper bound for C , it follows that $a \preccurlyeq f(a)$. Thus $f(a) \preccurlyeq f(f(a))$, since f is an order homomorphism. Hence $f(a) \in C$. Therefore $f(a) \preccurlyeq a$, because a is an upper bound for C . Using antisymmetry, we deduce that $f(a) = a$. \square

Corollary 7.5.7. *Let (L, \preccurlyeq) be a lattice, and let $f : L \rightarrow L$ be an order homomorphism. If L is finite, then there is some $a \in L$ such that $f(a) = a$.*

Proof. This follows immediately from Exercise 7.5.5 and Theorem 7.5.6 \square

Theorem 7.5.6 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 map $f : \mathbb{N} \rightarrow \mathbb{N}$ given by $f(x) = x + 1$ for all $x \in \mathbb{N}$. This map 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 or greatest lower bounds, so Theorem 7.5.6 does not apply.

Exercises

7.5.1. Which of the posets given in Exercise 7.4.3 are lattices?

7.5.2. Which of the posets represented as Hasse diagrams in Figure 7.5.2 are lattices?

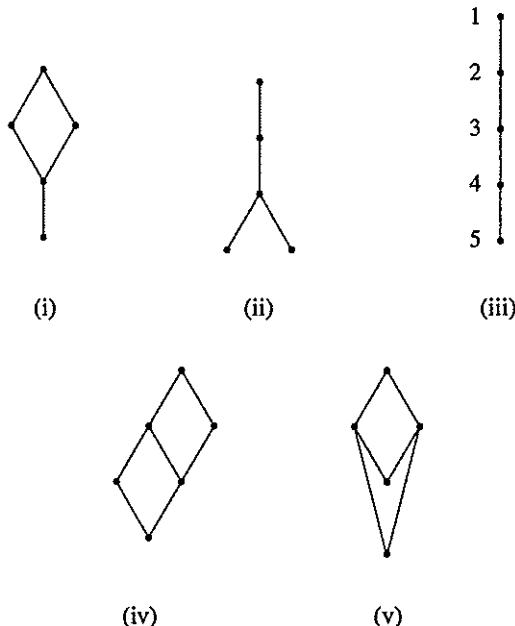


Figure 7.5.2.

7.5.3. [Used in Section 7.5.] Prove Theorem 7.5.2 parts (i) – (iii) and (vi) – (vii).

7.5.4. Find Hasse diagrams corresponding to all possible distinct lattices with five elements (there are five such lattices).

7.5.5. [Used in Section 7.5.] Let (L, \preccurlyeq) be a lattice and suppose that L is finite. Let $X \subseteq A$. Show that X has a least upper bound and a greatest lower bound.

7.5.6. Let (L, \preccurlyeq) be a lattice and let $a, b \in L$. Show that $a \wedge b = a \vee b$ iff $a = b$.

7.5.7. [Used in Section 7.5.] Let (L, \preccurlyeq) be a lattice, and let $a, b, c \in L$. Show that the following four inequalities hold. The first two inequalities are called the distributive inequalities, and the latter two are called the modular inequalities.

- (1) $a \wedge (b \vee c) \succcurlyeq (a \wedge b) \vee (a \wedge c)$.
- (2) $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$.
- (3) If $a \succcurlyeq c$, then $a \wedge (b \vee c) \succcurlyeq (a \wedge b) \vee c$.
- (4) If $a \preccurlyeq c$, then $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge c$.

7.5.8. Let (L, \preccurlyeq) be a lattice. Show that $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in A$ iff $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ for all $a, b, c \in A$. We say (L, \preccurlyeq) is **distributive** if either (and hence both) of these conditions holds.

7.5.9. Let (L, \preccurlyeq) be a lattice. Suppose that (L, \preccurlyeq) is distributive, as defined in Exercise 7.5.8. Let $a, b, c \in A$. Suppose that $a \wedge c = b \wedge c$ and $a \vee c = b \vee c$. Show that $a = b$.

7.5.10. Let (L, \preccurlyeq) be a lattice. We say (L, \preccurlyeq) is **complemented** if the following conditions hold: (1) the lattice has a least element O and a greatest element I , as defined in Exercise 7.4.5, with $I \neq O$; (2) for each $a \in L$, there exists an element $a' \in L$ such that $a \wedge a' = O$ and $a \vee a' = I$. In a complemented lattice, is there a unique a' for each $a \in L$?

7.5.11. Let (L, \preccurlyeq) be a lattice. We say (L, \preccurlyeq) is a **boolean algebra** if it is distributive and complemented, as defined in Exercises 7.5.8 and 7.5.10 respectively. Suppose that (L, \preccurlyeq) is a boolean algebra. Let $a, b \in L$.

- (1) Show that a' is unique.
- (2) Show that $(a \wedge b)' = a' \vee b'$ and $(a \vee b)' = a' \wedge b'$.

7.5.12. Which of the following lattices are distributive, which are complemented, and which are boolean algebras, using the definitions in Exercises 7.5.8, 7.5.10 and 7.5.11 respectively.

- (1) The lattice given in Example 7.5.1 (2).
- (2) The lattice given in Example 7.5.1 (3).
- (3) The lattices given by Hasse diagrams in Figure 7.5.3.

7.5.13. Let (L, \preccurlyeq) and (M, \preccurlyeq') respectively denote the lattices corresponding to the Hasse diagrams in Figure 7.5.3 (ii) and Figure 7.5.2 (iii) respectively. Described below are various maps $L \rightarrow M$. Is each of the following an order homomorphisms, a meet homomorphisms, a join homomorphisms 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 $f(e) = 5$.

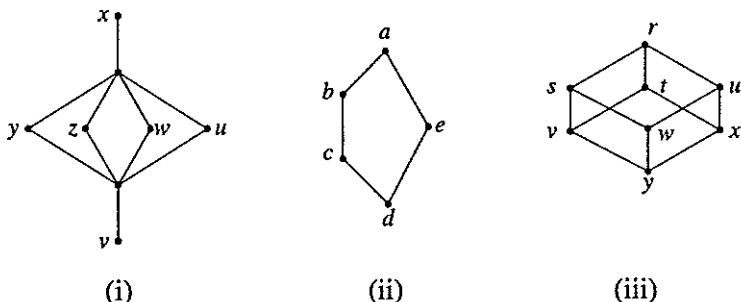


Figure 7.5.3.

7.5.14. [Used in Section 7.5.] Prove Theorem 7.5.5 parts (ii) and (iii).

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.

In the terminology we have developed so far, a counting problem is the determination of the cardinality of a finite set. The difficulty arises when the elements of the set are described, but not explicitly listed. 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

$$S = \{n \in \mathbb{N} \mid 1 \leq n \leq 20 \text{ and } n \text{ is not divisible by 3, 5 or 13}\}.$$

This problem is trivial, because we could write out this set explicitly as $S = \{1, 2, 4, 7, 8, 11, 14, 16, 17, 19\}$. Hence $|S| = 10$. Now suppose 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 of all the elements of the set. We will answer this problem without listing the elements in Example 7.6.9 (2), after we have developed some useful techniques.

In this section and the next we will discuss some of the most basic ways of figuring out the cardinalities of finite sets; we will only be scratching the surface of a very large subject. Our treatment of some issues 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 (to be discussed below). 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 maps from one finite set to another, the proof of which is much simpler 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 that is certainly worthwhile), but rather as an interesting and useful application of the ideas developed throughout this text. Thus, rather than hypothesizing the product and sum rules, and using counting arguments in our proofs, we will formulate all our ideas in terms of our familiar notions of sets, functions and relations. In particular, we will prove the product and sum rules (as well as other results), by relating these topics to ideas such as injective maps 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 — which is true, but reasonable given our goal of providing proofs that use the definitions and the standards of rigor found throughout this text. We will make use of results about finite sets in Section 6.1, as well as proof by mathematical induction in Section 6.3.

We start our discussion of counting, as do many texts, with the “product rule.” A typical statement of this result, as given in [Rob84, Chapter 2], is “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 $N \cdot M$ ways.” Some simple examples of the use of this rule are as follows.

Example 7.6.1.

(1) Seven female cats each have five kittens. How many ways can you choose a mother/kitten pair? By the product rule, there are $7 \cdot 5 = 35$ ways.

(2) Suppose 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, then 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. Note 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 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 before, we deduce that there are $6 \cdot 5 \cdot 4 = 120$ choices. \diamond

Although the product rule is often stated in term of numbers of ways that “things can happen,” the following theorem shows how it can be stated in terms of cardinalities of finite sets. (We will restrict our attention here to the product of two “choices,” since this is the simplest to state directly in terms of cardinalities of sets, and since it is all we will need later on.)

Theorem 7.6.2. *Let A be a finite set, and let $\{B_a\}_{a \in A}$ be a family of equal sized finite sets. Suppose $|A| = N$, and that $|B_a| = M$ for all $a \in A$. Let $X = \{(a, b) \mid a \in A \text{ and } b \in B_a\}$. Then the set X is finite, and $|X| = N \cdot M$.*

The various sets B_a in the above theorem might or might not intersect each other. To prove the theorem, we start with the following lemma, the statement of which is intuitively clear. The proof of this lemma makes use of an important fact about the integers, namely the Division Algorithm (Theorem 8.4.9). You could either read the statement of the theorem (which uses slightly strange notation, but is about the standard integers) now, or you could simply accept the consequences of the theorem when it is invoked below. In either case, this theorem is certainly intuitively believable given your experience with arithmetic.

Lemma 7.6.3. *Let A, B be finite sets. Then the set $A \times B$ is finite, and $|A \times B| = |A| \cdot |B|$.*

Proof. As in Section 6.1, we use the notation $\llbracket 1, m \rrbracket$ to denote the set $\{1, 2, \dots, m\}$, for any $m \in \mathbb{N}$. Suppose $|A| = n$ and $|B| = p$. Let $f: A \rightarrow \llbracket 1, n \rrbracket$ and $g: B \rightarrow \llbracket 1, p \rrbracket$ be bijective maps, which exist by the definition of the cardinality of finite sets. Define the map $h: A \times B \rightarrow \llbracket 1, np \rrbracket$ by letting $h((a, b)) = (f(a) - 1)p + g(b)$ for all $(a, b) \in A \times B$. We claim that h is bijective; the desired result would then follow.

To show that h is surjective, let $x \in \llbracket 1, np \rrbracket$. By the Division Algorithm (Theorem 8.4.9) there are $q, r \in \mathbb{Z}$ such that $x = pq + r$ and $0 \leq r < p$. Since $1 \leq x \leq np$, it follows that $0 \leq q \leq n$. We now have two cases. First, suppose that $r \neq 0$. Then $q \neq n$. Since f and g are surjective, we can find $a \in A$ and $b \in B$ such that $f(a) = q + 1$ and $g(b) = r$. It can be verified that $h((a, b)) = x$. Next, suppose that $r = 0$. Then $q \neq 0$, because $1 \leq x$. Since f and g are surjective, we can find $m \in A$ and $n \in B$ such that $f(m) = q$ and $g(n) = p$. Again, it can be verified that $h((m, n)) = x$.

To show that h is injective, suppose $h((a, b)) = h((c, d))$ for some $(a, b), (c, d) \in A \times B$. Then $(f(a) - 1)p + g(b) = (f(c) - 1)p + g(d)$. Hence $[f(a) - f(c)]p + [g(b) - g(d)] = 0$. Note that $0 \leq |g(b) - g(d)| < p$. Since $0 \cdot p + 0 = 0$, we can apply 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 $(a, b) = (c, d)$. Thus h is injective. \square

If the above proof seems needlessly complicated, given that the result being proved is intuitively simple, the reader is referred to a different proof, using mathematical induction, given in Exercise 7.6.5. Although this alternative proof has the advantage of avoiding the Division Algorithm, it does not give an explicit bijection, as is constructed in the proof used above.

We are now ready for the proof of Theorem 7.6.2.

Proof of Theorem 7.6.2. Let B be a set with M elements. There is a bijective map $g_a : B_a \rightarrow B$ for each $a \in A$ by Corollary 6.1.4. Define a map $\Phi : X \rightarrow A \times B$ 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 then follows from Corollary 6.1.4 and Lemma 7.6.3 that $|X| = |A \times B| = |A| \cdot |B| = N \cdot M$. \square

The other standard counting rule given in introductory treatments of combinatorics is the “sum rule.” A typical statement of this result, also in [Rob84, Chapter 2], is “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).” Note that the product rule, about multiplication, involves “and” situations, whereas the sum rule, 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 7.6.4.

(1) Murkstown High 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 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. \diamond

The sum rule can also be stated in terms of cardinalities of finite sets, as given in part (ii) of the following theorem. Part (iii) 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 7.6.5. *Let A, B be finite sets.*

(i) *The sets $A \cup B$ and $A \cap B$ are finite.*

(ii) *If A and B are disjoint, then $|A \cup B| = |A| + |B|$.*

(iii) $|A \cup B| = |A| + |B| - |A \cap B|$.

Proof. (i). That $A \cap B$ is finite follows immediately from Theorem 6.1.6 (i), since $A \cap B \subseteq A$. It is shown in Exercise 6.1.5 that $A \cup B$ is finite.

(ii). This is a special case of part (iii), which is proved below.

(iii). Viewing $A \cap B$ as a subset of B , it follows from Theorem 6.1.6 (ii) that $|B| = |A \cap B| + |B - (A \cap B)|$. Thinking of A as a subset of $A \cup B$, we know that $|A \cup B| = |A| + |(A \cup B) - A|$. Also, observe that $(A \cup B) - A = B - A = B - (A \cap B)$. Combining all our calculations, we obtain

$$\begin{aligned}|A \cup B| &= |A| + |(A \cup B) - A| = |A| + |B - (A \cap B)| \\&= |A| - |A \cap B| + |A \cap B| + |B - (A \cap B)| \\&= |A| - |A \cap B| + |B|.\end{aligned}$$

\square

Example 7.6.6. Hicksville has two radio stations, namely 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 this 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 we know that $|A| = 15$, that $|B| = 11$ and $|A \cap B| = 9$. By Theorem 7.6.5 (iii) we deduce 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. \diamond

Theorem 7.6.5 can be generalized to the union of finitely many finite sets, rather than just two sets, as seen in the following theorem. Part (iv) 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 7.6.7. *Let A_1, \dots, A_n be finite sets, for some $n \in \mathbb{N}$.*

(i) *The set $A_1 \cup \dots \cup A_n$ is finite.*

(ii) *If $A_i \cap A_j = \emptyset$ for all $i, j \in \{1, \dots, n\}$ with $i \neq j$,
then $|A_1 \cup \dots \cup A_n| = |A_1| + \dots + |A_n|$.*

(iii) *Let $\{r_1, \dots, r_k\} \subseteq \{1, \dots, n\}$. Then $A_{r_1} \cap \dots \cap A_{r_k}$ is finite.*

(iv)

$$\begin{aligned} |A_1 \cup \dots \cup A_n| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ &\quad + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ &\quad - \dots + (-1)^{n+1} |A_1 \cap \dots \cap A_n|. \end{aligned}$$

Proof. (i). This is proved by induction on n together with Theorem 7.6.5 (i); the details are left to the reader.

(ii). This is a special case of part (iv), which is proved below.

(iii). This follows from Theorem 6.1.6 (i).

(iv). We prove this result by induction on n . If $n = 1$ the result is evidently true. Now suppose that the result is true for $n - 1$. Making use of Theorem 7.6.5 (iii) and the inductive hypothesis we compute

$$\begin{aligned}
 |A_1 \cup \cdots \cup A_n| &= |(A_1 \cup \cdots \cup A_{n-1}) \cup A_n| \\
 &= |A_1 \cup \cdots \cup A_{n-1}| + |A_n| - |(A_1 \cup \cdots \cup A_{n-1}) \cap A_n| \\
 &= |A_n| + |A_1 \cup \cdots \cup A_{n-1}| - |(A_1 \cap A_n) \cup \cdots \cup (A_{n-1} \cap A_n)| \\
 &= |A_n| + \left\{ \sum_{i=1}^{n-1} |A_i| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| \right. \\
 &\quad \left. + \sum_{1 \leq i < j < k \leq n-1} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{(n-1)+1} |A_1 \cap \cdots \cap A_{n-1}| \right\} \\
 &\quad - \left\{ \sum_{i=1}^{n-1} |(A_i \cap A_n)| - \sum_{1 \leq i < j \leq n-1} |(A_i \cap A_n) \cap (A_j \cap A_n)| \right. \\
 &\quad \left. + \cdots + (-1)^{(n-1)+1} |(A_1 \cap A_n) \cap \cdots \cap (A_{n-1} \cap A_n)| \right\} \\
 &= |A_n| + \sum_{i=1}^{n-1} |A_i| - \sum_{1 \leq i < j \leq n-1} |A_i \cap A_j| \\
 &\quad + \sum_{1 \leq i < j < k \leq n-1} |A_i \cap A_j \cap A_k| - \cdots + (-1)^n |A_1 \cap \cdots \cap A_{n-1}| \\
 &\quad - \sum_{1 \leq i < j = n} |A_i \cap A_j| + \sum_{1 \leq i < j < k = n} |A_i \cap A_j \cap A_k| - \cdots \\
 &\quad + (-1)^{n+1} |A_1 \cap \cdots \cap A_n| \\
 &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\
 &\quad - \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|. \tag*{\square}
 \end{aligned}$$

Corollary 7.6.8. Let X be a finite set, and let $A_1, \dots, A_n \subseteq X$, for some $n \in \mathbb{N}$. Then

$$\begin{aligned}
 |X - (A_1 \cup \cdots \cup A_n)| &= |X| - \sum_{i=1}^n |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\
 &\quad - \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\
 &\quad + \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|.
 \end{aligned}$$

Proof. This is left to the reader in Exercise 7.6.7. \square

Example 7.6.9.

(1) A class of 30 students was surveyed to find out how many people 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 that every one in the class liked at least one of these foods. In the survey they 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. Then the survey says that $|B \cup P \cup I| = 30$, that $|B| = 11$, that $|P| = 16$, that $|I| = 17$, that $|B \cap P| = 5$, that $|B \cap I| = 4$ and that $|P \cap I| = 8$. By Theorem 7.6.7 (iv) we have

$$|B \cup P \cup I| = (|B| + |P| + |I|) - (|B \cap P| + |B \cap I| + |P \cap I|) + |B \cap P \cap I|,$$

which yields

$$30 = (11 + 16 + 17) - (5 + 4 + 8) + |B \cap P \cap I|.$$

Hence $|B \cap P \cap I| = 3$, which is the solution to our problem.

(2) We can now solve a problem stated at the beginning of this section, namely to find the number of integers from 1 to 1,000,000 that are not divisible by any of 3, 5 or 13. We start by defining the sets

$$X = \{n \in \mathbb{N} \mid 1 \leq n \leq 1,000,000\},$$

$$B_3 = \{n \in X \mid n \text{ is divisible by } 3\},$$

$$B_5 = \{n \in X \mid n \text{ is divisible by } 5\},$$

$$B_{13} = \{n \in X \mid n \text{ is divisible by } 13\}.$$

We wish to find $|X - (B_3 \cup B_5 \cup B_{13})|$, which we will do by Corollary 7.6.8. To find $|B_3|$, we note 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 $1,000,000/3$. Thus $|B_3| = 333,333$. Similar considerations show that $|B_5| = 200,000$ and $|B_{13}| = 76,923$. Next, an integer will be in $B_3 \cap B_5$ iff it is divisible by both 3 and 5. Thus $|B_3 \cap B_5|$ will be the greatest integer less than or equal to $1,000,000/15$, 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 7.6.8 we have

$$\begin{aligned}
 & |X - (B_3 \cup B_5 \cup B_{13})| \\
 &= |X| - (|B_3| + |B_5| + |B_{13}|) \\
 &\quad + (|B_3 \cap B_5| + |B_3 \cap B_{13}| + |B_5 \cap B_{13}|) - |B_3 \cap B_5 \cap B_{13}| \\
 &= 1,000,000 - (333,333 + 200,000 + 76,923) \\
 &\quad + (66,666 + 25,641 + 15,384) - 5,128 \\
 &= 492,307. \quad \diamond
 \end{aligned}$$

Another consequence of Theorem 7.6.7 is the following result, the statement of which may seem obvious, but is worth proving, because we will be using it in the next section.

Proposition 7.6.10. *Let A be a finite set, and let \sim be an equivalence relation on A . Suppose that all the equivalence classes are the same size. 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, \dots, A_N be the equivalence classes of A with respect to \sim . By hypothesis $|A_i| = S$ for all $i \in \{1, \dots, N\}$. Using Theorem 5.3.3 we know that $A_i \cap A_j = \emptyset$ for all $i, j \in \{1, \dots, N\}$ with $i \neq j$, and that $A = A_1 \cup \dots \cup A_N$. It now follows from Theorem 7.6.7 (ii) that $|A| = |A_1| + \dots + |A_N| = N \cdot S$. \square

Exercises

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?

7.6.2. Bonesville has 1000 residents. Explain why at least two of them must have the same initials, if they only use their first and last names, and if they only use letters from the English alphabet. If they use middle initials as well, must it be the case that two residents have the same initials? (For simplicity assume that every resident has precisely one middle name.)

7.6.3. A cheese factory labels each of its products 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?

7.6.4. The first 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 at the school. How many choices of delegations are there?

7.6.5. [Used in Section 7.6.] Give an alternate proof of Lemma 7.6.3 using induction on $|A|$, but without the Division Algorithm.

7.6.6. [Used in Section 7.6.] Prove that the map Φ defined in the proof of Theorem 7.6.2 is bijective.

7.6.7. [Used in Section 7.6.] Prove Corollary 7.6.8.

7.6.8. 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?

7.6.9. 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?

7.6.10. 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?

7.6.11. 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 he right?

7.6.12. Find the number of integers from 1 to 100,000 that are not divisible by any of 2, 5, 11 or 67.

7.7 Counting: Permutations and Combinations

In this section we are concerned with problems involving the choice of some objects out of a collection of objects, for example cards out of a deck, people out of a classroom, etc. In some problems the order of choosing matters, for example in choosing a president, vice-president and secretary for a three person committee 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. Some references for a standard discussion of these topics are [Bog90] and [Rob84]. In this section we will be using results from Section 7.6.

We start with some examples where the order of choosing matters. We will consider three types of problems. First, we saw in Example 7.6.1 (2) an example of choosing 2 things out of 6 where order matters. Second, suppose 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 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 right informally, though it would take mathematical 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, etc. All told, there are $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$ possibilities.

Our goal is to find general formulas to solve the above three types of problems. Rather than using the standard approach of repeatedly applying the product rule (via an often unstated mathematical induction), we will proceed by reformulating the above problems in terms of functions (and thus using mathematical induction). Recall the notation $\mathcal{F}(A, B)$, $\mathcal{I}(A, B)$ and $\mathcal{B}(A, B)$ defined in Section 4.5.

Suppose A and B are finite sets with $|A| = k$ and $|B| = n$. To find the number of ways of choosing k things out of n with replacement (meaning that the same object can be chosen repeatedly), where order matters, we need to find $|\mathcal{F}(A, B)|$. To find the number of ways of choosing k things out of n without replacement (meaning that each object can be chosen only once), where order matters, we need to find $|\mathcal{I}(A, B)|$. To find the number of ways of arranging n things, where order matters, we need to

find $|\mathcal{B}(A, B)|$. The values of $|\mathcal{F}(A, B)|$, $|\mathcal{I}(A, B)|$ 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 4.5.2 and Exercise 4.5.8. The following theorem gives formulas for $|\mathcal{F}(A, B)|$, $|\mathcal{I}(A, B)|$ and $|\mathcal{B}(A, B)|$ in terms of k and n .

In two of the formulas in the following theorem we will make use of factorials, as discussed in Example 6.4.4, where we discussed the factorial $n! = n(n - 1)(n - 2) \cdots 2 \cdot 1$ for all $n \in \mathbb{N}$. This formula does not work per se for $n = 0$, but for convenience we define $0! = 1$ (this definition may seem strange if you have not encountered it previously, but with some experience you will see that it works out perfectly). Recall also the formula $(n + 1)! = (n + 1)n!$ for all $n \in \mathbb{N}$.

Theorem 7.7.1. *Let $k, n \in \mathbb{Z}^{nn}$. Let A and B be finite sets with $|A| = k$ and $|B| = n$.*

- (i) *If $n = 0 = k$ then $|\mathcal{F}(A, B)| = 1$. If $n \neq 0$ or $k \neq 0$, then $|\mathcal{F}(A, B)| = n^k$.*
- (ii) *If $k > n$ then $|\mathcal{I}(A, B)| = 0$. If $k \leq n$ then $|\mathcal{I}(A, B)| = \frac{n!}{(n-k)!}$.*
- (iii) *If $k \neq n$ then $|\mathcal{B}(A, B)| = 0$. If $k = n$ then $|\mathcal{B}(A, B)| = n!$.*

Proof. (i). If $k = 0$, then $\mathcal{F}(A, B) = \{\emptyset\}$, and so $|\mathcal{F}(A, B)| = 1$. It is straightforward to see that the desired formulas hold in this case, both when $n = 0$ and when $n \neq 0$. We now prove the result for $k \geq 1$, using induction on k . Suppose first that $k = 1$, and that $n \in \mathbb{N}$ is any number. It is straightforward to see that $\mathcal{F}(A, B) \sim B$, and thus $|\mathcal{F}(A, B)| = n = n^1$ using Corollary 6.1.4. Hence the desired result holds when $k = 1$.

Now assume that the result holds for some k , and for all $n \in \mathbb{Z}^{nn}$. We will deduce the result for $k + 1$, and for all $n \in \mathbb{Z}^{nn}$. Let $n \in \mathbb{Z}^{nn}$ be fixed. We will show the result for $k + 1$ and this n . If $n = 0$, then $\mathcal{F}(A, B) = \emptyset$, and so $|\mathcal{F}(A, B)| = 0 = n^{k+1}$. Now suppose that $n \geq 1$. Choose elements $a \in A$ and $b \in B$, and define $F_{a,b} \subseteq \mathcal{F}(A, B)$ to be $F_{a,b} = \{f \in \mathcal{F}(A, B) \mid f(a) = b\}$. By Exercise 4.5.9 (1) we see that $F_{a,b} \sim \mathcal{F}(A - \{a\}, B)$. Hence $|F_{a,b}| = |\mathcal{F}(A - \{a\}, B)|$. Since $|A - \{a\}| = k$, it follows from the inductive hypothesis that $|\mathcal{F}(A - \{a\}, B)| = n^k$. Therefore $|F_{a,b}| = n^k$. Next, we observe that $\mathcal{F}(A, B) = \bigcup_{b \in B} F_{a,b}$ and that $F_{a,b} \cap F_{a,c} = \emptyset$ for all $b, c \in B$ with $b \neq c$. It follows from Theorem 7.6.7 (ii) that

$$|\mathcal{F}(A, B)| = \sum_{b \in B} |F_{a,b}| = \sum_{b \in B} n^k = n \cdot n^k = n^{k+1}.$$

(ii). This is left to the reader in Exercise 7.7.19.

(iii). First suppose that $k \neq n$. Then by Corollary 6.1.4 we see that $A \not\sim B$. Hence there is no bijective map $A \rightarrow B$, and thus $\mathcal{B}(A, B) = \emptyset$. Hence $|\mathcal{B}(A, B)| = 0$. Now suppose that $k = n$. It follows from Exercise 6.1.6 that $\mathcal{B}(A, B) = \mathcal{I}(A, B)$. It follows from part (ii) of this theorem that $|\mathcal{B}(A, B)| = |\mathcal{I}(A, B)| = \frac{n!}{(n-k)!} = n!$ \square

The number $\frac{n!}{(n-k)!}$ is called the number of permutations of n elements taken k at a time, and is often denoted $P(n, k)$ or ${}_nP_k$, or other similar notations.

Example 7.7.2.

(1) The license plates in a certain state have seven letters. How many different license plates can be made if all letters are allowed? Since there are 26 letters, by Theorem 7.7.1 (i) 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 select 3 people out of 10, where the order of selection matters. By Theorem 7.7.1 (ii) there are $\frac{10!}{(10-3)!} = 720$ 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 Theorem 7.7.1 (iii). By the theorem, 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. \diamond

We now turn to problems where the order of the chosen objects does not matter. We have two types of problems. First, suppose you go to a shoe store, and they have 6 pairs in your size. You might buy anywhere from none of the pairs to all 6 of them. How many choices can you make? Another type of problem would be to choose 5 cards out of a deck of cards. Again, how many ways can this happen? We cannot solve these problems by direct application of the sum and product rules (though it is possible to do so indirectly). This time we will reformulate our problem in terms of subsets of sets. These problems involve counting either the number of all possible subsets of a set, or the number of subsets of a given size.

The following theorem, which formalizes a fact that was stated without proof in Section 3.2, resolves the first type problem mentioned above. The intuitive idea 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 7.7.3. *Let A be a finite set. Then $|\mathcal{P}(A)| = 2^{|A|}$.*

Proof. We saw in Proposition 4.5.3 that $\mathcal{P}(A) \sim \mathcal{F}(A, \{0, 1\})$, and thus by Corollary 6.1.4 we know that $|\mathcal{P}(A)| = |\mathcal{F}(A, \{0, 1\})|$. By Theorem 7.7.1 (i) we know that $|\mathcal{F}(A, \{0, 1\})| = 2^{|A|}$. \square

If the reader finds the above proof unsatisfying, due to its reliance on some heavy machinery involving sets of functions, we note that it is also possible to prove this result by induction on the number of elements of A , without using sets of functions. Such a proof is left to the reader in Exercise 7.7.20.

Some texts use the notation 2^A to denote $\mathcal{P}(A)$, whether or not A is finite. This alternate notation might seem strange, but it does allow for the nice formula $|2^A| = 2^{|A|}$ when A is a finite set.

Example 7.7.4. You pass by a pizza shop that advertises that it has over 1000 varieties of pizza. You want to verify 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 thus a choice of a subset of the set of 10 toppings (the empty set corresponds to a cheese pizza). By Theorem 7.7.3 we know that the power set of a 10 element set has $2^{10} = 1024$ elements. Thus there are indeed over 1000 varieties of pizza (that some of them might be unpalatable is another matter). \diamond

We now turn to our second type of problem where order does not matter, in which we choose k elements out of an n element set, for a fixed number k .

Definition. Let A be a set. Let $k \in \mathbb{Z}$. We let $\mathcal{P}_k(A)$ denote the collection of all subsets of A with k elements, that is

$$\mathcal{P}_k(A) = \{S \in \mathcal{P}(A) \mid |S| = k\}.$$

Δ

Example 7.7.5. Let $A = \{a, b, c\}$. We saw in Example 3.2.5 that the subsets of A are $\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}$ and $\{a, b, c\}$. It is then

easy to count that $|\mathcal{P}_0(A)| = 1$, that $|\mathcal{P}_1(A)| = 3$, that $|\mathcal{P}_2(A)| = 3$, that $|\mathcal{P}_3(A)| = 1$, and that $|\mathcal{P}_k(A)| = 0$ whenever $k < 0$ or $k > 3$. \diamond

If a set A is infinite, then $\mathcal{P}_k(A)$ is infinite for any positive integer k . If a set A is finite, then the set $\mathcal{P}_k(A)$ will also be finite for any integer k ; The following theorem gives a formula for $|\mathcal{P}_k(A)|$.

Theorem 7.7.6. *Let $n \in \mathbb{Z}^{nn}$ and let $k \in \mathbb{Z}$. Let A be a set such that $|A| = n$. Then*

$$|\mathcal{P}_k(A)| = \frac{n!}{k!(n-k)!}$$

when $0 \leq k \leq n$, and $|\mathcal{P}_k(A)| = 0$ when $k < 0$ or $k > n$.

Proof. First, suppose that $n = 0$. Then $A = \emptyset$, and so $\mathcal{P}_0(A) = \{\emptyset\}$ and $\mathcal{P}_k(A) = \emptyset$ when $k \neq 0$. Thus $|\mathcal{P}_0(A)| = 1$ and $|\mathcal{P}_k(A)| = 0$ when $k \neq 0$. The desired formulas are seen to hold in these cases. From now on assume $n \geq 1$.

If $k < 0$, then it is clear that there are no subsets of A of order k , and hence $\mathcal{P}_k(A) = \emptyset$. Thus $|\mathcal{P}_k(A)| = 0$. If $k > n$, then it follows from Theorem 6.1.6 (iii) that $\mathcal{P}_k(A) = \emptyset$, and hence $|\mathcal{P}_k(A)| = 0$. If $k = 0$, then $\mathcal{P}_k(A) = \{\emptyset\}$, and so $|\mathcal{P}_k(A)| = 1$. Because $\frac{n!}{0!(n-0)!} = 1$, the theorem holds when $k = 0$.

We now turn to the case where $1 \leq k \leq n$. Let E be a set with k elements. Form the set $\mathcal{I}(E, A)$. Define a relation \sim on the set $\mathcal{I}(E, A)$ by letting $f \sim g$ iff $f_*(E) = g_*(E)$, for all $f, g \in \mathcal{I}(E, A)$. It is straightforward to verify that \sim is an equivalence relation. We now make two claims: (1) Each equivalence class of $\mathcal{I}(E, A)$ with respect to \sim has $k!$ elements; (2) the number of equivalence classes equals $|\mathcal{P}_k(A)|$. Once we prove these two claims, it will then follow from Proposition 7.6.10 that $|\mathcal{I}(E, A)| = |\mathcal{P}_k(A)|k!$. Since $|\mathcal{I}(E, A)| = \frac{n!}{(n-k)!}$ by Theorem 7.7.1 (ii), we deduce that $|\mathcal{P}_k(A)| = \frac{n!}{k!(n-k)!}$.

