Some proof-writing examples

Here are just some examples of proofs to get you started. Be sure to also read the handout on logic and methods of proof on the course website! **A few general notes to keep in mind:**

- A good proof is an argument that leads from assumptions to conclusions, and it should be written clearly. That is, the goal is to convince the reader that what you’ve claimed follows from statements you’ve already agreed are true.

- Though I am trying to get you into the habit of translating logical statements into symbols (for various reasons), *reading* a proof that is written entirely in logical expressions is both difficult and unenlightening.

  In this course and others like it, the person who is reading your work is usually grading it, as well, so it would be good to make their life easier! Use *words*. Words!

More examples can be found in the textbook, particularly Sections 1 (which has some good examples of induction proofs) and 3 (which has some good examples of direct proofs based on the axioms of \( \mathbb{R} \)).

Some direct proofs

Claim: \( \forall x \in \mathbb{R} : x \cdot 0 = 0 \).

**Proof.** Let \( x \in \mathbb{R} \). By (A3) we have \( 1 + 0 = 1 \), so \( x(1 + 0) = x \cdot 1 = x \) by (M3). Applying (DL) and using (M3) again on the left-hand side, we have

\[
x + x \cdot 0 = x
\]

By (A4), \( x \) has an additive inverse, which we now add to both sides:

\[
x + x \cdot 0 + (-x) = x + (-x)
\]
\[
x + x \cdot 0 + (-x) = 0 \quad \text{since } -x \text{ is the additive inverse of } x,
\]
\[
x + (-x) + x \cdot 0 = 0 \quad \text{by (A2),}
\]
\[
0 + x \cdot 0 = 0 \quad \text{since } -x \text{ is the additive inverse of } x,
\]
\[
x \cdot 0 + 0 = 0 \quad \text{by (A2),}
\]
\[
x \cdot 0 = 0 \quad \text{by (A3)}. \square
\]

Note: This is also Theorem 3.1(ii) in the book. Ross’ proof is different: It does not use (A4), which means his proof can be used to show that the property is valid in \( \mathbb{N} \), while the one above cannot! The study of “which axioms do you need?” to prove a given theorem is called *reverse mathematics*. 
Remarks:

- This proof (and similar ones in Chapter 3 and Problem Set 1) will seem pedantic or over-formal, and they are! No one writes proofs that invoke axioms at every step except when developing a new area of mathematics.

We will eventually graduate to using facts that follow from the axioms, rather than the axioms directly, themselves. That being said, seeing that the basic rules of mathematics you know and (such as the above claim) follow from the axioms is a crucial part of your instruction.

- When proving a claim that looks like $\forall x \in S : P(x)$ directly, start by taking any old $x \in S$ and showing that $P(x)$ is true (without assuming anything new or special about $x$). You’ll notice that the axioms we invoked made no assumptions about $x$ (for example, we didn’t use (M4) on $x$).

Claim: $\forall x, y \in \mathbb{R} : x^2 + y^2 \geq 2xy$.

Proof. Let $x, y \in \mathbb{R}$. By Theorem 3.2(iv), $(x - y)^2 \geq 0$. Since $(x - y)^2 = x^2 - 2xy + y^2$, we have $x^2 - 2xy + y^2 \geq 0$, so we may conclude that $x^2 + y^2 \geq 2xy$. □

Remarks:

- The inequality in the claim is called the arithmetic-geometric mean inequality.

- Here we didn’t directly appeal to any axioms, we just used Theorem 3.2 (which itself follows from the axioms).

A proof by contradiction

Claim: The equation $x^2 - 2 = 0$ has no rational solutions. (Equivalently, $\sqrt{2}$ is irrational.)

