Writing proofs

* Potential Reading - An introduction to Mathematical Reasoning by Peter J Eccles

What is a proof?

- a proof is a sequence of statements starting from statements we know to be true and finishing with the statement to be proved
- each statement is true because the earlier statements are true
- How do we link statements together?

Implication Signs

- $A \Rightarrow B$ means IF A is true then B is true
- which of the following are true?
  - $x^2 = 1 \Rightarrow x = 1$
  - $x^2 = 1 \Rightarrow x = \pm 1$
  - $x = \pm 1 \Rightarrow x^2 = 1$
  - $x = 1 \Rightarrow x^2 = 1$
- Standard proof layout

Statement A_1 which we know is true/ is given in the question

$\Rightarrow A_2$ (A_2 is true because A_1 is true)

$\Rightarrow A_3$

$\Rightarrow \ldots$

$\Rightarrow A_{n-1}$

$\Rightarrow A_n$ = Statement we wanted to prove (A_n is true because A_{n-1} is true)

At each stage maybe add a note as to why $A_i \Rightarrow A_{i+1}$ eg- by vector space axiom V3

Some types of Proofs + Examples

- Direct Proofs

Thm- The sum of two even integers is even

Proof

let m, n be even integers

$\Rightarrow m = 2i,\ n = 2j$ for $i, j \in \mathbb{Z}$

$\Rightarrow m+n = 2i + 2j$

$= 2(i+j)$ with $i+j \in \mathbb{Z}$

$\Rightarrow m+n$ is an even integer $\square$

- Proof by cases

Thm- x and x^2 have the same parity, $x \in \mathbb{Z}$

Proof

let x be even

$\Rightarrow x = 2i$ for some $i \in \mathbb{Z}$

$\Rightarrow x^2 = (2i)^2$

$= 2^2 i^2$

$= 2(2i^2)$

$\Rightarrow x^2$ is also even

let x' be odd

$\Rightarrow x' = 2i+1$ for some $i \in \mathbb{Z}$

$\Rightarrow x'^2 = (2i+1)^2$

$= 4i^2 + 4i + 1$

$= 2(2i^2 + 2i) + 1$

$\Rightarrow x'^2$ is odd

All integers are odd or even. The statement holds for odd + even

$\Rightarrow$ always true $\square$

- Proof by contradiction

Thm - $\sqrt{2}$ is irrational (can't be written as $\frac{a}{b}$ $a,b \in \mathbb{Z}$ $b \neq 0$)

Proof

Assume for contradiction that $\sqrt{2}$ is rational

$\Rightarrow \sqrt{2} = \frac{a}{b}$ for $a,b \in \mathbb{Z}$ $b \neq 0$

we can assume that a,b have no common factors ($\frac{a}{b}$ is in simplest form) (✡)

$\sqrt{2} = \frac{a}{b}$

$\Rightarrow 2 = \frac{a^2}{b^2}$) square both sides

$\Rightarrow 2b^2 = a^2$

$\Rightarrow a^2$ is even by definition

$\Rightarrow a$ is even (we proved this in proof by cases)

$\Rightarrow a = 2i$ for some $i \in \mathbb{Z}$

$\Rightarrow 2b^2 = (2i)^2$

$= 4i^2$

$= 2(2i^2)$

$\Rightarrow b^2 = 2i^2$

$\Rightarrow b^2$ is even

$\Rightarrow b$ is also even

Hence a and b share the common factor 2

This contradicts ✡

Therefore $\sqrt{2}$ cannot be written as $\frac{a}{b}$ □

Proof by Induction

Thm - $11^n - 6$ is divisible by 5 $\forall n \in \mathbb{N}$ (means for all $n \in \mathbb{N}$)

