Contents

Preface

This book contains an introduction to mathematical proofs, including fundamental material on logic, proof methods, set theory, number theory, relations, functions, cardinality, and the real number system. The book can serve as the main text for a proofs course taken by undergraduate mathematics majors. No specific prerequisites are needed beyond familiarity with high-school algebra. Most readers are likely to be college sophomores or juniors who have taken calculus and perhaps some linear algebra, but we do not assume any knowledge of these subjects. Anyone interested in learning advanced mathematics could use this text for self-study.

Structure of the Book

This book evolved from classes given by the author over many years to students at the College of William and Mary, Virginia Tech, and the United States Naval Academy. I have divided the book into eight chapters and 54 sections, including three review sections. Each section corresponds very closely to the material I cover in a single 50-minute lecture. Sections are further divided into many short subsections, so that my suggested pacing can readily be adapted for classes that meet for 75 minutes, 80 minutes, or other time intervals. If the instructor omits all sections and topics designated as optional, it should be just possible to finish all of the core material in a semester class that meets for 2250 minutes (typically forty-five 50-minute meetings or thirty 75-minute meetings). More suggestions for possible course designs appear below.

I have tried to capture the best features of live mathematics lectures in the pages of this book. New material is presented to beginning students in small chunks that are easier to digest in a single reading or class meeting. The book maintains the friendly conversational style of a classroom presentation, without relinquishing the necessary level of precision and rigor. Throughout this text, you will find the personal pronouns "I" (the author), "you" (the reader), and "we" (the author and the reader, working together), reminding us that teaching and learning are fundamentally human activities. Teaching this material effectively can be as difficult as learning it, and new instructors are often unsure how much time to spend on the fundamentals of logic and proof techniques. The organization of this book shows at a glance how one experienced teacher of proofs allocates time among the various core topics. The text develops mathematical ideas through a continual cycle of examples, theorems, proofs, summaries, and reviews. A new concept may be introduced briefly via an example near the end of one section, then examined in detail in the next section, then recalled as needed in later sections. Every section ends with an immediate review of the key points just covered, and three review sections give detailed summaries of each major section of the book. The essential core material is supplemented by more advanced topics that appear in clearly labeled optional sections.

Contents of the Book

Here is a detailed list of the topics covered in each chapter of the book.

1. **Logic:** propositions, logical connectives (NOT, AND, OR, XOR, IF, IFF), truth tables, logical equivalence, tautologies, contradictions, universal and existential quantifiers, translating and denying complex logical statements, uniqueness.

2. **Proofs:** ingredients in mathematical theories (definitions, axioms, inference rules, theo-

rems, proofs), proof by example, direct proof, contrapositive proof, contradiction proof, proof by cases, generic-element proofs, proofs involving multiple quantifiers.

3. **Set Theory:** set operations (union, intersection, set difference), subset proofs, set equality proofs, circle proofs, chain proofs, power sets, ordered pairs, product sets, unions and intersections of indexed collections.

4. **Integers:** recursive definitions, ordinary induction proofs, induction starting anywhere, backwards induction, strong induction, integer division with remainder, greatest common divisors, Euclid's GCD algorithm, primes, existence and uniqueness of prime factorizations.

5. **Relations and Functions:** relations, images, inverse of a relation, identity relation, composition of relations, formal definition of a function, function equality, operations on functions (pointwise operations, composition, restriction), direct images, preimages, injections, surjections, bijections, inverse functions.

6. **Equivalence Relations and Partial Orders:** reflexivity, symmetry, transitivity, equivalence relations, congruence modulo n, equivalence classes, set partitions, antisymmetry, partial orders, well-ordered sets.

7. **Cardinality:** finite sets, basic counting rules, countably infinite sets, countable sets, theorems on countability, uncountable sets, Cantor's Theorem.

