

One of the goals of the course is:

- B. Students will be able to reason mathematically, to write simple proofs, and are able to judge when an attempted proof in group theory is correct/complete or is not.

The prerequisite course, Math U165 Introduction to Mathematical Reasoning is good preparation for this goal. Here we are reasoning in a new context that you are learning. Some of the proofs here are more complicated, so we will take a slightly more formal step-by-step approach to writing down a proof. The steps need to be clear to a reader.

**Note:** Most of the proofs in the text are careful, but many nevertheless will require study before you will follow them well, and some are opaque. Most of the solutions at the back of the text are the barest of outline of a main idea (see (a) just below).

### I. What is a proof?

: Writing a proof involves two tasks:

- a. Understanding for oneself some main idea(s) behind an assertion, so constructing a line (or web) of proof.
- b. Communicating these in a somewhat formal manner clearly enough so that you and also a trained reader can see that the steps to the conclusion are correct.

One can communicate the main idea(s) without writing a proof, and in fact, this is how we usually learn math from each other. But as I work with a colleague to understand, say “commuting nilpotent matrices” we have in mind the following goals/questions:

- i. Can we understand more deeply (or at all) what is going on in a phenomenon? We often try many examples to help us understand. Often we use analogy, mental pictures, an arrangement of data on the paper, other tools we already know. We often look at very special extreme cases (for example  $n=0$ , or 1 or 2), or several connected straight lines in place of a curve, to help us understand. What is the pattern? Do we have a belief, or conjecture as to the solution?
- ii. Is the viewpoint we have strong enough to give a proof? How can we refine our work to a proof?
- iii. Does the viewpoint we have generalize to a larger context? This would add interest. And a broader context can allow a more conceptual proof.

There are many levels of proof, both in rigor and style. There often are several different proof methods for an assertion. You may prefer one proof method over another, we may feel that one proof is more illuminating than another, or easier to follow. Note Deligne’s comment, quoted in the “Making Mathematics” website:

*“I would be grateful if anyone who has understood this demonstration would explain it to me”*

- Fields Medal winner Pierre Deligne regarding a theorem that he proved using methods that did not provide insight into the question.

## 2. Criteria for a proof: “ASTERS”

**A.** The *assertion* to be proved should be stated at the beginning.

**S.** The *status* of each sentence or line of the proof should be clear.

Status questions: Is the sentence/line an assumption? Or is it something to be shown?  
Or is this line a step, already shown?

Also, for an intermediate step or “Claim” you should make clear to the reader when you are working on the proof of the claim, and when you have finished it.

**TE.** The *terms* used should be clearly defined, either in the text, or by common knowledge, or by you. As I’ve refereed papers, I’ve seen this issue contribute to unclear or false proofs. For example, authors sometimes have not defined “general.” What does “general point of a variety X”, or “general element of a set S” mean?

**R.** The *reason* for each line’s truth should be clear, and preferably written on the right. These reasons may be group axioms, past results, results in the text (prior to or in the section on which we are working), or results obtained in class.

**S.** The *summary* at the end of the proof of the assertion or of a claim reads “Therefore [assertion]” or “Therefore the claim is shown”. The writer clarifies to the reader that he/she feels the proof is complete.

Before writing a formal proof, you may wish also to state briefly the main idea(s).

**3. Example.** (Problem #19 Chapter 0 ip. 23 of text. (Hint: proof by contradiction).

Definition: a prime integer  $p$  is an integer greater than 1, having divisors only 1 and  $p$ .

Symbol:  $\mathbf{N}$  : non-negative integers;  $\therefore$  = “because” or “reason for this is”

**Claim:** *There are infinitely many prime integers*

Proof. 1. Suppose by way of contradiction that there are only a finite number of primes:

1a. Label them  $p_1, p_2, \dots, p_n$  for some  $n \in \mathbf{N}$   $\therefore$  meaning of “finite number of primes”

2. Consider the integer  $s = (p_1 p_2 \cdots p_n) + 1$  (the product of the primes plus 1 is an integer)

3. Then none of the primes  $p_1, p_2, \dots, p_n$  is a divisor of  $s$   $\therefore$  each leaves remainder 1

4. But  $s$  must have a prime divisor  $p$   $\therefore$  Theorem 0.1 (Fund Thm. Arithmetic)

5. Therefore there is a prime  $p$  different from each of  $p_1, p_2, \dots, p_n$   $\therefore$  lines (3), (4)

6. This contradicts line (1a). Hence the assumption that there are a finite number of primes is false.

7. Therefore there are an infinite number of prime integers. QED.

*Question:* Does line (5) directly contradict the assumption (1)? Hasn’t one only shown by line (5) that there are still a finite number of primes?

One never lists in this proof an infinite set of primes. A proof that there are an infinite number of even integers could be much simpler (why?).

**4. Exercises** **A.** Show that there are an infinite number of even integers, using a list.

**B** Give proofs for Chapter 0, p. 23 of text, #20,

**C.** Text p. 24 #35 (show that for every integer  $n$ ,  $n^3 - n \equiv 0 \pmod{6}$ .)

**References on Proofs:**

A. A. Bogomolny, "What is Proof", from "Interactive Mathematics Miscellany and Puzzles" [http://www.cut-the-knot.org/fta/what\\_is\\_proof.shtml](http://www.cut-the-knot.org/fta/what_is_proof.shtml) (accessed Jan 1, 2009) (excellent overview and links)

Steven Krantz: The History and Concept of Mathematical Proof  
<http://www.math.bgu.ac.il/~urionn/algebra1/proof.pdf>

Steven Krantz: Techniques of Problem Solving, American Mathematical Society, 1996.

Making Mathematics group: Mathematics Research Teacher Handbook: "Proofs"  
<http://www2.edc.org/makingmath/handbook/Teacher/Proof/Proof.asp>  
[Intended for math enrichment in grades 7-12, I found this a better account than many.]

George Polya, "How to Solve it: a new aspect of mathematical reasoning, Princeton Univ. Press, 1988.

George Polya, Induction and Analogy in Mathematics (Mathematics and Plausible Reasoning, Vol 1).

Julie Rowlett, "A fun and rigorous introduction to number theory", Chapter 3 Proof and logic, p. 29-40. <http://www.math.ucsb.edu/~rowlett/NumberTheory1.pdf>  
[Good discussion of proof, with examples, and exercises].

Julie Rowlett "Theorems, proof, problems and tricks, a handbook for the mathematics competitor" <http://www.math.ucsb.edu/~rowlett/olympiad1.pdf>  
[despite the title, this is engaging and has useful ideas of how to approach a proof].

Edward Scheinerman, "Mathematics, a Discrete Introduction", 2<sup>nd</sup> Edition, Brooks Cole, 2006. [text for Math U165]

W. Thurston, "On Proof and Progress in Mathematics" Bull Amer Math Soc 30 #2, April 1993, 161-177). <http://arxiv.org/abs/math.HO/9404236>  
[This is excellent on how mathematics is actually done, and is an assigned reading]

Wayne Wickelgren: How to Solve Problems, Elements of a theory of problems and Problem solving" (1974) W. H. Freeman and Company. Corrected reprint: "How to Solve Mathematical Problems", Dover (1995).  
[He was my teacher in "problem solving" and in writing protocols of problem solving]

Andrei Zelevinsky: Math U165, "Introduction to Mathematical Reasoning"  
[http://www.math.neu.edu/zelevinsky/syllabi/U165\\_f08.html](http://www.math.neu.edu/zelevinsky/syllabi/U165_f08.html)