CLARK UNIVERSITY

Writing Proofs
Math 225 Modern Algebra

D Joyce, Fall 2017

One of the goals of this course is to develop abstract and critical reasoning by studying logical proofs and the axiomatic method as applied to linear algebra. A big part of that is learning how to write proofs. Indeed, about half of your homework assignments this semester will involve writing proofs.

The general purpose of a proof is to convince yourself and anyone else why something is true. Proofs come in various levels of formality. Some proofs are fairly intuitive, use diagrams, and skip details. They're not very formal, but they're easy to understand.

Formal proofs fill in the details, use a lot of symbols, and are often difficult to understand, but they don't have gaps that informal proofs generally have.

In class, our proofs will range from intuitive proofs where only the main points are mentioned to detailed formal proofs. We'll be as complete as time permits.

The structure of a theorem. A theorem is a statement that's accompanied by a proof of that statement. We'll usually introduce a theorem with the word *Theorem* underlined or italicized to indicate what follows is the precise statement that we'll prove. It's a good idea not to use too many symbols in the statement of the theorem. If you can state it completely in English, that's nice, but frequently equations are necessary.

After the statement of the theorem comes its proof. That should be introduced with the word *Proof*, and when the proof is complete, some indication should be given that you're done with the proof, such as QED, which is an abbreviation for the Latin *quod erat demonstrandum* which means "which was to be shown." Lots of textbooks use a simple square to indicate the end of a proof.

The structure of a proof. There are two main kinds of proofs—synthetic proofs and analytic proofs.

Synthetic proofs. These are the standard proofs that you see in textbooks. They build up to the conclusion one step at a time. You can easily follow a synthetic proof, but it's hard to construct them, except the easiest ones.

One kind of synthetic proof is a *direct proof*. For a direct proof of an implication $P \implies Q$, assume the hypothesis P and derive the conclusion Q. There may intermediate steps. From P you derive R, from R you derive S, and from S you derive the final conclusion Q.

There are other kinds of synthetic proofs such as *indirect proofs* and *proof by contrapositive*. For an *indirect proof*, also called a *proof by contradiction*, to prove P, instead assume P is false and derive any contraction, that is, any statement of the form Q and not Q. For a *proof by contrapositive*, to prove P implies Q, you can instead prove the contrapositive, which is logically equivalent, that is, assume that Q is false and derive that P is false.

Also note that many theorems are *"if and only if" statements.* To prove a statement of the form P if and only if Q, give two proofs. First prove that $P \implies Q$, then prove that $Q \implies P$.

Analytic proofs. Although it's often easier to find an indirect proof than a direct proof, there's a different kind of proof that's closer to what we do when we're looking for a proof. That is, we start at the end and work back. To prove an implication $P \implies Q$, start with the goal Q and break it down into simpler statements that imply it. You might find that Q follows from S, then S follows from R, and then R follows from P. You've succeeded in showing that $P \implies Q$.

You can always turn an analytic proof into a synthetic proof by reversing the order of your statements. It makes it easier to follow the proof, but it hides the process you used to find the proof.

Proofs involving universal quantifiers. Many theorems are universal statements. They state Q is true for all things of a certain kind P. Symbolically $\forall x, P(x) \implies Q(x)$. To prove such a theorem, introduce a new symbol, say x, and start with the statement "let x be such that $P(x)$." Then work with x and derive $Q(x)$.

Note that to disprove a universal statement, it's enough to find one counterexample. But to prove universal statement, you need prove it for a generic x, it's not enough to prove it for a specific value of x. When searching for the proof of a universal statement, you may, however, want to take a specific example, and once you've found a proof for that specific example, then generalize it to get the real proof.

Proof by induction. This is used to prove statements about all positive integers. There are generalizations of mathematical induction, but let's just take the basic form right now.

To prove a statement $P(n)$ for $n = 1, 2, 3, \ldots$, proof by induction involves two steps: the base case and the inductive step. For the base case, simply verify that $P(1)$ is true. For the inductive step, assume that $P(n)$ is true and show $P(n+1)$ is true. (Alternatively, you can show $P(n-1) \implies P(n)$.)

Some standard symbols seen in proofs. There are a whole lot of symbols and abbreviations that are used in proofs. Although these are fairly standard, sometimes other symbols are used instead.

Symbol	Read As	Explanation
$\wedge$	and	The statement $A \wedge B$ is true if A and B are both true; else it is false.
$\vee$	(inclusive) or	The statement $A \vee B$ is true if A or B (or both) are true; if both are false, the statement is false.
$\neg$	not	The statement $\neg A$ is true just when A is false
$\implies$	implies; if... then	$A \implies B$ means if A is true, then B is also true; if A is false, then nothing is said about B.
$\iff$ or "iff"	if and only if	$A \iff B$ means *both* $A \implies B$ *and* $B \implies A$.
$\forall$	for all; for any; for each	when it's true universally
$\exists$	there exists; there is an	when there's at least one
$\exists!$	there exists a unique	when there is exactly one

Writing up proofs. Your proofs should be read like stories with full sentences, but unlike most stories, they're not full of action, but full of logical connections that convince the listener. Frequently there will be equations in a proof, but they need to be connected together by words explaining whether the equation is an assumption, a goal, or a conclusion, and if it's a conclusion, why it follows from the preceding statements.

A synthetic proof is a sequence of statements, each being justified based on previously proved statements or explicit assumptions.

An assumption could be a hypotheses of the theorem your proving, it could be an axiom of the theory you're working in, it could be a hypothesis in a proof by contradiction, or it could be an inductive hypothesis in a proof by mathematical induction. Your wording should make it clear.

Use correct English grammar in your proofs. Use full sentences and punctuation. And, of course, use mathematical symbols correctly, especially the equals sign.

Note that equations are usually read as sentences, but they need to be connected to the rest of the proof. Other times equations are nouns as they are in this example proof of the quadratic formula for the roots to a quadratic polynomial.

Theorem 1. The roots of the quadratic polynomial $ax^2 + bx + c$ are $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Proof. Suppose x is a root of the polynomial, that is, x satisfies the equation $ax^2+bx+c = 0$. Since it's a quadratic polynomial, a is not 0, therefore we can divide the original equation by a to get an equivalent condition

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0$$

which can be rewritten as

$$x^2 + \frac{b}{a}\,x = -\frac{c}{a}.$$

Complete the square by adding $\dfrac{b^2}{4a^2}$ to both sides of the equation to get

$$x^2 + \frac{b}{a}\,x + \frac{b^2}{4a^2} = \frac{b^2}{4a^2} - \frac{c}{a}.$$

The left hand side is now a perfect square, and we can rewrite the equation as

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

Taking square roots, we see that's equivalent to the pair of equations

$$x + \frac{b}{2a} = \pm\frac{\sqrt{b^2 - 4ac}}{2a},$$

which, in turn, is equivalent to the quadratic formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Q.E.D.

Math 225 Home Page at `http://math.clarku.edu/~djoyce/ma225/`