TEXTBOOKS IN MATHEMATICS

AN INTRODUCTION TO PROOF AND ANALYSIS

Exploring the INFINITE

Jennifer Brooks

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

AN INTRODUCTION TO
PROOF AND ANALYSIS

Exploring the
INFINITE

TEXTBOOKS in MATHEMATICS

Series Editors: Al Boggess and Ken Rosen

PUBLISHED TITLES

ABSTRACT ALGEBRA: A GENTLE INTRODUCTION
Gary L. Mullen and James A. Sellers

ABSTRACT ALGEBRA: AN INTERACTIVE APPROACH, SECOND EDITION
William Paulsen

ABSTRACT ALGEBRA: AN INQUIRY-BASED APPROACH
Jonathan K. Hodge, Steven Schlicker, and Ted Sundstrom

ADVANCED LINEAR ALGEBRA
Hugo Woerdeman

APPLIED ABSTRACT ALGEBRA WITH MAPLE™ AND MATLAB®, THIRD EDITION
Richard Klima, Neil Sigmon, and Ernest Stitzinger

APPLIED DIFFERENTIAL EQUATIONS: THE PRIMARY COURSE
Vladimir Dobrushkin

A BRIDGE TO HIGHER MATHEMATICS
Valentin Deaconu and Donald C. Pfaff

COMPUTATIONAL MATHEMATICS: MODELS, METHODS, AND ANALYSIS WITH MATLAB® AND MPI, SECOND EDITION
Robert E. White

DIFFERENTIAL EQUATIONS: THEORY, TECHNIQUE, AND PRACTICE, SECOND EDITION
Steven G. Krantz

DIFFERENTIAL EQUATIONS: THEORY, TECHNIQUE, AND PRACTICE WITH BOUNDARY VALUE PROBLEMS
Steven G. Krantz

DIFFERENTIAL EQUATIONS WITH APPLICATIONS AND HISTORICAL NOTES, THIRD EDITION
George F. Simmons

DIFFERENTIAL EQUATIONS WITH MATLAB®: EXPLORATION, APPLICATIONS, AND THEORY
Mark A. McKibben and Micah D. Webster

ELEMENTARY NUMBER THEORY
James S. Kraft and Lawrence C. Washington

PUBLISHED TITLES CONTINUED

EXPLORING CALCULUS: LABS AND PROJECTS WITH MATHEMATICA®
Crista Arangala and Karen A. Yokley

EXPLORING GEOMETRY, SECOND EDITION
Michael Hvidsten

EXPLORING LINEAR ALGEBRA: LABS AND PROJECTS WITH MATHEMATICA®
Crista Arangala

GRAPHS & DIGRAPHS, SIXTH EDITION
Gary Chartrand, Linda Lesniak, and Ping Zhang

INTRODUCTION TO ABSTRACT ALGEBRA, SECOND EDITION
Jonathan D. H. Smith

INTRODUCTION TO MATHEMATICAL PROOFS: A TRANSITION TO ADVANCED MATHEMATICS, SECOND EDITION
Charles E. Roberts, Jr.

INTRODUCTION TO NUMBER THEORY, SECOND EDITION
Marty Erickson, Anthony Vazzana, and David Garth

LINEAR ALGEBRA, GEOMETRY AND TRANSFORMATION
Bruce Solomon

MATHEMATICAL MODELLING WITH CASE STUDIES: USING MAPLE™ AND MATLAB®, THIRD EDITION
B. Barnes and G. R. Fulford

MATHEMATICS IN GAMES, SPORTS, AND GAMBLING–THE GAMES PEOPLE PLAY, SECOND EDITION
Ronald J. Gould

THE MATHEMATICS OF GAMES: AN INTRODUCTION TO PROBABILITY
David G. Taylor

A MATLAB® COMPANION TO COMPLEX VARIABLES
A. David Wunsch

MEASURE THEORY AND FINE PROPERTIES OF FUNCTIONS, REVISED EDITION
Lawrence C. Evans and Ronald F. Gariepy

NUMERICAL ANALYSIS FOR ENGINEERS: METHODS AND APPLICATIONS, SECOND EDITION
Bilal Ayyub and Richard H. McCuen

