1 First pointers

- A proof consists solely of complete sentences. A sentence starts with a capital letter and ends with a period. Avoid starting a sentence with a mathematical symbol.
- When giving a counterexample (disproving) a statement, be as concrete and specific as possible. Try to find the most simple counterexample. In this way, the form your argument should take when disproving a statement is the opposite of that used in providing a proof. A proof requires a general argument, covering all possible cases.
- The symbol "$\Rightarrow$" means "implies", as in $x = 3 \Rightarrow 2x = 6$. It does not mean "equals" or "my next thought is", etc. As you are reading what you have written, make sure that substituting the word "implies" for "$\Rightarrow$" makes sense.
- The symbol "$\Leftrightarrow$" means "if and only if" (which is sometimes abbreviated "iff"). If P and Q are statements that are either true or false, then $P \Leftrightarrow Q$ means $P \Rightarrow Q$ and $Q \Rightarrow P$, i.e., the truth of P implies the truth of Q, and conversely, the truth of Q implies that of P.
- The symbol "$\forall$" means "for all" and "$\exists$" means "there exists". I use "s. t." for "such that". I do not use "$\ni$" for "such that", since it conflicts with the following usage: $\{1, 2, 3\} \ni 2$. Also, do *not* use "$\vee$" for "or", "$\wedge$" for "and", or "$\sim$" for "not". It is just as easy to write the words, and it is a lot easier to read the words.
- If you have given a proof by contradiction or by proving the contrapositive, consider whether a straightforward proof is at least as clear as the one you have given.
- When writing down a calculation, avoid crossing out terms (for example, when terms cancel in fractions or when they add up to zero). This type of bookkeeping is easy for the writer, who is crossing out sequentially, but is usually confusing for the reader.
- If you say some statement follows "by definition", make sure it follows *directly* from a definition in the statement. Rule of thumb: if you use the phrase "by definition" in a proof, make sure to be specific, e.g. "by definition of the derivative ...". In some sense, every true statement follows "from the definitions". Your proof should guide the reader by showing the relevance of various definitions and already-established results to the statement you are trying to prove.

2 Proof templates

2.1 Induction

Theorem 1

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

for $n = 1, 2, \ldots$

Proof. We will prove this by induction. First note that the statement holds when $n = 1$:

$$1 = \frac{1(1+1)}{2}.$$

Next, suppose the statement holds for some n:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

It follows that

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}, \end{aligned}$$

and the result holds for $n + 1$, too. Hence, the statement holds for all $n = 1, 2, \ldots$ by induction. □

Note: A common mistake in induction proofs is the "backwards proof". See section 3.1 now to avoid this mistake.

2.2 Set inclusion

Theorem 2 *Let* S *be the set of* ..., *and let* T *be the set of* ...
Then $S \subseteq T$.

Proof. Let $s \in S$. Then blah, blah, blah, ...
....
....
It follows that $s \in T$. □

Theorem 3 *Let S be the set of ..., and let T be the set of ...*
Then $S = T$.

Proof. Let $s \in S$. Then blah, blah, blah, ...
....
....
It follows that $s \in T$. Hence, $S \subseteq T$.

Now take $t \in T$. It follows that blah, blah, blah, ...
....
....
Thus, $t \in S$. Hence, $T \subseteq S$, as well. □

2.3 Implications

The symbols P and Q denote mathematical statements that may be true or false.

Theorem 4 *$P \Rightarrow Q$.*

Proof. Suppose P. Then blah, blah, blah, ...
....
....
It follows that Q. □

Theorem 5 *$P \Leftrightarrow Q$.*

Proof. First, suppose P. Then blah, blah, blah, ...
....
....
It follows that Q.

Conversely, suppose Q. Then blah, blah, blah, ...
....
....
It follows that P. □

Sometimes the two parts of the proof are explicitly labeled, as in the following.

Theorem 6 *$P \Leftrightarrow Q$.*

Proof. ($\Rightarrow$) Suppose P. Then blah, blah, blah, ...
. . . .
. . . .
It follows that Q.

($\Leftarrow$) Suppose Q. Then blah, blah, blah, ...
. . . .
. . . .
It follows that P. $\square$

Theorem 7 *For all $x, y, z \in S$, it follows that [some statement involving x, y, and z].*

Proof. Let $x, y, z \in S$. Then blah, blah, blah. (Show the statement holds for this arbitrary choice of elements x, y, and z.) $\square$

2.4 Equivalence relations

Here is a template for a proof that a given relation is an equivalence relation.

Theorem 8 *Let S be a set and let $\sim$ be the relation on S defined by ... Then $\sim$ is an equivalence relation.*

Proof. Let $x, y, z \in S$.

Reflexivity. Since ..., we see that $x \sim x$. Hence, $\sim$ is reflexive.

Symmetry. Suppose that $x \sim y$. Since ..., it follows that $y \sim x$. Hence, $\sim$ is symmetric.

