Topic for this Video: Section 4.1: Dirct Proof and Counterexample I

In this section, we begin discussing how to build proofs. Learning to build proofs is the biggest hurdle in the transition from lower level, computation-based courses like Calculus, to upper level, more abstract courses like Analysis or Abstract Algebra. I find that there is a rather frustrating attitude among some math teachers that writing proofs is a *mysterious* art that cannot be taught, that students either have the knack for it, or they don't.

While I certainly agree that there is often something mysterious about building a proof—a certain leap that has to be made, a connection that has to be spotted—I feel very strongly that there is much about building proofs that is *not mysterious*, and that can be taught. Much about the *structure* of a proof is inevitable: How the proof must begin and end, how definitions must be used in a proof, for example, do not involve any choices on the part of the proof writer. These things have to be done a certain way. Knowing what aspects of proof structure are inevitable allows the proof writer to build a sort of *frame* for the proof and to put in some proof steps. There may still remain leaps that have to be made, connections that have to be spotted, but they will be smaller leaps. That is what our book's Chapter 4 is about.

Because learning to build proofs can be difficult, it helps to start with proofs that are about very basic mathematical concepts. That way, the focus can be on the building of the proof, without the confusion of also having to understand a difficult mathematical concept. The concepts that we will use are just three:

- *Even & Odd Numbers*
- *Composite Numbers*
- *Prime Numbers.*

The definitions follow

Definition of Even and Odd Numbers

Words: n *is even*

Meaning: $\exists k \in \boldsymbol{Z}(n = 2k)$

Words: n *is odd*

Meaning: $\exists k \in Z(n = 2k + 1)$

Remark: As a consequence of the definition, *even* and *odd* numbers are *integers*.

Definition of Composite Numbers

Words: n *is composite*

Meaning: $\exists r, s \in \boldsymbol{Z}\big((1 < r < n) \wedge (1 < s < n) \wedge (n = rs)\big)$

Remark: As a consequence of the definition, every composite number will be an integer and will be greater than 1.

Definition of Prime Numbers

Words: n *is prime*

Meaning: $(n \in \boldsymbol{Z}) \wedge (n > 1) \wedge (n$ is not *composite*$)$

Remark: As a consequence of the definition, every integer that is greater than 1 will be either composite or prime. (exclusive or)

You will notice that the book presents its definitions as *if and only if* statements, written in words. For instance, the book's definition of Even and Odd Numbers is

Definitions

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, for any integer, n

$$n \text{ is even} \iff n = 2k \text{ for some integer } k$$
$$n \text{ is odd} \iff n = 2k + 1 \text{ for some integer } k$$

Personally, I prefer to write definitions in a way that makes it clear that the definitions are simply the introduction of new terminology, or new symbols. I feel that presenting definitions the way that I do makes it easier to understand how definitions must be used in a proof. That is the subject of our first discussion about proof structure.

Proof Structure: Using Definitions in a Proof

As mentioned earlier, I feel that there is much about building proofs that is *not mysterious*, and that can be taught. Much about the *structure* of a proof is inevitable. The first aspect of proof structure that we will discuss is how one *uses* a definition in a proof.

Suppose that, at some point in a proof, one wishes to prove that some number n is *even*. Since even is a defined term, there is no choice about how the proof would have to go.

⋮

(7) $\exists k \in \boldsymbol{Z}(n = 2k)$ (some justification provided for this step)

(8) n is *even* (by (7) and the *definition of even*)

⋮

On the other hand, suppose that one is given that a number n is even. The only thing that one can do with that information is include some lines in a proof like the following

⋮

(4) n is *even* (by given information)

(5) $\exists k \in \boldsymbol{Z}(n = 2k)$ (by (5) and the *definition of even*)

⋮

I refer to this second use of a definition as *unpacking the definition*. That is, we were given some information that included words that were defined terms—we were told that n *is even*—and we unpacked that abbreviated sentence and wrote what it really means on the next line.

The previous use of the definition could be thought of as *packing up the definition*. That is, we had some lengthy information, that $\exists k \in \boldsymbol{Z}(n = 2k)$, and we packed it up into the more abbreviated expression n *is even*.

[Example 1] (4.1#3) Suppose that m and n are particular integers.

(a) Is $6m + 8n$ even? Solution I think that $6m+8n$ is even.

We have to come up with an integer k that works

Observe: $6m+8n = 2\cdot(3m+4n) = 2k$

We have found an integer k such that $6m+8n = 2k$

let $k = 3m+4n$. Then k is an integer

Conclude that $6m+8n$ is even.

(b) Is $10mn + 7$ odd?

Solution: I think that $10mn+7$ is odd. So I must find an integer k that works,

$10mn+7 = 10mn+(6+1) = (10mn+6)+1 = 2(5mn+3)+1 = 2k+1$

Let $k = 5mn+1$. Observe that $k \in \mathbb{Z}$ and $10mn+7 = 2k+1$

Conclude $10mn+7$ is odd.

