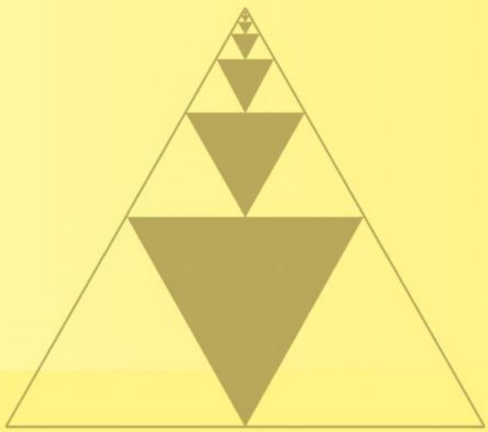
Matthias Beck
Ross Geoghegan

UNDERGRADUATE TEXTS IN MATHEMATICS

The Art of Proof

Basic Training for Deeper Mathematics



Springer

Matthias Beck • Ross Geoghegan

The Art of Proof

Basic Training for Deeper Mathematics

Springer

Matthias Beck
Department of Mathematics
San Francisco State University
San Francisco, CA 94132
USA
beck@math.sfsu.edu

Ross Geoghegan
Department of Mathematical Sciences
Binghamton University
State University of New York
Binghamton, NY 13902
USA
ross@math.binghamton.edu

ISSN 0172-6056
ISBN 978-1-4419-7022-0 e-ISBN 978-1-4419-7023-7
DOI 10.1007/978-1-4419-7023-7
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010934105

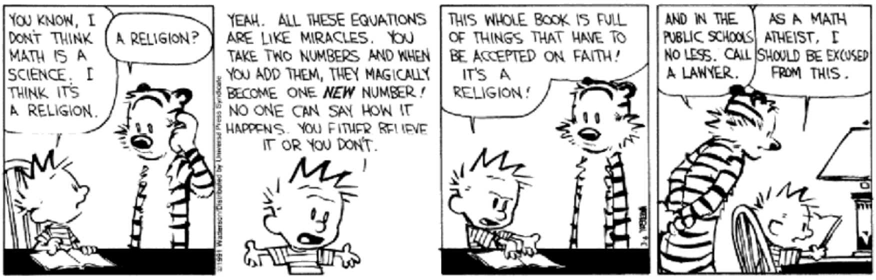
Mathematics Subject Classification (2010): 00A05, 00A35

Printed on acid-free paper

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

Contents

Notes for the Student



You have been studying important and useful mathematics since the age of three. Most likely, the body of mathematics you know can be described as Sesame-Street-through-calculus. This is all good and serious mathematics—from the beautiful algorithm for addition, which we all learned in elementary school, through high-school algebra and geometry, and on to calculus.

Now you have reached the stage where the details of what you already know have to be refined. You need to understand them from a more advanced point of view. We want to show you how this is done. We will take apart what you thought you knew (adding some new topics when it seems natural to do so) and reassemble it in a manner so clear that you can proceed with confidence to deeper mathematics—algebra, analysis, combinatorics, geometry, number theory, statistics, topology, etc.

Actually, we will not be looking at everything you know—that would take too long. We concentrate here on numbers: integers, fractions, real numbers, decimals, complex numbers, and cardinal numbers. We wish we had time to do the same kind of detailed examination of high-school geometry, but that would be another book, and, as mathematical training, it would only teach the same things over again. To put that last point more positively: once you understand what we are teaching in this book—in this course—you will be able to apply these methods and ideas to other parts of mathematics in future courses.

The topics covered here form part of the standard "canon" that everyone trained in mathematics is assumed to know. Books on the history of mathematics, for example, *Mathematics and Its History* (by J. Stillwell, Springer, 2004) and *Math Through the Ages* (by W. P. Berlinghoff and F. Q. Gouvea, Oxton House, 2002), discuss who first discovered or introduced these topics. Some go back hundreds of years; others were developed gradually, and reached their presently accepted form in the early twentieth century. We should say clearly that no mathematics in this book originates with us.

On first sight you may find this book unusual, maybe even alarming. Here is one comment we received from a student who used a test version:

> The overall feel of the book is that it is very "bare bones"; there isn't much in the way of any additional explanations of any of the concepts. While this is nice in the sense that the definitions and axioms are spelled right out without anything getting in the way, if a student doesn't initially understand the concepts underlying the sentence, then they're screwed. As it stands, the book seems to serve as a supplement to a lecture, and not entirely as a stand-alone learning tool.