Transitivity. Suppose that $x \sim y$ and $y \sim z$. Since ..., it follows that $x \sim z$. Hence, $\sim$ is symmetric. $\square$

2.5 Functions

Theorem 9 *The function $f\colon A \to B$ is injective.*

Proof. Let $x, y \in A$, and suppose that $f(x) = f(y)$. Then blah, blah, blah. It follows that $x = y$. Hence, f is injective. $\square$

Theorem 10 *The function $f\colon A \to B$ is surjective .*

Proof. Let $b \in B$. Then blah, blah, blah. Thus, there exists $a \in A$ such that $f(a) = b$. Hence, f is surjective. $\square$

2.6 Boundedness, sups, and infs

Theorem 11 *Let $S \subset \mathbb{R}$ satisfying … Then $B \in \mathbb{R}$ is an upper bound for S.*

Proof. Let $s \in S$. Then blah, blah, blah. So $s \leq B$. Hence, B is an upper bound for S. $\square$

Theorem 12 *Let $S \subset \mathbb{R}$ satisfying … Then $L \in \mathbb{R}$ is a lower bound for S.*

Proof. Let $s \in S$. Then blah, blah, blah. So $L \leq s$. Hence, L is a lower bound for S. $\square$

Theorem 13 *Let $S \subset \mathbb{R}$ satisfying …, and let $s = \ldots$ Then $s = \sup S$.*

Proof. We first check that s is an upper bound for S. Let $t \in S$. Then blah, blah, blah. So $t \leq s$. Hence s is an upper bound for S.

We know check that s is the least upper bound for S. Suppose that t is an upper bound for S. Then blah, blah, blah. So $s \leq t$. Hence, s is the least upper bound for S. $\square$

Theorem 14 *Let $S \subset \mathbb{R}$ satisfying …, and let $s = \ldots$ Then $s = \inf S$.*

Proof. We first check that s is a lower bound for S. Let $t \in S$. Then blah, blah, blah. So $s \leq t$. Hence s is a lower bound for S.

We know check that s is the greatest lower bound for S. Suppose that t is a lower bound for S. Then blah, blah, blah. So $t \leq s$. Hence, s is the greatest lower bound for S. $\square$

Theorem 15 *Let S and T be subsets of $\mathbb{R}$ satisfying … Then $\sup T \leq \sup S$.*

Proof. We first show that $\sup S$ is an upper bound for T. Let $t \in T$. Then blah, blah, blah. So $t \leq \sup s$. Then since $\sup S$ is an upper bound for T and $\sup T$ is the least upper bound for T, it follows that $\sup T \leq \sup S$. $\square$

2.7 Limit proofs

Theorem 16

$$\lim_{x \to a} f(x) = L.$$

Proof. Given $\epsilon > 0$, let $\delta =$ [fill in some function of ϵ, but not of x]. Suppose $0 < |x-a| < \delta$. Then

$$\begin{aligned} |f(x) - L| &= \text{etc.} \\ &= \text{etc.} \\ &\leq \text{etc.} \\ &= \text{etc.} \\ &< \text{etc.} \\ &< \epsilon. \end{aligned}$$

□

Theorem 17

$$\lim_{n\to\infty} a_n = a.$$

Proof. Given $\epsilon > 0$, let $N =$ [fill in]. Then $n > N$ implies

$$\begin{aligned} |a_n - a| &= \text{etc.} \\ &= \text{etc.} \\ &\leq \text{etc.} \\ &= \text{etc.} \\ &< \text{etc.} \\ &< \epsilon. \end{aligned}$$

□

3 Common proof-writing mistakes

.

3.1 The backwards proof

Theorem 18 *Suppose* $x \in \mathbb{R}$. *Then* $(x+1)^2 - (x-1)^2 = 4x$.

Incorrect proof. Calculate:

$$\begin{aligned} (x+1)^2 - (x-1)^2 &= 4x \\ (x^2 + 2x + 1) - (x^2 - 2x + 1) &= 4x \\ x^2 + 2x + 1 - x^2 + 2x - 1 &= 4x \\ 4x &= 4x. \end{aligned}$$

□

PROBLEM: The first line of the above "proof" seems to assert as true exactly what it is trying to prove—circular reasoning. To make the mistake even more clear, consider the following:

Theorem 19

$$1 = 0.$$

Incorrect proof. Calculate:

$$\begin{aligned} 1 &= 0 \\ 0 \cdot 1 &= 0 \cdot 0 \\ 0 &= 0. \end{aligned}$$

□

Here is the **correct form**:

Theorem 20 *Suppose* $x \in \mathbb{R}$*. Then* $(x+1)^2 - (x-1)^2 = 4x$*.*

Proof. Calculate:

$$\begin{aligned} (x+1)^2 - (x-1)^2 &= (x^2 + 2x + 1) - (x^2 - 2x + 1) \\ &= x^2 + 2x + 1 - x^2 + 2x - 1 \\ &= 4x. \end{aligned}$$

□