Proof

* Base case

  when $n = 1$ $\quad 11^1 - 6 = 5$

  5 is divisible by 5

  $\Rightarrow$ The statement is true for the base case

* Inductive hypothesis

  Assume the statement is true for $n = k$

  $\Rightarrow 11^k - 6$ is divisible by 5

  $\Rightarrow 11^k - 6 = 5i \quad i \in \mathbb{Z}$

* Inductive Step

  (Show the statement is true for $n = k+1$ using the fact we've assumed it is true for $n = k$)

$$11^{k+1} - 6 = 11(11^k) - 6$$

$11^k - 6 = 5i \Rightarrow 11^k = 5i + 6$

(Try and rewrite in terms of k)

$$= 11(5i + 6) - 6$$
$$= 5(11i) + 66 - 6$$
$$= 5(11i) + 60$$
$$= 5(11i + 12)$$

$\Rightarrow 11^{k+1} - 6$ is divisible by 5

$\Rightarrow$ Statement true for $k+1$

Hence by induction $11^n - 6$ is divisible by 5 for all $n \in \mathbb{N}$ $\quad \square$

When you're stuck

To start a question

1- Pick out each bit of important info in the question

2- Think of the definitions for each term

3- Can you think of any relevant theorems

4- Is there any way to rewrite the given information

At the end of a question

5- Check you've used each bit of info

6- have you answered each part of the question

7- have you linked your statements with words or "$\Rightarrow$"

8- have you defined all your notation

Example

Inside the vector space $\mathbb{R}^4$ consider the following set

$$U = \{(x, y, z, t) \in \mathbb{R}^4 \mid x - y = z,\ t = 2x\}$$

Prove that U is a subspace of $\mathbb{R}^4$. Write down an element of U and an element of $\mathbb{R}^4$ that does not belong to U

Start

1 - $U \subseteq \mathbb{R}^4$ (we know $\mathbb{R}^4$ is a vector space)

- we know the structure of U (we'll probably have to use this)

2 - let V be a vector space over a field F. A subspace W of V is a non-empty subset of V which it self forms a vector space under the same operations (we know the operations are the "usual" in $\mathbb{R}^4$)

3 - let V be a vector space over a field F. let W be a subset of V which is non-empty. Then W is a subspace of V iff

- $v, w \in W \Rightarrow v + w \in W$
- $v \in W \quad \alpha \in F \Rightarrow \alpha v \in W$

4 - $U = \{(x, y, z, t) \in \mathbb{R}^4 \mid x - y = z,\ t = 2x\}$

$= \{(x, y, x - y, 2x) \in \mathbb{R}^4\}$

Answer to the question (the only bit you need to write) 6

We can rewrite U as

$$U = \{(x, y, x-y, 2x) \in \mathbb{R}^4\}$$

- Setting $x = y = 0$ shows $(0,0,0,0) \in U$
  $\Rightarrow$ U is non-empty
- let $u, w \in U$
  $\Rightarrow$ $u = (x, y, x-y, 2x)$ $\quad x, y \in \mathbb{R}$
  $w = (a, b, a-b, 2a)$ $\quad a, b \in \mathbb{R}$

$$u + w = (x+a, y+b, (x-y)+(a-b), 2x+2a)$$
$$= (x+a, y+b, (x+a)-(y-b), 2(x+a))$$
$$\in U$$

let $\lambda \in F$

$$\lambda u = (\lambda x, \lambda y, \lambda(x-y), \lambda(2x))$$
$$= (\lambda x, \lambda y, \lambda x - \lambda y, 2(\lambda x))$$
$$\in U$$

$\Rightarrow$ U is a subspace of $\mathbb{R}^4$ by the subspace test

we have already shown $(0,0,0,0) \in U$

clearly $(0,0,0,1) \notin U$ as ~~$2(0) \neq 1$~~ $2(0) \neq 1$ and U requires $2x = t$

End of question

5 - used "$U \subseteq \mathbb{R}^4$" to apply subspace test
- used the definition of U several times

6 - yes, we've answered all 3 parts

7 - yes, everything is linked together, we've referenced the theorems we've used and the argument is easy to follow

8 - yes, we introduced $u, w, x, y, a, b, \lambda$ and we explained clearly where each element was from