CHAPTER 2

Proof Techniques

2.1 Propositions

If P and Q are statements then

$$P \implies Q$$

means that P **implies** Q, i.e. that whenever P is true then Q must also be true. There are several other ways of saying this. Simplest is just "If P then Q", and there is "P only if Q". You can also say that P is a **sufficient condition** for Q; or that Q is a **necessary condition** for P. For example, if A is the statement "n is a prime" and B is the statement "n is a natural number" then $A \implies B$ is a **proposition**.

The sort of propositions that are important in mathematics are **theorem**s, **corollaries** (singular: **corollary**) and **lemma**s. Theorems are the most important: everybody knows about Pythagoras' Theorem. In this course, (and in other advanced mathematics) a theorem appears in two parts. The first is a statement of the theorem, with some sort of label like "Theorem 5" or "Lagrange's Theorem". The second part is the proof of the theorem which begins with the word "Proof" and ends with the symbol □. Lemmas are (usually short, easy) propositions that are used to prove theorems; corollaries are propositions that follow easily from theorems.

$\neg P$ is the negation of P, e.g. if A is the statement "n is a prime" then $\neg A$ would mean "n is not a prime."

If $P \implies Q$ and $Q \implies P$ we write '$P \iff Q$' or 'P **if and only if** Q'. We can also say P is a **necessary and sufficient condition** for Q. A shorthand way of writing "if and only if" is the odd-looking word **iff**.

Definition 2.1.1. The **converse** of '$P \implies Q$' is '$Q \implies P$'.

Note that we might have $P \implies Q$ being true but $Q \implies P$ being false. Can you think of statements P and Q for which this is so?

Definition 2.1.2. The **contrapositive** of '$P \implies Q$' is '$\neg Q \implies \neg P$'.

If $P \implies Q$ is true then its contrapositive is true, and vice versa. Thus we can say for any statements P and Q,

$$P \implies Q \qquad \text{iff} \qquad \neg Q \implies \neg P.$$

2.2 Direct Proofs

The most straightforward way of proving a theorem is by **direct proof**. To prove $P \implies Q$ we show

$$\begin{aligned} P &\implies A_1 \\ A_1 &\implies A_2 \\ A_2 &\implies A_3 \\ &\vdots \\ A_{n-1} &\implies A_n \\ A_n &\implies Q \end{aligned}$$

In writing such a proof, we generally omit the repetition of A_i on the next line, and we usually preface the initial P with 'Assume'. And, often the statement we are asked to prove is given in a convoluted way, so that it it's advisable to reorganise it by collecting *all the given conditions* as P and *what we have to deduce* as Q, and write this succinctly before we start the proof as:

RTP: $P \implies Q$

where 'RTP' stands for *Required To Prove*. And finally we like to say *we have finished the proof* with a little box: □. This is the modern fashionable way to end proofs; the old-fashioned way was to write QED which is short for "Quod erat demonstrandum," Latin for "which was to be demonstrated".

Putting all that together, our proof looks like this:

RTP: $P \implies Q$

Proof. Assume P
$\implies A_1$
$\implies A_2$
$\implies A_3$
$\vdots$
$\implies A_n$
$\implies Q$ □

Example 2.2.1.

Proposition. *The sum of two even integers is even.*

RTP: *a, b are even* $\implies$ *$a + b$ is even.*

Proof. Assume a, b are even.

$\implies a, b$ are multiples of 2
$\implies \exists m, n \in \mathbb{Z}$ such that $a = 2m$ and $b = 2n$
$\implies a + b = 2m + 2n$
$= 2(m + n)$
$\implies a + b$ is even. □

2.3 Proof by Contraposition

We said above that '$P \implies Q$' is equivalent to its contrapositive '$\neg Q \implies \neg P$'. Sometimes it's easier to prove the contrapositive proposition than the original one. Thus, to prove we can show that $\neg Q \implies \neg P$ by direct proof.

