100% Mathematical Proof

Rowan Garnier

Richmond College, London

John Taylor

University of Brighton, Sussex

JOHN WILEY & SONS, LTD
Chichester • New York • Brisbane • Toronto • Singapore

Start of Citation[PU]John Wiley & Sons, Ltd. (UK)[/PU][DP]1996[/DP]End of Citation

Baffins Lane, Chichester,
West Sussex PO19 IUD, England

National (01243) 779777
International (+44) 1243 779777

Other Wiley Editorial Offices

John Wiley & Sons, Inc., 605 Third Avenue,
New York, NY 10158-0012, USA

Jacaranda Wiley Ltd, 33 Park Road, Milton,
Queensland 4064, Australia

John Wiley & Sons (Canada) Ltd, 22 Worcester Road,
Rexdale, Ontario M9W 1L1, Canada

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01,
Jin Xing Distripark, Singapore 0512

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0 471 96198 1; 0 471 96199 X (pbk)

Typeset in 11/13pt Palatino by Laser Words, Madras, India
Printed and bound in Great Britain by Bookcraft (Bath) Ltd.

This book is printed on acid-free paper responsibly manufactured from sustainable forestation, for which at least two trees are planted for each one used for paper production.

Start of Citation[PU]John Wiley & Sons, Ltd. (UK)[/PU][DP]1996[/DP]End of Citation

Contents

Start of Citation[PU]John Wiley & Sons, Ltd. (UK)[/PU][DP]1996[/DP]End of Citation

Start of Citation[PU]John Wiley & Sons, Ltd. (UK)[/PU][DP]1996[/DP]End of Citation

Preface

Although there have been suggestions that mathematics is becoming more 'experimental,' and the notion of proof less salient, this has provoked vigorous denials from the mathematical community which continues to maintain that proof is one of the key concepts which characterise the discipline. It is surprising therefore, that the fundamentals of mathematical proof have rarely been taught in a systematic way. Most students of mathematics are expected to develop their understanding of proof and the associated theorem-proving skills by a process of 'osmosis' through encounters with the various techniques and methods. The result is that students frequently have an inadequate appreciation of the underlying structure of proofs and a consequent inability to distinguish a correct proof from a flawed one. It is therefore no wonder that they have considerable difficulty in constructing their own proofs, often not knowing how to start a suitable line of reasoning.

Because it has not been the custom to teach the principles of mathematical proof systematically, there are few, if any, books on 'structured theorem proving'. As a consequence some authors of textbooks in abstract algebra and analysis, for example, have found it necessary to include appendices outlining some of the principal methods of proof. Naturally, such summaries tend to concentrate on describing proof techniques without looking too deeply at their underlying structure. On the other hand, the notion of 'formal proof' is covered well in many books on mathematical logic, but the proofs that mathematicians write are not formal proofs in this sense.

It is our intention in this book to explore the principles which underpin the various methods of mathematical proof and to describe how proofs may be discovered and communicated. We aim to examine the

structural features common to all mathematical proofs as well as those which are specific to particular techniques. We also consider some of the less tangible skills associated with the discovery and communication of proofs. These aspects are, of course, explored at greater depth in Polya's much admired book (Polya, 1957).

Whilst our primary aim has been to write a book for students of mathematics, we hope this text will also be useful to others interested in unravelling and understanding the nature of mathematical proof—for instance, teachers of mathematics or students of philosophy. The mathematical background we assume is little more than would be provided by a GCSE course in the UK or a high-school algebra course in the USA, although some degree of mathematical sophistication beyond this is necessary. We have included, in examples and exercises, some proofs drawn from more advanced mathematics but these can be omitted without jeopardising the comprehensibility of the text.

University mathematics departments are becoming increasingly concerned about their students' inability to understand and write mathematical proofs so that a number of institutions are introducing courses in which proof is taught systematically. We hope that this text will prove useful to those designing, teaching and studying such courses. Of course, not everyone will agree with our approach to proof and how (indeed, whether) it should be taught. However, we do believe there is a need to address the question of 'proof education' more directly than has hitherto been the case and we hope this book will make some contribution.

Our sincere thanks are due to those colleagues who commented on various parts of the manuscript, to Clifford Mould and Elizabeth Taylor for their continued support, to Alice Tomič for her hospitality following many 'authors' meetings' and to Pam Taylor for, once again, providing excellent cartoons on a less than promising subject at short notice.

RG and **JT**
Περα Ορεινης
August 1995

1 Proofs, Mathematical and Non-mathematical

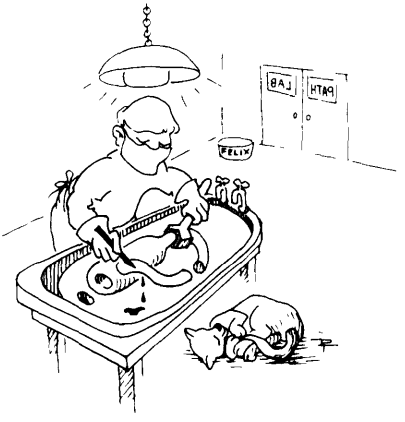
1.1 Introduction

This book is unusual so far as mathematics textbooks are concerned in that its primary purpose is not to teach any specific body of mathematics. Instead, the text considers mathematics itself in an attempt to understand its *modus operandi*. In particular, we shall explore the notion of rigorous proof which is unique to mathematics and logic. (It could be argued that rigorous proofs are also employed in software engineering where so-called 'safety critical' programs need to be proved correct. For the purposes of this book, these aspects of software engineering are regarded as being part of mathematics itself.)

The mathematician's concept of proof is rather different from, say, the lawyer's. In criminal law, the prosecution seeks to prove 'beyond reasonable doubt' that the accused is guilty of the alleged offence. Since the courts deal with people and events in the real world, the criterion of 'proof beyond reasonable doubt' is the most rigorous practical requirement. Rarely, if ever, can guilt be established beyond *all* doubt. By contrast, the mathematical notion of proof is (in principle) far more rigorous. We do not speak, for example, of Pythagoras' theorem being true 'beyond reasonable doubt.' This is not to say that mathematical proofs are completely reliable; they are not. In practice, proofs do not always conform to the ideal standard because they are constructed by fallible human beings. However, *in principle*, there can be no room for doubt in a formal mathematical proof.

Our purpose in this book is two-fold. One aim is to explain what mathematical proofs are so that they may be better understood. Since proofs are written by human beings (or in a very few limited situations by

computer programs which are themselves written by human beings) there are many different styles and approaches adopted. Proofs are written for a variety of different audiences in various cultures and in many languages. We shall attempt to delve beneath surface features such as style and language to examine the underlying logical structures of proofs. This aspect of the book could be summarised as 'proofs dissected, examined and their structure revealed'.



Proofs dissected, examined and their structure revealed

Our second goal is more difficult to achieve. Put simply, it is to show how to construct proofs. On one level, such a goal is unattainable. There is no magic formula which, if learned, will enable us to construct a proof of any result we care to choose. However, we can provide hints and guidance which we hope will be useful. Traditionally, there has been little systematic attempt to teach 'theorem-proving'. Instead, it is expected that proof techniques will be absorbed simply through repeated exposure to examples of proofs. We hope this text will go some way to redressing the balance.

1.2 Inductive and Deductive Reasoning

Most readers would, no doubt, be able to give an informal and reasonably accurate description of what is, say, physics or psychology, astronomy or anthropology. The educated person's definition of any of these disciplines is likely to be fairly close to the accepted definition of the experts in the field. But, what of mathematics? What *is* mathematics? And what is it that professional mathematicians do when

they are engaged in their discipline? Perhaps a reasonable brief job description of the (pure) mathematician is someone who proves things about abstract objects such as numbers or geometrical configurations, their interrelations and their generalisations.

We can safely assume that our readers will know that in mathematics we prove things. It is really the notion of rigorous proof which distinguishes mathematics from other fields of study. In most academic disciplines, theories are proposed and explored, evidence for and against is accumulated, differing opinions are expressed and so on. It is true that certain facts are established: Christopher Columbus discovered the New World in 1492, the metal copper will conduct an electric current, the majority of the Earth's surface is covered in water, etc. But such facts are discovered by observation and collation of data and not because they have been proved in the sense that mathematicians use the word.

In science, theories are judged on the basis of how well they explain and predict observable phenomena; in other words, by how well they 'fit' experimental data. The scientist draws on a mass of observations to make inferences which become the building blocks for new theories which are tested and then modified in the light of further experimental data. The method of reasoning which makes inferences and draws conclusions from observations is known as **inductive reasoning**.

There are limits to the power of inductive reasoning, however. It is sometimes said that scientific theories are not provable, they are only falsifiable. At best, experimental observations can be consistent with a particular theory and give the scientist greater confidence in it. However, no amount of experimental data can prove that a theory is correct, because there is always the possibility that another experiment will turn out to be inconsistent with the theory and hence show it to be false. (We are assuming here that experiments accord with the rigorous standards of scientific practice. One important criterion, for example, is that experimental results should be essentially repeatable. A single experiment could produce freak results and a successful theory would not be modified on the basis of a single unrepeatable experiment.) In short, data which agree with theoretical predictions increase confidence in the theory whereas data which disagree with theoretical predictions destroy the theory.

It is not only scientists who employ inductive reasoning—it is probably the basis of most human belief and knowledge. To illustrate the

point, we would all presumably accept as a fact that the Sun will rise tomorrow morning. (We ignore the problem that we may not be able to *see* the Sun rise due to climatic conditions. Equally we ignore possibilities such as being situated north of the arctic circle in mid-winter.) Our belief in this 'fact' is based on inductive reasoning: we and our forebears have observed the Sun to rise on many thousands of mornings. Indeed, we have never known the Sun not to rise! In this way, we have established 'beyond all reasonable doubt' that the Sun will rise tomorrow morning.

In mathematics, on the other hand, conclusions based solely on observation are not sanctioned. Thus inductive reasoning is not acceptable in a mathematical proof. For instance, we may observe that whenever we square an odd positive integer (whole number) the result is always another odd positive integer. (For example, $3^2 = 9$, $19^2 = 361$, $321^2 = 103041$, etc.) But, no matter how many times we perform the 'experiment' and obtain the expected outcome, this will not constitute a mathematical proof that the square of an odd positive integer is also an odd positive integer. The reasoning acceptable in a mathematical proof is of a different kind altogether. It is **deductive reasoning**, whereby a conclusion is reached by logical inference from a collection of assumptions.

Using correct deductive reasoning, we can be confident that a conclusion does indeed follow from the assumptions in force at the time. One can immediately appreciate the appeal of deductive reasoning when compared to inductive reasoning. It appears to offer us certainty. However, two words of caution are in order. The first is that any conclusion obtained deductively can only be as 'sound' as the premises on which it is based. Deductive reasoning allows us to pass with confidence from assumptions to conclusions but any such conclusion will be useless if it is based on incorrect assumptions. If the assumptions are false then we cannot guarantee the truth of any conclusion deduced from them. It is said that a chain is only as strong as its weakest link. Similarly, a conclusion obtained by deduction is only as 'strong' as the assumptions upon which it is based.

There is a more theoretical reason why we must temper any enthusiasm for deductive arguments, though. In the 1930s, the Austrian logician Kurt Gödel showed that there are certain limitations to the power and scope of deductive reasoning. Gödel's results, known as his incompleteness theorems, are amongst the most profound of the twentieth

century. In one of the theorems, Gödel showed that there must always be true results about the arithmetic of the positive integers which we will never be able to prove using strict deductive reasoning. In other words, even if deductive arguments offer some form of certainty, that certainty can never extend to include all true facts about a system as familiar to us as the positive integers.

Despite these limitations to the power of deduction, it is the basis of the vast, powerful and applicable body of human knowledge known as mathematics. It is our purpose in this book to explore the inner workings of this discipline which is, regrettably, poorly understood by that mythical being, the person in the street.

1.3 A Proof or Not a Proof?

In much of the remainder of the book we shall be illustrating various techniques of proof using fairly short, elementary proofs. Naturally, in 'real' mathematics, not all proofs are like this. In this section, we shall examine briefly three well-known theorems whose proofs are neither short nor elementary. Each of the theorems, or more accurately their proofs, will tell us something about the nature of mathematical proof. In many areas of human endeavour, actual practice does not always conform to some theoretical ideal. So, too, it is in mathematics. Although none of our three examples could be regarded as a typical mathematical proof, the lessons we can learn from them are relevant. They serve to keep in perspective the main thrust of this book which is to explore the theoretical framework of proof. The choice of the three theorems to consider is a personal one—there are many we could have examined. Each theorem is either well-known, has an interesting history or is remarkable in its own right. Each proof is particularly demanding in some aspect; each is a remarkable achievement worthy of examination.

Fermat's last theorem

Pierre de Fermat (1601–1665) was a French jurist and amateur mathematician who made many significant contributions to number theory. The statement which was to become known as 'Fermat's last theorem' originates from a note Fermat made in the margin of his copy of the works of the ancient Greek mathematician Diophantus. Having stated

the 'theorem' Fermat wrote, 'I have discovered a truly remarkable proof which this margin is too small to contain'. It would appear that Fermat did not write down his 'remarkable proof' elsewhere either, as he never communicated a proof to anyone, nor was a proof found amongst his papers. In fact, Fermat rarely wrote down proofs of his discoveries although virtually every one has subsequently been proved by others.

Fermat's last theorem can be understood by anyone who has studied a little elementary algebra. We all know Pythagoras' theorem. Symbolically, it states that the sides x, y and hypotenuse z of a right-angled triangle satisfy the equation $x^2 + y^2 = z^2$. Furthermore, there are known to be many solutions (infinitely many, in fact) of this equation where x, y and z are integers. (Examples of solutions include $(x, y, z) = (3, 4, 5)$, $(5, 12, 13)$, $(517, 1044, 1165)$.) Fermat's last theorem states that, for $n > 2$, the corresponding equation $x^n + y^n = z^n$ has no solutions where x, y and z are integers.

It is not surprising that such an easy-to-state theorem about familiar objects, the integers, has attracted the attention of many mathematicians, both professional and amateur. And yet, for some 350 years the theorem defied all attempts at a proof (and all attempts at a disproof, too). It earned the status of the most famous unsolved problem in mathematics. Lack of success in finding a proof or disproof was not for the want of trying, though. Many thousands of person-hours have been devoted to the problem since Fermat's original marginal note.

In the nineteenth century, the Académie de Sciences de Paris twice offered a prize for a solution to the problem. Later, in 1908, under the terms of the will of Dr. Paul Wolfskehl, a prize of 100 000 Marks was offered for a proof of the theorem. The prize was to be conferred by the Königliche Gellschaft der Wissenschaften in Göttingen on or before September 13, 2007. In the early years of the Wolfskehl Prize several hundred attempts were received each year. In recent years, this has dwindled to a few dozen. Over the years inflation and financial charges have taken their toll on the value of the prize too; it is now worth a little over DM 10 000, a fraction of its original value. Of course, the importance of Fermat's last theorem is not to be measured in monetary terms.

In purely mathematical terms, too, the theorem *itself* is not of great importance, although a great deal of significant mathematics has been developed in the search for a proof. The importance of the theorem

lies in its fame, the fact that it turned out to be inordinately difficult to prove and, most importantly, in the mathematical spin-offs resulting from attempts to prove the theorem.

By the 1980s much had been achieved, although a proof was still not in sight. For example, it was known that the theorem was true for all values of the index n less than 125 000. Furthermore, if the equation $x^n + y^n = z^n$ did have a solution (x, y, z) for some value of n, then the number x would have to be at least $10^{1800\,000}$, a truly unimaginably huge number which would take several hundred pages just to write down in the usual decimal notation. In 1983 a German mathematician Gerd Faltings proved that the equation had at most a finite number of solutions where x, y and z have no common factors[1]. Faltings' theorem was the first major step towards a proof for several decades although it was still far from a proof—proving that there are only a finite number of solutions is a long way from showing that there are none.

Given the long history of unsuccessful attempts it was with much delight and surprise (and not a little scepticism) that the mathematical community received the news in June 1993 that a British mathematician, Andrew Wiles, had finally succeeded in proving Fermat's theorem. (Actually, Wiles had proved a highly technical theorem, known as the Shimura-Taniyama-Weil conjecture; however Fermat's last theorem had previously been shown to follow from this result.) The ideas used in the proof are very deep and complicated—a far cry, indeed, from the simplicity of the last theorem itself. Until Wiles' arguments have been thoroughly examined and understood, there remains the possibility that there is a flaw somewhere in his reasoning. However, the experts agree that any flaw is likely to be minor and relatively easily corrected. It appears, then, that mathematics' most famous unsolved problem has become one of its most celebrated solved problems. (In fact, a few months after announcement of the proof a flaw *was* discovered. However, in October 1994, Wiles and a colleague, Richard Taylor, issued a manuscript which appears to have repaired the gap in the original proof. At the time of writing—summer 1995—it is believed that the proof is now complete.)

What are the major lessons we can learn from the history of Fermat's last theorem? An obvious lesson is that theorems which are simple to

[1] Faltings actually proved a result known as the Mordell conjecture, which implies the stated result. For his work in this area, Faltings was awarded the Fields Medal in 1986. The Fields Medal is mathematics' highest prize, equivalent in status to, if not so well known as, the Nobel prizes.

state may not be simple to prove. Fermat's last theorem is probably the supreme example—a little algebra is all that is needed to understand the statement of the theorem, but it defeated mathematicians for three and a half centuries. Another important 'moral' is that failure to produce a proof does not necessarily mean outright failure. It is undoubtedly the case that the cause of number theory has been very well-served by Fermat's last theorem. Much interesting and useful mathematics has resulted from some of the unsuccessful attempts to prove the theorem.

In less mathematical terms, it is clear that the fame of a theorem is not related to its importance. Naturally, it is difficult to define precisely what makes a particular theorem important. Among the criteria are its applicability within and outside mathematics, whether it provides new insights, to what extent it paves the way for further work, and so on. Most mathematicians would agree that there are more important unsolved problems (the Riemann hypothesis, for instance) which are completely unknown outside the mathematical community. Fermat's last theorem captured the imagination of generations primarily for non-mathematical, even romantic, reasons. Important among these was, of course, the possibility that an amateur mathematician would beat the experts in the race to discover a proof.

The four-colour theorem

Like Fermat's last theorem, the four-colour theorem is simple to state and, as it transpired, extraordinarily difficult to prove. Also like Fermat's theorem (or will it now be the Fermat-Wiles theorem?), it became very well-known and defied proof for a considerable period of time. In contrast to Fermat's last theorem, the proof, when it eventually appeared in 1976, was not greeted with universal acclaim and delight in the mathematical community. Indeed, the proof sparked a vigorous debate amongst mathematicians about the very nature of proof itself.

Consider a map of countries drawn on the plane or the surface of a sphere. Is it always possible to colour the map in such a way that two countries which share a common border are coloured differently and to do so using only four colours? The four-colour theorem says that it is always possible.

The question of whether four colours are always sufficient to colour a map in this way originated with a young mathematician, Francis

Guthrie, in 1852. Via Guthrie's brother, the problem was drawn to the attention of Augustus De Morgan, then Professor of Mathematics at the University of London. Unable to prove the theorem, De Morgan passed the problem on to fellow mathematicians, but it did not gain widespread attention until 1878 when Arthur Cayley asked for a proof at a meeting of the London Mathematical Society. Within a year, a barrister called Alfred Kempe had published a 'proof' which was to be accepted for eleven years. In 1890, Percy Heawood pointed out a fatal flaw in Kempe's 'proof'. Heawood was able to salvage enough of Kempe's argument to prove that five colours would always be enough to colour a map in the appropriate manner. Indeed, Heawood generalised the problem and considered maps drawn on other surfaces with 'handles' and 'twists'—see Figure 1.1. Heawood conjectured a formula for the number of colours which are sufficient to colour a map on any such surface (excluding the sphere and plane). Subsequently it was shown that Heawood's formula does indeed give the minimum number of colours required for all these more complicated surfaces except one, the so-called Klein bottle.

Although Kempe's argument turned out to be flawed, the ideas contained in his unsuccessful attempt were to be the basis of the subsequent work on the problem, including the final proof itself. Despite much work on the problem in the first half of the twentieth century, there was little real progress; until 1976 that is, when Kenneth Appel and Wolfgang Haken, working at the University of Illinois, announced that they had proved the theorem.

Appel and Haken's proof, though, is very unusual in that it used some 1200 hours of computer time to examine thousands of possible configurations of countries. It must be emphasised that they were not using inductive reasoning. Their argument was definitely not along

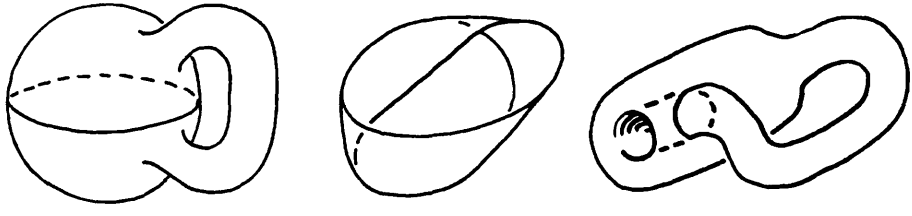


Figure 1.1

the following lines: *we have examined thousands of possible maps and have found that all are four-colourable, therefore four colours must surely always be sufficient.* As we have mentioned, such reasoning is not acceptable in a mathematical proof. (Their proof was deductive, but based on a method confusingly called 'proof by mathematical induction'—see Chapter 9.) Nevertheless, the quantity of direct computation required by their method was such that the use of a large amount of computer time was essential. Thus the correctness of their proof could not be checked by 'hand calculation' alone.

This was the first example of a proof which used the computer in an *essential* way and it generated considerable debate amongst mathematicians about its acceptability. The mathematical community had been used to proofs which could be verified by direct examination of the arguments. Some simply refused to accept that Appel and Haken's work did amount to a proof of the four-colour theorem. It is true that software used in the proof, though complicated, could be checked by others—but what of the occasional hardware errors to which every machine is prone? Could not one such error render the proof useless? In defence of the proof, it was argued that the possibility of error exists in any long and complicated proof and that the likelihood of computer error was considerably less than that of human error. Since its first appearance, Appel and Haken's proof has come under considerable scrutiny and as a result it is now generally accepted.

There are a number of lessons to be learnt from the history and eventual proof of the four-colour theorem. Again we see a situation where an incorrect 'proof' was not worthless. Although Kempe's attempt was unsuccessful, the underlying ideas were useful. They were the starting point for much subsequent work as they were extensively modified and extended over the years. Some of the important strands of the final proof can trace their ancestors back to Kempe's original incorrect 'proof'. Of course, Kempe's attempt was widely accepted for a number of years. Such a situation is not uncommon—the level of complexity of many proofs is such that errors may lie undetected for a considerable time.

It may be that the four-colour theorem is the first of many examples of theorems whose proof will involve computers in an essential way. Certainly Appel and Haken believed this to be the case although to date there have been no further examples of major theorems of this type. However, as hardware becomes increasingly powerful and software

increasingly sophisticated, few would say with confidence that the four-colour theorem is a unique example of this kind of theorem.

The classification of finite simple groups

Classification theorems must rank amongst the most satisfying of all mathematical theorems. Given any class of mathematical objects, an obvious question is: *what examples are there*? A classification theorem answers this question in the most complete possible way. It provides a list (often infinite) of all the examples of the particular mathematical object. In a sense, a classification theorem says two things—these (the objects in the list) are all examples of the particular class of object *and there are no others*. It is not only in mathematics where classification 'theorems' are important. For instance, when physicists discover that matter is composed of fundamental particles, they want to know precisely what such particles there are. Exactly which particles are regarded as fundamental has changed over time—in the early part of this century, atoms were regarded a fundamental whereas now quarks and leptons are given this status.

Unfortunately, in mathematics classification theorems are all too rare. Our aim now is to consider some features of a particularly remarkable classification theorem, that for the class of objects called finite simple groups.

Unlike the two previous theorems, we cannot give a precise statement of the classification theorem of finite simple groups. However, we can give an idea of what the theorem is saying. A 'group' is a particular kind of algebraic structure—it comprises a set with a binary operation (like addition, multiplication or composition of functions) satisfying three or four simple properties. (A definition is given in the appendix.) It turns out that some groups can be 'broken down' or 'factored' into simpler pieces; on the other hand, there are various ways of combining two or more groups to form new groups. A loose analogy is often used here: some integers (greater than 1) can be factored into the product of smaller ones; similarly, multiplying two or more such integers together produces a larger integer. Molecular physics provides a non-mathematical analogy. Molecules can be split into atoms of various kinds and atoms can combine together to form complex molecules.

In the number theory analogy, those numbers which cannot be factored are, of course, the prime numbers. Similarly, in molecular physics it is

the atoms which cannot be split into smaller entities *of a similar nature.* There is an analogous concept in group theory. A **simple** group is one which cannot be 'factored' into the 'product' of two groups. Note that the word 'simple' here has a technical meaning. It most definitely does not mean that such groups have a simple structure, as we shall see. The finite simple groups are the basic building blocks for all finite groups in the same way that prime numbers are the building blocks for all positive integers and atoms are the basic building blocks for molecules.

To classify finite simple groups, we need to know exactly what examples there are. What, then, is the complete list of finite simple groups? Firstly, we can identify various 'families' of simple groups, each family containing groups of the same kind but with different numbers of elements. In fact there are 18 such families, each containing an infinite number of different groups. Then, curiously, there are 26 finite simple groups which do not fit into any of the families. These 'outsiders' are called the **sporadic groups**. They range considerably in size from the smallest which has 7290 elements to the largest which has about 8×10^{53} elements, more elements than there are atoms in the Earth! (This latter group, which is known to group theorists as 'the monster' or 'the friendly giant' can be represented as a certain group of matrices of dimension $196\,883 \times 196\,883$!) That is the complete list: 18 infinite families and 26 sporadic groups.

Already, we can appreciate something of the scale of the theorem, but the proof is even more remarkable. When the proof was finally completed in 1981, it was estimated to run to between 10 000 and 15 000 pages spread over many articles published in mathematical journals during the previous four decades or so. Many mathematicians had contributed to the proof and (we need hardly add) no one person had read the whole proof. In contrast to the four-colour theorem, though, computers were used very little in the overall proof.

What does the existence of such a monumental proof tell us about the nature of proof itself? The most startling point to realise is that when the proof was finally completed, it was almost certainly wrong! With such a large and complicated proof, the chance that it was error-free was very small indeed. To quote Michael Aschbacher (1981), one of the major contributors to the proof, writing at the time:

> The probability of an error in the Classification Theorem is virtually 1. On the other hand the probability that any single error cannot

> easily be corrected is virtually zero, and as the proof is finite, the probability that the theorem is incorrect is close to zero. As time passes and we have an opportunity to assimilate the proof, that confidence level can only increase.

Aschbacher's comments seem to run counter to the view of mathematics as a precise, deductive science. It appears odd, to say the least, for a highly regarded professional mathematician to be writing about the *probability* that a theorem is correct and our *confidence level* in its correctness. Where is the certainty of deductive reasoning? In reality, Aschbacher is only stating the obvious. Mathematics is a human endeavour and human beings make mistakes; therefore a very large mathematical enterprise is almost certain to contain errors. In other words, real mathematics like the classification theorem for finite simple groups, remarkable though it certainly is, does not always live up to the austere standards of the ideal.

Human beings make mistakes

The monumental nature of the proof is also testimony to the perseverance, dedication and collaborative spirit of those involved. Without the collaboration of many mathematicians in several countries the venture would not yet have been brought to a successful conclusion. There are no immediate applications of the theorem which will benefit mankind—this was a search for knowledge for its own sake. Whether or not one regards that as a noble aspiration, it is impossible not to admire the achievement itself.

There is one further lesson we can learn from our discussion of these three famous theorems. In practice mathematical proofs do not always conform to the ideal of a completely rigorous, logical argument. Perhaps

a better description of most mathematical proofs is that of a plausible argument sufficient to convince the mathematical community of the truth of the particular theorem. Whether we regard a mathematical proof as completely rigorous or 'merely' an argument of sufficient power and persuasiveness to convince the experts, there are standard techniques and methods which are employed. It is the purpose of the remaining chapters to explore and understand these methods.

2 Propositional Logic

2.1 Propositions and Truth Values

We shall consider the detailed structure of a mathematical proof later but, very broadly speaking, constructing a proof consists of showing that, given the truth of certain statements, the truth of the theorem to be proved inevitably follows. Normally such a proof takes the form of a sequence of statements whose truth is guaranteed either by the truth of earlier statements in the sequence or because they follow from other statements whose truth is assumed. For example, if we accept that 'Today is Tuesday and it is raining' is a true statement then we could not dispute the truth of the statement 'It is raining'. 'It is raining' follows from (or is implied by) 'Today is Tuesday and it is raining'.

In claiming that the truth of one statement is guaranteed by the truth of others we shall need to supply some justification. The only justification which is acceptable in a mathematical proof is one which is sanctioned by the laws of logic. It is these laws which govern what can be deduced from what and as such they provide us with a means of distinguishing a proof which is valid from one which has some fault in the sequence of steps which purports to establish the inevitable truth of the 'theorem'.

The statements which appear in a mathematical proof are ones which can (under appropriate circumstances) be declared true or false. We refer to such statements as **propositions** and we denote particular propositions using upper case letters, e.g. $P, Q, R, \ldots$. We use lower case letters (e.g. $p, q, r, \ldots$) to denote **propositional variables**, i.e. variables for which any proposition may be substituted. The following are examples of propositions:

(a) P: Two is an even number.
(b) Q: I have three brothers.

(c) R: $4 \geq 7$
(d) S: $\sqrt{-1}$ does not exist.

The truth (T) or falsity (F) of a proposition is termed its **truth value**. For our purposes a proposition which is not true will be regarded as false and one which is not false will be viewed as true. It is important to note that the truth value of a proposition may depend on the context in which it is stated. Of the propositions listed above P is true and R is false. However, Q is true only if uttered by someone who has three brothers and is false otherwise. Proposition S is true if we have agreed to restrict our discussion to the real numbers. However, if we make the statement within the context of the complex numbers, then it is a false proposition.

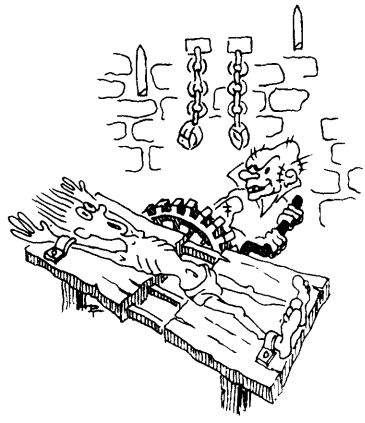
Sentences which cannot be viewed as true or false are not propositions. These include questions, demands, exhortations and exclamations. Hence the following are not propositions.

(e) Show your working clearly.
(f) Has a trapezium got four sides?
(g) Vote for Mickey Mouse!

It is clear that, for any proposition, adding the prefix 'It is not the case that ...' or inserting 'not' appropriately results in another proposition with the reverse truth value. For example, if the proposition 'I have three brothers' is true then the proposition 'It is not the case that I have three brothers' or 'I do not have three brothers' is false and vice versa. If we reverse the truth value of any proposition P in this way, the resulting proposition, denoted by $\overline{P}$ (or $\sim P$ or $\neg P$) is called the **negation** of P. There are a variety of different ways of stating the negation of a proposition but what is important about $\overline{P}$ is that it is true in all circumstances that P is false and false whenever P is true. We can summarise this in a table where we show, for each of the possible truth values of the propositional variable p, the corresponding truth value of $\overline{p}$, the negation of p.

p	$\overline{p}$
T	F
F	T

A table which summarises truth values in this way is called a **truth table**.



Truth table

2.2 Logical Connectives

Each of the propositions P, Q, R and S defined above makes a single statement about an object or individual. Such propositions are called **simple propositions**. The proposition 'Today is Tuesday and it is raining' is not a simple proposition since it makes two statements, one concerning the day of the week and the other about the state of the weather. However, it can be viewed as being composed of the two simple propositions 'Today is Tuesday' and 'It is raining' conjoined using the word 'and'. The truth value of 'Today is Tuesday and it is raining' is dependent upon the truth values of these two component simple propositions. It is true if both components are true and false otherwise. We summarise this in the table below where we now use Q and R denote 'Today is Tuesday' and 'It is raining' respectively.

Q	R	Q and R
T	T	T
T	F	F
F	T	F
F	F	F

The right hand column of the table gives the truth value of the proposition 'Q and R' for each possible pair of truth values of the individual propositions Q and R. For instance, the last line indicates that, if Q and R are both false, then the proposition 'Q and R' is also false.

Propositions which are formed by joining two or more simple propositions are called **compound propositions**. The items which are used to join the simple components are called **logical connectives**. The truth value of a compound proposition is determined by two factors: the truth value of each of its component simple propositions and how particular logical connectives are used to link them. There are five connectives which are important: conjunction, inclusive disjunction, exclusive disjunction, conditional and biconditional. We now look at the properties of each of these.

Conjunction

The truth table for the conjunction of any two propositional variables p and q, denoted by $p \wedge q$ (or by $p.q$), is given below.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

The table shows that the conjunction $p \wedge q$ is true only when true propositions are substituted for each of p and q. Otherwise the conjunction is false. As we have already seen, this sense is conveyed using the word 'and' between the two component propositions (often termed the **conjuncts**). For example, if B denotes the proposition 'Bob is a footballer' and S denotes 'Sue is a student' then the conjunction of B and S is expressed by 'Bob is a footballer and Sue is a student' and is denoted by $B \wedge S$. Although 'and' is the most common linguistic expression for logical conjunction, there are alternatives. The following would also be denoted by $B \wedge S$ although they do have nuances which are slightly different from when the two components are joined using 'and':

Bob is a footballer although Sue is a student;
Bob is a footballer whereas Sue is a student;
Bob is a footballer but Sue is a student.

These are conjunctions because, in each case, we would view the compound proposition as true only when both of its two components are true.