ORDINARY DIFFERENTIAL EQUATIONS: AN INTRODUCTION TO THE FUNDAMENTALS
Kenneth B. Howell

PRINCIPLES OF FOURIER ANALYSIS, SECOND EDITION
Kenneth B. Howell

PUBLISHED TITLES CONTINUED

RISK ANALYSIS IN ENGINEERING AND ECONOMICS, SECOND EDITION
Bilal M. Ayyub

SPORTS MATH: AN INTRODUCTORY COURSE IN THE MATHEMATICS OF SPORTS SCIENCE AND SPORTS ANALYTICS
Roland B. Minton

TRANSFORMATIONAL PLANE GEOMETRY
Ronald N. Umble and Zhigang Han

TEXTBOOKS in MATHEMATICS

AN INTRODUCTION TO PROOF AND ANALYSIS

Exploring the INFINITE

Jennifer Brooks
University of Montana, USA

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20161019

International Standard Book Number-13: 978-1-4987-0449-6 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Preface

Mathematics is an incredibly broad endeavor, encompassing areas as diverse as number theory, numerical analysis, graph theory, and topology, just to name a few. What holds the discipline together as a single, recognizable unit are its quest to identify and abstract patterns and its reliance on logical argumentation.

This book guides the reader through these processes of abstraction and logical argumentation, to make the transition from student of mathematics to practitioner of mathematics. Such a transition requires more than knowledge of the definitions of mathematical structures, elementary logic, and standard proof techniques. Indeed, the student focused on only these will develop little more than the ability (common among young students but nearly useless in research) to identify a number of proof templates and to apply them in predictable ways to standard problems. This book aims to do something more; it aims to help readers learn to explore mathematical situations, to make conjectures, and only then to apply methods of proof. Practitioners of mathematics must do all of these things.

How do we teach exploration? First, we provide many opportunities for creative mathematical thought. Whenever possible, we pose questions for readers to explore, hopefully ending in a proof of a conjecture, rather than suggesting the result to prove. Thus we would ask readers to find and prove a formula for the sum of the first n natural numbers rather than asking for a proof that $1+2+3+\ldots+n = n(n+1)/2$. Second, we help readers develop an invaluable skill for mathematical exploration, namely basic facility with programming.

Learning to program does more than help with the exploration of a mathematical situation; it may also lead from the conjecture phase toward a valid proof. For example, suppose we are given a continuous function $f\colon [0,1] \to \mathbb{R}$ such that $f(0) < 0$ and $f(1) > 0$ and we want an x between 0 and 1 for which $f(x) = 0$. We could hit on the idea of finding it with a simple divide-and-conquer program: start with $a_0 = 0$ and $b_0 = 1$. $f(a_0) < 0$ and $f(b_0) > 0$ by hypothesis. Now consider their average, $c_0 = \frac{1}{2}$. If $f(c_0) = 0$, we have found our x. Suppose we aren't so lucky. If $f(c_0) < 0$, set $a_1 = \frac{1}{2}$ and $b_1 = 1$. Otherwise set $a_1 = 0$ and $b_1 = \frac{1}{2}$. Now repeat the process; $f(a_1) < 0$ and $f(b_1) > 0$. Consider their average $c_1 = \frac{a_1+b_1}{2}$. Based on the value $f(c_1)$, define a_2 and b_2 so that f still changes sign on the new, smaller interval $[a_2, b_2]$. Writing a computer program to carry out this algorithm is trivial. *But we have also found a viable approach to a general proof of the Intermediate Value Theorem.*

Prerequisites; Ground rules An awkward feature of all books of this type is that one must decide what readers are expected to know and what they can assume as known in their proofs. Our approach is to avoid pedantry, perhaps at the cost of some rigor. We believe that proof is better presented as “a clear, logical explanation of the solution to an interesting non-obvious question” than as “the construction of a formal argument using only axioms, definitions, and previously-established theorems.” It is not that we believe that the latter is incorrect, but rather that we have seen students become almost paralyzed in their early proof-writing efforts, not sure if they are allowed to assume that, say, the basic rules of algebra are valid. We would rather readers think more about the mathematical process of exploring, conjecturing, and proving, and less about the formal rules.

That said, here are our ground rules: we assume readers know that the real number system satisfies the ordered field axioms (even if they don’t recognize the term “ordered field”). Thus the basic rules learned in school for doing arithmetic and for solving equations and inequalities are indeed valid. We will briefly review the properties of familiar number systems in Chapter 1, but after Chapter 1 we will use them without comment. Later in the book, we will step back and look more closely at how one can build up the field of rational numbers from the integers and how one can construct the real numbers from the rational numbers. At that time, we may pause to consider again why all of these rules work.

Format of the book The chapters of this text are divided into two parts. The first part serves as an introduction to proof and abstract mathematics and aims to prepare the reader for advanced course work in all areas of mathematics. It thus includes all the standard material from a “transition to proof” course: induction, basic logic, elementary set theory, functions and relations, and basic number theory and combinatorics. Part II constitutes an introduction to the basic concepts of analysis, including limits of sequences of real numbers and of functions, infinite series, the structure of the real line, and continuous functions.

