There are three main things that appear in proofs in this course.

- Some parts of proofs are *straight from the definitions.*
  In these proofs, almost every single sentence is just explaining the definitions of words. There are not any strategy to the proof, just at each step, do the only thing you can.
  What goes wrong in this kind of proof most often, is not having the first step correct, or misinterpretting what a definition tells you.
- Some parts of proofs are just playing with notation.
  You have seen this with the proof for matricies that $A(BC) = (AB)C$.
  What goes wrong in this kind of proof most often is you make a mistake about manipulating the notation or you can't figure out how to *introduce* notation that works out sensibly.
- Some proofs require clever and random ideas, that seem like they come out of nowhere.
  For assignments, I will generally give hints about these ideas, if you think you are stuck on an idea on an assignment question you are encouraged to ask about hints.
  For (non-bonus) questions on exams, every idea will be something you have seen in an assignment)

Examples of things going wrong.

Theorem If $f : A \to B$ and $g : B \to C$ are functions such that $g \circ f : A \to C$ is injective, prove that f is injective.

First sentence:

- f injective means that if $f(x) = f(y)$ then $x = y$.
  Problems what is x, what is y, is anything in the sentence you just wrote *something that you know?*.
- $g \circ f$ injective means that

$$(g \circ f(x) = g \circ f(y)) \Rightarrow (x = y)$$

  Problems what is x, what is y? It is very likely in your proof you will eventually need an x and a y, if you already write the sentence above, you might accidentally think things are true about your x, y.
- We know that if f and g are both injective then $g \circ f$ is injective and so we conclude f is injective.
  Problems This isn't a proof!!! What you said would also imply g is injective, but in fact, g doesn't have to be just because $g \circ f$ is!.

A Correct Proof.

Proof:
We need to show f is injective, which means we need to prove:

$$\forall x, y \in A, (f(x) = f(y)) \Rightarrow (x = y).$$

Let $x, y \in A$ be arbitrary.

We now need to prove

$$(f(x) = f(y)) \Rightarrow (x = y).$$

Assume $(f(x) = f(y))$.

Because $f(x) = f(y)$, and g is a function, we know $g(f(x)) = g(f(y))$.
(As a general rule, if you are writing a proof, and your theorem talks abouve a function, and you have an element in the domain of that function, you should apply that function to that element because it is the only thing a function is good for.)

Because $g \circ f$ is injective we know $(g(f(x)) = g(f(y))) \Rightarrow (x = y)$, and as $g(f(x)) = g(f(y))$ we conclude $x = y$.

This shows that $(f(x) = f(y)) \Rightarrow (x = y)$ and so we conclude f is injective.

One Solution to avoid problems.

Always start by setting yourself up to prove the thing you want to prove, don't be distracted by the meaning of the hypothesis, you will need to explain these later, but if you do it too soon you can distract yourself.

If you are proving any of $\exists$, $\forall$, $\Rightarrow$, etc., think about the general structure of such a proof and start the proof that corresponds to what you are trying to prove.

Once you unravel the setup of what you are trying to prove, think about how to apply hypothesis, use objects you are given, or other things you know.

Another solution (optional).

Before you start your proof, have a separate paragraph titled **discussion**:

Proof layout becomes:
Discussion
Explain definitions/hypothesis here, and what you need to show.

Proof
We now begin the proof... and remember, things you said in your discussion may not be known to be true.

Pattern of a forall proof

To prove:

$$\forall x \in A, P(x)$$

You will almost always write something of the general form:
Let $x \in A$ be arbitrary
A proof of P(x)
Because $x \in A$ was arbitrary, and we proved $P(x)$, we conclude $\forall x \in A, P(x)$.

Note that in this course, the expressions might involve vectors, but the same pattern still applies

- $\forall a_1, \ldots, a_n \in \mathbb{R}, (a_1\vec{v}_1 + \cdots + a_n\vec{v}_n = 0) \Rightarrow (a_1 = a_2 = \cdots = a_n = 0)$.
- $\forall \vec{v} \in V, \exists a_1, \ldots, a_n \in \mathbb{R}, \vec{v} = a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$

Pattern of an $\Rightarrow$ proof

To prove:

$$\mathcal{A} \Rightarrow \mathcal{B}$$

You will almost always write something of the general form:
Assume $\mathcal{A}$
A proof of $\mathcal{B}$
Because assuming $\mathcal{A}$ we could show $\mathcal{B}$ this proves $\mathcal{A} \Rightarrow \mathcal{B}$.

Note that in this course, the assertions $\mathcal{A}, \mathcal{B}$ could be something complicated, but the same patter still holds.

- $(a_1\vec{v}_1 + \cdots + a_n\vec{v}_n = 0) \Rightarrow (a_1 = a_2 = \cdots = a_n = 0)$

Example

The first few lines of a proof of

$$\forall a_1, \ldots, a_n \in \mathbb{R}, (a_1\vec{v}_1 + \cdots + a_n\vec{v}_n = 0) \Rightarrow (a_1 = a_2 = \cdots = a_n = 0).$$

(which means $\vec{v}_1, \ldots, \vec{v}_n$ are linearly independent, we will define that later)
would look like

Let $a_1, \ldots, a_n \in \mathbb{R}$ be arbitrary.
Assume that $a_1\vec{v}_1 + \cdots + a_n\vec{v}_n = 0$.
We now need to prove $a_1 = a_2 = \cdots = a_n = 0$.

how you do this will clearly depend on the meaning of all those symbols and whatever hypothesis you have

Pattern of a subset proof

To prove:

$$\mathcal{A} \subset \mathcal{B}$$

You will almost always write something of the general form:
Let $x \in \mathcal{A}$ be arbitrary
A proof that $x \in \mathcal{B}$
Because $x \in \mathcal{A}$ was arbitrary, and we proved $x \in \mathcal{B}$, we conclude every element of $\mathcal{A}$ is an element of $\mathcal{B}$ meaning that $\mathcal{A} \subset \mathcal{B}$.

Note that in this course, the set $\mathcal{A}$ could be something complicated:

- The intersection of vector space V_1 and V_2
- $\mathrm{Span}(\vec{x}_1, \ldots, \vec{x}_n)$

but the same patter still holds.

Pattern of a exists proof

To prove:

$$\exists x \in A, P(x)$$

You will almost always write:
Make use of some hypothesis that tell you some things exist
Consider $x =$ A construction of x based on things you know exist
A proof of P(x)
Because x is an example of something in A for which we know $P(x)$, we conclude $\exists x \in A, P(x)$.

Note that in this course, the expressions might involve vectors, but the same pattern still applies

- $\exists a_1, \ldots, a_n \in \mathbb{R}, \vec{v} = a_1\vec{v}_1 + \cdots + a_n\vec{v}_n$

Pattern of an equation proof

To prove something of the form

$$\mathcal{A} = \mathcal{B}$$

where $\mathcal{A}$ and $\mathcal{B}$ are some sort of equations you almost always want to do something like:

We calculate that

$$\begin{aligned} \mathcal{A} &= \text{this thing it equals} && \text{for this reason it is true} \\ &= \text{this other thing} && \text{for this other reason it is true} \\ &\vdots \\ &= \mathcal{B} \end{aligned}$$

which proves that $\mathcal{A} = \mathcal{B}$.

Sometimes it is easier to do a $LHS = \cdots$ and a $RHS = \cdots$ calculation and have them meet in the middle