Example 2.3.1.

Proposition. *If $a \in \mathbb{Z}$ and a^2 is odd then a is odd.*

Proof. Suppose $\neg(a \text{ is odd})$.

$$\begin{aligned}
&\implies a \text{ is even} \\
&\implies \exists m \text{ such that } a = 2m \\
&\implies a^2 = 4m^2 = 2(2m^2) \\
&\implies a^2 \text{ is even} \\
&\implies \neg(a^2 \text{ is odd})
\end{aligned}$$

Thus the proposition is proved by contraposition. □

2.4 Proof by Contradiction

To prove a statement by contradiction, we show that the statement being false leads to an absurdity, leaving us to conclude that if the statement is not false, then in fact it is true.

Now a statement of form $P \implies Q$ is *vacuously true* whenever P is *false*. It is also *true* if Q is *true*.

This leaves the case when both P is *true* and Q is *false*. If we can show this combination of possibilities cannot occur, we will have shown that a statement of form: $P \implies Q$ is *true*.

Thus a proof of $P \implies Q$ generally starts by assuming P and $\neg Q$ and proceeds until a condition known to be untrue occurs, in which case we have what's termed a contradiction (which we can signal with a lightning bolt: $\lightning$), and are then able to deduce that the original statement was in fact true.

It is enormously helpful to the reader to add the phrase "*for a contradiction*" before the assumption $\neg Q$. Thus a contradiction proof is shaped like this:

Proof. Assume P and, for a contradiction, suppose $\neg Q$.

$$\begin{aligned}
&\implies \ldots \\
&\vdots \\
&\implies R \lightning \qquad [\text{where } R \text{ is something known to be untrue}]
\end{aligned}$$

Hence in fact, $P \implies Q$ (is true). □

If the reason for the contradiction is clear, then the symbol $\lightning$ is enough; often however a reason should be given in brackets after the $\lightning$ symbol.

It may happen that the statement is of form: Q. In this case, one can think of P as being true, and there is no need to write "Assume true".

The following famous result demonstrates a proof by contradiction.

Theorem 2.4.1. *The set of primes is infinite.*

Proof. For a contradiction, suppose there are only finitely many primes and label them

$$p_1 = 2 < p_2 = 3 < p_3 = 5 < \cdots < p_n.$$

Let $N = p_1 p_2 \cdots p_n + 1$. Now N is a product of primes,

$$\begin{aligned}
&\implies N \text{ is divisible by some prime in our list, say } p_i \\
&\implies \exists m \in \mathbb{Z} \text{ such that } N = p_i m \\
&\implies p_i m = p_1 p_2 \cdots p_n + 1 \\
&\implies p_i m - p_1 p_2 \cdots p_n = 1 \\
&\implies p_i(m - p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n) = 1 \;\lightning\; (p_i \,|\, \text{LHS, but } p_i \nmid \text{RHS})
\end{aligned}$$

Thus, in fact, the set of primes is infinite. □

2.5 Identities

An equation that it is true for any choice of the variables is called an **identity**. Some well-known identities that should be familiar to you are

$$\begin{aligned}
(a+b)^2 &= a^2 + 2ab + b^2 \\
(a-b)^2 &= a^2 - 2ab + b^2 \\
(a+b)(a-b) &= a^2 - b^2
\end{aligned}$$

To *prove* an identity, one starts with one side, e.g. the *lefthand side* (LHS), and by a sequence of steps reduces it to the other side, e.g. the *righthand side* (RHS). The proof should have this shape:

$$\begin{aligned}
\text{LHS} &= \cdots \\
&\vdots \\
&= \text{RHS}
\end{aligned}$$

As an example, we prove the first of the identities above:

$$\begin{aligned}
\text{LHS} &= (a+b)^2 \\
&= (a+b)(a+b) \\
&= a(a+b) + b(a+b) \\
&= a^2 + ab + ba + b^2 \\
&= a^2 + 2ab + b^2, && \text{since } ab = ba \\
&= \text{RHS}
\end{aligned}$$

2.6 Proof by Mathematical Induction

In this case we want to prove an infinite set of statements $P(1), P(2), P(3), \ldots$, or equivalently we want to prove,

$$\forall n \in \mathbb{N},\ P(n) \text{ is true.}$$

We prove this in two steps:

(i) We show that $P(1)$ is true.

