How to write proofs: a quick guide

Eugenia Cheng

Department of Mathematics, University of Chicago
E-mail: eugenia@math.uchicago.edu
Web: http://www.math.uchicago.edu/∼eugenia

October 2004

A proof is like a poem,
or a painting,
or a building,
or a bridge,
or a novel,
or a symphony.

"Help! I don't know how to write a proof!" Well, did anyone ever tell you what a proof *is*, and *how* to go about writing one? Maybe not. In which case it's no wonder you're perplexed.

Writing a good proof is not supposed to be something we can just sit down and do. It's like writing a poem in a foreign language. First you have to learn the language. And then you have to know it well enough to write poetry in it, not just say "Which way is it to the train station please?"

Even when you know how to do it, writing a proof takes planning, effort and inspiration. Great artists do make sketches before starting a painting for real; great architects make plans before building a building; great engineers make plans before building a bridge; great authors plan their novels before writing them; great musicians plan their symphonies before composing them. And yes, great mathematicians plan their proofs in advance as well.

Contents

1 What does a proof look like? 3

2 Why is writing a proof hard? 3

3 What sort of things do we try and prove? 4

4 The general shape of a proof 4

5 What doesn't a proof look like? 6

6 Practicalities: how to think up a proof 9

7 Some more specific shapes of proofs 10

8 Proof by contradiction 15

9 Exercises: What is wrong with the following "proofs"? 16

1 What does a proof look like?

> *A proof is a series of* ***statements****, each of which follows* ***logically*** *from what has gone before. It* ***starts*** *with things we are assuming to be true. It* ***ends*** *with the thing we are trying to prove.*

So, like a good story, a proof has a beginning, a middle and an end.

- **Beginning:** things we are assuming to be true, including the definitions of the things we're talking about
- **Middle:** statements, each following logically from the stuff before it
- **End:** the thing we're trying to prove

The point is that we're *given* the beginning and the end, and somehow we have to fill in the middle. But we can't just fill it in randomly – we have to fill it in in a way that "gets us to the end".

It's like putting in stepping stones to cross a river. If we put them too far apart, we're in danger of falling in when we try to cross. It might be okay, but it might not... and it's probably better to be safe than sorry.

2 Why is writing a proof hard?

One of the difficult things about writing a proof is that the order in which we write it is often *not* the order in which we thought it up. In fact, we often think up the proof *backwards.*

> *Imagine you want to catch a movie at the Music Box. How are you going to get there? You see that the Brown Line will take you there from the Loop. You know that you can get the #6 Bus to the Loop, and you know that you can walk to the #6 Bus stop from Campus. But when you actually make the journey, you* ***start*** *by walking to the #6, and you* ***end*** *by getting the Brown Line. And if someone asks you for directions, it will not be very helpful if you explain it to them backwards...*

Or to put it another way, to build a bridge across a river, we might well start at both ends and work our way towards the middle. We might even put some preliminary supports at various points in the middle and fill in all the gaps afterwards. But when we actually go across the bridge, we start at one end and finish at the other.

One of the easiest mistakes to make in a proof is to *write it down in the order you thought of it.* This may contain all the right steps, but if they're in the wrong order it's no use. It's like taking a piece of music and playing all the notes in a different order. Or writing a word with all the letters in the wrong order.

This means that for all but the simplest proofs, you'll probably need to plan it out in advance of actually writing it down. Like building a long bridge or a large building – it needs some planning, even though building a small bridge or a tiny hut might not.

3 What sort of things do we try and prove?

Here is a classification of the sorts of things we prove (this list is not exhaustive, and it's also not clear cut – there is some overlap, depending on how you look at it):

1. $x = y$ i.e. "something equals something else"
2. $x \Longrightarrow y$
3. $x \iff y$
4. x is purple (or has some other interesting and relevant property)
5. $\forall x\ p(x)$ is true i.e. "all animals of a certain kind x behave in a certain way $p(x)$"
6. $\exists x$ s.t. $p(x)$ is true i.e. "there is an animal that behaves in a certain way $p(x)$"
7. Suppose that a, b, c and d are true. Then e is true. [Note that this is just a version of 2 in disguise.]

