Mathematical Proofs

Gary Chartrand, Albert D. Polimeni, Ping Zhang

August 2022

Contents

1 Communicating Mathematics

1.1 Learning Mathematics

One of the major goals of this book is to assist you as you progress from an individual who uses mathematics to an individual who understands mathematics. Perhaps this will mark the beginning of you becoming someone who actually develops mathematics of your own. This is an attainable goal if you have the desire.

The fact that you've gone this far in your study of mathematics suggests that you have ability in mathematics. This is a real opportunity for you. Much of the mathematics that you will encounter in the future is based on what you are about to learn here. The better you learn the material and the mathematical thought process now, the more you will understand later. To be sure, any area of study is considerably more enjoyable when you understand it. But getting to that point will require effort on your part.

There are probably as many excuses for doing poorly in mathematics as there are strategies for doing well in mathematics. We have all heard students say (sometimes, remarkably, even with pride) that they are not good at mathematics. That's only an alibi. Mathematics can be learned like any other subject. Even some students who have done well in mathematics say that they are not good with proofs. This, too, is unacceptable. What is required is determination and effort. To have done well on an exam with little or no studying is nothing to be proud of. Confidence based on being well prepared is good, however.

Here is some advice that has worked for several students. First, it is important to understand what goes on in class each day. This means being present and being prepared for every class. After each class, recopy any lecture notes. When recopying the notes, express sentences in your own words and add details so that everything is as clear as possible. If you run into snags (and you will), talk them over with a classmate or your instructor. In fact, it's a good idea (at least in our opinion) to have someone with whom to discuss the material on a regular basis. Not only does it often clarify ideas, it gets you into the habit of using correct terminology and notation.

In addition to learning mathematics from your instructor, solidifying your understanding by careful note-taking and talking with classmates, your textbook is (or at least should be) an excellent source as well. Read your textbook carefully with pen (or pencil) and paper in hand. Make a serious effort to do every homework problem assigned and, eventually, be certain that you know how to solve them. If there are exercises in the textbook that have not been assigned, you might even try to solve these as well. Another good idea is to try to create your own problems. In fact, when studying for an exam, try creating your own exam. If you start doing this for all of your classes, you might be surprised at how good you become. Creativity is a major part of mathematics. Discovering mathematics not only contributes to your understanding of the subject but has the potential to contribute to mathematics itself. Creativity can come in all forms. The following quote is from the well-known writer J. K. Rowling (author of the *Harry Potter* novels).

> *Sometimes ideas just come to me. Other times I have to sweat and almost bleed to make ideas come. It's a mysterious process, but I hope I never find out exactly how it works.*

In her book *Defying Gravity: The Creative Career of Stephen Schwartz from Godspell to Wicked*, Carol de Giere writes a biography of Stephen Schwartz, one of the most

successful composer-lyricists, in which she discusses not only creativity in music but how an idea can lead to something special and interesting and how creative people may have to deal with disappointment. Indeed, de Giere dedicates her book to the *creative spirit within each of us*. While Schwartz wrote the music for such famous shows as *Godspell* and *Wicked*, he discusses creativity head-on in the song "The Spark of Creation," which he wrote for the musical *Children of Eden*. In her book, de Giere writes:

> *In many ways, this song expresses the theme of Stephen Schwartz's life – the naturalness and importance of the creative urge within us. At the same time he created an anthem for artists.*

In mathematics our goal is to seek the truth. Finding answers to mathematical questions is important, but we cannot be satisfied with this alone. We must be certain that we are right and that our explanation for why we believe we are correct is convincing to others. The reasoning we use as we proceed from what we know to what we wish to show must be logical. It must make sense to others, not just to ourselves.

There is joint responsibility here. As writers, it is our responsibility to give an accurate, clear argument with enough details provided to allow the reader to understand what we have written and to be convinced. It is the reader's responsibility to know the basics of logic and to study the concepts involved so that a well-presented argument will be understood. Consequently, in mathematics writing is important, *very* important. Is it *really* important to write mathematics well? After all, isn't mathematics mainly equations and symbols? Not at all. It is not only important to write mathematics well, it is important to write well. You will be writing the rest of your life, at least reports, letters and email. Many people who never meet you will know you only by what you write and how you write.

Mathematics is a sufficiently complicated subject that we don't need vague, hazy and boring writing to add to it. A teacher has a very positive impression of a student who hands in well-written and well-organized assignments and examinations. You want people to enjoy reading what you've written. It is important to have a good reputation as a writer. It's part of being an educated person. Especially with the large number of email letters that so many of us write, it has become commonplace for writing to be more casual. Although all people would probably subscribe to this (since it is more efficient), we should know how to write well, formally and professionally, when the situation requires it.

You might think that considering how long you've been writing and that you're set in your ways, it will be very difficult to improve your writing. Not really. If you want to improve, you can and will. Even if you are a good writer, your writing can always be improved. Ordinarily, people don't think much about their writing. Often just thinking about your writing is the first step to writing better.

1.2 What others have said about writing

Many people who are well known in their areas of expertise have expressed their thoughts about writing. Here are quotes by some of these individuals.

Anything that helps communication is good. Anything that hurts it is bad.

I like words more than numbers, and I always did—conceptual more than computational.

Paul Halmos, mathematician

Writing is easy. All you have to do is cross out all the wrong words.

Mark Twain, author (*The Adventures of Huckleberry Finn*)

You don't write because you want to say something; you write because you've got something to say.

F. Scott Fitzgerald, author (*The Great Gatsby*)

Writing comes more easily if you have something to say.

Scholem Asch, author

Either write something worth reading or do something worth writing.

Benjamin Franklin, statesman, writer, inventor

What is written without effort is in general read without pleasure.

Samuel Johnson, writer

Easy reading is damned hard writing.

Nathaniel Hawthorne, novelist (*The Scarlet Letter*)

Everything that is written merely to please the author is worthless.

