MAA 4102/5104 – Introduction to Advanced Calculus I

Notes on Proof Techniques

• The study of sets is fundamental to any area of mathematics. By a **set** we mean a collection of well-defined objects called **elements**, and by **well-defined** we mean that there is a definite way of determining whether or not a given element belongs to the set.

To write a set it is customary to use brackets $\{\}$, with elements of the set listed or described. Lowercase letters are generally used to represent the elements, whereas capital letters denote sets themselves.

If an element x belongs to the set A, then we write $x \in A$. If x is not an element of the set A, then we write $x \notin A$. For example, if $A = \{1, 2, 3\}$, then $1 \in A$, but $4 \notin A$.

There are many ways of describing any one particular set. For example, $D = \{2, 3\}$ can also be written as

$$D = \{x : x^2 - 5x + 6 = 0\}, \text{ or}$$

$$D = \{x : x \text{ is a prime number less than } 4\}.$$

The first set read as "x such that $x^2 - 5x + 6 = 0$", and the second as "x such that x is a prime number less than 4".

Sets of numbers encountered in this course are

$$\begin{aligned}
\mathbb{N} &= \text{set of all } \textbf{natural} \text{ numbers} = \{0, 1, 2, \dots\}, \\
\mathbb{Z} &= \text{set of all } \textbf{integers} = \{\dots, -2, -1, 0, 1, 2, \dots\}, \\
\mathbb{Q} &= \text{set of all } \textbf{rational} \text{ numbers} = \{x : x = \frac{p}{q},\ p \in \mathbb{Z},\ q \in \mathbb{Z} \setminus \{0\}\}, \\
\mathbb{R} &= \text{set of all } \textbf{real} \text{ numbers.}
\end{aligned}$$

One may wonder whether all real numbers are rationals. We will prove below that $\sqrt{2}$ is not rational. Real numbers that are not rationals are called **irrationals**.

• In mathematics we rarely say that some property is true most of the time. An expression is defined, and properties that will require proof are proposed. Those properties are either right or wrong. If we can demonstrate one situation, called a **counterexample**, in which the property in question is not true, then that property is false. Being unable to find a counterexample leads us to believe that a statement is true, but it remains a **conjecture** until we prove or disprove it. By **axiom** (or **postulate**) we mean a statement that is accepted without proof from which other propositions can be derived.

Results in mathematics are constructed from two parts. One part is made up of assumptions called **hypotheses** (plural for "hypothesis"). The second part is what must be proven. Of course, all previously proven results can be used to prove new problem. Results that are proven are usually called **theorems** or **propositions**. If some preliminary steps exist in preparation for the main statement, we call those preliminary results **lemmas**. Thus, we can say that every result can be made up of a sequence of lemmas or steps that require verification. Often, one can draw a few conclusions or consequences, called **corollaries**, from the main theorem. A corollary, like theorems and lemmas, requires a proof.

Suppose that P and Q represents statements, and we wish to prove that P implies Q (that is, assume P and prove Q). We write this as $P \implies Q$. Several ways exist to accomplish this task:

1. Mathematical induction can be attempted if the statement involves natural numbers.
2. A direct proof would involve writing the hypotheses in different ways and linking the ideas together. To complete these tasks successfully, knowledge of the definitions, the meaning of the given statement, and having an intuitive idea of the task are all necessary. So intuition and knowledge of material play a major part in success with proof writing.
3. A contrapositive proof, denoted by $\neg Q \implies \neg P$, involves proving that the negation of Q, that is, $\neg Q$ (not Q), implies the negation of P, that is, $\neg P$ (not P).
4. A proof by contraction involves assuming that P is true and Q is not. Since we assume that the negation of Q is true and want to prove that Q is true, a contradiction, that is, a statement that we know is false is expected. When a contradiction is reached, the proof of $P \implies Q$ is complete.

Writing proofs takes practice!

Let us illustrate the proof techniques with the following statements and their proofs:

Theorem 1. *Let $n \geq 1$. Then,*

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof. We use a proof by induction. For $n \geq 1$, denote by $P(n)$ the following statement

$$P(n) : \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Let us show that $P(1)$ is true. We have $\sum_{k=1}^{1} k^2 = 1^2 = 1$, and $\frac{1(1+1)(2\cdot1+1)}{6} = \frac{6}{6} = 1$. Hence, $P(1) : \sum_{k=1}^{1} k^2 = \frac{1(1+1)(2\cdot1+1)}{6}$ is true.