That said, we aim for a fresh perspective; we achieve additional coherence by focusing on exploring the infinite, as the title suggests. Thus in Part I, we emphasize sequences, recurrence relations, and the cardinality of infinite sets as our main applications of induction, sets, and functions. In Part II, the infinite is everywhere, as a first analysis course is primarily about limiting processes. Still, we emphasize sequences. We think of real numbers as those objects that can be approximated by Cauchy sequences of rational numbers. We define continuous functions as those that send convergent sequences to convergent sequences. And we define compact sets as those with the property that every sequence in the set has a subsequence converging to a point of the set. We leave more abstract topological notions for a future course. This approach to analysis is somewhat non-standard; often a first analysis course is presented as “single-variable calculus made rigorous.” Such a course would certainly cover not only limits and continuity, but also differentiation and integration. Such material is an important part of the undergraduate curriculum. We choose, however, to worry less about whether we cover all of calculus once again and focus instead on understanding the idea of a limit at a very deep level. It has been our observation from teaching this material that students understand limits more easily in the context of sequences (as opposed to functions), and thus time spent here is time well spent. An additional advantage of our focus on sequences is that it allows readers to continue to use their new programming skills to explore concepts in analysis. Many theorems in analysis can be proved by inductively constructing sequences whose limit is an object of interest (the supremum of a set, the zero of a continuous function, the fixed point of a contractive mapping, etc.). If one can write a program to execute such an algorithm, one has come a long way towards understanding the result and its proof.

How to use this book This book is designed not only to be readable, but to help students learn how to read math books. Each section is a combination of exposition, motivation, examples, and embedded exercises. Readers should do all these exercises, as they ask them to use new definitions, practice new techniques, fill in details of a calculation, or prove corollaries and extensions of results in the text. The point is that reading mathematics is a very active endeavor, not at all like reading other books. It is a slow process, requiring paper, pencil, and active struggle.

The text also includes many problems at the ends of chapters. Unlike the exercises, which are focused and explicit, the problems encourage exploration. In a problem, we pose a question but seldom say what the result is; the reader must first find the result and then prove it. Such problems do have more potential to frustrate than requests for proofs of specific statements. But doing mathematics is at least as much about trying to figure out what is true as it is about trying to find a good proof of a known result.

Acknowledgements First, I would like to thank Jeffrey Kacmarcik. He is a Senior Systems Programmer at the University of Wisconsin and consulted with me on the Appendix and the Python code throughout the book. I thank John D'Angelo for his encouragement, advice, and feedback. I thank my daughter, the joy of my life, for her love and friendship. Finally, I thank Curtis for his love and support, and for his companionship on this wonderful path we have chosen.

Part I

Fundamentals of Abstract Mathematics

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Chapter 1

Basic Notions

If you are reading this chapter, you are probably beginning a course with a title like *Introduction to Abstract Mathematics* or *Mathematical Reasoning*. Such courses are designed to help you make a transition from courses like calculus that focus mainly on developing the computational fluency needed by a *user* of mathematics to advanced courses that focus on developing the understanding of the theoretical underpinnings of mathematics needed by a *creator* of mathematics. Where should such a course begin? If it is an "introductory" course, perhaps it should start at the beginning, not assuming any particular mathematical knowledge. In a sense, we do this; we do not assume you have any experience with reading or writing mathematical proofs. On the other hand, this is far from your first course in mathematics. At this point, you are certainly fluent in arithmetic and algebra and very comfortable with trigonometry, calculus, and basic plane geometry. This course would feel like some formal game if we asked you to pretend you do not have all this knowledge.

Here is what we do ask: think of your journey through mathematics as a journey up a spiral staircase. In a sense, each time around you seem to be moving over the same territory, but in fact each time you come upon it, you do so at a higher level. In this chapter, we discuss what facts about number systems you can freely use as you embark on this stage of the journey. Later in the book, however, we may circle back around and ask you to think more deeply about these basic notions and justify statements that you had previously taken as facts.

1.1 A First Look at Some Familiar Number Systems

1.1.1 Integers and natural numbers

We let $\mathbb{Z}$ denote the set of integers $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. This set is *closed* under the operations of addition ($+$) and multiplication ($\cdot$). In other words, when we add two integers, the result is a unique integer, and when we multiply two integers, the result is a unique integer.

We must know what properties these operations satisfy. Even if you have never seen a formal enumeration of these properties, you have freely used them for many years. The first two properties, for example, imply that if you want to add up a list of numbers, you can add them in any order you like and group them in any way you like. Here's the complete list.