The last thing one knows when writing a book is what to put first.

I have made this letter longer because I lack the time to make it short.

Blaise Pascal, mathematician and physicist

The best way to become acquainted with a subject is to write a book about it.

Benjamin Disraeli, prime minister of England

In a very real sense, the writer writes in order to teach himself, to understand himself, to satisfy himself; the publishing of his ideas, though it brings gratification, is a curious anticlimax.

Alfred Kazin, literary critic

The skill of writing is to create a context in which other people can think.

Edwin Schlossberg, exhibit designer

A writer needs three things, experience, observation, and imagination, any two of which, at times any one of which, can supply the lack of the other.

William Faulkner, writer (*The Sound and the Fury*)

If confusion runs rampant in the passage just read,
It may very well be that too much has been said.

So that's what he meant! Then why didn't he say so?

Frank Harary, mathematician

A mathematical theory is not to be considered complete until you have made it so clear that you can explain it to the first man whom you meet on the street.

David Hilbert, mathematician

Everything should be made as simple as possible, but not simpler.

Albert Einstein, physicist

Never let anything you write be published without having had others critique it.

Donald E. Knuth, computer scientist and writer

Some books are to be tasted, others to be swallowed, and some few to be chewed and digested.

Reading maketh a full man, conference a ready man, and writing an exact man.

Francis Bacon, writer and philosopher

Judge an article not by the quality of what is framed and hanging on the wall, but by the quality of what's in the wastebasket.

Anonymous (Quote by Leslie Lamport)

We are all apprentices in a craft where no-one ever becomes a master.

Ernest Hemingway, author (*For Whom the Bell Tolls*)

There are three rules for writing a novel. Unfortunately, no one knows what they are.

W. Somerset Maugham, author (*Of Human Bondage*)

1.3 Mathematical Writing

Most of the quotes given above pertain to writing in general, not to mathematical writing in particular. However, these suggestions for writing apply as well to writing mathematics. For us, mathematical writing means writing assignments for a mathematics course (particularly a course with proofs). Such an assignment might consist of writing a single proof, writing solutions to a number of problems, or perhaps writing a term paper which, more than likely, includes definitions, examples, background *and* proofs. We'll refer to any of these as an "assignment." Your goal should be to write correctly, clearly and in an interesting manner.

Before you even begin to write, you should have already thought about a number of things. First, you should know what examples and proofs you plan to include if this is appropriate for your assignment. You should not be overly concerned about writing good proofs on your first attempt – but be certain that you do have *proofs*.

As you're writing your assignment, you must be aware of your audience. What is the target group for your assignment? Of course, it should be written for your instructor. But it should be written so that a classmate would understand it. As you grow mathematically, your audience will grow with you and you will adapt your writing to this new audience.

Give yourself enough time to write your assignment. Don't try to put it together just a few minutes before it's due. The disappointing result will be obvious to your instructor. And to you! Find a place to write that is comfortable for you: your room, an office, a study room, the library and sitting at a desk, at a table, in a chair. Do what works best for you. Perhaps you write best when it's quiet or when there is background music.

Now that you're comfortably settled and have allowed enough time to do a good job, let's put a plan together. If the assignment is fairly lengthy, you may need an outline, which, most likely, will include one or more of the following:

1. background and motivation
2. definitions to be presented and possibly notation to be used
3. examples to include
4. results to be presented (whose proofs have already been written, probably in rough form)
5. references to other results you intend to use
6. the order of everything mentioned above.

If the assignment is a term paper, it may include extensive background material and may need to be carefully motivated. The subject of the paper should be placed in perspective. Where does it fit in with what we already know?

Many writers write in "spirals." Even though you have a plan for your assignment that includes an ordered list of things you want to say, it is likely that you will reach some point (perhaps sooner than you think) when you realize that you should have included something earlier – perhaps a definition, a theorem, an example, some notation. (This happened to us many times while writing this textbook.) Insert the missing material, start over again and write until once again you realize that something is missing. It is important, as you reread, that you start at the beginning each time. Then repeat the steps listed above.

We are about to give you some advice, some "pointers," about writing mathematics. Such advice is necessarily subjective. Not everyone subscribes to these suggestions on writing. Indeed, writing "experts" don't agree on all issues. For the present, your instructor will be your best guide. But writing does not follow a list of rules. As you mature mathematically, perhaps the best advice about your writing is the same advice given by Jiminy Cricket to Disney's Pinocchio: *Always let your conscience be your guide.* You must be yourself. And one additional piece of advice: Be careful about accepting advice on writing. Originality and creativity don't follow rules. Until you reach the stage of being comfortable and confident with your own writing, however, we believe that it is useful to consider a few writing tips.

Since a number of these writing tips may not make sense (since, after all, we don't even have anything to write yet), it will probably be most useful to return to this chapter periodically as you proceed through the chapters that follow.

1.4 Using Symbols

Since mathematics is a symbol-oriented subject, mathematical writing involves a mixture of words and symbols. Here are several guidelines to which a number of mathematicians subscribe.

1. *Never start a sentence with a symbol.*
   Writing mathematics follows the same practice as writing all sentences, namely that the first word should be capitalized. This is confusing if the

sentence were to begin with a symbol since the sentence appears to be incomplete. Also, in general, a sentence sounds better if it starts with a word. Instead of writing:

$$x^2 - 6x + 8 = 0 \text{ has two distinct roots.}$$

write:

$$\text{The equation } x^2 - 6x + 8 = 0 \text{ has two distinct roots.}$$

2. *Separate symbols not in a list by words if possible.*
Separating symbols by words makes the sentence easier to read and therefore easier to understand. The sentence:

$$\text{With the exception of } a, b \text{ is the only root of } (x-a)(x-b) = 0.$$

would be clearer if it were written as:

With the exception of a, the number b is the only root of $(x-a)(x-b) = 0$.