4 The general shape of a proof

Let's now have a look at the general shape of a proof, before taking a closer look at what it might look like for each of the cases above. **We must always remember that there is a beginning, a middle and an end.**

Example 1. *Using the field axioms, prove that $a(b-c) = ab - ac$ for any real numbers a, b, c. You may use the fact that $x.0 = 0$ for any real number x.*

BEGINNING field axioms
definition $x - y = x + (-y)$
given $x.0 = 0$

MIDDLE

$$\begin{aligned} a(b-c) &= a(b+(-c)) && \text{definition} \\ &= ab + a(-c) && \text{distributive law} \\[1em] ac + a(-c) &= a(c+(-c)) && \text{distributive law} \\ &= a.0 && \text{additive inverse} \\ &= 0 && \text{given} \\ \therefore\ a(-c) &= -(ac) && \text{definition of additive inverse} \\[1em] \therefore\ ab + a(-c) &= ab - ac \end{aligned}$$

END $\therefore$ by line 2, $a(b-c) = ab - ac$ as required □

Example 2. *Let f and g be functions $A \xrightarrow{f} B \xrightarrow{g} C$. Show that if f and g are injective then $g \circ f$ is injective*

BEGINNING definition of injective

definition $(g \circ f)(a) = g(f(a))$

assumption that f and g are injective i.e.

$\forall a, a' \in A \quad f(a) = f(a') \Longrightarrow a = a'$

$\forall b, b' \in B \quad g(b) = g(b') \Longrightarrow b = b'$

MIDDLE

$$\begin{aligned} (g \circ f)(a) = (g \circ f)(a') &\Longrightarrow g(f(a)) = g(f(a')) && \text{by definition} \\ &\Longrightarrow f(a) = f(a') && \text{since g is injective} \\ &\Longrightarrow a = a' && \text{since f is injective} \end{aligned}$$

$$\therefore (g \circ f)(a) = (g \circ f)(a') \Longrightarrow a = a'$$

END i.e. $g \circ f$ is injective, as required □

Example 3. *Prove by induction that $\forall n \in \mathbb{N}, 1 + \cdots + n = \dfrac{n(n+1)}{2}$*

BEGINNING Principle of Induction

MIDDLE

$$\begin{aligned} \text{for } n = 1, \text{ LHS} &= 1 \\ \text{RHS} &= \frac{1(1+1)}{2} \\ &= 1 \end{aligned}$$

$\therefore$ result is true for $n = 1$

If result is true for $n = k$ then

$$\begin{aligned} 1 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} && \text{i.e. result true for } n = k+1 \end{aligned}$$

$\therefore$ result true for $k \Longrightarrow$ result true for $k+1$

END $\therefore$ by the Principle of Induction, the result is true for all $n \in \mathbb{N}$ □

Of course, when we write a good story, we don't actually *label* the beginning, the middle and the end with BEGINNING, MIDDLE, and END – it's supposed to be sort of obvious where they are. The same is true of a proof. So here's the thing I keep going on about but which is apparently not as obvious as it might sound:

> **The end of a proof should come at the end, not at the beginning.**

Of course, I've deliberately made it sound really obvious there. But here's a more illuminating way of putting it:

> **The proof should *end* with the thing you're trying to prove. The proof should not *begin* with the thing you're trying to prove.**

This is not to be confused with the fact that we often begin by *announcing* what the end is going to be. This is a bit like a story that starts at the end and then the entire story is a flashback. Like *The Go-Between* or *Brideshead Revisited* or *Rebecca.* Or, it's like taking someone on a journey – you might well tell them where you're going right at the start. But once you've told them what the destination is *you still start the journey from the beginning.* The same is true of proofs. Even if we begin by announcing what the end is going to be, *we then have to start at the beginning* and work our way to the pre-announced end.

5 What doesn't a proof look like?

There are more plastic flamingoes in America than real ones.

There are more bad novels in the world than good ones, and there are more bad proofs in the world than good ones. Here are some of the most popular ways to write a bad proof.

1. Begin at the end and end at the beginning

This is a really, really terrible thing to do. This might be even worse than leaving out gaps in the middle. Because if you begin at the end and end at the beginning you *monumentally* haven't got where you're trying to go. Here's an example of this for Example 1 from Section 4:

$$\begin{aligned}
\mathsf{a(b-c)} &= \mathsf{ab-ac}\\
\mathsf{ab+a(-c)} &= \mathsf{ab-ac}\\
\mathsf{a(-c)} &= \mathsf{-ac}\\
\mathsf{ac+a(-c)} &= \mathsf{0}\\
\mathsf{a(c+(-c))} &= \mathsf{0}\\
\mathsf{a.0} &= \mathsf{0}\\
\mathsf{0} &= \mathsf{0} \qquad \square
\end{aligned}$$

Try comparing this with the *good* proof given in Section 4 – you'll see that all the correct steps are there, but they're all in the wrong order.