1. The operations of addition and multiplication of integers are *associative.* That is, if m, n, p are integers, $(m+n)+p = m+(n+p)$ and $(m \cdot n) \cdot p = m \cdot (n \cdot p)$.

2. The operations of addition and multiplication of integers are *commutative.* That is, if m, n are integers, $m + n = n + m$ and $m \cdot n = n \cdot m$.

3. There is a unique integer, 0, such that $n+0 = 0+n = n$ for all integers n. Furthermore, there is a unique integer, 1, such that $n \cdot 1 = 1 \cdot n = n$ for all integers n. 0 is called the *additive identity* and 1 is called the *multiplicative identity.*

4. Every integer has an *additive inverse.* That is, if n is an integer, there is a unique integer m such that $n + m = m + n = 0$. We write $-n$ for the unique additive inverse of n.

5. Multiplication *distributes* over addition. That is, if m, n, p are integers, $m \cdot (n + p) = m \cdot n + m \cdot p$ and $(m + n) \cdot p = m \cdot p + n \cdot p$.

When no confusion can arise, we will use juxtaposition to denote multiplication of integers, omitting the dot. Thus the distributive law can also be written

$$m(n + p) = mn + mp.$$

We will also freely use $n - m$ to mean $n + (-m)$, and we will use exponents to indicate repeated multiplication (for example, n^2 for $n \cdot n$, etc.).

We may use this list to obtain other *propositions* about the integers. For example, consider the following proposition:

Proposition 1.1. *For all integers n, $0 \cdot n = 0$.*

Of course, we all consider the above proposition to be true. In this book, however, we don't simply want to appeal to past experience or authority. Instead, we want to demonstrate that a given statement follows from other statements we have already agreed are true. Such a demonstration is a *proof.* Let's give the simple proof using the properties of integer operations given above.

Proof. Property 3 states that the integers contain a *unique* additive identity, 0. Thus to show that $0 \cdot n = 0$, it suffices to show that $0 \cdot n$ has the same property characterizing the additive identity. Observe that, for any integer n,

$$\begin{aligned} n + 0 \cdot n &= 1 \cdot n + 0 \cdot n && \text{(by Property 3)} \\ &= (1+0) \cdot n && \text{(by Property 5)} \\ &= 1 \cdot n && \text{(by Property 3)} \\ &= n && \text{(by Property 3).} \end{aligned}$$

Thus $0 \cdot n = 0$, as claimed. □

To summarize, in order to establish a new proposition about operations with integers, we must give a proof using only the Properties 1–5 and previously-proved propositions.

Exercise 1.1. Prove each of the following propositions about integers using only Properties 1–5 above and Proposition 1.1.

(a) For all integers m and n, $(m+n)^2 = m^2 + 2mn + n^2$.

(b) For all integers n, $(-1) \cdot n = -n$. Before proving this statement, explain carefully what $(-1) \cdot n$ means and what $-n$ means.

(c) For all integers m and n, $(-m)n = -(mn)$.

(d) For all integers n, $(-n)^2 = n^2$.

(e) For all integers m and n, $(m-n)^2 = m^2 - 2mn + n^2$.

What do we do if we are confronted with a proposition about operations with integers that we suspect is false? In a sense, this situation is easier; we need only supply one concrete counterexample. Suppose, for example, a classmate claims that, for all integers m and n,

$$(m+n)^4 = m^4 + m^3 n + m^2 n^2 + mn^3 + n^4.$$

All we need to do to disprove the claim is to find integers m and n for which equality fails. For instance, if we take $m = n = 1$, the left-hand side equals 16 whereas the right-hand side equals 5.

Natural numbers. The set $\mathbb{N} = \{1, 2, 3, \ldots\}$ of *natural numbers* gets special attention. The natural numbers are convenient for counting and for labeling terms in sequences and elements in sets. $\mathbb{N}$ is closed under addition and multiplication, but several of the other algebraic properties of the integers are not satisfied; $\mathbb{N}$ does not contain an additive identity, and elements of $\mathbb{N}$ do not have additive inverses in $\mathbb{N}$.

Divisibility and the Fundamental Theorem of Arithmetic. To this point, in our discussion of operations with integers, we have talked about addition, subtraction, and multiplication, but not division. The reason is that, unlike the other operations, which take a pair of integers and return another integer, dividing one integer by another does not always return an integer. Division is, nonetheless, an important operation.

Definition 1.1. Let m and n be integers, with $m \neq 0$. We say that m **divides** n (or that n **is divisible by** m) if there exists an integer k such that $n = mk$. When m divides n, we call m and k **factors** or **divisors** of n.

In the special case in which n is divisible by 2, we say that n is *even*. In this case, there exists an integer k such that $n = 2k$. If n is not even, it is *odd*, and there exists an integer k such that $n = 2k + 1$.