3. *Except when discussing logic, avoid writing the following symbols in your assignment:*

$$\Rightarrow,\ \forall,\ \exists,\ \ni,\ etc.$$

The first four symbols stand for "implies," "for every," "there exists" and "such that," respectively. You may have already seen these symbols and know what they mean. If so, this is good. It is useful when taking notes or writing early drafts of an assignment to use shorthand symbols but many mathematicians avoid such symbols in their professional writing. (We will visit these symbols later.)

4. *Be careful about using i.e. and e.g.*
These stand for *that is* and *for example,* respectively. There are situations when writing the words is preferable to writing the abbreviations as there may be confusion with nearby symbols. For example, $\sqrt{-1}$ and $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$ are not rational numbers, that is, i and e are not rational numbers.

5. *Write out integers as words when they are used as adjectives and when the numbers are relatively small or are easy to describe in words. Write out numbers numerically when they specify the value of something.*

There are exactly two groups of order 4.
Fifty million Frenchmen can't be wrong.
There are one million positive integers less than 1,000,001.

6. *Don't mix words and symbols improperly.*
Avoid writing:

$$\text{Every integer} \geq 2 \text{ is a prime or is composite.}$$

It is preferable to write:

Every integer exceeding 1 is prime or composite.

or

If $n \geq 2$ is an integer, then n is prime or composite.

Although

Since $(x-2)(x-3)=0$, it follows that $x=2$ or 3.

sounds correct, it is not written correctly. It should be:

Since $(x-2)(x-3)=0$, it follows that $x=2$ or $x=3$.

7. Avoid using a symbol in the statement of a theorem when it's not needed. Don't write:

Theorem *Every bijective function f has an inverse.*

Delete "f." It serves no useful purpose. The theorem does not depend on what the function is called. A symbol should not be used in the statement of a theorem (or in its proof) exactly once. If it is useful to have a name for an arbitrary bijective function in the proof (as it probably will be), then "f" can be introduced there.

8. *Explain the meaning of every symbol that you introduce.*
Although what you intended may seem clear, don't assume this. For example, if you write $n = 2k+1$ and k has never appeared before, then say that k is an integer (if indeed k *is* an integer).

9. *Use "frozen symbols" properly.*
If m and n are typically used for integers (as they probably are), then don't use them for real numbers. If A and B are used for sets, then don't use these as typical elements of a set. If f is used for a function, then don't use this as an integer. Write symbols that the reader would expect. To do otherwise could very well confuse the reader.

10. *Use consistent symbols.*
Unless there is some special reason to the contrary, use symbols that "fit" together. Otherwise, it is distracting to the reader.
Instead of writing:

If x and y are even integers, then $x = 2a$ and $y = 2r$ for some integers a and r.

replace $2r$ by $2b$ (where then, of course, we write "for some integers a and b"). On the other hand, you might prefer to write $x = 2r$ and $y = 2s$.

1.5 Writing Mathematical Expressions

There will be numerous occasions when you will want to write mathematical expressions in your assignment, such as algebraic equations, inequalities and formulas. If these expressions are relatively short, then they should probably be written within the text of the proof or discussion. (We'll explain this in a moment.) If the expressions are rather lengthy, then it is probably preferred for these expressions to be written as "displays."

For example, suppose that we are discussing the Binomial Theorem. (It's not important if you don't recall what this theorem is.) It's possible that what we are writing includes the following passage:

> For example, if we expand $(a+b)^4$, then we obtain $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.

It would probably be better to write the expansion of $(a+b)^4$ as a **display**, where the mathematical expression is placed on a line or lines by itself and is centered. This is illustrated below.

> For example, if we expand $(a+b)^4$, then we obtain
>
> $$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

If there are several mathematical expressions that are linked by equal signs and inequality symbols, then we would almost certainly write this as a display. For example, suppose that we wanted to write $n^3 + 3n^2 - n + 4$ in terms of k, where $n = 2k+1$. A possible display is given next:

Since $n = 2k+1$, it follows that

$$\begin{aligned} n^3 + 3n^2 - n + 4 &= (2k+1)^3 + 3(2k+1)^2 - (2k+1) + 4 \\ &= (8k^3 + 12k^2 + 6k + 1) + 3(4k^2 + 4k + 1) - 2k - 1 + 4 \\ &= 8k^3 + 24k^2 + 16k + 7 = 8k^3 + 24k^2 + 16k + 6 + 1 \\ &= 2(4k^3 + 12k^2 + 8k + 3) + 1. \end{aligned}$$

Notice how the equal signs are lined up. (We wrote two equal signs on one line since that line would have contained very little material otherwise, as well as to balance the lengths of the lines better.)

Let's return to the expression $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$ for a moment. If we were to write this expression in the text of a paragraph (as we are doing) and if we find it necessary to write portions of this expression on two separate lines, then this expression should be broken so that the first line ends with an operation or comparative symbol such as $+$, $-$, $<$, $\geq$ or $=$. In other words, the second line should *not* begin with one of these symbols. The reason for doing this is that ending the line with one of these symbols alerts the reader that more will follow; otherwise, the reader might conclude (incorrectly) that the portion of the expression appearing on the first line is the entire expression. Consequently, write

> For example, if we expand $(a+b)^4$, then we obtain $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.

and not

> For example, if we expand $(a+b)^4$, then we obtain $(a+b)^4 = a^4 + 4a^3b$
> $+ 6a^2b^2 + 4ab^3 + b^4$.

If there is an occasion to refer to an expression that has already appeared, then this expression should have been written as a display and labeled as below:

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4. \qquad \textbf{(1)}$$

Then we can simply refer to expression (1) rather then writing it out each time.

1.6 Common words and phrases in Mathematics

There are some words and phrases that appear so often in mathematical writing that it is useful to discuss them.

1. *I We One Let's*

   I will now show that n is even.
   We will now show that n is even.
   One now shows that n is even.
   Let's now show that n is even.