Sense any make doesn't it backwards but things right the write you if.

This is a terrible thing to do but not a terminal catastrophe – if you have all the right ideas but in the wrong order, all you need to do is work out how to put them in the right order...

2. Take flying leaps instead of earthbound steps.

This category includes leaping from one statement to another

- without justifying the leap
- leaving out too many steps in between
- using a profound theorem without proving it
- (worse) using a profound theorem without even mentioning it

For example, spot the flying leap in the following "proof":

$$\begin{aligned} \mathsf{a(b-c)} &= \mathsf{ab + a(-c)} \\ &= \mathsf{ab - ac} \qquad \square \end{aligned}$$

3. Take flying leaps and land flat on your face in the mud

By which I mean making steps that are actually wrong. The end may well justify the means in some worlds, but in mathematics if you use the wrong means to get to the right end, you haven't actually got to the end at all. You just think you have. But it's a figment of your imagination. Here's an example of a very imaginitive "proof" that is definitely flat on its face in the mud:

$$\begin{aligned} \mathsf{a(b-c)} &= \mathsf{ab + a(-c)} \\ &= \mathsf{ab + a(-c) + a.1} \\ &= \mathsf{ab + a(1-c)} \\ &= \mathsf{ab - ac} \qquad \square \end{aligned}$$

Of course, it's even worse if you do something illegal and thereby reach a conclusion that isn't even true. Like

$$\mathsf{x}^2 = \mathsf{y}^2 \Longrightarrow \mathsf{x} = \mathsf{y}$$

or

$$\mathsf{x}^2 < \mathsf{y}^2 \Longrightarrow \mathsf{x} < \mathsf{y}.$$

What is wrong with these two "deductions"?

4. Handwaving

Handwaving is when you arrive at a statement by some not-very-mathematical means. The step isn't necessarily wrong, but you haven't arrived at it in a good logical manner. Perhaps you had to resort to writing a few sentences of prose in English rather than Mathematics-speak. This is often a sign that you've got the right idea but you haven't worked out how to express it. Spot the handwaving here – you can see it from a mile off:

$$\begin{aligned} \mathsf{a(b-c)} &= \mathsf{ab + a(-c)} \\ \mathsf{a(-c)} &= \mathsf{-ac} \qquad \text{because if you add ac to} \\ & \qquad \text{both sides then both sides vanish} \\ & \qquad \text{which means they're inverse} \\ \\ \therefore \mathsf{ab + a(-c)} &= \mathsf{ab - ac} \qquad \square \end{aligned}$$

Handwaving is bad but is not ultimately catastrophic – you just need to learn how to translate from English into Mathematics. This is probably easier to learn than the problem of coming up with the right idea in the first place.

5. Incorrect logic

This includes the two great classics

- negating a statement incorrectly
- proving the converse of something instead of the thing itself

What is the negation of the following statement:

$$\forall\varepsilon > 0\ \exists\delta > 0 \text{ s.t. } \forall x \text{ satisfying } 0 < |x-a| < \delta, \quad |f(x) - l| < \varepsilon$$

The correct answer is at the bottom of the page[1]. If you get it wrong, you go directly to Jail. Do not pass Go. Do not collect $200.

6. Incorrect assumption

You could have all your logic right, you could make a series of perfectly good and sensible steps, but if you start in the wrong place then you're not going to have a good proof. Or, if you use any assumption along the way that simply isn't true, then it's all going to go horribly pear-shaped...

