Proof and Induction

Brief Notes

Mathematical argument

Writing mathematics clearly and carefully becomes increasingly important as you get further into the subject. Advanced mathematical arguments can have a complicated logical structure, and this structure must be clear to any reader (and even more importantly to the writer!).

In particular, written mathematics should not just be a list of equations but should make clear their logical relationship to each other. The careful use of words to express such relationships is important. For example, writing "$x \geq 1, x^2 \geq x$" is ambiguous, but "For all $x \geq 1$ we have $x^2 \geq x$" makes clear what is intended.

Styles of mathematical writing vary considerably. You should develop your own style using words as well as symbols, to make your arguments as clear as you can.

Implication

The notion of implication is fundamental in any mathematical argument. If A and B are statements then "A implies B" (in symbols A $\Rightarrow$ B) means that whenever A is true B must also be true. For example:

$$x = 2 \text{ implies } x^2 = 4.$$

Implication may be indicated in a variety of ways, such as:

A implies B, A $\Rightarrow$ B, B is implied by A, If A then B, B if A.

It is crucial to realise that "If A then B" and "If B then A" mean very different things. "If $x = 2$ then $x^2 = 4$" is true, but "If $x^2 = 4$ then $x = 2$" is false (x might be -2).

However, sometimes two statements A and B are each implied by the other, in which case we say "A and B are equivalent" (in symbols A $\Leftrightarrow$ B). Ways of writing this include:

A is equivalent to B, A $\Leftrightarrow$ B, A implies and is implied by B, A if and only if B,
A iff B, A is a necessary and sufficient condition for B.

For example, "$x^2 = 4$ if and only if $x = 2$ or $x = -2$". Note that if you are asked to show that A holds if and only if B holds you have to do *two* things.

Proof

A *proof* is a careful argument that establishes a new fact or *theorem*, given certain *assumptions* or *hypotheses*. There are various kinds of proof, some of which we mention here.

Proof by deduction

A deductive proof consists of a sequence of *statements* or *sentences* each of which is deduced from previous ones or from hypotheses using standard mathematical properties. The final statement may be called a *theorem*. For example:

Theorem. If $x^2 - 3x + 1 < 0$ then $x > 0$.

Deductive proof. Assume that $x^2 - 3x + 1 < 0$. Then $3x > x^2 + 1$ (rearranging the inequality), which implies that $3x > 1$ (since $x^2 \geq 0$). It follows that $x > \frac{1}{3}$ (dividing), so $x > 0$ (by the order property).

[Note that in this argument each step may be deduced from the previous one by a standard mathematical fact. However, the steps are not all reversible.]

Proof by contradiction

Sometimes it is easier to argue by contradiction, i.e. to assume that the desired conclusion is false and derive a contradiction to some known fact.

Theorem. If $x^2 - 3x + 1 < 0$ then $x > 0$.

Proof by contradiction. Assume that $x^2 - 3x + 1 < 0$ and suppose that $x \leq 0$. Then $x^2 < 3x - 1 \leq 3 \times 0 - 1$ (rearranging and using $x \leq 0$), so $x^2 < -1$, which contradicts that the square of a real number is non-negative. We conclude that $x > 0$.

Counter-examples

To show that a statement is false it is enough to give a single instance for which it does not hold, called a *counter-example.*

For example, the statement "$x^2 - 4x + 1 > 0$ for all $x > 0$" is false. To see this we simply note that $2^2 - 4 \times 2 + 1 = -3 \leq 0$, so that $x = 2$ is a counter-example to the statement. In particular, to demonstrate falsity there is no need to 'solve the inequality'.

Mathematical Induction

Mathematical induction is used to derive formulae and facts throughtout mathematics and we consider this in some detail. Induction is a method of proving statements involving the natural numbers $1, 2, 3, \ldots$. The idea is that (i) we prove the statement when $n = 1$ and (ii) show that if the statement is true for some integer n then it is true for the integer immediately above. From this we can conclude that the statement is true for all $n = 1, 2, 3, \ldots$. Formally:

The Principle of Mathematical Induction.

Let $P(n)$ be a statement depending on an arbitrary positive integer n. Suppose that we can do the following two steps:

(i) Verify that $P(1)$ is true,

(ii) for all positive integers n, show that if $P(n)$ is true then $P(n+1)$ is true.

Then the statement $P(n)$ is true for all positive integers n.

The statement $P(n)$ is called *the inductive hypothesis*, step (i) is called *starting the induction* and step (ii) is called *the inductive step.*

Note that the Principle of Induction is intuitively obvious: if $P(1)$ is true and $P(n) \Rightarrow P(n+1)$, that is the truth of $P(n)$ implies the truth of $P(n+1)$ for all $n = 1, 2, 3, \ldots$, then

$$P(1) \Rightarrow P(2) \Rightarrow P(3) \Rightarrow \ldots \Rightarrow P(n) \Rightarrow \ldots$$

by applying (ii) with $n = 1, 2, 3, \ldots$ in turn, so $P(n)$ is true for all n.

Note that induction is a general method that can be applied to many very different topics in mathematics. It is best understood by looking at specific examples.

Example 1 - Summation of series. Show that

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Proof by induction. Let $P(n)$ be the statement: $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$. Then $1 = \frac{1(1+1)}{2}$, so $P(1)$ holds, which starts the induction.