This student has a point, though we added more explanations in response to comments like this. We intend this book to be supplemented by discussion in an instructor's class. If you think about what is involved in writing any book of instruction you will realize that the authors had better be clear about the intended readership and the way they want the book to be used. While we do believe that *some* students can use this book for self-study, our experience in using this material—experience stretching over twenty-five years—tells us that this will not work for everyone. So please regard your instructor as Part 3 of this book (which comes in two parts), as the source for providing the insights we did not—indeed, could not—write down.

We are active research mathematicians, and we believe, for ourselves as well as for our students, that learning mathematics through oral discussion is usually easier than learning mathematics through reading, even though reading and writing are necessary in order to get the details right. So we have written a kind of manual or guide for a semester-long discussion—inside and outside class.

Please read the *Notes for Instructors* on the following pages. There's much there that's useful for you too. And good luck. Mathematics is beautiful, satisfying, fun, deep, and rich.

Notes for Instructors

Logic moves in one direction, the direction of clarity, coherence and structure. Ambiguity moves in the other direction, that of fluidity, openness, and release. Mathematics moves back and forth between these two poles. [...] It is the interaction between these different aspects that gives mathematics its power.
William Byers (*How Mathematicians Think*, Princeton University Press, 2007)

This book is intended primarily for students who have studied calculus or linear algebra and who now wish to take courses that involve theorems and proofs in an essential way. The book is also for students who have less background but have strong mathematical interests.

We have written the text for a one-semester or two-quarter course; typically such a course has a title like "Gateway to Mathematics" or "Introduction to proofs" or "Introduction to Higher Mathematics." Our book is shorter than most texts designed for such courses. Our belief, based on many years of teaching this type of course, is that the roles of the instructor and of the textbook are less important than the degree to which the student is invited/requested/required to do the hard work.

Here is what we are trying to achieve:

1. To show the student some important and interesting mathematics.
2. To show the student how to read and understand statements and proofs of theorems.
3. To help the student discover proofs of stated theorems, and to write down the newly discovered proofs correctly, and in a professional way.
4. To foster in the student something as close as feasible to the experience of doing research in mathematics. Thus we want the student to actually discover theorems and write down correct and professional proofs of those discoveries. This is different from being able to write down proofs of theorems that have been pre-certified as true by us (in the text) or by the instructor (in class).

Once the last of these has been achieved, the student is a mathematician. We have no magic technique for getting the student to that point quickly, but this book might serve as a start.

Many books intended for a gateway course are too abstract for our taste. They focus on the different types of proofs and on developing techniques for knowing when to use each method. We prefer to start with useful mathematics on day one, and to let the various methods of proof, definition, etc., present themselves naturally as they are needed in context.

Here is a quick indication of our general philosophy:

On Choice of Material

We do not start with customary dry chapters on "Logic" and "Set Theory." Rather we take the view that the student is intelligent, has considerable prior experience with mathematics, and knows, from common sense, the difference between a logical deduction and a piece of nonsense (though some training in this may be helpful!). To defuse fear from the start, we tell the student, "A theorem is simply a sentence expressing something true; a proof is just an explanation of why it is true." Of course, that opens up many other issues of method, which we gradually address as the course goes on.

We say to the student something like the following: "You have been studying important and useful mathematics since the age of three; the body of mathematics you know is Sesame-Street-through-calculus. Now it's time to revisit (some of) that good mathematics and to get it properly organized. The very first time most of you heard a theorem proved was when you asked some adult, Is there a biggest number? (What answer were you given? What would you answer now if a four-year-old asked you that question?) Later on, you were taught to represent numbers in base 10, and to add and multiply them. Did you realize how much is buried behind that (number systems, axioms, algorithms, . . .)? We will take apart what you thought you knew, and we will reassemble it in a manner so clear that you can proceed with confidence to deeper mathematics."

The Parts of the Book

The material covered in this book consists of two parts of equal size, namely a discrete part (integers, induction, modular arithmetic, finite sets, etc.) and a continuous part (real numbers, limits, decimals, infinite cardinal numbers, etc.) We recommend that both parts be given equal time. Thus the instructor should resist the temptation to let class discussion of Part 1 slide on into the eighth week of a semester. Some discipline concerning homework deadlines is needed at that point too, so that students will give enough time and attention to the second half. (The instructor who ignores this advice will probably come under criticism from colleagues: this course is often a prerequisite for real analysis.) Still, an instructor has much freedom on how to go through the material. For planning purposes, we include below a diagram showing the section dependencies.