Note that the conjunction $p \wedge q$ (read as 'p and q') is symmetric in the sense that it has exactly the same set of truth values as $q \wedge p$. Both are true only when each of the components p and q are true. Hence, from the point of view of logic, 'Bob is a footballer and Sue is a student' and 'Sue is a student and Bob is a footballer' are equivalent propositions. (We shall give a more precise definition of 'equivalent propositions' later.)

Disjunction

There are two forms of logical disjunction—the inclusive and exclusive forms. The inclusive disjunction of two propositional variables p and q is denoted by $p \vee q$ and the exclusive disjunction of the two components by $p \veebar q$. The truth table for each of these is given below.

p	q	$p \vee q$	$p \veebar q$
T	T	T	F
T	F	T	T
F	T	T	T
F	F	F	F

The only difference between the truth values of $p \vee q$ and $p \veebar q$ is when p and q (often termed the **disjuncts**) are both true propositions. In this case the inclusive disjunction $p \vee q$ is true but the exclusive disjunction $p \veebar q$ is false. An inclusive disjunction is true only when either or both of its disjuncts are true whereas an exclusive disjunction is true only when one disjunct is true and the other is false.

Unfortunately, in English the word 'or' is used between disjuncts (sometimes with the first disjunct preceded by 'either') as the linguistic expression for both inclusive and exclusive disjunction. Therefore a proposition containing 'or' is often ambiguous as to whether the inclusive or exclusive sense is intended. Sometimes the context suggests which form of disjunction is appropriate. For instance, 'On Monday I shall stay in London or visit a friend in Paris' has components which seem to be mutually exclusive and so we would interpret the proposition as true only when just one of the disjuncts is true. Exclusive disjunction therefore seems to be the intended interpretation of 'or'. On the other hand, 'Applicants for the job must have a degree or three years relevant experience' does not seem to preclude applicants who

satisfy both criteria and therefore suggests that the underlying logical connective is inclusive disjunction.

The ambiguity surrounding the word 'or' can be resolved by adding 'or both' to the proposition to indicate that the disjunction is inclusive or by adding 'but not both' to make clear the exclusive sense. For instance, 'Tom has a brother or a sister, but not both' is clearly to be read as the exclusive disjunction of its two components whereas 'Tom has a brother or a sister, or both' indicates inclusive disjunction. Sometimes 'and/or' is used between disjuncts to indicate inclusive disjunction. However, where only the word 'or' is used and the disjunctive proposition is ambiguous as to which form is intended, the convention in logic is to interpret the connective as inclusive disjunction.

As with conjunction, both forms of disjunction are symmetric. The forms $p \vee q$ (usually read as 'p or q') and $q \vee p$ have exactly the same set of truth values; they are false only when both p and q are false. The forms $p \veebar q$ (often read as 'p exclusive or q' or 'p x-or q') and $q \veebar p$ also have identical truth tables. Each is false only when propositions with the same truth value are substituted for p and q.

Conditional

A conditional proposition is denoted by $P \rightarrow Q$ (or by $P \supset Q$). The truth table for this propositional form is given below.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

The component p of the conditional expression $p \rightarrow q$ is called the **antecedent** and the component q is called the **consequent**. A conditional proposition is true unless its antecedent is true and its consequent is false. This sense is conveyed linguistically by preceding the antecedent with 'if' and inserting 'then' between antecedent and consequent (although 'then' can be omitted). For example, consider the proposition 'If you clean the car then I'll give you £10'. Here the antecedent is C: 'You clean the car' and the consequent is G: 'I'll give

you £10'. If you cleaned the car and didn't get £10 (the case where the antecedent is true and the consequent is false), then you could justifiably claim that you had been told a falsehood. However the proposition makes no claims about what will happen if you don't clean the car. I may give you £10 (if you mow the lawn instead, for instance) or I may not.

As with the other connectives, there are alternative ways of stating a conditional proposition. With C and G defined as above, the following would also be symbolised by $C \rightarrow G$:

I'll give you £10 if you clean the car.
When (or whenever) you clean the car, I'll give you £10.
You will clean the car only if I give you £10.
That you clean the car implies that I'll give you £10.

Note that, when 'only if' is used to convey the conditional $P \rightarrow Q$, it precedes the consequent so that the proposition is expressed as 'P only if Q'. However, when the same proposition is expressed using 'if', this precedes the antecedent as in 'if P then Q' or 'Q if P'.

The conditional connective is also referred to as **implication** and $P \rightarrow Q$ is often read as 'P implies Q'. For any conditional proposition of the form $P \rightarrow Q$, P (the antecedent) is said to be a **sufficient condition** for Q (the consequent) and Q is said to be a **necessary condition** for P.

As we can see from the truth table for the two forms given below, the conditional $p \rightarrow q$ is not equivalent to $q \rightarrow p$ logically.

p	q	$p \rightarrow q$	$q \rightarrow p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

The propositional form $p \rightarrow q$ is false if p is true and q is false. However, for these truth values of p and q, $q \rightarrow p$ has a false antecedent and a true consequent and is therefore true. Hence a conditional proposition is not symmetric and the two propositions 'If you clean the car then I'll give you £10' and 'If I give you £10 then you clean the car' do not mean the same.

Biconditional

The truth table for a biconditional propositional form, symbolised by $p \leftrightarrow q$, is shown below. Note that a biconditional proposition is true only when both its components have the same truth value. The form $p \leftrightarrow q$ is false when p and q have different truth values.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

A biconditional proposition is expressed linguistically by preceding either component by 'if and only if'. If this phrase is used before the first component, then the second component may be preceded by 'then'. Hence, if C and G are defined as above, each of the following would be symbolised by $C \leftrightarrow G$.

If and only if you clean the car then I'll give you £10.
You'll clean the car if and only if I give you £10.

The biconditional is also symmetric and $p \leftrightarrow q$ (usually read as 'p if and only if q') and $q \leftrightarrow p$ are equivalent logically. Hence the propositions above could also be stated as follows.

If and only if I give you £10 then you'll clean the car.
I'll give you £10 if and only if you clean the car.

Examples 2.1

1. Symbolise the following propositions.

(i) Jane is at work or she is playing tennis.
(ii) If I win the lottery then I'll buy a racehorse.
(iii) Rain falls if and only if there is a northerly wind.
(iv) Today is Friday and I won't go to college.
(v) If I don't work hard then I won't pass my exams.

Solution

(i) Define the following simple propositions:

W: Jane is at work.
T: Jane is playing tennis.

Assuming that Jane's work does not involve her in playing tennis, we would interpret 'or' in its exclusive sense and symbolise this proposition as $W \veebar T$.

(ii) We symbolise the two component simple propositions as follows:

L: I win the lottery.
R: I'll buy a racehorse.

The compound proposition given is then symbolised by the conditional $L \rightarrow R$.

(iii) We define:

R: Rain falls.
N: There is a northerly wind.

The proposition given is symbolised $R \leftrightarrow N$.

(iv) We define:

F: Today is Friday.
C: I go to college.

The proposition given is the conjunction of F and the negation of C, denoted by $\overline{C}$. It is therefore symbolised as $F \wedge \overline{C}$. (Note that we may have chosen instead to define C as 'I won't go to college' and to symbolise the proposition by $F \wedge C$.)

(v) We define:

W: I work hard.
P: I'll pass my exams.

We are given a conditional proposition in which the antecedent and consequent are the negations of W and of P respectively. This is symbolised by $\overline{W} \rightarrow \overline{P}$. (Again, we could have defined W: I don't work hard and P: I won't pass my exams and symbolised the proposition by $W \rightarrow P$.)

2. Let the propositions J and M be defined as follows:

J: Jo spent September in New York.
M: Mary had a little lamb.

Translate the following symbolised propositions into reasonable English sentences:

(i) $J \wedge \overline{M}$ (ii) $M \vee J$

(iii) $\overline{M} \rightarrow \overline{J}$ (iv) $J \leftrightarrow M$

Solution

(i) Jo spent September in New York and Mary didn't have a little lamb.

(ii) Mary had a little lamb or Jo spent September in New York or both. (Alternatively: Mary had a little lamb and/or Jo spent September in New York.)

(iii) If Mary didn't have a little lamb then Jo didn't spend September in New York. (This sounds a little odd but there is no cause and effect implied between the antecedent and consequent of a conditional proposition in logic!)

(iv) If and only if Jo spent September in New York then Mary had a little lamb.

3. Let the propositions P, Q, R and S be defined as follows:

P: $6 > 24$.
Q: 12 is an even number.
R: $1000 = 10^3$.
S: π is a rational number.

State whether each of the propositions symbolised below is true or false.

(i) $P \rightarrow Q$ (ii) $R \veebar Q$ (iii) $S \leftrightarrow P$

(iv) $\overline{R} \wedge Q$ (v) $\overline{P} \wedge \overline{S}$

Solution

Note that Q and R are true propositions whereas P and S are false.

(i) This is a conditional proposition with a false antecedent and a true consequent. It is therefore true.

(ii) Both of the disjuncts in the exclusive disjunction are true. Hence the proposition is false.

(iii) Since both components of the biconditional are false, this proposition is true.

(iv) Since R is true, the negation $\overline{R}$ is false. The conjunction has components of which one is true and one false. This proposition is therefore false.

(v) Since P and S are both false, $\overline{P}$ and $\overline{S}$ are true propositions and hence their conjunction is true.

As we have seen, logical connectives can be used to join two simple propositions to form compound propositions. However, they can also be used between compound propositions to form other compound propositions. The following examples show how we can symbolise more complicated compound propositions.

Examples 2.2

1. Consider the following propositions:

   J: Jack ran.
   K: Ken laughed.
   S: Sally skipped.

Translate the following into reasonable English sentences:

(i) $(J \wedge K) \rightarrow S$ (ii) $\overline{J} \vee (K \wedge S)$
(iii) $(\overline{S} \rightarrow \overline{K}) \wedge (J \rightarrow K)$ (iv) $(J \vee S) \leftrightarrow \overline{K}$

Solution

(i) Note that the conjunction of J and K forms the antecedent of a conditional for which the consequent is S. This can be translated as 'If Jack ran and Ken laughed then Sally skipped'.

(ii) This is an inclusive disjunction in which the two disjuncts are $\overline{J}$ and $K \wedge S$. We must be careful to ensure that our translation gives the sense of $\overline{J} \vee (K \wedge S)$ rather than $(\overline{J} \vee K) \wedge S$ since the two are not equivalent. The best translation is probably 'Either Jack didn't run or both Ken laughed and Sally skipped'.

(iii) This is a conjunctive proposition with conjuncts which are the conditionals $\overline{S} \rightarrow \overline{K}$ and $J \rightarrow K$. It can be translated as 'If Sally didn't skip then Ken didn't laugh and, if Jack ran then Ken laughed'.

(iv) This biconditional translates as 'Jack ran or Sally skipped (or both) if and only if Ken didn't laugh'.

2. Consider the propositions defined as follows:

   T: I'll have more time.
   P: I'll learn to play the piano.
   S: I'll double my salary.

Symbolise the following:

(i) If I have more time then I'll double my salary and I won't learn to play the piano.

(ii) If and only if I double my salary or have more time then I won't learn to play the piano.

(iii) If I have more time then I'll learn to play the piano and if I don't have more time then I'll double my salary.

(iv) I'll learn to play the piano or I'll double my salary, and if I don't learn to play the piano then I'll have more time.

Solution

(i) There is an ambiguity here and it is not entirely clear whether this proposition should be symbolised $T \rightarrow (S \wedge \overline{P})$ or $(T \rightarrow S) \wedge \overline{P}$. However, the former symbolisation seems to convey the sense better.

(ii) Inclusive disjunction seems to be the most appropriate interpretation of 'or' in the first component of the biconditional. We would therefore symbolise this as $(S \vee T) \leftrightarrow \overline{P}$.

(iii) We symbolise this: $(T \rightarrow P) \wedge (\overline{T} \rightarrow S)$.

(iv) Again inclusive disjunction seems appropriate and we therefore symbolise this: $(P \vee S) \wedge (\overline{P} \rightarrow T)$.

Recall that we use upper case letters to denote particular propositions and lower case letters for propositional variables. Therefore an expression such as $(p \wedge q) \rightarrow (\overline{r} \vee \overline{p})$ does not denote a proposition. Such an expression is termed a **propositional form**. When specific propositions are substituted for the variables in a propositional form, this then becomes a proposition. Any proposition which can be obtained by substituting propositions for propositional variables in a propositional form is said to be a **substitution instance** of that form. Of course, the same proposition must be substituted for each occurrence of the same variable throughout the expression. For example, if T, P and S are

defined as in Example 2.2.2, the following are all substitution instances of the propositional form $(p \wedge q) \rightarrow (\overline{r} \vee \overline{p})$:

$(T \wedge S) \rightarrow (\overline{P} \vee \overline{T})$;
$(S \wedge P) \rightarrow (\overline{P} \vee \overline{S})$;
$[(T \vee S) \wedge (P \leftrightarrow R)] \rightarrow [(\overline{S \rightarrow R}) \vee (\overline{T \vee S})]$.

Note that in the second of these three propositions, we have substituted the same proposition, P, for each of the variables q and r. This is permissible. We may substitute the same proposition for different variables but we must not substitute different propositions for different occurrences of the same variable. There is an analogy here with substitution into algebraic expressions. Given an expression such as $f(x, y) = x^2 + 4xy + y^2$, substituting 2 for x and 3 for y gives $f(2, 3) = 2^2 + 4 \times 2 \times 3 + 3^2 = 37$. We may, of course, substitute the same values for x and y. For instance, substituting 1 for x and 1 for y gives $f(1, 1) = 1^2 + 4 \times 1 \times 1 + 1^2 = 6$.

We may reasonably ask, for what truth values of its simple components is a compound proposition true? For instance, given the propositional form $p \rightarrow (q \wedge \overline{r})$ (of which Example 2.2.2(i) is a substitution instance), for what combinations of truth values of p, q and r is this true? (Strictly speaking, it is the propositions which may be substituted for p, q and r which have truth values rather than the variables themselves.)

One way of answering this question is to draw up a truth table in which we list all the possible combinations of truth values of p, q and r and, for each of these, evaluate the truth or falsity of $p \rightarrow (q \wedge \overline{r})$. The truth table is built up in stages. We first list the possible combinations of truth values of the component propositional variables. There are eight of these as shown in the table below. (It is common practice to list the combinations of truth values in the order used in this table.)

p	q	r
T	T	T
T	T	F
T	F	T
T	F	F
F	T	T
F	T	F
F	F	T
F	F	F

Next we add a column which will show the truth values of $\overline{r}$ for each of the listed truth values of r. Then we add a column of truth values for $q \wedge \overline{r}$.

p	q	r	$\overline{r}$	$q \wedge \overline{r}$
T	T	T	F	F
T	T	F	T	T
T	F	T	F	F
T	F	F	T	F
F	T	T	F	F
F	T	F	T	T
F	F	T	F	F
F	F	F	T	F

Note that the truth values of $\overline{r}$ are the reverse of those of r shown in the adjacent column. The expression $q \wedge \overline{r}$ is true when both conjuncts are true, that is in the second and sixth rows of the truth table. Otherwise this propositional form is false.

We now add the final column to the truth table where we evaluate the truth values of $p \rightarrow (q \wedge \overline{r})$. This is a conditional and is false only when p is true and $q \wedge \overline{r}$ is false. This occurs in the first, third and fourth rows of the truth table. The final truth table is shown below.

p	q	r	$\overline{r}$	$q \wedge \overline{r}$	$p \rightarrow (q \wedge \overline{r})$
T	T	T	F	F	F
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	T	F	F
F	T	T	F	F	T
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	T	F	T

From the table we can see that the propositional form $p \rightarrow (q \wedge \overline{r})$ is true in all but the following three cases: p, q and r are all true; p and r are true but q is false; p is true but q and r are false.

Example 2.3

Draw up the truth table for the propositional form $(p \vee q) \wedge (\overline{p} \rightarrow r)$. (Example 2.2.2(iv) is a substitution instance of this form.)

Solution

Again we first list the possible combinations of truth values for p, q and r and then add a column to the table listing the corresponding truth values of $\overline{p}$. The next column to add is one for $p \vee q$ followed by a further column listing the truth values of $\overline{p} \rightarrow r$. The truth table up to this stage is shown below.

p	q	r	$\overline{p}$	$p \vee q$	$\overline{p} \rightarrow r$
T	T	T	F	T	T
T	T	F	F	T	T
T	F	T	F	T	T
T	F	F	F	T	T
F	T	T	T	T	T
F	T	F	T	T	F
F	F	T	T	F	T
F	F	F	T	F	F

The proposition $p \vee q$ is true when either or both of p and q are true, i.e. in all rows of the truth table except the last two. The proposition $\overline{p} \rightarrow r$ is true except when $\overline{p}$ is true and r is false. This occurs in the sixth and eighth rows of the table.

We now add the final column of the truth table listing the truth values for $(p \vee q) \wedge (\overline{p} \rightarrow r)$. This expression is the conjunction of the two components $p \vee q$ and $\overline{p} \rightarrow r$ and is true only when both these components are true (all rows of the truth table except the last three).

p	q	r	$\overline{p}$	$p \vee q$	$\overline{p} \rightarrow r$	$(p \vee q) \wedge (\overline{p} \rightarrow r)$
T	T	T	F	T	T	T
T	T	F	F	T	T	T
T	F	T	F	T	T	T
T	F	F	F	T	T	T
F	T	T	T	T	T	T
F	T	F	T	T	F	F
F	F	T	T	F	T	F
F	F	F	T	F	F	F

Exercises 2.1

1. Let the propositions S, W, R and T be defined as follows:

S: The sun shines.
W: The wind blows.
R: The rain falls.
T: The temperature rises.

Translate the following into reasonable English sentences:

(i) $W \rightarrow (\overline{S} \vee R)$ (ii) $(W \wedge R) \leftrightarrow \overline{S}$
(iii) $(W \vee R) \wedge \overline{T}$ (iv) $(\overline{S \wedge W}) \rightarrow (R \vee \overline{T})$
(v) $(\overline{R} \veebar T) \rightarrow (S \wedge \overline{W})$

2. With propositions S, W, R and T defined as in Exercise 1 above, symbolise the following propositions.

(i) If and only if the temperature rises, then the sun shines and the rain doesn't fall.

(ii) Whenever the sun shines or the rain falls (or both) then, if the temperature rises, the wind doesn't blow.

(iii) Either the sun shines and the temperature rises or the wind blows and the rain falls.

(iv) The sun shines and the wind doesn't blow, and the temperature rises only if the rain falls.

(v) If the sun doesn't shine or the wind blows with rain falling, then the temperature doesn't rise.

3. Suppose that the propositions S, W, R and T (as defined in Exercise 1 above) are all true. Decide whether each of the following is true or false:

(i) $(S \rightarrow W) \wedge (\overline{R} \wedge T)$ (ii) $(\overline{R \veebar \overline{T}}) \wedge S$
(iii) $(S \wedge \overline{R}) \leftrightarrow (T \vee \overline{W})$ (iv) $(\overline{R \wedge T}) \rightarrow (\overline{W} \wedge S)$
(v) $(\overline{R \vee T}) \wedge (W \rightarrow S)$

4. Let propositions S, W, R and T be defined as in Exercise 1 above. Suppose that S and W are true propositions and that R and T are false.

Find the truth value of each of the following compound propositions:

(i) $(S \wedge \overline{W}) \veebar (W \wedge R)$
(ii) $\overline{(R \rightarrow \overline{T})} \wedge W$
(iii) $W \rightarrow (\overline{T \vee R})$
(iv) $(R \rightarrow \overline{W}) \vee (W \rightarrow T)$
(v) $(R \veebar \overline{T}) \leftrightarrow (W \wedge \overline{S})$

5. Draw up a truth table for each of the following propositional forms:

(i) $(p \wedge q) \leftrightarrow \overline{q}$
(ii) $p \veebar (q \rightarrow \overline{p})$
(iii) $(p \rightarrow r) \wedge (r \rightarrow q)$
(iv) $(r \wedge p) \vee (\overline{q} \wedge \overline{p})$
(v) $(\overline{p \wedge q}) \rightarrow (p \wedge \overline{r})$

2.3 Tautologies and Contradictions

The truth table for the propositional form $p \rightarrow (p \vee q)$ is given below.

p	q	$p \vee q$	$p \rightarrow (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Note that, no matter what the truth values of the components p and q, the propositional form $p \rightarrow (p \vee q)$ is always true. This means that, no matter what propositions we substitute for the variables p and q, the result will be a true proposition. A propositional form which has this property is called a 'tautology'.

There are also propositional forms whose structure is such that they are always false no matter what the truth values of their components. Such propositional forms are called 'contradictions'. (Of course, the negation of a tautology is a contradiction and vice versa.) An example of a contradiction is the form $(\overline{p} \wedge q) \wedge (p \vee \overline{q})$. This is shown in the truth table below.

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \wedge q$	$p \vee \overline{q}$	$(\overline{p} \wedge q) \wedge (p \vee \overline{q})$
T	T	F	F	F	T	F
T	F	F	T	F	T	F
F	T	T	F	T	F	F
F	F	T	T	F	T	F

Definitions 2.1

A **tautology** is a propositional form which is true for all combinations of truth values of its component propositional variables.

A **contradiction** is a propositional form which is false for all combinations of truth values of its component propositional variables.

Note that any substitution instance of a tautology is a true proposition and that any substitution instance of a contradiction is a false proposition. The property of being a tautology or a contradiction is a direct consequence of the structure of a propositional form. The two propositions 'Paris is the capital of France' and 'If Paris is the capital of France, then Paris is the capital of France or Florence is the capital of Italy' are both true propositions but for fundamentally different reasons. The former is true by virtue of its content—Paris really is the capital of France. The latter is true by virtue of its structure—it is a substitution instance of the tautological form $p \rightarrow (p \vee q)$. The content of the component simple propositions has no bearing on the truth of any substitution instance of this propositional form. In particular, if France decided to move its capital to Lyons, the second proposition would still be true whereas the first would not.

Exercises 2.2

Determine whether each of the following propositional forms is a tautology, a contradiction or neither.

1. $p \wedge \overline{p}$
2. $\overline{p} \vee p$
3. $(p \wedge q) \leftrightarrow (q \wedge p)$
4. $(p \wedge q) \wedge (p \rightarrow \overline{q})$
5. $(p \wedge \overline{q}) \wedge (\overline{p} \vee q)$
6. $(p \rightarrow q) \leftrightarrow (p \wedge \overline{q})$
7. $(p \vee q) \wedge \overline{(p \vee q)}$ (*Hint*: compare with Exercise 1 above.)
8. $\overline{(p \rightarrow q)} \vee (p \rightarrow q)$ (*Hint*: compare with Exercise 2 above.)
9. $(p \rightarrow \overline{r}) \vee (\overline{q} \rightarrow p)$

10. $(p \wedge \overline{p}) \rightarrow (p \rightarrow r)$
11. $(p \veebar q) \wedge (q \wedge r)$
12. $(p \vee q) \leftrightarrow (q \rightarrow r)$
13. $[(p \rightarrow q) \wedge (p \vee r)] \wedge (\overline{r} \wedge \overline{q})$
14. (a) Explain why, if p_1 is a contradiction, then $p_1 \rightarrow p_2$ is a tautology for any propositional form p_2.
    (b) Explain why, if p_2 is a tautology, then $p_1 \rightarrow p_2$ is a tautology for any propositional form p_1.

2.4 Logical Implication and Logical Equivalence

At the beginning of this chapter, we described a mathematical proof as a sequence of propositions where the truth of each is assumed or is guaranteed by the truth of earlier propositions in the sequence. Part of the skill in constructing a proof is being able to deduce what propositions can be shown to be true given the truth of other propositions. In this section we consider some ways in which the truth of one proposition guarantees the truth of another.

A structure-dependent relation

There is a structure-dependent relation which may exist between a pair of propositional forms p_1 and p_2 whereby, whenever p_1 is true, p_2 is true also. In this case we say that p_1 **logically implies** p_2 and we write $p_1 \vdash p_2$. Consider for example the two forms $\overline{p}$ and $\overline{p} \vee \overline{q}$. The truth values of each of these are shown in the truth table below.

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \vee \overline{q}$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

From the table, we can see that whenever $\overline{p}$ is true (the third and fourth rows of the table), $\overline{p} \vee \overline{q}$ is also true. Hence $\overline{p}$ logically implies $\overline{p} \vee \overline{q}$ and we denote this by $\overline{p} \vdash (\overline{p} \vee \overline{q})$. (We can also see from the table that $\overline{q} \vdash (\overline{p} \vee \overline{q})$.)

If the two propositional forms p_1 and p_2 are such that $p_1 \vdash p_2$, then there is no combination of truth values of the propositional variables which renders p_1 true and p_2 false. Recall that this is the only situation where the conditional $p_1 \rightarrow p_2$ would be false. Hence if p_1 logically implies p_2 then $p_1 \rightarrow p_2$ is true for all truth values of its component propositional variables and is therefore a tautology. (This can be illustrated by reference to the truth table above, where completing one further column for $\overline{p} \rightarrow (\overline{p} \vee \overline{q})$ will show this propositional form to be a tautology.) It is also the case that, if two propositional forms p_1 and p_2 are such that $p_1 \rightarrow p_2$ is a tautology, then $p_1 \vdash p_2$.

It is important to note that for the relationship $p_1 \vdash p_2$ all we require is that p_2 is true in all circumstances that p_1 is true. The propositional form p_2 may also be true in some or all of the cases where p_1 is false. This is so in the second row of the table above where $\overline{p}$ is false and $\overline{p} \vee \overline{q}$ is true. What is useful about logical implication is that, if $p_1 \vdash p_2$, then, given a true substitution instance of p_1, substituting the same propositions for the variables in p_2 also results in a true proposition. For example, if P and Q denote particular propositions and we know that $\overline{P}$ is true, then the fact that $\overline{p} \vdash (\overline{p} \vee \overline{q})$ guarantees that $\overline{P} \vee \overline{Q}$ is also a true proposition.

If two propositional forms p_1 and p_2 are such that $p_1 \vdash p_2$, then we know that p_2 is true whenever p_1 is true. However, $p_1 \vdash p_2$ gives us no information about the truth value of p_2 when p_1 is false, so that we cannot infer that p_2 logically implies p_1. From the truth table above, we established that $\overline{p} \vdash (\overline{p} \vee \overline{q})$. However, if we examine the cases where $\overline{p} \vee \overline{q}$ is true (all but the first row of the truth table) we note that $\overline{p}$ is false in one of these so that $\overline{p} \vee \overline{q}$ does not logically imply $\overline{p}$. Consider, however, the two propositional forms $p \rightarrow q$ and $\overline{p} \vee q$ for which the truth table is given below.

p	q	$\overline{p}$	$p \rightarrow q$	$\overline{p} \vee q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Whenever $p \rightarrow q$ is true then so is $\overline{p} \vee q$ so that $(p \rightarrow q) \vdash (\overline{p} \vee q)$. Also, whenever $\overline{p} \vee q$ is true then so is $p \rightarrow q$ so that $(\overline{p} \vee q) \vdash (p \rightarrow q)$. The two propositional forms $\overline{p} \vee q$ and $p \rightarrow q$ have exactly the same set of truth values. When this is the case, we say that the two forms are **logically equivalent** and we write $(\overline{p} \vee q) \equiv (p \rightarrow q)$ (or $(p \rightarrow q) \equiv (\overline{p} \vee q)$). Note that if the two propositional forms p_1 and p_2 are logically equivalent so that $p_1 \equiv p_2$ then $p_1 \vdash p_2$ and also $p_2 \vdash p_1$.

Logically equivalent propositional forms have identical truth values for each assignment of truth values to their component propositional variables. Recall that the biconditional form $p \leftrightarrow q$ is true whenever the components p and q have the same truth value. So, if we substitute logically equivalent propositional forms p_1 and p_2 for p and q, the biconditional $p_1 \leftrightarrow p_2$ cannot be false. Therefore, if $p_1 \equiv p_2$ then $p_1 \leftrightarrow p_2$ is a tautology and also, if $p_1 \leftrightarrow p_2$ is a tautology then $p_1 \equiv p_2$. Hence we have a similar relation between logical equivalence and the biconditional as we have between logical implication and the conditional.

What is useful about logical equivalence is that we can replace one propositional form by another which is logically equivalent, secure in the knowledge that we have not altered the set of truth values. Logically equivalent forms can therefore be regarded as alternative expressions of a propositional form in the same way that $(x + 2)^2$ and $x^2 + 4x + 4$ are regarded as equivalent algebraic expressions.

Given two logically equivalent propositional forms, the substitution instances obtained by substituting the same propositions for the same variables throughout each form will be referred to as **equivalent propositions**. To all intents and purposes, equivalent propositions say the same thing although they may express it differently. What is important about a set of equivalent propositions is that, if one is true, then so are all the others and if any one of the set is false, then we can be sure that the rest are too. For instance, we have established the logical equivalence of $\overline{p} \vee q$ and $p \rightarrow q$. Hence, given two propositions P and Q, $\overline{P} \vee Q$ and $P \rightarrow Q$ are equivalent propositions and therefore have the same truth value. Of course we do not have to substitute simple

propositions for the variables. Given four propositions P, Q, R and S, if we replace p by $P \wedge R$ and q by $Q \wedge \overline{S}$ we obtain the equivalent propositions $(\overline{P \wedge R}) \vee (Q \wedge \overline{S})$ and $(P \wedge R) \rightarrow (Q \wedge \overline{S})$.

Example 2.4

Draw up a truth table to establish the set of truth values for each of the propositional forms $q \vee \overline{p}$, $\overline{q} \rightarrow \overline{p}$ and $\overline{p} \wedge \overline{q}$. Between which pairs of these forms does the relation of (a) logical equivalence, (b) logical implication, exist?

Solution

The truth table for these three forms is given below.

p	q	$\overline{p}$	$\overline{q}$	$q \vee \overline{p}$	$\overline{q} \rightarrow \overline{p}$	$\overline{p} \wedge \overline{q}$
T	T	F	F	T	T	F
T	F	F	T	F	F	F
F	T	T	F	T	T	F
F	F	T	T	T	T	T

(a) We first look for logical equivalences. Since the fifth and sixth columns of the table are identical, we can conclude that $q \vee \overline{p}$ and $\overline{q} \rightarrow \overline{p}$ are logically equivalent, i.e. $(q \vee \overline{p}) \equiv (\overline{q} \rightarrow \overline{p})$ (or $(\overline{q} \rightarrow \overline{p}) \equiv (q \vee \overline{p})$). None of the remaining columns are the same so there are no other logical equivalences.

(b) Since $q \vee \overline{p}$ and $\overline{q} \rightarrow \overline{p}$ are logically equivalent, we have the two logical implications $(q \vee \overline{p}) \vdash (\overline{q} \rightarrow \overline{p})$ and $(\overline{q} \rightarrow \overline{p}) \vdash (q \vee \overline{p})$. There are other logical implications. Note that when $\overline{p} \wedge \overline{q}$ is true (the fourth row of the truth table), each of $q \vee \overline{p}$ and $\overline{q} \rightarrow \overline{p}$ is also true. Hence we have $(\overline{p} \wedge \overline{q}) \vdash (q \vee \overline{p})$ and $(\overline{p} \wedge \overline{q}) \vdash (\overline{q} \rightarrow \overline{p})$. (But note that $q \vee \overline{p}$ does *not* logically imply $\overline{p} \wedge \overline{q}$ because, as is shown in the first and third rows of the truth table, it is possible for $q \vee \overline{p}$ to be true whilst $\overline{p} \wedge \overline{q}$ is false. For the same reason, $\overline{q} \rightarrow \overline{p}$ does not logically imply $\overline{p} \wedge \overline{q}$.)

As we shall see later, there are instances when we shall find it helpful to substitute for one propositional form another which is logically

Table 2.1 Replacement Rules

Commutation (Com)	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$
Association (Assoc)	$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
Distribution (Dist)	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
De Morgan's laws (De M)	$\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$ $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$
Double negation (DN)	$p \equiv \overline{\overline{p}}$
Transposition (Trans)	$p \rightarrow q \equiv \overline{q} \rightarrow \overline{p}$
Material implication (Impl)	$p \rightarrow q \equiv \overline{p} \vee q$
Material equivalence (Equiv)	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ $p \leftrightarrow q \equiv (p \wedge q) \vee (\overline{p} \wedge \overline{q})$
Tautology (Taut)	$p \wedge p \equiv p$ $p \vee p \equiv p$
Exportation (Exp)	$(p \wedge q) \rightarrow r \equiv p \rightarrow (q \rightarrow r)$

equivalent. Table 2.1 shows a list of logical equivalences which we shall find particularly useful. These are referred to as 'replacement rules' and all can be verified using the techniques described in the last section. We give the name of each rule and also the accepted abbreviation which is normally used to refer to that rule.

(Note that the association rules imply that we can omit the brackets from an expression such as $(p \vee q) \vee r$ and simply write $p \vee q \vee r$ without fear of ambiguity.)

We can use these logical equivalences to establish other logical equivalences as we show in the examples below.

Examples 2.5

1. Show that $\overline{q \wedge p} \equiv p \rightarrow \overline{q}$.

Solution

We start with the left-hand side of the 'equivalence' and proceed in steps, using the replacement rules to substitute one logically equivalent propositional form for another within the expression until we obtain the right-hand side. Each step is justified by referring to the rule which allows us to make the substitution used in that step.

$$\begin{aligned} \overline{q \wedge p} &\equiv \overline{q} \vee \overline{p} && \text{(De M)} \\ &\equiv \overline{p} \vee \overline{q} && \text{(Com)} \\ &\equiv p \rightarrow \overline{q} && \text{(Impl)} \end{aligned}$$

2. Show that $p \wedge [(p \wedge q) \vee r] \equiv p \wedge (q \vee r)$.

Solution

Proceeding as in the example above:

$$\begin{aligned} p \wedge [(p \wedge q) \vee r] &\equiv [p \wedge (p \wedge q)] \vee (p \wedge r) && \text{(Dist)} \\ &\equiv [(p \wedge p) \wedge q] \vee (p \wedge r) && \text{(Assoc)} \\ &\equiv (p \wedge q) \vee (p \wedge r) && \text{(Taut)} \\ &\equiv p \wedge (q \vee r) && \text{(Dist)} \end{aligned}$$

Note that the replacement rules can be used to substitute for part of a propositional form as in the second line of the example above where the association replacement rule was applied to the first disjunct $p \wedge (p \wedge q)$ and in the third line where we substitute p for $p \wedge p$.