Now assume that $P(n)$ is true for some positive integer n. We relate the sum in $P(n+1)$ to that in $P(n)$:

$$\begin{aligned}
1 + 2 + \ldots + n + (n+1) &= (1 + 2 + \ldots + n) + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \qquad \text{(using } P(n)\text{)} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \frac{(n+1)((n+1)+1)}{2}
\end{aligned}$$

which is the statement $P(n+1)$, completing the inductive step.

Thus by the Principle of Induction $P(n)$ is true for all positive integers n.

Example 2 - Factors. Show that $9^n - 2^n$ is divisible by 7 for all positive integers n.

Proof by induction. Let $P(n)$ be the statement: $9^n - 2^n$ is divisible by 7. Then $9^1 - 2^1 = 7$ is divisible by 7, so $P(1)$ is true, which starts the induction.

Now assume that $P(n)$ is true for some positive integer n. We relate $P(n+1)$ to $P(n)$:

$$\begin{aligned}
9^{n+1} - 2^{n+1} &= 9(9^n - 2^n) + 2^n(9-2) \\
&= 9(9^n - 2^n) + 2^n 7
\end{aligned}$$

which is a multiple of 7 since $P(n)$ is assumed to be true. Thus $P(n+1)$ is true, completing the inductive step.

Thus by the Principle of Induction $P(n)$ is true for all positive integers n.

There are many variants on the Principle of Induction. For instance we may wish to start at an integer other than 1. Thus if for some integer n_0 we can show (i) that $P(n_0)$ is true and (ii) for all $n \geq n_0$ that if $P(n)$ is true then $P(n+1)$ is true, the Principle of Induction gives that $P(n)$ is true for all $n \geq n_0$.

Example 3 - Inequalities. Show that $2^n \leq n!$ for all integers $n \geq 4$

Proof by induction. Let $P(n)$ be the statement: $2^n \leq n!$. Then $2^4 = 16 \leq 24 = 4!$, so $P(4)$ is true, which starts the induction.

Now assume that $P(n)$ is true for some $n \geq 4$. We relate $P(n+1)$ to $P(n)$:

$$\begin{aligned}
2^{n+1} &= 2 \times 2^n \\
&\leq 2 \times n! \qquad \text{(using } P(n)\text{)} \\
&\leq (n+1) \times n! = (n+1)!
\end{aligned}$$

which is $P(n+1)$, completing the inductive step.

Thus by the Principle of Induction $P(n)$ is true for all $n \geq 4$.

There are other ways of presenting an inductive argument, but it is always important that the structure of the proof is clear. In the following example we use a different style with the inductive hypothesis denoted by $(*)$ rather than by $P(n)$.

Example 4 - Integration. Show that for all $n \geq 0$

$$\int_0^\infty x^n e^{-x} dx = n!. \qquad (*)$$

Proof by induction. We have

$$\int_0^\infty e^{-x} dx = \left[-e^{-x}\right]_0^\infty = 0 + 1 = 0!$$

which is $(*)$ when $n = 0$, and this starts the induction.

Now suppose that $(*)$ holds for some $n \geq 0$. Integrating by parts:

$$\begin{aligned}
\int_0^\infty x^{n+1} e^{-x} dx &= \left[x^{n+1} \times -e^{-x}\right]_0^\infty + \int_0^\infty e^{-x}(n+1)x^n dx \\
&= 0 + (n+1)\int_0^\infty e^{-x} x^n dx \\
&= (n+1)n! \qquad \text{(using } (*)\text{)} \\
&= (n+1)!
\end{aligned}$$

which is $(*)$ with "n" replaced by "$n+1$", and this is the inductive step.

Thus by induction $(*)$ holds for all integers $n \geq 0$.

Sometimes we need to use that $P(k)$ is true for all $k \leq n$ to deduce $P(n+1)$. Thus if we can show (i) that $P(1)$ is true and (ii) that if $P(k)$ is true for all $k \leq n$ then $P(n+1)$ is true, the Principle of Induction gives that $P(n)$ is true for all $n \geq 1$.

Recall that an integer $n \geq 2$ is a *prime number* if is cannot be expressed as a product of integers $n = rs$ with $r > 1$ and $s > 1$.

Example 5 - Prime factorisation. Every integer ≥ 2 is a product of prime numbers.

Proof by induction. Let $P(n)$ be the statement: n may be expressed as a product of prime numbers. Since 2 is prime, $P(2)$ is true, which starts the induction.

Now assume that for some $n \geq 2$, $P(k)$ is true for all integers $2 \leq k \leq n$. Consider the integer $n+1$. Either $n+1$ is prime (so a product of a single prime factor) or $n+1 = rs$ where $r > 1$ and $s > 1$. In the latter case $2 \leq r, s \leq n$, so by $P(r)$ and $P(s)$ both r and s are products of primes, so $n+1 = rs$ is a product of primes. Thus $P(n+1)$ is true, completing the inductive step.

The result follows by induction.

Induction is a general method that is used in virtually every area of mathematics. Further examples include complex numbers (e.g. for a proof of de Moivre's theorem), finding powers of matrices, terms of sequences, in number theory, graph theory, group theory, mathematical logic, ...