(ii) We show that $\forall k \in \mathbb{N},\ P(k) \implies P(k+1)$.

Example 2.6.1.

Proposition. *If $n \in \mathbb{N}$ then*

$$P(n):\ 1+3+5+\cdots+(2n-1) = n^2 \tag{2.6.1}$$

Proof. (i) If $n = 1$ then the lefthand side of (2.6.1) equals 1, and the righthand side is $1^2 = 1$. So the proposition is OK for $n = 1$, i.e. $P(1)$ is true.
(ii) Suppose (2.6.1) is OK for k, i.e. suppose that $P(k)$ is true. Then

$$\begin{aligned} \text{LHS of } P(k+1) &= 1+3+\cdots+(2k-1)+(2(k+1)-1) \\ &= \text{LHS of } P(k) + 2k + 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 = \text{RHS of } P(k+1) \end{aligned}$$

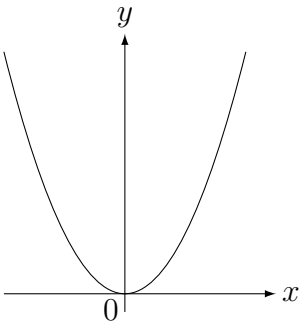
Thus $P(k+1)$ follows from $P(k)$.
Now from (i) and (ii) together, we have

$$1+3+5+\cdots+(2n-1) = n^2\ \forall n \in \mathbb{N}. \qquad \square$$

Note 2.6.2. Above we just introduced the idea of *Mathematical Induction*. In general, when we are asked to prove something by induction, the $P(n)$ won't be given. A good practice is to define the statement $P(n)$ at the beginning of your proof. Then step (i) is usually called the *base case* and step (ii) is called the *inductive step*. Finally, we usually have a *conclusion*, essentially saying that from (i) and (ii), by the *Principle of Mathematical Induction* we have the desired conclusion. For readability, it's nice to have the headings, *base case*, *inductive step*, and *conclusion* in your proof. You will see these embellishments in the next chapter.

2.7 Another example of a Direct Proof

Below we will need the following useful idea. Recall that the graph of $y = x^2$ looks like:



The important observation to make is that for any real number x, x^2 is never negative, and is only zero when x itself is zero, i.e.

$$x^2 \geqslant 0 \text{ for all real } x, \text{ and}$$
$$\text{if } x^2 = 0 \text{ then } x = 0.$$

This innocuous statement is *incredibly useful.* Keep it in your box of tricks!! We use it in the third line of the proof below.

Exercise 2.7.1. Prove that: If $a, b \geqslant 0$ then $\sqrt{ab} \leqslant \dfrac{a+b}{2}$.

Proof. Assume $a, b \geqslant 0$.

$$\begin{aligned}
&\implies \sqrt{a}, \sqrt{b} \text{ exist, i.e. are real numbers} \\
&\implies (\sqrt{a} - \sqrt{b})^2 \geqslant 0 \\
&\implies a - 2\sqrt{a}.\sqrt{b} + b \geqslant 0 \\
&\implies a + b \geqslant 2\sqrt{ab} \\
&\implies \frac{a+b}{2} \geqslant \sqrt{ab} \\
&\implies \sqrt{ab} \leqslant \frac{a+b}{2}.
\end{aligned}$$

□

2.8 More examples of Proofs by Contradiction

We gave a scheme for setting out a *proof by contradiction* of a statement of form '$P \implies Q$' earlier. The exercise below doesn't have a P part. One can think of the P as being *true* and just omit it; otherwise the structure is as it was given.

