1.4. Proofs: Structures and Strategies

Note. In this section we describe (sometimes informally) the approach to presenting a proof. The reason to prove a mathematical theorem, beyond establishing its validity, is to gain a *deeper understanding* of the theorem. By giving a detailed logical argument based on known results, we see why the theorem is true and how it relates to previous results (in research, the "previous results" are often the existing body of literature).

Note. Gerstein comments (see pages 18 and 19):

> "But mathematics extends far beyond the uninspired linking of one randomly chosen proposition to another. ... In an interesting mathematical system, the formal requirements of the laws of deduction are likely to be so awesome in their complexity and rigidity that it is a common practice to adopt a less formal style of discussion, consisting of a palatable mixture of mathematical expressions and ordinary sentences in our natural language. We will follow that practice here. So what we customarily call a proof is usually only an outline of the genuine article, and we must be on guard for irrational leaps that cannot be justified by the available body of axioms, theorems, and logical rules."

Note/Definition. Suppose we want to prove a proposition Q. If we can find a true proposition P such that $P \Rightarrow Q$, then this will do! Symbolically, we need to prove $P \wedge (P \Rightarrow Q)$ (where P is known to have truth value T). An argument of

this sort is a *direct proof*. The logical principle employed here is called (mostly by philosophers) the *rule of modus ponens* (or the *law of detachment*).

Note. The Greek philosopher Aristotle (384 BCE-322 BCE) introduced an approach to logic, now known variously as Aristotelian logic, term logic, traditional logic, or syllogistic logic. Aristotle published six works which make up the *Organon*: I. Categories, II. On Interpretation, III. Prior Analytics, IV. Posterior Analytics, V. Topics, and VI. On Sophistical Refutations (a copy of these works in English is available at Archive.org). A basic idea behind Aristotelian logic is that propositions are composed of two terms (thus the label "term logic") and the reasoning process draws a conclusion based on the two terms. A standard example is the line of reasoning: "All men are mortal. Socrates is a man. Therefore Socrates is mortal." This is a *syllogism* where the first two sentences are "premises" and the third sentence is the "conclusion." Aristotelian logic was updated by the now more-dominant *predicate logic* in the late 1800s.

A close up of Raphael's"The School of Athens," painted 1509-1511, of Plato and Aristotle from Wikipedia (accessed 12/24/2021)

Note. In Example 1.20, Gerstein dissects the argument that if a triangle has one vertex at the center of a circle and the other two vertices on the circle, then the triangle has two equal angles. He discusses the thought process (complete with "Hmmm") that one might go through to create the proof. We now give a similar analysis of his Example 1.21 (which is related to number theory).

Example 1.21. Take the facts of elementary arithmetic as our body of "known truths," and consider a proof of this proposition: The square of an odd integer has the form $8k+1$ for some integer k. We first paraphrase Gerstein's "rambling style" of proof.

Proof. *(Rambling Style).* We start with an odd integer n. But we need a more thorough quantitative description of n. Now an even integer is a multiple of 2; say $2q$ where q is *some* integer (with no conditions on q, other than the fact that it an integer). An odd integer, then, is 1 greater than (or less than) an even integer. Equivalently, when an odd integer is divided by 2, the remainder is 1. So we must have $n = 2q + 1$ (say) for some integer q. Next, we can address the claim about the square of n. We have (using the "known truths," like FOIL)

$$n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1.$$

The factoring of $4q$ is inspired by the fact that we are trying to change n^2 into an expression of the form $8k+1$, and this factoring produces the desired "+1." Notice that we have that n^2 is a multiple of 4 plus 1, which is close to the desired conclusion but is *not yet* the desired conclusion; we want a multiple of 8 plus 1, so we further explore the term $4q(q + 1)$. You might view this as somewhat experimental (and

it might fail!), but it is motivated. Now, either q or $q+1$ is an even integer and hence 2 either divides q or $q+1$. Therefore $q(q+1)/2$ is an integer (and, of course, $q(q+1) = 2q(q+1)/2$), we can conclude

$$n^2 = 4q(q+1) + 1 = 4\left(2q(q+1)/2\right) + 1 = 8(q(q+1)/2) + 1 = 8k + 1,$$

where we take $k = q(q+1)/2$ (and, as argued above, k is an integer). We conclude this argument with the standard contemporary symbol used to end a proof: $\square$

A text book proof would be more concise and would not include the thought process and the inspiration for various steps (though in a pedagogical environment it is wise to motivate the steps taken, especially in complicated abstract settings). Homework solutions in proof-based classes should follow a streamlined proof process as well. So we take the ideas of the "Rambling Style" proof and clean things up as follows.

Proof. *(Compact Style).* An odd integer is of the form $n = 2q+1$ for some integer q. Then

$$n^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4q(q+1) + 1 = 8(q(q+1)/2) + 1 = 8k + 1,$$

where $k = q(q+1)/2$ is an integer. $\square$

With the introduction of the representation $n = 2q+1$ (established by the definition of "even/odd integer"), both arguments above are based on the implication

$$\underbrace{(n = 2q+1)}_{P} \Rightarrow \underbrace{(n^2 = 8k+1)}_{Q}.$$

Now proposition P has truth value T by the definitions, the proofs establish the implication $P \Rightarrow Q$, and *modus ponens* gives that the truth value of Q is then T. Beyond this class (in fact, after we finish this section) you are very unlikely to hear the use of *modus ponens* by name.