Exercise 1.2. Is the set of even integers closed under addition and multiplication? If so, give proofs. If not, provide counterexamples.

Exercise 1.3. Is the set of odd integers closed under addition and multiplication? If so, give proofs. If not, provide counterexamples.

When discussing divisibility, *prime* numbers play a particularly important role. Let's recall the definition.

Definition 1.2. A natural number $p > 1$ is **prime** if the only natural numbers dividing it are 1 and p.

Thus 7 is prime because its only positive divisors are 1 and 7, but 21 is not prime because 3 and 7 divide 21. For the moment, we accept the following important (dare we say, fundamental) theorem as fact.

Theorem 1.1 (Fundamental Theorem of Arithmetic)**.** *Let n be a natural number. Then there exist primes $p_1, \ldots, p_d$, unique up to reordering, and unique natural numbers $a_1, \ldots, a_d$ such that*

$$n = p_1^{a_1} \cdots p_d^{a_d}.$$

The above is called the **prime factorization** *of n.*

Perhaps we should take a moment to talk about reading mathematics. Often when you read the statement of a theorem for the first time, you will find it hard to understand. Such statements often need to be read many times. A good way to try to understand what a theorem says is to figure out what it says for some concrete examples. Look again at the statement of the Fundamental Theorem of Arithmetic; it is a theorem about natural numbers. What does the theorem say, for example, about the natural number 300? Stripping away all the notation for a moment, it says simply that we can write our natural number as a product of powers of primes. For 300, we can write

$$300 = 3 \cdot 2^2 \cdot 5^2.$$

For a general natural number n, we can't say how many primes we will need. Thus in the statement of the theorem it just says there exist primes $p_1, \ldots, p_d$. For $n = 300$, we had $d = 3$. The theorem also says that, up to reordering, the primes are unique. So we could write $300 = 2^2 \cdot 3 \cdot 5^2$, but there is no way to write 300 without having two factors of 2, two factors of 5, and one factor of 3.

Statements of theorems are often very dense. You can come to understand them better if you read them several times, try to paraphrase them using simpler language, and work out what they say in the context of familiar examples.

1.1.2 Rational numbers and real numbers

Although every integer has an additive inverse in the integers, most integers do not have a multiplicative inverse in the integers. We thus form the set $\mathbb{Q}$ of *rational numbers*. Each x in $\mathbb{Q}$ can be written as a quotient of integers in which the denominator is not zero. As you are no doubt aware, however, the representation of a rational number as a ratio of integers is not unique. For example, $\frac{1}{2}$, $\frac{5}{10}$, and $\frac{-4}{-8}$ all represent the same rational number.

You are, of course, very familiar with addition and multiplication of rational numbers. The set $\mathbb{Q}$ together with these operations forms a *field*. The defining properties of a field are the same as the defining properties of the integers described above except that, in a field, every non-zero element has a *multiplicative inverse*. We summarize in the following definition:

Definition 1.3. A set F that is closed under two operations (addition and multiplication) is a **field** if the following properties are satisfied:

(F1) (Associativity of operations) For all x, y, z in F, $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$.

(F2) (Commutativity of operations) For all x, y in F, $x+y = y+x$ and $xy = yx$.

(F3) (Existence of identities) There is a unique element of F, denoted 0, such that $x + 0 = 0 + x = x$ for all x in F. Furthermore, there is a unique element of F different from 0, denoted 1, such that $x \cdot 1 = 1 \cdot x = x$ for all x in F. 0 is the **additive identity** and 1 is the **multiplicative identity**.

(F4) (Existence of inverses) If x is in F, there exists a unique element of F, denoted $-x$, such that $x + (-x) = (-x) + x = 0$. Furthermore, if x is in F and $x \neq 0$, there exists a unique element of F, denoted x^{-1}, such that $xx^{-1} = x^{-1}x = 1$. $-x$ is the **additive inverse** of x and x^{-1} is the **multiplicative inverse** of x.

(F5) (Distributive property) For all x, y, z in F, $x(y+z) = xy+xz$ and $(x+y)z = xz + yz$.

We use the notation $x - y$ to mean $x + (-y)$ and we use $\frac{x}{y}$ to mean xy^{-1}. Because this list includes all the properties satisfied by operations with integers, all of the results above (Proposition 1.1 and Exercise 1.1) hold in any field as well.