8. **Real Numbers (Optional):** ordered field axioms for $\mathbb{R}$, algebraic properties, formal definition of $\mathbb{N}$ and $\mathbb{Z}$ and $\mathbb{Q}$, ordering properties, absolute value, distance, Least Upper Bound Axiom and its consequences (Archimedean ordering of $\mathbb{R}$, density of $\mathbb{Q}$ in $\mathbb{R}$, existence of real square roots, Nested Interval Theorem).

Possible Course Designs

A standard three-credit (2250 minute) proofs class could cover most of the topics in Chapters 1 through 7, which are essential for further study of advanced mathematics. When pressed for time, I have sometimes omitted or condensed the material on cardinality (Chapter 7) or prime factorizations (last half of Chapter 4). Many variations of the standard course are also feasible. Instructors wishing to preview ideas from abstract algebra could supplement the standard core with the following optional topics:

- the group axioms (end of Section 2.1);
- unique factorization properties for $\mathbb{Z}$ and $\mathbb{Q}$ (last four sections of Chapter 4);
- formal construction of the integers mod n and the rational numbers using equivalence relations (Section 6.6);
- algebraic properties of $\mathbb{R}$ developed from the ordered field axioms (Sections 8.1, 8.2, 8.3, and possibly 8.4).

A course introducing ideas from advanced calculus could include these topics:

- how to prove statements containing multiple quantifiers (Sections 2.6 and 2.7);
- general unions and intersections (Section 3.6);
- properties of preimages of sets under functions (Section 5.7);

- countable and uncountable sets (Sections 7.2, 7.3, and 7.4);
- rigorous development of the real numbers (and related number systems) from the ordered field axioms (Chapter 8).

A quarter-long (1500 minute) course focusing on basic proof methods might only cover Chapter 1, Chapter 2, and the early sections in Chapters 3 through 6. A quarter course on set theory, aimed at students with some prior familiarity with logic and proofs, might cover all of Chapters 3, 5, 6, and 7.

Topics can also be studied in several different orders. Chapter 1 on logic *must* come first, and Chapter 2 on proof methods *must* come second. Thereafter, some flexibility is possible. Chapter 4 (on induction and basic number theory) can be covered before Chapter 3 (on sets) or omitted entirely. Chapter 6 (on equivalence relations) can be covered before the last five sections of Chapter 5 (on functions). Chapter 7 (on cardinality) requires material from Chapter 5 on bijections, but it does not rely heavily on Chapter 6. Finally, the optional Chapter 8 (axiomatic development of the real numbers) could be covered anytime after Chapter 2, with minor adjustments to avoid explicit mention of functions and relations. However, Chapter 8 is more challenging than it may appear at first glance. We are all so familiar with basic arithmetic and algebraic facts about real numbers that it requires considerable intellectual discipline to deduce these facts from the axioms without accidentally using a property not yet proved. Nevertheless, it is rewarding and instructive (albeit somewhat tedious) to work through this logical development of $\mathbb{R}$ if time permits.

Book's Approach to Key Topics

This book adopts a methodical, detailed, and highly structured approach to teaching proof techniques and related mathematical topics. We start with basic logical building blocks and gradually assemble these ingredients to build more complex concepts. To give you a flavor of the teaching philosophy used here, the next few paragraphs describe my approach to explaining four key topics: proof-writing, functions, multiple quantifiers, and induction.

Skills for Writing Proofs

Like any other complex task, the process of writing a proof requires the synthesis of many small atomic skills. Every good proofs textbook develops the fundamental skill of breaking down a statement to be proved into its individual logical constituents, each of which contributes certain structure to the proof. For example, to begin a direct proof of a conditional statement "If P, then Q," we write: "Assume P is true; we must prove Q is true." I explain this particular skill in great detail in this text, introducing explicit *proof templates* for dealing with each of the logical operators.