To prove claim (1), let $f \in \mathcal{I}(E, A)$. We want to find $|[f]|$. First, define $\hat{f}: E \rightarrow f_*(E)$ by letting $\hat{f}(x) = f(x)$ for all $x \in E$. Since f is injective, then \hat{f} is bijective. We now define a map $\Psi: [f] \rightarrow \mathcal{B}(f_*(E), f_*(E))$ by letting $\Psi(g) = g \circ \hat{f}^{-1}$ for all $g \in [f]$. To see that the definition of Ψ makes sense, let $g \in [f]$. Because $g_*(E) = f_*(E)$, it follows that $\Psi(g)$ is indeed a map $f_*(E) \rightarrow f_*(E)$. It is straightforward to see that $g \circ \hat{f}^{-1}$ is bijective, and so $\Psi(g) \in \mathcal{B}(f_*(E), f_*(E))$. Thus Ψ is well-defined. We leave it to the reader in Exercise 7.7.21 to show that the map Ψ is bijective. We then deduce that $|[f]| = |\mathcal{B}(f_*(E), f_*(E))|$. We note that

$|f_*(E)| = |E| = k$, and hence $|\mathcal{B}(f_*(E), f_*(E))| = k!$ by Theorem 7.7.1 (iii). Claim (1) then follows.

To prove claim (2), let $\mathcal{I}(E, A)/\sim$ denote the set of equivalence classes of $\mathcal{I}(E, A)$ with respect to \sim , as discussed in Section 5.3. Define a map $\Phi: \mathcal{I}(E, A)/\sim \rightarrow \mathcal{P}_k(A)$ by $\Phi([f]) = f_*(E)$ for all $f \in \mathcal{I}(E, A)$. We leave it to the reader in Exercise 7.7.21 to show that the map Φ is well-defined, and that it is bijective. Claim (2) then follows. \square

An alternative proof of the above result, using mathematical induction and some of the properties of binomial coefficients given below, but without sets of functions and equivalence relations, can be found in Exercise 7.7.22.

The formula given in the above theorem is so useful in mathematics that we make the following definition. We will shortly see why this name is used.

Definition. Let $n \in \mathbb{Z}^{nn}$ and let $k \in \mathbb{Z}$. We define the **binomial coefficient** $\binom{n}{k}$ as follows. If $0 \leq k \leq n$ we let

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

If $k < 0$ or $k > n$ we let $\binom{n}{k} = 0$. Δ

Other common notations for $\binom{n}{k}$ are $C(n, k)$ and ${}_nC_k$, the number of combinations of n elements taken k at a time. 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, since it is equal to the number of elements of a certain set by Theorem 7.7.6.

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, since there are a total of 20 people at the meeting, and since the order of the members of the committee does not matter, by Theorem 7.7.6 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 in each case. First, suppose 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. All told, 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) An important use of counting techniques is to compute probabilities. Although the computation of probabilities can be quite complicated, and has a whole theory behind it (see, for example, [Pit93] or [Ros93b]). We can use binomial coefficients to compute probabilities in some elementary cases. 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. Since 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 thus $4 \cdot \binom{13}{5} = 5148$. The probability of a flush is therefore $5148/2,598,960 \approx 0.00198$. The probabilities of other poker hands can be computed similarly.

(3) Probability calculations sometimes yield rather counter-intuitive results; we discuss here a well-known example of such a result. Suppose that we choose n random people, and then list their birthdays in the order in which they are chosen. (For simplicity, we will ignore leap year.) Assume that $1 \leq n \leq 365$. How many different outcomes are possible? The problem is the same as choosing n objects from a set of 365 objects, with repeats allowed, and order mattering. The total number of outcomes is therefore 365^n . Of these possible outcomes, how many have n different birthdays listed? That would be choosing n objects from the set of 365 objects, but this time with no repeats. We thus have $365 \cdot 364 \cdot \dots \cdot (365 - n + 1)$ possibilities. The remaining choices, of which there are $365^n - 365 \cdot 364 \cdot \dots \cdot (365 - n + 1)$, all have at least two people with the same birthday. Thus, the probability of having at least two people with the same birthday is

$$\begin{aligned} P_n &= \frac{365^n - 365 \cdot 364 \cdot \dots \cdot (365 - n + 1)}{365^n} \\ &= 1 - \frac{365 \cdot 364 \cdot \dots \cdot (365 - n + 1)}{365^n} = 1 - \frac{365 P_n}{365^n}. \end{aligned}$$

We can compute these probabilities using a calculator (scientific calculators often have keys for $_n P_k$), obtaining for example that $P_2 \approx 0.0027$, and that $P_3 \approx 0.0082$. Continuing with these calculations, we obtain the surprising result that $P_{23} \approx 0.507$, which says that if 23 people are randomly chosen, there is roughly a 50% chance that two people will have the same birthday. \diamond

We now prove a few basic properties of the binomial coefficients. Some of these properties will be useful to us here, while others are simply interesting (and have uses elsewhere). Further properties of the binomial coefficients can be found in the exercises for this section. For more than you ever wanted to know about the binomial coefficients (as well as some very clever arguments) see [GKP94, Chapter 5].

Proposition 7.7.8. *Let $n \in \mathbb{Z}^m$, and let $k \in \mathbb{Z}$.*

$$(i) \quad \binom{n}{0} = 1 = \binom{n}{n} \text{ and } \binom{n}{1} = n = \binom{n}{n-1}.$$

$$(ii) \quad \binom{n}{n-k} = \binom{n}{k}.$$

$$(iii) \quad \binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}.$$

Proof. We will prove part (iii), leaving the rest to the reader in Exercise 7.7.14. (iii). There are a number of cases, depending upon the value of k . First, suppose that $k < 0$. Then $\binom{n-1}{k} + \binom{n-1}{k-1} = 0 + 0 = 0 = \binom{n}{k}$. If $k = 0$, then making use of part (i) of this proposition we have $\binom{n-1}{k} + \binom{n-1}{k-1} = 1 + 0 = 1 = \binom{n}{k}$. Similar calculations show that the equation holds when $k = n$ or when $k > n$. We are left with the case $1 \leq k \leq n-1$. We then compute

$$\begin{aligned}
 \binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} \\
 &= \frac{(n-1)!}{k(k-1)!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)(n-k-1)!} \\
 &= \frac{(n-1)!}{(k-1)!(n-k-1)!} \left\{ \frac{1}{k} + \frac{1}{n-k} \right\} \\
 &= \frac{(n-1)!}{(k-1)!(n-k-1)!} \frac{n}{k(n-k)} \\
 &= \frac{n!}{k!(n-k)!} = \binom{n}{k}.
 \end{aligned}$$

Part (iii) of the above proposition leads to a convenient way of displaying and computing the binomial coefficients. Consider the following arrangement of the binomial coefficients:

$$\begin{matrix} & \binom{0}{0} \\ & \binom{1}{0} & \binom{1}{1} \\ \binom{2}{0} & \binom{2}{1} & \binom{2}{2} \\ \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \\ \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} \\ & \vdots \end{matrix}$$

Replacing the binomial coefficients with their numerical values, we obtain

$$\begin{matrix}
 & & & 1 \\
 & & 1 & & 1 \\
 & 1 & & 2 & & 1 \\
 1 & & 3 & & 3 & & 1 \\
 1 & & 4 & & 6 & & 4 & & 1 \\
 1 & 5 & 10 & & 10 & & 5 & & 1 \\
 & & & & \vdots
 \end{matrix}$$

Observe that each entry in the triangle can be computed by adding the two entries above it in the previous row. This observation is equivalent to Proposition 7.7.8 (iii), and allows for easy computation of binomial coefficients with small numbers. The left-right symmetry of the triangle is equivalent to Proposition 7.7.8 (ii). This triangle of binomial coefficients is known as Pascal's triangle, though it was known in China earlier than in Pascal's time; see [Ifr85, p. 396] for more details of the history. 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 7.7.9 (Binomial Theorem). *Let $n \in \mathbb{N}$ and let $x, y \in \mathbb{R}$. Then*

$$\begin{aligned}(x+y)^n &= x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + y^n \\ &= \sum_{i=0}^n \binom{n}{i}x^{n-i}y^i.\end{aligned}$$

Proof. The proof is by induction on n . When $n = 1$, then

$$(x+y)^1 = x+y = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1 = \sum_{i=0}^1 \binom{1}{i}x^{1-i}y^i,$$

which is the desired result. Now suppose that the result is true for n . Making use of Proposition 7.7.8 (i), (iii) we compute

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n = (x+y) \sum_{i=0}^n \binom{n}{i}x^{n-i}y^i \\ &= \sum_{i=0}^n \binom{n}{i}x^{n-i+1}y^i + \sum_{i=0}^n \binom{n}{i}x^{n-i}y^{i+1} \\ &= \sum_{i=0}^n \binom{n}{i}x^{(n+1)-i}y^i + \sum_{i=1}^{n+1} \binom{n}{i-1}x^{n-(i-1)}y^{(i-1)+1}\end{aligned}$$

$$\begin{aligned}
&= \binom{n}{0} x^{n+1} + \sum_{i=1}^n \left[\binom{n}{i} + \binom{n}{i-1} \right] x^{(n+1)-i} y^i + \binom{n}{n} y^{n+1} \\
&= \binom{n+1}{0} x^{n+1} + \sum_{i=1}^n \binom{n+1}{i} x^{(n+1)-i} y^i + \binom{n+1}{n+1} y^{n+1} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} x^{(n+1)-i} y^i.
\end{aligned}$$

□

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 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 techniques we have learned.

Proposition 7.7.10. *Let $n \in \mathbb{Z}^{nn}$. Then*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Proof. First Proof: This proof is by induction on n . The result is easily seen to hold when $n = 0$ or $n = 1$, since $\binom{0}{0} = 1 = 2^0$, and $\binom{1}{0} + \binom{1}{1} = 1 + 1 = 2 = 2^1$. Now suppose that the result holds for n . We then use Proposition 7.7.8 (iii) and the inductive hypothesis to compute

$$\begin{aligned}
\sum_{k=0}^{n+1} \binom{n+1}{k} &= \sum_{k=0}^{n+1} \left\{ \binom{n}{k} + \binom{n}{k-1} \right\} = \sum_{k=0}^{n+1} \binom{n}{k} + \sum_{k=0}^{n+1} \binom{n}{k-1} \\
&= \sum_{k=0}^n \binom{n}{k} + \binom{n}{n+1} + \binom{n}{-1} + \sum_{k=1}^{n+1} \binom{n}{k-1} \\
&= \sum_{k=0}^n \binom{n}{k} + \binom{n}{n+1} + \binom{n}{-1} + \sum_{k=0}^n \binom{n}{k} \\
&= 2^n + 0 + 0 + 2^n = 2 \cdot 2^n = 2^{n+1}.
\end{aligned}$$

Second Proof: This proof uses Theorem 7.7.6, which interprets the binomial coefficients as the numbers of subsets of appropriate sizes. Let A be a set with n elements. We observe that

$$\mathcal{P}(A) = \mathcal{P}_0(A) \cup \mathcal{P}_1(A) \cup \cdots \cup \mathcal{P}_n(A).$$

Moreover, we have $\mathcal{P}_i(A) \cap \mathcal{P}_k(A) = \emptyset$ for $i, k \in \{0, \dots, n\}$ with $i \neq k$. Using Theorem 7.6.7 (ii) we deduce

$$|\mathcal{P}(A)| = |\mathcal{P}_0(A)| + |\mathcal{P}_1(A)| + \cdots + |\mathcal{P}_n(A)|.$$

By Theorems 7.7.3 and 7.7.6 we see that

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}.$$

Third Proof: This proof makes use of the Binomial Theorem (Theorem 7.7.9). Since that theorem holds for all values of x and y , it holds in particular in the case when $x = 1 = y$. Plugging these values into the Binomial Theorem yields

$$2^n = (1+1)^n = \sum_{i=0}^n \binom{n}{i} 1^{n-i} 1^i = \sum_{i=0}^n \binom{n}{i}. \quad \square$$

We conclude our treatment of counting issues with the so-called “hat check problem,” which makes use of a number of the ideas we have learned. Suppose 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 (2), 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 $T(n)$, since this is just the number of ways of arranging n things, where order matters. Thus $T(n) = n!$ by Theorem 7.7.1 (iii).

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. Let A be a set with n elements, where $n \in \mathbb{N}$. Then each derangement of n objects corresponds to a bijective map $f: A \rightarrow A$ such that $f(a) \neq a$ for all $a \in A$. To use standard terminology, a fixed point of a map $f: A \rightarrow A$ is a point $x \in A$ such that $f(x) = x$. We are thus interested in bijective maps $A \rightarrow A$ with no fixed points. The following theorem gives a formula for $S(n)$.

Theorem 7.7.11. Let $n \in \mathbb{N}$ and let A be a set such that $|A| = n$. Let $F = \{f \in \mathcal{B}(A, A) \mid f(a) \neq a \text{ for all } a \in A\}$. Then

$$|F| = n! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^n \frac{1}{n!} \right).$$

Proof. Suppose that $A = \{a_1, \dots, a_n\}$. Let $i \in \{1, \dots, n\}$. We define $G_i = \{f \in \mathcal{B}(A, A) \mid f(a_i) = a_i\}$. Note that if $f \in G_i$, it might also be the case that $f(a_k) = a_k$ for some $k \in \{1, \dots, n\}$ with $k \neq i$. It follows from Exercise 4.5.9 (3) that there is a bijective map from G_i to $\mathcal{B}(A - \{a_i\}, A - \{a_i\})$. Hence $|G_i| = (n-1)!$, using Theorem 7.7.1 (iii). Now suppose we have $i_1, \dots, i_p \in \{1, \dots, n\}$ such that $i_1 < i_2 < \cdots < i_p$, for some $p \in \{1, \dots, n\}$. Then

$$G_{i_1} \cap \cdots \cap G_{i_p} = \{f \in \mathcal{B}(A, A) \mid f(a_{i_1}) = a_{i_1}, \dots, f(a_{i_p}) = a_{i_p}\}.$$

It can be verified, similarly to Exercise 4.5.9 (3), that there is a bijective map from $G_{i_1} \cap \cdots \cap G_{i_p}$ to $\mathcal{B}(A - \{a_{i_1}, \dots, a_{i_p}\}, A - \{a_{i_1}, \dots, a_{i_p}\})$. Using Theorem 7.7.1 (iii) we deduce that $|G_{i_1} \cap \cdots \cap G_{i_p}| = (n-p)!$.

Observe that $F = \mathcal{B}(A, A) - (G_1 \cup \cdots \cup G_n)$. From Theorem 7.7.1 (iii) we know that $|\mathcal{B}(A, A)| = n!$. Using Corollary 7.6.8 we then compute

$$\begin{aligned} |F| &= |\mathcal{B}(A, A) - (G_1 \cup \cdots \cup G_n)| \\ &= |\mathcal{B}(A, A)| + \sum_{p=1}^n (-1)^p \sum_{1 \leq i_1 < \cdots < i_p \leq n} |G_{i_1} \cap \cdots \cap G_{i_p}| \\ &= n! + \sum_{p=1}^n (-1)^p \sum_{1 \leq i_1 < \cdots < i_p \leq n} (n-p)! \\ &= n! + \sum_{p=1}^n (-1)^p (n-p)! \sum_{1 \leq i_1 < \cdots < i_p \leq n} 1. \end{aligned}$$

For each $p \in \{1, \dots, n\}$, observe that $\sum_{1 \leq i_1 < \cdots < i_p \leq n} 1$ is simply the number of different ways of choosing p distinct numbers out of the set $\{1, \dots, n\}$, which is equal to $\binom{n}{p}$ by Theorem 7.7.6. Hence

$$\begin{aligned} |F| &= n! + \sum_{p=1}^n (-1)^p (n-p)! \binom{n}{p} = n! + \sum_{p=1}^n (-1)^p (n-p)! \frac{n!}{p!(n-p)!} \\ &= n! + \sum_{p=1}^n (-1)^p \frac{n!}{p!} = n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!} \\ &= n! \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^n \frac{1}{n!} \right). \end{aligned}$$

□

Returning to the hat check problem, we now see 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 6 people the probability is approximately 0.36667. It is interesting to note that as $n \rightarrow \infty$, the probability goes to $1/e$, as can be seen using the power series for e^x (consult most any calculus text for this power series).

Exercises

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?

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*?

7.7.3. A group of 8 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?

7.7.4. You have 5 books in Esperanto and 5 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?

7.7.5. A horse race has 8 horses, out of which 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?

7.7.6. We want to select 5 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 3 consonants followed by 2 vowels?
- (3) How many different ways can this selection be done if we write 4 consonants followed by 1 vowel, or 5 consonants and no vowels?

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?

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?

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 $\mathcal{P}_4(X)$.

7.7.10. Xavier has 6 pairs of cotton pants, and 4 pairs of wool pants. He needs to take 5 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 3 pairs of cotton pants and 2 pairs of wool pants?

7.7.11. The Al Jolson fan club of Flugletown has 8 men and 5 women, including Mr. and Ms. Atiyah-Singer. The club want to pick a steering committee.

- (1) How many possible 5 person committees can be formed?
- (2) How many possible 4 or 5 person committees can be formed?

(3) How many possible 4 person committees can be formed if there must be 2 men and 2 women on the committee?

(4) How many possible 4 person committees can be formed if there must be 2 men and 2 women on the committee, and not both Mr. and Ms. Atiyah-Singer are allowed to be on the committee at the same time?

7.7.12. You choose 3 cards from a deck of cards. Find the probability of drawing each of the following options.

- (1) 3 red cards.
- (2) A face card.
- (3) 3 Aces.
- (4) 2 Queens and 1 Jack.
- (5) 3 cards of the same suit.
- (6) 3 Aces or 3 Kings.

7.7.13. Expand the following expressions.

- (1) $(a + 3b)^6$.
- (2) $(2x + \frac{1}{x})^7$.

7.7.14. [Used in Section 7.7.] Prove Proposition 7.7.8 (i) and (ii).

7.7.15. Let $n, s \in \mathbb{Z}^{nn}$, 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 $k \neq 0$.
- (2) $\binom{n}{s} \binom{s}{k} = \binom{n}{k} \binom{n-k}{s-k}$, when $k \leq n$.
- (3) $\binom{n}{2} + \binom{n+1}{2} = n^2$.
- (4) $\binom{n+2}{3} - \binom{n}{3} = n^2$.

7.7.16. Let $n, s \in \mathbb{Z}^{nn}$. Prove that the following formulas hold.

- (1) $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.
- (2) $\sum_{k=0}^n \binom{s+k}{k} = \binom{s+n+1}{n}$.
- (3) $\sum_{k=0}^n \binom{k}{s} = \binom{n+1}{s+1}$.

7.7.17. (1) Let $n \in \mathbb{Z}^{nn}$. Show that

$$\sum_{\substack{k \text{ even} \\ 0 \leq k \leq n}} \binom{n}{k} = \sum_{\substack{k \text{ odd} \\ 0 \leq k \leq n}} \binom{n}{k}.$$

(2) Let A be a finite set. Let $\mathcal{P}_E(A)$, respectively $\mathcal{P}_O(A)$, denote the collection of all subsets of A with an even, respectively odd, number of elements. Show that $|\mathcal{P}_E(A)| = |\mathcal{P}_O(A)|$.

7.7.18. In Figure 7.7.1 are indicated certain diagonals in Pascal's triangle.

(1) Make a conjecture for a formula for the sums of the entries along these diagonals. State your conjecture in terms of binomial coefficients. (Recall the Fibonacci numbers discussed in Section 6.4.)

(2) Prove your conjecture.

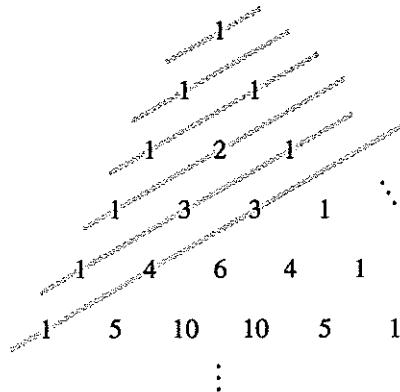


Figure 7.7.1.

7.7.19. [Used in Section 7.7.] Prove Theorem 7.7.1 (ii).

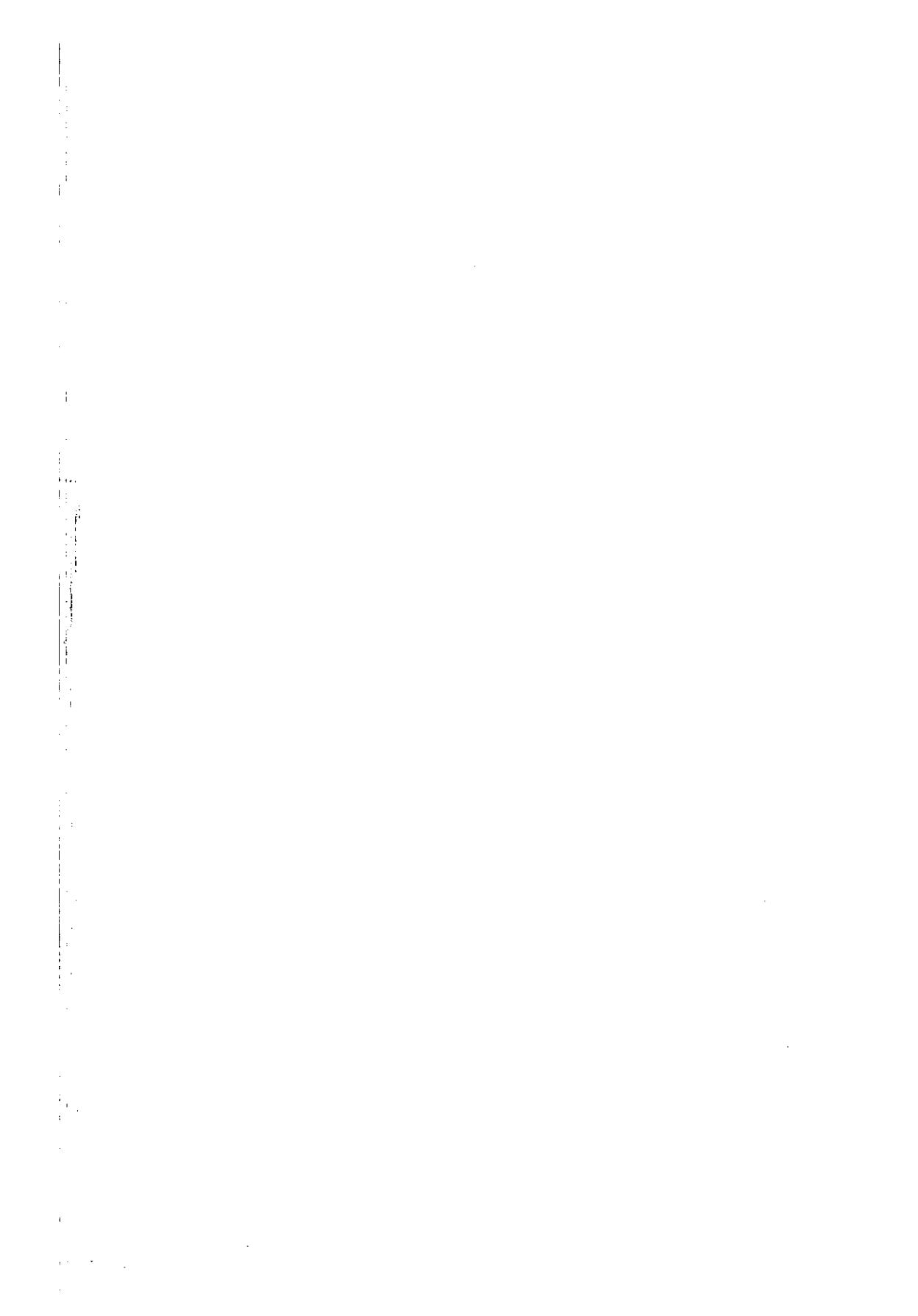
7.7.20. [Used in Section 7.7.] Prove Theorem 7.7.3 directly by induction on the number of elements in A , without making use of Proposition 4.5.3.

7.7.21. [Used in Section 7.7.] Let Ψ and Φ be the maps defined in the proof of Theorem 7.7.6. Show that map Φ is well-defined, and that both Φ and Ψ are bijective.

7.7.22. [Used in Section 7.7.] Prove Theorem 7.7.6 directly by induction on n , without using sets of functions. Only the case $0 \leq k \leq n$ needs to be treated, since the other cases were directly taken care of at the start of the proof of Theorem 7.7.6.

7.7.23. Let A and B be sets (not necessarily finite). Prove that $A \sim B$ implies that $\mathcal{P}_k(A) \sim \mathcal{P}_k(B)$ for all $k \in \mathbb{Z}^m$. (Note that you cannot use Theorem 7.7.6, since A and B need not be finite.)

7.7.24. Let $f : A \rightarrow B$ be a map 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.



8

Number Systems

The integers have been made by God. All else is the work of man.

Leopold Kronecker (1823–1891)

8.1 Back to the Beginning

We end our mathematical journey by going back to the beginning. Up till now we have used various sets of numbers, for example the natural numbers, the integers, the rational numbers and the real numbers, and have assumed familiarity with the standard properties of these numbers, for example commutativity and associativity of addition and multiplication of numbers. For the most part we have used these numbers only in examples of the concepts we defined using sets, and did not have to rely on these numbers for our formal definitions and proofs. (There are a few exceptions to this claim, such as when we used properties of the natural numbers in Chapter 6 and in Sections 7.6 and 7.7, but we will not be using the discussion from those sections in the present chapter.)

What precisely are these numbers that we use on a daily basis, and how do we know that they work the way we think they do intuitively? The study of numbers goes back to the ancient world (though it was only much more recently that the standard number systems were put on a firm mathemat-

ical foundations); a complete answer to our questions would involve history, philosophy and mathematics. Given our limited space, we go straight to the mathematical details, with an axiomatic treatment of the standard sets of numbers (except for the real numbers, which require a lengthier discussion). We start, as is commonly done, with an axiomatization of the natural numbers. We then construct the integers from the natural numbers, and the rational numbers from the integers, and we conclude the chapter with a brief mention of the construction of the real numbers from the rationals, and a more detailed treatment of the much simpler construction of the complex numbers from the reals. See [CE63] or [Fef64] for more thorough treatments of the topic in this chapter. Details of the construction of the real numbers from the rational numbers can also be found in many real analysis texts (see, for example, [Pow94, Section 2.7]). For historical accounts of the development of the number systems, see [Eea90, Chapters 1–3], [SR81] or [Die92, Section 6.2]. (Books on the history of numbers that are aimed at a more popular audience, such as [Fle83] and [Ifr85], contain many interesting cultural facts, but tend to focus more on notations for writing numbers than on the mathematical properties of numbers.)

The material in this chapter, which is not only of inherent interest, and fundamental to a thorough understanding of the number systems, but makes extensive use of the material from previous chapters, provides a suitable grand finale to our treatment of the foundations of modern mathematics.

8.2 The Natural Numbers

We start our treatment of the number systems with the widely used Peano Postulates for the natural numbers. We will simply accept the Peano Postulates as given, and proceed to prove various properties of the natural numbers starting from these axioms. It is possible to derive the existence of a set satisfying the Peano Postulates from the axioms of Zermelo–Fraenkel set theory (mentioned briefly in Section 3.2); see [Vau95, Chapters 2–3] and [Mor87, Chapter 5] for further discussion.

To make an efficient axiomatization for the natural numbers, we need to strip these numbers down to their bare essentials. Intuitively, we know various things about the natural numbers, such as the existence and basic properties of the binary operations addition and multiplication, and the relation “less than.” How few of these notions can we take as axioms, from which we can deduce everything else that we need to know about the natural numbers? It turns out, although it is far from obvious, that the property

of the natural numbers that distinguishes these numbers from other number systems is the ability to prove things by mathematical induction. (We discussed standard applications of mathematical induction in Section 6.3; at present we are concerned only with its theoretical ramifications.)

Although we think of the natural numbers as having the two operations addition and multiplication, we will see that we need only the ability to add 1 to each natural number in order to state the notion of proof by mathematical induction. Hence, in bare bones form, the natural numbers will consist of a set, a distinguished element (intuitively, the number 1), and one operation on the set (intuitively, the map from the set of natural numbers to itself that adds 1 to each natural number). These three entities will be required to satisfy a few simple properties, one of which is the ability to prove things by mathematical induction. Addition and multiplication will be constructed from these more fundamental properties.

Because the natural numbers will be given axiomatically as a set with a distinguished element and a map from itself to itself, we start with the following convenient definition.

Definition. A Henkin set is a triple (H, e, k) , where H is a non-empty set, where $e \in H$ and where $k: H \rightarrow H$ is a map. Δ

The next definition gives our set of axioms that characterize the natural numbers. Intuitively, we can think of the function $s: N \rightarrow N$ in this definition as the function given by $s(n) = n + 1$ for all $n \in N$, though formally we have not yet defined the operation “+” (we will show that our intuitive approach is correct in Theorem 8.2.3).

Definition. Let $(N, 1, s)$ be a Henkin set. We say $(N, 1, s)$ satisfies the Peano Postulates if the following three properties hold.

- (1) There is no $n \in N$ such that $s(n) = 1$.
- (2) The map s is injective.
- (3) Suppose $G \subseteq N$ has the properties that $1 \in G$, and that if $g \in G$ then $s(g) \in G$. Then $G = N$. Δ

Part (1) of the Peano Postulates says that 1 is, intuitively, the “first” number in N . (It would also have worked to choose 0 as the “first” number to be used, in which case a set of axioms similar to the Peano Postulates would yield the set $\{0, 1, 2, \dots\}$.) Parts (1) and (2) together are needed to insure that $(N, 1, s)$ is infinite. To see why, let $M = \{1, a\}$, and let $s: M \rightarrow M$ be defined by $s(1) = a$ and $s(a) = a$. It is straightforward

to see that the analog of parts (1) and (3) of the postulates holds for the Henkin set $(M, 1, s)$, even though M is not what we would intuitively call the set of natural numbers; of course, this function s does not satisfy part (2) of the Peano Postulates. A similar example (using the same set M , and with $s(1) = a$ and $s(a) = 1$) shows that a finite set may satisfy parts (2) and (3) of the postulates, but not part (1). Thus, to insure that a set satisfying the Peano Postulates truly models the natural numbers, we need both parts (1) and (2) of the postulates, or something like them. That we need something like part (3) of the postulates seems reasonable, if we want to use mathematical induction.

For the rest of this chapter we will always use the symbol $(N, 1, s)$ to denote a Henkin set satisfying the Peano Postulates, and we will think of N as the natural numbers. We cannot *prove* that N is precisely what our intuition tells us it should be, because we cannot prove things about our intuition. The best we can do, and we will indeed do this, is to prove that N satisfies all the basic properties we can think of for the natural numbers. Formally, we simply define the natural numbers to be the set N .

Before we can deal with familiar aspects of the natural numbers such as addition and multiplication, two preliminary results about $(N, 1, s)$ are needed. The first is the following somewhat abstract but very important theorem, which will be useful when we define addition and multiplication. We saw in Section 6.4 that this theorem is essentially just a formal statement of the notion of recursive definition. See Section 6.4 for more details. The proof of this theorem is rather long and tedious, and might certainly be skipped upon a first reading; the proof is found in Section 8.7. (This proof uses nothing other than the Peano Postulates, and is delayed only to avoid interrupting the discussion in the present section.)

Theorem 8.2.1. *Let (H, e, k) be a Henkin set. Then there is a unique map $f: N \rightarrow H$ such that $f(1) = e$ and $f \circ s = k \circ f$.*

The equation $f \circ s = k \circ f$ in the statement of the above theorem means that $f(s(n)) = k(f(n))$ for all $n \in N$, and it can be expressed by saying that the following diagram is commutative (in the sense discussed in Section 4.3).

$$\begin{array}{ccc} N & \xrightarrow{s} & N \\ f \downarrow & & \downarrow f \\ H & \xrightarrow{k} & H \end{array}$$

Our next preliminary result is much more concrete than the previous one, and its statement certainly fits in with our intuitive sense of the natural numbers.

Lemma 8.2.2. *Let $a \in N$. If $a \neq 1$, then there is unique $b \in N$ such that $a = s(b)$.*

Proof. We start with uniqueness. Suppose there are $n, m \in N$ such that $a = s(n)$ and $a = s(m)$. Then $s(n) = s(m)$. By the injectivity of s , which is part (2) of the Peano Postulates, then $n = m$.

To prove existence, we define the set

$$G = \{1\} \cup \{c \in N \mid \text{there is some } b \in N \text{ such that } s(b) = c\}.$$

We will use part (3) of the Peano Postulates to prove that $G = N$; the existence part of the lemma will then follow immediately. It is clear that $G \subseteq N$ and that $1 \in G$. Now suppose $n \in G$. We need to show that $s(n) \in G$. Let $p = s(n)$. To show that $p \in G$, we have to show that either $p = 1$ or $p \in \{c \in N \mid \text{there is some } b \in N \text{ such that } s(b) = c\}$; we will prove the latter. To show this, we need to find some $b \in N$ such that $s(b) = p$. Let $b = n$. Then $s(b) = p$ is true by the definition of p . Thus $p \in \{c \in N \mid \text{there is some } b \in N \text{ such that } s(b) = c\}$, so $p \in G$, and therefore $s(n) \in G$. Hence $G = N$. \square

We are now ready to define the operations addition and multiplication for the natural numbers, using only the Peano Postulates, and the two results we have seen so far. Addition and multiplication are binary operations; see Section 7.1 for the definition of this concept. As discussed in that section, although we formally write addition as a function $+ : N \times N \rightarrow N$, for convenience we will write $a + b$ rather than $+(a, b)$; similarly for multiplication.