Exercises 2.3

1. In each of the following, two propositional forms p_1 and p_2 are given. For each pair of propositional forms, draw up a truth table and determine which, if any, of the following logical relationships hold: $p_1 \vdash p_2$, $p_2 \vdash p_1$, $p_1 \equiv p_2$.

	p_1	p_2
(i)	$\overline{p} \vee \overline{q}$	$\overline{p \wedge q}$
(ii)	$p \rightarrow q$	$q \rightarrow p$
(iii)	p	$q \wedge (p \leftrightarrow q)$
(iv)	p	$q \rightarrow p$
(v)	$\overline{p \veebar q}$	$p \veebar \overline{q}$
(vi)	$p \rightarrow q$	$\overline{p \wedge \overline{q}}$
(vii)	$\overline{p \vee q}$	$\overline{p} \vee \overline{q}$
(viii)	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$
(ix)	$p \vee (q \vee r)$	$(p \vee q) \vee r$
(x)	$p \wedge (q \vee r)$	$(p \wedge q) \vee (p \wedge r)$
(xi)	$p \rightarrow q$	$\overline{q} \rightarrow \overline{p}$

2. Suppose that the following are true propositions:

If I pass my exams then I shall get a new job.
Tomorrow is my birthday.

Use the appropriate logical relations established in Exercise 1 above to determine what, if anything, can be deduced about the truth value of each of the following propositions:

(i) If I get a new job then I shall pass my exams.

(ii) If Today is Tuesday then tomorrow is my birthday.

(iii) I shall get a new job.

(iv) I'll throw a party and, if and only if tomorrow is my birthday, then I'll throw a party.

(v) If I don't get a new job then I won't pass my exams.

3. Use the appropriate logical relations established in Exercise 1 above to determine whether each of the following propositional forms is or is not a tautology.

(i) $(\overline{p} \vee \overline{q}) \leftrightarrow (\overline{p \wedge q})$

(ii) $(q \rightarrow p) \rightarrow p$

(iii) $p \leftrightarrow [q \wedge (p \leftrightarrow q)]$

(iv) $(p \veebar \overline{q}) \rightarrow (\overline{p \veebar q})$

(v) $\overline{(\overline{p} \wedge \overline{q})} \leftrightarrow (p \rightarrow q)$
(vi) $\overline{(\overline{p} \vee \overline{q})} \rightarrow (\overline{p} \vee \overline{q})$
(vii) $[(p \vee q) \vee r)] \leftrightarrow [p \vee (q \vee r)]$
(viii) $p \rightarrow (q \rightarrow p)$
(ix) $(p \leftrightarrow q) \rightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$
(x) $[(p \rightarrow q) \wedge (q \rightarrow p)] \rightarrow (p \leftrightarrow q)$

4. Given the propositional form $p \rightarrow q$, we define the following:

(a) the **converse** of $p \rightarrow q$: $q \rightarrow p$;
(b) the **inverse** of $p \rightarrow q$: $\overline{p} \rightarrow \overline{q}$;
(c) the **contrapositive** of $p \rightarrow q$: $\overline{q} \rightarrow \overline{p}$.

Show that a conditional propositional form is logically equivalent to its contrapositive (i.e. verify the replacement rule called 'transposition') but not to either its converse or inverse. Show also that the converse and inverse of a conditional propositional form are logically equivalent (the transposition rule again).

5. Show that $[(p \rightarrow q) \wedge (p \rightarrow r)] \equiv [p \rightarrow (q \wedge r)]$. Use this result to show that, if p_1, p_2 and p_3 are propositional forms such that $p_1 \vdash p_2$ and $p_1 \vdash p_3$, then $p_1 \vdash (p_2 \wedge p_3)$.

6. Show that $(p \rightarrow q) \wedge [(p \wedge q) \rightarrow r]$ logically implies $p \rightarrow r$.

7. By considering the appropriate underlying propositional forms, determine whether or not each of the following pairs of propositions are equivalent:

(i) $\overline{P \vee Q}$ and $P \wedge \overline{Q}$
(ii) $R \wedge (S \vee T)$ and $(R \wedge T) \vee (S \wedge R)$
(iii) $P \rightarrow \overline{Q}$ and $\overline{P \vee Q}$
(iv) $\overline{R} \rightarrow S$ and $S \rightarrow \overline{R}$
(v) $P \rightarrow (\overline{Q} \vee \overline{R})$ and $(Q \wedge R) \rightarrow \overline{P}$

8. (a) Use truth tables to demonstrate the following logical equivalences, where t denotes any tautology and f denotes any contradiction. (Note that all tautologies are logically equivalent as are all contradictions.)

Identity laws

$$p \vee f \equiv p \qquad p \wedge t \equiv p$$
$$p \vee t \equiv t \qquad p \wedge f \equiv f$$

Complement laws

$$p \vee \overline{p} \equiv t$$
$$p \wedge \overline{p} \equiv f$$

(b) Use the replacement rules together (where necessary) with the rules established above to demonstrate each of the following logical equivalences. Justify each step (as in Examples 2.5).

(i) $\overline{p} \vee (p \wedge q) \equiv \overline{p} \vee q$

(ii) $(\overline{p \vee q}) \vee (\overline{p} \wedge q) \equiv \overline{p}$

(iii) $(\overline{\overline{p} \wedge q}) \wedge (p \vee \overline{q}) \equiv (p \vee \overline{q})$

(iv) $p \vee [q \wedge (p \vee \overline{q})] \equiv p \vee (p \wedge q)$

(v) $p \wedge [(p \wedge q) \vee \overline{p}] \equiv p \wedge q$

2.5 Arguments and Argument Forms

The importance of logic is that it supplies us with a means of establishing whether a line of reasoning called an 'argument' is correct or incorrect. An argument in this sense consists of a set of propositions (simple or compound) called **premises** and another proposition called the **conclusion**, which, it is claimed, is the inevitable consequence of the premises. The proposition which constitutes the conclusion is usually introduced by 'therefore' or 'hence' to distinguish it from the premises. The following are examples of arguments.

Examples 2.6

Symbolise the premises and conclusion in each of the following arguments.

1. Today Sue has a biology exam or a maths exam or both. She doesn't have a biology exam today. Therefore she must have a maths exam today.

Solution

The premises of this argument are the two propositions 'Today Sue has a biology exam or a maths exam or both' and 'Sue doesn't have a biology exam today'. The conclusion is 'Sue has a maths exam today'.

We symbolise the component simple propositions of which the argument is constituted as follows:

B: Sue has a biology exam today.
M: Sue has a maths exam today.

The premises of the argument are: $B \vee M$ and $\overline{B}$.
The conclusion is: M.

2. If Jack plays the piano or Mary sings, then Pete will dance. Jack won't play the piano. So Pete won't dance.

Solution

We define the following simple propositions:

J: Jack plays the piano.
M: Mary sings.
P: Pete will dance.

The premises of the argument are: $(J \vee M) \rightarrow P$ and $\overline{J}$.
The conclusion is: $\overline{P}$.

In judging the 'quality' of each of these two arguments, there would probably be no difficulty in correctly assessing the first one as 'a good argument'—even with no knowledge of formal logic. The justification would probably run roughly as follows: 'We know that Sue has either a biology or a maths exam today. We also know that she hasn't a biology exam today. Assuming these statements to be true, we must conclude that she has a maths exam today.' Given the truth of the premises, we have no option but to accept the truth of the conclusion and hence we would judge the argument to be 'correct' or 'valid'.

With the second argument, however, it is not difficult to see that it is possible for the premises to be true and the conclusion false. Such would be the case, for instance, when Pete dances and Jack doesn't play the piano but Mary nevertheless sings. (It is also the case when Pete dances, Jack doesn't play the piano and Mary doesn't sing, although

this may not be so obvious.) What is important is that the truth of the premises does not guarantee the truth of the conclusion and, for this reason, we would say that the argument is not valid.

It is important to note that it is not the content of an argument which determines whether or not it is valid. What is important is its structure. For instance, if we accept the validity of the argument in Example 2.6.1, then we must also accept the validity of the following: 'There are either unicorns or dinosaurs in my garden, or both. There are no unicorns in my garden. Therefore there are dinosaurs in my garden.' Although we might well question the truth of the premises, this has no relevance to the validity of the argument. *If* the premises are true, then the conclusion must be true also. The fact that we may believe that there are no circumstances in which the premises could be true may well limit the usefulness of that particular argument. However, it does not detract from its validity. Both of these two arguments have premises which are substitution instances of the propositional forms $p \vee q$ and $\overline{p}$ and a conclusion which is the corresponding substitution instance of q. Any proposition can be substituted for the propositional variables p and q (as long as the same proposition is substituted for the same variable throughout) and the result is a valid argument.

As we have seen, what an argument is about has no bearing upon its validity. The only important factor is the structure of the propositional forms of which its premises and conclusion are substitution instances. We shall therefore make a distinction between arguments and argument forms which parallels that between propositions and propositional forms. An **argument form** has premises and conclusion expressed as propositional variables or propositional forms. When propositions are substituted for the propositional variables so that the premises and conclusion are propositions, we shall call the structure an **argument** and refer to it as a **substitution instance** of the corresponding argument form. Hence the two arguments:

(a) 'Today Sue has a biology exam or a maths exam or both. She doesn't have a biology exam today. Therefore she must have a maths exam today.'

and

(b) 'There are either unicorns or dinosaurs in my garden, or both. There are no unicorns in my garden. Therefore there are dinosaurs in my garden.'

are both substitution instances of the argument form with premises $p \vee q$, $\bar{p}$ and conclusion q. Similarly the argument in Example 2.6.2 is a substitution instance of the argument form with premises $(p \vee q) \rightarrow r$, $\bar{p}$ and conclusion $\bar{r}$.

We shall define an argument form as valid if its conclusion is true in all circumstances that its premises are true. What is important about argument forms is that, if we decide that a given argument form is valid, then it follows that any substitution instance of it is a valid argument. Argument forms therefore enable us to assess the validity of whole families of arguments.

Definitions 2.2(a)

An argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q is said to be **valid** if, whenever $p_1, p_2, \ldots, p_n$ are true, then q is also true. Otherwise the argument form is said to be **invalid**.

An argument is said to be **valid** if it is a substitution instance of a valid argument form. Otherwise the argument is said to be **invalid**.

To establish whether or not an argument is valid, we shall examine the underlying argument form. If the argument form is valid, then so is the argument. If the argument is a substitution instance of an invalid argument form then it is an invalid argument.

Consider an argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q. To decide whether or not the argument form is valid, we must examine the possible truth values of q for the cases when $p_1, p_2, \ldots, p_n$ are all true. Note that when $p_1, p_2, \ldots, p_n$ are all true then their conjunction $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ is also true. The converse is also the case: when the conjunction $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ is true, then its conjuncts $p_1, p_2, \ldots, p_n$ are all true. The statement '$p_1, p_2, \ldots, p_n$ are all true' is therefore equivalent to '$p_1 \wedge p_2 \wedge \ldots \wedge p_n$ is true'. For an argument form to be valid we require that, whenever $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ is true, the conclusion q is also true. This, of course, is exactly the same as requiring that $p_1 \wedge p_2 \wedge \ldots \wedge p_n$ logically implies q, i.e. $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \vdash q$. This gives us an alternative to Definition 2.2(a) for a valid argument form. An argument form is valid if the conjunction of its premises logically implies

its conclusion. Of course the definition of a valid argument remains as given in Definitions 2.2(a).

Definition 2.2(b)

An argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q is said to be **valid** if $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \vdash q$. Otherwise the argument form is said to be **invalid**.

We could also define validity in terms of the alternative way of expressing logical implication. An argument form is valid if the conditional with the conjunction of the premises as the antecedent and the conclusion as the consequent is a tautology, i.e. if $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is a tautology. If this is not the case, then the argument form is invalid.

We now have a method for establishing whether or not an argument is valid. We examine the corresponding argument form and test whether the conjunction of the premises logically implies the conclusion using the truth table technique described in Section 2.4.

Examples 2.7

1. Test the validity of the following argument.

If Jim arrives tomorrow then I'll eat my hat. Jim won't arrive tomorrow. Therefore I won't eat my hat.

Solution

We symbolise the component simple propositions as follows:

J: Jim arrives tomorrow.
H: I'll eat my hat.

The premises of the argument are: $J \rightarrow H$ and $\overline{J}$.
The conclusion is: $\overline{H}$.

The underlying argument form has premises $p \rightarrow q$ and $\overline{p}$. Its conclusion is $\overline{q}$. We must therefore test whether or not $(p \rightarrow q) \wedge \overline{p}$ logically implies $\overline{q}$. The appropriate truth table, drawn up in the usual way, is given below.

p	q	$\overline{p}$	$\overline{q}$	$p \rightarrow q$	$(p \rightarrow q) \wedge \overline{p}$
T	T	F	F	T	F
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

We now examine the table to determine the truth values of $\overline{q}$ when $(p \rightarrow q) \wedge \overline{p}$ is true, i.e. in the third and fourth rows. We note that, in the third row $\overline{q}$ is false when $(p \rightarrow q) \wedge \overline{p}$ is true. Hence the conjunction of the premises of the argument form does not logically imply the conclusion and the argument form is invalid. Hence the argument is not valid.

2. Test the validity of the following argument.

If you work hard then you'll get a good job. If you get a good job then you'll be a respected member of the community. Therefore if you work hard then you'll be a respected member of the community.

Solution

There are three underlying simple propositions:

W: You work hard.
J: You get a good job.
R: You'll be a respected member of the community.

The premises of the argument are $W \rightarrow J$ and $J \rightarrow R$. The conclusion is $W \rightarrow R$.

The underlying argument form has premises $p \rightarrow q$ and $q \rightarrow r$ and it has conclusion $p \rightarrow r$. We must therefore test whether or not $(p \rightarrow q) \wedge (q \rightarrow r)$ logically implies $p \rightarrow r$.

p	q	r	$p \rightarrow q$	$q \rightarrow r$	$(p \rightarrow q) \wedge (q \rightarrow r)$	$p \rightarrow r$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	T	F	T
T	F	F	F	T	F	F
F	T	T	T	T	T	T
F	T	F	T	F	F	T
F	F	T	T	T	T	T
F	F	F	T	T	T	T

Whenever $(p \to q) \wedge (q \to r)$ is true (the first, fifth, seventh and eighth rows), $p \to r$ is also true. Hence $[(p \to q) \wedge (q \to r)] \vdash (p \to r)$ and so the argument form is valid. Since the argument is a substitution instance of this argument form, it is a valid argument.

Inconsistent premises

Consider the following argument.

If Mike is on holiday then he's in Bermuda. Either Mike is on holiday or he's in the office. Mike is not in the office and he's not in Bermuda. Therefore Mike is ill.

The underlying argument form has premises $p \to q$, $p \vee r$ and $\bar{r} \wedge \bar{q}$. If we construct the truth table for the conjunction of these premises (see Exercise 2.2.13), we find that this propositional form is false for all combinations of truth values of the propositional variables p, q and r. In other words, it is impossible for the premises to be true simultaneously. We refer to a set of premises with this property as **inconsistent.**

For an argument form to be valid we require $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ to be a tautology where $p_1, p_2, \ldots, p_n$ are premises and q is the conclusion. For a set of inconsistent premises, the antecedent of this conditional is a contradiction, i.e. it is always false. Since a conditional with a false antecedent is true, it follows that $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ is a tautology regardless of the form of the conclusion q. We are therefore faced with what might seem to be a rather disconcerting fact—an argument form with inconsistent premises is always valid so that any substitution instance is a valid argument. Hence the argument above is valid and would remain so were we to replace the conclusion by 'Mike is in Bermuda', 'Pigs can fly' or any other proposition.

Even though they are always valid, argument forms with inconsistent premises are not particularly useful since they support any conclusion whatsoever. We shall therefore find it useful to distinguish what are known as 'sound' arguments from those which are 'unsound'. A **sound argument** is defined as one which is valid and whose premises are all true. It follows that the conclusion of such an argument has two desirable properties. Firstly it is justified by the rules of logic. Secondly, because the premises are true, it is a true proposition. Of course, it is not always possible to establish whether or not a valid argument is sound

because we may be ignorant as to the truth value of one or more of the premises. However, if an argument is a substitution instance of an argument form with inconsistent premises, then it will certainly not be sound. So, although the conclusion is justified on logical grounds, we have no guarantee of its truth.

Exercises 2.4

Test the validity of each of the following arguments.

1. If you exercised regularly then you'd be healthy. You're not healthy. Therefore you don't exercise regularly.

2. If weapons are banned then we'll all live in peace. We'll all live in peace or the human race will become extinct. We won't live in peace. Therefore weapons won't be banned.

3. You are rich only if you are clever or dishonest. You are neither clever nor dishonest. Therefore you are not rich.

4. Jane will come to my party if and only if Mark doesn't come. If Jane doesn't come to my party then Jim won't come. Therefore, either Jim or Mark will come to my party but not both.

5. The temperature rises if and only if the sun shines. The sun isn't shining and there are clouds in the sky. If there are clouds in the sky then the temperature rises. Therefore it will not rain today.

6. If you read a lot then you will become a brilliant conversationalist. If you become a brilliant conversationalist then you will have many friends. Therefore if you haven't many friends then you don't read a lot.

7. I shall mow the lawn or clean the car but not both. If I mow the lawn then it won't rain. Therefore, it rains only if I clean the car.

8. If the car's out of oil then the engine has seized up. The engine hasn't seized up or the car's out of petrol. The car's not out of petrol but it's out of oil. So the engine has seized up.

9. Either prices fall or there will be an election. If prices don't fall there will be widespread poverty. Therefore if there is an election then there won't be widespread poverty.

10. If I buy a new car then I will not go on holiday. If I don't buy a new car then I will buy a motorcycle. Therefore either I go on holiday or I buy a motorcycle but not both.

2.6 Formal Proof of the Validity of Arguments

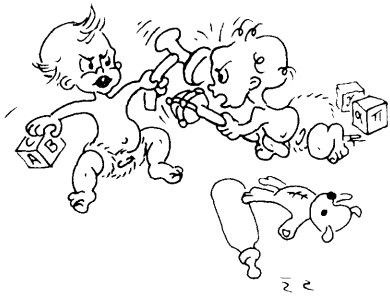
It is clear that the truth table method for assessing the validity of an argument can become unwieldy if the premises are complicated. Also, if the argument involves n simple propositions, the truth table requires 2^n rows. Hence the method becomes impractical if the number of simple propositions exceeds three or four.

There is an alternative method for showing an argument to be valid which does not necessitate constructing a truth table. The method involves deriving a sequence of propositions all of which are known to be true when the premises are true. The premises themselves form the starting point for the list. From these, other propositions may be added subject only to the constraint that their truth is guaranteed by the truth of one or more propositions already included in the list. The list is complete when the conclusion of the argument is shown to satisfy this 'eligibility criterion'. The list of propositions, terminating with the argument's conclusion, is called a **formal proof** of the validity of the argument.

Premises are automatically eligible for inclusion in the sequence of propositions which constitutes the formal proof. However, how do we determine which other propositions may be included? Suppose that the list currently contains the propositions (simple or compound) $P_1, P_2, \ldots, P_n$ with underlying propositional forms $p_1, p_2, \ldots, p_n$. That is to say, P_i is a substitution instance of p_i for $i = 1, 2, \ldots, n$ with the same proposition substituted for the same variable throughout the sequence. Now suppose we have a propositional form p_{n+1} which is logically implied by the conjunction of some (or all) of the propositional forms $p_1, p_2, \ldots, p_n$. Then whenever the propositional forms in question are true, p_{n+1} is true also. We may therefore add to the list the appropriate substitution instance of p_{n+1}. For example, suppose that the list contains the propositions P and $P \rightarrow Q$. These are substitution instances of p and $p \rightarrow q$. Since $[p \wedge (p \rightarrow q)] \vdash q$, we may include in the formal proof the proposition Q if we wish.

Note that in this example, to say that $[p \wedge (p \rightarrow q)] \vdash q$ is the same as saying that the argument form with premises p and $p \rightarrow q$ and

conclusion q is valid. Therefore propositions which are eligible for inclusion in the formal proof are those which form the conclusions of valid arguments with premises which are propositions already included in the proof. In constructing formal proofs it would therefore be helpful to have a stock of valid argument forms from which to draw. These are termed **rules of inference** and we will find that nine will suffice. Each is an elementary argument form whose validity can be confirmed using truth tables as in the previous section. We summarise these in Table 2.2 together with the usual name of the rule and the abbreviation by which we shall refer to it.



Elementary argument form

Of course, the 'eligibility criterion' described above also allows us to include in our proof the corresponding substitution instance of any propositional form which is logically equivalent to one of the p_i, $i = 1, 2, \ldots, n$. In other words, it allows us to include any proposition which is equivalent to one already in the list. For instance if the proof contains

Table 2.2 Rules of inference for constructing formal proofs

Name of rule	Premises	Conclusion
Simplification (Simp)	$p \wedge q$	p
Addition (Add)	p	$p \vee q$
Conjunction (Conj)	p, q	$p \wedge q$
Disjunctive syllogism (DS)	$p \vee q, \overline{p}$	q
Modus ponens (MP)	$p \rightarrow q, \quad p$	q
Modus tollens (MT)	$p \rightarrow q, \quad \overline{q}$	$\overline{p}$
Hypothetical syllogism (HS)	$p \rightarrow q, \quad q \rightarrow r$	$p \rightarrow r$
Absorption (Abs)	$p \rightarrow q$	$p \rightarrow (p \wedge q)$
Constructive dilemma (CD)	$(p \rightarrow q) \wedge (r \rightarrow s)$, $p \vee r$	$q \vee s$

the proposition $\overline{P \wedge Q}$, then we may add, if we wish, the equivalent proposition $\overline{P} \vee \overline{Q}$ because of the logical equivalence of $\overline{p \wedge q}$ and $\overline{p} \vee \overline{q}$ (De Morgan's law—see Section 2.4). We may also use logical equivalence (but not logical implication) to substitute for any part of a compound proposition. For instance, if our proof contains $(R \wedge S) \vee (Q \rightarrow R)$, we may add $(R \wedge S) \vee (\overline{R} \rightarrow \overline{Q})$. This is because the transposition rule states that $p \rightarrow q \equiv \overline{q} \rightarrow \overline{p}$, from which we can deduce the logical equivalence of $(q \wedge r) \vee (p \rightarrow q)$ and $(q \wedge r) \vee (\overline{q} \rightarrow \overline{p})$ and hence the equivalence of the propositions $(R \wedge S) \vee (Q \rightarrow R)$ and $(R \wedge S) \vee (\overline{R} \rightarrow \overline{Q})$. To help us identify equivalent propositions, we shall find it useful to refer to the replacement rules given in Section 2.4.

We summarise the essential features of the method of formal proof below.

Method of formal proof

Given an argument with premises $P_1, P_2, \ldots, P_n$ and conclusion Q, a formal proof of the validity of the argument consists of a list of propositions which terminates with Q. Every proposition in the list must satisfy one or more of the following criteria:

(a) it is a premise of the argument;

(b) it can be derived from one or more of the propositions already included in the list using one of the rules of inference;

(c) it is equivalent to a proposition already included in the list because one of the replacement rules guarantees the logical equivalence of the appropriate underlying propositional forms.

It is not always easy to see one's way through a formal proof. Having commenced the proof by listing the premises, it often helps to examine the conclusion and to decide which propositions need to be added to justify its inclusion. A justification for adding these propositions can then be sought.

We now give some examples to illustrate how we can construct formal proofs of the validity of simple arguments. We shall number each proposition as it is added to the list so that we can refer to it. Also we must provide a justification for the addition of each proposition.

Examples 2.8

1. Construct a formal proof of the validity of the following argument:

Jack is in Paris only if Mary is in New York. Jack is in Paris and Fred is in Rome. Therefore Mary is in New York.

Solution

We symbolise the component simple propositions:

J: Jack is in Paris.
M: Mary is in New York.
F: Fred is in Rome.

The premises of the argument are $J \rightarrow M$ and $J \wedge F$. The conclusion is M.

We commence our list with the premises:

1.	$J \rightarrow M$	(premise)
2.	$J \wedge F$	(premise)

Note that if the proposition J could be added to the list then we could add the conclusion by applying the modus ponens rule of inference to J and $J \rightarrow M$. Is there any justification for J to be included? Yes—we can apply the rule of simplification to the second premise $J \wedge F$. The following is the complete proof.

1.	$J \rightarrow M$	(premise)
2.	$J \wedge F$	(premise)
3.	J	(2. Simp)
4.	M	(1, 3. MP)

Note that after each proposition we have indicated the proposition or propositions from which it is derived and the rule which sanctions its derivation.

2. Provide a formal proof of the validity of the following argument.

If Mark is correct then unemployment will rise and if Ann is correct then there will be a hard winter. Ann is correct. Therefore unemployment will rise or there will be a hard winter or both.

Solution

We symbolise the component simple propositions as follows:

M: Mark is correct.
U: Unemployment will rise.
A: Ann is correct.
H: There will be a hard winter.

The premises of the argument are: $(M \rightarrow U) \wedge (A \rightarrow H)$ and A.
The conclusion is: $U \vee H$.

We commence the formal proof, as usual, with the premises.

1.	$(M \rightarrow U) \wedge (A \rightarrow H)$	(premise)
2.	A	(premise)

Note that we can add H to the list using modus ponens if we can first add $A \rightarrow H$. The conclusion then follows using the addition rule of inference (which allows us to deduce $H \vee U$ from H) followed by the commutation rule $p \vee q \equiv q \vee p$. We can add $A \rightarrow H$ if we first reverse the order of the conjuncts in the first premise. This is justified by the commutation rule for conjunction, $p \wedge q \equiv q \wedge p$. The complete proof is as follows.

1.	$(M \rightarrow U) \wedge (A \rightarrow H)$	(premise)
2.	A	(premise)
3.	$(A \rightarrow H) \wedge (M \rightarrow U)$	(1. Com)
4.	$A \rightarrow H$	(3. Simp)
5.	H	(2, 4. MP)
6.	$H \vee U$	(5. Add)
7.	$U \vee H$	(6. Comm)

For many arguments there are alternative formal proofs. The following is also a formal proof for the argument above.

1.	$(M \rightarrow U) \wedge (A \rightarrow H)$	(premise)
2.	A	(premise)
3.	$A \vee M$	(2. Add)
4.	$M \vee A$	(3. Com)
5.	$U \vee H$	(1, 4. CD)

3. Provide a formal proof of the validity of the following argument.

If he'd taken my advice or had his wits about him, he would have sold his house and moved to the country. If he'd sold his house, Jenny

would have bought it. Jenny didn't buy his house. Therefore he didn't take my advice.

Solution

We symbolise the simple propositions as follows:

A: He took my advice.
W: He had his wits about him.
H: He sold his house.
C: He moved to the country.
J: Jenny bought his house.

The argument has premises: $(A \vee W) \rightarrow (H \wedge C)$, $H \rightarrow J$ and $\overline{J}$. The conclusion is $\overline{A}$.

We commence the proof, as usual, with the premises.

1.	$(A \vee W) \rightarrow (H \wedge C)$	(premise)
2.	$H \rightarrow J$	(premise)
3.	$\overline{J}$	(premise)

The proof centres around the addition of $\overline{H \wedge C}$ to the list which allows us to deduce $\overline{A \vee W}$ using modus tollens. By De Morgan's law $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$ so that $\overline{A \vee W}$ and $\overline{A} \wedge \overline{W}$ are equivalent propositions. Having added $\overline{A} \wedge \overline{W}$ we apply simplification and deduce the conclusion $\overline{A}$. Below is the complete proof.

1.	$(A \vee W) \rightarrow (H \wedge C)$	(premise)
2.	$H \rightarrow J$	(premise)
3.	$\overline{J}$	(premise)
4.	$\overline{H}$	(2, 3. MT)
5.	$\overline{H} \vee \overline{C}$	(4. Add)
6.	$\overline{H \wedge C}$	(5. De M)
7.	$\overline{A \vee W}$	(1, 6. MT)
8.	$\overline{A} \wedge \overline{W}$	(7. De M)
9.	$\overline{A}$	(8. Simp)

4. Prove the validity of the following argument.

If he didn't get the job then he didn't become an lawyer. He didn't get the job and he took up golf. He became a lawyer or he didn't take up golf. Therefore he won the Ryder Cup.

Solution

As usual we commence by symbolising the component simple propositions.

J: He got the job.
L: He became a lawyer.
G: He took up golf.
R: He won the Ryder Cup.

The premises are $\overline{J} \rightarrow \overline{L}$, $\overline{J} \wedge G$, $L \vee \overline{G}$ and the conclusion is R.

At this stage (or earlier) we may be alerted to the fact that there is something suspect about this argument. The simple proposition which constitutes its conclusion is not a component of any premise. Presumably, if we can provide a formal proof of the validity of this argument then we could do so for any argument with the same premises, no matter what its conclusion.

A formal proof is in fact quite easy to construct.

1.	$\overline{J} \rightarrow \overline{L}$	(premise)
2.	$\overline{J} \wedge G$	(premise)
3.	$L \vee \overline{G}$	(premise)
4.	$\overline{J}$	(2. Simp)
5.	$\overline{L}$	(1, 4. MP)
6.	$\overline{G}$	(3, 5. DS)
7.	$G \wedge \overline{J}$	(2. Com)
8.	G	(7. Simp)
9.	$G \vee R$	(8. Add)
10.	R	(6, 9. DS)

We now have further cause to view this argument with suspicion. We have proved it to be valid but lines 6 and 8 indicate that the truth of the premises allows us to infer the truth of the proposition G and also that of its negation $\overline{G}$.

The reason for this is that the premises are inconsistent—it is not possible for all of them to be true simultaneously. This inconsistency surfaces in the formal proof by supporting the inference of a proposition together with its negation. Once this occurs, we can infer any proposition whatsoever. We simply apply the addition rule of inference

(as in line 9 above) followed by disjunctive syllogism (as in line 10). As we demonstrated in Section 2.5, an argument with inconsistent premises is always valid regardless of its conclusion.

Exercises 2.5

Provide formal proofs of the validity of each of the following arguments.

1. I shall either play golf or I shall stay at home and read. Therefore I shall either play golf or stay at home.

2. The moon's not a balloon only if I'm the Queen of Sheba. I'm not the Queen of Sheba. Therefore the moon's a balloon.

3. If the summer is hot then we won't go on holiday in August. We'll either go on holiday in August or we'll buy a new car (perhaps both). Therefore, if the summer is hot, we'll buy a new car.

4. If she drinks wine or eats cheese, she gets a terrible headache. She's drinking wine and eating chocolates. Therefore she'll get a terrible headache.

5. People are happy if and only if they are charitable. Nobody is both happy and charitable. Hence people are both unhappy and uncharitable.

6. If the battery is flat or the car's out of petrol then it won't start and I shall be late for work. Either the car's out of petrol or the battery is flat. Therefore I shall be late for work.

7. You will win the game if and only if you follow the rules. If you follow the rules then you are conventional. You are not conventional and you are always successful. If you are always successful then you will win the game. So you will win the game.

8. If roses are red and violets are blue then sugar is sweet and I love you. Violets are blue and roses are red. Therefore sugar is sweet.

9. Either the project wasn't a success or he didn't invest his inheritance or both. If he was sensible then he invested his inheritance. The project was a success. If he wasn't sensible and he didn't invest his inheritance, then he is ruined. Therefore he is ruined.

10. Peter is either brave or brainy and also he is either brainy or bald. Peter isn't brainy. Therefore he is brave and bald.

11. The murder was committed either by A or by both B and C. If A or B committed the murder then the victim was poisoned. Therefore either C committed the murder or the victim was poisoned.

12. If it is useful then I shall keep it and if it is valuable then I shall keep it. If it belonged to Ben then it is either useful or valuable. It belonged to Ben. So I shall keep it.

13. If it doesn't rain, then I'll go shopping. If I go shopping then, if I don't take an umbrella it'll rain. If I go by car then I won't take an umbrella. Hence it will rain or I won't go by car.

14. If ghosts are a reality then there are spirits roaming the Earth and if ghosts are not a reality then we do not fear the dark. Either we fear the dark or we have no imagination. We do have an imagination and ghosts are not a reality. Therefore there are spirits roaming the Earth.

2.7 The Method of Conditional Proof

We conclude this chapter by considering a method of formal proof which is particularly useful for establishing the validity of valid arguments which have a conclusion which can be expressed as a conditional proposition. Since (as we shall see later) many mathematical theorems can be expressed as conditionals, the 'method of conditional proof' as it is known, will be an important component of our theorem-proving toolkit.

To justify the method, consider an argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion $q \to r$. This argument form is valid if and only if $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to (q \to r)$ is a tautology. Now the exportation replacement rule states that $p \to (q \to r) \equiv (p \wedge q) \to r$ so that the validity condition

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to (q \to r) \text{ is a tautology}$$

can be replaced by

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n \wedge q) \to r \text{ is a tautology.}$$

However, this condition is equivalent to saying that the argument form with premises $p_1, p_2, \ldots, p_n, q$ and conclusion r is valid. Therefore, if

Theorem-proving toolkit

this argument form is valid then so is that with premises $p_1, p_2, \ldots, p_n$ and conclusion $q \rightarrow r$. Also, if the former argument form is invalid, then so is the latter.

This suggests a method of formal proof for establishing the validity of an argument with a conditional conclusion of the form $Q \rightarrow R$. We simply add the antecedent Q to the premises of the argument and construct a formal proof (as described in Section 2.6) which terminates with the consequent R. We can then add the conclusion of the argument $Q \rightarrow R$ to the list of propositions in the proof. We shall justify this step by referring to the **method of conditional proof**, abbreviated to CP. We illustrate the method in the examples below.