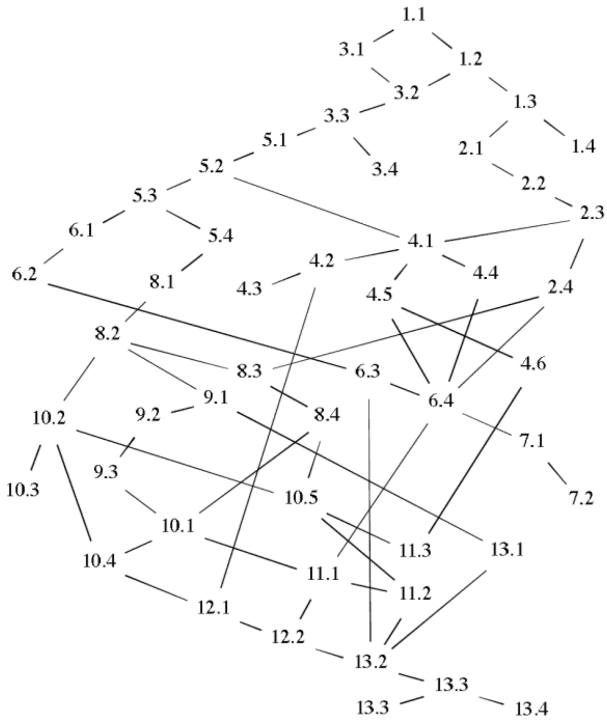


Fig. 0.1 The partially ordered set of section dependencies.

To add flexibility and material for later reading, we end the book with a collection of further topics, for example Cayley graphs of groups and public-key encryption. These additional chapters are independent of each other and can be inserted in the course as desired. They should also be suitable for student presentations in class.

Problems

There are three kinds of exercises for students in this book:

1. The main body of the text consists of *propositions* (called *theorems* when they are particularly important), in which the mathematics is developed. In principle, these propositions are meant to be proved by the students; however, proving *all* of them is likely to be overwhelming, so the instructor must exercise judgment. Besides this, some of the propositions are proved in the text to give the student a feel for how to develop a proof of a certain statement, and also to introduce different proof methods. Of the remaining propositions, we tend to prove roughly half in class on the blackboard and give the other half as homework problems.

   Upon request (see `www.springer.com/instructors`), the instructor can obtain a free copy of this book (in PDF format) in which most proofs are worked out in detail.

2. There are also exercises called *projects*. These are more exploratory, sometimes open-ended, problems for the students to work on. They vary greatly in difficulty—some are more elementary than the propositions, some concern unsolved conjectures, and some are writing projects intended to foster exploration by the students. We would encourage students to do these in groups. Some could be the basis for an outside-class pizza party, one project per party. The further topics at the end of the book also lend themselves to group projects.

3. We start every chapter with an introductory project labeled *Before You Get Started*. These are meant to be more writing intensive than the *projects* in the main text. They typically invite the students to reflect on what they already know from previous classes as a lead-in to the chapter. These introductory projects encourage the student to be creative by thinking about a topic before formally studying it.

On Grading Homework—The Red-Line Method

It is essential that the student regularly hand in written work and get timely feedback. One method of grading that we have found successful lessens the time-burden on the instructor and puts the responsibility on the shoulders of the student. It works like this:

Certain theorems in the book are assigned by the instructor: proofs are to be handed in. The instructor reads a proof until a (real) mistake is found—this might be a sentence that is false or a sentence that has no meaning. The instructor draws a red line under that sentence and returns the proof to the student at the next meeting. No words are written on the paper by the instructor: it is the student's job to figure out why the red line was put there. Pasting as necessary so as not to have to rewrite the correct part—the part above the red line—the student then hands in a new version, and the process of redlining is repeated until the proof is right.

The instructor will decide on the details of this method: how many rewrites to allow, and whether to give the same credit for a successful proof on the sixth attempt as on the first. Another issue that arises is how to handle students' questions about red lines in office hours. Some instructors will want to explain to the students why the red line was drawn. Another approach, which we have found successful, is to have the student read the proof aloud, sentence by sentence. Almost always, when the student reaches the redlined sentence it becomes clear what the issue is.