Note. In an axiomatic system, we would desire that the truth value of every (meaningful) proposition P could be determined within the system (such an axiomatic system is *complete*). That is, we want to be able to prove either P or $\sim P$. However, it was shown by Kurt Gödel (April 28, 1906–January 14, 1978) that some common axiomatic systems (he refers to them as "formal systems") have *undecidable* propositions (that is, propositions which cannot be given a truth value in the formal system). This is heavy stuff for this stage of the course, but for the record Gödel proved:

Gödel's First Incompleteness Theorem. There are provably unprovable but nonetheless true propositions in any formal system that contains elementary arithmetic, assuming that system to be consistent.

Gödel's Second Incompleteness Theorem. The consistency of a formal system that contains arithmetic cant be formally proved with that system.

These versions of Gödel's theorems are from R. Goldstein's *Incompleteness: The Proof and Paradox of Kurt Gödel*, W. W. Norton, Great Discoveries Series (2005). For more details on Gödel's ideas, see my online notes on Introduction to Math Philosophy and Meaning, and my online notes for Introduction to Modern Geometry (MATH 4157/5157) on Section 1.6. Completeness and Categoricalness. An example of one "provably unprovable" result relates to the sizes (or "cardinalities") of sets. We'll see in Section 4.3. Countable and Uncountable Sets that some infinite sets are bigger than other infinite sets! In fact, the set of integers is an infinite set that is strictly smaller than the infinite set of real numbers. That is, in symbols that we will use later, $|\mathbb{Z}| < |\mathbb{R}|$. It is reasonable to ask if there is a set A that is "bigger" than $\mathbb{Z}$ and "smaller" than $\mathbb{R}$ (in the sense of cardinality). In other

words, does a set A exist where $|\mathbb{Z}| < |A| < |\mathbb{R}|$? This is known to be neither true nor false (though it is meaningful) within the standard axioms of set theory! The denial of the existence of such a set A is called the Continuum Hypothesis. Of course, we could just as easily hypothesize that such a set A *does* exist. For more details on the Continuum Hypothesis, see my online presentation on Magical Math Results. . . and Their Explanations (see the section on "Neither True Nor False").

Note. On page 23, Gerstein gives a bit of a pep-talk about searching for a proof (making an analogy with climbing a mountain' give it a read!). We quote some of his suggestions and his more symbolic statements:

> "Now suppose you want to prove proposition Q, and you think you know all that is needed for the job; say you know that a proposition P is true. Think: If I know P, what else do I know as a consequence? . . . Also, what does it mean to say that Q is true? Are there one or more statements, perhaps simpler than Q, and perhaps separately provable, from which Q will follow readily?"

Gerstein also defines "definition." This seems a bit tongue-in-cheek, but here it is. . .

Definition. A *definition* is a statement introducing a new symbol or word that abbreviates a package of statements or expressions (or both) whose meanings or uses are already understood.

Note/Definition. If we can prove for proposition Q that the truth value of $\sim Q$ is F, then we know that Q itself has truth value T. Such a proof of Q is an *indirect proof* or *proof by contradiction* (or, as the philosophers say, "*reductio ad absurdum*"). In such an argument, we show that $\sim Q$ implies a false statement, so that $\sim Q$ cannot be true. The truth table associated with this is (Table 1.19):

P	Q	$P \Rightarrow Q$	$\sim P$	$\sim Q$	$\sim Q \Rightarrow \sim P$	$Q \Rightarrow P$
F	F	T	T	T	T	T
F	T	T	T	F	T	F
T	F	F	F	T	F	T
T	T	T	F	F	T	T

In the bottom line of the table, we have $\sim Q \Rightarrow \sim P$ and $\sim p$ false, as desired for a proof by contradiction. Notice that in this line of the table we have Q is true, justifying the proof by contradiction. In addition, notice that the truth values of $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are the same so that these two propositions are equivalent. Sentential form $\sim Q \Rightarrow \sim P$ is the *contrapositive* or sentential form $P \Rightarrow Q$. Sentential form $Q \Rightarrow P$ is the *converse* of sentential form $P \Rightarrow Q$ (and these are *not* equivalent).

Note. We illustrate the use of the contrapositive to prove a claim by re-examining Example 1.21.

Example 1.23. Let n denote an integer. Prove the implication

$$\text{If } \underbrace{n^2 \text{ is even}}_{P} \text{ then } \underbrace{n \text{ is even}}_{Q}.$$

Proof. We prove the contrapositive. Suppose $\sim Q$; that is, suppose n is not even. In other words, suppose n is odd so that n is of the form $n = 2k + 1$. Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 = 2\underbrace{(k(k+1))}_{\text{integer}} + 1.$$

So n^2 is odd and $\sim P$ holds. That is, we have shown $\sim Q \Rightarrow \sim P$ and so the logically equivalent claim $P \Rightarrow Q$ holds, as claimed. □

Exercise 1.4(a). Prove that the sum of two odd numbers is even.

Proof. Let m and n be two odd numbers. Then neither m nor n are even and hence neither m for n are divisible by 2. So $m = 2k_m + 1$ and $n = 2k_n + 1$ for some integers k_m and k_n. Then the sum is

$$m + n = (2k_m + 1) + (2k_n + 1) = 2(k_m + k_n) + 2 = 2(k_m + k_n + 1),$$

where $k_m + k_n + 1$ is an integer. That is, 2 divides the sum $m+n$ (namely, $k_m + k_n + 1$ times) and so the sum is even, as claimed. □

Revised: 10/10/2023