Exercise 2.8.1. Prove that: $\sqrt{2}$ is irrational.

Proof. For a contradiction assume that $\sqrt{2}$ is rational.

$$\begin{aligned}
&\implies \sqrt{2} = \frac{p}{q} \text{ for some } p, q \in \mathbb{Z} \text{ with } \gcd(p,q) = 1, \text{ i.e. } p/q \text{ is reduced to "lowest terms"} \\
&\implies 2 = \frac{p^2}{q^2} \\
&\implies 2q^2 = p^2 \\
&\implies 2 \,|\, p^2, \text{ since } 2 \,|\, 2q^2 \\
&\implies 2 \,|\, p \\
&\implies p = 2r \text{ for some } r \in \mathbb{Z} \\
&\implies 2q^2 = (2r)^2 = 4r^2 \\
&\implies q^2 = 2r^2 \\
&\implies 2 \,|\, q^2, \text{ since } 2 \,|\, 2r^2 \\
&\implies 2 \,|\, q \\
&\implies \gcd(p,q) \geqslant 2 \; \lightning (\gcd(p,q) = 1), \text{ since now } 2 \,|\, p \text{ and } 2 \,|\, q
\end{aligned}$$

$\therefore$ in fact, $\sqrt{2}$ is not rational.
$\therefore$ $\sqrt{2}$ is irrational. □

In many of the examples up to now we have not rewritten the problem with an RTP statement. When the "If part" and "then part" are clear, it's unnecessary. However, a problem where this device is particularly important is Exercise 7 (in the exercise set at the end of the chapter) which could be set out in the following fashion.

RTP: $x \in \mathbb{Q}, y \notin \mathbb{Q} \implies x + y \notin \mathbb{Q}$

Proof. Assume $x \in \mathbb{Q}, y \notin \mathbb{Q}$ and, for a contradiction, assume $x + y \in \mathbb{Q}$.

$$\begin{aligned} &\implies \dots \\ &\implies \dots \\ &\vdots \\ &\implies y \in \mathbb{Q} \lightning \\ &\therefore \text{ in fact, } x + y \notin \mathbb{Q} \\ &\therefore x \in \mathbb{Q}, y \notin \mathbb{Q} \implies x + y \notin \mathbb{Q} \end{aligned}$$

□

2.9 Relations

We now define various types of **binary relations**.

Definition 2.9.1. An **equivalence relation** is a binary relation $\sim$ on a set S that satisfies $\forall x, y, z \in S$:

E1: $x \sim x$, (**reflexivity**)

E2: $x \sim y \implies y \sim x$, (**symmetry**)

E3: $x \sim y$ and $y \sim z \implies x \sim z$. (**transitivity**)

Remark 2.9.2. An *equivalence relation* is essentially something that behaves like "=". Other examples are $\cong$ (*congruence*) on the set of triangles, $\sim$ (*similarity*) on the set of triangles, $\iff$ (*if and only if*) on the set of true-false statements.

The main reason we have includes the concept of an *equivalence relation* here, is that it helps explain a desirable way for setting out the proof of an **identity**. An *identity* is a statement of the form

$$\text{LHS} = \text{RHS},$$

that's generally true. The idea is that if we have a sequence of statements,

$$\text{LHS} = a,\ a = b,\ b = c, \dots,\ z = \text{RHS}, \tag{2.9.1}$$

then we can deduce LHS = RHS, by repeated application of the *transitivity* property, and we set out the proof, in the following way:

$$\begin{aligned} \text{LHS} &= a \\ &= b \\ &= c \\ &\vdots \\ &= z \\ &= \text{RHS}. \end{aligned}$$

Moreover, such a proof is just as valid, by the *symmetry* property, if we instead start with RHS and finish with the LHS.