Examples 2.9

1. Prove the validity of the following argument using the method of conditional proof.

If we have a party then we'll invite Lana and Bob. If we invite Lana or Bob then we must invite Jake. Therefore if we have a party then we must invite Jake.

Solution

We symbolise the following simple propositions:

P: We have a party.
L: We'll invite Lana.
B: We'll invite Bob.
J: We must invite Jake.

The premises of the argument are: $P \rightarrow (L \wedge B)$ and $(L \vee B) \rightarrow J$ and the conclusion is the conditional $P \rightarrow J$.

We commence the proof as usual by listing the two premises. We then add the conclusion's antecedent, P, and treat this as a further premise, justifying this step by indicating that we are using the method of conditional proof (CP). We then aim to produce a formal proof terminating with J, the consequent of the conclusion. We are then justified in adding $P \rightarrow J$, the conclusion of the argument, to the proof. The full proof is given below.

1.	$P \rightarrow (L \wedge B)$	(premise)
2.	$(L \wedge B) \rightarrow J$	(premise)
3.	P	(CP)
4.	$L \wedge B$	(1, 3. MP)
5.	L	(4. Simp)
6.	$L \wedge B$	(5. Add)
7.	J	(2, 6. MP)
8.	$P \rightarrow J$	(3–7. CP)

Note that the conclusion $P \rightarrow J$ is justified by the sequence of propositions starting at line 3 where the antecedent was added to the list of premises and finishing at line 7 where we infer the consequent J.

2. Use the method of conditional proof to establish the validity of the following argument.

If we invite Lana then Jake will sulk, and if we invite Bob then Alice will leave. So if we invite Lana and Bob then Jake will sulk and Alice will leave.

Solution

We define the following simple propositions:

L: We invite Lana.
J: Jake will sulk.

B: We invite Bob.
A: Alice will leave.

The premise of the argument is: $(L \rightarrow J) \wedge (B \rightarrow A)$ and the conclusion is $(L \wedge B) \rightarrow (J \wedge A)$.

Having commenced the proof with the premise, we add the antecedent of the conclusion $L \wedge B$. Once we have inferred the consequent $J \wedge A$, we can then use the method of conditional proof to justify the addition of the conclusion $(L \wedge B) \rightarrow (J \wedge A)$. The full proof is as follows.

1.	$(L \rightarrow J) \wedge (B \rightarrow A)$	(premise)
2.	$L \wedge B$	(CP)
3.	$L \rightarrow J$	(1. Simp)
4.	$(B \rightarrow A) \wedge (L \rightarrow J)$	(1. Com)
5.	$B \rightarrow A$	(4. Simp)
6.	L	(2. Simp)
7.	J	(3, 6. MP)
8.	$B \wedge L$	(2. Com)
9.	B	(8. Simp)
10.	A	(5, 9. MP)
11.	$J \wedge A$	(7, 10. Conj)
12.	$(L \wedge B) \rightarrow (J \wedge A)$	(2–11. CP)

3. Using the method of conditional proof, provide a formal proof of the validity of the following argument.

If I don't go on holiday or I sell some shares then I'll buy a new car and save some money. Therefore I'll go on holiday or I'll buy a new car.

Solution

We symbolise the component simple propositions of the argument as follows:

H: I'll go on holiday.
S: I'll sell some shares.
C: I'll buy a new car.
M: I'll save some money.

The argument has premise $(\overline{H} \vee S) \rightarrow (C \wedge M)$ and conclusion $H \vee C$.

It is not obvious that the method of conditional proof can be applied to this argument since its conclusion is not a conditional. However, it is equivalent to the conditional $\overline{H} \rightarrow C$. The justification for this is:

$$\begin{aligned} p \vee q &\equiv \overline{\overline{p}} \vee q && \text{(DN)} \\ &\equiv \overline{p} \rightarrow q && \text{(Impl).} \end{aligned}$$

So, if we wish to, we may apply the method of conditional proof to infer $\overline{H} \rightarrow C$ and then apply the two appropriate replacement rules to obtain $H \vee C$. The full proof is given below.

1.	$(\overline{H} \vee S) \rightarrow (C \wedge M)$	(premise)
2.	$\overline{H}$	(CP)
3.	$\overline{H} \vee S$	(2. Add)
4.	$C \wedge M$	(1, 3. MP)
5.	C	(4. Simp)
6.	$\overline{H} \rightarrow C$	(2–5. CP)
7.	$\overline{\overline{H}} \vee C$	(6. Impl)
8.	$H \vee C$	(7. DN)

The method of conditional proof provides an alternative for constructing a formal proof for valid arguments with conclusions which can be expressed as conditionals. However, although its use will often result in a shorter proof for such arguments, this is not invariably the case and the method described in Section 2.6 may sometimes be preferable.

Exercises 2.6

Provide a formal proof of the validity of each of the following arguments using (a) the method of conditional proof and (b) the method of formal proof described in Section 2.6.

1. If you don't confront him then you're a coward. Therefore if you don't confront him then you're a coward or a fool.

2. If the Conservatives win the election then taxes will rise and there will be mass unemployment. If taxes rise and there is mass unemployment then I shall stand for parliament. I won't stand for parliament. Therefore if the Conservatives win the election then taxes will rise.

3. If you are happy then you are fortunate. So if you are happy then you are happy and fortunate.

4. If France or Brazil wins the World Cup then we'll drink champagne and dance all night. Hence if France wins the World Cup then we'll drink champagne.

5. Either you mow the lawn and clean the car or you'll get no pocket money. If you get no pocket money then you'll have to stay at home this evening. Therefore, either you clean the car or you'll have to stay at home this evening.

6. If Steve robbed the bank then he'll leave the country and we'll never see him again. If we see Steve again then he is not Al's friend. Therefore if Steve robbed the bank or he is Al's friend then we'll never see him again.

3 Predicate Logic

3.1 Introduction

There are certain types of argument which cannot be analysed using the techniques developed in Chapter 2. Consider, for instance: 'All athletes are physically fit. Dan is an athlete. Therefore Dan is physically fit.' Identifying the simple propositions of which the argument is composed gives:

A: All athletes are physically fit.
D: Dan is an athlete.
P: Dan is physically fit.

The argument has premises A and D and conclusion P. The underlying argument form therefore has propositional variables p and q as premises and another variable r as its conclusion. The argument is clearly valid. However, truth table analysis of the associated argument form would be of no use in proving this to be the case and, with this symbolisation of premises and conclusion, any attempt at a formal proof of validity would be equally unsuccessful.

The validity of the argument above rests on the fact that the first proposition states that all members of the class of individuals having the property of being athletes also possess the property of being physically fit. Therefore, from knowing that a particular individual (for example, Dan) belongs to the class of athletes, we may deduce that he or she is physically fit. The validity of the argument does not depend upon the structure of the premises and conclusion in the same way as the arguments considered in Chapter 2. What is important is the common content of its component simple propositions. The problem with our previous method of denoting simple propositions is that it provides

no means of showing that propositions refer to the same property. Two propositions as similar as 'Dan is an athlete' and 'Sheila is an athlete' must be denoted by, say, D and S. Our notation has no means of conveying the fact that both propositions refer to the property of 'being an athlete'.

A proposition of the form 'Dan is an athlete' may be viewed as having two components. One is an object or individual (in this case 'Dan') and the other is a property which that object or individual is said to possess. We refer to that property as a **predicate** so that the predicate in this example is 'is an athlete'. We shall denote objects and individuals using lower case letters—usually the first letter of the name of that object or individual. For example:

d: Dan.
s: Sheila.

Predicates are denoted using upper case letters:

A: is an athlete.
P: is physically fit.

The proposition 'Dan is an athlete' is then denoted by Ad. Note that the letter denoting the predicate is written to the left of that denoting the object or individual said to possess that particular attribute. Other examples of propositions involving the individuals 'Dan' and 'Sheila' and the predicates 'is an athlete' and 'is physically fit' are as follows:

As: Sheila is an athlete.
Pd: Dan is physically fit.
Ps: Sheila is physically fit.

Of course these propositions may be negated or conjoined using logical connectives to form compound propositions in the same way as described in Chapter 2. Hence we may have:

$\neg As$: Sheila is not an athlete.

(Note that we tend to use the symbol $\neg$ to negate propositions expressed in predicate form. The expression $\overline{As}$ is perfectly acceptable as the negation of As but $\neg$ tends to be more convenient for negating the notationally more complicated expressions which tend to occur in predicate logic.)

Examples of compound propositions are:

$As \wedge Ad$: Sheila is an athlete and Dan is an athlete (*or* Sheila and Dan are athletes).
$\neg Pd \rightarrow \neg Ad$: If Dan is not physically fit then he is not an athlete.

To form these propositions, we combined a predicate with the name of an object or individual. However, we may also form expressions such as:

Ax: x is an athlete.
Py: y is physically fit.

Here the letters x and y are variables. Each acts as a place-marker to indicate where the name of an object or individual may be substituted. Expressions such as Ax and Py are not propositions since they cannot be declared true or false. They are called **propositional functions**. A propositional function is converted to a proposition once a specific name is substituted for the variable. We have an analogous situation in such algebraic expressions as $2x > 7$. As it stands, this is neither true nor false and is not therefore a proposition. If we substitute 6 for the variable x, we obtain the (true) proposition $2 \times 6 > 7$.

Propositional functions can be negated in the same way as propositions so that $\neg Ax$ and $\neg Py$ denote the propositional functions 'x is not an athlete' and 'y is not physically fit' respectively. They can also be joined using logical connectives so that we can form such expressions as:

$Ax \wedge Py$: x is an athlete and y is physically fit.
$Ax \rightarrow Px$: If x is an athlete then x is physically fit.

Note that the first of these is a propositional function of the two variables x and y. We may therefore substitute the names of two different individuals in each of the component propositional functions Ax and Py. (We may also substitute the name of the same individual for x and y.) The second expression is a propositional function of the single variable x and the same individual must be substituted for x throughout the expression.

3.2 Quantification of Propositional Functions

For the argument at the beginning of the previous section, we can now symbolise the second premise 'Dan is an athlete' and the conclusion

'Dan is physically fit'. However, as yet, we have no means of symbolising the first premise 'All athletes are physically fit'. This proposition asserts that anyone who is an athlete has the property of being physically fit. We can therefore paraphrase it as follows: 'For all x, if x is an athlete then x is physically fit'. Using the notation defined in the previous section we denote 'x is an athlete' by Ax and 'x is physically fit' by Px. We denote 'for all x' (or 'for every x') by $\forall x$ and the proposition 'All athletes are physically fit' is denoted by $\forall x(Ax \rightarrow Px)$. The symbol $\forall$ is called the **universal quantifier**. Note that, since the expression $\forall x(Ax \rightarrow Px)$ can be declared true or false, it does denote a proposition even though it contains the variable x. The quantified variable $\forall x$ converts the propositional function $Ax \rightarrow Px$ into a proposition.

We shall also require a means of symbolising propositions such as 'Some athletes are physically fit'. This proposition asserts that there are certain individuals having the property of 'being an athlete' who also have the property of 'being physically fit'. We can therefore paraphrase this as follows: 'There exists at least one x such that x is an athlete and x is physically fit'. If we denote 'there exists at least one x' by $\exists x$, then the proposition may be symbolised by $\exists x(Ax \wedge Px)$. The symbol $\exists$ is called the **existential quantifier** and the quantified variable $\exists x$ converts the propositional function 'x is an athlete and x is physically fit' (denoted by $Ax \wedge Px$) to the proposition 'Some athletes are physically fit'.

Examples 3.1

Suppose that predicates and individuals are defined as follows:

S: should be shunned,
U: is prone to unruly behaviour,
P: is a friend of Peter's,
M: is a friend of mine,
a: Ann,
d: David.

Symbolise the following:

(i) Ann is a friend of Peter's and David is a friend of mine.
(ii) Some of Peter's friends are prone to unruly behaviour.
(iii) Anyone who is a friend of Peter's is not a friend of mine.

(iv) If Ann is a friend of Peter's then she is prone to unruly behaviour and should be shunned.

(v) Some of my friends are friends of Peter's and some of Peter's friends are prone to unruly behaviour.

(vi) If all Peter's friends are prone to unruly behaviour, then some of his friends should be shunned.

Solution

(i) This is the conjunction of the two simple propositions 'Ann is a friend of Peter's' and 'David is a friend of mine' which are denoted by Pa and Md respectively. The complete proposition is therefore symbolised by $Pa \wedge Md$.

(ii) This proposition may be paraphrased: 'There exists at least one x where x is a friend of Peter's and x is prone to unruly behaviour'. It is therefore symbolised using the existential quantifier thus: $\exists x(Px \wedge Ux)$.

(iii) This proposition states that 'For every x, if x is a friend of Peter's then x is not a friend of mine'. It can therefore be symbolised by $\forall x(Px \rightarrow \neg Mx)$.

(iv) This is a conditional proposition with antecedent 'Ann is a friend of Peter's' and consequent which is the conjunction of the two propositions 'Ann is prone to unruly behaviour' and 'Ann should be shunned'. We can therefore symbolise it thus: $Pa \rightarrow (Ua \wedge Sa)$.

(v) This is the conjunction of two propositions. The first conjunct is 'Some of my friends are friends of Peter's' which can be symbolised by $\exists x(Mx \wedge Px)$. The second conjunct is 'Some of Peter's friends are prone to unruly behaviour' symbolised by $\exists x(Px \wedge Ux)$. The complete proposition is therefore given by: $\exists x(Mx \wedge Px) \wedge \exists x(Px \wedge Ux)$.

Note that, although we use the same variable in each of the conjuncts, this does not necessarily mean that there is any individual that satisfies both of the properties $Mx \wedge Px$ and $Px \wedge Ux$. Each of the conjunctive components guarantees the existence of an individual with the given property but there is no implication that an individual c for which $Mc \wedge Pc$ is a true proposition is also such that $Pc \wedge Uc$ is a true proposition. For this reason, we could use different variables within each of the two conjuncts, e.g. $\exists x(Mx \wedge Px) \wedge \exists y(Py \wedge Uy)$.

(vi) This is a conditional proposition with antecedent 'All Peter's friends are prone to unruly behaviour' and consequent 'Some of Peter's

friends should be shunned'. The symbolisation is therefore:

$$\forall x(Px \rightarrow Ux) \rightarrow \exists x(Px \wedge Sx).$$

As with example (v) above, we may use different variables within the antecedent and consequent and write this as

$$\forall x(Px \rightarrow Ux) \rightarrow \exists y(Py \wedge Sy).$$

Universe of discourse

There are often situations where our discussion is restricted to a particular set of objects or individuals. For instance, in the propositional functions Ax (x is an athlete) and Px (x is physically fit) referred to in the sections above, it is understood that, when substituting for the variable x, we cannot choose the name of a fish or a piece of furniture. The domain of the variable x is restricted to people. Given a propositional function Fx, the **universe of discourse** for the variable x is defined to be the set from which we may select an object or individual to substitute for x. Often this universe is unstated when it is obvious from the nature of the propositional functions. However, defining a universe of discourse can often simplify the symbolisation of quantified propositional functions. For example, suppose we are concerned with investigating the validity of an argument wherein the premises and conclusion are propositions concerning attributes of athletes, such as: H: eats a healthy diet; T: trains daily. If we define the universe of discourse as 'athletes' then it can be assumed that any variables can be replaced only by specific athletes. In this case the proposition 'All athletes eat a healthy diet' can be symbolised by $\forall x\, Hx$ rather than by $\forall x(Ax \rightarrow Hx)$, since there is now no need to specify that 'x is an athlete'. The proposition $\forall x\, Hx$ simply says that all x's in the universe of discourse (i.e. athletes) eat healthy diets. Similarly, with the same universe defined, the proposition 'There are athletes who train daily and don't eat a healthy diet' can be symbolised $\exists x(Tx \wedge \neg Hx)$.

Whilst we are sometimes careless about defining the universe of discourse, it is important to realise that the truth value of a proposition may depend critically on this universe. For instance consider:

G: is greater than 0,
E: is even.

A proposition such as $\forall x\, Gx$ is true if the universe of discourse is the positive integers but it is false if the universe is the real numbers. Similarly $\exists x(Ex \wedge Gx)$ would be false in such universes as the negative integers or the odd integers but would be true if the universe were the real numbers or the integers. These examples serve to highlight the need to ensure that, for quantified propositional functions, there is no ambiguity concerning the underlying universe of discourse.

Negation of propositions involving quantifiers

At first glance the proposition 'No athletes are physically fit' might suggest the negation of $\forall x\, Px$ (where the universe of discourse is 'athletes'), i.e. $\neg\forall x\, Px$. However, recall that the negation of a proposition must be true in all circumstances that the proposition is false and false whenever that proposition is true. Therefore the negation of 'All athletes are physically fit' is not 'No athletes are physically fit' since a state of affairs where, for instance, just one athlete is not physically fit renders both propositions false. The negation of 'All athletes are physically fit' is 'There is at least one athlete who is not physically fit'. Hence the proposition which is equivalent to $\neg\forall x\, Px$ (in the sense that it makes the same statement) is $\exists x \neg Px$.

The negation of the existentially quantified proposition 'Some athletes are physically fit' is the proposition which states that it is not the case that some athletes are physically fit, i.e. 'No athletes are physically fit'. We can paraphrase this 'For every x in the universe, x is not physically fit' and symbolise it $\forall x \neg Px$. Hence $\neg\exists x\, Px$ is equivalent to $\forall x \neg Px$.

These two rules are known as **quantification denial** (abbreviated to QD) and are summarised below.

Rules of quantification denial (QD)

Suppose that a universe of discourse is defined for the variable x. Then, for any propositional function Fx:

$\neg\forall x\, Fx$ is equivalent to $\exists x \neg Fx$

and $\neg\exists x\, Fx$ is equivalent to $\forall x \neg Fx$.

Exercises 3.1

1. Assume that the replacement rules (see page 37) apply to propositional functions as well as to propositional forms. Use these and the quantification denial rules above to show that:

$\neg\forall x(Fx \rightarrow Gx)$ is equivalent to $\exists x(Fx \wedge \neg Gx)$

and $\neg\exists x(Fx \wedge Gx)$ is equivalent to $\forall x(Fx \rightarrow \neg Gx)$.

2. Suppose that the following predicates and individuals are defined:

p: Peter,
f: Peter's father,
P: lives in Peru,
D: drives a Mercedes,
C: is a company director.

Symbolise the following:

(i) Peter lives in Peru and his father drives a Mercedes.

(ii) If Peter drives a Mercedes then his father is a company director.

(iii) Peter lives in Peru or he drives a Mercedes and his father is not a company director.

(iv) Everyone who lives in Peru drives a Mercedes.

(v) Everyone who lives in Peru drives a Mercedes or is a company director.

(vi) No-one who isn't a company director drives a Mercedes.

(vii) Some people who live in Peru drive a Mercedes but are not company directors.

(viii) If no-one living in Peru drives a Mercedes then Peter doesn't live in Peru and his father is not a company director.

3. Suppose that the following predicates are defined on the universe of discourse 'people':

D: is dishonest,
S: values success,
T: is to be trusted,
C: cannot make decisions.

Express the following as idiomatic English sentences.

(i) $\forall x(Dx \rightarrow \neg Tx)$
(ii) $\exists x[(\neg Dx \vee \neg Cx) \wedge \neg Tx]$
(iii) $\forall x[Sx \rightarrow (\neg Dx \wedge Tx)]$
(iv) $[\forall x(Sx \rightarrow Dx)] \rightarrow (\exists x \neg Tx)$
(v) $[\exists x(Dx \wedge Sx)] \rightarrow (\neg \exists x\, Tx)$
(vi) $\forall x[Cx \rightarrow (Dx \vee \neg Tx)]$
(vii) $[\neg \forall x(Sx \rightarrow Tx)] \wedge [\exists x(Sx \wedge \neg Dx)]$
(viii) $\forall x([(Dx \vee \neg Tx) \wedge Cx] \rightarrow \neg Sx)$

4. Suppose that the following predicates are defined:

G: is greater than 15,
T: is an integer multiple of 3,
E: is a perfect square,
N: is an integer multiple of 9.

State the truth value of each of the following propositions for each of the following universes of discourse:

(a) the real numbers;
(b) the positive integers;
(c) the negative integers;
(d) integer multiples of 9 (i.e. $\ldots -18, -9, 0, 9, 18, \ldots$).

(i) $\forall x(Nx \rightarrow Gx)$
(ii) $\exists x(Gx \wedge \neg Ex)$
(iii) $\forall x(Nx \rightarrow Tx)$
(iv) $\forall x[Nx \rightarrow (Tx \wedge Gx)]$
(v) $\exists x\, Tx \rightarrow \exists x\, Nx$
(vi) $[\neg \exists x(Gx \wedge Tx)] \wedge (\neg \forall x\, Ex)$

3.3 Two-place Predicates

The predicate 'is an athlete' is an example of a **one-place predicate**. To convert a one-place predicate to a proposition requires the name of just one member of the universe of discourse or quantification over a single variable. There are predicates which require the names of more than one object or individual to convert them to propositions. Consider, for

example, 'is greater than'. To form a proposition from this predicate we need to supply the names of two items, one from each of two universes of discourse. If we define both universes to be the positive integers, then we can form such propositions as '3 is greater than 17' and '9 is greater than 9'. The predicate 'is greater than' is an example of a **two-place predicate**—it requires the names of two objects or individuals to convert it to a proposition. Two-place predicates are often referred to as 'relational predicates' because they express a relation between two components.

We symbolise propositions formed from two-place predicates in a similar way to the symbolisation of those using one-place predicates. For example, if we denote 'is frightened of' by F and define d and s as in Section 3.1, then Fds denotes 'Dan is frightened of Sheila'. Note that the order of the letters denoting the individuals is important. The proposition denoted by Fsd is 'Sheila is frightened of Dan' which is not the same proposition. There are predicates where reversing the order of these letters results in the same proposition. For example, if S denotes 'is the same age as', then Ssd and Sds are equivalent propositions in the sense that they always have the same truth value.

We can form propositional functions from two-place predicates in the same way as from one-place predicates. For example, if O denotes 'is older than', Oxy denotes the propositional function 'x is older than y'. Of course, a propositional function resulting from a two-place predicate will contain two variables, each with an underlying universe of discourse. These two universes may or may not be the same. To form a proposition, the name of an object or individual (chosen from the appropriate universe) may be substituted for each variable. Substituting for only one variable does not result in a proposition. For example, if Oxy denotes the propositional function defined above and t denotes 'Tom', the expression Oty denotes 'Tom is older than y'. This is a propositional function of the single variable y.

Two-variable propositional functions can be quantified. For instance, assuming a universe of discourse of people for both x and y, we can write $\forall x\, Oxy$. This denotes 'Everyone is older than y'. But note that this is not a proposition since it still contains the variable y. It is therefore a propositional function of y which can be converted to a proposition in the usual way, either by substituting for y or by further quantification. If we substitute t for y, we obtain the proposition 'Everyone is older than Tom' denoted by $\forall x\, Oxt$.

The conversion of a two-variable propositional function to a proposition by quantification requires the use of two quantifiers. For instance, $\forall x \forall y\, Oxy$ may be read as 'For all x and for all y, x is older than y'. Put into idiomatic English, this is equivalent to 'Everyone is older than everyone'. This is a proposition since it clearly has the truth value 'false'.

There are eight propositions which can be formed by quantifying a two-variable propositional function. For the propositional function Lxy 'x likes y' and a universe of 'people' for each variable, these are:

1. $\forall x \forall y\, Lxy$
2. $\forall y \forall x\, Lxy$
3. $\forall x \exists y\, Lxy$
4. $\exists y \forall x\, Lxy$
5. $\exists x \forall y\, Lxy$
6. $\forall y \exists x\, Lxy$
7. $\exists x \exists y\, Lxy$
8. $\exists y \exists x\, Lxy$

These denote the following propositions:

1. Everyone likes everyone.
2. For everyone, everyone likes them (*or* Everyone is liked by everyone).
3. Everyone likes someone.
4. There is someone who is liked by everyone.
5. There is someone who likes everyone.
6. For everyone, there is someone who likes them (*or* Everyone is liked by someone).
7. There is someone who likes someone.
8. There is someone who is liked by someone.

Clearly 1 and 2 denote equivalent propositions, as do 7 and 8. However, although 3 and 4 contain the same quantifiers attached to the same variable, the propositions are not equivalent. Proposition 3 claims that, for every individual in the universe, there is someone whom that individual likes. If this proposition is true then, if we select Tom from the universe, we shall find that he likes Jim for example (amongst others perhaps). Similarly, Jane likes Ben, etc. However, proposition 4 claims that there is one particularly popular individual whom everyone likes. If this is a true proposition, then we shall be able to identify one person (at least), denoted by a, say, such that $\forall x\, Lxa$ is a true proposition, i.e. every x in the universe likes individual a.

Propositions 5 and 6 are also not equivalent. If proposition 5 is true, then we shall be able to identify at least one generous spirited individual in the universe who likes everyone. Proposition 6, on the other hand, claims that everyone is liked by someone but, unlike 5, it does not propose that the 'someone' is the same individual for everyone in the universe.

Propositions formed from two-place predicates can, of course, be negated in the same way as any other proposition. For example, if we define:

Txy: x is taller than y,
a: Anne,
b: Brett,

then $\neg Tab$ denotes 'Anne is not taller than Brett'. Examples of the negation of quantified two-variable propositional functions are:

$\neg\forall x\forall y\, Txy$: It is not the case that everyone is taller than everyone.

$\forall x\neg\exists y\, Txy$: For all x, there does not exist a y such that x is taller than y (i.e. every individual is not taller than any other individual).

$\exists y\neg\forall x\, Txy$: There is a y such that not everyone is taller than y (i.e. there is an individual such that not everyone is taller than that individual).

We can use logical connectives between propositions and propositional functions formed from two-place predicates. The following examples show how we symbolise more complex propositions using connectives, quantifiers and one- and two-place predicates.

Examples 3.2

1. We define the following:

Bxy:	x belongs to y	a: Anna
Dxy:	x detests y	b: Barry
Cx:	x is a cat	c: Charlie
Fx:	x is ferocious	
Px:	x is a person	

Write the propositions symbolised below as idiomatic English sentences.

(i) $Cb \wedge Fb \wedge Bbc$
(ii) $\forall x(Cx \rightarrow Dax)$
(iii) $\exists x(Cx \wedge Fx \wedge Bxc)$
(iv) $\forall x \forall y[(Cx \wedge Fx) \rightarrow (Py \rightarrow Dyx)]$
(v) $\forall x[Cx \rightarrow \exists y(Py \wedge Bxy)]$
(vi) $\forall x \exists y[Cx \rightarrow (Py \wedge Bxy)]$
(vii) $\exists x \forall y(Cx \wedge Fx \wedge Py \wedge Dyx)$
(viii) $\neg \exists x(Cx \wedge Bxa) \wedge \forall x(Fx \rightarrow Dax)$

Solution

(i) This is the conjunction of the three propositions 'Barry is a cat', 'Barry is ferocious' and 'Barry belongs to Charlie'. We can express this thus: 'Barry is a ferocious cat who belongs to Charlie'.

(ii) The 'literal' translation of this proposition is 'For all x, if x is a cat, then Anna detests x'. The idiomatic version would be 'Anna detests (all) cats'.

(iii) This proposition states that there exists an x which has all the three properties 'is a cat', 'is ferocious' and 'belongs to Charlie'. The proposition symbolised is therefore 'There is a ferocious cat which belongs to Charlie' or 'Charlie has a ferocious cat'.

(iv) Literally: 'For all x and for all y, if x is a cat and x is ferocious then, if y is a person, then y detests x'. Idiomatically: 'Everyone detests (all) ferocious cats'.

(v) Literally: 'For all x, if x is a cat then there is a y such that y is a person and x belongs to y'. Idiomatically: 'Every cat belongs to someone'.

(vi) This is an alternative way of writing proposition (v). Note that the existential quantifier applies to y and therefore has no effect on the propositional function Cx. It governs the propositional function $Py \wedge Bxy$ and must therefore be written before this expression although not necessarily immediately before it.

(vii) Literally: 'There exists an x for all y such that x is a cat, x is ferocious, y is a person and y detests x'. Idiomatically: 'There is

a ferocious cat which everyone detests'. Note that with the order of the quantified variables reversed (i.e. $\forall y \exists x (Cx \wedge Fx \wedge Py \wedge Dyx)$) the proposition would be 'For everyone, there is a ferocious cat which he or she detests'. The difference between these two is that the first claims that everyone detests one particular ferocious cat whilst the second allows the detested cat to be a different one for each person.

(viii) This is the conjunction of the two propositions 'There does not exist a cat which belongs to Anna' and 'Anna detests all ferocious things'. It can therefore be expressed as 'No cat belongs to Anna and Anna detests anything which is ferocious'.

2. We define the following where the universe of discourse for each variable is 'people':

Mxy: x is married to y,
Fxy: x is a friend of y,
Yxy: x is younger than y,
p: Paul,
e: Esra.

Symbolise the following:

(i) Paul is married to Esra.
(ii) Esra is everyone's friend.
(iii) There is someone who is everyone's friend.
(iv) Everyone has a friend.
(v) Everyone has a friend who is younger than themselves.
(vi) Paul is unmarried and has no friends.
(vii) Everyone who is married has a friend.
(viii) Everyone who is married is married to someone who is their friend.
(ix) No-one who is younger than Esra is married.

Solution

(i) To form this proposition we simply substitute 'Paul' for x and 'Esra' for y in the propositional function 'x is married to y'. This is symbolised Mpe.

(ii) Fey symbolises the propositional function 'Esra is a friend of y'. The proposition given states that, for any individual y, Esra is y's friend. It is therefore symbolised $\forall y\, Fey$.

(iii) This proposition is the same as that in (ii) but with 'Esra' replaced by an unspecified individual. It may be paraphrased 'There exists an x such that, for all y, x is the friend of y' and is symbolised $\exists x \forall y\, Fxy$.

(iv) Note that proposition (iii) claims that there is one particularly popular individual whom everyone has as their friend. Proposition (iv) similarly states that everyone has a friend but, unlike (iii), it does not state that this friend is the same individual for every person. It can be paraphrased 'For every x there exists a y such that y is a friend of x'. It can therefore be symbolised $\forall x \exists y\, Fyx$ (or $\forall y \exists x\, Fxy$).

(v) This proposition, like proposition (iv), states that everyone has a friend but further qualifies the friend as being younger. A possible paraphrase is 'For every x there exists a y such that y is a friend of x and y is younger than x'. We symbolise this $\forall x \exists y (Fyx \wedge Yyx)$ (or $\forall y \exists x (Fxy \wedge Yxy)$).

(vi) This proposition states that there does not exist an individual to whom Paul is married and also that there does not exist an individual who is a friend of Paul's. This is symbolised $\neg \exists x\, Mpx \wedge \neg \exists x\, Fxp$. We could, of course, use different variables in each of the propositional functions. (However, note that the following is *not* a correct symbolisation of the proposition: $\neg \exists x (Mpx \wedge Fxp)$. This proposition states that there does not exist an individual who is both married to Paul and also a friend of Paul.)

(vii) The first stage might be to paraphrase this 'For every x, if x is married then x has a friend'. The phrase 'x is married' can be symbolised by $\exists y\, Mxy$ and 'x has a friend' by $\exists y\, Fyx$. The complete proposition can therefore be written: $\forall x (\exists y\, Mxy \rightarrow \exists y\, Fyx)$. Note that the use of the same variable in each of the two quantified parts of the conditional does not imply that the spouse and the friend are the same individual. We could, if we liked, use different variables and symbolise the proposition: $\forall x (\exists y\, Mxy \rightarrow \exists z\, Fzx)$.

(viii) Like proposition (vii) this states that everyone who is married has a friend but goes further to claim that the spouse and the friend are one and the same individual. A paraphrase is 'For all x, if there is a y such that x is married to y then y is a friend of x'. In symbols this is: $\forall x \forall y (Mxy \rightarrow Fyx)$.

(ix) This states that, for all x, if x is younger than Esra, then there is no-one to whom x is married. In symbols: $\forall x (Yxe \rightarrow \neg \exists y\, Mxy)$.

Exercises 3.2

1. The following propositional functions are defined. The universe of discourse for x is 'students' and for y it is 'courses'.

Txy: x takes y,
Exy: x enjoys y,
Pxy: x passes y.

We also define:

c: Carl,
s: statistics.

Symbolise the following:

(i) Carl passes every course that he takes.

(ii) Every student who takes statistics enjoys it.

(iii) Some students who take statistics do not pass.

(iv) There are students who take courses which they do not enjoy.

(v) There are students who pass every course that they take.

(vi) If Carl passes statistics then any student who takes statistics passes.

(vii) If all students take courses which they don't enjoy then no student passes any course.

If the propositional functions are defined as above but the universes of discourse for x and y are not defined, symbolise each of the propositions (i)-(vii) using two further propositional functions:

Sx: x is a student,
Cx: x is a course.

2. The following propositional functions are defined:

Sx: x is a sports car,
Mx: x is a motorcycle,
Exy: x is more expensive than y,
Fxy: x is more economical than y,
Lxy: x is slower than y.

Write the following as idiomatic English sentences.

(i) $\neg\exists x(Sx \wedge Mx)$
(ii) $\forall x\forall y(Exy \rightarrow Lyx)$
(iii) $\forall x\forall y[(Mx \wedge Sy) \rightarrow Fxy]$
(iv) $\forall x[Sx \rightarrow \exists y(My \wedge Exy)]$
(v) $\exists x\forall y(Sx \wedge My \wedge Lxy)$

3. Symbolise each of the following defining carefully all predicates. The universe of discourse for each variable is 'people'.

(i) People who are rich are not always happy.
(ii) Someone shouted and everyone clapped and sang.
(iii) Everyone who went to the auction bought something.
(iv) No-one likes people who are rude.
(v) No-one spends all their time working.
(vi) Some people never give anything to anyone.
(vii) Everyone applauds someone who is courageous.
(viii) He who respects no-one has no friends.