Addition on N is given by the following theorem. Though it might not be evident at first why we choose the two properties given in the theorem rather than other more common properties, with hindsight they turn out to work well, allowing for nice proofs of other properties of addition.

Theorem 8.2.3. *There is a unique binary operation $+ : N \times N \rightarrow N$ such that the following two conditions hold.*

- (i) *If $a \in N$ then $a + 1 = s(a)$.*
- (ii) *If $a, b \in N$ then $a + s(b) = s(a + b)$.*

Proof. Let $p \in N$. Then the triple $(N, s(p), s)$ is a Henkin set. By Theorem 8.2.1 there is a unique map $f_p: N \rightarrow N$ such that $f_p(1) = s(p)$ and $f_p \circ s = s \circ f_p$. (There is a distinct map f_a for each $a \in N$.) We now define a function $+: N \times N \rightarrow N$ as follows. Let $(a, b) \in N \times N$. Then define $a + b = f_a(b)$. To show property (i), let $a \in N$. Then $a + 1 = f_a(1) = s(a)$. To show property (ii), let $a, b \in N$. Then $a + s(b) = f_a(s(b)) = (f_a \circ s)(b) = (s \circ f_a)(b) = s(f_a(b)) = s(a + b)$. \square

Part (i) of the above theorem says that the map s works exactly as we had initially thought of it intuitively.

The following theorem gives some of the standard properties of addition of natural numbers. The main technique of proof for these properties is part (3) of the Peano Postulates. The different parts of the theorem have been arranged so that to prove each, it is permissible to use everything stated up till then, but not subsequently. For example, we will not use commutativity of addition (part (iv)) in the proofs of parts prior to part (iv). This same strategy of using only previously stated results will hold throughout this chapter.

Theorem 8.2.4. *Let $a, b, c \in N$.*

- (i) *If $a + c = b + c$, then $a = b$.*
- (ii) *$(a + b) + c = a + (b + c)$.*
- (iii) *$1 + a = s(a) = a + 1$.*
- (iv) *$a + b = b + a$.*
- (v) *$a + b \neq 1$.*
- (vi) *$a + b \neq a$.*

Proof. We will prove parts (i), (v) and (vi); the other parts are left to the reader in Exercise 8.2.3.

(i). Let

$$G = \{z \in N \mid \text{if } x, y \in N \text{ and } x + z = y + z, \text{ then } x = y\}.$$

To prove the desired result, we will show that $G = N$. Clearly $G \subseteq N$. To show that $1 \in G$, suppose that $j, k \in N$ and $j + 1 = k + 1$. Then $s(j) = s(k)$ by Theorem 8.2.3 (i), and so $j = k$ by the injectivity of s (part (2) of the Peano Postulates). Hence $1 \in G$. Now suppose $r \in G$. Suppose

further that $j, k \in N$ and that $j + s(r) = k + s(r)$. By Theorem 8.2.3 (ii) we deduce that $s(j + r) = s(k + r)$. Since s is injective, it follows that $j + r = k + r$. Because $r \in G$, it follows that $j = k$. Hence $j + s(r) = k + s(r)$ implies $j = k$, and thus $s(r) \in G$. Hence $G = N$ by part (3) of the Peano Postulates.

(v). Suppose that $a + b = 1$; we will derive a contradiction. There are two cases. First, suppose that $b = 1$. Then $1 = a + b = a + 1 = s(a)$, which contradicts part (1) of the Peano Postulates. Now suppose $b \neq 1$. By Lemma 8.2.2 there is some $x \in N$ such that $s(x) = b$. By Theorem 8.2.3 (ii) we have $1 = a + b = a + s(x) = s(a + x)$, again a contradiction to part (1) of the Peano Postulates.

(vi). Let

$$H = \{z \in N \mid \text{if } y \in N \text{ then } z + y \neq z\}.$$

It will suffice to show that $H = N$. Clearly $H \subseteq N$. To show that $1 \in H$, suppose otherwise, so that there is some $k \in N$ such that $1 + k = 1$. Then by part (iii) of this theorem we have $s(k) = 1$, which contradicts part (1) of the Peano Postulates. Hence $1 \in H$. Now suppose $r \in H$. Suppose further that there is some $k \in N$ such that $s(r) + k = s(r)$. By part (iv) of this theorem, we see that $k + s(r) = s(r)$, and then by Theorem 8.2.3 (ii), we deduce that $s(k + r) = s(r)$. Since s is injective (part (2) of the Peano Postulates), it follows that $k + r = r$. By part (iv) of this theorem, we have $r + k = r$. Since $r \in H$, we have a contradiction. Hence there is no $k \in N$ such that $s(r) + k = s(r)$. Therefore $s(r) \in H$. Hence $H = N$. \square

The following two theorems define and describe the main properties of multiplication of natural numbers, similarly to what we have just seen for addition.

Theorem 8.2.5. *There is a unique binary operation $\cdot : N \times N \rightarrow N$ such that the following two conditions hold.*

(i) *If $a \in N$ then $a \cdot 1 = a$.*

(ii) *If $a, b \in N$ then $a \cdot s(b) = (a \cdot b) + a$.*

Proof. Let $q \in N$. Define a function $h_q : N \rightarrow N$ by $h_q(m) = m + q$ for all $m \in N$. The triple (N, q, h_q) is a Henkin set, and by Theorem 8.2.1 there is a unique map $g_q : N \rightarrow N$ such that $g_q(1) = q$ and $g_q \circ s = h_q \circ g_q$. (There is a distinct map g_a for all $a \in N$.) We now define a function $\cdot : N \times N \rightarrow N$ as follows. Let $(a, b) \in N \times N$. Then define $a \cdot b = g_a(b)$.

The proof that properties (i) and (ii) of the theorem hold is left to the reader in Exercise 8.2.4. \square

Theorem 8.2.6. *Let $a, b, c \in N$.*

- (i) $a \cdot 1 = a = 1 \cdot a$.
- (ii) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.
- (iii) $a \cdot b = b \cdot a$.
- (iv) $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$.
- (v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (vi) *If $a \cdot b = a \cdot c$ then $b = c$.*
- (vii) *$a \cdot b = 1$ iff $a = b$.*

Proof. We will prove parts (i) and (vi); the other parts are left to the reader in Exercise 8.2.5. We know from Theorem 8.2.5 (i) that $x \cdot 1 = x$ for all $x \in N$; we therefore need to prove only that $1 \cdot x = x$ for all $x \in N$. Let

$$G = \{z \in N \mid 1 \cdot z = z\}.$$

By Theorem 8.2.5 (i) we know that $1 \cdot 1 = 1$, and thus $1 \in G$. Suppose $x \in G$. Combining Theorem 8.2.5 (ii), the hypothesis on x and Theorem 8.2.3 (i), we see that $1 \cdot s(x) = (1 \cdot x) + 1 = x + 1 = s(x)$. Thus $s(x) \in G$. Hence $G = N$, and the desired result follows.

(vi). Let

$$H = \{y \in N \mid \text{if } x, z \in N \text{ and } x \cdot y = x \cdot z, \text{ then } y = z\}.$$

We first show that $1 \in H$. Suppose that $j, k \in N$ and that $j \cdot 1 = j \cdot k$. We will deduce that $k = 1$, and it will follow that $1 \in H$. Assume that $k \neq 1$. By Lemma 8.2.2 there is some $t \in N$ such that $k = s(t)$. Then $j = j \cdot 1 = j \cdot k = j \cdot s(t) = (j \cdot t) + j = j + (j \cdot t)$, using by Theorems 8.2.5 (i), (ii) and 8.2.4 (iv). We now have a contradiction to Theorem 8.2.4 (vi). Thus $k = 1$, and hence $1 \in H$.

Now let $r \in H$. Suppose further that we have $j, k \in N$ such that $j \cdot s(r) = j \cdot k$. By Theorem 8.2.5 (ii) we deduce that $(j \cdot r) + j = j \cdot k$. We have two cases, either $k = 1$ or $k \neq 1$. Assume first that $k = 1$. Then by Theorem 8.2.5 (i) we have $(j \cdot r) + j = j$, and by Theorem 8.2.4

(iv) it follows that $j + (j \cdot r) = j$, a contradiction to Theorem 8.2.4 (vi). Thus $k \neq 1$. By Lemma 8.2.2 there is some $t \in N$ such that $k = s(t)$. Thus $(j \cdot r) + j = j \cdot s(t) = (j \cdot t) + j$. Using Theorem 8.2.4 (i) we deduce that $j \cdot r = j \cdot t$. Because $r \in H$, it follows that $r = t$. Therefore $s(r) = s(t) = k$. Thus $s(r) \in H$. Hence $H = N$ by part (3) of the Peano Postulates, and the proof is complete. \square

Addition and multiplication are the two most important binary operations on the natural numbers. The most important relations on the natural numbers are “less than” and “less than or equal to,” to which we now turn.

Definition. Let $<$ be the relation on N given by $a < b$ iff there exists $p \in N$ such that $a + p = b$, for all $a, b \in N$. Let \leq be the relation on N given by $a \leq b$ iff $a < b$ or $a = b$, for all $a, b \in N$. Δ

As we would expect, if $a, b \in N$ are such that $a < b$, then the element $p \in N$ such that $a + p = b$ is unique. See Exercise 8.2.7. The following theorem gives some of the basic properties of $<$ and \leq .

Theorem 8.2.7. *Let $a, b, c, d \in N$.*

- (i) $a \leq a$ and $a < s(a)$.
- (ii) $1 \leq a$.
- (iii) If $a < b$ and $b < c$, then $a < c$.
- (iv) $a < b$ iff $s(a) < s(b)$.
- (v) $a \leq b$ iff $a < s(b)$.
- (vi) $a < b$ iff $s(a) \leq b$.
- (vii) $a < b$ iff $a + c < b + c$.
- (viii) $a < b$ iff $a \cdot c < b \cdot c$.

Proof. We will prove parts (ii) and (v); the other parts are left to the reader in Exercise 8.2.6.

(ii). There are two cases. First, suppose that $a = 1$. Then certainly $1 \leq a$. Second, suppose that $a \neq 1$. By Lemma 8.2.2 there is some $p \in N$ such that $a = s(p)$. By Theorem 8.2.4 (iii) we see that $a = 1 + p$. Hence $1 < a$, and therefore $1 \leq a$.

(v). First suppose that $a \leq b$. Thus $a = b$ or $a < b$. If $a = b$, then by part (i) of this theorem we have $a < s(a) = s(b)$. If $a < b$, then since $b < s(b)$ by part (i) of this theorem, it follows that $a < s(b)$ by part (iii).

Now suppose that $a < s(b)$. Hence there is some $g \in N$ such that $a + g = s(b)$. Using Theorem 8.2.3 (i) we see that $a + g = b + 1$. We now have two cases. First, suppose that $g = 1$. Then $a + 1 = b + 1$. By Theorem 8.2.4 (i) it follows that $a = b$. Now suppose that $g \neq 1$. Then by Lemma 8.2.2 there is some $p \in N$ such that $g = s(p)$. By Theorem 8.2.3 (i) we have $g = p + 1$. Hence $a + (p + 1) = b + 1$. By Theorem 8.2.4 (ii) we have $(a + p) + 1 = b + 1$, and by part (i) of the same theorem, we deduce $a + p = b$. Thus $a < b$. Since $a = b$ in one case and $a < b$ in the other case, we have that $a \leq b$. \square

Exercises

8.2.1. [Used in Section 6.4.] Let H be a non-empty set, let $a, b \in H$, and let $p: H \times H \rightarrow H$ be a map. Show that there is a unique map $g: N \rightarrow H$ such that $g(1) = a$, that $g(s(1)) = b$ and that $g(s(s(n))) = p((g(n), g(s(n))))$ for all $n \in N$.

8.2.2. [Used in Section 6.4.] Let H be a non-empty set, let $e \in H$, and let $q: H \times N \rightarrow H$ be a map. Show that there is a unique map $h: N \rightarrow H$ such that $h(1) = e$ and that $h(s(n)) = q((h(n), n))$ for all $n \in N$.

8.2.3. [Used in Section 8.2.] Prove Theorem 8.2.4 parts (ii) – (iv).

8.2.4. [Used in Section 8.2.] Fill in the missing details in the proof of Theorem 8.2.5.

8.2.5. [Used in Section 8.2.] Prove Theorem 8.2.6 parts (ii) – (v), (vii).

8.2.6. [Used in Section 8.2.] Prove Theorem 8.2.7 parts (i), (iii) – (iv), (vi) – (viii).

8.2.7. [Used in Section 8.2.] Let $a, b \in N$, and suppose that $a < b$. Show that there is a unique $p \in N$ such that $a + p = b$.

8.2.8. Let $a, b \in N$. Show that if $a + a = b + b$, then $a = b$.

8.2.9. Let $a, b \in N$. Show that if $a + b = s(b)$, then $a = 1$.

8.2.10. Let $a, b, c \in N$. Suppose that either $a < b$ and $b \leq c$, or $a \leq b$ and $b < c$. Show that $a < c$.

8.3 Further Properties of the Natural Numbers

In the previous section we saw some of the basic properties of addition, multiplication and less than for the natural numbers. Most of these properties are quite familiar, as are their analogs for other number systems such as the rational numbers and the real numbers. In this section we present some very important, and more subtle, properties of the natural numbers. Some of these properties, such as Theorem 8.3.1 (iv) and Theorems 8.3.2 – 8.3.5, do not hold for the rational numbers or the real numbers.

Theorem 8.3.1. *Let $a, b \in N$.*

- (i) *Precisely one of the following holds: either $a < b$, or $a = b$, or $a > b$.*
- (ii) *$a \leq b$ or $b \leq a$.*
- (iii) *If $a \leq b$ and $b \leq a$, then $a = b$.*
- (iv) *It cannot be that $b < a < s(b)$.*

Proof. (i). We will first show that no two of the three possibilities can hold simultaneously. Suppose that $a < b$ and $a = b$. Then by the first of these statements, there is some $p \in N$ such that $a + p = b$, and by the second, we have $a + p = a$. This last statement contradicts Theorem 8.2.4 (vi). Hence it is not the case that $a < b$ and $a = b$. A similar argument shows that it is not the case that $a > b$ and $a = b$. Now suppose that $a < b$ and $b < a$. Hence there are $h, k \in N$ such that $a + h = b$ and that $b + k = a$. Hence $(a + h) + k = a$, and by Theorem 8.2.4 (ii) we have $a + (h + k) = a$. Again we have a contradiction to Theorem 8.2.4 (vi), and hence it is not the case that $a < b$ and $a > b$.

We now show that at least one of $a < b$ or $a = b$ or $a > b$ holds. Let

$$G = \{x \in N \mid \text{if } y \in N, \text{ then } x < y \text{ or } x = y \text{ or } x > y\}.$$

We will show that $G = N$, and the desired result will follow. We start by showing that $1 \in G$. Let $j \in N$. By Theorem 8.2.7 (ii), we know that $1 \leq j$. It follows that either $1 = j$ or $1 < j$. Hence $1 \in G$. Now suppose that $k \in G$; we will show that $s(k) \in G$. Let $j \in N$. By hypothesis on k , we know that $k < j$ or $k = j$ or $k > j$. First suppose that $k < j$. By Theorem 8.2.7 (v) it follows that $s(k) \leq j$, which means that $s(k) < j$ or $s(k) = j$. Next suppose that $k = j$. Then by Theorem 8.2.7 (i) it follows that $s(k) > k = j$. Finally, suppose $k > j$. Then by Theorem 8.2.7 (i) we

know that $s(k) > k$, and by part (iii) of the same theorem, it follows that $s(k) > j$. Putting all three cases together, we see that one of $s(k) < j$ or $s(k) = j$ or $s(k) > j$ always holds. Hence $s(k) \in G$. Therefore $G = N$.

(ii) & (iii). These follow directly from part (i).

(iv). Suppose that $b < a < s(b)$. Then there are $g, h \in N$ such that $b + q = a$ and that $a + h = s(b)$. Then $(b + q) + h = s(b)$. Using Theorem 8.2.4 (ii) – (iv) we derive $(q + h) + b = 1 + b$. By Theorem 8.2.4 (i) we then have $q + h = 1$. This last statement contradicts Theorem 8.2.4 (v). \square

Part (i) of the above theorem is known as the trichotomy property of $<$, and part (iv) says that the natural numbers are “discrete.”

One of the features of the set of natural numbers, which distinguishes it from the set of integers, is the intuitive notion that the natural numbers are discrete, and go to infinity in only one direction. Hence, as we now prove, every non-empty subset of N has a smallest element (though not necessarily a largest one).

Theorem 8.3.2. (Well-Ordering Principle) *Let $G \subseteq N$ be non-empty. Then there exists $m \in G$ such that $m \leq g$ for all $g \in G$.*

Proof. Suppose that there is no $m \in G$ such that $m \leq g$ for all $g \in G$. We will derive a contradiction. Let

$$H = \{a \in N \mid \text{if } n \in N \text{ and } n \leq a, \text{ then } n \notin G\}.$$

It follows from the definition of H that $H \cap G = \emptyset$. We will show that $H = N$, and it will then follow that G is empty, the desired contradiction.

Suppose $1 \notin H$. Then there is some $q \in N$ such that $q \leq 1$ and $q \in G$. From Theorems 8.2.7 (ii) and 8.3.1 (iii) it follows that $q = 1$. Hence $1 \in G$. By Theorem 8.2.7 (ii) it would then follow that G has an element, namely $m = 1$, such that $m \leq g$ for all $g \in G$, contradicting our hypothesis that no such element exists. Thus $1 \in H$.

Now suppose $a \in H$. Suppose further that $s(a) \notin H$. Then there is some $p \in N$ such that $p \leq s(a)$ and $p \in G$. If it were the case that $p \leq a$, then we would have a contradiction to the fact that $a \in H$. Hence, by Theorem 8.3.1 (i) we deduce that $a < p$. Hence $a < p \leq s(a)$. From part (iv) of the same theorem, we deduce that $p = s(a)$. Hence $s(a) \in G$. We now show that if $x \in G$, then $s(a) \leq x$. Let $x \in G$, and suppose that $x < s(a)$. Then $x \leq a$ by Theorem 8.2.7 (v). Since $a \in H$, it follows that

$x \notin G$, a contradiction. Hence $s(a) \leq x$ by Theorem 8.3.1 (i). We now have a contradiction to the fact that no element such as $s(a)$ exists in G . It follows that $s(a) \in H$, and hence that $H = N$, completing the proof. \square

An amusing “application” of the Well-Ordering Principle is the following well-known proof that all natural numbers are interesting — whatever that might mean. (Some natural numbers certainly are interesting, for example prime numbers, Fibonacci numbers, etc.) Suppose that not all natural numbers are interesting. Let $U \subseteq N$ denote the set of uninteresting natural numbers. By hypothesis, U is non-empty. By the Well-Ordering Principle, the set U must have a smallest element; by Exercise 8.3.1 this element is unique. Let q denote the smallest element of U . Well, being the smallest uninteresting natural number is an interesting property of q , and hence $q \notin U$, a contradiction. Thus our hypothesis that U is non-empty must be false, and we deduce that every natural number must be interesting.

In Section 6.3 we had an intuitive discussion of mathematical induction. What we called PMI in that section is just what we call part (3) of the Peano Postulates here. To allow for more flexibility, we used in Section 6.3 a number of variants of mathematical induction, which we will now prove. Because we have already discussed these variants, we skip further discussion here.

Definition. Let $a, b \in N$ be such that $a \leq b$. We let $\llbracket a, b \rrbracket$ and $\llbracket a, \infty \rrbracket$ denote the sets

$$\llbracket a, b \rrbracket = \{n \in N \mid a \leq n \leq b\} \text{ and } \llbracket a, \infty \rrbracket = \{n \in N \mid a \leq n\}. \quad \Delta$$

Sets of the form $\llbracket a, b \rrbracket$ and $\llbracket a, \infty \rrbracket$ are never empty, since $a, b \in \llbracket a, b \rrbracket$ and $a \in \llbracket a, \infty \rrbracket$. The notations $\llbracket a, b \rrbracket$ and $\llbracket a, \infty \rrbracket$ are not standard, but there appears to be no single standard notation for either of these concepts.

Theorem 8.3.3. (Principle of Mathematical Induction – Variant 1) *Let $G \subseteq N$, and let $k_0 \in N$. Suppose that*

- (1) $k_0 \in G$;
- (2) *if $n \in N$ is such that $n \geq k_0$ and $n \in G$, then $s(n) \in G$.*

Then $\llbracket k_0, \infty \rrbracket \subseteq G$.

Proof. If $k_0 = 1$, then the statement of this theorem is precisely the same as part (3) of the Peano Postulates, since by Theorem 8.2.7 (ii) we know

that $n \geq 1$ for all $n \in N$, and hence $\llbracket 1, \infty \rrbracket = N$. Hence there is nothing to prove if $k_0 = 1$. From now on assume that $k_0 \neq 1$. By Lemma 8.2.2 we know that there is some $b \in N$ such that $s(b) = k_0$.

We start by defining $G' = \llbracket 1, b \rrbracket \cup G$. We will show that $G' = N$. It will then follow that $\llbracket 1, b \rrbracket \cup G = N$, and hence that $\llbracket k_0, \infty \rrbracket \subseteq G$ by using Exercise 8.3.2. To show that $G' = N$, we will use part (3) of the Peano Postulates. By definition we know that $1 \in G'$. Now suppose that $g \in G'$. We will show that $s(g) \in G'$, and the proof will be complete. By Theorem 8.3.1 (i) 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: $g < b$. Then $s(g) \leq b$ by Theorem 8.2.7 (vi). By part (ii) of the same theorem, we know that $1 \leq s(g)$, and hence $s(g) \in \llbracket 1, b \rrbracket \subseteq G'$.

Case 2: $g = b$. Then $s(g) = s(b) = k_0$. Hence $s(g) \in G \subseteq G'$.

Case 3: $g > b$. Then $g \not\leq b$ by Theorem 8.3.1 (i), and hence $g \notin \llbracket 1, b \rrbracket$. Since $g \in G' = \llbracket 1, b \rrbracket \cup G$, it follows that $g \in G$. Moreover, since $g > b$, we use Theorem 8.2.7 (vi) to deduce that $g \geq s(b) = k_0$. We now use the hypothesis on G to see that $s(g) \in G \subseteq G'$. \square

Theorem 8.3.4. (Principle of Mathematical Induction – Variant 2) *Let $G \subseteq N$. Suppose that*

- (1) $1 \in G$;
- (2) *if $n \in N$ and $\llbracket 1, n \rrbracket \subseteq G$, then $s(n) \in G$.*

Then $G = N$.

Proof. Suppose that $G \neq N$; we will derive a contradiction. Let $H = N - G$. Since $H \subseteq N$ and $H \neq \emptyset$, we know by Theorem 8.3.2 that there is some $m \in H$ such that $m \leq h$ for all $h \in H$. Since $1 \in G$ we know that $1 \notin H$, and thus $m \neq 1$. By Lemma 8.2.2 we know that there is some $b \in N$ such that $s(b) = m$. Now let $p \in \llbracket 1, b \rrbracket$. It follows that $p \leq b < s(b) = m$ by Theorem 8.2.7 (i). Hence $p \not\leq m$ using Theorem 8.3.1 (i). Therefore $p \notin H$, and so $p \in G$. We have thus shown that $\llbracket 1, b \rrbracket \subseteq G$. By part (2) of the hypothesis on G , we derive that $s(b) \in G$, which means that $m \in G$. This last statement contradicts the fact that $m \in H$. Hence $G = N$. \square

Theorem 8.3.5. (Principle of Mathematical Induction – Variant 3) *Let $G \subseteq N$, and let $k_0 \in N$. Suppose that*

- (1) $k_0 \in G$;
- (2) *if $n \in N$ is such that $n \geq k_0$ and $\llbracket k_0, n \rrbracket \subseteq G$, then $s(n) \in G$.*

Then $\llbracket k_0, \infty \rrbracket \subseteq G$.

Proof. Left to the reader in Exercise 8.3.3. \square

We postulated the natural numbers as a Henkin set satisfying the Peano Postulates. As mentioned, the existence of such a set can be either accepted axiomatically or derived from the axioms for set theory. Might there be two (or more) essentially distinct systems that satisfy the Peano Postulates? The following theorem, the conclusion of our discussion of the natural numbers, says that all systems that satisfy the Peano Postulates are essentially the same. Hence it is proper to refer to “the” natural numbers (as we have done all along). If you have read Sections 7.3 and 7.4, observe the resemblance of the properties stated in part (ii) of the theorem to the notions of group isomorphism discussed in Section 7.3 and order isomorphism discussed in Section 7.4.

Theorem 8.3.6. (Uniqueness of the Natural Numbers) *Let $(N, 1, s)$ and $(N', 1', s')$ be Henkin sets satisfying the Peano Postulates. Then there is a bijective map $f: N \rightarrow N'$ such that the following properties hold:*

- (i) $f(1) = 1'$.
- (ii) If $a, b \in N$, then
 - (a) $f(a + b) = f(a) + f(b)$;
 - (b) $f(a \cdot b) = f(a) \cdot f(b)$;
 - (c) $a \leq b$ iff $f(a) \leq f(b)$.

Proof. Left to the reader in Exercise 8.3.4. \square

Exercises

8.3.1. [Used in Section 8.3.] Show that the element m whose existence is guaranteed by Theorem 8.3.2 is unique.

8.3.2. [Used in Section 8.3.] Let $b \in N$. Show that $\llbracket 1, b \rrbracket \cup \llbracket s(b), \infty \rrbracket = N$ and that $\llbracket 1, b \rrbracket \cap \llbracket s(b), \infty \rrbracket = \emptyset$

8.3.3. [Used in Section 8.3.] Prove Theorem 8.3.5.

8.3.4. [Used in Section 8.3.] Prove Theorem 8.3.6.

8.3.5. [Used in Section 6.1.] Let $n \in N$ and let $f: \llbracket 1, n \rrbracket \rightarrow N$ be a map. Show that there is some $k \in \llbracket 1, n \rrbracket$ such that $f(k) \geq f(i)$ for all $i \in \llbracket 1, n \rrbracket$.

8.3.6. [Used in Section 9.2.] Let $F \subseteq N$ be a non-empty finite set. Use Exercise 8.3.5 to show that there is some $k \in F$ such that $p \leq k$ for all $p \in F$.

8.3.7. [Used in Section 6.1.] Let $n \in N$ and let $S \subseteq \llbracket 1, n \rrbracket$ be a non-empty subset. Show that there is a bijective map $h: \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket$, such that $h_*(S) = \llbracket 1, k \rrbracket$ for some $k \in N$ such that $k \leq n$. If S is a proper subset of $\llbracket 1, n \rrbracket$, show that $k < n$.

8.3.8. [Used in Section 6.1.] Let $k, m \in N$ and let $f: \llbracket 1, m \rrbracket \rightarrow \llbracket 1, k \rrbracket$ be a map.

- (1) Show that if f is bijective, then $m = k$.
- (2) Show that if f is injective but not bijective, then $m < k$.
- (3) Show 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.

8.3.9. [Used in Section 6.1.] Let $a, b \in N$ and suppose that $a < b$. Let $p \in N$ be the unique element such that $a + p = b$, using Exercise 8.2.7. Show that there is a bijective map $\llbracket a, b \rrbracket \rightarrow \llbracket 1, p + 1 \rrbracket$.

8.4 The Integers

We now use the natural numbers to construct the integers. The constructions and proofs in this section are quite different from the previous two sections, and are usually much easier. For the sake of brevity we will use the results of the previous two sections without always giving explicit references whenever a property of the natural numbers is a standard one (for example, the fact that $a + b = b + a$ for all $a, b \in N$).

The natural numbers have many nice properties, but they are not completely satisfactory, since we cannot always subtract one natural number from another and still obtain a natural number. Actually, we have not formally defined subtraction for the natural numbers, since we will not be

needing it. Rather than using subtraction, it is easier to deal with the related notion of adding a negative number. There are, of course, no such things as negative numbers inside the natural numbers (which is simply another way of stating that we cannot always subtract one natural number from another and still obtain a natural number). Also missing from the natural numbers is something that plays the role of zero. We could simply adjoin zero and negative numbers by brute force to the set of natural numbers, though doing so would leave us unsure that we are on safe ground, unless we assume additional axiomatic properties, which we would prefer not to do. Instead, we will construct a new set out of the set of natural numbers, and we will show that this new set acts precisely as we would intuitively expect the set of integers to behave. As expected, this new set will contain a copy of the natural numbers.

The intuitive idea in our construction is that we can think of an integer as given by an expression of the form " $a - b$," where $a, b \in N$. Since we don't have the operation subtraction on N , we replace " $a - b$ " by the pair (a, b) . It could happen, however, that " $a - b$ " equals " $c - d$ " for some $a, b, c, d \in N$, where $a \neq c$ and $b \neq d$. Then both the pairs (a, b) and (c, d) ought to represent the same integer. To take care of this problem we define the following relation on $N \times N$.

Definition. Let \sim be the relation on $N \times N$ given by $(a, b) \sim (c, d)$ iff $a + d = b + c$, for all $(a, b), (c, d) \in N \times N$. Δ

Lemma 8.4.1. *The relation \sim defined above is an equivalence relation on $N \times N$.*

Proof. We will prove reflexivity and symmetry, leaving transitivity to the reader in Exercise 8.4.1. Let $(a, b), (c, d) \in N \times N$. We note that $a + b = b + a$, and hence $(a, b) \sim (a, b)$. Thus \sim is reflexive. Now suppose that $(a, b) \sim (c, d)$. Then $a + d = b + c$. Hence $c + b = d + a$, and thus $(c, d) \sim (a, b)$. Thus \sim is symmetric. \square

The set of integers, together with addition, multiplication, negation and the relation less than for this set, are given in the following definition. We use the standard symbols $+$, \cdot , $-$ and $<$ in the definition, though we need to be careful to note that these symbols formally mean different things when used with the integers as well as with the natural numbers. (Moreover, it is not possible to "add" a natural number and an integer, as we have defined addition; this problem will be taken care of when we see that a copy of the natural numbers sits inside the set of integers.)

Definition. Let Z denote the set of equivalence classes of $N \times N$ with respect to the equivalence relation \sim . Let $\hat{0}, \hat{1} \in Z$ be the equivalence classes $\hat{0} = [(1, 1)]$ and $\hat{1} = [(s(1), 1)]$. Let $+$ and \cdot be the binary operations $+$ and \cdot on Z given by

$$\begin{aligned} [(a, b)] + [(c, d)] &= [(a + c, b + d)], \\ [(a, b)] \cdot [(c, d)] &= [(a \cdot c) + (b \cdot d), (a \cdot d) + (b \cdot c))] \end{aligned}$$

for all $[(a, b)], [(c, d)] \in Z$. Let $-$ be the unary operation on Z given by $-[(a, b)] = [(b, a)]$ for all $[(a, b)] \in Z$. Let $<$ be the relation on Z given by $[(a, b)] < [(c, d)]$ iff $a + d < b + c$, for all $[(a, b)], [(c, d)] \in Z$. Let \leq be the relation on Z given by $[(a, b)] \leq [(c, d)]$ iff $[(a, b)] < [(c, d)]$ or $[(a, b)] = [(c, d)]$, for all $[(a, b)], [(c, d)] \in Z$. Δ

Lemma 8.4.2. *The binary operations $+$ and \cdot , the unary operation $-$ and the relation $<$ defined above are well-defined.*

Proof. We will show that $+$ and $<$ are well-defined; the other parts of the lemma are left to the reader in Exercise 8.4.2. Let $(a, b), (c, d), (a', b'), (c', d') \in N \times N$. Suppose that $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$. Then $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$. Hence $a + b' = b + a'$ and $c + d' = d + c'$. By adding these two equations and doing some rearranging we obtain $(a + c) + (b' + d') = (b + d) + (a' + c')$, which implies that $[(a + c, b + d)] = [(a' + c', b' + d')]$. Thus $+$ is well-defined.

Now suppose $[(a, b)] < [(b, d)]$. Therefore $a + d < b + c$. Adding $b + a' = a + b'$ and $c + d' = d + c'$ to this inequality, we obtain $a + d + b + a' + c + d' < b + c + a + b' + d + c'$. Canceling yields $a' + d' < b' + c'$, which implies that $[(a', b')] < [(b', d')]$. This process can be done backwards, and thus $[(a', b')] < [(b', d')]$ implies $[(a, b)] < [(b, d)]$. Because $[(a, b)] < [(b, d)]$ iff $[(a', b')] < [(b', d')]$, then $<$ is well-defined. \square

The following lemma will be of use in some later proofs.

Lemma 8.4.3. *Let $a, b \in N$.*

$$(i) \quad [(a, b)] = \hat{0} \text{ iff } a = b.$$

$$(ii) \quad [(a, b)] = \hat{1} \text{ iff } a = s(b).$$

$$(iii) \quad [(a, b)] = [(n, 1)] \text{ for some } n \in N \text{ such that } n \neq 1 \text{ iff } a > b \text{ iff } [(a, b)] > \hat{0}.$$

(iv) $[(a, b)] = [(1, m)]$ for some $m \in N$ such that $m \neq 1$ iff $a < b$ iff $[(a, b)] < \hat{0}$.