But there are other equally crucial skills in proof-writing: memorizing and expanding definitions; forming useful denials of complex statements; identifying the logical status of each statement and variable in a proof via appropriate status words; using known universal and existential statements in the correct way; memorizing and using previously proved theorems; and so on. I cover each of these skills on its own, in meticulous detail, before assembling the skills to build increasingly complex proofs. Remarkably, this reduces the task of writing many basic proofs into an almost completely automatic process. It is very rewarding to see students gain confidence and ability as they master the basic skills one at a time and thereby develop proficiency in proof-writing.

Here is an example to make the preceding ideas concrete. Consider a typical practice problem for beginning proof writers: *prove that for all integers x, if x is odd then $x+5$ is* *even.* In the proof below, I have annotated each line with the basic skill needed to produce that line.

Line in Proof	*Skill Needed*
1. Let x_0 be a fixed, arbitrary integer.	Prove $\forall$ statement using generic element.
2. Assume x_0 is odd; prove $x_0 + 5$ is even.	Prove an IF statement by direct proof.
3. We assumed there is $k \in \mathbb{Z}$ with $x_0 = 2k + 1$.	Expand a memorized definition.
4. We'll prove there is $m \in \mathbb{Z}$ with $x_0 + 5 = 2m$.	Expand a memorized definition.
5. Doing algebra on the assumption gives:	Use logical status words.
6. $x_0 + 5 = (2k + 1) + 5 = 2k + 6 = 2(k + 3)$.	Do basic algebraic manipulations.
7. Choose $m = k + 3$, so $x_0 + 5 = 2m$ holds.	Prove $\exists$ statement by giving an example.
8. Note m is in $\mathbb{Z}$, being the sum of two integers.	Verify a variable is in the required set.

Virtually every line in this proof is generated automatically using memorized skills; only the manipulation in line 6 requires a bit of creativity to produce the multiple of 2. Now, while many texts present a proof like this one, we seldom see a careful explanation of how the proof uses an assumed existential statement (line 3) to prove another existential statement (line 4) by *constructing an example* (lines 6 and 7) depending on the variable k in the assumption. This explanation may seem unnecessary in such a simple setting. But it is a crucial ingredient in understanding harder proofs in advanced calculus involving limits and continuity. There we frequently need to use an assumed multiply-quantified IF-statement to prove another multiply-quantified IF-statement. These proofs become much easier for students if they have already practiced the skill of using one quantified statement to prove another quantified statement in more elementary cases.

Similarly, there is not always enough prior coverage of the skill of *memorizing* and *expanding* definitions (needed to generate lines 3 and 4). This may seem to be a minor point, but it is in fact essential. Before writing this proof, students *must* have memorized the definition stating that "x is even" means "there exists $k \in \mathbb{Z}$ with $x = 2k$." But to generate line 4 from this definition, k must be replaced by a new variable m (since k was already given a different meaning in line 3), and x must be replaced by the expression x_0+5. I devote many pages to in-depth coverage of these separate issues, before integrating these skills into full proofs starting in Section 2.2.

Functions

A key topic in a proofs course is the rigorous definition of a function. A function is often defined to be a set of ordered pairs no two of which have the same first component. This definition is logically acceptable, but it causes difficulties later when studying concepts involving the codomain (set of possible outputs) for a function. Since the codomain cannot be deduced from the set of ordered pairs, great care is needed when talking about concepts that depend on the codomain (like surjectivity or the existence of a two-sided inverse). Furthermore, students accustomed to using the function notation $y = f(x)$ find the ordered pair notation $(x, y) \in f$ jarring and unpalatable. My approach includes the domain and codomain as part of the technical definition of a function; the set of ordered pairs by itself is called the *graph* of the function. This terminology better reflects the way most of us conceptualize functions and their graphs. The formal definition in Section 5.4 is preceded by carefully chosen examples (involving arrow diagrams, graphs in the Cartesian plane, and formulas) to motivate and explain the key elements of the technical definition. We introduce the standard function notations $y = f(x)$ and $f : X \to Y$ without delay, so students do not get bogged down with ordered triples and ordered pairs. Then we describe exactly what must be checked when a new function is introduced: single-valuedness and the fact that every x in the domain X has an associated output *in the claimed codomain* Y. We conclude with examples of formulas that do or do not give well-defined functions.