7. Incorrect use of definitions – or use of incorrect definitions

This is a very, very avoidable error. Especially if it's not a test and so you have all your notes and all the books in the world to consult: getting the definitions wrong is a really

[1] $\exists\varepsilon > 0$ s.t. $\forall\delta > 0\ \ \exists x$ satisfying $0 < |x-a| < \delta$ s.t. $|f(x) - l| \geq \varepsilon$

pointless way of going wrong. What's wrong with the following "proof" for the second example from Section 4?

$$\begin{aligned} \mathsf{f}(\mathsf{a}) = \mathsf{f}(\mathsf{a}') &\implies \mathsf{a} = \mathsf{a}' \\ \mathsf{g}(\mathsf{a}) = \mathsf{g}(\mathsf{a}') &\implies \mathsf{a} = \mathsf{a}' \end{aligned}$$

$$\begin{aligned} (\mathsf{g} \circ \mathsf{f})(\mathsf{a}) = (\mathsf{g} \circ \mathsf{f})(\mathsf{a}') &\implies \mathsf{g}(\mathsf{a}) \circ \mathsf{f}(\mathsf{a}) = \mathsf{g}(\mathsf{a}') \circ \mathsf{f}(\mathsf{a}') \\ &\implies \mathsf{a} = \mathsf{a}' \end{aligned}$$

$$\therefore\ \mathsf{g} \circ \mathsf{f} \textsf{ is injective.} \qquad \square$$

8. Assuming too much

This is a tricky one, especially when you're a student at the beginning of a course. What are you allowed to assume? How much do you have to justify each step? A good rule of thumb is:

> *You need to justify everything enough for your peers to understand it.*

This is not a hard and fast rule, but it's a guideline that will always remain true however far you progress in mathematics, even if you become an internationally acclaimed Fields-medal-winning mathematician. The point is that as you become more advanced your peers do too, so you are eventually going to be taking bigger steps in your proofs than you do now. i.e. don't worry, you won't be required to write down every use of the distributive law forever!

> *If in doubt, justify things more rather than less.*

Very few people give too much explanation of things. In fact, I have only ever encountered one student who consistently explained things too much.

6 Practicalities: how to think up a proof

The harsh reality is that when you sit down to prove something you usually have to start by just **staring** at it really hard and hoping for some inspiration to hit you. However, you can put yourself in the best possible place to find that inspiration by doing some of the following things, probably on a piece of rough paper.

- Write out the BEGINNING very carefully. Write down the definitions very explicitly, write down the things you are allowed to assume, and write it all down in careful mathematical language.

- Write out the END very carefully. That is, write down the thing you're trying to prove, in careful mathematical language.

- Try and manipulate both the beginning *and* the end to try and make them look like one another. This is like building from both ends of the bridge until they meet in the middle, and it's okay as long as you *write the whole thing out properly in the right order afterwards.*
- Take big leaps to see what happens, and then make the big leaps into smaller leaps afterwards.
- See if the situation reminds you of any situations you've ever seen before. If so, perhaps you can copy the method.

You should *always* read over your proof after you've written it to make sure every single step makes sense. When you're writing a proof the first time through, you might get carried away in a frenzy of inspiration and become blind to the world around you – by which I mean that you might do something wrong without noticing it. It's important to go back in a calm state and *pretend to be more stupid than you are.* Or more sceptical. Or untrusting. When you finish a proof you should feel like you understand what's going on, but you should go back over it pretending that you *don't* understand, and see if your proof explains it to you.

7 Some more specific shapes of proofs

Now let's look at the various types of THINGS that we try to prove (as listed in Section 3), and think about how we can prove them.

1. $x = y$ or "something equals something else"

The proof might take the following general shape:

$$\begin{aligned} \mathsf{x} &= \mathsf{a} \\ &= \mathsf{b} \\ &= \mathsf{c} \\ &= \mathsf{d} \\ &= \mathsf{y} \qquad\qquad \square \end{aligned}$$

Or:

$$\begin{aligned} \mathsf{x} &= \mathsf{a} \\ &= \mathsf{b} \\ &= \mathsf{c} \\[2ex] \mathsf{y} &= \mathsf{e} \\ &= \mathsf{d} \\ &= \mathsf{c} \\[2ex] \therefore \mathsf{x} &= \mathsf{y} \qquad\qquad \square \end{aligned}$$

Note that this is *very* different from:

$$\begin{array}{ccc} \mathsf{x} & = & \mathsf{y} \\ \mathsf{a} & = & \mathsf{e} \\ \mathsf{b} & = & \mathsf{d} \\ \mathsf{c} & = & \mathsf{c} \qquad\qquad \square \end{array}$$

