Proofs - Part I

‘ For this particular part of the course we will rely on sections from Scheinerman’s book which has a good explanation of how a proof needs to be written. While it might be too detailed initially, it is important to establish the fundamentals.

Example of a proof

Consider the following statement of a result that we want to prove.

Theorem 1. *The sum of two even integers is even*

A possible proof goes as follows

1. We show that if x and y are even, then $x + y$ is even.
2. Let x and y be any even integers
3. Since x is even, by the definition of even integers we know that $2|x$
4. Similarly y being even means $2|y$
5. Since $2|x$ we know $\exists b \in \mathbb{Z}$ such that $x = 2b$
6. Similarly $\exists c \in \mathbb{Z}$ such that $y = 2c$
7. Now observe $x + y = 2b + 2c = 2(b + c)$
8. Therefore there is an integer a (which happens to equal $b + c$) such that $x + y = 2a$.
9. Therefore $2|(x + y)$
10. Therefore $x + y$ is even

The steps of a proof

The first step is to convert to statement of the theorem into logic. In this case we are able to convert it into an ‘if-then’ statement.

We also need to introduce some notation in order to begin the proof. For a universally quantified statement like this, we need to show that the statement holds for any value. Therefore it begins with x and y being even integers, but there is nothing special about the choice of these. It would be just as fine to say, ‘Consider any x and y even integers.’

Once we have our initial step of the proof, we write down what we need to show at the end of the proof. In this case, we need to show $x + y$ is even.

The rest of the proof consists of filling the space from the starting point to the end point.

Generally, it is a good idea to use definitions. We unravel the definition of even and of the word divisible. Once you have seen this a few times, you can jump directly to the step of saying that x is even implies $\exists a \in \mathbb{Z}$ such that $2a = x$. If you unravel the definitions all the way through, you get to step 6 and then seemingly you are stuck.

That is when you have to unravel the definitions that are in the final statement. You work your way backwards and get to step 8.

That gets to stage where you have to connect the top part of the proof with the bottom part of the proof. This middle-part of the proof generally the hard part. You have to establish a connection between what you've got and what you need.

In this particular case, manufacturing an a is not hard since we are able to produce one just by adding x and y and observing the result.

Proof for sets

There are two basic things to remember for proving things in set theory from first principles

Showing $A \subseteq B$

The technique is to consider any element $x \in A$ and then logically work out why $x \in B$.

Example Prove that $A = \{x \in \mathbb{Z} | 18 \text{ divides } x\}$ is a subset of $B = \{x \in \mathbb{Z} | 6 \text{ divides } x\}$

Proof:

Consider any $x \in A$. Then because $18|x$ this means $x = 18y$ for some $y \in \mathbb{Z}$. But that can be written as $x = 6(3y)$, so that means x is divisible by 6.

Therefore $x \in B$.

Since any $x \in A$ is also going to be in B, therefore $A \subseteq B$.

Showing A = B

The technique is to show $A \subseteq B$ and $B \subseteq A$.

Example: To show the distributive property of sets from first principle

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof:

First we need to show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Consider any $x \in A \cup (B \cap C)$

By definition $x \in A$ or $x \in B \cap C$

Case 1: $x \in A$

Then by definition of union $x \in A \cup B$ and $x \in A \cup C$.

By definition of interesection this would mean $x \in (A \cup B) \cap (A \cup C)$

That means $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Case 2: $x \in B \cap C$
By definition this means $x \in B \wedge x \in C$
By definition of union $x \in (A \cup B) \wedge x \in (A \cup C)$.
This would then mean $x \in (A \cup B) \cap (A \cup C)$.
That means $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$
So in both cases $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$

Now to show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$
Consider any $x \in (A \cup B) \cap (A \cup C)$
By definition $x \in A \cup B$ and $x \in A \cup C$
Consider $x \in A \cup B$. Then $x \in A$ or $x \in B$.
When $x \in A \cup C$. Then $x \in A$ or $x \in C$.
Combining everything there are two possibilities either $x \in A$ or $x \in B \cap C$.
Using the definition of $\cup$ this can just be written as $x \in A \cup (B \cap C)$.
We have therefore shown $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.
By showing $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$
and
$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.
we can now conclude that
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$