Proof. We prove part (iii), leaving the rest to the reader in Exercise 8.4.3. First assume $[(a, b)] = [(n, 1)]$ for some $n \in N$ such that $n \neq 1$. Then $(a, b) \sim (n, 1)$, and hence $a + 1 = b + n$. Thus $s(a) = b + n$. Since $n \neq 1$, there is some $p \in N$ such that $n = s(p)$ by Lemma 8.2.2. Using Theorem 8.2.3 (ii), we thus have $s(a) = b + s(p) = s(b + p) = s(p + b) = p + s(b) = s(b) + p$. It follows that $s(a) > s(b)$. Using Theorem 8.2.7 (iv), we deduce that $a > b$.

Now assume $a > b$. Then $a + 1 > b + 1$ by Theorem 8.2.7 (vii), and thus $[(a, b)] > [(1, 1)] = \hat{0}$.

Finally, assume $[(a, b)] > \hat{0}$. Then $[(a, b)] > [(1, 1)]$, and thus $a + 1 > b + 1$. Therefore $a > b$ by Theorem 8.2.7 (vii). Hence there is some $p \in N$ such that $b + p = a$. Thus $(b + p) + 1 = a + 1$, and so $b + (p + 1) = a + 1$. Let $m = p + 1$, and so $b + m = a + 1$. Hence $[(a, b)] = [(m, 1)]$. By Theorem 8.2.4 (v) we see that $m \neq 1$. \square

The next three theorems state many of the basic properties of the integers. The idea of the proofs of these theorems is to rephrase things in terms of natural numbers, and then use the appropriate facts proved in the previous section.

Theorem 8.4.4. *Let $x, y, z \in Z$.*

- (i) $(x + y) + z = x + (y + z)$.
- (ii) $x + y = y + x$.
- (iii) $x + \hat{0} = x$.
- (iv) $x + (-x) = \hat{0}$.
- (v) *If $x + z = y + z$, then $x = y$.*
- (vi) $-(-x) = x$.
- (vii) $-(x + y) = (-x) + (-y)$.

Proof. We will prove part (ii); the other parts are left to the reader in Exercise 8.4.4.

(ii). Suppose that $x = [(a, b)]$ and $y = [(c, d)]$ for some $a, b, c, d \in N$. Then $x + y = [(a, b)] + [(c, d)] = [(a + c, b + d)] = [(c + a, d + b)] = [(c, d)] + [(a, b)] = y + x$, where the middle equality holds by Theorem 8.2.4 (iv). \square

Theorem 8.4.5. Let $x, y, z \in Z$.

- (i) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- (ii) $x \cdot y = y \cdot x$.
- (iii) $x \cdot \hat{1} = x$.
- (iv) $x \cdot y = \hat{0}$ iff $x = \hat{0}$ or $y = \hat{0}$.
- (v) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.
- (vi) If $z \neq \hat{0}$ and if $x \cdot z = y \cdot z$, then $x = y$.
- (vii) $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$.
- (viii) $x \cdot y = \hat{1}$ iff $x = \hat{1}$ or $x = -\hat{1} = y$.

Proof. We will prove part (iv); the other parts are left to the reader in Exercise 8.4.5.

(iv). Suppose that $x = [(a, b)]$ and $y = [(c, d)]$ for some $a, b, c, d \in N$. Then $x \cdot y = [((a \cdot c) + (b \cdot d), (a \cdot d) + (b \cdot c))]$.

\Leftarrow . Suppose that $x = \hat{0}$ or $y = \hat{0}$. There are two cases. First, assume that $x = \hat{0}$. Then $a = b$ by Lemma 8.4.3 (i). Hence

$$\begin{aligned} x \cdot y &= [((a \cdot c) + (b \cdot d), (a \cdot d) + (b \cdot c))] \\ &= [((a \cdot c) + (a \cdot d), (a \cdot d) + (a \cdot c))] \\ &= [((a \cdot c) + (a \cdot d), (a \cdot c) + (a \cdot d))] \\ &= \hat{0}, \end{aligned}$$

where the penultimate equality holds by Theorem 8.2.4 (iv), and the final equality holds by Lemma 8.4.3 (i). The case where $y = \hat{0}$ is similar.

\Rightarrow . We need to show that if $x \cdot y = \hat{0}$, then $x = \hat{0}$ or $y = \hat{0}$. As mentioned in Section 2.4, we can prove this statement, which has the form $P \rightarrow (A \vee B)$, by proving the equivalent statement $(P \wedge \neg A) \rightarrow B$. Thus, assume that $x \cdot y = \hat{0}$ and that $x \neq \hat{0}$; we will deduce that $y = \hat{0}$. Applying Lemma 8.4.3 (i) to our hypotheses on both $x \cdot y$ and x , we see that $(a \cdot c) + (b \cdot d) = (a \cdot d) + (b \cdot c)$ and $a \neq b$. By Theorem 8.3.1 (i), we know that either $a < b$ or $a > b$. We thus have two cases; we will deal with former case, the latter case being similar. Assume that $a < b$. Hence there is some $g \in N$ such that $a + g = b$. It then follows that $(a \cdot c) + ((a + g) \cdot d) = (a \cdot d) + ((a + g) \cdot c)$. Using various parts

of Theorems 8.2.4 and 8.2.6, we can simplify this equation to deduce that $g \cdot d = g \cdot c$. Using Theorem 8.2.6 (vi), we see that $d = c$. By Lemma 8.4.3 (i), it follows that $y = \hat{0}$. \square

Theorem 8.4.6. *Let $x, y, z, w \in Z$.*

- (i) $\hat{0} < \hat{1}$.
- (ii) $x \leq x$.
- (iii) If $x < y$ and $y < z$, then $x < z$.
- (iv) Precisely one of the following holds: either $x < y$, or $x = y$, or $x > y$.
- (v) It cannot be that $x < y < x + \hat{1}$.
- (vi) If $x \leq y$ and $y \leq x$, then $x = y$.
- (vii) $x < y$ iff $x + z < y + z$.
- (viii) If $\hat{0} < z$, then $x < y$ iff $x \cdot z < y \cdot z$.
- (ix) $\hat{0} < x$ iff $-x < \hat{0}$.

Proof. We will prove parts (v) and (vii); the other parts are left to the reader in Exercise 8.4.6. Suppose that $x = [(a, b)]$, that $y = [(c, d)]$ and that $z = [(e, f)]$ for some $a, b, c, d, e, f \in N$.

(v). Suppose that $x < y < x + \hat{1}$. Then $[(a, b)] < [(c, d)] < [(a, b)] + [(s(1), 1)] = [(a + s(1), b + 1)]$. From the first inequality we obtain $a + d < b + c$. From the second inequality we obtain $c + (b+1) < (a+s(1))+d$, and thus $(c+b)+1 < ((a+d)+1)+1$ by Theorem 8.2.4 (ii)–(iv). Using parts (i) and (iii) of the same theorem, we deduce that $c + b < s(a + d)$. Putting everything together we have $a + d < c + b < s(a + d)$. This last statement contradicts Theorem 8.3.1 (iv). Therefore it is not the case that $x < y < x + \hat{1}$.

(vii). Suppose $x < y$. Then $[(a, b)] < [(c, d)]$, and so $a + d < b + c$. Hence $(a + d) + (e + f) < (b + c) + (e + f)$, and thus $(a + e) + (d + f) < (b + f) + (c + e)$. Therefore $[(a + e, b + f)] < [(c + e, d + f)]$, and hence $[(a, b)] + [(e, f)] < [(c, d)] + [(e, f)]$. This last statement is equivalent to $x + z < y + z$. To show that $x + z < y + z$ implies $x < y$, simply reverse the argument. \square

The set of integers has two very important subsets, namely the set of positive integers and the set of negative integers.

Definition. Let Z^+ and Z^- denote the sets

$$\begin{aligned} Z^+ &= \{x \in Z \mid \hat{0} < x\} \\ Z^- &= \{x \in Z \mid \hat{0} > x\}. \end{aligned}$$

The elements of Z^+ are called **positive** integers, and the elements of Z^- are called **negative** integers. Δ

It follows from Theorem 8.4.6 (iv) that $Z = Z^- \cup \{0\} \cup Z^+$, and that these three sets are disjoint. The set of positive integers is essentially the same as the set of natural numbers, a relationship made more precise in the following theorem.

Theorem 8.4.7. Let $i : N \rightarrow Z$ be given by $i(n) = [(s(n), 1)]$ for all $n \in N$.

(i) *The map $i : N \rightarrow Z$ is injective.*

(ii) $i(N) = Z^+$.

(iii) $i(1) = \hat{1}$.

(iv) *Let $a, b \in N$. Then*

(a) $i(a + b) = i(a) + i(b)$;

(b) $i(a \cdot b) = i(a) \cdot i(b)$;

(c) $a < b$ iff $i(a) < i(b)$;

Proof. We prove part (iv)(a), leaving the rest to the reader in Exercise 8.4.7. (iv)(a). Making use of the definitions of addition for Z , the relation \sim and the map i , together with Theorem 8.2.4 parts (i) – (iv), we have

$$\begin{aligned} i(a) + i(b) &= [(s(a), 1)] + [(s(b), 1)] = [(s(a) + s(b), 1 + 1)] \\ &= [(a + 1) + (b + 1), 1 + 1] = [((a + b) + 1) + 1, 1 + 1] \\ &= [(a + b) + 1, 1] = [s(a + b), 1] = i(a + b). \quad \square \end{aligned}$$

The above theorem implies that from the point of view of addition, multiplication and the relation $<$, we can identify the natural numbers with the

positive integers. Thus we can essentially dispense with the set of natural numbers as a separate entity (except when we need it in proofs), since we have a copy of the natural numbers inside the integers that works just as well. The following theorem, a version of the Well-Ordering Principle (Theorem 8.3.2), gives one example that the set of positive integers works just like as the set of natural numbers.

Theorem 8.4.8. *Let $S \subseteq \mathbb{Z}^+$ be non-empty. Then there exists $z \in S$ such that $z \leq x$ for all $x \in S$.*

Proof. Left to the reader in Exercise 8.4.8. \square

The following theorem, a very important tool in number theory and other areas, states intuitively that long division works as expected. Although this theorem is called the “Division Algorithm,” it is not an algorithm, but simply an existence theorem; the name of the theorem is a historical artifact. We start with a definition.

Definition. Let $|\cdot|: \mathbb{Z} \rightarrow \mathbb{Z}$ be the map defined by

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

If $x \in \mathbb{Z}$, we call $|x|$ the absolute value of x . Δ

Theorem 8.4.9. (Division Algorithm) *Let $x, y \in \mathbb{Z}$, and suppose $y \neq \hat{0}$. Then there are unique $q, r \in \mathbb{Z}$ such that $x = y \cdot q + r$ and $\hat{0} \leq r < |y|$.*

Proof. We will be using various parts of Theorems 8.4.4 – 8.4.6 throughout this proof; since these properties of \mathbb{Z} are familiar, we will avoid clutter by not citing these theorems each time they are used.

Uniqueness: Suppose there are $q, q', r, r' \in \mathbb{Z}$ such that $y \cdot q + r = x = y \cdot q' + r'$, that $\hat{0} \leq r < |y|$ and that $\hat{0} \leq r' < |y|$. We have two cases.

Case 1: Suppose $q = q'$. Since $y \cdot q + r = y \cdot q' + r'$, it follows that $r = r'$.

Case 2: Suppose $q \neq q'$. Without loss of generality, we assume $q > q'$. It follows that $q + (-q') > \hat{0}$, and from Exercise 8.4.12, we see that $q + (-q') \geq \hat{1}$. There are now two subcases, depending upon whether $y > \hat{0}$ or $y < \hat{0}$. First suppose that $y > \hat{0}$. Since $y \cdot q + r = y \cdot q' + r'$, we then have $r' = y \cdot (q + (-q')) + r \geq y \cdot \hat{1} + \hat{0} = y = |y|$, and this inequality contradicts the hypothesis on r' . If $y < \hat{0}$, then we have $r = y \cdot (q' + (-q)) + r' = (-y) \cdot (q + (-q')) + r' = |y| \cdot (q + (-q')) + r' \geq$

$|y| \cdot \hat{1} + \hat{0} = |y|$, and this inequality contradicts the hypothesis on r . Thus $q \neq q'$ cannot happen.

Existence: There are four cases, depending upon whether $x \geq \hat{0}$ or not, and whether $y > \hat{0}$ or not.

Case 1: $x \geq \hat{0}$ and $y > \hat{0}$. Let

$$S = \{w \in Z \mid w \geq \hat{0} \text{ and } x < (w + \hat{1}) \cdot y\}.$$

A straightforward computation shows that $x \in S$, and hence $S \neq \emptyset$. We have two subcases.

Subcase (a): Suppose that $\hat{0} \in S$. Then we have $x < (\hat{0} + \hat{1}) \cdot y = y$. We now let $q = \hat{0}$ and $r = x$. Then $y \cdot q + r = y \cdot \hat{0} + x = x$, and $\hat{0} \leq r = x < y = |y|$. Hence we have found the desired q and r .

Subcase (b): Suppose that $\hat{0} \notin S$. Then $S \subseteq Z^+$. By Theorem 8.4.8, we know there is some $q \in S$ such that $q \leq p$ for all $p \in S$. Since $q \in S$, we have $x < (q + \hat{1}) \cdot y = y \cdot q + y$. Observe that $q + (-\hat{1}) < q$, which follows from various parts of Theorem 8.4.4 and 8.4.6. Thus, given that $q \leq p$ for all $p \in S$, it follows that $q + (-\hat{1}) \notin S$, using Exercise 8.4.13. Hence, using the definition of S , we know $x \geq [(q + (-\hat{1})) + \hat{1}] \cdot y = q \cdot y$.

Now let $r = x + y \cdot (-q)$. Hence $y \cdot q + r = x$. Also, we compute $r = x + y \cdot (-q) < (y \cdot q + y) + y \cdot (-q) = y = |y|$, because $x < y \cdot q + y$, as shown in the previous paragraph. Moreover, since $x \geq q \cdot y$, it follows that $r = x + y \cdot (-q) \geq q \cdot y + y \cdot (-q) = \hat{0}$. Thus q and r have the desired properties.

Case 2: $x \geq \hat{0}$ and $y < \hat{0}$. Let $x' = x$ and $y' = -y$. We now apply Case (1) to x' and y' , obtaining $q', r' \in Z$ such that $x' = y' \cdot q' + r'$ and $\hat{0} \leq r' < |y'|$. We now let $q = -q'$ and $r = r'$. Then $y \cdot q + r = (-y) \cdot (-q) + r = y' \cdot q' + r' = x' = x$, and since $r = r'$, we have $\hat{0} \leq r < |y'| = |y|$. Thus q and r have the desired properties.

Case 3: $x < \hat{0}$ and $y > \hat{0}$. Let $x' = -x$ and $y' = y$. We now apply Case (1) to x' and y' , obtaining $q', r' \in Z$ such that $x' = y' \cdot q' + r'$ and $\hat{0} \leq r' < |y'|$. There are now two subcases, depending upon whether $r' = \hat{0}$ or not. If $r' = \hat{0}$, we let $q = -q'$ and $r = \hat{0}$. If $r' \neq \hat{0}$, we let $q = (-q') + (-\hat{1})$ and $r = y' + (-r')$. We leave it to the reader to verify in both cases that q and r have the desired properties.

Case 4: $x < \hat{0}$ and $y < \hat{0}$. This case is similar to Case (3), and is left to the reader. \square

Exercises

8.4.1. [Used in Section 8.4.] Complete the proof of Lemma 8.4.1.

8.4.2. [Used in Section 8.4.] Complete the proof of Lemma 8.4.2. The proof for \cdot is a bit more complicated than might be expected.

8.4.3. [Used in Section 8.4.] Prove Lemma 8.4.3 parts (i), (ii), (iv).

8.4.4. [Used in Section 8.4.] Prove Theorem 8.4.4 parts (i), (iii)–(vii).

8.4.5. [Used in Section 8.4.] Prove Theorem 8.4.5 parts (i)–(iii), (v)–(viii).

8.4.6. [Used in Section 8.4.] Prove Theorem 8.4.6 parts (i)–(iv), (vi), (viii), (ix).

8.4.7. [Used in Section 8.4.] Prove Theorem 8.4.7 parts (i)–(iii), (iv)(b)–(iv)(d).

8.4.8. [Used in Section 8.4.] Prove Theorem 8.4.8.

8.4.9. Let $\hat{2} = \hat{1} + \hat{1}$. Show that $\hat{2} > \hat{1}$.

8.4.10. Let $x, y \in Z$. Show that $x < y$ iff $-x > -y$.

8.4.11. Let $x, y, z \in Z$. Show that if $\hat{0} > z$, then $x < y$ iff $x \cdot z > y \cdot z$

8.4.12. [Used in Section 8.4.] Let $x \in Z$. Show that if $x > \hat{0}$ then $x \geq \hat{1}$; Show that if $x < \hat{0}$ then $x \leq -\hat{1}$

8.4.13. [Used in Section 8.4.] Let $x \in Z$. Show that $x + (-\hat{1}) < x$.

8.4.14. Let $x \in Z$. Let $\hat{2}$ be as in Exercise 8.4.9. Show that $\hat{2} \cdot x \neq \hat{1}$.

8.4.15. [Used in Section 2.1.] Let $\hat{2}$ be as in Exercise 8.4.9. Let $x \in Z$. We say that x is an **even** integer if there is some $y \in Z$ such that $x = \hat{2} \cdot y$. We say that x is an **odd** integer if there is some $y \in Z$ such that $x = \hat{2} \cdot y + \hat{1}$. Prove that every $x \in Z$ is either even or odd, but not both.

8.4.16. [Used in Section 2.4.] Let $\hat{2}$ be as in Exercise 8.4.9, and let $\hat{3} = \hat{1} + \hat{1} + \hat{1}$. Let $x \in Z$. Prove that precisely one of the following holds: either $x = \hat{3}y$ for some $y \in Z$, or $x = \hat{3}y + \hat{1}$ for some $y \in Z$, or $x = \hat{3}y + \hat{2}$ for some $y \in Z$.

8.4.17. Let \approx be the relation on $N \times N$ given by $(a, b) \approx (c, d)$ iff $a^2 \cdot d = c^2 \cdot b$, for all $(a, b), (c, d) \in N \times N$ (where n^2 is an abbreviation for $n \cdot n$).

(i) Show that \approx is an equivalence relation.

- (ii) List or describe all the elements in $[(2, 3)]$, where $2 = s(1)$ and $3 = s(2)$.

8.5 The Rational Numbers

We now use the integers to construct the rational numbers, very much analogous to the way we constructed the integers from the natural numbers. Although the integers allow us to take negatives of numbers (unlike the natural numbers), we cannot divide integers and still expect to obtain an integer. The rational numbers will be constructed to allow for division, or equivalently, to allow for multiplication by reciprocals of integers. Once again we will use equivalence classes to construct the set of rational numbers, and again we will find a copy of the set of integers inside the set of rational numbers. Just as the standard symbols $+$, $,$, $-$ and $<$ formally meant different things when used with natural numbers and with integers, they will also mean something different when used with the rational numbers (though of course these symbols correspond to the same intuitive notion in all three cases). We leave all the proofs in this section to the reader.

Definition. Let $Z^* = Z - \{\hat{0}\}$. Let \asymp be the relation on $Z \times Z^*$ given by $(x, y) \asymp (z, w)$ iff $x \cdot w = y \cdot z$, for all $(x, y), (z, w) \in Z \times Z^*$. Δ

Lemma 8.5.1. *The relation \asymp defined above is an equivalence relation.*

Proof. Left to the reader in Exercise 8.5.1. \square

Definition. Let Q denote the set of equivalence classes of $Z \times Z^*$ with respect to the equivalence relation \asymp . Let $\bar{0}, \bar{1} \in Q$ be the equivalence classes $\bar{0} = [(\hat{0}, \hat{1})]$ and $\bar{1} = [(\hat{1}, \hat{1})]$. Let $Q^* = Q - \{\bar{0}\}$. Let $+$ and \cdot be the binary operations on Q given by

$$\begin{aligned} [(x, y)] + [(z, w)] &= [((x \cdot w) + (y \cdot z), y \cdot w)], \\ [(x, y)] \cdot [(z, w)] &= [(x \cdot z, y \cdot w)] \end{aligned}$$

for all $[(x, y)], [(z, w)] \in Q$. Let $-$ be the unary operation on Q given by $-[(x, y)] = [(-x, y)]$ for all $[(x, y)] \in Q$. Let $^{-1}$ be the unary operation on Q^* given by $[(x, y)]^{-1} = [(y, x)]$ for all $[(x, y)] \in Q^*$. Let $<$ be the relation on Q given by $[(x, y)] < [(z, w)]$ iff either $\hat{0} < (z \cdot y) - (x \cdot w)$ when $\hat{0} < y$ and $\hat{0} < w$ or when $\hat{0} > y$ and $\hat{0} > w$, or $\hat{0} > (z \cdot y) - (x \cdot w)$ when $\hat{0} < y$ and $\hat{0} > w$ or when $\hat{0} > y$ and $\hat{0} <$

w , for all $[(x, y)], [(z, w)] \in Q$. Let \leq be the relation on Q given by $[(x, y)] \leq [(z, w)]$ iff $[(x, y)] < [(z, w)]$ or $[(x, y)] = [(z, w)]$, for all $[(x, y)], [(z, w)] \in Q$. \triangle

Lemma 8.5.2. *The binary operations $+$ and \cdot , the unary operations $-$ and $^{-1}$, and the relation $<$ defined above are well-defined.*

Proof. Left to the reader in Exercise 8.5.2. \square

Lemma 8.5.3. *Let $x \in Z$ and $y \in Z^*$.*

- (i) $[(x, y)] = \bar{0}$ iff $x = \hat{0}$.
- (ii) $[(x, y)] = \bar{1}$ iff $x = y$.
- (iii) $\bar{0} < [(x, y)]$ iff $\hat{0} < x \cdot y$.

Proof. Left to the reader in Exercise 8.5.3. \square

Theorem 8.5.4. *Let $r, s, t \in Q$.*

- (i) $(r + s) + t = r + (s + t)$.
- (ii) $r + s = s + r$.
- (iii) $r + \bar{0} = r$.
- (iv) $r + (-r) = \bar{0}$.
- (v) If $r + t = s + t$, then $r = s$.
- (vi) $-(-r) = r$.
- (vii) $-(r + s) = (-r) + (-s)$.

Proof. Left to the reader in Exercise 8.5.4. \square

Theorem 8.5.5. Let $r, s, t \in Q$.

- (i) $(r \cdot s) \cdot t = r \cdot (s \cdot t)$.
- (ii) $r \cdot s = s \cdot r$.
- (iii) $r \cdot \bar{1} = r$.
- (iv) $r \cdot s = \bar{0}$ iff $r = \bar{0}$ or $s = \bar{0}$.
- (v) If $r \neq \bar{0}$, then $r \cdot r^{-1} = \bar{1}$.
- (vi) $r \cdot (s + t) = (r \cdot s) + (r \cdot t)$.
- (vii) If $t \neq \bar{0}$ and if $r \cdot t = s \cdot t$, then $t = s$.
- (viii) $(-r) \cdot s = -(r \cdot s) = r \cdot (-s)$.

Proof. Left to the reader in Exercise 8.5.5. □

Theorem 8.5.6. Let $r, s, t, u \in Q$.

- (i) $\bar{0} < \bar{1}$.
- (ii) $r \leq r$.
- (iii) If $r < s$ and $s < t$, then $r < t$.
- (iv) Precisely one of the following holds: either $r < s$, or $r = s$, or $r > s$.
- (v) If $r \leq s$ and $s \leq r$, then $r = s$.
- (vi) $r < s$ iff $r + t < s + t$.
- (vii) If $\bar{0} < t$, then $r < s$ iff $r \cdot t < s \cdot t$.
- (viii) $\bar{0} < r$ iff $-r < \bar{0}$.

Proof. Left to the reader in Exercise 8.5.6. □

Theorem 8.5.7. Let $i: \mathbb{Z} \rightarrow \mathbb{Q}$ be given by $i(x) = [(x, \hat{1})]$ for all $x \in \mathbb{Z}$.

(i) The map $i: \mathbb{Z} \rightarrow \mathbb{Q}$ is injective.

(ii) $i(\hat{0}) = \bar{0}$ and $i(\hat{1}) = \bar{1}$.

(iii) Let $x, y \in \mathbb{Z}$. Then

(a) $i(x + y) = i(x) + i(y)$;

(b) $i(x \cdot y) = i(x) \cdot i(y)$;

(c) $x < y$ iff $i(x) < i(y)$.

(iv) For each $r \in \mathbb{Q}$ there are $x, y \in \mathbb{Z}$ such that $y \neq \hat{0}$ and $r = i(x) \cdot (i(y))^{-1}$.

Proof. Left to the reader in Exercise 8.5.7. □

Theorem 8.5.7 implies that from the point of view of addition, multiplication and the relation $<$, we can identify the integers with a subset of the rational numbers. Thus we can essentially dispense with the set of integers as a separate entity (except for when we need it in proofs), since we have a copy of the integers inside the rational numbers that works just as well.

Although many of the properties of the rational numbers are similar to properties of the integers, we note that there are no analogs for the rational numbers of Theorems 8.4.6 (v) and 8.4.8; see Exercises 8.5.8 and 8.5.9 for counterexamples.

Exercises

8.5.1. [Used in Section 8.5.] Prove Lemma 8.5.1.

8.5.2. [Used in Section 8.5.] Prove Lemma 8.5.2.

8.5.3. [Used in Section 8.5.] Prove Lemma 8.5.3.

8.5.4. [Used in Section 8.5.] Prove Theorem 8.5.4.

8.5.5. [Used in Section 8.5.] Prove Theorem 8.5.5.

8.5.6. [Used in Section 8.5.] Prove Theorem 8.5.6.

8.5.7. [Used in Section 8.5.] Prove Theorem 8.5.7.

8.5.8. [Used in Section 8.5.] Find an example to show that the analog of Theorem 8.4.6 (v) does not hold for the rational numbers.

8.5.9. [Used in Section 8.5.] Find an example to show that the analog of Theorem 8.4.8 does not hold for the rational numbers.

8.6 The Real Numbers and the Complex Numbers

In the preceding sections of this chapter we postulated the existence of the set of natural numbers N , and then constructed the sets of integers Z and rational numbers Q . Technically these sets are all distinct, but as we have seen, we can identify N with a subset of Z , and Z with a subset of Q , in a very natural way. For convenience, we will now think of these identifications as always being made, and thus we will assume that $N \subseteq Z \subseteq Q$. Since these sets of numbers are the formally constructed versions of the number systems we have been using all along, we will now revert to the standard notation $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$ for these sets of numbers, and we will write 0 and 1 rather than $\bar{0}$ and $\bar{1}$. Thus we are essentially back where we started with regard to the rational numbers and its subsets, except that now we know it can all be done rigorously.

Though the set Q has many nice properties, two larger sets of numbers are needed, namely the real numbers, denoted \mathbb{R} , and the complex numbers, denoted \mathbb{C} . As before, it is possible to construct \mathbb{R} from Q , and \mathbb{C} from \mathbb{R} . Once these sets are constructed, it will be possible to think of $Q \subseteq \mathbb{R} \subseteq \mathbb{C}$. In this section, we will briefly (and informally) discuss the somewhat intricate construction of \mathbb{R} from Q , and then give a more complete treatment of the construction of \mathbb{C} from \mathbb{R} .

From the point of view of the operations addition and multiplication, the set Q has all the properties we might wish for. Using the terminology of Section 7.1, we see from Theorems 8.5.4 and 8.5.5 that both operations satisfy the commutative, associative and identity laws, where 0 and 1 are the identity elements for addition and multiplication respectively. Addition satisfies the inverses law (negation is the inverse operation), and multiplication restricted to $Q - \{0\}$ also satisfies this law (taking the reciprocal as the inverse operation). Also, multiplication distributes over addition. A set with two operations that behave as do addition and multiplication in Q is called a “field,” a concept studied extensively in abstract algebra (see [Fra94] for example). From the point of view of addition and multiplication, we could not reasonably ask for more than the properties of a field.

Nonetheless, the set of rational numbers Q is not satisfactory. At the simplest level, there are familiar numbers such as $\sqrt{2}$, π and e that are not in the set of rational numbers (see Theorem 2.3.3 for a proof that $\sqrt{2}$ is not rational). For this reason alone, we need to construct a larger set of numbers. The precise conceptual problem with the rational numbers is,

however, rather subtle, in contrast to the natural numbers (where we could not subtract) and the integers (where we could not take reciprocals).

Though the set of rational numbers has all the desired properties with respect to addition and multiplication, it is with the relation $<$ that something is wrong. Intuitively, the set \mathbb{Q} has “holes” with respect to this relation, a notion captured more precisely as follows. Consider the set $S \subseteq \mathbb{Q}$ defined by $S = \{q \in \mathbb{Q} \mid q^2 < 2\}$. Using our informal knowledge of the real numbers, we can think of this set S as $\{q \in \mathbb{Q} \mid -\sqrt{2} < q < \sqrt{2}\}$, though we cannot technically write this last expression using only the rational numbers. The set S has plenty of upper bounds in \mathbb{Q} , that is, numbers in \mathbb{Q} that are larger than everything in S . For example, the number 2 is an upper bound for S . However, and this is the crucial problem, there is no *least* upper bound for S in \mathbb{Q} ; in other words, there is no number in \mathbb{Q} that is an upper bound for S , and is less than or equal to every other upper bound for S in \mathbb{Q} . (The number $\sqrt{2}$ “wants” to be the least upper bound for S , but it is not in \mathbb{Q} .) Similar considerations hold for greatest lower bounds.

We want to construct a new set of numbers, which will include a copy of the rational numbers, but which will also satisfy the “Least Upper Bound Property,” which states that any subset that has an upper bound in the set also has a least upper bound in the set. A similar property holds for greatest lower bounds. There are two standard methods for such a construction, known as Cauchy sequences, and Dedekind cuts respectively. Both methods yield equivalent sets. It is beyond the scope of this book to give the details of either construction, though we will say a few words about the former method, which is more widely used today. See [Hos90, Chapter 3] for details of the Cauchy sequence approach, and some remarks about the Dedekind cuts approach.

The Cauchy sequence method is based on sequences of rational numbers. Using the ideas in Example 4.5.1 (3), such sequences are formally maps $\mathbb{N} \rightarrow \mathbb{Q}$, but we will use the more common notation for sequences r_1, r_2, r_3, \dots , and more briefly $\{r_n\}$. Informally, we say that a sequence $\{r_n\}$ of rational numbers converges to a rational number L if the numbers r_n get closer and closer to L as n goes to infinity. For example, the sequence $1, 1/2, 1/3, \dots$ converges to 0. A sequence $\{r_n\}$ is called a Cauchy sequence if, intuitively, its elements get closer and closer to each other as n goes to infinity. The notions of a sequence being convergent and Cauchy can both be made completely rigorous. For details, see many texts on real analysis, for example [Pow94, Chapter 2].

Every sequence $\{r_n\}$ of rational numbers that converges to a rational number L is also a Cauchy sequence, since if the numbers r_n get closer and closer to L as n goes to infinity, then they are getting closer and closer to each other. The converse is not necessarily true, however, if we are sticking to rational numbers. Consider the sequence $1, 1.4, 1.41, 1.414, \dots$ that converges to $\sqrt{2}$. The numbers in this sequence are rational (for example $1.41 = 141/100$), though as previously mentioned $\sqrt{2}$ is not rational. Given that this sequence converges to $\sqrt{2}$, then it must be a Cauchy sequence; however, since $\sqrt{2}$ is not rational, the sequence does not converge to anything in the rational numbers (it can be proved that a sequence that converges to one real number cannot simultaneously converge to another one). Thus a sequence of rational numbers can be Cauchy and yet not converge in the rational numbers. This phenomenon is related to the fact that the Least Upper Bound Property does not hold for the rational numbers.

The real numbers are constructed from the rational numbers using, once again, an equivalence relation. Rather than starting with pairs of rational numbers, however, we start with the set of all Cauchy sequences of rational numbers; denote this set \mathcal{CS} . An equivalence relation on \mathcal{CS} is formed by saying that two sequences are equivalent if their term-by-term difference is a sequence that converges to 0. The set of real numbers, denoted \mathbb{R} , is taken to be the set of all equivalence classes of \mathcal{CS} with respect to this equivalence relation. Binary operations $+$ and \cdot , a unary operation $-$ and a relation $<$ can all be defined on \mathbb{R} , and a unary operation $^{-1}$ can be defined on $\mathbb{R} - \{0\}$, all of which behave as expected. Further, we can think of \mathbb{Q} as sitting inside \mathbb{R} by identifying each rational number r with the sequence that is constantly r . Some of the properties of \mathbb{R} are given in the following theorems, which are stated without proof, but which can be proved using a rigorous treatment of Cauchy sequences.

Theorem 8.6.1. *Let $x, y, z \in \mathbb{R}$.*

$$(i) \quad (x + y) + z = x + (y + z).$$

$$(ii) \quad x + y = y + x.$$

$$(iii) \quad x + 0 = x.$$

$$(iv) \quad x + (-x) = 0.$$

$$(v) \quad \text{If } x + z = y + z, \text{ then } x = y.$$

- (vi) $-(-x) = x$.
 (vii) $-(x + y) = (-x) + (-y)$.

Theorem 8.6.2. Let $x, y, z \in \mathbb{R}$.