The *real number system* $\mathbb{R}$ is another familiar number system. Defining $\mathbb{R}$ precisely requires considerable care; we defer to Chapter 9. You can think of it as those numbers with finite or infinite decimal representations. For now, we take the real number system as essentially known from calculus. The real numbers form a field that contains the field of rational numbers. Essentially, $\mathbb{R}$ includes the rational numbers together with any number that can be approximated to arbitrary accuracy by rational numbers. The familiar numbers π, e, and $\sqrt{2}$ are examples of real numbers that are not rational; we compute with them by using a decimal approximation with sufficient accuracy for our intended application. The fact that $\mathbb{R}$ contains all numbers that can be approximated by rational numbers and not just the rational numbers means that $\mathbb{R}$ has no "holes." This property of $\mathbb{R}$ is called *completeness*. As a consequence of completeness, $\mathbb{R}$ is the correct number system to use when we are dealing with quantities that we think of as varying along a continuum. It is thus the number system best suited for calculus.

Properties (F1)–(F5) above justify all the algebraic manipulations we perform when we simplify or expand expressions involving rational or real numbers. They also justify all the algebraic manipulations we do when we solve equations.

What do we do when we solve equations? The basic idea, as you well know, is to convert the equation we are trying to solve into an equivalent equation by adding the same thing to both sides or by multiplying both sides by the same non-zero number. The next proposition justifies this approach.

Proposition 1.2. *Let a, b, and c be real numbers.*

(a) $a = b$ if and only if $a + c = b + c$. (Thus we don't change the solutions to an equation if we add the same thing to both sides.)

(b) Suppose $c \neq 0$. $a = b$ if and only if $ca = cb$. (Thus we don't change the solutions to an equation if we multiply both sides by a non-zero quantity.)

Proof. We prove part (a) and leave the proof of part (b) to the reader.

The statement to prove is an *if and only if*, or *biconditional*, statement, and so we must actually prove two things. The first is easy; suppose that $a = b$. Then by simple substitution, $a + c = b + c$.

For the second statement, suppose $a + c = b + c$. Then

$$\begin{aligned}
a &= a + 0 && \text{(by F3)}\\
&= a + (c + (-c)) && \text{(by F4)}\\
&= (a + c) + (-c) && \text{(by F1)}\\
&= (b + c) + (-c) && \text{(by substitution)}\\
&= b + (c + (-c)) && \text{(by F1)}\\
&= b + 0 && \text{(by F4)}\\
&= b && \text{(by F3)},
\end{aligned}$$

as claimed. □

Exercise 1.4. Prove part (b) of Proposition 1.2.

We illustrate the use of Proposition 1.2 to solve a simple linear equation.

Example 1.1. Suppose we want to find a real number x satisfying $3x + 3 = 4$. Let's do the algebra, observing at each step which of the properties (F1)–(F5) we are using.

We begin by adding -3 to both sides of the equation because -3 is the additive inverse of 3. This step is legitimate by part (a) of Proposition 1.2. Of course, when we add -3 to the right-hand side, we do the arithmetic and get 1. When we add -3 to the left-hand side we get

$$\begin{aligned}(3x+3)+(-3) &= 3x+(3+(-3)) && \text{(by F1)}\\ &= 3x+0 && \text{(by F4)}\\ &= 3x && \text{(by F3).}\end{aligned}$$

Our original equation is thus equivalent to the equation $3x = 1$. Next, we want to multiply both sides of the equation by the multiplicative inverse of 3, which we denote by $\frac{1}{3}$. This step is legitimate by part (b) of Proposition 1.2. The left-hand side becomes

$$\begin{aligned}\frac{1}{3}(3x) &= \left(\frac{1}{3}\cdot 3\right)x && \text{(by F1)}\\ &= 1x && \text{(by F4)}\\ &= x && \text{(by F3).}\end{aligned}$$

When we multiply the right-hand side of the equation by $\frac{1}{3}$, we get

$$\frac{1}{3}\cdot 1 = \frac{1}{3},$$

by (F4). Thus the original equation is equivalent to $x = \frac{1}{3}$.

Exercise 1.5. Let x and y be elements of $\mathbb{R}$. Show that if $xy = 0$, then either $x = 0$ or $y = 0$. Here is how you might proceed: Suppose that $xy = 0$ but $x \neq 0$. Show that y must be 0.

Throughout the remaining chapters of this book, you should feel free to do algebra *without* explicitly justifying every step by referring to Properties (F1)–(F5).

1.2 Inequalities

To this point, we have studied arithmetic in $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. In addition to these two operations, we typically define an *order relation* on each set, denoted $<$. For definiteness, let's think of the order relation as defined on $\mathbb{R}$. We then get an order relation on $\mathbb{Z}$ or on $\mathbb{Q}$ by restricting the order on $\mathbb{R}$ to these subsets.