In all this we are not looking for perfection of expression—that will hopefully come with time. We start with the attitude that a proof is just an explanation of why something is true, and the student should come to understand that a confused explanation is no more acceptable in mathematics than in ordinary life. But the red line should be reserved for real mistakes of thought. To put this another way, the student needs to believe that writing correct mathematics is not an impossible task. We should be teaching rigor, but not *rigor mortis*.

We sometimes say in class that we will read the proof as if it were a computer program: if the program does not run, there must be some first line where the trouble occurs. That is where the red line is.

If you open a mathematics book in the library, you usually will not see a list of axioms on the first page, but they are present implicitly: the author is assuming knowledge of more basic mathematics that rests on axioms known to the reader.

We begin by writing down a list of properties of the integers that your previous experience will tell you ought to be considered to be true, things you always believed anyway. We call these properties *axioms*. Axioms are statements that form the starting point of a mathematical discussion; items that are assumed (by an agreement between author and reader) without question or deeper analysis. Once the axioms are settled, we then explore how much can be logically deduced from them. A mathematical theory is rich if a great deal can be deduced from a few primitive (and intuitively acceptable) axioms.

In short, we have to start somewhere. The axioms in one course may in fact be theorems in a deeper course whose axioms are more primitive. The list of axioms is simply a clearly stated starting point.

1.1 Axioms

You might ask, how is a set defined? We will use the word intuitively: a set is a collection of "things" or elements or members. We will say more about this in Chapter 5.

We assume there is a set, denoted by $\mathbf{Z}$, whose members are called **integers**. This set $\mathbf{Z}$ is equipped with binary operations called **addition**, $+$, and **multiplication**, $\cdot$, satisfying the following five axioms, as well as Axioms 2.1 and 2.15 to be introduced in Chapter 2. (A **binary operation** on a set S is a procedure that takes two elements of S as input and gives another element of S as output.)

Axiom 1.1. *If m, n, and p are integers, then*

(i) $m+n=n+m$. *(commutativity of addition)*

(ii) $(m+n)+p=m+(n+p)$. *(associativity of addition)*

(iii) $m\cdot(n+p)=m\cdot n+m\cdot p$. *(distributivity)*

(iv) $m\cdot n=n\cdot m$. *(commutativity of multiplication)*

(v) $(m\cdot n)\cdot p=m\cdot(n\cdot p)$. *(associativity of multiplication)*

The right-hand side of (iii) should read $(m\cdot n)+(m\cdot p)$. It is a useful convention to always multiply before adding, whenever an expression contains both $+$ and $\cdot$ (unless this order is overridden by parentheses).

Axiom 1.2. *There exists an integer 0 such that whenever $m\in\mathbf{Z}$, $m+0=m$.* *(identity element for addition)*

Axiom 1.3. *There exists an integer 1 such that $1\neq 0$ and whenever $m\in\mathbf{Z}$, $m\cdot 1=m$.* *(identity element for multiplication)*

Axiom 1.4. *For each $m\in\mathbf{Z}$, there exists an integer, denoted by $-m$, such that $m+(-m)=0$.* *(additive inverse)*

Axiom 1.5. *Let m, n, and p be integers. If $m\cdot n=m\cdot p$ and $m\neq 0$, then $n=p$.* *(cancellation)*

The symbols $\in$ and $=$. The symbol $\in$ means **is an element of**—for example, $0 \in \mathbf{Z}$ means "0 is an element of the set $\mathbf{Z}$." The symbol "$=$" means **equals**. To say $m = n$ means that m and n are the same number. We note some properties of the symbol "$=$":

(i) $m = m$. *(reflexivity)*

(ii) If $m = n$ then $n = m$. *(symmetry)*

(iii) If $m = n$ and $n = p$ then $m = p$. *(transitivity)*

(iv) If $m = n$, then n can be substituted for m in any statement without changing the meaning of that statement. *(replacement)*

In other textbooks, (i)–(iv) *might form another axiom, alongside axioms for sets. In order to get to interesting mathematics early on, we chose* not *to include axioms on set theory and logic but count on your intuition for what a "set" should be and what it means for two members of a set to be equal.*

An example of (iv): If we know that $m = n$ then we can conclude that $m + p = n + p$.