- (i) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- (ii) $x \cdot y = y \cdot x$.
- (iii) $x \cdot 1 = x$.
- (iv) $x \cdot y = 0$ iff $x = 0$ or $y = 0$.
- (v) If $x \neq 0$, then $x \cdot x^{-1} = 1$.
- (vi) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.
- (vii) If $z \neq 0$ and if $x \cdot z = y \cdot z$, then $x = y$.
- (viii) $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$.

Theorem 8.6.3. Let $x, y, z, w \in \mathbb{R}$.

- (i) $0 < 1$.
- (ii) $x \leq x$.
- (iii) If $x < y$ and $y < z$, then $x < z$.
- (iv) Precisely one of the following holds: either $x < y$, or $x = y$, or $x > y$.
- (v) If $x \leq y$ and $y \leq x$, then $x = y$.
- (vi) $x < y$ iff $x + z < y + z$.
- (vii) If $0 < z$, then $x < y$ iff $x \cdot z < y \cdot z$.
- (viii) $0 < x$ iff $-x < 0$.

Theorem 8.6.3 (iv) allows us to think of the real numbers as being situated along a line. (Using the terminology of Section 7.4, parts (ii) – (v) of this theorem tell us that $(\mathbb{R}, <)$ is a totally ordered set). The Least Upper Bound Property can be proved for the real numbers using the details of the Cauchy sequence construction. We can thus think of the real number line as not having any “holes” in it.

The set of real numbers forms the entirety of the familiar number line, and as such, it might be reasonable to believe that we are now at the end of our construction of number systems. Though the set of real numbers suffices for many purposes (such as calculus), it too is not completely satisfactory. Consider the quadratic equation $x^2 - 1 = 0$. This equation has two solutions, namely $x = 1$ and $x = -1$. On the other hand, the very similar equation $x^2 + 1 = 0$ has no solutions in \mathbb{R} , since this equation is equivalent to $x^2 = -1$, and we know that $x^2 \geq 0$ for all $x \in \mathbb{R}$ (see Exercise 8.6.1). Given that both quadratic equations involve only real numbers, it is problematic that one has two solutions and the other has no solution. This inability to solve all quadratic equations (and higher degree equations) in the real numbers is the conceptual problem that leads, once again, to the construction of an even larger set of numbers, namely the set of complex numbers.

Recall the quadratic formula, which says that the solutions to an equation of the form $ax^2 + bx + c = 0$ are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

To be able to solve any quadratic equation, we have to be able to take the square root of negative numbers. To resolve this problem, when proceeding informally, we simply define a quantity i to be $i = \sqrt{-1}$.

Certainly i is not a real number, but that alone should not stop us from working with it. Earlier in the development of mathematics, people did not make use of negative numbers, which is a reasonable approach if we insist on only using numbers that are physically meaningful. There is no physical object corresponding to -3 , for example; you cannot hold -3 apples. You can think of -3 apples as owing someone else 3 apples, but that is a mental construct, which is what i is. Today we are used to working with negative numbers, due to years of practice in school, so we do not question their existence. With a bit of practice, the number i starts to seem reasonable too. It is all a matter of what we mean by “existence,” which to a mathematician does not refer to physical existence. From a mathematical point of view, the real question is not whether i exists, but whether it causes any problems. Our formal construction given below shows that there are no more problems with i than with the real numbers.

If $a \in \mathbb{R}$ is any positive number, then using i we could compute $\sqrt{-a} = \sqrt{a}i$. We define the set of complex numbers, denoted \mathbb{C} , as all numbers of the form $a + bi$, where $a, b \in \mathbb{R}$. Numbers of the form bi for $b \in \mathbb{R}$ are called “imaginary” numbers. A nice way to think of \mathbb{C} is as a plane,

as shown in Figure 8.6.1. We locate the point $a + bi$ in this plane by going a units horizontally and b units vertically. Much of what is done with real numbers can also be done with complex numbers. For example, it is possible to do calculus with complex numbers, the study of which is called complex analysis (see [Pal91] for example).

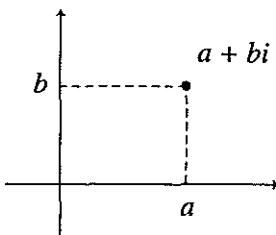


Figure 8.6.1.

Mathematicians today use the following construction of the complex numbers, due to William Rowan Hamilton in 1833, which erased any lingering doubts about the existence of i . The construction of the complex numbers from the real numbers is actually simpler than the constructions of the integers or rational numbers, in that it does not require the use of equivalence classes. Just as the standard symbols of $+$, \cdot and $-$ formally meant different things when used with the rational numbers versus the integers when we constructed the former from the latter, they will also mean something different when applied to the complex numbers (though, as before, these symbols correspond to the same intuitive notion in all three cases). We leave all the proofs in this section to the reader.

Definition. Let \mathbb{C} denote the set $\mathbb{R} \times \mathbb{R}$. Let $+$ and \cdot be the binary operations on \mathbb{C} given by

$$(a, b) + (c, d) = (a + c, b + d), \\ (a, b) \cdot (c, d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c)$$

for all $(a, b), (c, d) \in \mathbb{C}$. Let $-$ be the unary operation on \mathbb{C} given by $-(a, b) = (-a, -b)$ for all $(a, b) \in \mathbb{C}$. Let $\mathbb{C}^* = \mathbb{C} - \{(0, 0)\}$. Let $^{-1}$ be the unary operation on \mathbb{C}^* given by $(a, b)^{-1} = (a/(a^2+b^2), -b/(a^2+b^2))$ for all $(a, b) \in \mathbb{C}^*$. Δ

Analogously to previous constructions, we can define a map from \mathbb{R} to \mathbb{C} that is used to identify \mathbb{R} with a subset of \mathbb{C} .

Theorem 8.6.4. Let $j: \mathbb{R} \rightarrow \mathbb{C}$ be given by $j(x) = (x, 0)$ for all $x \in \mathbb{R}$.

(i) The map $j: \mathbb{R} \rightarrow \mathbb{C}$ is injective.

(ii) Let $x, y \in \mathbb{R}$. Then

- (a) $j(x + y) = j(x) + j(y)$;
- (b) $j(x \cdot y) = j(x) \cdot j(y)$.

Proof. Left to the reader in Exercise 8.6.2. □

We can now think of \mathbb{R} as sitting inside of \mathbb{C} . The set of all complex numbers of the form $(a, 0)$, where a is a real number, is virtually identical to the set of real numbers.

How does this formal construction relate to square roots of negative numbers? We formally define the complex number i by letting $i = (0, 1)$. There is nothing “imaginary” about this i ; it is a perfectly well-defined object. Using the definition of \cdot we compute

$$i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0).$$

Because the real number -1 is identified with the complex number $(-1, 0)$ via the map j defined above, then we essentially have “ $i^2 = -1$.” In this sense our rigorous construction of \mathbb{C} recaptures the intuitive notion of $\sqrt{-1}$. Even further, define “scalar multiplication” of a complex number by a real number by letting $c(a, b) = (ca, cb)$ for all $c \in \mathbb{R}$ and $(a, b) \in \mathbb{C}$. It then follows that for any complex number (a, b) , we have

$$(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1).$$

Using the definition of i , we see that $b(0, 1) = bi$. Since $(1, 0)$ is identified with the real number 1 , we can abbreviate $a(1, 0)$ by writing a . Hence we can write, as an abbreviation, that $(a, b) = a + bi$. Thus we recover our original approach to complex numbers, but without any doubts this time.

The complex numbers have the same nice properties as the real numbers and the rational numbers when it comes to addition and multiplication.

Theorem 8.6.5. Let $\alpha, \beta, \gamma \in \mathbb{C}$.

- (i) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
- (ii) $\alpha + \beta = \beta + \alpha$.
- (iii) $\alpha + (0, 0) = \alpha$.
- (iv) $\alpha + (-\alpha) = (0, 0)$.

(v) If $\alpha + \gamma = \beta + \gamma$, then $\alpha = \beta$.

(vi) $-(-\alpha) = \alpha$.

(vii) $-(\alpha + \beta) = (-\alpha) + (-\beta)$.

Proof. Left to the reader in Exercise 8.6.3. \square

Theorem 8.6.6. Let $\alpha, \beta, \gamma \in \mathbb{C}$.

(i) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

(ii) $\alpha \cdot \beta = \beta \cdot \alpha$.

(iii) $\alpha \cdot (1, 0) = \alpha$.

(iv) $\alpha \cdot \beta = (0, 0)$ iff $\alpha = (0, 0)$ or $\beta = (0, 0)$.

(v) If $\alpha \neq (0, 0)$, then $\alpha \cdot \alpha^{-1} = (1, 0)$.

(vi) If $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.

(vii) If $\gamma \neq (0, 0)$, then $\alpha \cdot \gamma = \beta \cdot \gamma$, then $\alpha = \beta$.

(viii) $(-\alpha) \cdot \beta = -(\alpha \cdot \beta) = \alpha \cdot (-\beta)$.

Proof. Left to the reader in Exercise 8.6.4. \square

One disadvantage of the complex numbers is that it is not possible to define a useful order relation on \mathbb{C} similar to $<$ on \mathbb{R} . This fact is not surprising, when we think of the set of complex numbers as a plane. The complex numbers are otherwise so useful that the price of not having an order relation is worth paying.

The major advantage of the complex numbers over the real numbers is the ability to solve polynomial equations in \mathbb{C} . Since we can take the square root of negative numbers in \mathbb{C} , it is easy to deduce from the quadratic formula that any quadratic polynomial with coefficients in \mathbb{R} must have one or two roots in \mathbb{C} . The quadratic formula also works for quadratic polynomials with coefficients in \mathbb{C} , and such equations also have roots in \mathbb{C} . What is much less obvious is that higher degree polynomials with coefficients in \mathbb{C} also always have roots in \mathbb{C} . This amazing result is stated in the following celebrated theorem.

Theorem 8.6.7. (Fundamental Theorem of Algebra) *Suppose that $a_0, a_1, \dots, a_n \in \mathbb{C}$. The equation $a_nx^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ has a solution in \mathbb{C} .*

The Fundamental Theorem of Algebra is an existence theorem, in that it tells us that roots of certain equations always exist, but it does not tell us how to find these roots. In fact, there is no general formula for the solution of polynomial equations of degree five or higher (see [Sti94, Section 8.4]). Although the theorem applies to polynomials with coefficients in \mathbb{C} , it also applies to polynomials with coefficients in \mathbb{R} , since real numbers are also complex numbers. The conclusion of the theorem, however, would still be that we are guaranteed a root in \mathbb{C} (though not necessarily in \mathbb{R}), even if the original polynomial had real coefficients. It is straightforward to deduce from the above theorem that any polynomial with complex coefficients can in fact be completely factored over \mathbb{C} . For historical background, and six proofs of the Fundamental Theorem of Algebra, see [FR97]; among the six proofs are the standard ones involving complex analysis and algebraic topology.

Finally, it might appear as if our constructions of ever larger sets of numbers could go on forever. For each new number system we construct, we could presumably always find some problem, and then remedy the problem by constructing new numbers. Actually, the set of complex numbers is quite satisfactory as is (even though it does not have an order relation). It has all the nice algebraic properties of \mathbb{Q} (technically, it is a field); it has the nice completeness property of the real numbers (technically, all Cauchy sequences in \mathbb{C} converge in \mathbb{C}); and all polynomial equations in \mathbb{C} have solutions in \mathbb{C} . Though it is possible to construct number systems that contain the complex numbers (for example the quaternions, as discussed in [Fra94, Section 5.7]), these sets of numbers lose some of the nice properties of the complex numbers, and while useful in some situations, they are generally not as good to work with. The set of complex numbers is the largest standard set of numbers that is commonly used.

Exercises

8.6.1. [Used in Section 8.6.] Let $x \in \mathbb{R}$. Show that $x^2 \geq 0$ (where $x^2 = x \cdot x$).

8.6.2. [Used in Section 8.6.] Prove Theorem 8.6.4.

8.6.3. [Used in Section 8.6.] Prove Theorem 8.6.5.

8.6.4. [Used in Section 8.6.] Prove Theorem 8.6.6.

8.7 Appendix: Proof of Theorem 8.2.1

We give here a lengthy proof that we skipped in Section 8.2; the argument, following [Dea66, Section 3.5], is standard.

Proof of Theorem 8.2.1. We have to prove both existence and uniqueness; we start with the latter. Suppose we have functions $f, f': N \rightarrow H$ such that $f(1) = e = f'(1)$, and that $f \circ s = k \circ f$ and $f' \circ s = k \circ f'$. Let

$$G = \{a \in N \mid f(a) = f'(a)\}.$$

We will prove that $G = N$; the fact that $f = f'$ will follow immediately. It is clear that $G \subseteq N$. We know that $1 \in N$, since $f(1) = e = f'(1)$. Now suppose $n \in G$; we need to show that $s(n) \in G$. Since $n \in G$ we know that $f(n) = f'(n)$. Then, using the hypotheses on f and f' , we have

$$\begin{aligned} f(s(n)) &= (f \circ s)(n) = (k \circ f)(n) = k(f(n)) \\ &= k(f'(n)) = (k \circ f')(n) = (f' \circ s)(n) = f'(s(n)). \end{aligned}$$

Hence $s(n) \in G$. It now follows from part (3) of the definition of the Peano Postulates that $G = N$, and the proof of uniqueness is complete.

We now prove that a function f as desired exists. Using the formal definition of functions given in Section 4.1, we can think of a function $N \rightarrow H$ as a subset of $N \times H$ satisfying certain properties. We start by defining a collection \mathcal{C} of subsets of $N \times H$ to be

$$\mathcal{C} = \{W \subseteq N \times H \mid (1, e) \in W, \text{ and if } (n, y) \in W \text{ then } (s(n), k(y)) \in W\}.$$

We note that \mathcal{C} is non-empty, since the set $N \times H$ is in \mathcal{C} . Now let $f = \bigcap_{W \in \mathcal{C}} W$. Clearly $f \subseteq N \times H$. Since $(1, e) \in W$ for all $W \in \mathcal{C}$, it follows that $(1, e) \in f$. Moreover, suppose that $(n, y) \in f$. Then $(n, y) \in W$ for all $W \in \mathcal{C}$, and thus $(s(n), k(y)) \in W$ for all W . Hence $(s(n), k(y)) \in f$. We therefore see that $f \in \mathcal{C}$. By the definition of f , it follows that $f \subseteq W$ for all $W \in \mathcal{C}$, and that nothing in \mathcal{C} is a proper subset of f .

Our goal is to show that f is a function $N \rightarrow H$, that $f(1) = e$ and that $f \circ s = k \circ f$. As a preliminary step, we show that if $(n, y) \in f$ and $(n, y) \neq (1, e)$, then there is some $(m, u) \in f$ such that $(n, y) = (s(m), k(u))$. Suppose to the contrary, so that there is some $(r, t) \in f$ such that $(r, t) \neq (1, e)$, and such that there is no $(m, u) \in f$ such that $(r, t) = (s(m), k(u))$. Define $f' = f - \{(r, t)\}$. Clearly $f' \subseteq N \times H$, and $(1, e) \in f'$. Moreover, suppose that $(n, y) \in f'$. Then $(n, y) \in f$, and since $f \in \mathcal{C}$,

it follows that $(s(n), k(y)) \in f$. Since $(r, t) \neq (s(n), k(y))$, we see that $(s(n), k(y)) \in f'$. We therefore deduce that $f' \in \mathcal{C}$, a contradiction to the fact that nothing in \mathcal{C} is a proper subset of f . Thus we have proved that if $(n, y) \in f$ and $(n, y) \neq (1, e)$, then there is some $(m, u) \in f$ such that $(n, y) = (s(m), k(u))$.

We now show that f is a function $N \rightarrow H$. Let

$$G = \{a \in N \mid \text{there is unique } x \in H \text{ such that } (a, x) \in f\}.$$

We will prove that $G = N$; the fact that f is a function follows immediately. It is clear that $G \subseteq N$. To show that $1 \in G$, we first recall that $(1, e) \in f$. Now suppose $(1, p) \in f$ for some $p \in H$ such that $p \neq e$. By the preliminary step shown in the previous paragraph, there is some $(m, u) \in f$ such that $(1, p) = (s(m), k(u))$. Hence $1 = s(m)$, a contradiction to part (1) of the Peano Postulates. Thus e is the unique element in H such that $(1, e) \in f$. Hence $1 \in G$.

Now suppose $n \in G$. We will show that $s(n) \in G$. Let $y \in H$ be the unique element such that $(n, y) \in f$. Since $f \in \mathcal{C}$, we know that $(s(n), k(y)) \in f$. Now suppose $(s(n), q) \in f$ for some $q \in H$ such that $q \neq k(y)$. Using the fact that $s(n) \neq 1$, because of part (1) of the Peano Postulates, we know that $(s(n), q) \neq (1, e)$. Hence, by the preliminary step there is some $(a, b) \in f$ such that $(s(n), q) = (s(a), k(b))$. Thus $s(n) = s(a)$ and $q = k(b)$. By part (2) of the Peano Postulates we know that s is injective, and hence $n = a$. Thus $(a, b) = (n, b)$. It follows that $(n, b) \in f$, and by the uniqueness of y we deduce that $b = y$. Thus $q = k(b) = k(y)$, a contradiction. Hence $k(y)$ is the unique element of H such that $(s(n), k(y)) \in f$. Hence $s(n) \in G$. It follows that $G = N$.

To complete the proof of the proposition, we need to show that $f(1) = e$ and $f \circ s = k \circ f$. The first of these two properties is equivalent to saying that $(1, e) \in f$, which we have seen already. To prove the second of these properties, let $n \in N$. If we let $y = f(n)$, then $(n, y) \in f$. As before, we know that $(s(n), k(y)) \in f$. This last statement can be rephrased as $f(s(n)) = k(y)$. From the definition of y it follows that $f(s(n)) = k(f(n))$. Since this last statement holds for all $n \in N$; we deduce that $f \circ s = k \circ f$. \square

9

Explorations

The imagination in a mathematician who creates makes no less difference than in a poet who invents.

Jean d'Alembert (1717–1783)

9.1 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 up till now. So far you have been learning the material from the text, using exercises as practice. Real mathematical research 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.

In research there is no text 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, 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, we cannot 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 you by giving you some open-ended topics to explore. These topics are all known to mathematicians, but we assume that you have not seen them. For each of these topics, we give a few definitions, and raise a few questions, and leave the rest to your imagination. You should pick a topic, and then play with it. Formulate conjectures, make whatever extra definitions are necessary and try to come up with theorems and proofs. When you are finished, you should write up your results as if you were writing an additional section for this book. Include definitions, examples, theorems and proofs, as well as informal discussion, in your exposition. You should assume that your audience is another student in your class, who has seen the same material from this book as you have, but who has not seen anything beyond this (and in particular, has not looked at the topic about which you are writing). Do not look your topic up in other books until you have finished your own exploration.

Rather than choosing one of the topics suggested below, you could try to come up with a choice of your own. Finding your own topic is the best way to ensure that you will enjoy working on it, but it is also the most risky, because some proposed avenues of exploration may not lead anywhere, and others may be too difficult. Consult with your instructor about your ideas.

9.2 Greatest Common Divisors

A standard construction that you learned 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. The notion of greatest common divisor, which is very useful in number theory, is our topic here. Recall the definition of an integer a dividing an integer b , denoted $a|b$, given in Section 2.2.

Definition. Let $a, b \in \mathbb{Z}$, and assume that at least one of a and 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 . We also say that $(0, 0) = 0$. Δ

For example, we have $(27, 36) = 9$. The notation (a, b) for the greatest common divisor of a and b is somewhat unfortunate, since the same

notation can also mean an ordered pair, or an interval in the real numbers, but it is quite standard, and rarely causes confusion when read in context. We can see that (a, b) exists for any $a, b \in \mathbb{Z}$, as follows. Let $a, b \in \mathbb{Z}$. If $a = 0 = b$ then (a, b) exists, so assume otherwise. The set

$$S = \{d \in \mathbb{N} \mid d|a \text{ and } d|b, \text{ and } d > 0\}$$

is non-empty (it contains 1), and it is bounded above by the larger of a and b . Hence S is a non-empty finite set, and by Exercise 8.3.6 there exists some $k \in S$ such that $p \leq k$ for all $p \in S$. Since any divisor of a and b that is not in S is negative, then clearly k is the greatest common divisor of a and b . Notice that (a, b) is always positive for any $a, b \in \mathbb{Z}$.

The following related definition is very useful.

Definition. Let $a, b \in \mathbb{Z}$. We say that a and b are **relatively prime** if $(a, b) = 1$. \triangle

For example, we see that 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 you are thinking 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 should not be used here. All results about greatest common divisors that you look at here should be proved directly from the definition (and any lemmas you have proved).

Proposition 9.2.1. *Let $a, b \in \mathbb{Z}$. If $d = (a, b)$ is not zero, then $(a/d, b/d) = 1$.*

Proof. Note that a/d and b/d are integers. Suppose that $r \in \mathbb{Z}$ is such that $r|(a/d)$ and $r|(b/d)$. Then there exist $m, n \in \mathbb{Z}$ such that $rm = a/d$ and $rn = b/d$. 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 $r \leq 1$. Since 1 does divides both a/d and b/d , we see that $(a/d, b/d) = 1$. \square

If you look at some examples of greatest common divisors, you might notice 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 result is always true.

Theorem 9.2.2. *Let $a, b \in \mathbb{Z}$. If $d \in \mathbb{Z}$ is such that $d|a$ and $d|b$, then $d|(a, b)$.*

The above theorem follows from the next result.

Theorem 9.2.3. *Let $a, b \in \mathbb{Z}$. Then there are $m, n \in \mathbb{Z}$ such that $(a, b) = ma + nb$.*

Theorem 9.2.3 is proved by using the Well-Ordering Principle (Theorem 8.3.2) applied to the set of all positive integers of the form $ma + nb$, and then using the Division Algorithm (Theorem 8.4.9).

Your task is to conjecture and prove as many results about greatest common divisors as possible using only what is stated above. While you are at it, prove Theorems 9.2.3 and 9.2.2.

Greatest common divisors are discussed in many number theory texts, such as [Ros93a, Section 2.1], which we have followed here.

9.3 Divisibility Tests

There are a number of known methods for determining whether an integer is divisible by a given integer. For example, an integer is divisible by 9 iff the sum of its digits is divisible by 9. Thus, we easily see that 107523 is divisible by 9, because $1 + 0 + 7 + 5 + 2 + 3 = 18$, and we know 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 5.2.11 that if $a_m a_{m-1} \cdots a_2 a_1$ is a positive integer 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 5.2.12. If x is a positive integer, 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 iff $\bar{\Sigma}(x) = 9$.)

Your 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 [Ros93a, Section 4.1].

9.4 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. For example, in calculus courses we regularly deal with sums, differences, products and quotients of functions $\mathbb{R} \rightarrow \mathbb{R}$. From the point of view of combining functions, it turns out to be irrelevant that the domain of these functions is \mathbb{R} (of course, the domain being \mathbb{R} is very important for taking derivatives and integrals). The addition, subtraction, multiplication and division takes place in the codomain. The notion of adding, subtracting, multiplying and dividing functions can be applied to any functions with codomain \mathbb{R} (or some other sets such as the complex numbers, but we will not deal with this here). For convenience we use the following terminology.

Definition. A **real-valued function** is a function of the form $f: X \rightarrow \mathbb{R}$, where X is a set. Δ

Your task is to explore the properties of real-valued functions. For example, we can define addition of real-valued functions as follows.

Definition. Let X be a set and let $f, g: X \rightarrow \mathbb{R}$ be functions. The **sum** of f and g , denoted $f + g$, is the function $f + g: X \rightarrow \mathbb{R}$ given by

$$(f + g)(x) = f(x) + g(x)$$

for all $x \in X$. Δ

Note that we can only add two real-valued functions if they have the same domains. The above definition is often referred to as “pointwise addition,” since it is done separately for each point in the domain. It is possible to define other operations pointwise, 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 9.4.1. *Let X be a set and let $f, g: X \rightarrow \mathbb{R}$ be functions. Then $f + g = g + f$.*

Proof. Clearly $f + g$ and $g + f$ have the same domain and codomain. 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 any real numbers $a, b \in \mathbb{R}$, and 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 $f + g = g + f$. \square

You should now try to conjecture and prove other results about addition of real-valued functions, and you should define other operations (such as multiplication) and relations (such as less than) for real-valued functions, and then prove results about these definitions.

9.5 Iterations of Functions

We mentioned the idea of iterations of functions in Exercises 4.4.18 and 4.4.19. Those two exercises are rather lengthy and difficult. Here we wish to look at some simpler properties of iterations of maps. For convenience, we repeat the basic definition.

Definition. Let $f: A \rightarrow A$ be a map. Let n be a positive integer. We let f^n denote the map $A \rightarrow A$ given by

$$f^n = \underbrace{f \circ \cdots \circ f}_{n \text{ times}}.$$

We refer to f^n as the **n -fold iteration** of f . \triangle

As simple as this definition seems, 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 includes the much talked about “chaos”).

Your task is to explore various properties of iterations of functions. Some possible questions to look at involve the following concepts.

Definition. Let $f: A \rightarrow A$ be a map. The map f is **nilpotent** if $f^n = 1_A$ for some $n \in \mathbb{N}$. The map f is **hidempotent** if $f^n = f$ for some $n \in \mathbb{N}$ such that $n \geq 2$. The map f is **constantive** if f^n is a constant map for some $n \in \mathbb{N}$. Δ

The term “nilpotent” is quite standard, whereas the other two terms in the above definition 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 map that is not constant? For any given positive integer r such that $r \geq 2$, is there a map $f: A \rightarrow A$ for some set A such that f^r is a constant map, but f^{r-1} is not a constant map? Is there a nilpotent map that is not the identity map? For any given positive integer r such that $r \geq 2$, is there a map $g: A \rightarrow A$ for some set A such that $g^r = 1_A$ but $g^{r-1} \neq 1_A$? If a map is nilpotent or hidempotent, is it necessarily bijective? If a map is hidempotent and bijective, is it necessarily nilpotent? If a map is nilpotent, is it necessarily hidempotent? Can you come to stronger conclusions when the set A is finite? What other questions can you think of concerning these definitions? What other definitions concerning iterations of maps can you come up with, and what can you prove about your definitions?

See [HW91, Chapter 5] or [ASY97] for details about iterations of maps in connection with dynamical systems and chaos.

9.6 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 Theorem 6.4.6, Corollary 6.4.8 and Exercises 6.4.5–6.4.8. Play with the Fibonacci numbers, and try to find (and prove) other formulas.

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

$$1, 3, 4, 7, 11, 18, 29, 47, 76, 123 \dots$$

The numbers in this sequence are referred to as Lucas numbers. Denote the elements of the Lucas sequence by L_1, L_2, \dots . We formally define the Lucas sequence as the sequence satisfying the recursive definition given 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 2.4–2.5] for more details.

Your 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? Can you find an explicit formula for the Lucas numbers, similar to Corollary 6.4.8?

C) Relations between Fibonacci and Lucas Numbers

There are some formulas relating the Fibonacci numbers and the Lucas numbers. A simple example is $L_n = F_n + 2F_{n-1}$ for all $n \in \mathbb{N}$ such that $n \geq 2$. Prove this formula, and try to find other such formulas.

D) Fibonacci Numbers Modulo k

Choose some $k \in \mathbb{N}$. 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 $\{0, 1, \dots, k-1\}$ that is congruent to it modulo k . For example, if we use $k = 3$, we obtain the modulo 3 Fibonacci sequence, which starts

$$1, 1, 2, 0, 2, 2, 1, 0, 1, 1, 2, 0 \dots$$

Denote the elements of this sequence by $F_1^{(3)}, F_2^{(3)}, \dots$. Observe that $F_{n+2}^{(3)} \equiv F_{n+1}^{(3)} + F_n^{(3)} \pmod{3}$ for all $n \in \mathbb{N}$, as can be proved using Lemma 5.2.5. Notice also that this sequence repeats itself. What can you deduce about the original Fibonacci sequence from this repetition? Play around with these ideas using various values for k .

Some sources with many results about Fibonacci numbers are [Knu73, Section 1.2.8 and exercises], [GKP94, Section 6.6] and [HHP97, Chapter 3].

9.7 Fuzzy Sets

A fundamental feature of sets is that any element is either 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 1960’s. 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 functions (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. Let X be a set. For each subset $A \subseteq X$, define the **characteristic function** $\chi_A^X: X \rightarrow \{0, 1\}$ by

$$\chi_A^X(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \in X - A. \end{cases}$$

(We write χ_A when X is understood from the context.) △

The characteristic function χ_A maps everything in the set A to 1, and everything else to 0, and is thus useful for identifying the set A . In Exercise 4.1.8, it was shown that if $A, B \subseteq X$, then $\chi_A = \chi_B$ iff $A = B$ (the former equality is of functions, the latter of sets).

To allow fuzziness, we use characteristic functions whose values can be 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 functions for such sets, we simply let our broader characteristic functions be the definition of our new kind of sets.

Definition. Let X be a set. A **fuzzy subset** A of X is a function $\mu_A: X \rightarrow [0, 1]$. △

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 $0 < \mu_A(x) < 1$. Note that a function $\mu_A: X \rightarrow [0, 1]$ is not

the name of the fuzzy subset of X , but rather A is the name of the subset. Note 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. Let X be a set, and let A and B be fuzzy subsets of X .

- (1) The **empty set** in X , denoted \emptyset , is defined by $\mu_\emptyset(x) = 0$ for all $x \in X$.
- (2) We say that A is a **subset** of 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 given 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 given 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 given 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 given 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 $A \hat{+} B$, is the fuzzy subset G of X given by $\mu_G(x) = \mu_A(x) + \mu_B(x) - \mu_A(x) \cdot \mu_B(x)$ for all $x \in X$. Δ

It is left to the reader to verify that the algebraic sum of two fuzzy sets is indeed a fuzzy set (the issue is that the characteristic map must have codomain $[0, 1]$). We are using some of the same notation for fuzzy sets 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 9.7.1. *Let X be a 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

$$\begin{aligned} & \min\{\mu_A(x), \max\{\mu_B(x), \mu_C(x)\}\} \\ &= \max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\}. \end{aligned}$$

There are a number of cases. First, suppose that $\mu_A(x) \leq \mu_B(x)$ and $\mu_A(x) \leq \mu_C(x)$. Then

$$\min\{\mu_A(x), \max\{\mu_B(x), \mu_C(x)\}\} = \mu_A(x)$$

and

$$\begin{aligned} \max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\} \\ = \max\{\mu_A(x), \mu_A(x)\} = \mu_A(x). \end{aligned}$$

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

$$\begin{aligned} \max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\} \\ = \max\{\mu_A(x), \mu_C(x)\} = \mu_A(x). \end{aligned}$$

Similarly if $\mu_B(x) \leq \mu_A(x) \leq \mu_C(x)$. 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

$$\begin{aligned} \max\{\min\{\mu_A(x), \mu_B(x)\}, \min\{\mu_A(x), \mu_C(x)\}\} \\ = \max\{\mu_B(x), \mu_C(x)\} = \mu_C(x). \end{aligned}$$

Similarly if $\mu_C(x) \leq \mu_B(x) \leq \mu_A(x)$. Putting all the cases together proves the desired result. \square

Your task is to conjecture and prove as many results as you can about the operations on fuzzy sets. Which of the analogs of the results in Lemma 3.2.2 and Theorem 3.3.2 hold with union and intersection of fuzzy sets, or with algebraic sum and product? Can you define similar operations for indexed families of sets, analogously to what we saw in Section 3.4?

See [BG95] and [Zim96] for further discussion of fuzzy sets and their applications.

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 more rigorous treatment of these numbers is given in Chapter 8.

All the numbers we deal with in this book are real numbers. In particular, we will not make use of complex numbers (except for a brief discussion of them in Section 8.6). We standardly think of the real numbers as forming the real number line, which extends infinitely in both positive and negative directions. We have the operations addition, multiplication and negation on the real numbers, and the relations $<$ and \leq on these numbers. (We will not be making much use of subtraction and division, since these can be defined in terms of addition and multiplication respectively.) Among the most important properties of these operations and relations are the following.

Fact. *Let x , y and z be real numbers.*

(i) $(x + y) + z = x + (y + z)$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(Associative Laws).

(ii) $x + y = y + x$ and $x \cdot y = y \cdot x$ *(Commutative Laws).*

(iii) $x + 0 = x$ and $x \cdot 1 = x$ *(Identity Laws).*

- (iv) $x + (-x) = 0$ (*Inverses Law*).
- (v) If $x \neq 0$, then $x \cdot x^{-1} = 1$ (*Inverses Law*).
- (vi) If $x + z = y + z$, then $x = y$ (*Cancelation Law*).
- (vii) If $z \neq 0$, then $x \cdot z = y \cdot z$ iff $x = y$ (*Cancelation Law*).
- (viii) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ (*Distributive Law*).
- (ix) $-(-x) = x$ (*Double negation*).
- (x) $-(x + y) = (-x) + (-y)$.
- (xi) $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$.
- (xii) If $x < y$ and $y < z$, then $x < z$.
- (xiii) Precisely one of the following holds: either $x < y$, or $x = y$, or $x > y$ (*Trichotomy Law*).
- (xiv) If $x \leq y$ and $y \leq x$, then $x = y$.
- (xv) If $0 < z$, then $x < y$ iff $x \cdot z < y \cdot z$.

There are the particularly useful collections of real numbers. The first is the integers, which are

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

The sum, difference, and product of any two integers is also an integer, though the quotient of two integers need not be an integer. The positive integers are often referred to as natural numbers. Being real numbers, the integers satisfy all the properties of real numbers listed above. There are some more subtle properties of the integers (for example unique factorization into prime numbers), but we will only make use of such properties on a few occasions.