Now, let $n \geq 1$, and assume that $P(n)$ is true. We need to show that $P(n+1)$ is true, that is

$$P(n+1) : \sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

By induction hypothesis, we know that $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, it follows that

$$\begin{aligned}
\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\
&= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\
&= \frac{(n+1)[n(2n+1) + 6(n+1)]}{6} \\
&= \frac{(n+1)[2n^2 + 7n + 6]}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6}.
\end{aligned}$$

Hence, $P(n+1)$ is true. We conclude by induction that $P(n)$ is true for all $n \geq 1$. □

Theorem 2. *The sum of two odd integers is even.*

Proof. We use a direct proof. The statement can equivalently be written as: if $m, n \in \mathbb{Z}$ are odd, then $m + n$ is even. Let $m, n \in \mathbb{Z}$ be odd integers. Since they are odd, they can be written as $m = 2k + 1$ and $n = 2k' + 1$ for some integers $k, k' \in \mathbb{Z}$. Hence,

$$m + n = 2k + 1 + 2k' + 1 = 2(k + k') + 2 = 2(k + k' + 1) = 2k'',$$

where $k'' = (k + k' + 1) \in \mathbb{Z}$. Thus, $m + n$ is even, as it can be written as $m + n = 2k''$, with $k'' \in \mathbb{Z}$. □

Theorem 3. *Let $m \in \mathbb{Z}$. If m^2 is even, then m is even.*

Proof. We use a proof by contrapositive. Writing P: m^2 is even, and Q: m is even, Theorem 3 can be stated as

$$\forall m \in \mathbb{Z}, \quad P \implies Q.$$

To prove the theorem by contrapositive, we prove that $\forall m \in \mathbb{Z}$, $\neg Q \implies \neg P$. We have

$$\neg Q\colon m \text{ is odd},$$

$$\neg P\colon m^2 \text{ is odd}.$$

If m is odd, then $m = 2k+1$, for some $k \in \mathbb{Z}$. Thus, $m^2 = (2k+1)^2 = 4k^2+4k+1 = 2k'+1$, where $k' = 2k^2 + 2k \in \mathbb{Z}$. Hence, m^2 is odd. We have shown $\neg Q \implies \neg P$, which is equivalent to $P \implies Q$, and the theorem is thus proven. □

Theorem 4. *$\sqrt{2}$ is irrational.*

Proof. We use a proof by contradiction. Assume that $\sqrt{2}$ is rational, then it can be written as the quotient of two integers. After simplifying the fraction, we can write $\sqrt{2} = \frac{m}{n}$, where $m, n \in \mathbb{Z}$, $n \neq 0$, and m and n have no common factors.

Taking the square leads to

$$2 = \frac{m^2}{n^2}.$$

Hence, $m^2 = 2n^2$, and we deduce that m^2 is even. Since m^2 is even, we know from Theorem 3 above that m is even. It follows that $m = 2k$, for some $k \in \mathbb{Z}$. Thus, $2n^2 = m^2 = (2k)^2 = 4k^2$, which leads to $n^2 = 2k^2$. Thus n^2 is even. Again by Theorem 3 above, this implies that n is even. We conclude that m and n are even, and thus have 2 has a common factor, which is a contradiction. Since the statement "$\sqrt{2}$ is rational" leads to a contradiction, we conclude that $\sqrt{2}$ is irrational. □

Examples are used to illustrate given statements, but do not usually prove anything. As stated previously, if a statement is false, a counterexample is enough. To prove a statement it is often easier to prove an equivalent statement. Often, the negation of a statement is needed. Some examples of a statement P and its negation $\neg P$ are given below:

1. P: $\forall n \in \mathbb{N}, \quad n \geq n^2 - 1$

   $\neg P$: $\exists n \in \mathbb{N}$, such that $n < n^2 - 1$

2. P: $\exists x > 0$, such that $1 \leq |x| < 5$

   $\neg P$: $\forall x > 0$, $|x| < 1$ or $|x| \geq 5$

3. P: $\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x \in D,\ |x-a| \leq \delta \Longrightarrow |f(x)-f(a)| \leq \varepsilon$

   $\neg P$: $\exists \varepsilon > 0,\ \forall \delta > 0,\ \exists x \in D,\ |x-a| \leq \delta$ and $|f(x)-f(a)| > \varepsilon$

4. P: $\forall m \in \mathbb{Z},\ A \Longrightarrow B$

   $\neg P$: $\exists m \in \mathbb{Z},\ A$ and $\neg B$