3.4 Validation of Arguments in Predicate Logic

Having considered how we symbolise propositions using the notation of predicate logic, we now look at how we might establish the validity of arguments whose premises and conclusion are expressed in this notation. The important difference between these arguments and those considered in the last chapter is that some or all of the propositions of which they are composed may be quantified propositional functions. The problem with constructing formal proofs of the validity of such arguments is that our rules of inference and substitution rules are of very limited use when applied to propositions containing quantifiers because they allow us to manipulate only complete quantified propositions. What we need therefore are some rules which will enable us to obtain propositions without quantifiers whose truth follows from true quantified propositional functions. There are two such rules. The first applies to universally quantified propositional functions and is referred to as the 'rule of universal instantiation'. The second, called the 'rule of existential instantiation' applies to existentially quantified propositional functions.

Rule of universal instantiation (UI)

Given any propositional function Fx, from the truth of $\forall x\, Fx$, we can infer the truth of Fa for any individual a in the universe of discourse.

Rule of existential instantiation (EI)

Given any propositional function Fx, from the truth of $\exists x\, Fx$, we can infer that there is at least one individual a in the universe of discourse for which Fa is true.

It is important to appreciate the difference between these two rules. Suppose that we have propositional functions defined as follows on the universe of 'people':

Sx: x is a student,
Tx: x is over twenty-one.

Suppose that t denotes 'Tom', a particular member of the universe of discourse. From the truth of 'Everyone is a student' (denoted by $\forall x\, Sx$), we can certainly deduce that St (i.e. 'Tom is a student') denotes a true proposition. However, given that 'Someone is over twenty-one', we cannot infer that Tom falls into that category. Hence the truth of Tt does not follow from the truth of $\exists x\, Tx$. All that the latter proposition guarantees is that there is a subset of the universe containing at least one individual a for which Ta is true. However, the subset may or may not contain 'Tom'.

The two instantiation rules allow us to deduce true propositions, free of quantifiers, from premises which are in the form of quantified propositional functions. We also need rules which will allow us to deduce the truth of a conclusion containing a quantifier. Again there are two rules, one for each type of quantifier.

Rule of universal generalisation (UG)

If the proposition Fa is true for any arbitrary member a of the universe of discourse, then $\forall x\, Fx$ is true.

Rule of existential generalisation (EG)

If Fa is true for some particular individual a in the universe of discourse, then $\exists x\, Fx$ is true.

The word 'arbitrary' in the rule of universal generalisation may require some clarification. An arbitrary member of the universe of discourse is one having no special attributes to distinguish it from any other member, i.e. its only assumed attributes are those shared by all members of the universe. The rule UG states that, if Fa is true for an arbitrarily selected individual, then it must be true for every member of the universe.

These four rules of inference allow us to infer true propositions without quantifiers from true quantified propositional functions and *vice versa*. We summarise this below.

$\forall x\, Fx$ $\underset{\text{UG}}{\overset{\text{UI}}{\rightleftharpoons}}$ Fa where a is an arbitrary member of the universe

$\exists x\, Fx$ $\underset{\text{EG}}{\overset{\text{EI}}{\rightleftharpoons}}$ Fa where a is an particular member of the universe

Adding these four extra rules gives us all the tools necessary to validate arguments expressed in predicate notation. We first use the instantiation rules to move from quantified premises to unquantified propositions. We then apply rules of inference and substitution rules to these to infer other propositions in the chain which leads towards the argument's conclusion. If the conclusion is a quantified propositional function then we can apply the appropriate rule of generalisation to obtain it from the final proposition in the chain. We demonstrate this in the examples below.

Examples 3.3

1. Prove the validity of the following argument:

All athletes are physically fit. Dan is an athlete. Therefore Dan is physically fit.

Solution

We denote the following propositional functions:

Ax: x is an athlete,
Px: x is physically fit,

and also

d: Dan.

The premises are $\forall x(Ax \rightarrow Px)$ and Ad. The conclusion is Pd. We commence our formal proof, as usual, with the premises.

1.	$\forall x(Ax \rightarrow Px)$	(premise)
2.	Ad	(premise)

From the premise $\forall x(Ax \rightarrow Px)$ we can infer (by applying universal instantiation) the proposition $Ad \rightarrow Pd$. The universal quantifier guarantees that we can substitute any member of the universe for x and obtain a true proposition. We now have:

1.	$\forall x(Ax \rightarrow Px)$	(premise)
2.	Ad	(premise)
3.	$Ad \rightarrow Pd$	(1. UI)

By applying modus ponens to 2 and 3 we obtain the conclusion. The full proof is therefore:

1.	$\forall x(Ax \rightarrow Px)$	(premise)
2.	Ad	(premise)
3.	$Ad \rightarrow Pd$	(1. UI)
4.	Pd	(2, 3. MP)

2. Construct a formal proof of the validity of the following argument:

All elephants are mammals. Some elephants are playful. Therefore some mammals are playful.

Solution

We define the following:

Ex: x is an elephant
Mx: x is a mammal
Px: x is playful

The argument has premises $\forall x(Ex \rightarrow Mx)$, $\exists x(Ex \wedge Px)$ and conclusion $\exists x(Px \wedge Mx)$. Now we can apply universal instantiation to the first premise and existential instantiation to the second but we must be careful. If we apply UI first we obtain $Ea \rightarrow Ma$ where a is an arbitrary member of the universe. However, we cannot assume that this particular individual a is also one for which $Ea \wedge Pa$ is a true proposition. The premise $\exists x(Ex \wedge Px)$ guarantees that there *is* at least one member of the universe having both the properties 'is an elephant' and 'is playful' but we cannot assume that a falls into this category.

We get around this problem by applying EI first. The premise $\exists x(Ex \wedge Px)$ allows us to infer $Ea \wedge Pa$ for some member a of the universe. The premise $\forall x(Ex \rightarrow Mx)$ implies that we can substitute any individual for the variable in $Ex \rightarrow Mx$ and obtain a true proposition. In particular we can substitute a and obtain $Ea \rightarrow Ma$. However, we must remember that a is not an arbitrary individual but is a member of the subset of the universe defined as 'playful elephants'.

The first four steps in the proof are as follows:

1.	$\forall x(Ex \rightarrow Mx)$	(premise)
2.	$\exists x(Ex \wedge Px)$	(premise)
3.	$Ea \wedge Pa$	(2. EI)
4.	$Ea \rightarrow Ma$	(1. UI)

Note that, if we can obtain $Pa \wedge Ma$, we can infer the conclusion by applying EG. The full proof is the following:

1.	$\forall x(Ex \rightarrow Mx)$	(premise)
2.	$\exists x(Ex \wedge Px)$	(premise)
3.	$Ea \wedge Pa$	(2. EI)
4.	$Ea \rightarrow Ma$	(1. UI)
5.	$Pa \wedge Ea$	(3. Com)
6.	Pa	(5. Simp)
7.	Ea	(3. Simp)
8.	Ma	(4, 7. MP)
9.	$Pa \wedge Ma$	(6, 8. Conj)
10.	$\exists x(Px \wedge Mx)$	(9. EG)

(Note that, because a is not an arbitrary member of the universe, we could not apply UG to $Pa \wedge Ma$ and infer $\forall x(Px \wedge Mx)$.)

3. Provide a formal proof of the validity of the following argument:

Everything is expensive or bad for you. Not everything is bad for you. Therefore there are some things which are expensive and not bad for you.

Solution

We define the following:

Ex: x is expensive,
Bx: x is bad for you.

As always, the proof commences with the premises:

1.	$\forall x(Ex \vee Bx)$	(premise)
2.	$\neg\forall x\, Bx$	(premise)

Note that the rule UI does not give us a means of inferring a quantifier-free proposition from the negation of a quantified propositional function such as 2. However, we can use the quantification denial rules (see page 69) to convert $\neg\forall x\, Bx$ to $\exists x\neg Bx$. We can then apply EI to obtain $\neg Ba$ for some a in the universe.

Note that, as in the last example, we must apply EI to $\exists x\neg Bx$ before we apply UI to the first premise. To obtain the conclusion, $\exists x(Ex \wedge \neg Bx)$, we derive $Ea \wedge \neg Ba$ and apply EG. The full proof is given below.

1.	$\forall x(Ex \vee Bx)$	(premise)
2.	$\neg\forall x\, Bx$	(premise)
3.	$\exists x\neg Bx$	(2. QD)
4.	$\neg Ba$	(3. EI)
5.	$Ea \vee Ba$	(1. UI)
6.	$Ba \vee Ea$	(5. Com)
7.	Ea	(6, 4. DS)
8.	$Ea \wedge \neg Ba$	(7, 4. Conj)
9.	$\exists x(Ex \wedge \neg Bx)$	(8. EG)

4. Prove the validity of the following:

Everyone is paid monthly or they work part-time. Everyone works a two-day week or they don't work part-time. Therefore everyone who isn't paid monthly works a two-day week.

Solution

We define the following propositional functions on the universe of 'people':

Mx: x is paid monthly,
Px: x works part-time,
Tx: x works a two-day week.

The premises are $\forall x(Mx \vee Px)$ and $\forall x(Tx \vee \neg Px)$. We apply UI to each of these to obtain $Ma \vee Pa$ and $Ta \vee \neg Pa$. Note that the 'a' in each of these refers to the same individual and furthermore, this individual is an arbitrary member of the universe. This means that we can apply UG to any proposition containing only a. In particular, we can apply UG to $\neg Ma \rightarrow Ta$ to obtain the conclusion $\forall x(\neg Mx \rightarrow Tx)$. The proof is as follows:

1.	$\forall x(Mx \vee Px)$	(premise)
2.	$\forall x(Tx \vee \neg Px)$	(premise)
3.	$Ma \vee Pa$	(1. UI)
4.	$Ta \vee \neg Pa$	(2. UI)
5.	$\neg\neg Ma \vee Pa$	(3. DN)
6.	$\neg Ma \rightarrow Pa$	(5. Impl)
7.	$\neg Ta \rightarrow \neg Pa$	(4. Impl)
8.	$\neg\neg Pa \rightarrow \neg\neg Ta$	(7. Trans)
9.	$Pa \rightarrow Ta$	(8. DN)
10.	$\neg Ma \rightarrow Ta$	(6, 9. HS)
11.	$\forall x(\neg Mx \rightarrow Tx)$	(10. UG)

5. Prove the validity of the following argument:

Every student who attends class and takes the examination has enrolled for the course. No student who has enrolled for the course has taken the examination. There are students who attend class. Therefore there are students who have not taken the examination.

Solution

We define the following propositional functions on the universe of 'students':

Cx: x attends class,
Tx: x takes the examination,
Ex: x has enrolled for the course.

The proof commences with the premises followed by the application of EI and then UI. We obtain $\neg Ta$ to which we apply EG to obtain the conclusion $\exists x \neg Tx$. The full proof is given below.

1.	$\forall x[(Cx \wedge Tx) \rightarrow Ex)]$	(premise)
2.	$\neg\exists x(Ex \wedge Tx)$	(premise)
3.	$\exists x\, Cx$	(premise)
4.	$\forall x \neg(Ex \wedge Tx)$	(2. QD)
5.	Ca	(3. EI)
6.	$(Ca \wedge Ta) \rightarrow Ea$	(1. UI)
7.	$Ca \rightarrow (Ta \rightarrow Ea)$	(6. Exp)
8.	$Ta \rightarrow Ea$	(7, 5. MP)
9.	$\neg(Ea \wedge Ta)$	(4. UI)
10.	$\neg Ea \vee \neg Ta$	(9. De M)
11.	$Ea \rightarrow \neg Ta$	(10. Impl)
12.	$Ta \rightarrow \neg Ta$	(8, 11. HS)
13.	$\neg Ta \vee \neg Ta$	(12. Impl)
14.	$\neg Ta$	(13. Taut)
15.	$\exists x \neg Tx$	(14. EG)

6. Prove that the following is a valid argument.

Everyone who lives in London or New York is urbane and intellectual. Therefore every one who lives in New York is urbane.

Solution

We define the following propositional functions:

Lx: x lives in London,
Nx: x lives in New York,
Ux: x is urbane,
Ix: x is intellectual.

The argument has premise $\forall x[(Lx \vee Nx) \rightarrow (Ux \wedge Ix)]$ and conclusion $\forall x(Nx \rightarrow Ux)$. Having applied UI to the premise, we must prove $Na \rightarrow Ua$. For this we use the method of conditional proof (see Section 2.7). We add Na to our list of propositions and deduce Ua. We can then deduce $Na \rightarrow Ua$ to which we apply UG and obtain the conclusion of the argument.

1.	$\forall x[(Lx \vee Nx) \rightarrow (Ux \wedge Ix)]$	(premise)
2.	$(La \vee Na) \rightarrow (Ua \wedge Ia)$	(1. UI)
3.	Na	(CP)
4.	$Na \vee La$	(3. Add)
5.	$La \vee Na$	(4. Com)
6.	$Ua \wedge Ia$	(2, 5. MP)
7.	Ua	(6. Simp)
8.	$Na \rightarrow Ua$	(3–7. CP)
9.	$\forall x(Nx \rightarrow Ux)$	(8. UG)

Exercises 3.3

Provide a formal proof of the validity of each of the following arguments.

1. Some people are good-looking and rich. Everyone who is rich is dishonest. Therefore there are people who are good-looking and dishonest.

2. Some people are good-looking and rich. Everyone who is rich is dishonest. Therefore not everyone who is good-looking is honest.

3. All even numbers are rational and are divisible by two. Some even numbers are divisible by four. Hence some numbers are divisible by two and by four.

4. All numbers which are integers are even or odd. All numbers which are integers are even or non-zero. Some numbers are integers. Therefore there are numbers which are either even or they are odd and non-zero.

5. All animals with feathers are not aquatic. There are aquatic animals which live in the sea. So there are animals which live in the sea and don't have feathers.

6. Some functions are continuous and differentiable. All functions which are continuous are defined for all values of x. Therefore some functions which are defined for all values of x are differentiable.

7. Everyone who is a doctor or a lawyer commands the respect of the community and earns a high salary. Hence everyone who is a lawyer commands the respect of the community.

8. Everything which is enjoyable and cheap is harmful to one's health. All holidays are enjoyable. There are holidays which are not harmful to one's health. Therefore some things are not cheap.

9. There are no polynomials which are not differentiable functions. All differentiable functions are continuous. Therefore all polynomials are continuous.

4 Axiom Systems and Formal Proof

4.1 Introduction

In Chapter 1 we emphasised that mathematical 'facts' are obtained by a process of deductive reasoning and in Chapters 2 and 3 we developed the laws and principles of deductive reasoning. We are now equipped with the basic 'toolkit' for a rigorous study of mathematics and we can turn our attention in this direction.

Our task in this chapter will be to attempt to say something about what mathematics actually is and how it develops. This is potentially a hazardous task as there is no universally held view of the nature of mathematics. However, it is not our aim to venture into controversial philosophical territory. Rather, it is to explore enough of the formal aspects of mathematics to gain a clear understanding of what mathematical theorems and proofs actually are. In doing so, we shall give a somewhat formal description of mathematics. This is not because we are formalists. Rather it is because a formal description of mathematical proof provides a useful framework for the subsequent chapters where we shall look more closely at different methods of proof.

Of course, most mathematicians do not write formal proofs. It could be argued persuasively that mathematical proofs are just convincing arguments, i.e. in practice a proof is simply an argument which will convince a fellow mathematician of the truth of the particular result. However, a proof is a convincing argument *of a particular kind and with a definite structure.* In order to understand what is and is not an acceptable mathematical proof, it is useful to have a formal notion of proof as a point of reference.

4.2 Case Study of a Proof

In much of this chapter, we will be considering theorems and proofs from a general standpoint. To help motivate our discussion, this section is devoted to an informal look at a particular theorem from elementary number theory together with a proof. Some of the points raised here will be picked up in the more general context later in the chapter.

There is, of course, a logical difficulty with doing this. We are putting the cart before the horse! So far, we have not said what is meant by the terms 'theorem' and 'proof', so to present a particular theorem and proof is somewhat problematic. However, it is probably safe to assume that our readers have at least an intuitive understanding of what is meant by 'theorem' and 'proof'. For the purposes of this section, it is sufficient to regard a theorem as a proposition (as defined in Chapter 2) and its proof as a correct step-by-step argument which will convince a reader with the relevant mathematical background of the truth of the theorem. One of our main aims in this chapter is to give more rigorous definitions of theorem and proof. At times our discussion will be rather abstract, so a particular example to refer to may be helpful.

The theorem says that every integer greater than 1 can be factored into prime numbers, and is part of the so-called 'Fundamental Theorem of Arithmetic'. The full fundamental theorem goes on to state that the factorisation for a given integer is unique apart from the ordering of the prime factors. However, the proof of the uniqueness part is more sophisticated and can wait until later (see Chapter 7).

The Prime Factorisation Theorem: *Every integer greater than* 1 *can be expressed as a product of prime numbers.*

Before embarking on a proof of the theorem, we need to understand precisely what a prime number is. A simple definition is that a **prime number** is an integer greater than 1 which is not divisible by any positive integer except 1 and itself. Thus 5 is a prime number since it is not divisible by any positive integer except 1 and 5, whereas 6 is not a prime number since it is divisible by 2, for instance, which is different from both 1 and 6 itself. (Notice that according to the definition, 1 is not a prime number.)

Now we understand the term 'prime number' (and, presumably, other terms such as 'integer', 'product', 'divisible', etc.), we could embark

on a search for a proof of the theorem. It is usually best though to ensure that we first understand thoroughly what the theorem is really saying. Often the most effective way of achieving this is to look at some examples.

Consider the integer 24. We can write $24 = 2 \times 12$, which expresses 24 as the product of a prime number (2) and a non-prime number (12). Since 12 is not prime, we can now look for its factors. We continue in this way as follows:

$$\begin{aligned} 24 &= 2 \times 12 \\ &= 2 \times 3 \times 4 \\ &= 2 \times 3 \times 2 \times 2. \end{aligned}$$

We have now expressed 24 as a product of prime numbers: $2 \times 3 \times 2 \times 2$. Of course, there are other such expressions, for example $2 \times 2 \times 2 \times 3$, but this just contains the same prime numbers written in a different order. Carrying out this process on 1234 567 890, for example, takes rather longer but eventually produce the expression:

$$1234\,567\,890 = 2 \times 3 \times 3 \times 5 \times 3607 \times 3803.$$

The theorem says that we can obtain such an expression for any integer bigger than 1.

Now that we have some intuitive 'feel' for the theorem, we can begin the search for a proof. In fact, the basis of the proof is already contained in the example above. There, we rather laboriously found the prime factors of 24 by first finding two factors (2 and 12) and then finding factors of these where possible, and so on. Since this process can be applied to any integer greater than 1, we can construct a proof of the general result. (A shorter, more sophisticated proof of this result will be given later—see Chapter 9.)

An informal proof

Let n be any integer greater than 1. If n is prime then there is nothing to prove as n itself is already expressed as a 'product' of primes, albeit in a rather trivial way.

If n is not prime then there exist factors n_1 and n_2 each greater than 1 such that

$$n = n_1 \times n_2.$$

Now consider n_1 and n_2 in turn. If n_1 is composite (that is, not prime) then it can be expressed as a product of two integers each greater than 1, say $n_1 = m_1 \times m_2$. Similarly, either n_2 is prime or it can be expressed as a product $n_2 = m_3 \times m_4$ where m_3 and m_4 are greater than 1. At this stage we have expressed n in one of the following four ways:

$n = n_1 \times n_2$ (if both n_1 and n_2 are prime),

$n = m_1 \times m_2 \times n_2$ (if n_1 is composite and n_2 is prime),

$n = n_1 \times m_3 \times m_4$ (if n_1 is prime and n_2 is composite),

$n = m_1 \times m_2 \times m_3 \times m_4$ (if n_1 and n_2 are both composite).

Next consider each m_i in turn and continue the process. At every step in the process, each factor is either prime or is split into two smaller factors. Therefore this 'subdivision' process must eventually stop. When the process stops, the result is an expression of the form

$$n = p_1 \times p_2 \times \cdots \times p_k$$

where each p_i is prime. Therefore we have shown that n can be expressed as a product of primes.

□

Our treatment of this theorem and its proof is more detailed than is usual for a mathematics text. There are several reasons for this. One is our desire to give some indication at least of how the proof might be discovered, rather than just presenting the proof itself. If we are to learn how to construct proofs, it is clearly desirable to gain some insight into how a proof evolves from underlying ideas. It will not be sufficient just to study completed proofs. Another reason is to indicate the importance of precisely defined terms, such as 'prime number'.

Perhaps the most important lesson to learn from this example is that any mathematical proof is an exercise in communication. A correct but incomprehensible proof is of little use to anyone (and we hope ours does not fall into that category). In writing proofs, clarity and comprehensibility, as well as correctness, are important goals. In the next two sections, we develop a formal description of mathematical proof which tends to underplay these more human aspects of clarity and comprehensibility. Ultimately, we must not lose sight of these goals, and we shall return to them in later chapters.

4.3 Axiom Systems

To understand properly what mathematicians mean by proof, we first need to look a little more closely at the nature of mathematics itself. From a formal standpoint, mathematics operates according to something known as the 'axiomatic method'. This was first introduced by Euclid over two thousand years ago and has subsequently evolved, particularly during the last one hundred and fifty years, into the current *modus operandi* of mathematics. It is the purpose of this section to give a brief, if somewhat incomplete, description of the axiomatic method which governs the development of any mathematical theory.

In outline, a branch of mathematics starts with a set of premises and proceeds by making deductions from these assumptions using the methods of logic described in the previous two chapters. The premises are called 'axioms', the statements deduced from them are the theorems and the sequences of deductions themselves are the proofs of the theorems. In the rest of this section and the next, we shall expand upon and make more precise this overview of the formal description of the mathematics. Now, mathematics is of course a discipline engaged in by human beings and in practice it does not develop in quite such a precise and orderly manner as we have indicated. In the last section of this chapter (and, indeed, in the remaining chapters), we shall consider in more detail how mathematicians really go about exploring their mathematical landscapes.

To state and understand any proposition, whether in mathematics or elsewhere, we need to know two things. The first is the basic rules of the language in which the proposition is stated, i.e. the rules for constructing sentences in the language. These rules are the **syntax** of the language. Secondly, we must be able to give meanings to the words (and, in the case of mathematics, the symbols) employed. This is the **semantics** of the language. For example, the sequence of words *'incomprehensible we is cricket agree that all'* is not a meaningful sentence in English. It simply does not conform to the syntactic rules of the language. (There is, of course, a re-ordering of the words which is a meaningful English sentence—in fact, a proposition. The truth value of the proposition will depend on the universe of people to which it refers.) On the other hand, the sentence *'A plicky is a large smoggly.'* does conform to the syntactic rules of English (provided 'plicky' and 'smoggly' are nouns). Although syntactically correct, the sentence makes no sense unless we know what 'plicky' and 'smoggly'

mean. If, in some dialect of English, *plicky* means 'tiger' and *smoggly* means 'cat', then the sentence is meaningful (and, furthermore, is a true proposition).

Similar considerations apply to mathematics. Before we can develop a mathematical theory, we need first to put in place the acceptable language of the theory, that is, we need to agree the symbols we will use and how we are allowed to combine these symbols. To illustrate the point, the formula $(5 \geq +)^2 = \surd$ is not a well constructed sentence, even though it employs standard mathematical symbols. The collection of symbols does not obey the syntactic rules of mathematics. On the other hand $\sqrt{5} + 2 \geq 3^2$ is syntactically correct. Most of us would agree that this statement is not only syntactically correct, but is a meaningful proposition (which happens to be false). The sentence is meaningful only because there is a generally accepted interpretation for the symbols employed; they are familiar to anyone who has studied high school mathematics. Consider the collection of symbols: $\pi_1(S^1) \cong (\mathbb{Z}, +)$. Is this sentence meaningful? The answer depends on whether it is syntactically correct and whether the symbols have any meaning. An algebraic topologist would immediately recognise the sentence as a meaningful (and true) proposition in the same way that the rest of us would recognise $\sqrt{5} + 2 \geq 3^2$ as a meaningful (but false) proposition. These examples illustrate the point that there are two criteria which must be satisfied for a sentence to be meaningful—it must be correctly constructed and the words and symbols used must have accepted meanings. They also underline the fact that 'meaningful' is not synonymous with 'true'.

Consider again the statement of the theorem we proved in the previous section: *every integer greater than 1 can be expressed as a product of prime numbers*. To comprehend the statement, we needed precise meanings for the terms 'divisible', 'prime number' and so on. This shows that any mathematical theory will need precisely stated definitions. However, it is not possible to define all the terms used in a given mathematical theory. A little thought should indicate why this is so. Consider the definition of a prime number given in the previous section: a prime number is an integer greater than 1 which is not divisible by any positive integer except 1 and itself. This relates the term 'prime number' to more basic concepts such as 'integer', 'positive', the number '1' and 'divisible'. Any definition is like this—it relates the term being defined to other terms. Some or all of these other terms may then be defined

using yet more terms, and so on. Clearly this process of definition must stop somewhere or we would spend all our time defining yet more and more terms and never get round to doing any mathematics proper. Therefore some terms must be left undefined.

The preceding discussion indicates what should be the first ingredients in any axiomatic mathematical theory. They are allowable symbols together with **undefined** or **primitive** terms and syntactic rules which govern the correct formation of sentences from the symbols and undefined terms. There is an omission here which may seem surprising—we have made no reference to semantics. In an axiomatic theory, the symbols and undefined terms are not given any meaning. There are good reasons for this and we shall return to the question of meaning later.

In the same way that we cannot define every term, so we cannot prove every result. For example, in our proof of the prime factorisation theorem, we used (implicitly as well as explicitly) various properties of the integers and prime numbers. For the most part we assumed that these properties were familiar and did not need referring to explicitly. If we were required to prove these properties, the proofs would need to be based on some other statements about the integers, and so on. Again to avoid an infinite regression we are forced to have some statements which will not be proved[1]. These are the **axioms** of the theory.

As we have mentioned, Euclid was the first person to state axioms explicitly in around 300 BC. Just five axioms were the basis for his famous development of geometry. To Euclid, however, axioms did not require proof because they were basic statements about the real physical world which he took to be *self-evidently true.* (The Greek word *axioma*—*αξιωμα*—means 'that which is thought fitting'.) Although mathematicians no longer view axioms in this way, the Euclidean perspective still lingers in our culture. In non-mathematical discourse or writing we may come across the phrase 'it is axiomatic that ...' meaning that what follows is not open to question. To see why mathematicians were forced to abandon the Euclidean view of axioms,

[1] The Greek philosopher Aristotle (384-322 BC) was well aware of this. In his *Metaphysics*, Aristotle wrote, 'Now it is impossible that there should be demonstration of absolutely everything, for there would be an infinite regress, so that even then there would be no proof.' Indeed, he went on to say of those who took the contrary view, 'Such a man, as such, is no better than a vegetable.' See *The History of Mathematics: A Reader* edited by John Fauvel and Jeremy Gray, 1987, Macmillan, Basingstoke, in association with The Open University.

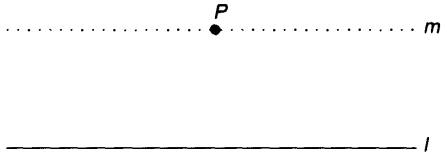


Figure 4.1

we indulge in a brief digression to describe the birth of non-Euclidean geometry.

One of Euclid's axioms, the parallel axiom, states that, for every line l and every point P not lying on l, there exists a line m containing P which is parallel to l in the sense that the two lines never meet (see Figure 4.1).

To claim that this statement is self-evidently true is problematic; the problem lies in the word 'never' in the statement that the lines l and m never meet. This means that, *no matter how far they are extended,* the lines will not meet. Since it is not possible to extend the lines for ever, to claim that the parallel axiom is self-evidently true seems at best to be overstating the case. There was enough doubt about this axiom for the mathematical community to spend some two thousand years attempting to show that it could be deduced from Euclid's other axioms. If this could have been achieved, then there would have been no need to include the proposition as an axiom because it would have been a theorem. Eventually, however, it was discovered that the axiom could not be deduced from the remaining Euclidean axioms.

In the first half of the nineteenth century, two young mathematicians, the Hungarian János Bolyai and the Russian Nikolai Lobachevsky[2], independently of one another found a geometry in which the parallel axiom is false. This new geometry shares the remaining Euclidean axioms and its discovery or invention (depending on your point of view) showed finally that the parallel axiom could not be deduced from the remaining Euclidean axioms. The reason for this is quite simple. If the parallel axiom were deducible from the remaining axioms, then it would be a theorem and so it would not be possible to construct a

[2] It is probable that the great German mathematician Carl Friedrich Gauss shared this discovery. Although he published relatively little, Gauss was the foremost mathematician of his time (many would say the greatest ever) and he was acutely aware of the controversy which would inevitably result from the discovery of non-Euclidean geometry.

geometry where the axiom was false. Since Bolyai and Lobachevsky found a geometry in which the parallel axiom was contradicted, it follows that it is not possible to deduce the axiom from the other Euclidean axioms.

The existence of two geometries, one in which the parallel axiom is true and one in which it is false, has certain implications. In particular, it is not possible for both the parallel axiom and its negation to be true, self-evidently or otherwise! Mathematicians were therefore forced to re-think their views of the nature of axioms.

Today, we no longer regard axioms as self-evident truths, but simply as statements about the undefined terms which are taken as assumptions to serve as the basic building blocks of the theory. It is not necessary for axioms to reflect any perceived property of the 'real world'. In principle, we are free to choose any consistent set of axioms as the starting point for a mathematical theory. The requirement of consistency though is vitally important. A set of axioms is **consistent** if it is not possible to deduce from it some proposition P as well as its negation $\overline{P}$. If it were possible to infer P and $\overline{P}$ then the axioms contain a hidden self-contradiction which make the system useless. Recall from Chapter 2 (pages 47–8) that if an argument has inconsistent premises then it is automatically valid *no matter what the conclusion.* Applied to axiom systems, this means that it is possible to deduce any proposition whatsoever from an inconsistent set of axioms. The modern perspective has replaced self-evidence by consistency as the paramount criterion for an axiom system[3]

We have said that, in principle, any consistent set of axioms can serve as the framework for a mathematical theory. In practice, though, mathematicians do not choose their axiom systems arbitrarily. Some sets of axioms are tailor-made for a particular purpose and others are studied because they have interesting and far-reaching applications. The reasons for studying a particular axiom system lie outside the system itself and relate to possible semantic interpretations of the system. We shall consider these interpretations shortly.

[3] Although crucially important, consistency is somewhat elusive. In 1931, the Austrian logician Kurt Gödel showed that any set of axioms for the arithmetic of the positive integers could not formally be proved to be consistent. Since elementary arithmetic is fundamental to just about all of mathematics, this is a rather depressing state of affairs. Although we know that axiom systems must be consistent, we will frequently be unable to prove them to be so.

There is one final ingredient in any axiom system, the **rules of inference**. These are the rules which determine how theorems may be deduced from the axioms. For us, every axiom system will have the same rules of inference. These are the replacement rules (page 37), the rules of inference for constructing formal proofs (page 50) and the rules of instantiation and generalisation introduced in Chapter 3 (pages 80–1).

Our description of an axiom system is summarised in the box below.

Axiom systems

An **axiom system** comprises:

1. a collection of undefined terms and symbols;
2. syntactic rules for constructing 'sentences' and formulae from the symbols and undefined terms;
3. a collection of properly constructed sentences called axioms;
4. rules of inference.

A mathematical theory can now be defined as the evolution of an axiom system by the use of deductive reasoning (the rules of inference) to prove theorems about the terms of the system. Definitions can be, and in practice always are, introduced to smooth the flow of the theory. They serve to simplify notation. In principle definitions are unnecessary. In practice, we could never get very far if we had only the language of the undefined terms to use. For example, once we have introduced the definition of a prime number we can use this concise term freely without having to refer constantly to an 'integer greater than 1 which is not divisible by any positive integer other than 1 and itself'. The basic core of the theory is its theorems and their proofs which we consider in more detail in the next section.

There is an analogy for an axiom system which may prove helpful here. We could loosely compare the development of an axiomatic mathematical theory with the construction of a building from, say, bricks and mortar. The raw materials—sand, cement, clay and so on—are like the symbols and undefined terms of the system. The

rules and procedures for turning the raw materials into useful building components (for example, how to bake clay to form bricks) play the role of the syntax rules which tell us how to construct sentences from the 'raw materials' of the symbols and undefined terms. The first layer of bricks forming the foundations of the building represents the axioms. It is vitally important that this first layer of bricks is laid properly if any building constructed on top is not to collapse. This is analogous to the consistency requirement of the axioms—if the axioms are inconsistent then any theory developed from them will 'collapse'. The rules of inference are 'rules of construction' which determine how further bricks can be laid onto the existing structure. At this stage, of course, there is no building but only foundations together with raw materials and rules which will permit a building to be constructed. So it is with an axiom system—the system itself is just the basic framework from which a theory can be developed. A building rises from its foundations by brick being laid on top of brick using mortar to hold the structure in place. In the mathematical context each individual brick could be likened to a theorem and the mortar holding it firmly in place is its proof.

Our discussion of axiom systems has so far been rather abstract. To help clarify the ideas we have introduced and to motivate what follows, it is time to consider a specific axiom system.

Example 4.1

We define a simple axiom system as follows.

The undefined terms are: **point**, **line** and **contains**.

There are four axioms (A1–A4):

A1: There exist exactly four points A, B, C, D.

A2: Every line contains at least two points.

A3: For every point P and every point Q not equal to P, there exists a unique line which contains P and Q.

A4: There exist three distinct points such that no line contains all three of the points.