The second useful collection is the rational numbers, which is another name for the fractions. In other words, a real number x is rational if $x = a/b$ for some integers a and b , where $b \neq 0$. It can be shown that the rational numbers are precisely those real numbers whose decimal expansions are either repeating, or are zero beyond some point. 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 Section 2.3. Again, being real numbers, the rational numbers satisfy all the properties of real numbers listed above. The rational numbers also satisfy some more subtle 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), and once again we will rarely make use of any such facts.

Hints for Selected Exercises

Section 1.2 Statements

- 1.2.1. Part (7): Not a statement.
- 1.2.2. Part (2): A statement (though a false one).
- 1.2.5. Part (7): $\neg Y \vee X$.
- 1.2.8. Part (6): True.
- 1.2.13. Part (1): Neither.

Section 1.3 Relations Between Statements

- 1.3.5. Part (1): The statements are equivalent. Use Fact 1.3.2 (viii).
- 1.3.8. Part (5): The inverse is “If you do not like him, do not give him a hug.” The converse is “If you give him a hug, you like him.” The contrapositive is “If you do not give him a hug, you do not like him.”
- 1.3.10. Part (2): $3 \geq 5$ and $7 < 8$.
- 1.3.12. Part (2): Show that the statement is equivalent to $A \rightarrow B$, using Exercises 1.3.2 (4) and 1.3.3 (2).

1.3.13. Part (1): There are four unary operations and sixteen binary operations.

Part (2): Use truth tables, and equivalences we already know, to show that the result of each operation in part (1) is equivalent to some combination of \wedge and \neg . For example, $P \vee Q \iff \neg(\neg P \wedge \neg Q)$, which follows from Fact 1.3.2 (i) and (xiii).

Part (3): By part (2) of this exercise, it suffices to show that \wedge and \neg are each equivalent to a combination of $\bar{\wedge}$ operations.

Section 1.4 Valid Arguments

1.4.1. Part (6):

(1) $\neg A \rightarrow (B \rightarrow \neg C)$	
(2) $C \rightarrow \neg A$	
(3) $(\neg D \vee A) \rightarrow \neg\neg C$	
(4) $\neg D$	
(5) $\neg D \vee A$	(4), Addition
(6) $\neg\neg C$	(3), (5), Modus Ponens
(7) C	(6), Double Negation
(8) $\neg A$	(2), (7), Modus Ponens
(9) $B \rightarrow \neg C$	(1), (8), Modus Ponens
(10) $\neg B$	(9), (6), Modus Tollens.

1.4.2. Part (3): Consider the case where the food is not green, is not undercooked, is not smelly and is stale.

1.4.3. Part (1): The premises are inconsistent. Deduce from the premises that amoebas can dance and that amoebas cannot dance, and then follow the method used in the derivation in the text that shows that Ferdinand plays the accordion.

Section 1.5 Quantifiers

1.5.1. Part (1): Every person has green hair.

1.5.5. Part (1): “For all people x , it is the case that x is nice.”

Part (5): Note that the expression “There is no . . .” is not one of the quantifiers we are using.

1.5.6. Part (1): “There is a boy who is not good.”

Part (2): “All bats weigh less than 50 lbs.”

1.5.9. A number x is non-gelatinous if it is not phlegmatic, or if there is an integer n such that for all real numbers y , we have y^2 does not upper-encapsulate x and $y + n$ does not lower-encapsulate x .

1.5.11. Part (2):

- (1) $(\forall a \text{ in } V)[(N(a) \rightarrow B(a)]$
 (2) $(\exists b \text{ in } V)[N(b) \wedge D(b)]$

(3) $N(x) \wedge D(x)$	(2), Existential Instantiation
(4) $N(x)$	(3), Simplification
(5) $D(x)$	(3), Simplification
(6) $N(x) \rightarrow B(x)$	(1), Universal Instantiation
(7) $B(x)$	(6), (4), Modus Ponens
(8) $B(x) \wedge D(x)$	(7), (5), Adjunction
(9) $(\exists c \text{ in } V)[B(c) \wedge D(c)]$	(8), Existential Gen.

Section 2.1 Mathematical Proofs

2.1.1. Part (1): If r is a real number, then any circle of radius r has area πr^2 .

Section 2.2 Direct Proofs

2.2.1. Part (1): Suppose that n is divisible by 7. Hence there is some integer k such that $n = 7k$ (argumentation) . . . Then n is bulbous.

2.2.2. Part (1): Observe that $1 \cdot n = n$. Hence $1|n$.

Part (3): Suppose that $m|n$. Then there is an integer j such that $mj = n$. Then $m(-j) = -n$. Because j is an integer, so is $-j$. Hence $m|(-n)$.

2.2.8. Suppose that $a|b$. Then there is an integer k such that $ak = b$. Let n be a positive integer. Then $(ak)^n = b^n$. Continue from there.

Section 2.3 Contrapositive and Contradiction

2.3.2. Use proof by contrapositive. Assume that n is odd, and deduce that n^2 is odd.

2.3.4. The proof is by contradiction. Let q be a non-zero rational number and let y be an irrational number. By the definition of rational numbers, there are integers a and b such that $b \neq 0$ and $q = a/b$. We want to show that qy is irrational; assume the contrary. Thus qy is rational. Hence there are integers m and n such that $n \neq 0$ and $qy = m/n$. Therefore $(a/b)y = m/n$. Deduce a contradiction to the fact that y is irrational.

2.3.5. Use proof by contradiction, and make use of Exercise 2.2.6.

2.3.7. Imitate the proof of Theorem 2.3.3, with q replacing 2.

Section 2.4 Cases, and If and Only If

2.4.5. Part (2): To show that if m or n is a multiple of 3 then mn is a multiple of 3, use various cases. To show that if mn is a multiple of 3 then m or n is a multiple of 3, use proof by contrapositive.

2.4.6. As mentioned in Exercise 2.4.5, precisely one of the following holds: either $p = 3k$ for some integer k , or $p = 3k + 1$ for some integer k , or $p = 3k + 2$ for some integer k . There are now three cases. For the first case, could $p = 3k$ be a prime number for any integer k ?

2.4.8. Since n is odd, there is an integer u such that $n = 2u + 1$. There are now two cases, depending upon whether u is even or odd.

2.4.11. Part (1): There are two cases, depending upon whether $\#x$ equals 0 or not. In the former case, we have $x = I_x$ and $-x = -I_x$, and so $[x] = I_x$ and $[-x] = -I_x$. If $\#x \neq 0$, then $x = I_x + \#x$ and $-x = -I_x + (-\#x) = (-I_x - 1) + (1 - \#x)$, and so $[x] = I_x$ and $[-x] = -I_x - 1$.

Section 2.5 Quantifiers in Theorems

2.5.1. Part (3): The statement could be rewritten as $(\forall k)(\exists w)(w \text{ is opulent, and } k|w)$, where k and w are integers.

2.5.3. Part (1): Let s be a non-negative number. Define $t = s/2$. Then t is non-negative, and $s \geq s/2 = t$.

Part (2): Let $t = 0$. Let s be a non-negative number. Then $s \geq 0 = t$.

Part (3): Let t be a non-negative number t . Define $s = t + 1$. Then s is non-negative, and $s = t + 1 \geq t$.

Part (4): The statement is false. The negation of the statement is “for each non-negative numbers s there is a non-negative number t such that $s < t$.” Show that this new statement is true.

2.5.10. Assume that s and t are both least P -numbers for c and d . Deduce that $s \leq t$ and $t \leq s$. Then use the fact that for any two real numbers x and y , if $x \leq y$ and $y \leq x$, then $x = y$.

Section 2.6 Writing Mathematics

2.6.1. Part (4): In addition to the missing capital letter at the start of the second sentence, the main problem is “so $(x - 5)(x + 2)$, so 5 and -2 ,” which is meaningless as written. A proper write-up would be: “We want to solve the equation $x^2 - 2x = x + 10$. Then $x^2 - 3x - 10$, so $(x - 5)(x + 2) = 0$, so $x = 5$ or $x = -2$.”

Part (6): The problem is the last sentence. We cannot say, “Since n is an integer,” because we have not defined n . The letter n in the first sentence is a bound variable, and is not defined outside of that sentence. A proper write-up would be “We say that a real number x is gloppy if there is some integer n such that $x^2 - n$ is sloppy. Suppose that x is gloppy. Then there is some integer n such that $x^2 - n$ is sloppy. Since n is an integer, then its square is an integer,”

Section 3.2 Sets — Basic Definitions

3.2.1. Part (6): Observe that $1.5 \in [1, 2]$ but $1.5 \notin \{0, 1, 2, 3\}$.

3.2.2. Part (2): The set of composite numbers.

3.2.8. Let $A = \{1\}$ and $B = \{1, \{1\}\}$.

3.2.11. The statement is false. Find a counterexample.

3.2.14. Part (1): $\mathcal{P}(\mathcal{P}(\emptyset))$ has two elements; list them.

Part (2): $\mathcal{P}(\mathcal{P}(\{\emptyset\}))$ has four elements; list them.

Section 3.3 Set Operations

3.3.2. Part (2): $(C - D) \cup E = \{b, d, e, f\}$.

3.3.11. The simplest formula is $A - (B - C) = (A - B) \cup (A \cap C)$. For the proof that $A - (B - C) \subseteq (A - B) \cup (A \cap C)$, let $x \in A - (B - C)$. Then $x \in A$ and $x \notin B - C$. Since $x \notin B - C$, then $x \in C$ or $x \notin B$. Continue from here. The other inclusion is similar.

3.3.13. Use a Venn diagram to help decide whether the statement is true or false. Then give a proof or a counterexample.

3.3.20. Use proof by contradiction. Suppose that $A \times E = B \times E$ and that $A \not\subseteq B$. Use the fact that $E \neq \emptyset$ to deduce that $A \times E \not\subseteq B \times E$, the desired contradiction.

3.3.21. Use proof by contradiction. Suppose that $E \neq \emptyset$. Use Exercise 3.3.20 to derive that $A = B$.

Section 3.4 Indexed Families of Sets

3.4.1. Part(3): $\bigcup_{k \in \mathbb{N}} B_k = (0, 7) \cup \{11, 12, 13, \dots\}$ and $\bigcap_{k \in \mathbb{N}} B_k = [3, 5]$.

3.4.2. Part (1): Let $E_k = [0, k]$ for all $k \in \mathbb{N}$.

3.4.7. To prove that $\bigcup_{i \in I} X_i$ is co- \mathcal{W} for some property \mathcal{W} , we would need to show that $\mathbb{R} - \bigcup_{i \in I} X_i$ satisfies property \mathcal{W} . Use Theorem 3.4.3 (v), and examine each particular property \mathcal{W} separately.

Section 4.1 Functions

4.1.2. Part (3): Does everyone have a best friend?

4.1.4. Part (4): This does not strictly define a function. It should say, “Let $g: \mathbb{R} \rightarrow \mathbb{R}$ be given by $g(x) = e^x$ for all $x \in \mathbb{R}$,” if that is what it means.

4.1.5. Part (6): What is $t(1)$?

4.1.7. Find a counterexample using $A = \{x, y\}$, and $S = \{x\}$ and $B = \{1, 2\}$.

4.1.8. Note that “ $\chi_A = \chi_B$ ” is a statement of equality of functions, whereas “ $A = B$ ” is a statement of equality of sets. It is evident from the definition of characteristic functions that if $A = B$, then $\chi_A = \chi_B$. Now suppose that $\chi_A = \chi_B$. We show that $A = B$ by showing that $A \subseteq B$ and $B \subseteq A$. Suppose that $x \in A$. Then $\chi_A(x) = 1$. Hence $\chi_B(x) = 1$. Deduce that $x \in B$.

Section 4.2 Image and Inverse Image

4.2.2. Part (3): $m^*([1, 3])$ is the set of all cows whose average daily milk production in gallons is between 1 and 3 gallons, including the endpoints.

4.2.3. Part (3): We have $f_*(T) = \{2, 3\}$ and $f^*(T) = (1, 2]$. The reader should find $f_*(f^*(T))$ and $f^*(f_*(T))$.

4.2.5. Part (3): Let $A = \mathbb{R} = B$ and let P be a circle in \mathbb{R}^2 .

4.2.10. Part (1): Look at the map $f: \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = 0$ for all $x \in \mathbb{R}$.

Part (2): Look at the map $g: \mathbb{R} \rightarrow \mathbb{R}$ given by $g(x) = x^2$ for all $x \in \mathbb{R}$.

4.2.13. Part (3): Use parts (1) and (2), and Theorem 4.2.3 (v).

Part (4): Use part (2).

Part (5): Use part (4).

Part (6): Use part (3).

Section 4.3 Composition and Inverse Functions

4.3.3. Observe that

$$(g \circ f)(x) \neq \begin{cases} 3(1 - 2x), & \text{if } x \geq 0 \\ |x| - 1, & \text{if } x < 0. \end{cases}$$

4.3.5. For the second part, let $x \in (g \circ f)^*(V)$. Then $(g \circ f)(x) \in V$, and hence $g(f(x)) \in V$, so $f(x) \in g^*(V)$, and thus $x \in f^*(g^*(V))$. The other inclusion is similar.

4.3.6. Show that $f^{-1} \circ g^{-1}$ works as an inverse for $g \circ f$, using the definition of inverse functions.

4.3.10. For each part, use proof by contradiction, and use Lemma 4.3.4.

4.3.13. Let $E = \{x \in A \mid f(x) = g(x)\}$, and let e be the inclusion map. Let t be given by $t(c) = h(c)$ for all $c \in C$. Show that t is well-defined, and that all the desired properties hold.

4.3.14. Let $P = \{(x, y) \in A \times B \mid f(x) = g(y)\}$.

Section 4.4 Injectivity, Surjectivity

4.4.8. Part (4): Suppose that $U(\mathbb{L}) \cap D(\mathbb{L}) \neq \emptyset$. Thus there are some $(a, b), (c, d) \in \mathbb{L}$ such that $U((a, b)) = D((c, d))$. Derive a contradiction.

4.4.9. Suppose f has a left inverse h . Let $x, y \in A$, and suppose that $f(x) = f(y)$. Then $h(f(x)) = h(f(y))$. Continue from there. Now suppose that f is injective. Define a map $k: B \rightarrow A$ as follows. Pick an element $a_0 \in A$ (it does not matter which one). Let $b \in B$. If $f^*(\{b\}) \neq \emptyset$, then by injectivity there is a single element a in $f^*(\{b\})$; let $k(b) = a$. If $f^*(\{b\}) = \emptyset$, let $k(b) = a_0$. Show that $k \circ f = 1_A$.

4.4.11. Part (1): Assume $E = f^*(f_*(E))$ for all subsets $E \subseteq A$. To show that f is injective, let $x, y \in A$, and suppose that $f(x) = f(y)$. Note that $f_*(\{x\}) = f_*(\{y\})$. Now apply the hypothesis to each of $\{x\}$ and $\{y\}$, and conclude that $\{x\} = \{y\}$. Thus $x = y$.

Part (2): Assume $F = f_*(f^*(F))$ for all subsets $F \subseteq B$. To show that f is surjective, let $b \in B$. Apply the hypothesis to $\{b\}$. Conclude that $b = f(a)$ for any $a \in f^*(\{b\})$.

4.4.14. First assume that f is injective; then use Theorem 4.4.3 (ii). Now assume f is not injective. Let $s, t \in A$ be distinct points such that $f(s) = f(t)$. Let $Y = \{1\}$. Define $g, h: Y \rightarrow A$ by $g(1) = s$ and $h(1) = t$.

4.4.15. Assume that f is surjective. Thus $f_*(A) = B$. Then use Exercise 4.2.11. Assume that $B - f_*(X) \subseteq f_*(A - X)$ for all $X \subseteq A$. Apply the hypothesis to the set $X = A$, and conclude that $f_*(A) = B$.

4.4.16. Assume that f is injective. Use Theorem 4.2.3 (vii). Assume that $h_*(A \cap B) = h_*(A) \cap h_*(B)$ for all $A, B \subseteq X$. Suppose that $s, t \in X$ are such that $s \neq t$. Apply the hypothesis to the sets $A = \{s\}$ and $B = \{t\}$, and conclude that $h_*(\{s\}) \neq h_*(\{t\})$. Note that $h_*(\{s\}) = \{h(s)\}$, and similarly for t .

4.4.17. Part (1): Suppose f is surjective. Let $S \in \mathcal{P}(B)$. Apply Exercise 4.4.11 (2). Now suppose f is not surjective. Let $b \in B$ not be in the image of f . Note that $\{b\} \in \mathcal{P}(B)$; is $\{b\}$ in the image of f_* ?

Part (2): Suppose f is injective. Let $P, R \in \mathcal{P}(A)$ be such that $f_*(P) = f_*(R)$. Apply Exercise 4.4.11 (1). Now suppose f is not injective. Let $x, y \in A$ be distinct elements such that $f(x) = f(y)$. Note that $\{x\}, \{y\} \in \mathcal{P}(A)$. Compare $f_*(\{x\})$ and $f_*(\{y\})$.

Part (3): Suppose f is injective. Let $P \in \mathcal{P}(A)$. Apply Exercise 4.4.11 (1). Now suppose f is not injective. Let $x, y \in A$ be distinct elements such that $f(x) = f(y)$. Note that $\{x\} \in \mathcal{P}(A)$. Is $\{x\}$ in the image of f^* ?

Part (4): Suppose f is surjective. Let $S, T \in \mathcal{P}(B)$, and suppose that $f^*(S) = f^*(T)$. Apply Exercise 4.4.11 (2). Now suppose f is not surjective. Let $b \in B$ not be in the image of f . Note that $\emptyset, \{b\} \in \mathcal{P}(B)$. Compare $f^*(\emptyset)$ and $f^*(\{b\})$.

Part (5): Use parts (1) – (4) of this exercise.

4.4.18. Part (1): Use the properties of f^n stated at the start of the exercise.

Part (2): (A) Let $z \in \mathcal{O}_{f,y}$. Then $z = f^k(y)$ for some $k \in \mathbb{Z}$. Hence $z = f^{k+m}(x)$. Thus $z \in \mathcal{O}_{f,x}$. Similarly for the other inclusion. (B) Use proof by contradiction. Suppose that $w \in \mathcal{O}_{f,x} \cap \mathcal{O}_{f,y}$, etc. (C) Suppose $x \in \mathcal{O}_{f,y}$. Then $x = f^j(y)$ for some $j \in \mathbb{Z}$. Hence $y = f^{-j}(x)$, so $y \in \mathcal{O}_{f,x}$. The other implication is similar. (D) Show that $x \in \mathcal{O}_{f,x}$ for all $x \in A$.

Part (3): Look at maps $f: \mathbb{Z} \rightarrow \mathbb{Z}$ of the form $f(x) = x + a$ for all $x \in \mathbb{Z}$, where $a \in \mathbb{Z}$ is appropriately chosen.

4.4.19. Part (1): Since A is finite, then there are only finitely many bijective maps $A \rightarrow A$; say there are q such maps. Consider the maps $f, f^2, f^3, \dots, f^{q+1}$. Since each of these maps is bijective, at least two of them must be equal. Proceed from there.

Part (2): Suppose $i < 0$. Note that $f^{|i|} = 1_A$. Consider $f^{|i|}(f^i(x))$, and use the properties of f^n stated at the start of Exercise 4.4.18.

Part (3): By definition, we know that $y = f^m(x)$ for some $m \in \mathbb{Z}$. Now use the properties of f^n stated at the start of Exercise 4.4.18.

Part (4): Suppose that $|A| = t$. Look at the elements $f(x), f^2(x), \dots, f^{t+1}(x)$. At least two of these elements must equal each other; say $f^j(x) = f^k(x)$ for some $j, k \in \{1, 2, \dots, t+1\}$ such that $j \neq k$. Without loss of generality, assume that $j < k$. Deduce that $f^{k-j}(x) = x$.

Part (5): Suppose that the order of y with respect to f is less than q .

Part (6): Let $y \in \mathcal{O}_{f,x}$. Then $y = f^s(x)$ for some positive integer s , using part (1) of this exercise. Next, if you divide s by q , let a be the quotient and b the remainder; thus $s = aq + b$, where a is a non-negative integer, and b is an integer such that $0 \leq b < q$. Proceed from there.

Part (7): Suppose that the result does not hold. If you divide r by q , let c be the quotient and d the remainder; thus $r = cq + d$, where c is a non-negative integer, and d is an integer such that $0 \leq d < q$. Since $f^r = 1_A$ then $f^d(x) = x$. Derive that $f^d(x) = x$, a contradiction.

Part (8): Use the fact that $y = f^m(x)$ for some positive integer m , and then look at $y, f(y), f^2(y), \dots, f^{r-1}(y)$.

Part (9): Look at $x, f(x), f^2(x), \dots, f^{r-1}(x)$, and use parts (5) and (6) of this exercise.

Part (10): Break A up into its orbits, which are disjoint by Exercise 4.4.18 (2), and show that for each orbit $\mathcal{O}_{f,y}$, we have $r = \sum_{z \in \mathcal{O}_{f,y}} |f_z|$, using parts (7) and (8) of this exercise.

Part (11): Note that the sum under consideration here counts the same number of things as the sum in part (9) of this exercise, namely the number of pairs $y \in A$ and $i \in \{0, \dots, r-1\}$ such that $f^i(y) = y$.

Section 4.5 Sets of Functions

4.5.5. If $f: C \rightarrow A \times B$ is a map, recall the definition of the coordinate functions $f_1: C \rightarrow A$ and $f_2: C \rightarrow B$ given in Section 4.3. Define a map $\Phi: \mathcal{F}(C, A \times B) \rightarrow \mathcal{F}(C, A) \times \mathcal{F}(C, B)$ by $\Phi(f) = (f_1, f_2)$ for all $f \in \mathcal{F}(C, A \times B)$.

4.5.6. Define a map $\Psi: \mathcal{F}(A, \mathcal{F}(B, C)) \rightarrow \mathcal{F}(B, \mathcal{F}(A, C))$ as follows. For each $f: A \rightarrow \mathcal{F}(B, C)$, let $\Psi(f): B \rightarrow \mathcal{F}(A, C)$ be defined by $[[\Psi(f)](b)](a) = [f(a)](b)$, for all $a \in A$ and $b \in B$.

4.5.7. Find inverse maps for Ω_g and Λ_g .

4.5.8. Both parts are similar to the proof of Lemma 4.5.2.

4.5.9. The same method applies to all three parts. For part (2), for example, let $I_{a,b}$ denote $\{f \in \mathcal{I}(A, B) \mid f(a) = b\}$. Define $\Psi: I_{a,b} \rightarrow \mathcal{I}(A - \{a\}, B - \{b\})$ as follows: For each $g \in I_{a,b}$, let $\Psi(g): (A - \{a\}) \rightarrow (B - \{b\})$ be the function defined by $[\Psi(g)](x) = g(x)$ for all $x \in A - \{a\}$. Show that Ψ is well-defined and bijective.

Section 5.1 Relations

5.1.5. Part (1): R' is always non-reflexive.

Part (2): R' is always symmetric.

Part (3): R' could be either transitive or not transitive.

5.1.9. Use Exercise 5.1.8.

5.1.11. Part (1): See the proof of Theorem 5.3.3 (ii).

5.1.12. Part (1): The function f respects the relation R , because if $x, y \in \mathbb{R}$ and $|x| = |y|$, then $f(x) = x^6 = y^6 = f(y)$.

5.1.13. Could anything in A be related to anything other than itself?

Section 5.2 Congruence

5.2.6. Part (1): This statement is true.

Part (2): This statement is false.

5.2.7. Prove the result by contradiction. Using the given congruence, write 1 as the difference of two integers. Then use the assumption that n is not prime to deduce that 1 is divisible by some integer greater than 1, which is impossible.

5.2.8. By Theorem 5.2.3 (ii) we know that one of $n \equiv 0 \pmod{6}$ or $n \equiv 1 \pmod{6}$ or ... or $n \equiv 5 \pmod{6}$ must hold. In each case, use Lemma 5.2.5 to compute n^2 modulo 6.

5.2.9. There are four cases, depending upon whether $n = 4k$ or $n = k + 1$ or $n = 4k + 2$ or $n = 4k + 3$ for some $k \in \mathbb{Z}$. (That precisely one of these cases holds follows from the Division Algorithm.)

5.2.11. Start by showing that $10^i \equiv 1 \pmod{9}$ for all i . It follows that $a_i 10^i \equiv a_i \pmod{9}$ for all i , by using Lemma 5.2.5. Continue from there.

5.2.12. Part (1): If a has more than one digit, show that $\Sigma(a) < a$.

Part (2): All three statements are false. For the last one, observe that $M(a) = 0$ if a has one digit.

Parts (3), (4): By Exercise 5.2.11 we see that $a \equiv \Sigma(a) \pmod{9}$. Deduce that $a \equiv \bar{\Sigma}(a) \pmod{9}$. Hence $a + b \equiv [\bar{\Sigma}(a) + \bar{\Sigma}(b)] \pmod{9}$, and similarly for multiplication. Note that two integers in $\{1, 2, \dots, 9\}$ are congruent modulo 9 iff they are equal.

Section 5.3 Equivalence Relations

5.3.6. Rewrite the proof of Theorem 5.2.3 in the more general setting of Theorem 5.3.3.

5.3.8. Use Exercise 5.3.7.

5.3.11. Let $Q \in \mathcal{D}$. Let $x \in Q$. Show that $Q = [x]$. Thus $Q \in A/\sim$. Let $[y] \in A/\sim$ for some $y \in A$. Then $y \in P$ for some $P \in \mathcal{D}$. Show that $[y] = P$. Thus $[y] \in \mathcal{D}$.

5.3.14. Show that $\mathcal{D} = \{P \cap Q \mid P \in \mathcal{D}_1 \text{ and } Q \in \mathcal{D}_2\}$.

5.3.15. Part (2): Use the product of sets for $\mathcal{R}(A)$; use repeated power sets for \mathcal{S}_A .

Part (4): Use part (2) of this exercise and Example 3.2.5.

5.3.16. Part (2): Let $x, y \in A$ be distinct elements. To show that $\tilde{\Phi}$ is not injective, let $R, T \in \mathcal{R}(A)$ be given by $R = \{(x, y)\}$ and $T = \{(y, x)\}$. Compute the relation classes $R[x], R[y], T[x]$ and $T[y]$, and then compute $\tilde{\Phi}(R)$ and $\tilde{\Phi}(T)$. To show that $\tilde{\Psi}$ is not injective, let $\mathcal{D}, \mathcal{F} \in \mathcal{S}_A$ be given by $\mathcal{D} = \{\{x, y\}\}$ and $\mathcal{F} = \{\{x, y\}, \{x\}\}$. Compute $\tilde{\Psi}(\mathcal{D})$ and $\tilde{\Psi}(\mathcal{F})$. To show that $\tilde{\Phi}$ is not surjective, note that anything in the image of $\tilde{\Phi}$ is a collection of at most $|A|$ sets (where $|A|$ is the number of elements in A). To show that $\tilde{\Psi}$ is not surjective, show that anything in the image of $\tilde{\Psi}$ must be a symmetric relation.

Part (3): The image of $\tilde{\Psi}$ is the set of all relations R satisfying two properties: the relation R is symmetric, and if $x \in A$ and xRy for some $y \in A$, then xRx . It is straightforward to verify that anything in the image of $\tilde{\Psi}$ satisfies these two conditions. If R is any relation satisfying these conditions, then it is the image under $\tilde{\Psi}$ of the collection of all two-element sets of the form $\{x, y\}$, where xRy and $x \neq y$. The image of $\tilde{\Phi}$ is the set of all collections of subsets of A such that each collection has at most $|A|$ subsets in it. Since anything in the image of $\tilde{\Phi}$ is a collection of relation classes, and there are at most $|A|$ distinct relation classes, the necessity of this condition is straightforward. Now suppose $\mathcal{D} = \{D_1, \dots, D_m\}$ is a collection of subsets of A , for some $m \leq |A|$. Label the elements of A be $\{x_1, \dots, x_n\}$, where $|A| = n$. Let R be the relation on A given by x_jRx_k iff $x_k \in D_j$, for all $j \in \{1, \dots, m\}$ and all $k \in \{1, \dots, n\}$. Then it is seen that $\mathcal{D} = \tilde{\Phi}(R)$.

Section 6.1 Cardinality of Sets

6.1.4. We give two hints, one to show that $[a, b] \sim (a, b)$, and the other to show that $(a, b) \sim (-\infty, \infty)$; the other parts are similar, and some can be obtained from others by Lemma 6.1.1 (iii). We start by noting that the proof in Example 6.1.2 (3) shows that $[a, b] \sim [-1, 1]$ and that $(a, b) \sim (-1, 1)$. Thus it suffices to prove the result when $a = 1$ and $b = -1$.

Observe that a bijective map $[-1, 1] \rightarrow (-1, 1)$ need not be continuous. Define such a map by sending the points -1 and 1 to somewhere inside $(-1, 1)$, and move everything else to make room, by using an infinite sequence inside $(-1, 1)$. To define a bijective map $(-1, 1) \rightarrow (-\infty, \infty)$, use the function $f(x) = \tan(\pi x/2)$ for all $x \in (-1, 1)$.

6.1.5. There are two cases, when $A \cap B = \emptyset$ and when $A \cap B \neq \emptyset$. In the former case, suppose $|A| = n$ and $|B| = m$; construct a bijective map $f: A \cup B \rightarrow \llbracket 1, n+m \rrbracket$. In the latter case, note that $A \cup B = A \cup (B - A)$; then use the first case, and the fact that $B - A$ is finite by Theorem 6.1.6 (i), which has already been proved.

6.1.6. Suppose that f is injective, but not surjective. Show that $f_*(A) \sim A \sim B$. Note that $f_*(A) \subsetneqq B$. Obtain a contradiction using Theorem 6.1.6. If f is surjective but not injective, then f has a right inverse g that is injective but not surjective. Obtain the same contradiction.

6.1.7. Part (3): Consider the case where C is countably infinite, and A and B are finite.

6.1.13. Assume that A and B are non-empty, or the result is trivial. For each $a \in A$, form the set $B_a = \{(a, b) \mid b \in B\}$. Show that each B_a is countable. Then observe that $A \times B = \bigcup_{a \in A} B_a$.

6.1.14. Use Exercise 6.1.13, Theorem 6.1.8 and Corollary 6.1.7.

6.1.15. Assume $A \times T$ is countable, and use Theorem 6.1.9.

6.1.16. There are two ways to proceed. One is to mimic the proof given for the case that I is countably infinite. This time, apply Exercise 6.3.13 to the function $f: \mathbb{N} \rightarrow \mathbb{N}$ given by $f(n) = (n-1)s$ for all $n \in \mathbb{N}$. Alternately, assume that at least one of the sets A_i is non-empty, since otherwise there is not much to prove. Let $x \in A_j$ for some $j \in \llbracket 1, s \rrbracket$. For all $k \in \mathbb{N}$ with $k > s$, define by $A_k = \{x\}$. Then apply the case of this part of the

lemma that has already been proved to $\bigcup_{i \in \mathbb{N}} A_i$, and compare this union to $\bigcup_{i \in I} A_i$.

6.1.17. Part (1): Since f has a left inverse but no right inverse, then it is injective but not surjective by Theorem 4.4.3. By injectivity, we know that $f^*(\{b\})$ is a single element set if $b \in f_*(A)$; let $f^*(\{b\}) = \{x_b\}$. By non-surjectivity, we know that $B - f_*(A)$ is non-empty. Let L denote the set of all left inverses of f ; we will show that L is infinite.

First, suppose that A is infinite. For each $a \in A$, define the map $g_a: B \rightarrow A$ by

$$g_a(b) = \begin{cases} x_b, & \text{if } b \in f_*(A) \\ a, & \text{if } b \in B - f_*(A). \end{cases}$$

Let $G = \{g_a \mid a \in A\}$. Show that $G \subseteq L$ and that G is infinite (show that $G \sim A$). Use Corollary 6.1.7 to deduce that L is infinite.

Second, suppose that $B - f_*(A)$ is infinite and A has at least 2 elements. Let $y, z \in A$ be distinct elements. For each $c \in B - f_*(A)$, define the map $h_c: B \rightarrow A$ by

$$h_c(b) = \begin{cases} x_b, & \text{if } b \in f_*(A) \\ y, & \text{if } b = c \\ z, & \text{if } b \in B - (f_*(A) \cup \{c\}). \end{cases}$$

Let $H = \{h_c \mid c \in B - f_*(A)\}$. Show that $H \subseteq L$ and that H is infinite. Use Corollary 6.1.7 to deduce that L is infinite.

Part (2): Since k has a right inverse but no left inverse, then it is surjective but not injective by Theorem 4.4.3. By surjectivity, we know that $k^*(\{b\})$ is non-empty for all $b \in B$; choose a fixed element $u_b \in k^*(\{b\})$ for all $b \in B$ (doing so requires the Axiom of Choice). By non-injectivity, we know that at least one of the sets $k^*(\{b\})$ has more than one element. Let R denote the set of all left inverses of k ; we will show that R is infinite.

First, suppose that S is infinite. For each $s \in S$, choose an element $w_s \in k^*(\{s\})$ such that $w_s \neq u_s$, and define the map $j_s: B \rightarrow A$ by

$$j_s(b) = \begin{cases} u_b, & \text{if } b \neq s \\ w_b, & \text{if } b = s. \end{cases}$$

Let $J = \{j_s \mid s \in S\}$. Show that $J \subseteq R$ and that J is infinite. Use Corollary 6.1.7 to deduce that R is infinite.