2. $x \Longrightarrow y$

Now the proof might look like this:

$$\begin{array}{ccl} \mathsf{x} & \Longrightarrow & \mathsf{a} \\ & \Longrightarrow & \mathsf{b} \\ & \Longrightarrow & \mathsf{c} \\ & \Longrightarrow & \mathsf{d} \\ & \Longrightarrow & \mathsf{y} \qquad\qquad \square \end{array}$$

Or:

$$\begin{array}{lccc} \text{We know that} & \mathsf{a} & \Longrightarrow & \mathsf{b} \\ \\ \text{Also} & \mathsf{a} & \Longleftrightarrow & \mathsf{x} \\ \text{and} & \mathsf{b} & \Longleftrightarrow & \mathsf{y} \\ \\ \therefore & \mathsf{x} & \Longrightarrow & \mathsf{y} \qquad\qquad \square \end{array}$$

3. $x \iff y$

Now the proof might look like this:

$$\begin{array}{rccl} & \mathsf{x} & \Longrightarrow & \mathsf{a} \\ & & \Longrightarrow & \mathsf{b} \\ & & \Longrightarrow & \mathsf{c} \\ & & \Longrightarrow & \mathsf{d} \\ & & \Longrightarrow & \mathsf{y} \\ \\ \text{Conversely} & \mathsf{y} & \Longrightarrow & \mathsf{p} \\ & & \Longrightarrow & \mathsf{q} \\ & & \Longrightarrow & \mathsf{r} \\ & & \Longrightarrow & \mathsf{x} \\ \\ \text{Hence} & \mathsf{x} & \Longleftrightarrow & \mathsf{y} \qquad\qquad \square \end{array}$$

Or

$$\begin{aligned} \mathsf{x} &\iff \mathsf{a} \\ &\iff \mathsf{b} \\ &\iff \mathsf{c} \\ &\iff \mathsf{d} \\ &\iff \mathsf{y} \qquad\qquad \square \end{aligned}$$

However, beware that this can be a dangerous way of taking a short cut – you might find that you're going the wrong way up a one way street. Do those implications *really* work backwards? It's always safer to do the forwards and the backwards separately, and write "conversely" at the point where you're about to start doing the converse direction.

4. x is purple

A good way to start is to write down the definition. What does it mean for x to be purple?

"x is purple" means y

We know a and

$$\begin{aligned} \mathsf{a} &\implies \mathsf{b} \\ &\implies \mathsf{c} \\ &\implies \mathsf{d} \\ &\implies \mathsf{y} \end{aligned}$$

$\therefore$ x is purple as required □

5. $\forall x, p(x)$ is true

In practice this will usually be "$\forall x$ of a certain kind", like "for any rational number x" or "for any continuous function f" or "for any braided monoidal category $\mathcal{C}$". Then the point is probably to *use the assumed properties of* x to prove $p(x)$. So a good way to start is to write down the definition of those assumed properties, carefully, in mathematical language. e.g.

> *Prove that any rational number can be expressed as $\frac{m}{n}$ where m and n are integers that are not both even.*

So we start by saying:

> Let x be a rational number. So x can be expressed as $\mathsf{\frac{p}{q}}$ where p and q are integers and $\mathsf{q} \neq 0$.

Note that we have picked an *arbitrary* x, and then we just can just prove that this x has the desired property, and we're done. You might say, "But we've only proved it for *this* x, and not *every* x". But the point is that this is a *random* x not one specific one, it's a sort of generic x that shows the proof will work for any specific one that we substituted in. It's not like proving the result for one particular number, say, 23.

6. $\exists x$ s.t. $p(x)$ is true

Here, all we have to do is *find one* x for which $p(x)$ is true. So we can just say "let $x = 23$" and then show that 23 has the desired property p. For example, prove that:

$$\exists\, \delta > 0 \;\text{ s.t. }\; |x| < \delta \implies |x^2| < \frac{1}{100}$$

Put $\delta = \frac{1}{10}$. Now $|x^2| = |x|^2$ so we have

$$|x| < \frac{1}{10} \implies |x^2| < \frac{1}{100} \qquad \square$$

This is fine; of course we could also have picked

$$\delta = \frac{1}{1000}$$

or

$$\delta = \frac{1}{476002}$$

The latter especially would be a little eccentric but would still be a perfectly valid (if violent) choice of δ to finish the problem off.