   These are four ways that we might write a sentence in a proof. Which of these sounds the best to you? It is not considered good practice to use "I" unless you are writing a personal account of something. Otherwise, "I" sounds egotistical and can be annoying. Using "one" is often awkward. Using "we" is standard practice in mathematics. This word also brings the reader into the discussion with the author and gives the impression of a team effort. The word "let's" accomplishes this as well but is much less formal. There is a danger of being *too* casual, however. In general, your writing should be balanced, maintaining a professional style. Of course, there is the possibility of avoiding all of these words:

   The integer n is now shown to be even.

2. *Clearly Obviously Of course Certainly*

   These and similar words can turn a reader off if what's written is not clear to the reader. It can give the impression that the author is putting the reader down. These words should be used sparingly and with caution. If they *are* used, then at least be certain that what you say is true. There is also the possibility that the writer (a student?) has a lack of understanding of the mathematics or is not being careful and is using these words as a cover-up. This gives us even more reasons to avoid these words.

3. *Any Each Every*

   This statement is true for any integer n.

   Does this mean that the statement is true for *some* integer n or *all* integers n? Since the word "any" can be vague, perhaps it is best to avoid it. If by "any," we mean "each" or "every," then use one of these two words instead. When the word "any" is encountered, most of the time the author means "each" or "every."

4. *Since $\cdots$, then $\cdots$*

   A number of people connect these two words. You should use either "If $\cdots$, then $\cdots$" (should this be the intended meaning) or "Since $\cdots$, it follows that $\cdots$" or, possibly, "Since $\cdots$, we have $\cdots$". For example, it is correct to write

   If n^2 is even, then n is even.

or

Since n^2 is even, it follows that n is even.

or perhaps

Since n^2 is even, n is even.

but avoid

Since n^2 is even, then n is even.

In this context, the word "since" can be replaced by "because."

5. *Therefore Thus Hence Consequently So It follows that This implies that*

   This is tricky. Mathematicians cannot survive without these words. Often within a proof, we proceed from something we've just learned to something else that can be concluded from it. There are many (many!) openings to sentences that attempt to say this. Although each of the words or phrases

   Therefore Thus Hence Consequently So It follows that This implies that

   is suitable, it is good to introduce some variety into your writing and not use the same words or phrases any more often than necessary.

6. *That Which*

   These words are often confused with each other. Sometimes they are interchangeable; more often they are not.

The solution to the equation is the number less than 5 that is positive. **(2)**

The solution to the equation is the number less than 5 which is positive. **(3)**

Which of these two sentences is correct? The simple answer is: Both are correct – or, at least, both might be correct.

For example, sentence (2) could be the response to the question: Which of the numbers -2, 3 and 5 is the solution of the equation? Sentence (3) could be the response to the question: Which of the numbers 4.9 and 5.0 is the solution of the equation?

The word "that" introduces a *restrictive clause* and, as such, the clause is essential to the meaning of the sentence. That is, if sentence (2) were written only as "The solution to the equation is the number less than 5." then the entire meaning is changed. Indeed, we no longer know what the solution of the equation is.

On the other hand, the word "which" does *not* introduce a restrictive clause. It introduces a nonrestrictive (or parenthetical) clause. A *nonrestrictive clause* only provides additional information that is not essential to the meaning of the sentence. In sentence (3) the phrase "which is positive" simply provides more information about the solution. This clause may have been added because the solution to an earlier equation is negative. In fact, it would be more appropriate to add a comma:

The solution to the equation is the number less than 5, which is positive.

For another illustration, consider the following two statements:

I always keep the math text that I like with me. **(4)**

I always keep the math text which I like with me. **(5)**

What is the difference between these two sentences? In (4), the writer of the sentence clearly has more than one math text and is referring to the one that he/she likes. In (5), the writer has only one math text and is providing the added information that he/she likes it. The nonrestrictive clause in (5) should be set off by commas:

I always keep the math text, which I like, with me.

A possible guideline to follow as you seek to determine whether "that" or "which" is the proper word to use is to ask yourself: Does it sound right if it reads "which, by the way"? In general, "that" is normally used considerably more often than "which." Hence, the advice here is: Beware of wicked which's!

While we are discussing the word "that," we mention that the words "assume" and "suppose" often precede restrictive clauses and, as such, the word "that" should immediately follow one of these words. Omitting "that" leaves us with an *implied* "that." Many mathematicians prefer to include it rather than omit it.

In other words, instead of writing:

Assume N is a normal subgroup.

many would write

Assume that N is a normal subgroup.

1.7 Some closing comments about writing

1. Use good English. Write in complete sentences, ending each sentence with a period (or a question mark when appropriate) and capitalize the first word of each sentence. (Remember: No sentence begins with a symbol!)
2. Capitalize theorem and lemma as in Theorem 1.15 and Lemma 4.11. (For example, write: In order to verify the truth of Result 3.14, we first prove the following lemma.)
3. Many mathematicians do not hyphenate words containing the prefix "non," such as

   nonempty, nonnegative, nondecreasing, nonzero.

4. Many words that occur often in mathematical writing are commonly misspelled. Among these are:

   commutative (independent of order)
   complement (supplement, balance, remainder)
   consistent (conforming, agreeing)
   feasible (suitable, attainable)

its (possessive, not "it is")
occurrence (incident)
parallel (non-intersecting)
preceding (foregoing, former)
principle (postulate, regulation, rule)
proceed (continue, move on)

and, of course,

corollary, lemma, theorem.

5. There are many pairs of words that fit together in mathematics (while interchanging words among the pairs do not). For example,

We ask questions.
We pose problems.
We present solutions.
We prove theorems.
We solve problems.
and
We conclude this chapter.

2 Sets

3 Logic

The ***disjunction*** of the statements P and Q is the statement P or Q.
The ***conjunction*** of the statements P and Q is the statement P and Q.
For statements (or open sentences) P and Q, the conjunction

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

of the implication $P \Rightarrow Q$ and its converse is called the ***biconditional*** of P and Q and is denoted by $P \iff Q$.