Multiple Quantifiers

A hallmark of this book is its extremely careful and explicit treatment of logical quantifiers: $\forall$ ("for all") and $\exists$ ("there exists"). The placement and relative ordering of these quantifiers has a big impact on the meaning of a logical statement. For example, the true statement $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, y > x$ ("for every integer x there is a larger integer y") asserts something very different from the false statement $\exists y \in \mathbb{Z}, \forall x \in \mathbb{Z}, y > x$ ("there exists an integer y larger than every integer x"). However, these doubly-quantified examples do not reveal the full complexity of statements with three or more nested quantifiers. Such statements are quite common in advanced calculus, as mentioned aerlier.

I give a very detailed explanation of multiple quantifiers in Sections 2.6 and 2.7. After examining many statements containing two quantifiers, I introduce more complicated statements with as many as six quantifiers, focusing on the structural outline of proofs of such statements. Using these big examples is the best way to explain the main point: an existentially quantified variable may only depend on quantified variables *preceding* it in the given statement. Other examples examine disproofs of multiply-quantified statements, where the proof-writer must first form a useful denial of the given statement (which interchanges existential and universal quantifiers). Many exercises develop these themes using important definitions from advanced calculus such as continuity, uniform continuity, convergence of sequences, and least upper bounds.

Induction

Another vital topic in a proofs course is mathematical induction. Induction proofs are needed when working with recursively defined entities such as summations, factorials, powers, and sequences specified by a recursive formula. I discuss recursive definitions immediately before induction, and I carefully draw attention to the steps in an induction proof that rely on these definitions. Many expositions of induction do not make this connection explicit, causing some students to stumble at the point in the proof requiring the expansion of a recursive definition (for example, replacing a sum $\sum_{k=1}^{n+1} x_k$ by $[\sum_{k=1}^{n} x_k] + x_{n+1}$).

Induction proofs are often formulated in terms of *inductive sets*: sets containing 1 that are closed under adding 1. Students are told to prove a statement $\forall n \in \mathbb{Z}_{\geq 0}, P(n)$ by forming the set $S = \{n \in \mathbb{Z}_{\geq 0} : P(n) \text{ is true}\}$ and checking that S is inductive. This extra layer of translation confuses many students and is not necessary. Inductive sets do serve an important technical purpose: they provide a rigorous construction of the set of natural numbers as the intersection of all inductive subsets of $\mathbb{R}$. I discuss this advanced topic in the optional final chapter on real numbers (see Section 8.3), but I avoid mentioning inductive sets in the initial treatment of induction. Instead, induction proofs are based on the Induction Axiom, which says that the statements $P(1)$ and $\forall n \in \mathbb{Z}_{\geq 0}, P(n) \Rightarrow P(n+1)$ suffice to prove $\forall n \in \mathbb{Z}_{\geq 0}, P(n)$. This axiom is carefully motivated both with the visual metaphor of a chain of falling dominos and a more formal comparison to previously discussed logical inference rules.

Additional Pedagogical Features

(a) *Section Summaries and Global Reviews.* Every section ends with a concise recap of the key points just covered. Each major part of the text (logic and proofs; sets and integers; relations, functions, and cardinality) ends with a global review summarizing the material covered in that part. These reviews assemble many definitions, theorem statements, and proof techniques in one place, facilitating memorization and mastery of this vast amount of information.

(b) *Avoiding Logical Jargon.* This text avoids ponderous terminology from classical logic (such as conjunction, disjunction, modus ponens, modus tollens, modus tollendo ponens, hypothetical syllogism, constructive dilemma, universal instantiation, and existential instantiation). I use only those terms from logic that are essential for mathematical work (such as tautology, converse, contrapositive, and quantifier). My exposition replaces antiquated Latin phrases like "modus ponens" by more memorable English names such as "the Inference Rule for IF." Similarly, I refer to the *hypothesis* P and the *conclusion* Q of the IF-statement $P \Rightarrow Q$, rather than calling P the antecedent and Q the consequent of this statement.