(c) If $m > n > 0$, is $m^2 - n^2$ composite?

example: let $n=1$, $m=2$

Then $m>n>0$ is true and $m^2-n^2 = 4-1 = 3$ is not composite! (it is prime)

Not always

example let $n=2$, $m=5$. Then $m^2-n^2 = 25-4 = 21 = 7\cdot 3$

notice $m^2-n^2 = (m+n)(m-n)$

$2^2-1^2 = (2+1)(2-1) = 3\cdot 1 = 3$ prime

Proof Structure: Proving Existential Statements

We have discussed how there is no choice about how *definitions* must be used in a proof. Another aspect of proof structure that does not involve any choice is issue of how one proves an *existential statement*. An existential statement says that an object (at least one) exists that has a certain property. There is only one way to prove such a statement.

Proving an Existential Statement

To prove the existential statement

There exists some $x \in D$ *such that* $P(x)$.

one must produce an *example* of an $x \in D$ that makes $P(x)$ true.

[Example 2] (4.1#8) Prove the following statement.

There is an integer $n > 5$ such that $2^n - 1$ is *prime*.

Solution try various values of n

n	2^n	$2^n - 1$	Prime?
6	64	63	no! $63 = 21 \cdot 3$
7	128	127	yes!

The number $n = 7$ is an example of an integer $n > 5$ such that $2^n - 1$ is prime

So the existential statement is true.

Proof Structure: Disproving Universal Statements

Recall that the negation of the *universal* statement S

$$\forall x \in D\big(P(x)\big)$$

is the the statement $\sim S$ which is an *existential* statement

$$\exists x \in D\big(\sim P(x)\big)$$

If one wishes to prove that the universal statement S is false, then one needs to prove that $\sim S$ is true. Since $\sim S$ is an existential statement, one proves $\sim S$ by providing an example. The example that proves $\sim S$ is true (and therefore S is ~~false~~ false) is called a counterexample for S.

~~Disroving~~ Disproving a Universal Statement

To disprove the universal statement

$$\textit{For all } x \in D,\ P(x).$$

one must produce an *example* of an $x \in D$ that makes $P(x)$ false. Such an example is called a counterexample.

[Example 3] (4.1#15) Disprove the following statement.

Statement S: For every integer p, if p is *prime* then $p^2 - 1$ is even.

$\sim S \equiv \sim(\forall p \in \mathbb{Z}\ (\text{IF } p \text{ is prime THEN } p^2-1 \text{ is even}))$

$\equiv \exists p \in \mathbb{Z}\ (\sim(\text{IF } \underbrace{p \text{ is prime}}_{A} \text{ THEN } \underbrace{p^2-1 \text{ is even}}_{B}))$

$\equiv \exists p \in \mathbb{Z}\ (\underbrace{p \text{ is prime}}_{A} \text{ AND } \underbrace{\sim(p^2-1 \text{ is even})}_{\sim B})$

$\equiv \exists p \in \mathbb{Z}\ (p \text{ is prime AND } p^2-1 \text{ is not even})$

p	p^2-1
2	$2^2-1 = 4-1 = 3$ odd!!
3	$3^2-1 = 9-1 = 8$ even
5	$5^2-1 = 25-1 = 24$ even
7	$7^2-1 = 49-1 = 48$ even

The number $p=2$ is a counterexample that shows that S is false.

Proof Structure: Proving Universal Statements by Method of Exhaustion

When a domain set D is a finite set, the *universal* statement

$$\forall x \in D\big(P(x)\big)$$

can be proven by confirming that $P(x)$ for each element of the domain.

This is called the ***Method of Exaustion***.

[Example 4] Let $D = \{-3, -2, 2, 3\}$. Prove $\forall x \in D(x^2 \geq x)$

x	x^2	$x^2 \geq x$	
-3	9	$9 \geq -3$	true
-2	4	$4 \geq -2$	true
2	4	$4 \geq 2$	true
3	9	$9 \geq 3$	true

This proves (by method of exhaustion) that $\forall x \in D(x^2 \geq x)$ is true.

Remark: In the video for Section 3.1 we let domain $D = \{-3, -2, 2, 3\}$ and let $A(x)$ be the predicate $x^2 \geq x$. We found that the truth set for the predicate $A(x)$ to be all of D. In other words, $\forall x \in D(x^2 \geq x)$.

Proof Structure: Proving Universal Statements by Method of Generalizing from the Generic Particular

When a domain set D is an infinite set, it is not possible to prove a universal statement $\forall x \in D\big(P(x)\big)$ by the Method of Exhaustion. Instead, one must use the method of *Generalizing from the Generic Particular*.

> **Generalizing from the Generic Particular**
>
> To show that *every* element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

So the proof structure would be

Start

(1) Suppose $x \in D$ (generic particular element)

⋮ some steps here

(*) we have shown that $P(x)$ is true. (some justification here)

End of proof

[Example 5] (4.1#31) Whenever n is an odd integer, $5n^2 + 7$ is even.