The symbol "$\neq$" means **is not equal to**. To say $m \neq n$ means m and n are different numbers. Note that "$\neq$" satisfies symmetry, but not transitivity and reflexivity.

Similarly, the symbol $\notin$ means **is not an element of**.

1.2 First Consequences

At this point, the only facts we consider known about the integers are Axioms 1.1–1.5. In the language of mathematics, the axioms are **true** or are **facts**. Every time we prove that some statement follows logically from the axioms we are proving that it too is true, just as true as the axioms, and from then on we may add it to our list of facts. Once we have established that the statement is a fact (i.e., is true) we may use it in later logical arguments: it is as good as an axiom because it follows from the axioms.

What is truth? That is for the philosophers to discuss. Mathematicans try to avoid such matters by the axiomatic method*: in mathematics a statement is considered true if it follows logically from the agreed axioms.*

From now on, we will use the common notation mn to denote $m \cdot n$. We start with some propositions that show that our axioms still hold when we change the orders of some terms:

Proposition 1.6. *If m, n, and p are integers, then $(m+n)p = mp + np$.*

Here is a proof of Proposition 1.6. Let $m, n, p \in \mathbf{Z}$. The left-hand side $(m+n)p$ of what we are trying to prove equals $p(m+n)$ by Axiom 1.1(iv). Now we may use Axiom 1.1(iii) to deduce that $p(m+n) = pm + pn$. Finally, we use Axiom 1.1(iv) again: $pm = mp$ and $pn = np$. In summary we have proved:

$$(m+n)p \overset{\text{Ax.1.1(iv)}}{=} p(m+n) \overset{\text{Ax.1.1(iii)}}{=} pm + pn \overset{\text{Ax.1.1(iv)}}{=} mp + np,$$

that is, $(m+n)p = mp + np$. □

We use □ to mark the end of a proof.

Proposition 1.16. *If m and n are even integers, then so are $m+n$ and mn.*

Proposition 1.17.

(i) 0 *is divisible by every integer.*

(ii) *If m is an integer not equal to* 0*, then m is not divisible by* 0*.*

Thus the integer 1 mentioned in Axiom 1.3 is the unique solution of the equation $mx = m$.

Proposition 1.18. *Let $x \in \mathbf{Z}$. If x has the property that for all $m \in \mathbf{Z}$, $mx = m$, then $x = 1$.*

Proposition 1.19. *Let $x \in \mathbf{Z}$. If x has the property that for some nonzero $m \in \mathbf{Z}$, $mx = m$, then $x = 1$.*

This is another if–then statement: *if* statement ♡ is true *then* statement ♣ is true as well. Statement ♡ here is "x has the property that for some nonzero $m \in \mathbf{Z}$, $mx = m$," and statement ♣ is "$x = 1$." Again, the setup of our proof will be this: assume ♡ is true; then try to show that ♣ follows.

Proof of Proposition 1.19. We assume (in addition to what we already know from previous propositions and the axioms) that somebody gives us an $x \in \mathbf{Z}$ and the information that there is some nonzero $m \in \mathbf{Z}$ for which $mx = m$. We first use Axiom 1.3:

$$m \cdot x = m = m \cdot 1\,,$$

and then apply Axiom 1.5 to the left- and right-hand sides of this last equation (note that $m \neq 0$) to deduce that $x = 1$. In summary, assuming x has the property that $mx = m$ for some nonzero $m \in \mathbf{Z}$, we conclude that $x = 1$, and this proves our if–then statement. □

Here are some more propositions about inverses and cancellation:

Proposition 1.20. *For all $m, n \in \mathbf{Z}$, $(-m)(-n) = mn$.*

Proof. Let $m, n \in \mathbf{Z}$. By Axiom 1.4,

$$m + (-m) = 0 \qquad \text{and} \qquad n + (-n) = 0\,.$$

Multiplying both sides of the first equation (on the right) by n and the second equation (on the left) by $-m$ gives, after applying Proposition 1.14 on the right-hand sides,

$$(m + (-m))\, n = 0 \qquad \text{and} \qquad (-m)\,(n + (-n)) = 0\,.$$

With Axiom 1.1(iii) and Proposition 1.6 we deduce

$$mn + (-m)n = 0 \qquad \text{and} \qquad (-m)n + (-m)(-n) = 0\,.$$

Index