4 Direct Proof and Proof by Contrapositive

4.1 Introduction to Axioms, lemmas, etc.

We are now prepared to begin discussing our main topic: mathematical proofs. Initially, we will be primarily concerned with one question: For a given true mathematical statement, how can we show that it is true?

A true mathematical statement whose truth is accepted without proof is referred to as an *axiom*. For example, an axiom of Euclid in geometry states that for every line l and point P not on l, there is a unique line containing P that is parallel to l.

A true mathematical statement whose truth can be verified is often referred to as a *theorem*., although many mathematicians reserve the word"theorem" for such statements that are especially significant or interesting. For example, the mathematical statement "2+3=5" is true bu few, if any, would consider this to be a theorem under this latter interpretation. In addition to the word "theorem", other common terms for such statements include proposition, result, observation and fact, the choice often depending on the significance of the statement or the degree of difficulty of its proof. We will use the word "theorem" sparingly, however, primarily reserving it for true mathematical statements that will be used to verify other mathematical statements that we will encounter later. Otherwise, we will simply use the word "result". For the most part then, our results are examples used to illustrate proof techniques and our goal is to prove these results.

A *corollary* is a mathematical result that can be deduce from, and is thereby a consequence of, some earlier result.

A *lemma* is a mathematical result that is useful is establishing the truth of some other result. Some people like to think of a lemma as a "helping result". Ordinarily then, a lemma is not of primary importance itself. Indeed, its very existence is due only to its usefulness in proving another (more interesting) result.

Most theorems (or results) are stated as implications.

4.2 A sign that you've finished your proof

In the past, the most common way to indicated that a proof has concluded was to write Q.E.D., which stands for the Latin phrase "quod erat demonstrandum", whose English translation is "which was to be demonstrated.".

4.3 Vacuous Proof

Let $P(x)$ and $Q(x)$ be open sentences over a domains S. Then $\forall x \in S, P(x) \Rightarrow Q(x)$ is a true statement if it can be shown that $P(x)$ is false for all $x \in S$ (regardless of the truth value of $Q(x)$), according to the truth table for implication. Such a proof is called a ***vacuous proof*** of $\forall x \in S, P(x) \Rightarrow Q(x)$.

Example. Let $x \in \mathbb{R}$. If $x^2 - 2x + 2 \leq 0$, then $x^3 \geq 8$. **Proof**.

First observer that that

$$x^2 - 2x + 1 = (x-1)^2 \geq 8.$$

Therefore, $x^-2 - 2x + 2 = (x-1)^2 + 1 \geq 1 > 0$. Thus, $x^2 - 2x + 2 \leq 0$ is false for all $x \in \mathbb{R}$ and the implications is true.

For

$$P(x) : x^2 - 2x + 2 \leq 0 \text{ and } Q(X) : x^3 \geq 8$$

over the domain $\mathbb{R}$, the result asserts the truth of $\forall x \in \mathbb{R}, P(x) \Rightarrow Q(x)$. Since we verified that $P(x)$ is false for every $x \in \mathbb{R}$, it follows that $P(x) \Rightarrow Q(x)$ is true for each $x \in \mathbb{R}$. Hence, the result is true. In this case, $P(x)$ is a false statement for each $x \in \mathbb{R}$. This is what permitted us to give a vacuous proof of the previous result.

In the proof of the previous result, the truth or falseness of $x^3 \geq 8$ played no role whatsoever. Indeed, had we replaced $x^3 \geq 8$ by $x^3 \leq 8$, for example then neither the truth nor the proof of the result would be affected. Whenever there is a vacuous proof of a result, we often say that the result follows **vacuously**. As we mentioned, a trivial proof is almost never encountered in mathematics; however, the same cannot be said of vacuous proofs, as we will see later.

Example. Let $S = n \in \mathbb{Z} : n \geq 2$ and let $n \in S$. If $2n + \frac{2}{n} < 5$, then $4n^2 + \frac{4}{n^2} < 25$.j **Proof**. First, we observer that if $n = 2$, then $2n + \frac{2}{n} = 5$. Of course, $5 < 5$ is false. If $n \geq 3$, then $2n + \frac{2}{n} > 2n \geq$. So, when $n \geq 3$,$2n + \frac{2}{n} < 5$ is false as well. Thus, $2n + \frac{2}{n} < 5$ is false for all $n \in S$. Hence, the implication is true.

4.4 Proof Strategy and Proof Analysis

From time to time, we will find ourselves in a position where we have a result to prove and it may not be entirely clear how to proceed. In such a case, we need to consider our options and develop a plan, which we refer to as a **proof strategy**. The idea is to discuss proof strategy for the result and, from it, construct a proof. At other times, we may wish to reflect on a proof that we havejust given in order to understand it better. Such a discussion will be referred to as a **proof analysis**.

5 Mathematical Induction

5.1 The Principle of Mathematical Induction

Let A be a nonempty set of real numbers. A number $m \in A$ is called a **least element** (or a **minimum** or **smallest element**) of A if $x \geq m$ for every $x \in A$. Some nonempty sets of real numbers have a least element; others do not. The set N has a smallest element, namely 1, while $\mathbb{Z}$ has no least element. The closed interval $[2, 5]$ has the minimum element 2 but the open interval $(2, 5)$ has no minimum element. The set

$$A = \{\tfrac{1}{n} : n \in N\}$$

also has no least element.

If a nonempty set A of real numbers has a least element, then this element is necessarily unique. We will verify this fact. Recall that when attempting to prove that an element possessing a certain property is unique, it is customary to assume that there are two elements with this property. We then show that these elements are equal, implying that there is exactly one such element.

5.1.1 Theorem of the unique least element.

If a set A of real numbers has a least element, then A has a unique least element.

Proof. Let m_1 and m_2 be least elements of A. Since m_1 is a least element, $m_2 \geq m_1$. Also, since m_2 is a least element, $m_1 \geq m_2$. Therefore, $m_1 = m_2$.