Once we have set up the axiom system, we can begin to prove theorems about it, i.e. we can build our mathematical theory. It is worth remarking that we are taking an informal, descriptive approach to the

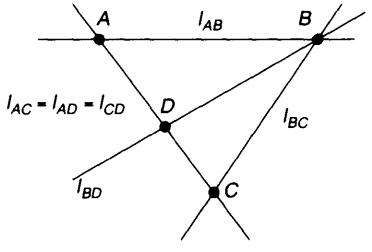
axiom system. Technically, the axioms and theorems should be stated and the theorems proved within the language of symbolic logic (plus whatever symbols we decide to define within the system). For example, using the convention that the universe for upper case letters is 'points', the universe for lower case letters is 'lines' and using $\ni$ to denote 'contains', one way of stating the third axiom is:

A3. $\forall P \forall Q((P \neq Q) \rightarrow$

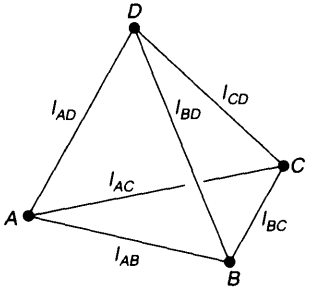
$$\exists l[l \ni P \wedge l \ni Q \wedge \forall m[(m \ni P \wedge m \ni Q) \rightarrow (l = m)]])$$

Whilst reading the previous example, most readers would probably have had a mental picture of points and lines in the plane or in three-dimensional space similar to one of the configurations in Figure 4.2.

Each of these represents a 'model' of the axiom system and it is here that semantics at last enters the picture. In a model, the undefined terms are given meaning so that the axioms become true propositions. In each of these models, the undefined terms 'point' and 'line' are given



(i)



(ii)

Figure 4.2

their standard interpretations as referring to points and straight lines in space and a line 'contains' a point is interpreted as meaning that the point lies on the line.

When defining an axiom system, we often have an interpretation of the axioms in mind, i.e. a situation where the undefined terms are given meanings such that the axioms are true propositions. We define an **interpretation** of an axiom system to be a situation where the undefined terms of the system are given a meaning. In other words, it is in an interpretation of the system where semantics is introduced. An interpretation is called a **model** of the axiom system if the axioms, when interpreted according to the given meanings, are true propositions.

Models are the *raison d'être* of axiom systems. We could hardly claim that the manipulation of meaningless undefined terms and symbols is a worthwhile occupation in its own right. The reason that axiom systems are useful is because they provide information about their models, which is where meaning resides and hence is where our interest lies. Indeed, it is the models which really determine which axioms systems are studied. We have said that, in principle, any consistent axiom system is just as valid or worthy of study as any other. In practice though, some axiom systems are more important and hence more deeply studied than others. The importance of any axiom system lies in its models and not in some intrinsic property of the system itself.

We used the terms 'point', 'line' and 'contains' in Example 4.1 because we had geometric interpretations in mind. In principle, though, since these are undefined terms any words would have been equally acceptable. Suppose, for example, we had chosen to use 'mog' and 'zog' as undefined terms in Example 4.1 instead of 'point' and 'line' respectively. Then axiom A2 would have read, 'every zog contains at least two mogs'. (Using nonsense words like this emphasises the fact that the axioms themselves are meaningless and are therefore neither true nor false.) The German mathematician David Hilbert, who was one of the chief exponents of the formal axiomatic view of mathematics, expressed this idea more colourfully. He is reported to have said, 'One must be able to say at all times—instead of points, lines and planes—tables, chairs and beer mugs'; or, we might add, mogs, zogs and pogs.

When studying geometry, most people understandably prefer to talk about points and lines rather than tables and chairs or even mogs and zogs! Choosing to label the undefined terms using words which have

connotations suggesting a particular model or models can be helpful as this may suggest possible theorems as well as potentially fruitful lines of proof. However, there is the obvious drawback that other models, which may turn out to be just as useful, do not come so readily to mind.

There are many possible models of the axiom system in Example 4.1, completely unrelated to geometry. For instance, suppose four people, Annie, Bob, Carol and David, belong to a certain club and that the club has four committees whose membership is as follows: {Annie, Bob}, {Bob, Carol}, {Bob, David} and {Annie, Carol, David}. Then there is an interpretation of the axiom system in which 'point' means person, 'line' means committee and 'contains' has the obvious meaning that a committee contains a person precisely when the person serves on the committee. Under this interpretation, each of the axioms of Example 4.1 becomes a proposition about committees and their membership. For example, axiom A3 is the proposition:

> For every pair of people, there is a unique committee on which they both serve (i.e. containing them both).

With this interpretation, each of the axioms is a true proposition, so we have another model of the axiom system. This particular model with four committees could be represented in diagrammatic form by Figure 4.2(i) where the lines represent committees.

Axiom systems studied by mathematicians fall into one of two categories which serve separate purposes. Some axiom systems, like that given in Example 4.1, have many different models. Examples which some readers may have encountered are the axiom systems for various kinds of algebraic objects such as groups, rings, fields, vector spaces, Boolean algebras, monoids and the like. In each of these cases there are many examples of the particular algebraic structure. Each example is a model of the axiom system. An important advantage in studying the axiom system in such cases is that of economy of labour. If we can prove some theorem *directly from the axioms* then it must be the case that the theorem becomes a true proposition in every model of the axiom system. Thus we will know that every example of the particular algebraic structure will possess whatever property is described by the theorem. For instance, using the group theory axioms (see Appendix) it is not too difficult to prove that inverses are unique. From this we know that, *in every example of a group*, inverses are unique (see

Exercise 7.4.6(ii)) and we do not need to prove this fact for each and every group.

The second category of axiom systems commonly studied comprises those which have essentially only one model. In other words, all models are for all practical purposes the same. (The notion of two models being 'essentially the same' is one which can be made completely precise. The word mathematicians use for this notion is **isomorphic** which is derived from Greek and means literally 'having the same shape or form.' The details of how 'being essentially the same' is given a precise meaning need not concern us here.) Usually in these cases, the model is a familiar structure such as the set of integers or of real numbers or the Euclidean geometry of two or three-dimensional space. Here, the purpose of using axiom systems is rather different. The axioms represent a few basic properties of the given structure from which it is possible to deduce many other properties of the structure (the theorems of the system). For example, there is an axiom system with thirteen axioms, describing an algebraic object called a 'complete ordered field'. It can be shown that there is essentially only one example of a complete ordered field in the sense that all models of the axiom system are equivalent in a very precise way. 'The' example is the set $\mathbb{R}$ of real numbers together with the operations of addition and multiplication as well as the usual less-than-or-equal-to ordering, $\leq$, of real numbers. What this means is that all the usual properties of the real numbers can be deduced from just thirteen axioms. The advantage of the axiomatic approach is that we need assume only a limited number of properties as the remainder can be rigorously deduced from these. It also means that, in a sense, the thirteen axioms define what we mean by the system of real numbers, i.e. the axioms characterise the real number system.

Exercises 4.1

1. Express the axioms A1, A2 and A4 of Example 4.1 in the symbols of logic.

2. In spherical geometry, 'points' are interpreted as points on the surface of a sphere and 'lines' are interpreted as great circles on the surface of the sphere (that is, circles whose diameter is equal to the diameter of the sphere).

Explain how Euclid's parallel axiom fails in spherical geometry.

3. Consider the following axiom system.

Undefined terms: $\mathbf{0}$, $'$, $+$, $\times$.

Syntax rules:

Valid expressions are defined by:

(i) $\mathbf{0}$ is a valid expression.

(ii) If x is a valid expression, then so is x'.

(iii) If x and y are valid expressions then so are $x + y$ and $x \times y$.

Valid sentences are of the form:

$x = y$ where x and y are valid expressions.

Definition: for valid expressions x and y, $x \neq y$ means $\neg(x = y)$.

Axioms: The universe of discourse is the set of all valid expressions.

A1. $\forall x \forall y[(x' = y') \rightarrow (x = y)]$

A2. $\forall x(\mathbf{0} \neq x')$

A3. $\forall x[(x \neq \mathbf{0}) \rightarrow [\exists y(x = y')]]$

A4. $\forall x(x + \mathbf{0} = x)$

A5. $\forall x \forall y[x + y' = (x + y)']$

A6. $\forall x(x \times \mathbf{0} = \mathbf{0})$

A7. $\forall x \forall y[x \times y' = (x \times y) + x]$

The following is an interpretation of the axiom system.

$\mathbf{0}$ is interpreted as the integer 0.

$'$ is interpreted as 'the next largest integer'. For example, $\mathbf{0}'$ is interpreted as 1, $\mathbf{0}''$ is interpreted as 2, $\mathbf{0}'''$ as 3, etc.

$+$ is interpreted as addition of integers.

$\times$ is interpreted as multiplication of integers.

Show that, with this interpretation, the set of natural numbers $\mathbb{N}$ (non-negative integers) with the operations of addition and multiplication is a model of the axiom system.

4. (For those readers familiar with modulo arithmetic.)

Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ where n is a fixed integer greater than 1.

An interpretation of the axiom system introduced in Exercise 3 above is given as follows.

0 is interpreted as the integer 0.

$'$ is interpreted as 'the next largest integer' as in Exercise 3, but with $(n-1)' = 0$, of course.

$+$ is interpreted as addition modulo n.

$\times$ is interpreted as multiplication modulo n.

Show that this interpretation is not a model of the axiom system given in Exercise 3. Which of the axiom(s) is/are false in the interpretation?

5. The axiom system given in Exercise 3 does not uniquely determine the system of natural numbers $\mathbb{N}$. In other words, there are other models of the system which are essentially different from $\mathbb{N}$. We can define one such model as follows.

Let $\mathbb{N}^*$ be $\mathbb{N}$ with an additional element ω, $\mathbb{N}^* = \mathbb{N} \cup \{\omega\}$. We extend the interpretation given in Exercise 3 as follows.

$$\omega' = \omega$$

For all $n \in \mathbb{N}^*$, $\quad n + \omega = \omega = \omega + n$.

For all $n \in \mathbb{N}^*$, $\quad$ if $n \neq 0$ then $n \times \omega = \omega = \omega \times n$

and $0 \times \omega = 0 = \omega \times 0$.

Show that this interpretation is also a model of the axiom system given in Exercise 3.

(In order to understand the motivation behind the definitions, it may be helpful to think of ω as, in some sense, an 'infinitely large' element of $\mathbb{N}^*$.)

4.4 Theorems and Formal Proofs

In the previous section we considered the foundations of mathematical theories, namely axiom systems. It is now time to consider how such a theory develops by proving theorems using the rules of logic. We

need first to define precisely what we mean by a theorem. Consider, for example, the theorem known to anyone who has studied elementary geometry: *the sum of the angles of any triangle is* 180°. In fact this is a theorem of Euclidean geometry but is not a theorem of non-Euclidean geometry. Non-Euclidean geometry has a different set of axioms from Euclidean geometry (Euclid's parallel axiom is replaced in non-Euclidean geometry by a different axiom concerning parallel lines). Hence the two axiom systems have different sets of theorems. In fact, the corresponding theorem in the non-Euclidean geometry described by Bolyai and Lobachevsky states: *all triangles have angle sum less than* 180°. The important point here is that what is or is not a theorem depends on the particular axiom system.

Suppose we are given a particular axiom system $a_1, a_2, \ldots, a_n$. A theorem in this axiom system is a statement about the terms of the system which can be inferred from the axioms using the rules of inference. Formally, we can define a **theorem in the axiom system** to be a statement about the terms of the system which is logically implied by the conjunction of the axioms. Symbolically, t is a theorem in the system if

$$(a_1 \wedge a_2 \wedge \cdots \wedge a_n) \vdash t.$$

Now we have previously said that an axiom system lacks semantics—its sentences are constructed from undefined terms to which no meanings have been given. This implies that the axioms, and hence the theorems also, are not propositions since they do not have truth values. It is only in an interpretation of the system, when the undefined terms are given meanings, that the axioms and theorems become propositions.

It is important to realise that we are really interested in axioms systems for what they tell us about their models—those interpretations where the axioms are true propositions. Few mathematicians would seriously claim that their discipline is nothing more than the manipulation of meaningless symbols.

Associated with a given axiom system there is a universe of models. As we mentioned in the previous section, sometimes this universe will contain many different models and sometimes all the models will be essentially the same ('isomorphic' in mathematical jargon). Whatever the nature of the universe of models, the axiom system determines those properties which are common to all models. To give an example, we have mentioned that every group can be viewed as a model of the

axiom system for groups. Now there are a great variety of groups, finite and infinite, those with a relatively simple structure and those with a highly complex structure, and so on. The axiom system for groups governs the features which are common to all groups—the so-called **group-theoretic** properties—but gives no information about other properties such as the number of elements in the group.

Since axiom systems are really studied for what they tell us about their models, given an axiom system $a_1, a_2, \ldots, a_n$, we suppose that our work is carried out in an arbitrary model of the system. By this we mean a model which is assumed to have no properties other than those possessed by all models. This corresponds precisely to the notion of an arbitrary element of a universe of discourse. Anything we can prove about our arbitrary model will be true for all models. Thus we have a system of axioms, $A_1, A_2, \ldots, A_n$ which are now regarded as propositions in the arbitrary model. A not insignificant benefit of working an arbitrary model, rather than the axiom system itself, is that it feels more natural to be dealing with propositions instead of strings of undefined terms. A theorem can be defined as a proposition which can be inferred from the axioms using the by now familiar rules of inference and replacement rules. Since our rules of inference are the laws of logic introduced in Chapters 2 and 3, this means that a theorem is the conclusion of a valid argument which has the axioms as premises. In a model the axioms are all true propositions so a valid argument with the axioms as premises is also sound. Recall from Chapter 2 that the conclusion of a sound argument is a true proposition. Thus all theorems will be true propositions in our model. Since the model is arbitrary, this means that a theorem is a true proposition in every model of the axiom system. This is precisely what theorems should be—statements which are true in all possible situations where the axioms are true.

This notion of theorem illustrates the power of the axiomatic method for those axiom systems which have many models. If we can prove a theorem in an arbitrary model, then we can be sure that the theorem is a true proposition in every model. This represents a great economy of labour—proving a theorem in the setting of an arbitrary model gives true results in many different situations, i.e. in all the models.

There is another benefit, too. Some models of the system may be very familiar and well understood. They may be systems, such as that for elementary geometry, for which we have a well-developed intuition. Our understanding of a particular model may suggest theorems or

methods of proof which we can extend to the more general setting of an arbitrary model. If this is the case, then the methods developed for the arbitrary model will apply to all models of the system. In this way we obtain a cross fertilisation of ideas and techniques from one model to another, via the axiom system (or, at least, an arbitrary model).

Now that we know what a theorem in an axiom system is, we turn to the notion of proof. Since a theorem P is the conclusion of a valid argument which has the axioms as premises, we define a **formal proof** of P to be a formal proof of the validity of this argument as defined in Section 2.6. Thus a formal proof of P is a sequence $S_1, S_2, \ldots, S_N$ of propositions where $S_N = P$ and each S_i satisfies one or more of the following criteria:

(a) it is an axiom, or

(b) it can be inferred from earlier propositions in the list using the rules of inference (page 50), or

(c) one of the replacement rules (page 37) guarantees that it is equivalent to a previous proposition in the list.

Note that in cases (b) and (c), the proposition S_i has underlying propositional form s_i which is logically implied by the underlying forms of earlier steps in the proof, i.e. $(s_1 \wedge s_2 \wedge \cdots \wedge s_{i-1}) \vdash s_i$. (It may well be the case that not *all* the $s_1, s_2, \ldots, s_{i-1}$ will be required in order to infer s_i although we must allow this possibility.) This means that an alternative definition of a formal proof of P is a sequence of propositions $S_1, S_2, \ldots, S_N$ where $S_N = P$ and for each i,

$$S_i = A_k \text{ for some } k \text{ or } (s_1 \wedge s_2 \wedge \cdots \wedge s_{i-1}) \vdash s_i,$$

where A_k is an axiom and s_i is the underlying propositional form of the proposition S_i.

It would prove uneconomical to adhere rigidly to this notion of proof. Although it must be possible in principle to provide a proof of a theorem P with only the axioms as premises, such proofs would inevitably be extremely long. Frequently in proving a theorem, we wish to draw upon other theorems which have already been proved. Once a theorem has been proved, we may use it together with the axioms to prove further theorems. (Recall the analogy of the building—each new brick is laid on the existing structure and not directly onto the foundations.) Our notion of a proof of P may be modified accordingly.

Suppose that $T_1, T_2, \ldots, T_m$ are theorems which have already been proved and let $t_1, t_2, \ldots, t_m$ be their underlying propositional forms. To prove a new theorem P, with underlying form p, we need to show that

$$(a_1 \wedge a_2 \wedge \cdots \wedge a_n \wedge t_1 \wedge t_2 \wedge \cdots \wedge t_m) \vdash p.$$

A proof of P is a sequence of propositions $S_1, S_2, \ldots, S_N$ where $S_N = P$ and each S_i satisfies one or more of the following criteria:

(a) it is an axiom or previously proved theorem, or

(b) it can be inferred from earlier propositions in the list using the rules of inference, or

(c) it is equivalent, using the replacement rules, to a previous proposition in the list.

Intuitively it seems reasonable to allow the previously proved theorems as premises in addition to the axioms and it is not hard to justify. Let $\boldsymbol{a}$ be the conjunction of the axioms,

$$\boldsymbol{a} = a_1 \wedge a_2 \wedge \cdots \wedge a_n$$

and $\boldsymbol{t}$ be the conjunction of the theorems so far proved,

$$\boldsymbol{t} = t_1 \wedge t_2 \wedge \cdots \wedge t_m.$$

Then $\boldsymbol{a} \vdash \boldsymbol{t}$. (This follows from a repeated application of the fact that, if $\boldsymbol{a} \vdash t_1$ and $\boldsymbol{a} \vdash t_2$, then $\boldsymbol{a} \vdash (t_1 \wedge t_2)$—see Exercise 2.3.5.) Now suppose $(\boldsymbol{a} \wedge \boldsymbol{t}) \vdash p$, that is, we can prove P provided we allow the previously proved theorems as well as the axioms as premises. Then both $\boldsymbol{a} \rightarrow \boldsymbol{t}$ and $(\boldsymbol{a} \wedge \boldsymbol{t}) \rightarrow p$ are tautologies (since $p \vdash q$ is equivalent to $p \rightarrow q$, being a tautology). It can be shown that (see Exercise 2.3.6)

$$(\boldsymbol{a} \rightarrow \boldsymbol{t}) \wedge ((\boldsymbol{a} \wedge \boldsymbol{t}) \rightarrow p) \vdash (\boldsymbol{a} \rightarrow p).$$

Therefore, since $\boldsymbol{a} \rightarrow \boldsymbol{t}$ and $(\boldsymbol{a} \wedge \boldsymbol{t}) \rightarrow p$ are both tautologies, it follows that $\boldsymbol{a} \rightarrow p$ is also a tautology and so $\boldsymbol{a} \vdash p$. This shows that if P can be deduced from the axioms and previously proved theorems, then P can be deduced from the axioms alone.

Frequently, the theorems we prove are in the form of a conditional $P \rightarrow Q$. For such theorems, we generally use the method of conditional proof introduced in Section 2.7. That is, we add the antecedent P to the premises (axioms and previously proved theorems) and construct

a formal proof whose last line is the consequent Q. (The justification of the method is given in Section 2.7.)

The structure of a formal proof is summarised in the box below.

Formal proof

Proof of a proposition P	Proof of a conditional proposition $P \to Q$ using conditional proof
$1.\ A_1$ $\vdots$ $n.\ A_n$ } axioms	$1.\ A_1$ $\vdots$ $n.\ A_n$ } axioms
$n+1.\ T_1$ $\vdots$ $n+m.\ T_m$ } theorems	$n+1.\ T_1$ $\vdots$ $n+m.\ T_m$ } theorems
	$n+m+1.\ P$ (CP)
$\vdots$	$\vdots$
$r.\ P$	$s.\ Q$ $s+1.\ P \to Q$ $((n+m+1)-s.\ \text{CP})$

To give some flavour for what a formal proof might look like, we consider a very elementary proposition from number theory. Example 4.2 below is a formal proof, based on the axiom system given in Exercise 4.1.3. The axiom system is intended to formalise the arithmetic properties of the natural numbers (non-negative integers) although the proof does not require all the axioms. (Recall from Exercise 4.1.3 that the set of natural numbers $\mathbb{N}$ is a model for this axiom system.) The example is included for two main reasons. One is that it shows that 'obvious' properties of familiar systems can be proved formally using only a very few axioms as the starting point. It is indeed surprising that the arithmetic properties of the natural numbers can be deduced from a handful of axioms. (There is an important axiom—the induction axiom—not included in the system given in Exercise 4.1.3. The importance of this axiom is demonstrated in Chapter 9.) The second reason for including the example is to show that formal proofs can be quite complicated, even for the very simplest

propositions. The example shows clearly why mathematicians almost never give formal proofs of their theorems.

Example 4.2 *Theorem.* $1 \times 2 = 2$.

Note: to distinguish the natural numbers 0, 1, 2 used in the proof from the line numbers of the proof, the natural numbers are printed in bold face type. The symbol $'$ denotes 'successor' so that x' is the successor of x, which is the number $x + 1$. Thus we may define number 1 to be $0'$, 2 to be $1'$ or $0''$ etc.

Proof

1.	$\forall x(x + \mathbf{0} = x)$	(axiom)
2.	$\forall x \forall y[x + y' = (x + y)']$	(axiom)
3.	$\forall x(x \times \mathbf{0} = \mathbf{0})$	(axiom)
4.	$\forall x \forall y[x \times y' = (x \times y) + x]$	(axiom)
5.	$\forall y[\mathbf{1} \times y' = (\mathbf{1} \times y) + \mathbf{1}]$	(4. UI)
6.	$\mathbf{1} \times \mathbf{1}' = (\mathbf{1} \times \mathbf{1}) + \mathbf{1}$	(5. UI)
7.	$\mathbf{1} \times \mathbf{2} = (\mathbf{1} \times \mathbf{1}) + \mathbf{1}$	(6. definition of **2**)
8.	$\forall y[(\mathbf{1} \times \mathbf{1}) + y' = ((\mathbf{1} \times \mathbf{1}) + y)']$	(2. UI)
9.	$(\mathbf{1} \times \mathbf{1}) + \mathbf{0}' = ((\mathbf{1} \times \mathbf{1}) + \mathbf{0})'$	(8. UI)
10.	$(\mathbf{1} \times \mathbf{1}) + \mathbf{0} = (\mathbf{1} \times \mathbf{1})$	(1. UI)
11.	$(\mathbf{1} \times \mathbf{1}) + \mathbf{0}' = (\mathbf{1} \times \mathbf{1})'$	(9, 10. substitution[4])
12.	$(\mathbf{1} \times \mathbf{1}) + \mathbf{1} = (\mathbf{1} \times \mathbf{1})'$	(11. definition of **1**)
13.	$\mathbf{1} \times \mathbf{2} = (\mathbf{1} \times \mathbf{1})'$	(7, 12. substitution)
14.	$\mathbf{1} \times \mathbf{0}' = (\mathbf{1} \times \mathbf{0}) + \mathbf{1}$	(5. UI)
15.	$\forall y[(\mathbf{1} \times \mathbf{0}) + y' = ((\mathbf{1} \times \mathbf{0}) + y)']$	(2. UI)

[4] We are using here the familiar property of equality which states that if $a = b$ and $b = c$ are two lines of a formal proof, then we may add the line $a = c$. There is an axiom of formal logic, sometimes called the **substitution rule**, which governs when this substitution is acceptable. We shall consider this rule again in Chapter 8.

16.	$(\mathbf{1} \times \mathbf{0}) + \mathbf{0}' = ((\mathbf{1} \times \mathbf{0}) + \mathbf{0})'$	(15. UI)
17.	$(\mathbf{1} \times \mathbf{0}) + \mathbf{1} = ((\mathbf{1} \times \mathbf{0}) + \mathbf{0})'$	(16. definition of **1**)
18.	$(\mathbf{1} \times \mathbf{0}) + \mathbf{0} = \mathbf{1} \times \mathbf{0}$	(1. UI)
19.	$(\mathbf{1} \times \mathbf{0}) + \mathbf{1} = (\mathbf{1} \times \mathbf{0})'$	(17, 18. substitution)
20.	$\mathbf{1} \times \mathbf{0}' = (\mathbf{1} \times \mathbf{0})'$	(14, 19. substitution)
21.	$\mathbf{1} \times \mathbf{0} = \mathbf{0}$	(3. UI)
22.	$\mathbf{1} \times \mathbf{0}' = \mathbf{0}'$	(20, 21. substitution)
23.	$\mathbf{1} \times \mathbf{1} = \mathbf{1}$	(22. definition of **1**)
24.	$\mathbf{1} \times \mathbf{2} = \mathbf{1}'$	(13, 23. substitution)
25.	$\mathbf{1} \times \mathbf{2} = \mathbf{2}$	(24. definition of **2**)

□

Many, perhaps most, theorems take the form of a quantified propositional function of the form $\forall x\, Tx$ or $\forall x \forall y\, Txy$. The prime factorisation theorem in Section 4.2 was of this form. We can see this if we write the theorem in the form: *for all integers n greater than* 1, *n can be expressed as the product of prime numbers*. The proof we gave began by assuming that n is an integer greater than 1, that is, n is an *arbitrary* integer greater than 1. The required result, that n is expressible as a product of prime numbers, was then proved for this arbitrarily chosen n. Thus we really proved Tn for an arbitrary n in the universe (of integers greater than 1). However, since n was chosen arbitrarily, we made no special assumptions about n other than that it was an integer greater than 1. This means that we could use the rule of universal generalisation (see Section 3.4) to deduce the theorem $\forall x\, Tx$.

Note, however, that no specific mention of the use of universal generalisation was made in the proof itself. This implicit use of universal generalisation is very common. We can describe the general technique as follows. Suppose we are required to prove $\forall x\, Tx$. We simply prove Ta where a is an arbitrary element of the universe of discourse and then, as a final step, infer $\forall x\, Tx$ justified by universal generalisation. If, as is frequently the case, the theorem to be proved is a quantified conditional, $\forall x(Px \rightarrow Qx)$, then we may use the method of conditional proof to prove $Pa \rightarrow Qa$, where a is an arbitrary element of the universe of discourse. That is we assume Pa and deduce Qa.

Hence we can infer $Pa \rightarrow Qa$, justified by conditional proof, and then $\forall x(Px \rightarrow Qx)$ justified by universal generalisation. This technique is summarised below.

Formal proof using universal generalisation

Proof of $\forall x\, Px$

1.	A_1	} axioms
⋮		
n.	A_n	
$n+1$.	T_1	} theorems
⋮		
$n+m$.	T_m	
⋮		
r.	Pa	
$r+1$.	$\forall x\, Px$	(r. UG)

Proof of $\forall x(Px \rightarrow Qx)$ using conditional proof

1.	A_1	} axioms
⋮		
n.	A_n	
$n+1$.	T_1	} theorems
⋮		
$n+m$.	T_m	
$n+m+1$.	Pa	(CP)
⋮		
s.	Qa	
$s+1$.	$Pa \rightarrow Qa$	$((n+m+1)-s$. CP)
$s+2$.	$\forall x(Px \rightarrow Qx)$	($s+1$. UG)

The axioms and previously proved theorems themselves will also generally be quantified propositional functions. Thus, in the body of the formal proof we will usually need to apply the laws of instantiation to those axioms and theorems in order to obtain unquantified propositions. In fact we have seen this process before in Section 3.4. To provide the formal proof of validity of an argument whose conclusion is a quantified propositional function, we first apply the rules of instantiation to any premises which are quantified propositional functions to obtain non-quantified propositions. Then we give a formal proof in propositional logic and finally apply one of the laws of generalisation to obtain the desired conclusion.

As an illustration of this, consider Example 3.3.4. In the example we provided a proof of the validity of an argument which had two premises and a conclusion, each of which was a universally quantified

propositional function. The essential structure of the proof given in Example 3.3.4 is summarised below where the premises are denoted $\forall x\, P_1(x)$ and $\forall x\, P_2(x)$ and the conclusion is $\forall x\, Q(x)$.

1.	$\forall x\, P_1(x)$	(premise)
2.	$\forall x\, P_2(x)$	(premise)
3.	$P_1(a)$	(1. UI)
4.	$P_2(a)$	(2. UI)
5.		a formal proof in propositional logic
⋮		
10.	$Q(a)$	
11.	$\forall x\, Q(x)$	(10. UG)

Of course, in formal mathematical proofs there are likely to be many more premises. Also the formal proof in propositional logic will generally be considerably more complicated than that given in Example 3.3.4 as Example 4.2 illustrates. Nevertheless, the underlying process is similar to that shown here.

There is one final piece of notation which we wish to introduce to conclude this section. Very many mathematical theorems are expressed in the form of the conditional $P \to Q$. We shall use the symbol $\Rightarrow$ between propositions to mean that the second follows logically from the first *within the current axiom system*. More precisely, we shall use $P \Rightarrow Q$ to mean that

$$(a_1 \wedge a_2 \wedge \cdots \wedge a_n \wedge t_1 \wedge t_2 \wedge \cdots \wedge t_m \wedge p) \vdash q,$$

with our usual notation for axioms and previously proved theorems. In other words, $P \Rightarrow Q$ means that the underlying form of Q is logically implied by the conjunction of the underlying forms of P and the axioms and previously proved theorems. Using the method of conditional proof, we then have

$$(a_1 \wedge a_2 \wedge \cdots \wedge a_n \wedge t_1 \wedge t_2 \wedge \cdots \wedge t_m) \vdash (p \to q).$$

This means that an alternative definition of $P \Rightarrow Q$ is that the conditional $P \to Q$ is a theorem in the given axiom system. Our definition is just a way of making more precise the common informal usage of $P \Rightarrow Q$ to mean 'P implies Q'.

It should be noted that $\Rightarrow$ is a *relation* between propositions. It is not a connective like $\rightarrow$ which joins two propositions or propositional forms to form a new proposition or propositional form. If $P \Rightarrow Q$ then, in any model of the system, if P is a true proposition then Q must also be true, which conforms to the informal usage of the symbol $\Rightarrow$. (Wheeler (1981) similarly distinguishes between the connective $\rightarrow$ and the relation $\Rightarrow$, although many texts do not make this important distinction.)

It is important to understand the properties of this relation. In mathematical jargon, it is reflexive and transitive but not symmetric. To say that $\Rightarrow$ is reflexive just means that $P \Rightarrow P$ for all propositions P. The important transitive property means that if $P \Rightarrow Q$ and $Q \Rightarrow R$ then $P \Rightarrow R$ as well. This seems intuitively reasonable and can be justified as follows. Suppose that $P \Rightarrow Q$ and $Q \Rightarrow R$. Then $P \rightarrow Q$ and $Q \rightarrow R$ are both theorems of the current axiom system. Therefore, using hypothetical syllogism (see Section 2.6), $P \rightarrow R$ is also a theorem of the current axiom system so that $P \Rightarrow R$.

It is also important to note that $\Rightarrow$ is not symmetric. In other words, knowing $P \Rightarrow Q$ gives no information about the validity of the converse relation $Q \Rightarrow P$. We shall adopt the obvious and standard notation and write $P \Leftrightarrow Q$ in the case where both $P \Rightarrow Q$ and $Q \Rightarrow P$.

Exercises 4.2

1. Using the axiom system introduced in Exercise 4.1.3 together with the definitions $\mathbf{0}' = \mathbf{1}$, $\mathbf{1}' = \mathbf{2}$, $\mathbf{2}' = \mathbf{3}$ etc., give a formal proof of each of the following theorems.

(i) $\mathbf{1} + \mathbf{1} = \mathbf{2}$.

(ii) $\mathbf{2} + \mathbf{1} = \mathbf{3}$.

(iii) $\forall x(x + \mathbf{1} = x')$.

(iv) $\mathbf{1} + \mathbf{2} = \mathbf{3}$.

(v) $\mathbf{1} + \mathbf{3} = \mathbf{4}$.

Note that although the proof of $\forall x(x + \mathbf{1} = x')$ is not too difficult, and although it is possible to prove $\mathbf{1} + \mathbf{2} = \mathbf{3}$, $\mathbf{1} + \mathbf{3} = \mathbf{4}$, $\mathbf{1} + \mathbf{4} = \mathbf{5}$ and so on, it is *not possible* to prove $\forall x(\mathbf{1} + x = x')$ from these axioms. To prove this another axiom, the axiom of induction, is required—see Chapter 9.

2. Consider the following axiom system.

Undefined terms: a, b, string.

Syntax rules: a and b are valid expressions.

If x is a valid expression then so are xa and xb.

Axioms:
1. a is a string.
2. ab is a string.
3. If x is a string such that $x = ya$ (for some valid expression y) then xb is a string.
4. If x is a string such that $x = yb$ (for some valid expression y) then xa and xbb are both strings.

(We regard two strings as equal if they are identical as sequences of symbols.)

(a) Find proofs of each of the following theorems.

(i) $abab$ is a string.
(ii) $ababbbb$ is a string.

(b) Discover and prove further theorems.

Note that axiom systems such as this may seem arbitrary and rather useless. However, there are situations, such as in group theory, where important results can be proved using arguments about strings.

4.5 Informal Proofs

The previous section considered in some detail the formal notion of a mathematical proof. The briefest glance at Example 4.2 will indicate that most proofs that we come across do not conform to the rigid standards of formal proofs. Also, we hope that the case study in Section 4.2 indicated that proofs are not generally conceived as a logical step-by-step deduction from premises to conclusion. In this section, we look at proofs from a more practical point of view and try to answer (partially at least) questions such as: What makes a good proof? How are proofs arrived at? How much detail should be included in a proof?

We will use the term **informal proof** to cover any proof which does not adhere to the definition of formal proof given in Section 4.4. The

overwhelming majority of proofs ever written fall into this category so that the spectrum of informal proofs is clearly very wide. At one end of the spectrum, we find very detailed and highly structured arguments like those given in Chapters 2 and 3. Towards the other end of the spectrum we have proofs with a loose, even chatty, style where many of the details have been omitted.