To be an order relation on $\mathbb{R}$, $<$ has to satisfy three properties:

(ORD1) (Comparability) For all x, y in $\mathbb{R}$ with $x \neq y$, either $x < y$ or $y < x$.

(ORD2) (Non-reflexivity) There is no x for which $x < x$.

(ORD3) (Transitivity) For all x, y, z in $\mathbb{R}$, if $x < y$ and $y < z$, then $x < z$.

As is customary, we sometimes write $y > x$ instead of $x < y$, and we use $x \leq y$ (resp., $x \geq y$) to indicate that either $x < y$ (resp., $x > y$) or $x = y$.

The real numbers are, however, more than just a field with an order relation; $\mathbb{R}$ with the familiar order relation is actually an *ordered field*. In an ordered field, the order relation interacts in a certain way with the arithmetic operations.

Definition 1.4. Let F be a field with an order relation $<$. Let P be the set of all x in F satisfying $0 < x$. We call P the set of **positive elements** of F. F with the order relation $<$ is an **ordered field** if the following properties hold:

(OF1) (Trichotomy) For all x in F, precisely one of the following holds:

- (a) x is in P
- (b) $-x$ is in P
- (c) $x = 0$.

(OF2) (Closure under addition) If x and y are in P, then $x + y$ is in P.

(OF3) (Closure under multiplication) If x and y are in P, then xy is in P.

As an illustration of the order axioms, we prove that the square of any real number is non-negative.

Proposition 1.3. *Let F be an ordered field. If x is in F, then either $x^2 = 0$ or x^2 is in P.*

Proof. Let x be an element of our ordered field. By the trichotomy axiom (OF1), either $x = 0$, x is in P, or $-x$ is in P. Thus we consider three cases.

Suppose first that $x = 0$. Precisely the same argument used to prove Proposition 1.1 shows that $x^2 = 0 \cdot 0 = 0$.

Next, suppose x is in P. Then by the closure of the set of positives under multiplication (OF3), $x^2 = x \cdot x$ is in P.

Finally, suppose that $-x$ is in P. Thus by the closure of the set of positives under multiplication, $(-x)^2 = (-x) \cdot (-x)$ is in P. By the same argument that proves part (d) of Exercise 1.1, $(-x)^2 = x^2$. Thus x^2 is in P. Thus in all cases, either $x^2 = 0$ or x^2 is positive, as claimed. $\square$

Exercise 1.6. Let F be an ordered field.

(a) Prove that 1, the multiplicative identity, must be in P and that -1 can not be in P.

(b) Prove that, in an ordered field, there is no element x for which $x^2 = -1$. (For those of you who know something about the complex numbers $\mathbb{C}$, this exercise shows that there is no order relation on $\mathbb{C}$ making it an *ordered* field.)

Again, we don't wish to devote excessive time to proving that all the usual manipulations we do with inequalities are valid. At this point we simply want you to be aware of the defining properties of an order relation and the fact that properties of an ordered field justify the familiar algebraic manipulations we do with inequalities. We do, however, want to present several very important inequalities that we will use extensively throughout the book, especially in the second half. These inequalities involve the absolute value of a real number. Recall,

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

Proposition 1.4. *For all x, y in $\mathbb{R}$,*

(a) $|xy| = |x||y|$*,*

(b) $x^2 = |x|^2$*,*

(c) $x \leq |x|$*.*

Exercise 1.7. Prove Proposition 1.4.

Proposition 1.5. *For all x, y in $\mathbb{R}$,*

(a) (Triangle Inequality) $|x+y| \leq |x| + |y|$*,*

(b) (Reverse Triangle Inequality) $|x-y| \geq ||x| - |y||$*.*

Proof. We first prove part (a). Observe that

$$\begin{aligned} |x+y|^2 &= (x+y)^2 && \text{(by part (b) of Proposition 1.4)} \\ &= x^2 + 2xy + y^2 \\ &= |x|^2 + 2xy + |y|^2 && \text{(by part (b) of Proposition 1.4)} \\ &\leq |x|^2 + 2|xy| + y^2 && \text{(by part (c) of Proposition 1.4)} \\ &= |x|^2 + 2|x||y| + |y|^2 && \text{(by part (a) of Proposition 1.4)} \\ &= (|x| + |y|)^2. \end{aligned}$$

Because $|x+y|$ and $|x| + |y|$ are both non-negative, we may conclude that $|x+y| \leq |x| + |y|$, as claimed.