The proof we gave of this theorem is a direct proof. Suppose that we had replaced the first sentence of this proof by
Assume, to the contrary, that A contains distinct least elements m_1 and m_2.

If the remainder of the proof of the previous theorem were the same except for adding a concluding sentence that we have a contradiction, then this too would be a proof of the previous theorem. That is, with a small change, the proof technique used to verify the previous Theorem can be transformed from a direct proof to a proof by contradiction.

5.1.2 Well-ordered

There is a property possessed by some sets of real numbers that will be of great interest to us here. A nonempty set S of real numbers is said to be **well-ordered** *if every nonempty subset of S has a least element.*

Let $S = \{-7, -1, 2\}$. The nonempty subset of S are

$$\{-7, -1, 2\}, \{-7, -1\}, \{-7, 2\}, \{-1, 2\}, \{-7\}, \{-1\} \text{ and } \{2\}.$$

Since each of these subset has a least element, S is well-ordered. Indeed, it should be clear that ***every nonempty finite set of real numbers is well-ordered***.

The open interval $(0, 1)$ is *not* well-ordered, since, for example $(0, 1)$ itself has no least element. The closed interval $[0, 1]$ has the least element 0; however, $[0, 1]$ is *not* well-ordered since the open interval $(0, 1)$ is a (nonempty) subset of $[0, 1]$ without a least element. ***Because none of the sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ has a least element, none of these sets is well-ordered. Hence, having a least element is a necessary condition for a nonempty set to be well-ordered but it is not sufficient.***

Although it may appear evident that the set $\mathbb{N}$ of positive integers is well-ordered, this statement cannot be proved from the properties of positive integers that we have used and derived thus far. Consequently, this statement is accepted as an axiom, which we state below.

5.1.3 The Well-Ordering Principle

The set $\mathbb{N}$ of positive integers is well-ordered.

5.1.4 An Introduction to the Principle of Mathematical Induction

(**The Principle of Mathematical Induction**) For each positive integer n, let $P(n)$ be a statement. If

1. $P(1)$ is true and
2. the implication

$$\text{If } P(k), \text{ then } P(k+1)$$

is true for every positive integer k,

then $P(n)$ is true for every positive integer n.

Proof. Assume, to the contrary, that the thoerem is false. The conditions (1) and (2) are satisfied but there exist some positive integers n for which $P(n)$ is a false statement. Let

$$S = \{n \in \mathbb{N} : P(n) is false.\}$$

Since S is a nonempty subset of N, it follows by the Well-Ordering Principle that S contains a least element s. Since $P(1)$ is true, $1 \notin S$. Thus $s \geq 2$ and $s-1 \in \mathbb{N}$. Therefore, $s-1 \notin S$ and so $P(s-1)$ is a true statement. By condition (2), $P(s)$ is also true and so $s \notin S$. This, however, contradicts our assumption that $s \in S$.

The Principle of Mathematical Induction is stated more symbolically below.

5.1.5 The Principle of Mathematical Induction

For each positive integer n, let $P(n)$ be a statement. If

1. $P(1)$ is true and
2. $\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$ is true,

then $\forall n \in \mathbb{N}, P(n)$ is true.

5.1.6 Proof by induction

As a consequence of the Principle of Mathematical Induction, the quantified statement $\forall n \in \mathbb{N}, P(n)$ can be proved to be true if

1. we can show that the statement $P(1)$ is true and
2. we can establish the truth of the implication

$$\text{If } P(k) \text{ , then } P(k+1)$$

for every positive integer k.

A proof using the Principle of Mathematical Induction is called an **induction proof** or a **proof by induction**. The verification of the truth of $P(1)$ in an induction proof is called the **base step, basis step** or the **anchor** of the induction. In the implication

$$\text{If } P(k) \text{ , then } P(k+1)$$

for an arbitrary positive integer k, the statement $P(k)$ is called the **inductive**(or **induction**) **hypothesis**. Often we use a direct proof to verify

$$\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1).$$

although any proof technique is acceptable. That is, we typically assume that the inductive hypothesis $P(k)$ is true for an arbitrary positive integer k and attempt to show that $P(k+1)$ is true. Establishing the truth of $\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$ is called the **inductive step** in the induction proof.

5.1.7 Example of induction proof

Let

$$P(n) : 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

where $n \in \mathbb{N}$. Then $P(n)$ is true for every positive integer n.

Proof. We employ induction. Since $1 = (1 * 2)/2$, the statement $P(1)$ is true. Assume that $P(k)$ is true for an arbitrary positive integer k, that is, assume that

$$P(k) : 1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$$

We show that $P(k+1)$ is true, that is, we show that

$$1+2+3+\cdots+(k+1)=\tfrac{(k+1)(k+2)}{2}$$

Thus,

$$1+2+3+\cdots+(k+1)=(1+2+3+\cdots+k)+(k+1)=\tfrac{k(k+1)}{2}+(k+1)=\tfrac{k(k+1)+2(k+1)}{2}=\tfrac{(k+1)(k+2)}{2},$$

as desired.

By the Principle of Mathematical Induction, $P(n)$ is true for every positive integer n.

Typically, a statement to be proved by induction is not presented in terms of $P(n)$ or some other symbols.

5.2 A More General Principle of Mathematical Induction

The Principle of Mathematical Induction, described in the preceding section, gives us a technique for proving that a statement of type

For every positive integer n, $P(n)$.

is true. There are situations, however, when the domain of $P(n)$ consists of those integers greater than or equal to some fixed integer m different from 1. We now describe an analogous technique to verify the truth of a statement of the following type where m denotes some fixed integer:

For every integer $n \geq m$, $P(n)$.

According to the Well-Ordering Principle, the set $\mathbb{N}$ of natural numbers is well-ordered, that is, every nonempty subset of $\mathbb{N}$ has a least element. As a consequence of the Well-Ordering Principle, other sets are also well-ordered.