Proof Structure

(1) Suppose that n is an odd integer (generic particular element)

⋮ Some steps here

(*) $5n^2+7$ is even (some justification)

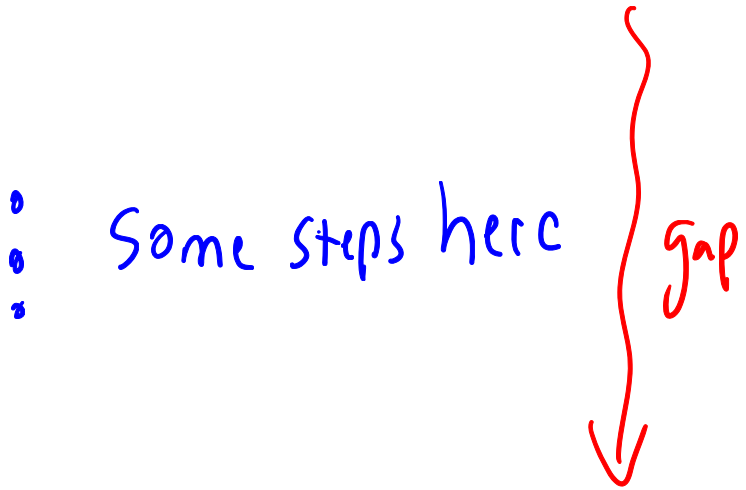
End of proof

Add some more structure that we have no choice about.

Proof Structure

(1) Suppose that n is an odd integer (generic particular element)

(2) There exists an integer k such that $n = 2k+1$ (by (1) and definition of odd)



(**) There exists an integer m such that $5n^2+7 = 2m$ (some justification)

(*) $5n^2+7$ is even (by (**) and definition of even)

End of proof

Proof

(1) Suppose that n is an odd integer (generic particular element)

(2) There exists an integer k such that $n = 2k+1$ (by (1) and definition of odd)

(3) $5n^2 + 7 = 5(2k+1)^2 + 7$ (by (2))

$= 5(4k^2 + 4k + 1) + 7$ by arithmetic

$= 20k^2 + 20k + 5 + 7$

$= 20k^2 + 20k + 12$

$= 2(10k^2 + 10k + 6)$

(4) let $m = 10k^2 + 10k + 6$.

Observe that m is an integer

(5) There exists an integer m such that $5n^2 + 7 = 2m$ (by 3, 4)

(6) $5n^2 + 7$ is even (by (5) and definition of even)

End of proof

Proof Structure: Proving Universal Conditional Statements by Method of Direct Proof

In the Section 3.1 (and its accompanying video), *universal conditional statements* were discussed. It was also discussed that it is often possible to express a *universal* statement in an equivalent form that is a *universal conditional* statement. For example, the universal statement from the previous example

Whenever n *is an odd integer,* $5n^2 + 7$ *is even.*

can be rephrased as a more obviously universal statement

For all n *in the set of odd integers,* $5n^2 + 7$ *is even.*

And this *universal* statement can be rephrased as a *universal conditional* statement.

For all n *in the set of integers, IF* n *is odd THEN* $5n^2 + 7$ *is even.*

When the method of *generalizing from the generic particular* is applied to a *universal conditional* statement, the resulting proof structure is called a *direct proof*.

Method of Direct Proof

1. Express the statement to be proved in the form "For every $x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

[Example 6] Revisit the *universal* statement from the previous example.

Whenever n is an odd integer, $5n^2 + 7$ *is even.*

Rewrite the *universal* statement as a *universal conditional* statement.

Then write the *frame* of the proof of the rewritten statement. That is write the first statement of the proof and the last statement of the proof.

For all integers n, If n is odd then $5n^2+7$ is even.

Proof Structure

(1) Suppose that n is an integer and that n is odd.

(generic particular element that satisfies the hypothesis)

(2) Some Steps

(*) Therefore $5n^2+7$ is even (some justification)

End of Proof

[Example 7] Consider the following *universal conditional* statement

$$\textit{For every integer } m, \textit{ IF } m > 1, \textit{ THEN } 0 < \frac{1}{m} < 1.$$

(a) (4.1#23) Write the *frame* of the proof. That is write the first statement of the proof and the last statement of the proof.

(b) Fill in the details of the proof.

(a) Solution

Proof Structure (Direct Proof)

(1) Suppose that m is an integer and $m > 1$ (generic particular element that satisfies the hypothesis)

o
o Some steps
o

(*) Therefore $0 < \frac{1}{m} < 1$ (Some justification here)

End of proof

Proof (Direct Proof)

(1) Suppose that m is an integer and $m > 1$ (generic particular element that satisfies the hypothesis)

(2) $0 < 1 < m$ (by (1))

multiply all three quantities by the positive number $\frac{1}{m}$

$$0 \cdot \frac{1}{m} < 1 \cdot \frac{1}{m} < m \cdot \frac{1}{m}$$

since m is positive, we know $m \neq 0$ so we can cancel $\frac{m}{m}$

(3) Therefore $0 < \frac{1}{m} < 1$ (by 2)

End of proof

End of Example

End of Video.