Second, suppose that $k^*(\{t\})$ is infinite for some $t \in S$. For each $p \in k^*(\{t\})$, define the map $i_p: B \rightarrow A$ by

$$i_p(b) = \begin{cases} u_b, & \text{if } b \neq t \\ p, & \text{if } b = t. \end{cases}$$

Let $I = \{i_p \mid p \in k^*(\{t\})\}$. Show that $I \subseteq R$ and that I is infinite. Use Corollary 6.1.7 to deduce that R is infinite.

Section 6.2 Cardinality of the Number Systems

6.2.1. Part (3): Use Theorem 6.1.9.

Part (4): By Exercise 6.1.4, we know that $[5, 6] \sim (4, 5]$. Now use Exercise 6.1.7, and Exercise 6.1.4 again.

6.2.3. Let $n \in \mathbb{Z}^m$. Let A_n be the set of all roots of polynomials of degree n with rational coefficients. Show that A_n is countable, by constructing a surjective map $\mathbb{Q}^{n+1} \times \{1, \dots, n\} \rightarrow A_n$, and then using Theorems 6.2.1, 6.1.11 and 6.1.9. Observe that the set of algebraic numbers is $\bigcup_{n=0}^{\infty} A_n$.

6.2.4. In Example 6.1.2 (3) we saw that $\mathbb{R} \sim (0, 1)$. Hence it suffices to construct a bijective map $f: (0, 1) \times (0, 1) \rightarrow (0, 1)$. Define this map by expressing elements of $(0, 1)$ as decimals, and map a pair of such decimals to one decimal by interpolating the digits in each decimal.

6.2.6. It is possible to choose a rational number in each element of \mathcal{D} . Then construct an injective map $\mathcal{D} \rightarrow \mathbb{Q}$. Next, construct an injective map $\mathcal{D} \rightarrow \mathbb{N}$. Then use Theorem 6.1.9.

6.2.7. Use Proposition 4.5.3 to show that $\mathcal{F}(\mathbb{N}, \{0, 1\}) \sim \mathcal{P}(\mathbb{N})$, and then use Corollary 6.1.14. Next, note that $\mathcal{F}(\mathbb{N}, \{0, 1\}) \subseteq \mathcal{F}(\mathbb{N}, \mathbb{N})$, and use Theorem 6.1.9.

6.2.8. Part (1): If $x \in (0, 1)$, let $x = 0.c_1 c_2 c_3 \dots$ be the unique binary expansion, and then define $f(x) = \{n \in \mathbb{N} \mid c_n = 1\}$. Note that this map is well-defined and injective, but not surjective.

Part (2): If $B \in \mathcal{P}(\mathbb{N})$, let $g(B) = 0.c_1 c_2 c_3 \dots$, where

$$c_n = \begin{cases} 2, & \text{if } n \in B \\ 3, & \text{if } n \notin B \end{cases}$$

for each $n \in \mathbb{N}$. Note that this map is well-defined and injective, though not surjective.

Section 6.3 Mathematical Induction

6.3.4. The statement that we are trying to prove for each $n \in \mathbb{N}$ is well-defined, and is not flawed. The flaw is in the inductive step, which breaks down for a particular value of n .

6.3.13. Note first that the hypotheses on f imply that f is injective, and that if $n \leq m$ then $f(n) \leq f(m)$ for any $n, m \in \mathbb{N}$. To prove uniqueness, suppose there are $n, m, p, q \in \mathbb{N}$ such that $f(n) < x \leq f(n+1)$ and $x = f(n) + p$, and that $f(m) < x \leq f(m+1)$ and $x = f(m) + q$. If $n = m$, it is simple to see that $p = q$. If $n \neq m$, then without loss of generality, assume that $n < m$. Then $n+1 \leq m$, and so $f(n+1) \leq f(m)$. Obtain a contradiction. To prove existence, proceed by induction on x .

Section 6.4 Recursion

6.4.10. Let $Z_n = \phi^n + \phi'^n$ for all $n \in \mathbb{N}$. Show that Z_1 and Z_2 are integers by computing them directly from the definition. Next, show that $Z_{n+2} = Z_{n+1} + Z_n$ for all $n \in \mathbb{N}$. It will then follow that all the Z_n are integers.

6.4.7. Use Binet's formula (Corollary 6.4.8) and Exercise 6.4.10.

6.4.8. Part (1): Proceed by induction on n , where the statement being proved is that the result holds for that n and all k .

Part (2): Proceed by induction on k , where the statement being proved is that the result holds for that k and all n .

6.4.11. Proceed as in the proof of part (i) of the proposition, but make use of the fact that if $x^2 - ax - b = 0$ only has one real solution r , then $a^2 + 4b = 0$ and $r = \frac{a}{2}$.

6.4.12. Part (1): Compute the slopes of the edges of the various pieces.

Part (2): The difference between the area of the square and the rectangle is $a^2 - ab - b^2$. To ensure zero overlap, we need to have $a^2 - ab - b^2 = 0$. Now divide this equation by b^2 .

Part (3): Suppose that $b = F_{n-1}$ and $a = F_n$ for some $n \in \mathbb{N}$ with $n \geq 2$. Then use the hint for part (2) of this exercise together with Proposition 6.4.6 (iii).

6.4.13. For the second part of the result, assume the limit exists. Suppose that the limit equals L . Show that L satisfies the polynomial $x^2 - x - 1$, of which only ϕ and ϕ' are the roots. Observe that L must be non-negative, since all the F_n are positive.

Showing the first part of the result, namely that the limit exists, is trickier. The strategy is to show that the sequence $F_2/F_1, F_3/F_2, \dots$ is a Cauchy sequence, and then use the completeness of the real numbers to deduce that the sequence has a limit. To show that the sequence is Cauchy, let $n, k \in \mathbb{N}$, and observe that

$$\frac{F_{n+k+1}}{F_{n+k}} - \frac{F_{n+1}}{F_n} = \left(\frac{F_{n+k+1}}{F_{n+k}} - \frac{F_{n+k}}{F_{n+k-1}} \right) + \dots + \left(\frac{F_{n+2}}{F_{n+1}} - \frac{F_{n+1}}{F_n} \right).$$

Now use Lemma 6.4.6 (iii) to compute the value of each of the terms in parentheses, and then use the Alternating Series Theorem (see for example [Pow94, Section 2.9]) to estimate the sum in the above equation, and to show that the sum can be made as small as desired for large enough n .

6.4.14. Part (1)(iv): As with parts (i) – (iii) of part (1) of the problem, the proof is by induction. First, however, use induction to prove the auxiliary fact that $R_n + 2(n+1)^2 = 3n^2 + 5n + 2$ for all $n \in \mathbb{N}$.

6.4.15. Each of the two parts is proved by induction on n . They are both trivial when $n = 0$. Assume that they both hold for some $n \in \mathbb{Z}^{nn}$, and then show that each part holds for $n+1$.

Part (1): Let $(a, b) \in \mathbb{L}$ be such that $1 \leq a, b \leq n+1$. Since a and b are relatively prime, they are not equal. Suppose first that $a > b$. Observe that $(a-b, b) \in \mathbb{L}$ by Exercise 2.4.3. Apply the inductive hypothesis to $(a-b, b)$, and note that $(a, b) = U((a-b, b))$. A similar argument works when $a < b$.

Part (2): Let $i, j, x, y \in \mathbb{Z}^{nn}$ be such that $0 \leq i, j \leq n+1$, that $1 \leq x \leq 2^i$ and that $1 \leq y \leq 2^j$. Clearly, if $i = j$ and $x = y$, then $a(i)^x = a(j)^y$. Now suppose that $a(i)^x = a(j)^y$. First, use Exercise 4.4.8 (1) to show that $a(i)^x = (1, 1)$ iff $i = 0$ and $x = 1$. It follows that if $a(i)^x = (1, 1) = a(j)^y$, then $i = 0 = j$ and $x = 1 = y$. Now suppose that $a(i)^x \neq (1, 1) \neq a(j)^y$. Then $i \neq 0$ and $j \neq 0$. Then $a(i)^x = U(a(i-1)^w)$ or $a(i)^x = D(a(i-1)^w)$, and $a(j)^y = U(a(j-1)^z)$ or $a(j)^y = D(a(j-1)^z)$, for some $w, z \in \mathbb{Z}^{nn}$ such that $1 \leq w \leq 2^{i-1}$ and that $1 \leq z \leq 2^{j-1}$. Now use the inductive hypothesis and Exercise 4.4.8 (3), (4) to show that $i = j$ and $x = y$.

Section 7.1 Binary Operations

7.1.1. Part (1): The formula does not define a binary operation on the set $\{-1, -2, -3, \dots\}$. For example, we see that $(-1) * (-2) = (-1)(-2) = 2$, which is not in the given set.

7.1.2. Part (3): The binary operation \otimes is associative and commutative, has an identity element, and all elements have inverses. For example, the identity element is 7, because $x \otimes 7 = x + 7 - 7 = x$ and $7 \otimes x = 7 + x - 7 = x$ for all $x \in \mathbb{R}$. Show the other properties.

7.1.4. To show that (3) \Rightarrow (1), assume that there exist $p, q \in \mathbb{Z}$ such that $ap + nq = 1$. Then $ap - 1 = (-q)n$, and so $ap \equiv 1 \pmod{n}$. Thus $[a] \cdot [p] = [1]$. Hence $[a]$ has an inverse with respect to multiplication.

7.1.5. A counterexample can be found using the set $A = \{a, b\}$. Define a map $\star: A \times A \times A \rightarrow A$ by $\star((a, a, a)) = b$, and $\star((a, a, b)) = b$, and $\star((b, b, b)) = a$ and arbitrarily for the other elements of $A \times A \times A$. Show that \star is not left-induced by a binary operation (assume otherwise and arrive at a contradiction).

Section 7.2 Groups

7.2.4. Look at Example 7.2.1 (4).

7.2.5. An example can be found with four elements; make sure it does not have an identity.

7.2.8. First show that Theorem 7.2.3 (i) still holds in the present situation. Next, let $a \in A$, and suppose $b \in A$ is such that $a * b = e$. Show that $b * a = e$, and it will follow that the inverses law holds. Look at $(b * a) * b$, and then use the associative law, the right inverses law, the identity law and Theorem 7.2.3 (i).

7.2.12. Part (3): Use Exercise 7.1.4.

7.2.13. For the first part, let $a, b \in G$. Note that $(ab)' = ab$, and thus $abab = e$. Now use the fact that $a' = a$ and $b' = b$. For the second part, look at Example 7.2.1 (4).

Section 7.3 Homomorphisms and Isomorphisms

7.3.1. Part (3): The map m is not a homomorphism, because $m(x + y) = (x + y) + 3 \neq (x + 3) + (y + 3) = m(x) + m(y)$, for any $x, y \in \mathbb{R}$.

7.3.3. (1) Do not forget to check whether the map is well-defined.

7.3.9. Assume there is an isomorphism $f: Q \rightarrow V$. Then $f(1) = e$ by Theorem 7.3.2 (i). Show that $f(x) \neq a$ and $f(x) \neq c$, by looking at $f(x \circ x)$. Deduce that $f(x) = b$. Use the same argument to show that $f(y) = b$, a contradiction.

7.3.10. Let $W = \{l, m, n, p\}$. Construct all possible binary operations \oplus on W that make (W, \oplus) a group by making operation tables for \oplus . Without loss of generality, let l be the identity element; that assumption fixes seven of the entries of any possible operation table. We can further reduce the possible cases by using the fact that each element of W appears once in each row and once in each column (as remarked after Theorem 7.2.3). By checking the operation tables that you obtain, observe that in each operation table that makes (W, \oplus) a group, either all four elements act as their own inverses, or precisely two of them do. Whenever the former case occurs, show that (W, \oplus) is isomorphic to (V, \star) ; whenever the latter case occurs, show that (W, \oplus) is isomorphic to (Q, \circ) .

Section 7.4 Partially Ordered Sets

7.4.2. Part (1): There cannot be any $x, y \in F$ such that x and y each eats more cheese annually than the other. That is, it can never happen that $xM y$ and $yM x$ for any $x, y \in F$. Hence M trivially satisfies the definition of antisymmetry. The relation M is not a partial ordering, because it is not reflexive, and hence it is also not a total ordering.

7.4.8. Part (3): You need to show that if $[x] = [a]$ and $[y] = [b]$, then $[x]S[y]$ iff $[a]S[b]$, which would be true if xRy iff aRb . Use part (2) of the problem.

7.4.10. Part (2): Suppose that $x, y \in A$ and that $f(x) = f(y)$. Then $f(x) \subseteq f(y)$ and $f(y) \subseteq f(x)$. Now use part (1) of this problem and the antisymmetry of \preccurlyeq to conclude that $x = y$.

7.4.14. Note that $1 \in \mathbb{N}$ has the property that $1 \leq n$ for all $n \in \mathbb{N}$. Suppose there were an order isomorphism $f: \mathbb{N} \rightarrow \mathbb{N}^-$. What can you say about the behavior of $f(1)$?

Section 7.5 Lattices

7.5.5. Prove the following more general statement by induction on n : For each $n \in \mathbb{N}$ such that $n \geq 2$, every subset X of a lattice, with $|X| = n$, has a least upper bound and a greatest lower bound.

7.5.6. Suppose that $a \wedge b = a \vee b$. Then $a = a \vee (a \wedge b) = a \vee (a \vee b) = \dots$

7.5.7. Part (1): We know that $(a \wedge b) \preccurlyeq a$, and that $(a \wedge b) \preccurlyeq b \preccurlyeq (b \vee c)$. It follows that $(a \wedge b) \preccurlyeq a \wedge (b \vee c)$. A similar inequality holds for $a \wedge c$.

Part (2): This is similar to part (1).

Parts (3) and (4): These follow from parts (1) and (2), using Theorem 7.5.2 (vi).

7.5.8. Suppose that $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in A$. Let $a, b, c \in A$. Then using our hypothesis and Theorem 7.5.2 we have $(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = (a \wedge (a \vee b)) \vee (c \wedge (a \vee b)) = \dots$

7.5.9. Using the hypothesis and various parts of Theorem 7.5.2 we have $a = a \wedge (a \vee c) = a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) = \dots$

7.5.10. Look at the lattices given by the Hasse diagrams in Figure 7.5.3.

7.5.14. Part(ii): Suppose f is a meet homomorphism; the other case is similar. Let $x, y \in M$. Since f is bijective, then $x = f(a)$ and $y = f(b)$ for unique $a, b \in L$. Then $f^{-1}(x \wedge' y) = f^{-1}(f(a) \wedge' f(b)) = f^{-1}(f(a \wedge b)) = \dots$, using the hypothesis on f .

Part(iii) Suppose f is an order isomorphism. We will show that f is a meet homomorphism; to show that f is a join homomorphism is similar. Let $x, y \in L$. Let $w = x \wedge y$, and let $p = f(x) \wedge' f(y)$. Show that $f(w) = p$, by showing that $f(w) \preccurlyeq p$ and that $p \preccurlyeq f(w)$. For the former, note that $w \preccurlyeq x$ and $w \preccurlyeq y$; and then use the fact that f is an order homomorphism, and the fact that p is the greatest lower bound for $f(x)$ and $f(y)$. The other inequality you need to prove is similar, and uses the fact that f^{-1} is an order homomorphism (don't forget that f is bijective). Now suppose that f is a bijective meet homomorphism. By part

(i) of this theorem f is an order homomorphism. Then use parts (ii) and (i) of this theorem to deduce that f^{-1} is an order homomorphism. Hence f is an order isomorphism. The remaining cases are similar.

Section 7.6 Products and Sums

7.6.2. By the product rule, the number of possible initials with only first and last names is $26 \times 26 = 676$, which is less than 1000. The number of possible initials using middle names is $26 \times 26 \times 26 = 17576$, which is larger than 1000.

7.6.5. Suppose $|A| = n$ and $|B| = p$. For the case $n = 1$, show that there is a bijective map $A \times B \rightarrow B$. Now suppose that the result holds for n , and prove it for $n + 1$. Thus, suppose that $|A| = n + 1$. Let $a \in A$, and let $A' = A - \{a\}$. Show that there is a bijective map $(A' \times B) \cup (\{a\} \times B) \rightarrow A \times B$. Then apply Theorem 7.6.5 (ii).

7.6.7. Use Theorems 6.1.6 (ii) and 7.6.7 (iv).

7.6.9. Let X be the set of rabbits in the study and let C , L and B be the sets of those rabbits that like carrots, lettuce and bratwurst respectively. We are given that $|X| = 50$, that $|C| = 29$, that $|L| = 18$, that $|B| = 27$, that $|C \cap L| = 9$, that $|C \cap B| = 16$, that $|L \cap B| = 8$ and that $|C \cup L \cup B| = 47$. Part (1): The number of rabbits that liked none of the three foods is $|X - (C \cup L \cup B)|$, which equals $|X| - |C \cup L \cup B|$ by Theorem 6.1.6 (ii).

Part (2): The number of rabbits that liked all three of the foods is $|C \cap L \cap B|$. Use Corollary 7.6.8, together with part (1) of this problem, and solve for the desired number.

Section 7.7 Permutations and Combinations

7.7.5. Part (1): The number of possible outcomes is $\frac{8!}{(8-3)!} = 336$.

Part (2): Using part (1) of this problem, the number of possible outcomes is $336^2 = 112,896$.

7.7.10. Part (2): The number of choices is $\binom{6}{3}\binom{4}{2} = 20 \cdot 6 = 120$.

7.7.16. Part (1): Use the Binomial Theorem (Theorem 7.7.9) with appropriate choices of x and y .

Parts (2) and (3): Use induction on n .

7.7.17. Part (1): Use Exercise 7.7.16 (1).

Part (2): Use part (1). When $|A|$ is odd, then it is also possible to find a simple bijective map $\mathcal{P}_E(A) \rightarrow \mathcal{P}_O(A)$.

7.7.18. Part (1): The sum of the entries along a diagonal has the form $\sum_{k=0}^n \binom{n-k}{k}$.

Part (2): Let A_n denote the sum mentioned in the hint for part (1). Prove that $A_{n+2} = A_{n+1} + A_n$ for all $n \in \mathbb{Z}^{nn}$, by using induction on n and Proposition 7.7.8 (iii). Calculate A_0 and A_1 . Conclude that $A_n = F_{n+1}$ for all $n \in \mathbb{Z}^{nn}$.

7.7.20. For the inductive step, choose some $a \in A$. Then $\mathcal{P}(A)$ is the union of two collections of subsets, namely those that contain a and those that do not.

7.7.22. We prove the result by induction on n . The cases $n = 0$ and $n = 1$, and all possible k , are straightforward. Assume that the result holds for some n , and for all k such that $0 \leq k \leq n$. Let A be a set such that $|A| = n + 1$. By Exercise 7.7.23 we know that the choice of set A makes no difference. Examine the case $k = n + 1$ separately. Now assume that $0 \leq k \leq n$. Choose an element $x \in A$. Write $\mathcal{P}_k(A) = W_x \cup N_x$, where

$$W_x = \{S \in \mathcal{P}(A) \mid |S| = k \text{ and } x \in S\},$$

$$N_x = \{S \in \mathcal{P}(A) \mid |S| = k \text{ and } x \notin S\}.$$

Show that $N_x = \mathcal{P}_k(A - \{x\})$, and apply the inductive hypothesis to find $|N_x|$. Show that there is a bijective map between W_x and $\mathcal{P}_{k-1}(A - \{x\})$. Apply the inductive hypothesis to find that $|W_x|$. Apply Theorem 7.6.5 (ii) to $\mathcal{P}_k(A)$ to complete the proof.

7.7.24. There are $|A|^{|B - f_*(A)|}$ left inverses, which you prove by using Theorem 7.7.1 (i), and the fact that if $g: B \rightarrow A$ is a left inverse of f , then g restricted to $f_*(A)$ is uniquely determined.

Section 8.2 The Natural Numbers

8.2.1. Define $k: H \times H \rightarrow H \times H$ by $k((x, y)) = (y, p(x, y))$ for all $(x, y) \in H \times H$. Apply Theorem 8.2.1 to the Henkin set $(H \times H, (a, b), k)$. The resulting map has two components; one of them will work as g .

8.2.2. Define $r: H \times N \rightarrow H \times N$ by $r((x, m)) = (q(x, m), s(m))$ for all $(x, m) \in H \times N$. Apply Theorem 8.2.1 to the Henkin set $(H \times N, (e, 1), r)$. The resulting map has two components, say j_1 and j_2 . First use the uniqueness part of Theorem 8.2.1 to show that $j_2 = 1_N$. Then show that $h = j_1$ works as desired.

8.2.5. Part (vii): Use proof by contradiction. Suppose that $a \cdot b = 1$, and that at least one of a or b is not 1. Without loss of generality, assume that $b \neq 1$. Then use Lemma 8.2.2 and Theorems 8.2.5 (ii) and 8.2.4 (v) to derive a contradiction.

8.2.6. Part (vi): First, suppose that $s(a) \leq b$. There are two cases, namely $s(a) < b$ or $s(a) = b$. Use parts (i) and (iii) of this theorem. Next, suppose that $a < b$. First show that $b \neq 1$, by assuming to the contrary that $b = 1$, and deriving a contradiction (use the definition of $<$ applied to $a < 1$, and Theorem 8.2.4 (v)). Then apply Lemma 8.2.2 to b , and use parts (iv) and (v) of this theorem.

Section 8.3 Further Properties of the Natural Numbers

8.3.4. Since $(N, 1, s)$ and $(N', 1', s')$ are both Peano systems, everything we have proved so far about Peano systems applies to both sets. By Theorem 8.2.1 there is a unique map $f: N \rightarrow N'$ such that $f(1) = 1'$ and $f \circ s = s' \circ f$, and there is a unique map $\hat{f}: N' \rightarrow N$ such that $\hat{f}(1') = 1$ and $\hat{f} \circ s' = s \circ \hat{f}$. Show that f is bijective by showing that f and \hat{f} are inverses. First, note that $\hat{f} \circ f: N \rightarrow N$ is a map such that $\hat{f} \circ f(1) = 1$ and $(\hat{f} \circ f) \circ s = s \circ (\hat{f} \circ f)$. Then observe that the identity map $1_N: N \rightarrow N$ satisfies these same two properties as $\hat{f} \circ f$. Use the uniqueness in Theorem 8.2.1 to deduce that $\hat{f} \circ f = 1_N$. Similarly, show that $f \circ \hat{f} = 1_{N'}$.

Now prove parts (a) – (c) of part (ii) in order. The first two parts use proofs by induction on a ; the third uses part (a).

8.3.5. First, use Theorem 8.3.1 (iv) to deduce that $\llbracket 1, n+1 \rrbracket - \llbracket 1, n \rrbracket = \{n+1\}$. Next, let $G \subseteq N$ be the set of all values of n for which the result holds; show that $G = N$ by the usual method.

8.3.6. There is a bijective map $g: \llbracket 1, n \rrbracket \rightarrow F$ for some $n \in \mathbb{N}$. Let $j: F \rightarrow \mathbb{N}$ be the inclusion map. Apply Exercise 8.3.5 to the map $j \circ g$.

8.3.7. Same hint as for Exercise 8.3.5.

8.3.8. Use Theorem 8.3.1 (iv) to deduce that $\llbracket 1, n+1 \rrbracket - \llbracket 1, n \rrbracket = \{n+1\}$. Now prove the result by induction on n .

Part (1): If $f: \llbracket 1, m \rrbracket \rightarrow \llbracket 1, n+1 \rrbracket$ is bijective, and if $f(m) \neq n+1$, then prior to using the inductive step, define a new bijective map $f': \llbracket 1, m \rrbracket \rightarrow \llbracket 1, n+1 \rrbracket$ such that $f'(m) = n$.

Part (2): If $g: \llbracket 1, m \rrbracket \rightarrow \llbracket 1, n+1 \rrbracket$ is injective but not bijective, then it is not surjective. If $n+1$ is in the image of g , then define g' as above. If $n+1$ is not in the image of g , then there is no need to modify g .

Part (3): This part follows from Parts (1) and (2).

8.3.9. Use induction on p .

Section 8.4 The Integers

8.4.2. To show that \cdot is well-defined, assume $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$. It follows that $a + b' = b + a'$ and $c + d' = d + c'$. Multiply the first of these equations by each of c, d, c', d' , and multiply the second equation by each of a, b, a', b' . Add the eight resulting equations (arranged appropriately), cancel, and use Exercise 8.2.8.

8.4.5. Part (viii): There are a number of cases, depending upon whether $x = \hat{0}$ or $x = \hat{1}$ or $x > \hat{1}$, etc., and similarly for y .

8.4.8. Use Lemma 8.4.3 and Theorem 8.3.2.

8.4.11. Use Exercise 8.4.10, and various results from Section 8.4.

8.4.14. Suppose that $\hat{2} \cdot x = \hat{1}$. Use Theorem 8.4.6 and Exercise 8.4.9 to show that $\hat{2} \neq \hat{1}$ and $\hat{2} \neq -\hat{1}$. Then use Theorem 8.4.5 (viii) to reach a contradiction.

8.4.15. To show that x is either even or odd, use the Division Algorithm (Theorem 8.4.9). To show that x is not both even and odd, assume otherwise, and use Exercise 8.4.14.

8.4.16. Use the Division Algorithm (Theorem 8.4.9), and note that if $z \in \mathbb{Z}$ is such that $\hat{0} \leq z < \hat{3}$, then z is one of $\hat{0}, \hat{1}$ or $\hat{2}$. You may use the fact that neither $\hat{1}$ nor $\hat{2}$ can be written in the form $\hat{3} \cdot x$ for any $x \in \mathbb{Z}$, which can be proved similarly to Exercise 8.4.14.

Section 8.5 The Rational Numbers

8.5.3. For part (i) of the lemma, we have $[(x, y)] = \bar{0}$ iff $[(x, y)] = [(\hat{0}, \hat{1})]$ iff $x \cdot \hat{1} = y \cdot \hat{0}$, by the definition of \asymp . Now use Theorem 8.4.5 (iii), (iv).

8.5.5. For part (iv) of the theorem, suppose that $r = [(x, y)]$ and $s = [(z, w)]$ for some $x, z \in Z$ and $y, w \in Z^+$. Then $r \cdot s = [(x, y)] \cdot [(z, w)] = [(x \cdot z, y \cdot w)]$. Hence $r \cdot s = \bar{0}$ iff $[(x \cdot z, y \cdot w)] = \bar{0}$, and the latter is true iff $x \cdot z = \hat{0}$ by Lemma 8.5.3 (i). Now use Theorem 8.4.5 (iv), and Lemma 8.5.3 (i) again.

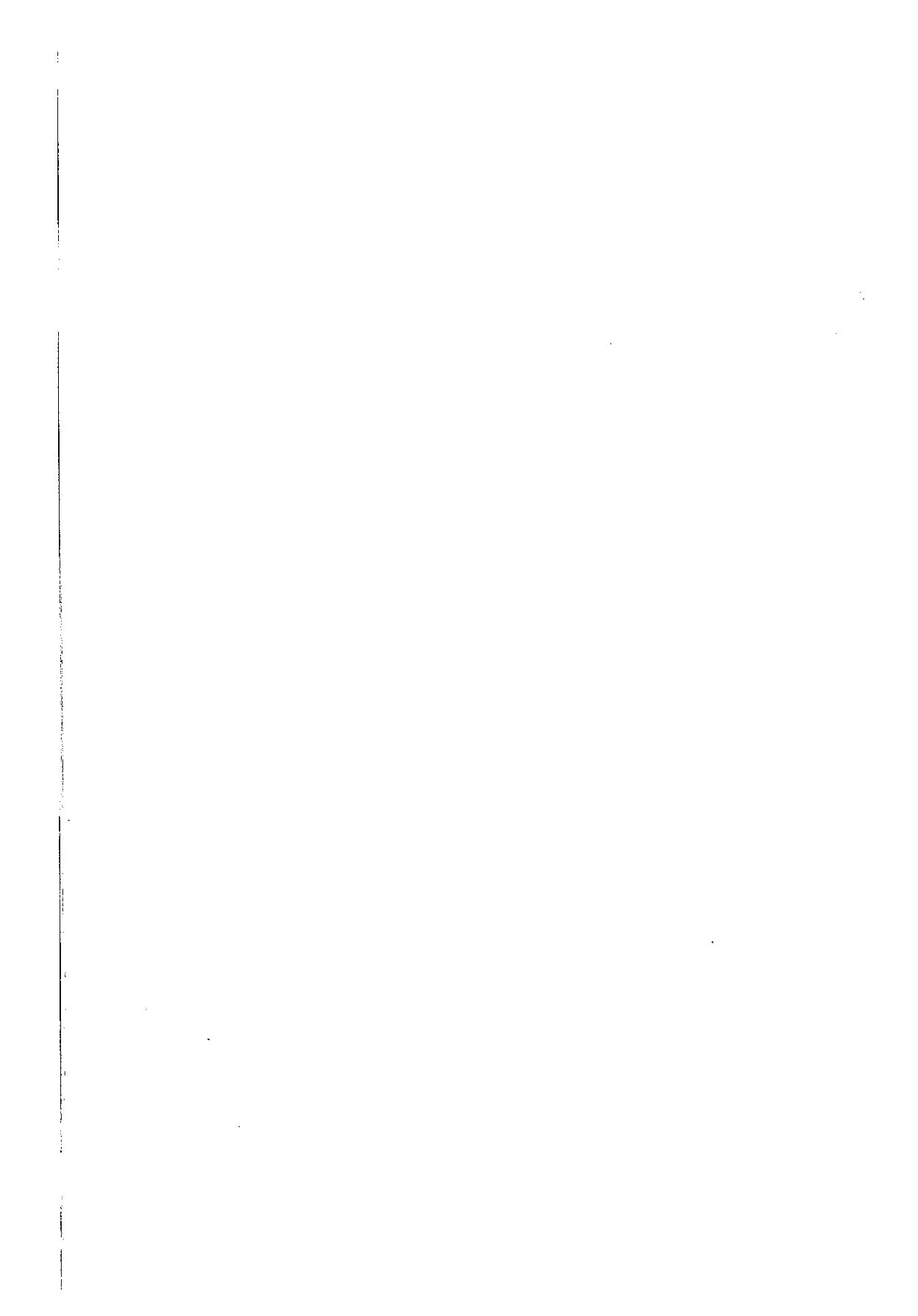
8.5.6. For part (iii) of the theorem, suppose that $r = [(x, y)]$, that $s = [(z, w)]$ and that $t = [(u, v)]$ for some $x, z, u \in Z$ and $y, w, v \in Z^+$. Assume that $r < s$ and $s < t$. Then $[(x, y)] < [(z, w)]$ and $[(z, w)] < [(u, v)]$. The first inequality implies that $\hat{0} < (z \cdot y) - (x \cdot w)$ when $\hat{0} < y$ and $\hat{0} < w$ or when $\hat{0} > y$ and $\hat{0} > w$, or that $\hat{0} > (z \cdot y) - (x \cdot w)$ when $\hat{0} < y$ and $\hat{0} > w$ or when $\hat{0} > y$ and $\hat{0} < w$; the second inequality implies that $\hat{0} < (u \cdot w) - (z \cdot v)$ when $\hat{0} < w$ and $\hat{0} < v$ or when $\hat{0} > w$ and $\hat{0} > v$, or that $\hat{0} > (z \cdot y) - (x \cdot w)$ when $\hat{0} < w$ and $\hat{0} > v$ or when $\hat{0} > w$ and $\hat{0} < v$. There are now four cases, resulting from combining each of the two cases from the two inequalities; we look at one of the four cases, where $\hat{0} < (z \cdot y) - (x \cdot w)$; where either $\hat{0} < y$ and $\hat{0} < w$, or $\hat{0} > y$ and $\hat{0} > w$; where $\hat{0} < (u \cdot w) - (z \cdot v)$; and where either $\hat{0} < w$ and $\hat{0} < v$, or $\hat{0} > w$ and $\hat{0} > v$. It follows that $x \cdot w < z \cdot y$ and that $z \cdot v < u \cdot w$. We now have two subcases: (a) $\hat{0} < y$ and $\hat{0} < w$ and $\hat{0} < v$, or (b) $\hat{0} > y$ and $\hat{0} > w$ and $\hat{0} > v$. In subcase (a), using Theorem 8.4.6 (viii) and some other properties of the integers, we deduce that $x \cdot v \cdot w < z \cdot y \cdot v$ and that $z \cdot y \cdot v < u \cdot y \cdot w$. Hence $x \cdot v \cdot w < u \cdot y \cdot w$, and thus $x \cdot v < u \cdot y$, and therefore $\hat{0} < (u \cdot y) - (x \cdot v)$. Since $\hat{0} < y$ and $\hat{0} < v$, it follows that $[(x, y)] < [(u, v)]$. Subcase (b) is similar, as are the other three cases.

8.5.9. Consider the set $S \subset Q$ defined by $S = \{[(1, x)] \mid x \in Z^+\}$.

Section 8.6 Real Numbers and Complex Numbers

8.6.1. Use various parts of Theorems 8.6.1 – 8.6.3; there are three cases, depending upon whether $x > 0$, or $x = 0$, or $x < 0$.

8.6.4. For part (ii) of the theorem, suppose that $\alpha = (a, b)$ and $\beta = (c, d)$ for some $a, b, c, d \in \mathbb{R}$. Then $\alpha \cdot \beta = (a, b) \cdot (c, d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c) = (c \cdot a - d \cdot b, c \cdot b + d \cdot a) = (c, d) \cdot (a, b) = \beta \cdot \alpha$.