Definition 2.9.3. A **partial order** is a binary relation $\preceq$ on a set S that satisfies $\forall x, y, z \in S$:

PO1: $x \preceq x$, (**reflexivity**)

PO2: $x \preceq y$ and $y \preceq x \implies x = y$, (**antisymmetry**)

PO3: $x \preceq y$ and $y \preceq z \implies x \preceq z$. (**transitivity**)

Remark 2.9.4. A *partial order* is essentially something that behaves like "$\leqslant$". Other examples are $\geqslant$, $\subseteq$, $\supseteq$.

Definition 2.9.5. A **strict partial order** is a binary relation $\prec$ on a set S such that $\forall x, y, z \in S$:

SPO1: $x \not\prec x$, (**irreflexivity**)

SPO2: $x \prec y \implies y \not\prec x$, (**asymmetry**)

SPO3: $x \prec y$ and $y \prec z \implies x \prec z$. (**transitivity**)

Remark 2.9.6. A *strict partial order* is essentially something that behaves like "$<$". Other examples are $>, \subset, \supset$.

This is not the end of the story; $<$ and $>$ are also **total order** (also called **full order**) relations, where SPO2 can be replaced by:

FO2: $x \prec y$ or $y \prec x$ or $x = y$, (**trichotomy**)

The relations: $\subset, \supset$ don't satisfy this stronger axiom, since two sets can be *incomparable* (none of the three given possibilities).

The reason for mentioning all three of the relations: *equivalence relation*, *partial order* and *strict partial order* here, is that they all possess the property of *transitivity*, so that if the relations of some of the equations in (2.9.1) are replaced by "$\leqslant$" and "$<$" then we can deduce LHS $\sim$ RHS where $\sim$ is the strictest of "$=$", "$\leqslant$" and "$<$" that appears in the sequence (where "$\leqslant$" is *stricter* than "$=$", and "$<$" is *stricter* than "$\leqslant$"). Thus,for example, from

$$\begin{aligned} \text{LHS} &= a \\ &\leqslant b \\ &< c \\ &= z \\ &\leqslant \text{RHS}, \end{aligned}$$

we can deduce LHS $<$ RHS.

Similarly, if we have a sequence of such statements where the relations are "$=$", "$\geqslant$" and "$>$" (which are again in order of increasing *strictness*), then we can deduce LHS $\sim$ RHS where $\sim$ is the strictest of "$=$", "$\geqslant$" and "$>$" that appears. It's important that the relations that occur in such a sequence have the same *directionality*.

Formalising above, we say that $(=, \leqslant, <)$ is a **supertransitive** triple, meaning that if we have an alternating sequence of expressions a_i and relations rel_i (from the triple):

$$a_1 \ \text{rel}_1 \ a_2 \ \text{rel}_2 \ a_3 \ \text{rel}_3 \cdots \text{rel}_{n-1} \ a_n \ \text{rel}_n \ a_{n+1}$$

then the relationship between a_1 and a_{n+1} is the strictest of the relations $\text{rel}_1, \ldots, \text{rel}_n$.

Similarly, $(=, \geqslant, >)$, $(=, \subseteq, \subset)$ and $(=, \supseteq, \supset)$ are **supertransitive** triples.

2.10 Application of functions to inequalities

We discuss inequalities more generally in Chapter 11 and functions in Section 14.6. In particular, we define **domain** in Section 14.6. For now, when we mention the word *domain* we mean an interval of the real line for which the statement (an *inequality*) is *valid*, i.e. a *set* of values x for which the *inequality* holds.

Here we are interested in the answer to the following question:

When can one apply a function to both sides of an inequality?

The key idea is embedded in the following definitions:

Definition 2.10.1. A function f is **increasing** if, for x, y in the *domain* of f,

$$x < y \implies f(x) < f(y).$$

From this definition, we see *increasing functions* **preserve** the *directionality* of an inequality.

