Tutorial 3: Introduction to Proof Writing

MATH 1200A02: Problems, Conjectures, and Proofs

Joe Tran (jtran0@yorku.ca)

York University

September 26, 2023

Contents

The Methods of Proof Writing

There are methods to writing proofs in mathematics:

1. Direct Proof
2. Proof by Contrapositive
3. Proof by Contradiction
4. Proof by Induction

In some, you might need to prove using cases, and in some statements that are false, the best way is to provide a counterexample.

Direct Proofs

Say we are given a statement $P \to Q$ is a true statement. To prove the statement directly,

1. Assume that P is true
2. Apply what you understand about P, i.e. definitions, facts, etc.
3. Use the steps about P to show that Q is true.

Let us first 'build' the direct proof of the following statement.

Theorem

If n is an odd integer, then $n+8$ is an odd integer.

Structure to Proof

1. Assume that n is an odd integer. (Hypothesis)
2. Since n is odd, there exists an integer $k \in \mathbb{Z}$ such that $n = 2k+1$ (definition of odd)
3. Then $n+8 = (2k+1)+8 = 2k+9 = 2k+8+1 = 2(k+4)+1$ (substitution to the conclusion)
4. Since $k \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition, it follows that $k+4 \in \mathbb{Z}$ as well (closure of $\mathbb{Z}$)
5. By the definition of an odd integer $2(k+4)+1$ is an odd integer (definition of odd).
6. This completes the proof. (Conclude the proof)

We can now transform the structure of the proof to an actual proof.

Proposition

If n is an odd integer, then $n+8$ is an odd integer.

Proof.

Assume that n is an odd integer. Since n is odd, there exists an integer $k \in \mathbb{Z}$ such that $n = 2k+1$. Then

$$n + 8 = (2k + 1) + 8 = 2k + 8 + 1 = 2(k + 4) + 1$$

Since $k \in \mathbb{Z}$ and since $\mathbb{Z}$ is closed under addition, it follows that $k + 4 \in \mathbb{Z}$, and therefore by the definition of an odd integer, $2(k+4)+1 = n+8$ is an odd integer, as desired. $\square$

Here is another example. Let us build our structure of proof.

Proposition

Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Structure of Proof

1. Assume that $a \mid b$ and $b \mid c$. (Hypothesis)
2. Since $a \mid b$, then there exists an integer $k_1 \in \mathbb{Z}$ such that $b = k_1 a$ (definition of divisibility)
3. Since $b \mid c$, then there exists an integer $k_2 \in \mathbb{Z}$ such that $c = k_2 b$ (definition of divisibility)
4. Substitute step (2) to (3) so that $c = k_2(k_1 a) = (k_1 k_2)a$ (algebraic steps)
5. Since $k_1, k_2 \in \mathbb{Z}$ and since $\mathbb{Z}$ is closed under multiplication, $k_1 k_2 \in \mathbb{Z}$ (closure of $\mathbb{Z}$)
6. By the definition of divisibility, $a \mid c$ (definition of divisibility)
7. This completes the proof. (Conclusion)

We can now transform the structure of the proof to an actual proof.

Proof.

Assume that $a \mid b$ and $b \mid c$. Since $a \mid b$, there exists an integer $k_1 \in \mathbb{Z}$ such that

$$b = k_1 a \tag{1}$$

Similarly, since $b \mid c$, there exists an integer $k_2 \in \mathbb{Z}$ such that

$$c = k_2 b \tag{2}$$

Now substitute (1) to (2) so that

$$c = k_2 k_1 a = (k_1 k_2) a$$

Note that since $k_1, k_2 \in \mathbb{Z}$ and since $\mathbb{Z}$ is closed under multiplication, it follows that $k_1 k_2 \in \mathbb{Z}$. Therefore, by the definition of divisibility, $a \mid c$ and the proof is complete. $\square$

Other Proof Methods

There are many other proof methods to show that $P \to Q$ instead of proving it directly. Say we want to prove $P \to Q$ using a proof by contradiction.

1. Assume that P is true.
2. Assume that $\neg Q$ is true.
3. Apply what you understand about P, i.e. definitions, facts, etc.
4. Apply what you understand about $\neg Q$, i.e. definitions, facts, etc.
5. Use the steps about P and $\neg Q$ to show that $\neg P$ is the contradiction.
6. Therefore, $P \to Q$ must be true.

Say we want to prove $P \to Q$ using a proof by contrapositive

1. Assume that $\neg Q$ is true.
2. Apply what you understand about $\neg Q$, i.e. definitions, facts, etc.
3. Use the steps about $\neg Q$ to show that $\neg P$ is true.
4. Therefore, $P \to Q$ must be true.