References

- [Alp99] Roger C. Alperin, Rationals and the modular group, *Amer. Math. Monthly* **106** (1999), 771–773.
- [AM75] Michael Arbib and Ernst Manes, *Arrows, Structures and Functions: The Categorical Imperative*, Academic Press, New York, 1975.
- [Ang94] W. S. Anglin, *Mathematics: A Concise History and Philosophy*, Springer-Verlag, New York, 1994.
- [AR89] R. B. J. T. Allenby and E. J. Redfern, *Introduction to Number Theory with Computing*, Edward Arnold, London, 1989.
- [AR94] Howard Anton and Chris Rorres, *Elementary Linear Algebra, Applications Version*, Seventh ed., John Wiley & Sons, New York, 1994.
- [Arm88] M. A. Armstrong, *Groups and Symmetry*, Springer-Verlag, New York, 1988.
- [ASY97] Kathleen Alligood, Tim Sauer, and James Yorke, *Chaos: An Introduction to Dynamical Systems*, Springer-Verlag, New York, 1997.

- [Ave90] Carol Avelsgaard, *Foundations for Advanced Mathematics*, Scott, Foresman, Glenview, IL, 1990.
- [BG95] Hans Bandemer and Siegfried Gottwald, *Fuzzy Sets, Fuzzy Logic, Fuzzy Methods*, Seventh ed., John Wiley & Sons, Chichester, 1995.
- [Bir48] Garrett Birkhoff, *Lattice Theory*, AMS Colloquium Publications, vol. 25, American Mathematical Society, New York, 1948.
- [Blo87] Norman J. Bloch, *Abstract Algebra with Applications*, Prentice-Hall, Englewood Cliffs, NJ, 1987.
- [Bog90] Kenneth Bogart, *Introductory Combinatorics*, Second ed., Harcourt, Brace, Jovanovich, San Diego, 1990.
- [Boy91] Carl Boyer, *A history of mathematics*, second ed., John Wiley & Sons, New York, 1991.
- [BR87] Douglas Bridges and Fred Richman, *Varieties of Constructive Mathematics*, London Mathematical Society Lecture Notes Series, vol. 97, Cambridge Univ. Press, Cambridge, 1987.
- [BS82] Robert G. Bartle and Donald R. Sherbert, *Introduction to Real Analysis*, John Wiley & Sons, New York, 1982.
- [Bur85] R. P. Burns, *Groups: A Path to Geometry*, Cambridge Univ. Press, Cambridge, 1985.
- [CD73] Peter Crawley and Robert Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall, Englewood Cliffs, NJ, 1973.
- [CE63] Leon Cohen and Gertrude Ehrlich, *The Structure of the Real Number System*, Van Nostrand, Princeton, NJ, 1963.
- [Cop68] Irving Copi, *Introduction to Logic*, Third ed., Macmillan, New York, 1968.
- [Cox61] H. S. M. Coxeter, *Introduction to Geometry*, John Wiley & Sons, New York, 1961.
- [Dea66] Richard Dean, *Elements of Abstract Algebra*, John Wiley & Sons, New York, 1966.

- [Deb86] 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*, Second ed., Springer-Verlag, New York, 1993.
- [DHM95] Phillip Davis, Reuben Hersh, and E. A. Marchisotto, *The Mathematical Experience*, Birkhäuser, Boston, 1995.
- [Die92] Jean Dieudonné, *Mathematics – the Music of Reason*, Springer-Verlag, Berlin, 1992.
- [DSW94] Martin Davis, Ron Sigal, and Elaine Weyuker, *Computability, Complexity, and Languages*, Second ed., Academic Press, San Diego, 1994.
- [Dub64] Roy Dubisch, *Lattices to Logic*, Blaisdell, New York, 1964.
- [EC89] Richard Epstein and Walter Carnielli, *Computability: Computable Functions, Logic, and the Foundations of Mathematics*, Wadsworth & Brooks/Cole, Pacific Grove, CA, 1989.
- [Eea90] H.-D. Ebbinghaus et al., *Numbers*, Springer-Verlag, New York, 1990.
- [EFT94] H.-D. Ebbinghaus, J. Flum, and W. Thomas, *Mathematical Logic*, Second ed., Springer-Verlag, New York, 1994.
- [End72] Herbert Enderton, *A mathematical introduction to logic*, Academic Press, Boston, 1972.
- [Epp90] Susanna Epp, *Discrete Mathematics with Applications*, Wadsworth, Belmont, CA, 1990.
- [Fab92] Eugene D. Fabricus, *Modern Digital Design and Switching Theory*, CRC Press, Boca Raton, FL, 1992.
- [Fef64] Solomon Feferman, *The Number Systems: Foundations of Algebra and Analysis*, Addison-Wesley, Reading, MA, 1964.
- [Fle83] Graham Flegg, *Numbers*, Andre Deutsch, London, 1983.

- [FP92] Peter Fletcher and C. Wayne Patty, *Foundations of Higher Mathematics*, PWS-Kent, Boston, 1992.
- [FR90] Daniel Fendel and Diane Resek, *Foundations of Higher Mathematics*, Addison-Wesley, Reading, MA, 1990.
- [FR97] Benjamin Fine and Gerhard Rosenberger, *The Fundamental Theorem of Algebra*, Springer-Verlag, New York, 1997.
- [Fra94] John Fraleigh, *A First Course in Abstract Algebra*, Fifth ed., Addison-Wesley, Reading, MA, 1994.
- [Gal74] Galileo Galilei, *Two New Sciences*, University of Wisconsin Press, Madison, WI, 1974.
- [Gar87] Trudi Garland, *Fascinating Fibonacci*, 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*, Second ed., PWS-Kent, Boston, 1988.
- [GG94] I. Grattan-Guinness (ed.), *Companion Encyclopedia of the History and Philosophy of the Mathematical Sciences*, vol. 1, Routledge, London, 1994.
- [Gil87] Leonard Gillman, *Writing Mathematics Well*, Mathematical Association of America, Washington, DC, 1987.
- [GKP94] Ronald Graham, Donald Knuth, and Oren Patashnik, *Concrete Mathematics*, Second ed., Addison-Wesley, Reading, MA, 1994.
- [Hal60] Paul Halmos, *Naive Set Theory*, Van Nostrand, Princeton, NJ, 1960.
- [Ham82] A. G. Hamilton, *Numbers, Sets and Axioms*, Cambridge Univ. 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.
- [Her75] I. N. Herstein, *Topics in Algebra*, Second ed., John Wiley & Sons, New York, 1975.
- [Her97] Reuben Hersh, *What is Mathematics, Really?*, Oxford Univ. Press, New York, 1997.
- [HHP97] Peter Hilton, Derek Holton, and Jean Pedersen, *Mathematical Reflections*, Springer-Verlag, New York, 1997.
- [Hil90] David Hilbert, Über die Theorie der algebraischen Formen, *Math. Ann.* **36** (1890), 473–534.
- [Hos90] R. F. Hoskins, *Standard and Non-Standard Analysis*, Ellis Horwood, New York, 1990.
- [Hun70] H. E. Huntley, *The Divine Proportion*, Dover, New York, 1970.
- [HW91] John H. Hubbard and Beverly H. West, *Differential equations: A dynamical systems approach*, Part I: Ordinary Differential Equations, Springer-Verlag, New York, 1991.
- [Ifr85] Georges Ifrah, *From One to Zero: A Universal History of Numbers*, Viking, New York, 1985.
- [KLR89] Donald Knuth, Tracy Larrabee, and Paul Roberts, *Mathematical Writing*, Mathematical Association of America, Washington, DC, 1989.
- [KMM80] Donald Kalish, Richard Montague, and Gary Mar, *Logic: Techniques of Formal Reasoning*, Second ed., Harcourt, Brace, Jovanovich, New York, 1980.
- [Knu73] Donald E. Knuth, *The Art of Computer Programming, Volume 1: Fundamental Algorithms*, Second ed., Addison-Wesley, Reading, MA, 1973.
- [Kob87] Neal Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 1987.
- [KR83a] K. H. Kim and F. W. Roush, *Competitive Economics: Equilibrium and Arbitration*, North-Holland, Amsterdam, 1983.

- [KR83b] Ki Hang Kim and Fred Roush, *Applied Abstract Algebra*, Ellis Horwood, Chichester, 1983.
- [Kri81] V. Sankrithi Krishnan, *An Introduction to Category Theory*, North-Holland, New York, 1981.
- [Loo40] Elisha Loomis, *The Pythagorean Proposition*, Edwards Brothers, Ann Arbor, 1940.
- [LP98] Rudolf Lidl and Günter Pilz, *Applied Abstract Algebra*, Second ed., Springer-Verlag, New York, 1998.
- [Mac96] Moshé Machover, *Set Theory, Logic and their Limitations*, Cambridge Univ. 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.
- [Nab80] Gregory Naber, *Topological Methods in Euclidean Spaces*, Cambridge Univ. Press, Cambridge, 1980.
- [OT92] Peter Orlik and Hiroaki Terao, *Arrangements of Hyperplanes*, Springer-Verlag, Berlin, 1992.
- [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.
- [Pal91] Bruce Palka, *An Introduction to Complex Function Theory*, Springer-Verlag, New York, 1991.
- [Pie91] Benjamin Pierce, *Basic Category Theory for Computer Scientists*, MIT Press, Cambridge, MA, 1991.
- [Pit93] Jim Pitman, *Probability*, Springer-Verlag, New York, 1993.
- [Pou99] Bruce Pourciau, The education of a pure mathematician, *Amer. Math. Monthly* **106** (1999), 720–732.

- [Pow94] Malcolm Pownall, *Real Analysis*, Wm. C. Brown, Dubuque, 1994.
- [Rib96] Paulo Ribenboim, *The New Book of Prime Nnumber Records*, Springer-Verlag, New York, 1996.
- [Rob84] Fred Roberts, *Applied Combinatorics*, Prentice-Hall, Englewood Cliffs, NJ, 1984.
- [Rob86] Eric Roberts, *Thinking Recursively*, John Wiley & Sons, New York, 1986.
- [Ros68] Maxwell Rosenlicht, *Introduction to Analysis*, Dover, New York, 1968.
- [Ros93a] Kenneth H. Rosen, *Elementary Number Theory and its Applications*, Third ed., Addison-Wesley, Reading, MA, 1993.
- [Ros93b] Sheldon Ross, *Introduction to Probability Models*, Fifth ed., Academic Press, Boston, 1993.
- [Rot73] Joseph J. Rotman, *Theory of Groups*, Second ed., Allyn & Bacon, Boston, 1973.
- [Rot96] Joseph J. Rotman, *An Introduction to the Theory of Groups*, Fourth ed., Springer-Verlag, New York, 1996.
- [Rya86] Patrick J. Ryan, *Euclidean and Non-Euclidean Geometry*, Cambridge Univ. Press, New York, 1986.
- [Set96] Ravi Sethi, *Programming Languages: Concepts and Constructs*, Second 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.
- [SR81] Ernst Sondheimer and Alan Rogerson, *Numbers and Infinity: A Historical Account of Mathematical Concepts*, Cambridge Univ. Press, Cambridge, 1981.
- [Sti94] John Stillwell, *Elements of Algebra*, Springer-Verlag, New York, 1994.

- [Str48] Dirk J. Struik, *A Concise History of Mathematics*, Dover, New York, 1948.
- [Sup60] Patrick Suppes, *Axiomatic Set Theory*, Van Nostrand, Princeton, 1960.
- [Sz63] Gabor Szasz, *Introduction to Lattice Theory*, Academic Press, New York, 1963.
- [Tho59] D’Arcy Wentworth Thompson, *On Growth and Form*, Second ed., Vol. 2, Cambridge Univ. Press, Cambridge, 1959.
- [Tru87] Richard Trudeau, *The Non-Euclidean Revolution*, Birkhauser, Boston, 1987.
- [Vau95] Robert Vaught, *Set Theory*, Second ed., Birkhauser, Boston, 1995.
- [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.
- [WW98] Edward Wallace and Stephen West, *Roads to Geometry*, Second ed., Prentice Hall, Upper Saddle River, NJ, 1998.
- [Zim96] H.-J. Zimmermann, *Fuzzy Set Theory and its Applications*, Third ed., Kluwer Academic Publishers, Boston, 1996.

Index

(f_1, \dots, f_n) , 153	$\text{GL}_2(\mathbb{R})$, 252, 266
$-$, 122	$\text{GL}_3(\mathbb{Z})$, 224
$/\!/$, xvi	glb , 279
$ A $, 208	$ x $, 80
A/\sim , 192	$\lfloor x \rfloor$, 81
$f^*(Q)$, 146	\iff , 23
f^n , 169, 368	\leftrightarrow , 10
$f_*(P)$, 146	$\llbracket a, b \rrbracket$, 335
$f_1 \times \dots \times f_n$, 154	$\llbracket a; \infty \rrbracket$, 335
i , 358	\vee , 284
\aleph_0 , 215	\wedge , 6
$\bigcap_{i \in I}$, 130	$\lceil x \rceil$, 158
$\bigcup_{i \in I}$, 130	$\bar{\wedge}$, 30
Δ , 128	\neg , 8
$\binom{n}{k}$, 309	\vee , 7
\cap , 119	\Diamond , xvi
\circ , 152	lub , 279
\cup , 119	\wedge , 284
\emptyset , 110	\mathbb{N} , 109
$\equiv (\text{mod } n)$, 185	$\not\subseteq$, 112
$\llbracket 1, n \rrbracket$, 207	\nwarrow , 81
$f: A \rightarrow B$, 138	\curvearrowleft , 81

- $\prod_{i \in I}$, 175
- $\mathcal{P}(A)$, 115
- \mathbb{Q} , 110
- \Rightarrow , 20
- \mathbb{R}^+ , 110
- \mathbb{R} , 110
- \sim , 205
- \square , xvi
- \subseteq , 112
- \subsetneq , 113
- $\mathrm{SL}_2(\mathbb{R})$, 266
- \times , 124
- \rightarrow , 9
- Δ , xvi
- \mathbb{Z}^{nn} , 110
- \mathbb{Z}_n , 187
- \mathbb{Z} , 110
- \mathbb{Z} -action, 176
- Abel, Neils, 259
- abelian group, 259
- absolute value, 80, 345
- absorption
 - law
 - sets, 121
- absorption law, 286
- abstract algebra, 56, 59
- abuse of notation, 147
- addition
 - complex numbers, 357
 - integers, 340
 - logical implication, 20
 - natural numbers, 327
 - rational numbers, 348
 - real numbers, 354
 - rule of inference, 33
- adjunction, 33
- affirming the consequent, fallacy of, 38
- algebra
 - abstract, 56, 59
 - boolean, 293
 - algebraic numbers, 219
 - algebraic product, 372
 - algebraic sum, 372
 - algebraic topology, 259, 360
 - and, 6, 119, 231; 284
 - antecedent, 10
 - antisymmetric relation, 274
 - argument, 31
 - conclusion, 31
 - consistent premises, 37
 - inconsistent premises, 37
 - premises, 31
 - valid, 32
 - Aristotle, 3
 - Arrow Impossibility Theorem, 273
 - associative law, 253, 258
 - functions, 155
 - lattices, 286
 - logic, 24
 - real numbers, 375
 - sets, 121
 - Axiom of Choice, 116, 165, 210, 211, 213, 216
 - axiomatic system, 55
 - backwards proof, 84, 98
 - Bernoulli, Daniel, 242
 - biconditional, 10
 - biconditional-conditional, 21, 33
 - bijective, 161, 204
 - binary operation, 251
 - Binet's formula, 242
 - binomial coefficient, 222, 309
 - Binomial Theorem, 313, 315
 - bivalence, 5
 - boolean algebra, 293

- bound
 - greatest lower, 277, 284, 353
 - least upper, 277, 284, 353
 - lower, 277, 353
 - upper, 277, 353
- bound variable, 42
- Brouwer Fixed Point Theorem, 291
- Burnside's Formula, 170
- calculus, 86, 97, 135, 139, 140, 152
- cancellation law
 - real numbers, 376
- canonical map, 200
- Cantor's diagonal argument, 220
- Cantor, Georg, 109, 204, 215, 220, 222
- Cantor–Bernstein Theorem, 216
- cardinality, 208, 294
 - same, 205
- Cartesian product, 124
- cases, proof by, 74
- Cauchy sequences, 353
- characteristic function, 145, 371
- China, 313
- Choice, Axiom of, 116, 165, 210, 211, 213, 216
- closed interval, 111
- codomain, 138
- Cohen, Paul, 222
- combinations, 309
- combinatorics, 294
- commutative diagram, 153
- commutative law, 253, 259
 - lattices, 286
 - logic, 23, 24
 - real numbers, 375
 - sets, 121
- complement, 372
- complex analysis, 360
- complex numbers, 352, 356
 - addition, 357
 - construction, 356
 - multiplication, 357
 - negation, 357
 - reciprocal, 357
- composite numbers, 72
- composition, 152, 264
 - associative law, 155
 - identity law, 155
 - noncommutativity, 154
- computer, 30, 230
 - programming language, 222
 - science, 4, 222, 236, 280
- conclusion, 31
- conditional, 9
- conditional-biconditional, 21, 33
- congruent modulo n , 185, 366
- conjunction, 6
 - associative law, 24
 - commutative law, 24
- consequent, 10
- consistent premises, 37
- constant, 140
 - map, 142
- constantive , 369
- constructive dilemma, 21, 33
- constructivism, 73
- Continuum Hypothesis, 222
- contradiction, 13
 - proof by, 69
- contrapositive, 24, 26
 - proof by, 68
- converse, 26
 - fallacy of, 38
- coordinate function, 153
- countable set, 207
- countably infinite, 207
- counterexample, 88

- counting, 294
- covers, 275
- crystallography, 259
- De Morgan's law, 27
 - logic, 24, 76
 - sets, 123, 131
- decimal expansion, 220
- Dedekind cut, 353
- denumerable set, 207
- denying the antecedent, fallacy of, 39
- derangement, 315
- derivation, 34
- determinant, 78, 83, 252, 266
- diagram
 - commutative, 153
 - Venn, 120
- difference of set, 122
- direct proof, 64
- disjoint sets, 122
- disjunction, 7
 - associative law, 24
 - commutative law, 23
- distributive law, 125, 287
 - logic, 24
 - real numbers, 376
 - sets, 121, 131, 133
- divides, 65, 364
- divisible, 65, 294, 301
- Division Algorithm, 186, 193, 296, 345
- domain, 138
- double negation, 23, 33, 69
 - real numbers, 376
- element, 109
 - greatest, 283, 293
 - identity, 254
 - inverse, 255
- least, 283, 293
- empty set, 110
 - fuzzy, 372
- epic, 161
- equality
 - functions, 138, 142
 - sets, 113
- equilateral triangle, 263
- equivalence, *see* logical equivalence
- equivalence classes, 192
- equivalence relation, 191
 - and partitions, 194
 - minimal, 198
- equivalent statements, 23
- Euclid, 55
- Euler, Leonhard, 82, 242
- even integers, 60, 347
- excluded middle, law of the, xvi, 5, 69
- existence
 - and uniqueness, 86
 - proof, 73
 - theorem, 345, 360
- existential
 - generalization, 49
 - instantiation, 49
 - quantifier, 44
- extension map, 143
- factor, 65
- factorial, 239, 305
- fallacy, 38
 - of affirming the consequent, 38
 - of denying the antecedent, 39
 - of the converse, 38
 - of the inverse, 39
 - of unwarranted assumptions, 39

- family of sets, 130
- Fibonacci, 239
 - numbers, 239, 320, 369
 - sequence, 239
- field, 352, 360
- finite set, 207
- first order logic, 42
- fixed point, 290, 315
- fixed set, 170
- fraction, 65, 70, 110, 218, 376
- free variable, 43
- frieze pattern, 265
- function, 138
 - constantive , 369
 - hidempotent , 369
 - bijective, 161, 204
 - characteristic, 145, 371
 - composition, 152, 264
 - coordinate, 153
 - epic, 161
 - equality, 138, 142
 - fixed set, 170
 - greatest integer, 81, 150, 158, 195
 - image, 146
 - injective, 161, 210, 211, 215
 - inverse, 155
 - left, 155
 - right, 155
 - inverse image, 146
 - iteration, 169, 368
 - least integer, 158
 - monic, 161
 - nilpotent, 369
 - one-to-one, 161
 - onto, 161
 - orbit, 169
 - order, 170
 - range, 146
- real-valued, 367
- relation preserving, 184
- respects relation, 183
- set of, 170
- stabilizer, 170
- surjective, 161, 210, 211
- Fundamental Theorem
 - of Algebra, 360
 - of Arithmetic, 234, 365
- fuzzy
 - algebraic product, 372
 - algebraic sum, 372
 - complement, 372
 - empty set, 372
 - intersection, 372
 - logic, 371
 - set, 371
 - subset, 371
 - union, 372
- Galileo, 203, 205, 207
- geometry, 259
- golden ratio, 242
- Gordan, Paul, 73
- grammar, xv, xx, 95, 98
- greatest common divisor, 364
- greatest element
 - lattice, 293
 - poset, 276, 283
- greatest integer function, 81, 150, 158, 195
- greatest lower bound
 - poset, 277, 284
 - rational numbers, 353
 - real numbers, 278, 353
- group, 258
 - abelian, 259
 - homomorphism, 267
 - isomorphism, 270
 - subgroup, 262

- symmetry, 265
- trivial, 259
- half-open interval, 111
- Hamilton, William Rowan, 357
- Hasse diagrams, 275
- Henkin set, 325
- hidempotent, 369
- Hilbert, David, 73
- history of mathematics, xvi
- homomorphism
 - group, 267
 - join, 289
 - meet, 289
 - order, 280
- horses, 229
- hypothetical syllogism, 21, 33
- idempotent
 - law
 - sets, 121
- idempotent law, 286
- identity
 - element, 254
 - law, 254, 258
 - functions, 155
 - real numbers, 375
 - sets, 121
 - map, 142
 - matrix, 86
- if and only if, 10
 - theorems, 76
- iff, *see* if and only if
- image, 146
- imaginary numbers, 356
- implication, *see* logical implication
- implies, 20
- inclusion map, 142
- inclusion-exclusion, principle of, 299
- inconsistent premises, 37
- indexing set, 130
- induction, *see* mathematical induction
- inductive
 - hypothesis, 228
 - reasoning, 226
 - step, 228
- infinite, 207
- infinite interval, 111
- injective, 161, 210, 211, 215
- integers, 110
 - addition, 340
 - construction, 338
 - even, 60, 347
 - less than, 340
 - less than or equal to, 340
 - modulo n , 187
 - multiplication, 340
 - negation, 340
 - negative, 344
 - non-negative, 110
 - odd, 60, 347
 - positive, 344
- interesting number, 335
- intersection, 119, 130
 - associative law, 121
 - commutative law, 121
 - fuzzy, 372
- interval, 110
 - closed, 111
 - half-open, 111
 - infinite, 111
 - open, 111
- intuition, 56
- intuitionism, 73

- inverse
 - element, 255
 - fallacy of, 39
 - function, 155
 - left, 155
 - right, 155
 - image, 146
 - matrix, 86
 - statement, 26
- inverses law, 255, 258
 - real numbers, 376
- invertible matrix, 224, 252
- irrational numbers, 70
- isometry, 263
- isomorphic, 270
- isomorphism
 - group, 270
 - order, 280
- iteration, 169, 368
- join, 284
 - homomorphism, 289
- kernel, 269
- lattice, 284
 - complemented, 293
 - distributive, 293
 - greatest element, 293
 - least element, 293
- law
 - absorption, 121, 286
 - associative, 24, 121, 155, 253, 258, 286, 375
 - cancelation, 376
 - commutative, 23, 24, 121, 253, 259, 286, 375
 - De Morgan's, 24, 27, 76, 123, 131
 - distributive, 24, 121, 125, 131, 133, 287, 376
- idempotent, 121, 286
- identity, 121, 155, 254, 258, 375
- inverses, 255, 258, 376
- of the excluded middle, xvi, 5, 69
- right inverses, 266
- trichotomy, 334, 376
- least element
 - lattice, 293
 - poset, 276, 283
- least integer function, 158
- least upper bound
 - poset, 277, 284
 - rational numbers, 353
 - real numbers, 278, 353
- Least Upper Bound Property, 278, 353
- left inverse function, 155
- Leonardo of Pisa, 239
- less than
 - integers, 340
 - natural numbers, 331
 - rational numbers, 348
 - real numbers, 354
- less than or equal to
 - integers, 340
 - natural numbers, 331
 - rational numbers, 349
- lexicographical order, 275
- limit, 244
- linear ordering, 274, 279
- logic, 3
 - first order, 42
 - fuzzy, 371
 - predicate, 42
 - propositional, 42
 - sentential, 42
- logical

- equivalence, 22
- implication, 18
- lower bound
 - greatest, 277, 284, 353
 - poset, 277
 - rational numbers, 353
 - real numbers, 278, 353
- Lucas
 - numbers, 370
 - sequence, 370
- map, 138
 - canonical, 200
 - constant, 142
 - extension, 143
 - identity, 142
 - inclusion, 142
 - order preserving, 280
 - projection, 143, 153
 - restriction, 143
- mathematical
 - notation, xv
 - terminology, xv
- mathematical induction, 226, 325
 - principle of, 226
 - variant one, 232, 335
 - variant three, 234, 337
 - variant two, 233, 336
- mathematics
 - history of, xvi
 - philosophy of, xvi
- matrix
 - determinant, 78, 83, 252, 266
 - identity, 86
 - inverse, 86
 - invertible, 224, 252
 - trace, 78, 83
 - upper triangular, 78
- meet, 284
 - homomorphism, 289
- member, 109
- minimal
 - equivalence relation, 198
 - relation, 183
- modus ponens, 20, 33
- modus tollendo ponens, 20, 33
- modus tollens, 20, 33
- monic, 161
- multiple, 67
- multiplication
 - complex numbers, 357
 - integers, 340
 - natural numbers, 329
 - rational numbers, 348
 - real numbers, 354
- nand, 30, 231
- natural numbers, 109, 324
 - addition, 327
 - less than, 331
 - less than or equal to, 331
 - multiplication, 329
 - uniqueness, 337
- necessary, 10
 - and sufficient, 11
- negation, 231
 - complex numbers, 357
 - integers, 340
 - logical, 8
 - of statements, 26
 - of statements with quantifiers, 47
- rational numbers, 348
- real numbers, 354
- negative integers, 344
- nilpotent, 369
- non-negative integers, 110
- not, 8
- null set, 110

- numbers
 - algebraic, 219
 - complex, 356
 - composite, 72
 - Fibonacci, 239, 320, 369
 - imaginary, 356
 - interesting, 335
 - irrational, 70
 - Lucas, 370
 - natural, 109
 - positive real, 110
 - prime, 72, 82, 189, 190, 234
 - rational, 70, 110, 348
 - real, 110
- odd integers, 60, 347
- one-to-one, 161
- onto, 161
- open interval, 111
- operation
 - binary, 251
 - ternary, 258
 - unary, 251
- or, 7, 119, 231, 284
- orbit, 169
- order, 170
 - homomorphism, 280
 - isomorphism, 280
 - preserving map, 280
- ordered pair, 123
- ordering
 - linear, 274, 279
 - partial, 274
 - quasi, 283
 - total, 274
- pair, ordered, 123
- partial ordering, 274
- partially ordered set, 274, *see* poset
- partition, 193
- and equivalence relations, 194
- Pascal's triangle, 313, 314
- Peano Postulates, 226, 325
- permutations, 306
- philosophy of mathematics, xvi
- phyllotaxis, 239
- pigeonhole principle, 338
- pointwise addition, 367
- polynomial, 219, 359
- poodle-o-matic, 31
- poset, 274
 - greatest element, 276, 283
 - greatest lower bound, 277, 284
 - least element, 276, 283
 - least upper bound, 277, 284
 - lower bound, 277
 - upper bound, 277
- positive
 - integers, 344
 - real numbers, 110
- power set, 115, 149, 172, 199, 214
 - cardinality, 115, 307
- predicate logic, 42
- premises, 31
 - consistent, 37
 - inconsistent, 37
- prerequisites, xiv
- prime numbers, 72, 82, 189, 190, 234
 - infinitely many, 72
- principle
 - of inclusion-exclusion, 299
 - of mathematical induction, 226
 - variant one, 232, 335
 - variant three, 234, 337
 - variant two, 233, 336
 - pigeonhole, 338
 - well-ordering, 334, 345
- product, 124, 175

- projection map, 143, 153
- proof, 55
 - backwards, 84, 98
 - by cases, 74
 - by contradiction, 69
 - by contrapositive, 68
 - direct, 64
 - existence, 73
 - existence and uniqueness, 86
 - two-column, xv, 1, 34, 57, 61, 96
- proper subset, 113
- propositional logic, 42
- puzzle, 243
- Pythagorean Theorem, xiii, 59
- quadratic
 - equations, 356
 - formula, 356
- quantifier, 41
 - existential, 44
 - in theorems, 81
 - universal, 43
- quantum mechanics, 259
- quaternions, 360
- quotient set, 192
- rabbits, 239
- range, 138, 146
- rational numbers, 70, 110
 - addition, 348
 - construction, 348
 - greatest lower bound, 353
 - least upper bound, 353
 - less than, 348
 - less than or equal to, 349
 - lower bound, 353
 - multiplication, 348
 - negation, 348
 - reciprocal, 348
- upper bound, 353
- real numbers, 110, 352
 - addition, 354
 - construction, 352
 - greatest lower bound, 278, 353
 - least upper bound, 278, 353
 - less than, 354
 - lower bound, 278, 353
 - multiplication, 354
 - negation, 354
 - reciprocal, 354
 - upper bound, 278, 353
- real-valued function, 367
- reciprocal
 - complex numbers, 357
 - rational numbers, 348
 - real numbers, 354
- recursion, 236
- recursive
 - definition, 236
 - description, 236
- reflection, 263
- reflexive relation, 180, 274
- relation, 178
 - antisymmetric, 274
 - class, 179
 - equivalence, 191
 - minimal, 198
 - minimal, 183
 - reflexive, 180, 274
 - symmetric, 180
 - transitive, 180, 274
- relation preserving function, 184
- relatively prime, 79, 258, 365
- repetition, 33
- respects relation, 183
- restriction map, 143
- right inverse function, 155
- right inverses law, 266

- rotation, 263
- rule
 - product, 295
 - sum, 297
- rules of inference, 33
- Russell's Paradox, 116
- Schroeder–Bernstein Theorem, 216, 218, 225
- sentential logic, 42
- sequence, 171
 - Cauchy, 353
 - Fibonacci, 239
 - Lucas, 370
- set difference, 122
- sets, 109
 - absorption law, 121
 - associative law, 121
 - commutative law, 121
 - countable, 207
 - countably infinite, 207
 - De Morgan's law, 123, 131
 - denumerable, 207
 - difference, 122
 - disjoint, 122
 - distributive law, 121, 131, 133
 - element, 109
 - empty, 110
 - fuzzy, 372
 - equality, 113
 - family of, 130
 - finite, 115, 207
 - fuzzy, 371
 - Henkin, 325
 - idempotent law, 121
 - identity law, 121
 - indexing, 130
 - infinite, 115, 207
 - intersection, 119, 130
 - member, 109
 - null, 110
 - of functions, 170
 - partially ordered, 274
 - power, 115, 149, 172, 199, 214, 307
 - product, 124, 175
 - quotient, 192
 - subset, 112
 - proper, 113
 - symmetric difference, 128
 - totally ordered, 274
 - uncountable, 207
 - union, 119, 130
 - simplification, 20, 33
 - square root, 71, 356
 - stabilizer, 170
 - Standard ML, 222
 - statement, 4
 - equivalent, 23
 - meta, 18
 - subgroup, 262
 - trivial, 263
 - subset, 112
 - fuzzy, 371
 - proper, 113
 - sufficient, 10
 - surjective, 161, 210, 211
 - switching circuits, 30, 230
 - symbols, xv
 - symmetric
 - difference, 128
 - relation, 180
 - symmetry, 263
 - group, 265
 - tautology, 13
 - ternary operation, 258
 - TFAE, *see* the following are equivalent
 - Thales of Miletus, 55

- the following are equivalent, 78
- Theorem
- Arrow Impossibility, 273
 - Binomial, 313, 315
 - Brouwer Fixed Point, 291
 - Cantor–Bernstein, 216
- theorem
- existence, 345, 360
 - if and only if, 76
- Theorem
- Pythagorean, xiii, 59
 - Schroeder–Bernstein, 216, 218, 225
 - Wilson's, 190
- topological sorting, 280
- total ordering, 274
- totally ordered set, 274
- trace, 78, 83
- transition course, ix
- transitive relation, 180, 274
- trichotomy law, 334, 376
- trivial subgroup, 263
- truth table, 6
- two-column proofs, xv, 1, 34, 57, 61, 96
- unary operation, 251
- uncountable set, 207
- union, 119, 130
 - associative law, 121
- commutative law, 121
- fuzzy, 372
- uniqueness, 86
- universal
- generalization, 49
 - instantiation, 49
 - quantifier, 43
- unwarranted assumptions, fallacy of, 39
- upper bound
- least, 277, 284, 353
 - poset, 277
 - rational numbers, 353
 - real numbers, 278, 353
- upper triangular matrix, 78
- valid argument, 32
- variable, 66, 99, 139
 - bound, 42
 - free, 43
- Venn diagram, 120
- wallpaper pattern, 265
- well-defined, 141
- Well-Ordering Principle, 334, 345
- Wilson's Theorem, 190
- writing mathematics, xv, xx, 93
- Zeno, 203
- Zermelo-Fraenkel axioms, 116