On one level, we may regard an informal proof as an approximation to, and a more reader-friendly version of, a formal proof which underlies it. Formal proofs are frequently too detailed and are difficult to follow; witness Example 4.2. The aim of an informal proof should be to communicate the essential reasons why a particular result holds. The important steps are stressed, but much of the routine detail is omitted, leaving the main reasoning highlighted for scrutiny by the reader. The emphasis of an informal proof should be on effective communication. To achieve understanding by the reader, a blend of words, symbols, diagrams, analogies and the like can be employed.

It is probably impossible to define what makes a good proof, just as it is impossible to define good art or literature. Of course, it is much easier recognise a good proof when we see it and probably easier still to recognise a bad proof! In fact, a proof cannot really be judged in isolation as the intended audience or readership is also important. The style and level of detail appropriate for communication between experts in a particular mathematical field will be considerably different from that which is appropriate for, say, undergraduate students.

In the proof of the prime factorisation theorem in Section 4.2, a lot of background information about the natural numbers was assumed and many of the small details were omitted. This is acceptable because, we hope, the intended readership of that proof is sufficiently familiar with the properties of the natural numbers to render the details both unnecessary and somewhat tiresome. In any proof, there is always a balance to be struck between giving too many details, in which case the proof is laborious and the key ideas may be obscured, or too few, in which case the intended reader may not follow the argument. In general it is better to err on the side of giving too much detail. Too few details may render a proof unintelligible whereas too many should 'merely' make it tedious to follow. More importantly perhaps, errors in incorrect 'proofs' are frequently to be found in the details which the writer has omitted. It is tempting to assume that the details fit into place in the manner in which we expect. Mathematics is often more

subtle than we anticipate and glossing over details can sometimes be hazardous for the proof writer.

The formal description of mathematics diverges from actual practice in another important respect also. Mathematicians do not generally discover theorems by a rigid step-by-step deduction from a set of axioms, contrary perhaps to popular belief. The role of human intuition, experience and inspiration is vitally important. Usually a theorem originates as a **conjecture** which is a belief, or hunch even, that the particular result ought to be true. The mathematician may come to believe in the conjecture for a number of different reasons. There may be many particular examples where the results holds, and no known example where it fails; the result may be the generalisation of a known theorem to a new setting; the result may be strongly analogous to other known theorems in similar settings; or the conjecture may be that inspiration of a gifted individual which is so hard to explain. In formulating conjectures, therefore, inductive reasoning often plays an important role. However, this does not contradict our comments regarding inductive and deductive reasoning in Chapter 1. Although inductive reasoning may play a part in formulating conjectures and suggesting possible methods of proof, only deductive reasoning is allowed in the proofs themselves.

Inspiration is vitally important

Regardless of how a particular conjecture arose, for it to be promoted to a theorem, a proof must be found. Here, too, human intuition, experience and inspiration are usually vital. Anyone who has tried to prove mathematical results will have had the experience of attempting several different lines of attack which turn out to be fruitless before (hopefully)

hitting on the right idea which then develops into a sound proof. Mathematics has been described as 90% perspiration and 10% inspiration although this breakdown does not take account of that other important element—luck. (Perhaps the reader would like to devise a subtitle for this book in the form 'x% perspiration, y% inspiration, z% luck' based on his or her own experience!) The formal description of mathematics given earlier cannot hope to explain these human aspects of the subject. So, even if axiomatic systems and formal proofs provide a reasonable description of mathematics itself (although some people would dispute even that), there is wide agreement that they do not explain at all well the human process of doing mathematics. Our aim in the remaining chapters of this book is to give some insight into this process.

Exercises 4.3

1. Using the axiom system introduced in Example 4.1, give informal proofs of the following theorems.

(i) There exist at most six different lines.
(ii) There exist at least four different lines.

2. Modify the axiom system introduced in Example 4.1 by replacing axiom A1 by:

A1′. There exist exactly five points A, B, C, D, E

whilst keeping the remaining axioms unchanged.

What can you now prove about the maximum and minimum number of distinct lines?

3. Consider the axiom system introduced in Exercise 4.2.2.

(a) Give informal proofs of each of the following. (We shall see in later chapters how such proofs can be made rigorous.)

(i) $abab\ldots ab$ (i.e. ab repeated n times) is a string.
(ii) There is no string of the form $yabb$ (where y is some valid expression).

(b) Suppose the following axiom is added to the system.

5. If xb is a string then x is a string.

(i) Give a formal proof that *abbbbb* is a string.

(ii) Give an informal proof that $abb\ldots b$ is a string, where the number of bs is arbitrary.

4. **Probability axioms.** Assuming set theory (see the appendix for the basic definitions) and the arithmetic of the real numbers, probability theory can be developed from just three axioms. We assume that a set S, called the **sample space**, is given. An **event** is defined to be a subset of the sample space S. The axioms are the following.

A1. For every event A there is a non-negative real number $p(A)$ (called the **probability** of A).

A2. $p(S) = 1$.

A3. For any infinite collection of pairwise disjoint events $A_1, A_2, A_3, \ldots$ (that is $A_i \cap A_j = \varnothing$ for all $i \neq j$),

$$p\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} p(A_n).$$

Prove each of the following theorems.

(i) $p(\varnothing) = 0$.

(ii) For any finite collection of pairwise disjoint events $A_1, A_2, \ldots, A_N$,

$$p\left(\bigcup_{n=1}^{N} A_n\right) = \sum_{n=1}^{N} p(A_n).$$

(iii) For any event A, $p(\overline{A}) = 1 - p(A)$.

(iv) For any events A and B, if $A \subseteq B$ then $p(A) \leq p(B)$

(v) For any events A and B, $p(A \cup B) = p(A) + p(B) - p(A \cap B)$.

5 Direct Proof

5.1 The Method of Direct Proof

Direct proof

In this chapter, we are concerned with the proofs of theorems which are, or can be expressed, in one of the following four forms.

1. (i) A simple proposition P.
   (ii) A universally quantified propositional function $\forall x\, P(x)$.
2. (i) A conditional proposition $P \to Q$.
   (ii) A universally quantified conditional propositional function $\forall x[P(x) \to Q(x)]$.

Note that there is a slight change of notation here regarding propositional functions. In mathematics, it is usual to write $P(x)$ for a propositional function rather than Px which we used in Chapter 3.

This does lead to a liberal use of brackets in some circumstances, but conforms more closely to usual practice and to other mathematical notation.

The four categories of theorem are not mutually exclusive, as the following examples indicate.

Examples 5.1

1. Examples of theorems which are simple propositions include the following.

(a) 59 is a prime number.

(b) A triangle with sides 6 cm, 8 cm, 10 cm has area 24 cm^2.

(c) The quadrilateral whose vertices have coordinates $(-1, 1)$, $(2, -1)$, $(4, 2)$ and $(1, 4)$ is a square.

(d) The sum of the first 100 positive integers is 5050.

(e) $2^7 + 3^{11}$ is divisible by 7.

It should be noted that each of these propositions could be expressed as a conditional proposition instead as follows.

(a) If $n = 59$ then n is prime.

(b) If $\triangle$ is a triangle with sides 6 cm, 8 cm and 10 cm, then $\triangle$ has area 24 cm^2.

(c) If Q is the quadrilateral whose vertices have coordinates $(-1, 1)$, $(2, -1)$, $(4, 2)$ and $(1, 4)$, then Q is a square.

(d) If $N = 1 + 2 + 3 + \cdots + 100$, then $N = 5050$.

(e) If $N = 2^7 + 3^{11}$ then N is divisible by 7.

This shows that the categories 1(i) and 2(i) above are not mutually exclusive. Whether we choose to express each of these theorems as a simple proposition or as a conditional proposition is largely a matter of taste.

2. Consider the following theorem:

Theorem: *All even integers have even squares.*

Clearly this is a universally quantified propositional function. If we define the universe of discourse to be the even integers and we define $P(x)$: x^2 *is even*, then the theorem can be symbolised as the quantified propositional function $\forall x\, P(x)$.

If, on the other hand, we do not restrict the universe of discourse and define

$$E(x): \quad x \text{ is an even integer,}$$

then the theorem can be symbolised as the quantified conditional propositional function $\forall x[E(x) \rightarrow E(x^2)]$.

This example shows that the categories 1(ii) and 2(ii) described above are not mutually exclusive. Again it is a matter of choice as to whether we define universes over which to quantify or instead define additional propositional functions.

From the discussion of the previous example, it should be clear that a proposition of the form

all objects of a certain type have a certain property

can be symbolised either as $\forall x\, P(x)$ or as $\forall x[T(x) \rightarrow P(x)]$ depending on the choice of universe of discourse. Let $P(x)$ symbolise: x *has the certain property.* If we define the universe to be objects of the required type, then the proposition is $\forall x\, P(x)$. However, if we do not restrict the universe to be the objects of the required type, then the proposition may be symbolised as $\forall x[T(x) \rightarrow P(x)]$, where $T(x)$ is the propositional function: x *is an object of the required type.*

In Section 4.4 we gave the outline structure of a formal proof of a proposition which is a universally quantified propositional function—see page 113. To prove $\forall x\, P(x)$ we actually prove $P(a)$ where a is an arbitrary element of the universe and then appeal to the rule of universal generalisation introduced in Section 3.4. To infer $P(a)$, we shall invariably need to apply the rules of instantiation to (some of) the axioms and previously proved theorems. Similarly, to prove $\forall x[P(x) \rightarrow Q(x)]$ we will, in fact, prove $P(a) \rightarrow Q(a)$ for an arbitrary a in the universe. In practice, as we shall see, the use of the rules of instantiation and generalisation is almost always not made explicit in informal proofs. (For theorems whose conclusion is an existentially quantified propositional function $\exists x\, P(x)$, we would prove $P(a)$ for a

specific element a of the universe. The rule of existential specification would then be applied to give the desired conclusion. We shall consider proofs of existentially quantified propositional functions $\exists x\, P(x)$ in Chapter 7.)

The preceding discussion shows that using the rules of instantiation and generalisation, the four classes of theorem defined at the beginning of this chapter (page 121) can be reduced to just the following two.

1. A simple proposition P.
2. A conditional proposition $P \rightarrow Q$.

As we have previously remarked, mathematicians generally do not construct formal proofs. Our aim now is to give a general scheme for proofs which maintains the basic structure of formal proofs but which is less rigid and better describes how proofs are actually constructed by mathematicians. Looking at Example 4.2, it is clear that a greater degree of flexibility will need to be built in to the description of proof. For instance, we certainly do not want to be required to list all the axioms and all previously proved theorems as premises at the beginning of each and every proof. Rather, we wish to introduce only *what* is actually needed for the proof at hand and we wish to introduce what is required *when* it is needed. Thus, in the sequence of propositions which will form a proof, we shall allow an axiom or previously proved theorem to be introduced at any stage.

We may regard the axioms and previously proved theorems as, in a sense, our 'background knowledge' of the system. They represent those propositions which are given (the axioms) or are already known to be true (the theorems). Now we can say that a proof of a proposition P is a sequence of propositions, the last of which is P, such that each proposition is either background knowledge or 'follows logically' from previous propositions in the sequence. Suppose that the sequence of propositions comprising the proof of P is $P_0, P_1, \ldots, P_N$ where, of course, $P_N = P$. To say that P_i 'follows logically' from the previous propositions in the sequence, we mean:

$$(P_0 \wedge P_1 \wedge \cdots \wedge P_{i-1}) \Rightarrow P_i$$

From our discussion in Chapter 4, this means that if all of the propositions $P_0, P_1, \ldots, P_{i-1}$ are true, then P_i is guaranteed to be true also. It should be noted that, although the general step is $(P_0 \wedge P_1 \wedge \cdots \wedge P_{i-1}) \Rightarrow P_i$, it is by no means the case that we will always require *all*

of the propositions $P_0, P_1, \ldots, P_{i-1}$ in order to infer P_i. It will be the case in many instances that $P_{i-1} \Rightarrow P_i$, for example. However, in general we must allow the possibility that all the propositions $P_0, P_1, \ldots, P_{i-1}$ are necessary in order to infer P_i.

This notion of proof, which we call the method of direct proof, is summarised in the box below. It is best thought of as a translation of the method of formal proof given on page 110 into a scheme which governs how proofs are constructed in practice. As with formal proofs there are two schemes in the method of direct proof depending on whether the proposition being proved is P or $P \rightarrow Q$. For a conditional proposition, the method is based on the method of conditional proof.

Method of direct proof

Proposition P

Construct a sequence of propositions $P_0, P_1, \ldots, P_N$ where P_0 is background knowledge, $P_N = P$ and, for each $i = 1, 2, \ldots, N$, the proposition P_i is such that

(a) P_i is background knowledge, or
(b) $(P_0 \wedge P_1 \wedge \cdots \wedge P_{i-1}) \Rightarrow P_i$.

Conditional proposition $P \rightarrow Q$

Construct a sequence of propositions $P_0, P_1, \ldots, P_N$ where $P_0 = P$, $P_N = Q$ and, for each $i = 1, 2, \ldots, N$, the proposition P_i is such that:

(a) P_i is background knowledge, or
(b) $(P_0 \wedge P_1 \wedge \cdots \wedge P_{i-1}) \Rightarrow P_i$.

Note that a direct proof of a simple proposition P must begin with a proposition P_0 which is an axiom or previously proved theorem—in other words, which is part of our background knowledge of the system. Informally, we must begin with a proposition whose truth we have accepted or already proved. From this we proceed in a direct manner to the desired conclusion.

To prove a conditional proposition $P \rightarrow Q$, we use the method of conditional proof. That is, we add the antecedent P to the premises and

produce a direct proof whose last line is the consequent Q. Thus, the first[1] proposition in the proof is the antecedent P. This is often signalled by the phrase 'Assume P ...' or 'Let P ...'. Informally, we assume the truth of P (together with our background knowledge of the system) and deduce a sequence of true propositions, the last of which is Q. Note that it is common to speak informally of 'assuming the truth of P' rather than 'adding P to the premises' which is strictly correct.

Our background knowledge of the system (the axioms and previously proved theorems) falls broadly into two categories. In one category are those propositions which may be regarded as basic or elementary. These would generally not be mentioned explicitly in a proof. An example of such a proposition is the commutative law for addition of real numbers: $\forall x \forall y (x + y = y + x)$. This is such a familiar property of the real numbers that we tend to use it 'automatically', without giving the property itself a conscious thought. Certainly, we would not appeal explicitly to the law each and every time it was used in a proof.

The second category of propositions which we may regard as background knowledge are those which are more directly relevant to the proof at hand. These are the propositions which will be appealed to explicitly in the proof. Generally such propositions will not be mere elementary facts. Often they will be theorems which have 'recently' been proved. Using our analogy, given in Chapter 4, of the development of an axiom system being akin to the construction of a building from bricks and mortar, the propositions in this second category are more likely to be comparable to those bricks immediately supporting the current brick (that is, theorem), rather than those bricks near the bottom of the construction.

Whilst some propositions clearly fall into one or other category of background knowledge, the boundary between the categories is by no means clear cut. For a given proof, what does and what does not need stating explicitly depends in part on who the proof is for. What may be an elementary fact for an expert in a particular branch of mathematics may require mentioning explicitly in a proof aimed at a more general audience. The proof-writer will always need to exercise his or her judgement as to what needs explicit mention and what may be taken for granted. These judgements will depend in part on the

[1] Actually we may choose to introduce some propositions which are background knowledge before writing the antecedent P. This is a stylistic choice; any proof could be structured along the lines described.

intended readership of the proof. The author should always have an intended audience in mind when writing a proof. Such considerations are part of the art of proof-writing—sufficient information must be included for the reader to follow the argument without introducing trivial details which tend to obscure the main thrust of the argument.

Our discussion thus far has been somewhat abstract. It is time now to look at some simple proofs and see how they fit into the framework we have outlined.

Examples 5.2

1. **Theorem:** 173 *is prime.*

The naive proof of this theorem would be to test each integer n from 2 to 172 to determine whether it is a factor of 173. If none of the integers is a factor, then 173 is prime. Although not difficult, this would be a laborious task and the resulting proof would be somewhat tedious both to write and to read. In fact, it is sufficient to test far fewer integers to see whether they are factors of 173, but to justify this reduction in workload we need a theorem which we shall not prove here.

Proof

To reduce the amount of work involved, we make use of the following theorem. (See Exercise 6.2.6 for a proof.)

If n is an integer greater than 1 which has no factor k where k is prime and $2 \leq k \leq \sqrt{n}$, then n is prime. (*)

Since $\sqrt{173} = 13.15\ldots$, we need to show that each of the prime numbers from 2 to 13 (inclusive) is not a factor of 173.

Now:

$173 = 86 \times 2 + 1$ so 2 is not a factor of 173.
$173 = 57 \times 3 + 2$ so 3 is not a factor of 173.
$173 = 34 \times 5 + 3$ so 5 is not a factor of 173.
$173 = 24 \times 7 + 5$ so 7 is not a factor of 173.
$173 = 15 \times 11 + 8$ so 11 is not a factor of 173.
$173 = 13 \times 13 + 4$ so 13 is not a factor of 173.

We have shown that 173 does not have a prime factor between 2 and 13 (inclusive). Therefore, from the theorem (*), we can conclude that 173 is prime.

□

Let's examine the structure of this proof. The first step is to quote a theorem about prime numbers. For the purposes of the proof, we suppose that this theorem is part of our background knowledge. We do not regard it as an elementary fact, however, which is why the theorem is explicitly mentioned. The next step is to apply the rule of universal instantiation to the theorem to obtain the corresponding result for the integer 173. This is the conditional proposition:

if 173 *has no prime factors in the range* $2, \ldots, 13$ *then* 173 *is a prime number.*

The subsequent lines of the proof verify the truth of the antecedent, i.e. 173 has no prime factors in the range $2, \ldots, 13$. Finally, the desired conclusion follows using *modus ponens*.

It should be noted that, although the structure of the proof is indeed that of a direct proof, it is expressed in an informal manner. We have not written out each detailed step line by line, with explicit justifications of each line. Provided we have the necessary background knowledge, the informal proof is considerably easier to follow than its formal counterpart would be. Nevertheless we ought to be aware that there is a formal version underlying our proof.

2. **Theorem:** *The square of any even integer is even.*

As explained earlier, this theorem may be stated in a number of different ways. For example, each of the following could be regarded as acceptable alternatives.

All even integers have even squares.

If n is an even integer, then n^2 is even.

The first of these is in the form *'all objects of a given type have a certain property'* and the second is the conditional form *'if n is an object of the required type, then n has the required property.'* In Example 5.1.2, we expressed the first symbolically as $\forall x[E(x) \rightarrow E(x^2)]$, where the universe of discourse is the set of integers and $E(x)$ denotes: x *is even*. The second version is $E(n) \rightarrow E(n^2)$ for an arbitrary integer n. The rules

of universal instantiation and generalisation allow us to pass between these two formulations of the theorem. If we know $\forall x[E(x) \rightarrow E(x^2)]$ then applying UI allows us to deduce $E(n) \rightarrow E(n^2)$ for an arbitrary integer n. Equally, if we know $E(n) \rightarrow E(n^2)$ for an arbitrary integer n, then UG allows us to deduce $\forall x[E(x) \rightarrow E(x^2)]$.

To apply the method of direct proof, we use the second formulation, $E(n) \rightarrow E(n^2)$; we assume the truth of $E(n)$ and deduce the truth of $E(n^2)$. Of course, before we can even contemplate writing a proof, we need to understand the precise meanings or definitions of the terms employed in the statement of the theorem. In our proofs we use the definition:

> n is an **even** integer if and only if there exists an integer m such that $n = 2m$.

Note that the definition applies to all integers and not just to the positive integers. There is a general point about definitions, which is also worth noting. Any definition is a biconditional. Most frequently, though, definitions are stated as conditionals. There is no apparent reason for this potentially confusing practice. However, it does seem to be a tradition in mathematics and we should be aware of it. In the course of the proof, we shall need to use both

$$(n \text{ is an even integer}) \Rightarrow (n = 2m \text{ for some integer } m)$$

and its converse (see page 115)

$$(n = 2m \text{ for some integer } m) \Rightarrow (n \text{ is an even integer}).$$

First Proof

Let n be an even integer. Then $n = 2m$ for some integer m, so

$$n^2 = (2m)^2 = 4m^2 = 2 \times (2m^2) = 2M$$

where $M = 2m^2$ is an integer. Therefore n is even, as required.

□

Note that the structure of the proof follows the method of direct proof of a conditional proposition, given on page 125. The first line of the proof is the antecedent, $E(n)$ in this case. This is signalled by the phrase 'Let n be an even integer', and it amounts to assuming the truth of $E(n)$ (or, more correctly, adding $E(n)$ to the premises). It is quite common for conditional direct proofs to begin in this way with a sentence 'Let ...'

or 'Suppose ...'. The last line of the proof is the consequent $E(n^2)$, n^2 is an even integer, although the fact that n^2 is an integer is not explicitly mentioned. (The implication 'n is an integer $\Rightarrow$ n^2 is an integer' is assumed to be an elementary fact which does not require explicit mention.) The proof ends at this point, but the formal proof underlying it would have two further lines. These would be $E(n) \rightarrow E(n^2)$, justified by conditional proof and $\forall x[E(x) \rightarrow E(x^2)]$, justified by universal generalisation.

As an alternative, we give below a version of this proof using a chain of implications.

Second proof

n is an even integer

$\Rightarrow$ $n = 2m$ where m is an integer

$\Rightarrow$ $n^2 = (2m)^2 = 4m^2 = 2 \times (2m^2)$

$\Rightarrow$ $n^2 = 2M$ where $M = 2m^2$ is an integer

$\Rightarrow$ n^2 is even.

□

Note that, although our second proof is more symbolic than the first, we have still given explanations of the various steps in words. It is very common when first starting to produce proofs to fail to give sufficient explanation of the steps in the proof. Mathematics uses words as well as symbols. An example of poor style is the following. We regard it as incomplete because it does not mention the crucial facts that m and M are integers. This proof is also unacceptable because it does not give sufficient explanation of the steps involved.

Not-a-good proof

$n = 2m \Rightarrow n^2 = (2m)^2 = 4m^2 = 2 \times (2m^2) \Rightarrow n^2 = 2M$.

□

3. **Theorem:** *If A, B and C are sets such that $C \subseteq A$ and $C \subseteq B$ then $C \subseteq (A \cap B)$.*

For those readers not familiar with the rudiments of set theory, the basic facts needed to understand the proof of the theorem are given in the appendix.

The theorem is clearly a conditional proposition. If a universe is not defined, the antecedent is the conjunction of five simple propositions: *A is a set, B is a set, C is a set, C is a subset of A* and *C is a subset of B*. The consequent is: *C is a subset of* $A \cap B$. Of course, if we are working within the universe of sets then the antecedent is just the conjunction of *C is a subset of A* and *C is a subset of B*.

There is a standard way of visualising sets, called a **Venn diagram**, in which the sets are represented as regions of the plane. Sets A, B and C satisfying the conditions of the theorem could be represented by the following diagram.

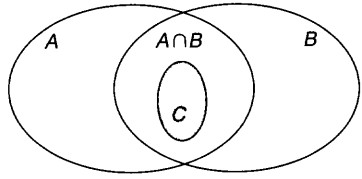


Figure 5.1

In the diagram, we draw the region representing C inside that representing A since C is a subset of A. Similarly we draw the region for C inside that for B. This means that we are forced to draw C inside the overlap region between A and B which represents the set $A \cap B$. It may seem rather obvious, therefore, that $C \subseteq (A \cap B)$. However *a diagram is not by itself a proof* even though it may seem extremely convincing. The reason is that although the regions in the plane represent the sets, they are not the sets themselves. We need, therefore, to give a proof based on the definitions and terminology of set theory (outlined in the appendix).

First proof

Let A, B and C be sets such that $C \subseteq A$ and $C \subseteq B$. To prove $C \subseteq (A \cap B)$, we need to show that, for all x,

$$x \in C \Rightarrow x \in (A \cap B).$$

So let x be an arbitrary element of C, $x \in C$. Since $C \subseteq A$ it follows that $x \in A$. Similarly, since $C \subseteq B$ it follows that $x \in B$. Now we have shown that $x \in A$ and $x \in B$ so it follows from the definition of intersection that $x \in (A \cap B)$. Hence we have shown $x \in C \Rightarrow x \in (A \cap B)$ and can therefore conclude $C \subseteq (A \cap B)$.

□

We could re-write this proof somewhat more symbolically and indeed more economically as follows. Those well-versed in set theory will probably prefer this second version. However, the first proof gives clearer and more detailed explanations of the steps involved and is probably more appropriate for those who are learning set theory for the first time. This illustrates a point we have made previously: there are various acceptable styles for a proof. What is an appropriate style and level of detail depends on the intended audience.

Second proof

Let A, B and C be sets such that $C \subseteq A$ and $C \subseteq B$.

Then $x \in C \Rightarrow x \in A$ (since $C \subseteq A$)

and $x \in C \Rightarrow x \in B$ (since $C \subseteq B$).

Therefore $x \in C \Rightarrow x \in A$ and $x \in B$

$\Rightarrow x \in (A \cap B)$ (from the definition of $A \cap B$).

Hence $C \subseteq (A \cap B)$.

□

Sometimes it is the case that the proof of a proposition needs to be split into several 'sub-proofs', each of which covers one of a number of different possible cases. Of course, it is preferable to keep the number of cases under consideration to a minimum. Also, it may be possible to restrict consideration of separate cases to just a portion of the proof. The following example illustrates that considerable savings in the length of a proof can be obtained by a careful choice of cases to consider.

Example 5.3

Theorem: *For all real numbers x and y, $|x + y| \leq |x| + |y|$.*

As usual, before we embark on a proof, we need to understand clearly what is meant by the **modulus** $|a|$ of a real number a. This is defined by:

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0. \end{cases}$$

Thus, if a is non-negative, $|a|$ is just a itself, but if a is negative then $|a| = -a$ which is positive. For example, $|4| = 4$ and $|-4| = -(-4) = 4$. It is clear therefore that $|a| \geq 0$ for all real numbers a. The fact that $|a|$

is defined by considering two cases separately indicates that the proof of our theorem may involve consideration of more than one case. In fact, our first proof of the theorem requires four cases, since there are two possibilities for x ($x \geq 0$ or $x < 0$) and two for y ($y \geq 0$ or $y < 0$).

First proof

There are four cases to consider.

Case 1: $x \geq 0$ and $y \geq 0$.

Here $|x| = x$ and $|y| = y$. Also, since $x + y \geq 0$, we have $|x + y| = x + y$. Therefore $|x + y| = |x| + |y|$ so that the inequality $|x + y| \leq |x| + |y|$ is certainly satisfied.

Case 2: $x \geq 0$ and $y < 0$.

This time we have $|x| = x$ and $|y| = -y$ but we do not know whether $x + y \geq 0$ or $x + y < 0$. Hence there are two sub-cases to consider.

If $x + y \geq 0$, then

$$\begin{aligned} |x + y| &= x + y \\ &\leq x - y \quad \text{(since } y < 0 \text{ we have } -y > 0 \text{ so that } y < -y\text{)} \\ &= x + (-y) \\ &= |x| + |y|. \end{aligned}$$

If $x + y < 0$, then

$$\begin{aligned} |x + y| &= -(x + y) \\ &= (-x) + (-y) \\ &\leq x + (-y) \quad \text{(since } x \geq 0, -x \leq 0 \text{ so } -x \leq x\text{)} \\ &= |x| + |y|. \end{aligned}$$

Case 3: $x < 0$ and $y \geq 0$.

This is the same as case 2 with x and y interchanged. This means that we could obtain a proof of case 3 simply by interchanging x and y in the proof given for case 2. There is little to be gained by actually writing out such a proof as it is tedious for both author and reader. Therefore, in situations such as this we simply state that the result follows from case 2, by symmetry.

Case 4: $x < 0$ and $y < 0$.

Here $|x| = -x$ and $|y| = -y$ and, since $x + y$ is also negative, $|x + y| = -(x + y)$. Therefore

$$\begin{aligned} |x + y| &= -(x + y) \\ &= (-x) + (-y) \\ &= |x| + |y|, \end{aligned}$$

so $$|x + y| \leq |x| + |y|.$$

We have established the required inequality in each of the four possible cases, which completes the proof.

□

In this proof we have really given three separate direct proofs (the second and third cases being dealt with by a single proof). There is another proof of the theorem which requires consideration of only two separate cases. This is our second proof. Further, it is only in one portion of the second proof where separate arguments need be provided for the two cases—for much of the proof, a single argument is sufficient.

Second proof

We begin by showing that $a \leq |a|$ for all real numbers a. Here there are two cases to consider.

Case A: $a \geq 0$. Then $a = |a|$.

Case B: $a < 0$. Then $a < 0 < |a|$.

Hence $a \leq |a|$ for all real numbers a.

Since $xy \leq |xy|$, it follows that $x^2 + 2xy + y^2 \leq x^2 + 2|xy| + y^2$. But $x^2 = |x|^2$, $y^2 = |y|^2$ and $|xy| = |x||y|$ so that the inequality becomes

$$x^2 + 2xy + y^2 \leq |x|^2 + 2|x||y| + |y|^2.$$

Therefore $(x + y)^2 \leq (|x| + |y|)^2$ and taking (positive) square roots gives the required result

$$|x + y| \leq |x| + |y|.$$

(Note that the last step involves the identity $\sqrt{a^2} = |a|$.)

□

The second proof is more economical than the first as it keeps to a minimum the proportion of the argument which needs to be split into separate cases. Figure 5.2 gives a diagrammatic representation of the structure of the two proofs. Clearly a proof with few 'strands' (that is, cases to consider) is likely to be more economical than one with many.

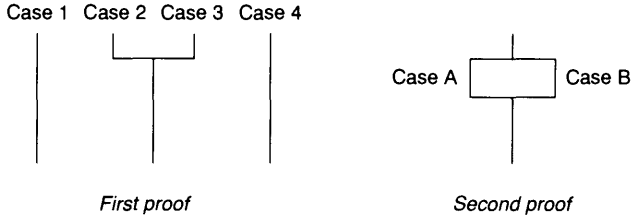


Figure 5.2

Exercises 5.1

1. For each of the following theorems:

(i) define a universe of discourse and a propositional function $Q(x)$ so that the theorem can be symbolised as $\forall x\, Q(x)$;

(ii) suppose that no universe of discourse has been defined; now define a propositional function $P(x)$ so that the theorem can be symbolised as $\forall x[P(x) \rightarrow Q(x)]$.

(a) All prime numbers greater than 2 are odd.
(b) Every integer of the form $4^{2n+1} + 3^{n+2}$ is divisible by 13.
(c) For all positive integers n, $2^n > n$.
(d) All rectangles are parallelograms.
(e) If A is a set with n elements then its power set $\mathcal{P}(A)$ has 2^n elements.

2. Find a direct proof of each of the following theorems.

(a) $2^7 + 3^{11}$ is divisible by 7.
(b) 437 is composite (not prime).
(c) A triangle with sides 20 cm, 21 cm and 29 cm is right-angled.
(d) A triangle with sides 11 cm, 13 cm and 20 cm has area 66 cm^2.

3. Consider the following theorem and proof.

Theorem: *A triangle with sides 6 cm, 8 cm and 10 cm has area 24 cm*^{2}.

Proof

Since $6^2 + 8^2 = 36 + 64 = 100 = 10^2$, the triangle is right-angled, with the right angle between the sides of length 6 cm and 8 cm. Therefore, its area is $1/2 \times 6 \times 8 = 24$ cm^2.

□

Re-write the proof in greater detail. Indicate what assumptions are being made and how the various lines are justified.

4. Without using a calculator, prove each of the following.

(a) $(1 + 2 + 3 + \cdots + 1000) < 4(1 + 2 + 3 + \cdots + 500)$.

(b) $\dfrac{200}{700^2} < \dfrac{1}{500} - \dfrac{1}{700} < \dfrac{200}{500^2}$.

Note: There are two things to prove here:

$$\frac{1}{500} - \frac{1}{700} < \frac{200}{500^2} \quad \text{and} \quad \frac{1}{500} - \frac{1}{700} > \frac{200}{700^2}.$$

(c) $2 < \dfrac{1}{2} + \dfrac{1}{3} + \dfrac{1}{4} + \dfrac{1}{5} + \cdots + \dfrac{1}{16} < 3\dfrac{1}{16}$.

(Again there are two inequalities to prove.)

5. Consider the following theorems and 'proofs'. Each proof is incomplete. Re-write each proof including the missing steps and justifications.

(a) **Theorem**: *The square of an odd integer is odd.*

'Proof'. $n = (2m + 1) \Rightarrow n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2M + 1$ so n^2 is odd.

□

(b) **Theorem**: *For all sets A, B and C, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.*

'Proof'. Let $x \in A$. Then $x \in B$ so $x \in C$. Therefore $A \subseteq C$ as required.

□

6. Prove each of the following theorems. In each case try to identify what background knowledge is being assumed.

(a) **Theorem:** *For any integer n, $n^2 + n$ is even.*

(b) **Theorem:** *If m and n are positive integers such that m is a factor of n and n is a factor of m, then $m = n$.*

(c) **Theorem:** *For every positive integer n, $n! \leq n^n$.*

Note: $n! = n \times (n-1) \times (n-2) \times \cdots \times 3 \times 2 \times 1$.

(d) **Theorem:** *For all sets A, B and C, $(A \cap B) - C = A \cap (B - C)$.*

7. Each of the following proofs is incorrect. Identify what is wrong with each of them. (The first and third are theorems but, of course, the second is not.)

(a) **Theorem:** *For all* $x \neq -2$, $\dfrac{x(x-1)^2 - 5x + 8}{x+2} = (x-2)^2$.

'Proof'. Suppose that $x \neq -2$. Then:

$$\frac{x(x-1)^2 - 5x + 8}{x+2} = (x-2)^2$$

$$\Rightarrow \quad x(x-1)^2 - 5x + 8 = (x+2)(x-2)^2$$

$$\Rightarrow \quad x(x^2 - 2x + 1) - 5x + 8 = (x+2)(x^2 - 4x + 4)$$

$$\Rightarrow \quad x^3 - 2x^2 + x - 5x + 8 = x^3 - 2x^2 - 4x + 8$$

$$\Rightarrow \quad x^3 - 2x^2 - 4x + 8 = x^3 - 2x^2 - 4x + 8.$$

Therefore $\dfrac{x(x-1)^2 - 5x + 8}{x+2} = (x-2)^2$.