(c) *Finding Useful Denials.* This is one of the most crucial skills students learn in a proofs course. Every good textbook states the basic denial rules, but students do not always realize (and texts do not always emphasize) that the rules must be applied *recursively* to find a denial of a complex statement. I describe this recursive process explicitly in Section 1.5 (see especially the table on page 35). Section 1.6 reinforces this key skill with many solved sample problems and exercises.

(d) *Annotated Proofs.* Advanced mathematics texts often consist of a series of definitions, theorems, and proofs with little explanation given for how the author found the proofs. This text is filled with explicit annotations showing the reader how we are generating the lines of a proof, why we are proceeding in a certain way, and what the common pitfalls are. These annotations are clearly delineated from the official proof by enclosing them in square brackets. Many sample proofs are followed by commentary discussing important logical points revealed by the proof.

(e) *Disproofs Contrasted with Proofs by Contradiction.* A very common student mistake is to confuse the disproof of a false statement P with a proof by contradiction of a true statement Q. This mistake occurs because of inattention to logical status words: the disproof of P begins with the goal of *proving* a denial of P, whereas a proof of Q by contradiction begins by *assuming* the denial of Q. We explicitly warn readers about this issue in Remark 2.60.

(f) *Set Definitions.* New sets and set operations are often defined using set-builder notation. For example, the *union* of sets S and T is defined by writing $S \cup T = \{x : x \in S \text{ or } x \in T\}$. This book presents these definitions in a format more closely matching how they arise in proofs, by explicitly stating what membership in the new set means. For instance, my definition of set union says that for all sets S and T and all objects x, the *defined term* $\boxed{x \in S \cup T}$ can be replaced by the *definition text* $\boxed{x \in S \text{ or } x \in T}$ at any point in a proof. This is exactly what the previous definition means, of course, but the extra layer of translation inherent in the set-builder notation causes trouble for many beginning students.

(g) *Careful Organization of Optional Material.* Advanced material and additional topics appear in clearly labeled optional sections. This organization provides maximum flexibility to instructors who want to supplement the material in the standard core, while signaling to readers what material may be safely skipped.

Exercises, Errata, and Feedback

The book contains more than 1000 exercises of varying scope and difficulty, which may be assigned as graded homework or used for self-study or review. Solutions and hints for selected exercises will be posted on the book's website:

```
https://www.math.vt.edu/people/nloehr/prfbook.html
```

I welcome your feedback about any aspect of this book, most particularly corrections of any errors that may be lurking in the following pages. Please send such communications to me by email at `nloehr@vt.edu`. I will post errata and other pertinent information on the book's website.

Words of Thanks

Some pedagogical elements of this book were suggested by the exposition in *A Transition to Advanced Mathematics* by Smith, Eggen, and St. Andre. My debt to this excellent text will be evident to anyone familiar with it. My development as a mathematician and a writer has also been deeply influenced by the superb works of James Munkres, Joseph Rotman, J. Donald Monk, and the other authors listed in the Suggestions for Further Reading (see page 383). I thank all the editorial staff at CRC Press, especially Bob Ross and Jose Soto, and the anonymous reviewers whose comments greatly improved the quality of my original manuscript.

I am grateful to many students, colleagues, friends, and family members who supported me during the preparation of this book. I especially thank my father Frank Loehr, my mother Linda Lopez, my stepfather Peter Lopez, Tony Mendes, Elizabeth Niese, Bill Floyd, Leslie Kay, and the students who took proofs classes from me over the years. Words cannot express how much I learned about teaching proofs from my students. Thank you all!

Very respectfully,
Nick Loehr