Definition 2.10.2. A function f is **decreasing** if, for x, y in the *domain* of f,

$$x < y \implies f(x) > f(y).$$

From this definition, we see that *decreasing functions* **reverse** the *directionality* of an inequality.

Thus the answer to the question is:

> The properties a function f must have, in order that it can be applied to both sides of an inequality (so that the statement remains true), are summed up as follows:
>
> - If a function f is *increasing* on the *domain of the inequality*, then its application to both sides of the inequality *preserves* the directionality of the inequality.
> - If a function f is *decreasing* on the *domain of the inequality*, then its application to both sides of the inequality *reverses* the directionality of the inequality.
> - Otherwise, application of the function will result in nonsense. Don't do it!

Since we have introduced above some ideas that can refine proofs, it makes sense to give some further examples that demonstrate their usage.

Exercise 2.10.3. Prove that if $a, b > 0$ such that $ab \geqslant a + b$ then $a + b \geqslant 4$.

RTP: $a, b > 0, ab \geqslant a + b \implies a + b \geqslant 4$

Proof. Assume $a, b > 0$ (1)

$ab \geqslant a + b$ (2)

$\implies a + b \geqslant 2\sqrt{ab}$, by Exercise 2.7.1

$\implies (a + b)^2 \geqslant 4ab$, since $u \mapsto u^2$ is increasing for $u \geqslant 0$

$\geqslant 4(a + b)$, by (2)

$\implies a + b \geqslant 4$, since $a, b > 0 \implies a + b > 0$ □

Finally, where symmetry exists and introducing an extra condition makes no essential difference to the proof, we can introduce that condition with the phase **without loss of generality** (abbreviated as: **w.l.o.g.**).

Exercise 2.10.4. Prove that if $0 < a, b \leqslant 1$ then $a/(b+1) + b/(a+1) \leqslant 1$.

RTP: $0 < a, b \leqslant 1 \implies \dfrac{a}{b+1} + \dfrac{b}{a+1} \leqslant 1.$

Proof. Assume $0 < a, b \leqslant 1$ and w.l.o.g. assume $a \geqslant b$. Then

$$\begin{aligned} \frac{a}{b+1} + \frac{b}{a+1} &\leqslant \frac{a}{b+1} + \frac{b}{b+1} \\ &\leqslant \frac{1}{b+1} + \frac{b}{b+1} \\ &= \frac{b+1}{b+1} \\ &= 1. \end{aligned}$$

□

Exercise Set 2.

1. Let n be a positive integer and d its smallest divisor greater than 1. Prove that d is prime.
2. Prove that if x, y are positive numbers then $x + y \geqslant 2\sqrt{xy}$.
3. A right-angled triangle has sides of length a, b, and c with c being the hypotenuse. If the triangle has area $c^2/4$, show that it is isosceles.
4. Prove that if p is a prime and q is a positive integer less than p, then p and q are relatively prime.
5. Prove that if a, b and c are real numbers such that $a^2 + b^2 + c^2 = 0$, then $a = b = c = 0$.
6. Prove that the numbers $n - 1$ and $n + 15$ are relatively prime for every even integer n.
7. Prove that the sum of two real numbers one of which is rational and the other irrational is an irrational number.
8. Prove that if m is an integer and $2^m - 1$ is a prime, then m is also a prime.
9. Prove that $\sqrt{2}$ is irrational, by the following approach.
   (i) Assume for a contradiction $\sqrt{2} \in \mathbb{Q}$.
   (ii) Deduce that there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $(a/b)^2 = 2$.
   (iii) Show that w.l.o.g. we may assume $a, b > 0$, and b as small as possible.
   (iv) Show that $\left(\dfrac{2b-a}{a-b}\right)^2 = 2$.
   (v) Show that $2b - a, a - b > 0$ with $a - b < b$, and thereby deduce a contradiction.