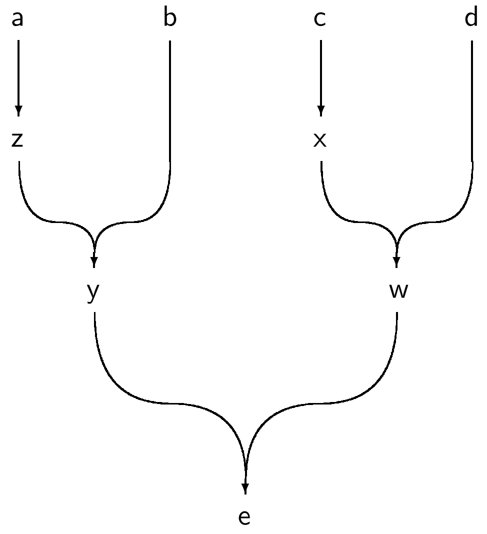
Of course, sometimes it's a bit hard to just pluck a valid x out of thin air. It's a bit like pulling a rabbit out of a hat – it looks like magic, but of course *you* are the one who put the rabbit there in the first place. So if it's a complicated example we probably work out (on a rough piece of paper) which x is going to do the trick, and once we have it all worked out we can pull it out of the hat.

7. If a, b, c, d are true then e is true

When you have a whole lot of things $(a, b, c, d, \ldots)$ you're allowed to assume, it gets more complicated. You might have to develop several parts of it sort of at the same time before proceeding to the end, like a novel where there are several strands of plot happening at the same time before they all come together at the end for the final *dénouement*. The proof might look like this:

$$\begin{array}{rcl} \text{a} & \implies & \text{z} \\ \text{b and z} & \implies & \text{y} \\ \text{c} & \implies & \text{x} \\ \text{x and d} & \implies & \text{w} \\ \text{y and w} & \implies & \text{e} \qquad \square \end{array}$$

In fact if we draw a little picture of what happened, it's much easier to see what's going on (and see where the beginning, the middle and the end have got to):



Here's an example of this phenomenon at work:

Prove that if $a > 0 \ \in \mathbb{R}$ then $a^2 > 0$. You may assume that for all $x, y \ \in \mathbb{R}$, $(-x)(y) = -(xy)$ and $-(-x) = x$.

Now $a < 0$ means

$$0 - a \in \ P$$

i.e.

$$-a \in P.$$

Therefore

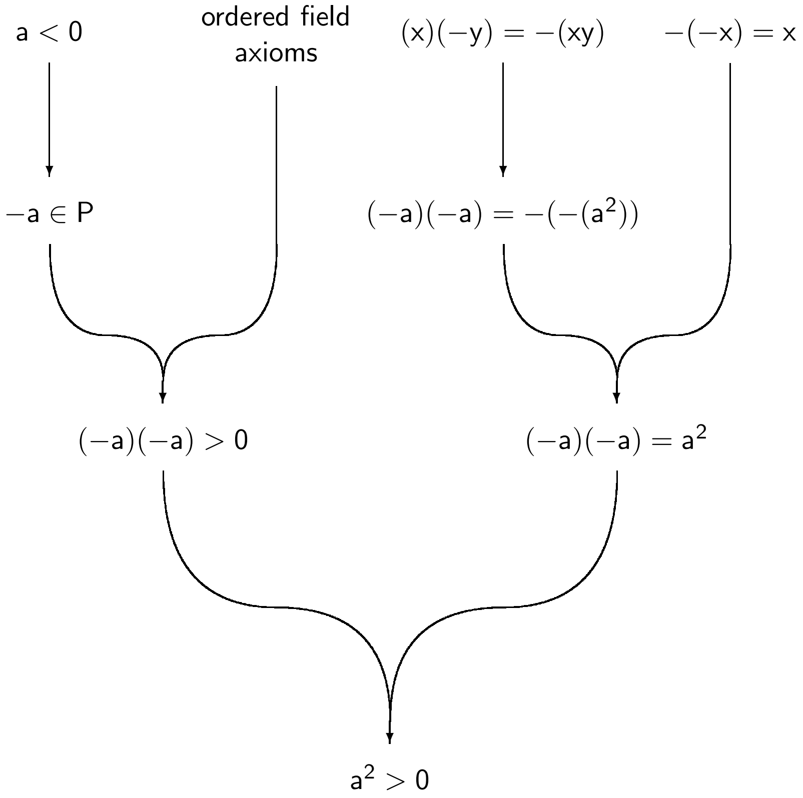
$$(-a)(-a) \in P$$

by closure of P under multiplication. Now

$$\begin{aligned} (-a)(-a) &= -a(-a) && \text{by the first given assumption} \\ &= -((-a)(a)) && \text{commutativity of multiplication} \\ &= -(-(a^2)) && \text{first given} \\ &= a^2 && \text{second given} \end{aligned}$$

$$\therefore \ (-a)(-a) > 0 \implies a^2 > 0 \ \text{ as required} \qquad \square$$