5.2.1 Theorem on well-ordered sets

For each integer m, the set

$$S = \{i \in \mathbb{Z} : i \geq m\}$$

is well-ordered.

5.2.2 The Principle of Mathematical Induction - using more general values

For a fixed integer m, let $S = \{i \in \mathbb{Z} : i \geq m\}$. For each integer $n \in S$, let $P(n)$ be a statement. If

1. $P(m)$ is true and
2. the implication

$$\text{If } P(k) \text{ , then } P(k+1)$$

is true for every integer $k \in S$,

then $P(n)$ is true for every integer $n \in S$.

5.2.3 The Principle of Mathematical Induction - General

For a fixed integer m, let $S = \{i \in \mathbb{Z} : i \geq m\}$. For each integer $n \in S$, let $P(n)$ be a statement. If

1. $P(m)$ is true and
2. $\forall k \in S, P(k) \Rightarrow P(k+1)$ is true,

then $\forall n \in S, P(n)$ is true.

This (more general) Principle of Mathematical Induction can be used to prove that certain quantified statements of the type $\forall n \in S, P(n)$ are true when $S = \{i \in \mathbb{Z} : i \geq m\}$ for a prescribed integer m. Of course, if $m = 1$, then $S = \mathbb{N}$.

5.2.4 Example of general PMI

Prove. For every nonnegative integer n,

$$2^n > n.$$

Proof. We proceed by induction. The inequality holds for $n = 0$ since $2^0 > 0$. Assume that $2^k > k$, where k is a nonnegative integer. We show that $2^{k+1} > k + 1$. When $k = 0$, we have $2^{k+1} = 2 > 1 = k + 1$. We therefore assume that $k \geq 1$. Then

$$2^{k+1} = 2 * 2^k > 2k = k + k \geq k + 1.$$

By the Principle of Mathematical Induction, $2^n > n$ for every nonnegative integer n.

5.3 The Strong Principle of Mathematical Induction

There is one last form of mathematical induction. This principle goes by many names: the Strong Principle of Mathematical Induction, the Strong Form of Induction, the Alternate Form of Mathematical Induction and the Second Principle of Mathematical Induction are common names.

5.3.1 Theorem - The Strong Principle of Mathematical Induction

For each positive integer n, let $P(n)$ be a statement. If

1. $P(1)$ is true and
2. the implication

   If $P(i)$ for every integer i with $1 \leq i \leq k$, then $P(k+1)$4a.

   is true for every positive integer k,

then $P(n)$ is true for every positive integer n.

5.3.2 Theorem 2 (more general) - The Strong Principle of Mathematical Induction

For each positive integer n, let $P(n)$ be a statement. If

1. $P(1)$ is true and
2. $\forall k \in \mathbb{N}, P(1) \wedge P(2) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)$ is true, is true for every positive integer k,

then $\forall n \in \mathbb{N}, P(n)$ is true.

The difference in the statement of the Principle of Mathematical Induction and the Strong Principle of Mathematical Induction lies in the inductive step (condition 2). To prove that $\forall n \in \mathbb{N}, P(n)$ is true by the Principle of Mathematical Induction, we are required to show that $P(1)$ is true and to verify this implication

$$\text{If } P(k), \text{ then } P(k+1).$$

is true for every positive integer k. On the other hand, to prove $\forall n \in \mathbb{N}$ is true by the Strong Principle of Mathematical Induction, we are required to show that $P(1)$ is true and to verify the implication:

$$\text{If } P(i) \text{ for every } i \text{ with } 1 \leq i \leq k, \text{ then } P(k+1).$$

is true for every positive integer k. If we were to give direct proofs of the implications, then we are permitted to assume more in the inductive step of the Strong Principle of Mathematical Induction than in the induction step of the Principle of Mathematical Induction and yet obtain the same conclusion. If the assumption that $P(k)$ is true is insufficient to verify the truth of $P(k+1)$ for an arbitrary positive integer k, but the assumption that all of the statements $P(1), P(2), \ldots, P(k)$ are true is sufficient to verify the truth of $P(k+1)$, then this suggests that we would use the Strong

Principle of Mathematical Induction. Indeed, any result that can be proved by the Principle of Mathematical Induction can also be proved by the Strong Principle of Mathematical Induction.

Just as there is a more general version of the Principle of Mathematical Induction, there is a more general version of the Strong Principle of Mathematical Induction. We shall also refer to this as the Strong Principle of Mathematical Induction.

5.3.3 The Strong Principle of Mathematical Induction

For a fixed integer m, let $S = \{i \in \mathbb{Z} : i \geq m\}$. For each $n \in S$, let $P(n)$ be a statement. If

1. $P(m)$ is true and
2. the implication

$$\text{If } P(i) \text{ for every integer } i \text{ with } m \leq i \leq k, \text{ then } P(k+1).$$

is true for every positive integer $k \in S$,

then $P(n)$ is true for every integer $n \in S$.

5.3.4 Recursively-Defined Sequences

We now consider a class of mathematical statements where the Strong Principle of Mathematical Induction is commonly the appropriate proof technique.

Suppose that we are considering a sequence $a_1, a_2, a_3, \ldots$ of numbers, also expressed as $\{a_n\}$. One way of defining a sequence $\{a_n\}$ is to specify explicitly the nth term a_n(as a function of n. For example, we might have $a_n = \frac{1}{n}$, $a_n = \frac{(-1)^n}{n^2}$ or $a_n = n^3 + n$ for each $n \in \mathbb{N}$. A sequence can also be **defined recursively**. In a **recursively-defined sequence** $\{a_n\}$, only the first term or perhaps the first few terms are defined specifically, say $a_1, a_2, \ldots, a_k$ for some $k \in \mathbb{N}$. These are called the **initial values**. Then a_{k+1} is expressed in terms of $a_1, a_2, \ldots, a_k$ and, more generally, for $n > k$, a_n is expressed in terms of $a_1, a_2, \ldots, a_{n-1}$. This is called the **recurrence relation**.