Proof. Suppose for contradiction that $r$ is a rational number such that $r^2 - 2 = 0$. We may assume that $r = p/q$ for a fraction $p/q$ in lowest terms ($q \neq 0$ and the integers $p$ and $q$ share no divisors aside from ±1). Rearranging $(p/q)^2 - 2 = 0$ yields $p^2 = 2q^2$. Since $2q^2$ is even, $p^2$ is even (since these quantities are equal), so $p$ is even (because if $p$ were odd, then $p^2$ would be odd). It follows that $p^2$ is divisible by 4, so $\frac{p^2}{4} = \frac{2q^2}{2} = \frac{q^2}{2}$ is an integer. Therefore, $q^2$ is even, so $q$ is even, but this contradicts the assumption that $p/q$ was in lowest terms. □

In this proof:

- Our assumption for contradiction was the negation of the claim. The negation of the claim is “$x^2 - 2 = 0$ has a rational solution.”

- The hypothesis that was eventually contradicted was that $p$ and $q$ have no common divisors aside from ±1.
• We argued that if \( r = p/q \) is a rational solution, then \( p \) and \( q \) must both be even, but this contradicted our hypotheses/assumptions about \( p \) and \( q \).

• Let \( P \) be the statement we wanted to prove. Since we proved that \( \neg P \) implies a false statement, it must be the case that \( \neg(\neg P) = P \) is true.

Two proofs by induction

Claim: \( n^2 > 3n + 1 \) for all \( n \geq 4 \).

Proof. We proceed by induction on \( n \). Let \( P_n \) be the statement \( n^2 > 3n + 1 \).

• (Base case.) \( 16 = 4^2 > 3 \cdot 4 - 1 = 11 \), and this establishes \( P_4 \).

• (Induction step.) Suppose that \( P_n \) is true for some \( n \geq 4 \). Consider \( (n + 1)^2 \):
  \[
  (n + 1)^2 = n^2 + 2n + 1 > (3n + 1) + (2n + 1) = 5n + 2
  \]
where the inequality is true by the inductive hypothesis.

We are done if we can prove that \( 5n + 2 > 3(n + 1) + 1 = 3n + 4 \). But this is indeed true when \( n \geq 4 \), since

\[
\begin{align*}
  n &> 1 \\
  2n &> 2 \\
  5n &> 3n + 2 \\
  5n + 2 &> 3n + 2
\end{align*}
\]

We have proven that if \( P_n \) is true then \( (n + 1)^2 > 3(n + 1) + 1 \) is true. Since that inequality is \( P_{n+1} \), this completes the proof. \( \square \)

Claim: Every convex polygon \( \Pi \) can be triangulated. That is, there is a set \( \{T_1, \ldots, T_k\} \) of non-overlapping* triangles such that \( \Pi = T_1 \cup \cdots \cup T_k \).

If \( S \) and \( T \) are two sets, \( S \cup T \) is the set consisting of points that lie in \( S \) or in \( T \) (or both). *Technically speaking, the triangles will overlap on their shared boundaries, but let’s not let that bother us.

Proof. We induct on \( n \), the number of vertices. Let \( P_n \) be the statement “If \( \Pi \) is a convex \( n \)-gon, then \( \Pi \) can be triangulated.” We will prove \( \forall n \geq 3 : P_n \).

• (Base case.) \( P_3 \) is true because if \( \Pi \) is a triangle, then \( \{\Pi\} \) is a triangulation of \( \Pi \).

• (Induction step.) Assume that \( P_n \) is true for some value of \( n \geq 3 \). Let \( \Pi \) be an \( (n + 1) \)-gon; our goal is to prove that \( \Pi \) is triangulable.

Choose any vertex \( v \) of \( \Pi \) and let \( w_1, w_2 \) be the vertices of \( \Pi \) that are adjacent to \( v \) (it helps to draw a picture). Since \( \Pi \) is convex, the line segment connecting \( w_1 \) and \( w_2 \) is contained inside \( \Pi \) and the triangle \( T = v w_1 w_2 \) is a subset of \( \Pi \). Let \( \Pi' = \Pi - T \) and note that \( \Pi' \) has \( n \) vertices. By our inductive hypothesis, \( \Pi' \) can be triangulated, and if \( \{T_1, \ldots, T_m\} \) is a triangulation of \( \Pi' \), then \( \{T_1, \ldots, T_m, T\} \) is a triangulation of \( \Pi \).