And here's the picture of it:



8 Proof by contradiction

Proof by contradiction is a very useful technique which it's important to understand. The idea is that a statement P is either true or false. So if it isn't false then it *must be true.* So instead of proving that P *is true*, we can prove that P *isn't be false* – because if it isn't false then it must be true. We then show that P being false *contradicts* something we know to be true, and this means that P can't possibly be fase, so it must be true.

To summarise:

- We are trying to prove that some statement P is true.
- We say "suppose P were not true", and find a contradiction
- Since P being false gives a contradiction, we deduce that P must be true.

We usually write a big # at the point where we reached the contradiction, to draw attention to it.

Here's an example:

Using the field axioms, prove that 0 has no multiplicative inverse in $\mathbb{R}$.

Suppose that 0 *does* have a multiplicative inverse. This means

$$\exists \mathsf{x} \text{ s.t. } 0.\mathsf{x} = 1$$

But we know that

$$0\mathsf{x} = 0 \ \forall \mathsf{x} \in \mathbb{R}$$

and

$$0 \neq 1 \quad \#$$

$\therefore$ $0.x$ has no multiplicative inverse. □

9 Exercises: What is wrong with the following "proofs"?

Example 1. *Prove that $\forall x \neq 0 \in \mathbb{R}$,*

$$\left|\frac{1}{x}\right| = \frac{1}{|x|}.$$

$$\begin{aligned}
\left|\frac{1}{x}\right| &= \frac{1}{|x|} \\
x \geq 0 &\iff \frac{1}{x} \geq 0 \\
\text{so } \frac{1}{x} &= \frac{1}{x} \\
\\
x < 0 &\iff \frac{1}{x} < 0 \\
\text{so } -\frac{1}{x} &= \frac{1}{-x} \\
&= -\frac{1}{x} \qquad \square
\end{aligned}$$

Example 2. *Let f and g be functions $A \xrightarrow{f} B \xrightarrow{g} C$. Show that if f and g are injective then $g \circ f$ is injective*

$$\begin{aligned} \mathsf{f(a) = f(a')} &\implies \mathsf{a = a'} \\ \mathsf{g(a) = g(a')} &\implies \mathsf{a = a'} \\ \mathsf{(g \circ f)(a) = (g \circ f)(a')} &\implies \mathsf{g(f(a)) = g(f(a'))} \\ \text{But g injective} &\implies \mathsf{a = a'}. \end{aligned}$$

$\therefore$ g $\circ$ f is injective as required. □

Example 3. *Prove that $\forall a > 0 \in \mathbb{R}, \quad \exists x \in \mathbb{R} \quad s.t.\ x^2 > a$*

$$(2a)^2 = 4a^2 > a$$

$\therefore$ put $x = 2a$ □

Example 4. *Using only the field axioms, prove that $\forall x, y \in \mathbb{R}$*

$$x^2 - y^2 = (x+y)(x-y).$$

$$\begin{aligned} (x+y)(x-y) &= x(x-y) + y(x-y) && \text{distributive law} \\ &= x^2 + x(-y) + yx + y(-y) && \text{distributive law} \\ &= x^2 + x(-y) + xy + y(-y) && \text{commutativity of multiplication} \\ &= x^2 + x.(-1).(y) + xy + y.(-1).(y) && \text{additive inverse} \\ &= x^2 + xy.(-1) + xy + (-1).(y^2) && \text{commutativity of multiplication} \\ &= x^2 + xy(-1+1) - y^2 && \text{distributivity, additive inverse} \\ &= x^2 + xy(0) - y^2 && \text{additive inverse} \\ &= x^2 + 0 - y^2 && \text{definition of 0} \\ &= x^2 - y^2 && \text{additive identity} \end{aligned}$$

□