A specific example of this is the sequence $\{a_n\}$ defined by $a_1 = 1$, $a_2 = 3$ and $a_n = 2a_{n-1} - a_{n-2}$ for $n \geq 3$. In this case, there are two initial values, namely $a_1 = 1$ and $a_2 = 3$. The recurrence relation here is

$$a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 3.$$

Letting $n = 3$,we find that $a_3 = 2a_2 - a_2 = 5$; while letting $n = 4$, we have $a_4 = 2a_3 - a_2 = 7$. Similarly, $a_5 = 9$ and $a_6 = 11$. From this information, one might well conjecture (guess) that $a_n = 2n - 1$ for every $n \in \mathbb{N}$. Using the Strong Principle of Mathematical Induction, we can, in fact, prove that htis conjecture is true.

5.3.5 Induction proof using The Strong Principle of Mathematical Induction

A sequence $\{a_n\}$ is defined recursively by

$$a_1 = 1,\ a_2 = 3 \text{ and } a_n = 2a_{n-1} - a_{n-2} \text{ for } n \geq 3.$$

Then $a_n = 2n - 1$ for all $n \in N$.

Proof. (from the book)
We proceed by induction. Since $a_1 = 2 * 1 - 1 = 1$, the formula holds for n=1. Assume for an arbitrary positive integer k that $a_i = 2i - 1$ for all integers i with $1 \leq i \leq k$. We show that $a_{k+1} = 2(k+1)-1 = 2k+1$. If $k = 1$, then $a_{k+1} = a_2 = 2 * 1 + 1 = 3$. Since $a_2 = 3$, it follows that $a_{k+1} = 2k + 1$ when $k = 1$. Hence, we may assume that $k \geq 2$. Since $k + 1 \geq 3$, it follows that

$$a_{k+1} = 2a_k - a_{k-1} = 2(2k - 1) - (2k - 3) = 2k + 1,$$

which is the desired result. By the Strong Principle of Mathematical Induction, $a_n = 2n - 1$ for all $n \in \mathbb{N}$.

Proof. (my work)

The second step of the strong principle of mathematical induction, simplified is the following:

$\forall k \in S[\forall i \in Z, m \leq i \leq k, P(i) \Rightarrow P(k+1)]$

For a fixed integer $m = 1$, let $S = i \in Z | i \geq 1$. Let $a_1 = 1$, $a_2 = 3$ and $a_n = 2a_{n-1} - a_{n-2}$ for $n \geq 3$.

Prove (1). Prove a_1.

$a_1 = 2 * 1 - 1 = 1$, the formula holds for $k = 1$.

Prove (2).

Let k be an arbitrary integer in S.

Let $a_i = 2i - 1$ such that $1 \leq i \leq k$.

We must show that $a_{k+1} = 2 * (k+1) - 1 = 2k + 1$.

We must first prove that it holds for the initial values since we can't use the recurrence relation only if $k \geq 3$, so we start with 1.

If $k = 1$, then $a_{k+1} = a_2 = 2 * 1 + 1 = 3$. Since $a_2 = 3$, $a_{k+1} = 2k + 1$ when $k = 1$. $k \geq 2$. Since $k + 1 \geq 3$,

$$a_{k+1} = 2a_k - a_{k-1} = 2(2k-1) - (2k-3) = 2k + 1, \text{ as needed.}$$

By The Strong Principle of Mathematical Induction, $\forall n \in S, a_n = 2n - 1$.

5.4 Proof by Minimum Counterexample

Suppose that $P(n)$ is a statement for each positive integer n. We have seen taht induction is a natural proof technique that can be used to verify the truth of the quantified statement

$$\forall n \in \mathbb{N}, P(n).$$

There are certainly such quantified statements where induction does not work or does not work well. If we would attempt to prove the previous statement using a proof by contradiction, then we would begin such a proof by assuming that the statement $\forall n \in \mathbb{N}, P(n)$ is false. Consequently, there are positive integers n such that $P(n)$ is a false statement. By the Well-Ordering Principle, there exists a smallest positive integer n such that $P(n)$ is a false statement. Denote this integer by m. Therefore, $P(m)$ is a false statement and for any integer k with $1 \leq k < m$, the statement $P(k)$ is true. The integer m is referred to as a **minimum counterexample** of the previous statement. In a proof (by contradiction) of $\forall n \in \mathbb{N}, P(n)$ ca be given using the fact that m is a minimum counterexample, then such a proof is called a **proof by minimum counterexample**.

5.4.1 Proof by Minimum Counterexample

Prove.
For every positive integer n,

$$6 \mid (n^3 - n).$$

Proof.
Assume, to the contrary, that there are positive integers n such that $6 \nmid (n^3 - n)$. Then there is a smallest positive integer n such that $6 \nmid (n^3 - n)$. Let m be this integer. If $n = 1$, then $n^3 - n = 0$; while if $n = 2$, then $n^3 - n = 6$. Since $6 \mid 0$ and $6 divides 6$, it follows that $6 \mid (n^3 - n)$ for $n = 1$ and $n = 2$. Therefore $m \geq 3$. So, we can write $m = k + 2$, where $1 \leq k < m$. Observe that

$$m^3 - m = (k+2)^3 - (k+2) = (k^3 + 6k^2 + 12k + 8) - (k+2) = \\ (k^3 - k) + (6k^2 + 12k + 6).$$

Since $k < m$, it follows that $6 \mid (k^3 - k)$. Hence, $k^3 - k = 6x$ for some integer x. So, we have

$$m^3 - m = 6x + 6(k^2 + 2k + 1 = 6(x + k^2 + 2k + 1).$$

Since $x + k^2 + 2k + 1$ is an integer, $6 \mid (m^3 - m)$, which produces a contradiction.