Next we prove part (b). We write $x = (x-y) + y$ and apply the triangle inequality to obtain

$$|x| = |(x-y) + y| \leq |x-y| + |y|.$$

Rearranging gives $|x-y| \geq |x| - |y|$. We could have started with $y = (y-x) + x$ instead and obtained

$$|x-y| \geq |y| - |x| = -(|x| - |y|).$$

Because $|x-y| \geq |x| - |y|$ and $|x-y| \geq -(|x| - |y|)$ both hold, we conclude that $|x-y| \geq ||x| - |y||$, as claimed. □

We end this section with a fact about the ordered field of real numbers that will be used surprisingly often. The result will strike you as obvious; the proof requires one to understand the rigorous definition of the real number system. Because we are postponing the discussion of the construction of the real number system to the second half of the book, at this point we treat the result as a basic fact.

Proposition 1.6 (Archimedean Property)**.** *Let $x \in \mathbb{R}$ with $x > 0$. Then there exists $N \in \mathbb{N}$ such that $x > \frac{1}{N}$.*

The rational number system also satisfies the Archimedean property, though this is not a particularly deep result; if x is a positive rational number, we can write $x = \frac{m}{n}$ for natural numbers m and n. If $m > 1$, $\frac{m}{n} > \frac{1}{n}$. If $m = 1$,

$$\frac{m}{n} = \frac{1}{n} = \frac{2}{2n} > \frac{1}{2n}.$$

In either case, we have obtained a natural number with the desired property.

1.3 A First Look at Sets and Functions

1.3.1 Sets, elements, and subsets

In mathematics, in order to avoid circular definitions, we must agree to leave a small number of terms undefined. The notion of *set* is one such undefined term. Let S be a set. We use the notation $x \in S$ to mean that *x is an element of S* and $x \notin S$ to mean that x is not an element of S. If S has no elements, we say S is *empty* and write $S = \emptyset$. We say that *T is a subset of S* and write $T \subseteq S$, if every element of T is also an element of S. If T is a subset of S and T is not equal to S, we call T a *proper* subset of S and write $T \subset S$.

We claim that, for any set S, $\emptyset \subseteq S$. Such a claim may initially strike you as strange, but it follows from the definition; it is indeed true that every element of the empty set (for there are none) is in S. Such a statement is often said to be *vacuously true.* When my daughter was a small child, we used to have great fun with vacuously true statements like "every dragon living under my bed likes cheesy potato chips."

Example 1.2. The elements of a set may be numbers, but they could be anything really, such as functions, matrices, other sets, etc. For example, consider $S = \{0, 1\}$. We can form a new set $\mathcal{P}(S)$, called the *power set* of S, consisting of all subsets of S. Thus

$$\mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}.$$

Exercise 1.8. Carefully explain the difference between the two sets $\emptyset$ and $\{\emptyset\}$.

Exercise 1.9. If $T = \{a, b, c\}$, find $\mathcal{P}(T)$, the set of all subsets of T.

Rather than listing the elements of a set, we can define a set by specifying the identifying property the elements satisfy. For example,

$$S = \{n \in \mathbb{Z} : 0 \le n \le 3\}$$

is an alternate way to describe the set $\{0, 1, 2, 3\}$.

1.3.2 Operations with sets

Given two sets S and T, there are several ways we can combine them to obtain a new set. We define

$$\begin{aligned} S \cup T &= \{x : x \in S \text{ or } x \in T\} \\ S \cap T &= \{x : x \in S \text{ and } x \in T\} \\ T^c &= \{x : x \notin T\} \\ S \setminus T &= \{x : x \in S \text{ and } x \in T^c\}. \end{aligned}$$

Note that the *or* we use in math is the *inclusive or*; thus we interpret the definition of $S \cup T$ above to mean that elements in both S and T are included in $S \cup T$. $S \cup T$ is called the *union* of S and T and $S \cap T$ is called the *intersection* of S and T. T^c is called the *complement* of T.

1.3.3 Special subsets of $\mathbb{R}$: intervals

For certain kinds of sets that we encounter frequently, it is convenient to have simpler notation. Thus we define *intervals* in $\mathbb{R}$.

Definition 1.5. Let $a, b \in \mathbb{R}$ with $a < b$. Then we define the **open interval** (a, b) to be

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

and we define the **closed interval** $[a, b]$ to be

$$[a, b] = \{x \in \mathbb{R} : a \le x \le b\}.$$

We also define half-open intervals:

$$[a, b) = \{x \in \mathbb{R} : a \le x < b\}$$

and

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

We also allow a or b to be infinite, writing (a, ∞) for $\{x \in \mathbb{R} : x > a\}$, $(-\infty, b]$ for $\{x \in \mathbb{R} : x \le b\}$, etc.

Example 1.3. Let $A = (0, 2)$ and $B = [1, 3]$. We want to describe $A \cup B$ and $A \cap B$.

Let x denote a real number. $x \in A$ if

$$0 < x < 2,$$