□

(b) '**Theorem**': $1 = 2$.

'Proof'.

$$x = 2$$

$$\Rightarrow \quad x - 1 = 1$$

$$\Rightarrow \quad (x-1)^2 = 1$$

$$\Rightarrow \quad (x-1)^2 = x - 1$$

$$\Rightarrow \quad x^2 - 2x + 1 = x - 1$$

$$\Rightarrow \quad x^2 - 2x = x - 2$$

$$\Rightarrow \quad x(x-2) = x - 2$$

$$\Rightarrow \quad \frac{x(x-2)}{x-2} = \frac{x-2}{x-2}$$

$$\Rightarrow \quad x = 1.$$

□

(c) **Theorem:** *For all sets A, B and C, if $C \subseteq (A \cup B)$ and $B \cap C = \varnothing$, then $C \subseteq A$.*

'Proof'. Let $A = \{a,b,c,d,e\}$ and $B = \{d,e,f,g\}$. If $C \subseteq (A \cup B)$ then the elements of C must be drawn from the list a, b, c, d, e, f, g. But $B \cap C = \varnothing$ so that B and C have no elements in common. Therefore the elements of C must, in fact, be drawn from the list a, b, c. Since each of these elements is also an element of A, it follows that $C \subseteq A$.
□

8. Give valid proofs of the theorems in Exercise 7, parts (a) and (c).

5.2 Finding Proofs

In the previous section we explained what is meant by the method of direct proof and gave some examples. However, so far we have given little indication as to how we might discover a line of reasoning which underlies the proof. For example, if we are required to prove a theorem of the form $P \rightarrow Q$, how do we find a sequence of intermediate

Finding proofs

propositions which links P to Q? It is one thing to understand what is meant by a direct proof and to follow some examples, but it is quite another to be able to sit down and actually construct proofs for oneself.

Our aim in this section is to offer some guidance which we hope will assist in developing theorem-proving abilities. Although we hope our guidance and examples will be helpful, there is really no substitute for practice and there is a wide variety of exercises at the end of this section and the next. It may be argued that, just as it is not possible to teach someone to write great literature or become a chess grandmaster, so it is not possible to teach someone to prove theorems. We can certainly teach the laws of logical deduction (as, indeed, we can teach the rules of grammar or of chess), but the more creative aspects are much harder to communicate, whether to the aspiring mathematician, writer or grandmaster.

Perhaps the most important ingredient in theorem-proving is experience of proving theorems. However, there are some general guidelines which will prove useful. The first point sounds obvious, but its importance should not be underestimated: before attempting a proof, the statement of the theorem must first be understood. We have seen, for example, that conditional propositions $P \to Q$ can be expressed in a variety of ways, so it is important to understand what is the antecedent P and what is the consequent Q. There are, in fact, several further ways in which a conditional proposition $P \to Q$ is sometimes expressed which we have not yet considered in this chapter. These include the following (see Section 2.2).

> P is sufficient for Q or P is a sufficient condition for Q;
> Q is necessary for P or Q is a necessary condition for P; and
> P only if Q.

From the statement of the theorem, we must ascertain what it is that we may assume (P) and what it is that we must deduce (Q). Achieving a clear understanding of the statement of the theorem is often half the battle in proving it.

Once the statement of the theorem is clearly understood, the next question is: have we seen a similar theorem before? If so, how was that other theorem proved, and can the proof be adapted to the present theorem? (It is here, of course, where the vital ingredient 'experience' is so important.) Even if the subject matter of the result to be proved is new and unfamiliar, it may be analogous to other results—it may have a flavour

similar to something more familiar. We try to explore any similarities or analogies that occur to us as they may be just what is needed to get us started in the right direction.

Another very helpful technique is to explore some examples of the result we are trying to prove. Often we are more comfortable working with specific, concrete examples, so we try to see why the result is true in one or two well-chosen cases. It should always be remembered, though, that a specific example, even if it seems to be typical, will not serve to prove a general result.

In a similar vein, it is often productive to begin a search for a proof by first considering a simpler special case. Depending on the theorem, there are various ways in which this may be done. We might, for example, restrict the number of variables or consider objects with special properties (equilateral triangles instead of general triangles, finite sets instead of arbitrary sets, the real numbers instead of an arbitrary field, etc.). Not surprisingly, we may be able to obtain a proof of the special case when the general case initially proved to be intractable. Having thoroughly understood the special case, it may then be possible to generalise and modify the arguments so that they apply to the general case. This process is sometimes called the **specialisation-generalisation process**[2]—we first specialise to a simpler situation and then generalise the resulting insights to the more general environment. We shall see an example of the specialisation-generalisation process in Example 5.5 below. It was also used in developing the proof of the prime factorisation theorem in Chapter 4.

We could liken the process of finding a proof to that of finding a route through a maze. (To the novice, a more apt analogy might seem to be finding the proverbial needle in the haystack.) To prove a conditional proposition $P \rightarrow Q$, for example, we need to find a 'route' from antecedent P to consequent Q (Figure 5.3). At each step there may be several choices of path to take, although the choices available are only those sanctioned by logical inference. Some choices will lead eventually to a dead end, even though they may initially look promising. At times we may seem to be doubling back on ourselves. Each choice we make will open a new set of possibilities and so on until hopefully we finally emerge from the maze at our destination Q.

[2] In his widely read book, Polya (1957) explores this and other problem-solving heuristics which are highly relevant to the task of discovering a proof. Polya's book is recommended reading for the aspiring 'proof-finder.'

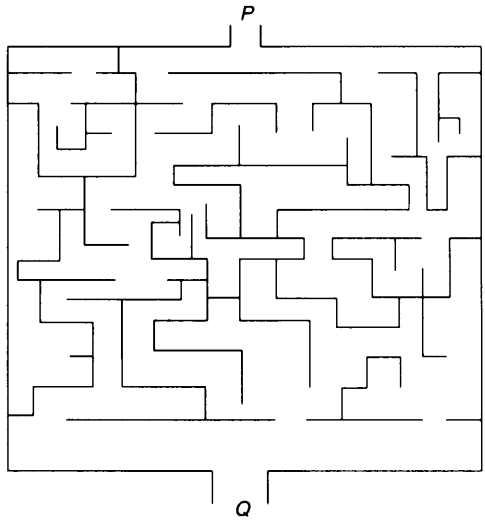


Figure 5.3

When walking through a real-life maze (as opposed to one drawn on paper), a good sense of direction is an extremely useful attribute. So, too, it is with theorem-proving. It is always important to keep the destination in mind. It is by no means the case that each step on the way will apparently bring us nearer our goal, the consequent Q. Nevertheless we should always be aware of where we are and in which direction our destination lies so that we can avoid travelling in completely the wrong direction.

There is one technique which is often helpful when solving mazes drawn on paper. A paper maze can be tackled from both ends by working backwards from the end, as well as forwards from the starting point, in the hope that the two paths may meet, in which case a path from beginning to end has been constructed.

Solow (1990) has pointed out that the same idea is often extremely useful when trying to construct a direct proof. As well as trying to work 'forwards' by deducing propositions which follow logically from the antecedent P, we can also work backwards. This means seeking propositions which *from which* we may deduce the antecedent Q. In other words, we may seek a proposition Q_1 the truth of which would be *sufficient* to deduce Q, i.e. $Q_1 \Rightarrow Q$. If we can find such a proposition Q_1 we have reduced the problem to showing $P \Rightarrow Q_1$. (This is because of the transitive property of $\Rightarrow$: $P \Rightarrow Q_1$ and $Q_1 \Rightarrow Q$ together imply

$P \Rightarrow Q$, see Section 4.4.) Then we can again ask what proposition Q_2 would be sufficient to guarantee the truth of Q_1, $Q_2 \Rightarrow Q_1$, and so on. Working both forwards and backwards we obtain two sequences of propositions

$$P \Rightarrow P_1, P_1 \Rightarrow P_2, P_2 \Rightarrow P_3, \ldots \quad \text{and} \quad \ldots, Q_3 \Rightarrow Q_2, Q_2 \Rightarrow Q_1, Q_1 \Rightarrow Q.$$

If we can get the two sequences to meet in the middle—that is, to have a common proposition R such that $P_n \Rightarrow R$ and $R \Rightarrow Q_m$ for some values of m and n—then the proof will be complete. We simply splice the two sequences of deductions together to produce the final direct proof:

$$P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow \cdots \Rightarrow P_{n-1} \Rightarrow P_n \Rightarrow R \Rightarrow Q_m \Rightarrow Q_{m-1} \Rightarrow \cdots \Rightarrow Q_2 \Rightarrow Q_1 \Rightarrow Q.$$

A word of caution is in order when working backwards from Q. We are seeking a proposition Q_1 such that $Q_1 \Rightarrow Q$; it is a common error to find Q_1 such that $Q \Rightarrow Q_1$. It may be that the converse $Q_1 \Rightarrow Q$ is also valid, but we cannot just assume this—we must be able to prove it.

Thus far, we have emphasised the linear nature of proofs—both formal proofs of the validity of arguments in Chapters 2 and 3 and in our discussion of mathematical proofs. Starting from the premises, the proof progresses in a linear fashion to the conclusion. However, proofs are not always discovered in this way. Indeed, very often proofs are not pieced together by working linearly in two directions, one forwards and one backwards. To use an analogy from software engineering, many proofs are discovered using a **top-down approach**. At the highest level, we outline the broad overall structure of the proof. At the next level, we may try to work from premises to conclusion, but temporarily ignoring any complications which may arise. At this stage we do not worry too much about any details which we cannot prove. Typically, we may reason (to ourselves): if I can prove such-and-such, then the proof can proceed along these lines. If the proof can be 'completed' assuming the various such-and-such's then we can go back and try to fill the various gaps by proving each of the missing pieces. Figure 5.4 illustrates this process. As we proceed further down the diagram so we fill in more and more of the required details.

Figure 5.5 shows the corresponding linear version of the proof shown in Figure 5.4. Note that in this linear version, the need for various phases of the proof may not become apparent until later. For example,

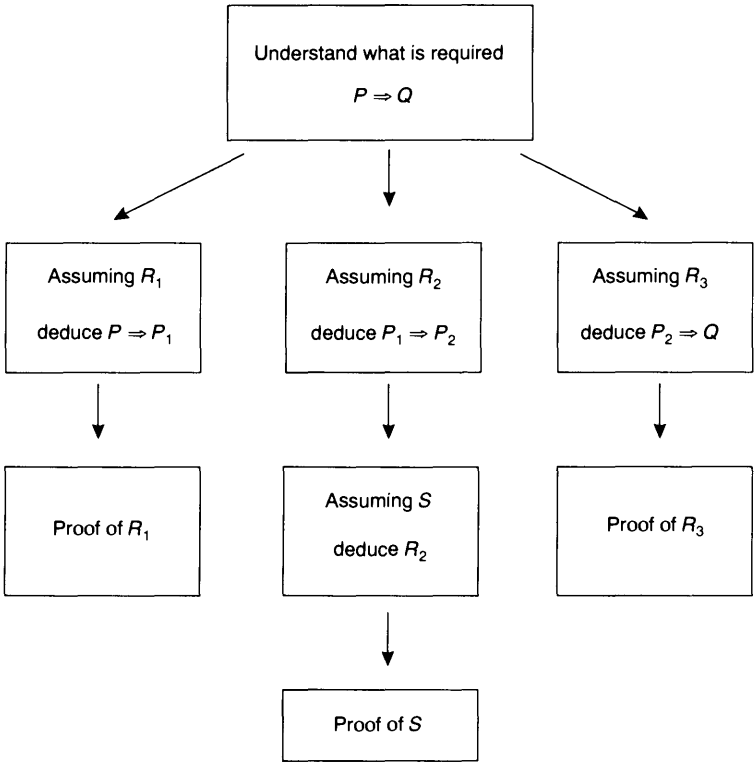


Figure 5.4

someone reading the linear version may wonder why it begins with a proof of R_1; it is only later in the proof that its relevance becomes apparent.

Given that proofs are often discovered in a top-down fashion, it is not surprising that they are frequently best understood, and therefore presented, in this way. (Leron (1983) contends that proofs are more comprehensible when presented in a top-down fashion, which he calls the 'structural method.') For complex proofs where there are many levels, it is often desirable to present the propositions at the lowest level (for example, R_1, S and R_3 in Figure 5.4) as separate theorems. These would be proved before the main theorem $P \Rightarrow Q$, thus removing some of the complications from the main proof. Often such 'little' theorems which are used to help prove a 'main' theorem are called **lemmas**. (Mathematicians often use the term **corollary** for a theorem which follows in a very straightforward manner from a theorem just

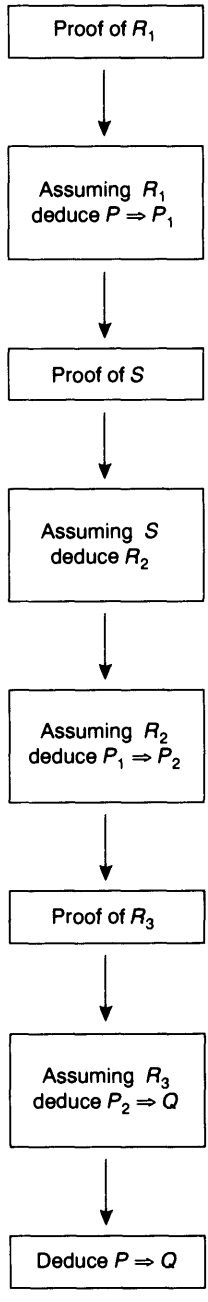
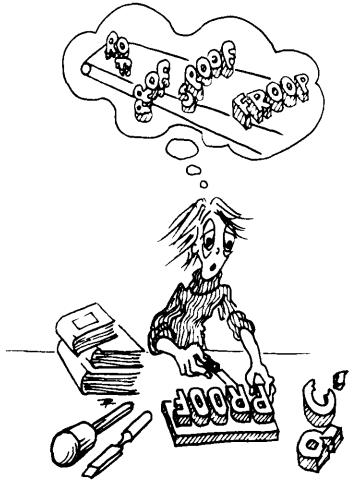

Proof of R_1
Assuming R_1 deduce $P \Rightarrow P_1$
Proof of S
Assuming S deduce R_2
Assuming R_2 deduce $P_1 \Rightarrow P_2$
Proof of R_3
Assuming R_3 deduce $P_2 \Rightarrow Q$
Deduce $P \Rightarrow Q$

Figure 5.5

proved. Thus it is fairly common to see theorems grouped as lemma 1, lemma 2, ..., theorem 1, corollary 1, corollary 2, ... The lemmas assist the proof of the 'main' theorem and the corollaries are simple consequences of it. Of course, whether a theorem should be labelled a lemma, a theorem or a corollary is a matter of subjective judgement.)

To illustrate our discussion so far, we now look at a few examples in some detail. We shall try to give some insight into the *process* of finding a proof rather than concentrating on the presentation of the proof itself. Each example will be relatively long and at times messy—but then so, all too frequently, is the discovery process. Proofs don't roll off some imaginary production line as immaculately finished objects!



Proofs don't roll off some imaginary production line...

Example 5.4

Theorem: *For all non-negative real numbers x and y, $(x+y)/2 \geq \sqrt{xy}$.*

Note: $(x+y)/2$ is the **arithmetic mean** and $\sqrt{xy}$ is the **geometric mean** of x and y, so the theorem says that the arithmetic mean of two non-negative real numbers is always at least as great as their geometric mean.

First note that the theorem can be reformulated as a conditional:

if x and y are real numbers such that $x \geq 0$ and $y \geq 0$

then $\dfrac{x+y}{2} \geq \sqrt{xy}$.

Therefore our initial assumption is: *x and y are non-negative real numbers* and our goal is to deduce the inequality $(x+y)/2 \geq \sqrt{xy}$.

The antecedent is very general so there are many possible deductions which could be made from it and it is not clear which is the best (forward) direction in which we should proceed. For example, from the proposition *x and y are real numbers such that $x \geq 0$ and $y \geq 0$* we could deduce any of the following:

$$x + y \geq 0$$

$$xy \geq 0$$

$$x - y \geq 0 \text{ or } y - x \geq 0$$

$$\frac{x}{y} \geq 0 \text{ or } y = 0$$

$$x - y \text{ is a real number.}$$

It is by no means clear if any of these provides a useful direction in which to proceed. Actually, one of these statements will be the first step in our final proof but it is not obvious which. Instead we turn to the conclusion and try working backwards. From $(x+y)/2 \geq \sqrt{xy}$, it may seem sensible to 'remove' the square root so we square both sides and conclude $((x+y)/2)^2 \geq xy$. (This is permissible since both sides of the inequality $(x+y)/2 \geq \sqrt{xy}$ are non-negative.) However, the implication here is in the wrong direction: we could deduce

$$\frac{x+y}{2} \geq \sqrt{xy} \Rightarrow \left(\frac{x+y}{2}\right)^2 \geq xy$$

but what we really need is the converse

$$\left(\frac{x+y}{2}\right)^2 \geq xy \Rightarrow \frac{x+y}{2} \geq \sqrt{xy}.$$

Unfortunately, the converse does not hold for arbitrary real numbers x and y. (Consider, for example, the case where $x = -1$, $y = -2$.) However, for *non-negative* real numbers x and y the converse

implication does hold:

$$\left(\frac{x+y}{2}\right)^2 \geq xy \text{ and } x \geq 0, y \geq 0 \quad \Rightarrow \quad \frac{x+y}{2} \geq \sqrt{xy}.$$

(This follows from the theorem: *if a and b are real numbers such that $a \geq 0$ and $b \geq 0$, then $a^2 \geq b^2 \Rightarrow a \geq b$.* The proof of this theorem is left as an exercise (Exercise 5.2.1(a)). For the purposes of the present proof we shall regard this as part of our background knowledge.)

Since $x \geq 0$ and $y \geq 0$ is part of the antecedent, we have completed the first backwards step: if we can prove

$$\left(\frac{x+y}{2}\right)^2 \geq xy$$

then we can complete the proof. Using some elementary algebra, this inequality is equivalent to

$$\frac{(x+y)^2}{4} \geq xy$$

which in turn is equivalent to $(x+y)^2 \geq 4xy$, by multiplying both sides by 4. In symbols, what we are saying here is:

$$\left(\frac{x+y}{2}\right)^2 \geq xy \quad \Leftrightarrow \quad \frac{(x+y)^2}{4} \geq xy \quad \Leftrightarrow \quad (x+y)^2 \geq 4xy.$$

In the proof (when we eventually come to write it down) we will need to proceed in the direction:

$$(x+y)^2 \geq 4xy \quad \Rightarrow \quad \frac{(x+y)^2}{4} \geq xy \quad \Rightarrow \quad \left(\frac{x+y}{2}\right)^2 \geq xy.$$

Still working backwards, we now ask the question: how can we prove $(x+y)^2 \geq 4xy$? In general, there are two useful ways of showing $a \geq b$ for non-negative real numbers a and b. We could show $a - b \geq 0$ or, if $b \neq 0$, we could show $a/b \geq 1$. Using the first of these, our problem becomes that of showing

$$(x+y)^2 - 4xy \geq 0.$$

Now $(x+y)^2 - 4xy = x^2 + 2xy + y^2 - 4xy = x^2 - 2xy + y^2 = (x-y)^2$ so we are required to show $(x-y)^2 \geq 0$. But this we know to be true since the square of any real number is non-negative. We have, therefore, worked our way back right back to the starting point and it is time to

write down the proof in a readable form, proceeding in the forwards direction from antecedent to consequent. Again we give the proof twice using slightly different styles of presentation.

First proof

Suppose that x and y are real numbers such that $x \geq 0$ and $y \geq 0$. Then $x - y$ is a real number so that $(x - y)^2 \geq 0$. Expanding the right-hand side gives $x^2 - 2xy + y^2 \geq 0$ and adding $4xy$ to both sides produces $x^2 + 2xy + y^2 \geq 4xy$ which is equivalent to $(x + y)^2 \geq 4xy$. Since both $x + y$ and $4xy$ are non-negative, we may take the (positive) square root of both sides: $x + y \geq \sqrt{4xy} = 2\sqrt{xy}$. Finally, dividing by 2 gives the desired result: $(x + y)/2 \geq \sqrt{xy}$.

□

This proof is very descriptive. We could re-write it more symbolically as follows. This second version of the proof shows its structure more clearly and so may be preferred to the first.

Second proof

Suppose that x and y are real numbers such that $x \geq 0$ and $y \geq 0$. Then $x - y$ is real so that

$$
\begin{array}{lll}
 & (x - y)^2 \geq 0 & \\
\Rightarrow & x^2 - 2xy + y^2 \geq 0 & \\
\Rightarrow & x^2 + 2xy + y^2 \geq 4xy & \text{(adding } 4xy \text{ to both sides)} \\
\Rightarrow & (x + y)^2 \geq 4xy & \\
\Rightarrow & x + y \geq \sqrt{4xy} = 2\sqrt{xy} & \text{(taking square roots which is valid since } x + y \geq 0, xy \geq 0\text{)} \\
\Rightarrow & \dfrac{x + y}{2} \geq \sqrt{xy}. &
\end{array}
$$

□

Example 5.5

Theorem: *Let $P(x_1, y_1, z_1)$ and $Q(x_2, y_2, z_2)$ be two points in three-dimensional space. Then the distance between them is*

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}.$$

The theorem is clearly a conditional proposition. The antecedent is the conjunction of

$$P(x_1, y_1, z_1) \text{ is a point in three-dimensional space}$$

and

$$Q(x_2, y_2, z_2) \text{ is a point in three-dimensional space}$$

and the consequent is

$$\text{the distance between } P \text{ and } Q \text{ is } d, \text{where}$$

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}.$$

Since the theorem is geometric in nature, we begin by drawing a diagram. This is very useful in setting the scene, but we must be a little careful. In Figure 5.6, we have drawn both points P and Q in the first octant, that is, with their coordinates all positive. This is convenient, but we must ensure that the argument we produce for our proof applies equally well to any pair of points.

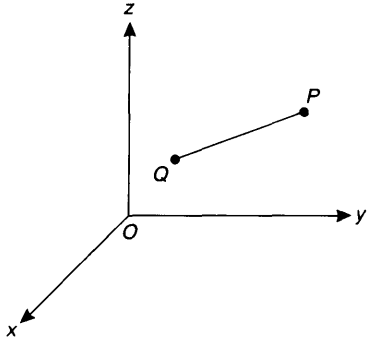


Figure 5.6

Perhaps the most useful question to ask first is: have we seen anything similar before? It may be that we have seen the corresponding theorem for points in two-dimensional space. Even if we have not previously met the distance formula for points in the xy-plane, we may be led to consider it as a useful special case.

Points in the plane are defined by pairs of coordinates (x, y), so the corresponding theorem in this restricted case is the following.

Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ be two points in two-dimensional space. Then the distance between them is d, where

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

Again a good starting point is a diagram (Figure 5.7). A little doodling on the diagram leads to us draw something familiar, namely a right-angled triangle PQR. This is useful because we all know something about right-angled triangles, namely Pythagoras' theorem. With our notation, Pythagoras' theorem says $PQ^2 = QR^2 + PR^2$, where PQ is shorthand for the distance between P and Q, etc.

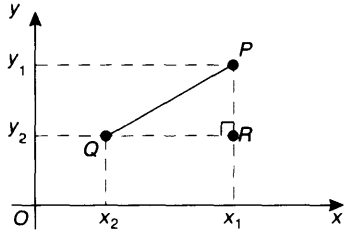


Figure 5.7

Now $PQ^2 = d^2$, so it is useful to perform one step backwards from our conclusion and note that, since all the distances are non-negative quantities,

$$d^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2 \quad \Rightarrow \quad d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

(We used a similar result in the previous example.)

From Figure 5.7, we can see that R has the same x-coordinate as P and the same y-coordinate as Q, so R is the point (x_1, y_2). Therefore $QR = x_1 - x_2$ and $PR = y_1 - y_2$ so from Pythagoras' theorem it follows that:

$$d^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$$

which is the antecedent of our single backwards step. It would appear that we have joined the forward and backward trails, but we need to be just a little more careful. The equations $QR = x_1 - x_2$ and $PR = y_1 - y_2$ assume that P lies above and to the right of Q in the diagram so that $x_1 \geq x_2$ and $y_1 \geq y_2$. In other words, we are assuming special properties of the points and this is not acceptable since they should be arbitrary points in the plane.

This slight deficiency is easily remedied. If P lies to the left of Q then $QR = x_2 - x_1$ and if P lies below Q then $PR = y_2 - y_1$. Note that we are still defining R to be the point (x_1, y_2). Geometrically, R is the point of intersection of the horizontal line through Q and the vertical line through P regardless of the relative positions of P and Q. (It is a useful exercise to draw diagrams to illustrate the other possibilities for the relative positions of P, Q and R.)

All the cases are covered by the equations $QR = |x_1 - x_2|$ and $PR = |y_1 - y_2|$. Since $|x_1 - x_2|^2 = (x_1 - x_2)^2$ and $|y_1 - y_2|^2 = (y_1 - y_2)^2$ we may still conclude

$$d^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2$$

as required.

It is time to organise these considerations into a coherent proof of the two-dimensional special case.

Proof of the two-dimensional case

Let $P(x_1, y_1)$ and $Q(x_2, y_2)$ be any two points in the xy-plane. Define the point R to be (x_1, y_2). Then PR is a vertical line (parallel to the y-axis) and QR is a horizontal line (parallel to the x-axis)—see Figure 5.7. Therefore the triangle PQR is right-angled with right angle at R, so

$$PQ^2 = QR^2 + PR^2$$

by Pythagoras' theorem.

Now $QR = |x_1 - x_2|$ and $PR = |y_1 - y_2|$ so

$$\begin{aligned} d^2 &= PQ^2 \\ &= |x_1 - x_2|^2 + |y_1 - y_2|^2 \\ &= (x_1 - x_2)^2 + (y_1 - y_2)^2 \end{aligned}$$

and, since d is non-negative, taking square roots gives

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

□

Now that we have considered in some detail the special case, we are in a position to move on to the three-dimensional situation (Figure 5.6). Since Pythagoras' theorem played such a key role in our special case,

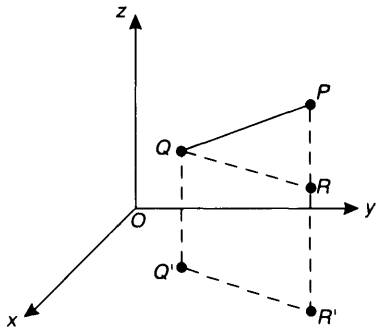


Figure 5.8

it is natural to ask how we can construct a right-angled triangle in the more general diagram. Imagine drawing a vertical line through P (as we did before) and constructing a horizontal plane through Q. (In the two-dimensional situation, we draw a horizontal line through Q, but we have now moved up a dimension.) The line and plane meet in a point R and produce a right-angled triangle PQR—Figure 5.8. (The triangle is right-angled because the vertical line through P is at right angles to any line drawn in the horizontal plane through Q.) For this triangle, Pythagoras' theorem gives:

$$PQ^2 = QR^2 + PR^2 \tag{1}$$

We need expressions for the lengths QR and PR. Note that P and R have the same x and y-coordinates and differ only in their z-coordinate. In fact R is the point (x_1, y_1, z_2) so the distance PR is just $|z_1 - z_2|$. In our diagram $PR = z_1 - z_2$ but we need also to take care of the situation where Q lies above P. Therefore

$$PR^2 = |z_1 - z_2|^2 = (z_1 - z_2)^2. \tag{2}$$

To find an expression for QR, we note that both points lie on the same horizontal plane so that the situation here is much the same as our two-dimensional special case. Instead of repeating all our arguments in the proof of the two-dimensional case, we can simply use the result. (We are at liberty to use any previously proved theorems.) To do this draw vertical lines from Q and R to points Q' and R' respectively in the xy-plane. Then Q' is the point (x_2, y_2) and R' is the point (x_1, y_1). Also, since $QQ'R'R$ is a rectangle, $QR = Q'R'$. Therefore

$$QR^2 = (Q'R')^2 = (x_1 - x_2)^2 + (y_1 - y_2)^2. \tag{3}$$

We can now piece together equations (1), (2) and (3) as follows:

$$\begin{aligned} d^2 &= PQ^2 \\ &= QR^2 + PR^2 && (1) \\ &= (x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2 && (2) \text{ and } (3) \end{aligned}$$

so taking square roots gives

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}.$$

We leave as an exercise to re-organise these arguments into a coherent proof proceeding from antecedent to consequent.

Exercises 5.2

1. (a) Prove that, if a and b are non-negative real numbers, then $a^2 \geq b^2 \Rightarrow a \geq b$.

   Hint: consider the expression $a^2 - b^2$.

   (b) Prove that, for all real numbers a and b, $a^2 \geq b^2 \Rightarrow |a| \geq |b|$.

2. (a) Show that the roots (solutions) of the quadratic equation

   $$x^2 - (2k + 1)x + (k^2 + k) = 0$$

   differ by 1.

   (b) Prove that, if both the roots of the quadratic equation

   $$x^2 + ax + b = 0$$

   are even integers, then a and b are also even integers.

3. (i) Show that, if the line $y = mx - 2$ intersects the parabola $y = 3x^2 + 1$, then $|m| \geq 6$.

   (ii) Show that, if $|m| \geq 6$, then the line $y = mx - 2$ intersects the parabola $y = 3x^2 + 1$.

4. (i) Prove that $x(x - 3) > 10 \Rightarrow x < -2$ or $x > 5$.

   (ii) Prove the converse of (i): $x < -2$ or $x > 5 \Rightarrow x(x - 3) > 10$.

5. Let x and y be real numbers. Prove that, if $x \neq 0$ or $y \neq 0$ then $x^2 + xy + y^2 > 0$.

6. Let n and m be positive integers. We say m **divides** n, written $m|n$, if there exists a positive integer k such that $n = km$. Prove each of the following for all positive integers m, n and p.

(i) $m|n$ and $n|p \Rightarrow m|p$.

(ii) $m|n$ and $n|m \Rightarrow m = n$.

(iii) $p|m$ and $p|n \Rightarrow p|(am + bn)$, for all positive integers a, b.

7. Prove that, given any three points in the plane which do not lie on a straight line, there exists a circle on which all three points lie.

8. Let x and y be positive real numbers such that $x + y = 1$. Show that:

(i) $xy \leq \frac{1}{4}$.

(ii) $\left(x + \frac{1}{x}\right)^2 + \left(y + \frac{1}{y}\right)^2 \geq \frac{25}{2}$.

5.3 More Advanced Examples

We conclude this chapter with a section devoted to some examples drawn from more advanced mathematics. This is not to say that the proofs themselves are necessarily more difficult than those of the previous section, just that the subject matter is more sophisticated. It is not our intention that all readers will be interested in or equipped to follow all of these. However, we expect that many of our readers will be required to produce proofs in 'higher mathematics', so we hope these examples will be useful.

Examples 5.6

1. We shall prove a result about symmetric matrices. (See the appendix for the relevant matrix terminology.)

Theorem: *For all matrices* $\mathbf{A}$, $\mathbf{A}^T\mathbf{A}$ *is symmetric.*

To begin with, we may look at a couple of examples to get a feel for what is going on.

Let $\mathbf{A} = \begin{pmatrix} 2 & -1 \\ 7 & 5 \end{pmatrix}$, then $\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} 2 & 7 \\ -1 & 5 \end{pmatrix}$

so $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \begin{pmatrix} 2 & 7 \\ -1 & 5 \end{pmatrix}\begin{pmatrix} 2 & -1 \\ 7 & 5 \end{pmatrix} = \begin{pmatrix} 53 & 33 \\ 33 & 26 \end{pmatrix}$

which is clearly symmetric.

We might try an example with a non-square matrix.

Let $\mathbf{B} = \begin{pmatrix} 3 & -4 & 0 \\ 1 & 6 & -5 \end{pmatrix}$, then $\mathbf{B}^{\mathrm{T}} = \begin{pmatrix} 3 & 1 \\ -4 & 6 \\ 0 & -5 \end{pmatrix}$

so $\mathbf{B}^{\mathrm{T}}\mathbf{B} = \begin{pmatrix} 3 & 1 \\ -4 & 6 \\ 0 & -5 \end{pmatrix}\begin{pmatrix} 3 & -4 & 0 \\ 1 & 6 & -5 \end{pmatrix} = \begin{pmatrix} 10 & -6 & -5 \\ -6 & 52 & -30 \\ -5 & -30 & 25 \end{pmatrix}$

which again is symmetric.

Of course, we know that examples do not prove general results. Unfortunately, the examples here have not given a great deal of insight into why $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is symmetric. We might be tempted to work more generally:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\mathrm{T}}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ba + dc & c^2 + d^2 \end{pmatrix}$$

which is symmetric since $ab + cd = ba + dc$. However such an argument is not acceptable for a general proof as it refers only to 2×2 matrices. (It is the basis of a proof in the 2×2 case, but not one that is very useful because it does not easily generalise to $n \times n$ matrices.)

Since the examples have not helped us a great deal, we are forced back to basics. We need to show that $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is symmetric. How can we show that a matrix is symmetric? According to the definition of a symmetric matrix, we need to show that the transpose of the matrix is equal to the matrix itself. Since $\mathbf{A}^{\mathrm{T}}\mathbf{A}$ is a product, we turn to the background information regarding the transpose of a product: $(\mathbf{AB})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$. For the product $\mathbf{A}^{\mathrm{T}}\mathbf{A}$, this gives:

$$(\mathbf{A}^{\mathrm{T}}\mathbf{A})^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}}(\mathbf{A}^{\mathrm{T}})^{\mathrm{T}}.$$

But we also know that $(\mathbf{A}^T)^T = \mathbf{A}$, so that $\mathbf{A}^T(\mathbf{A}^T)^T = \mathbf{A}^T\mathbf{A}$ and we are 'back to' our original matrix. All the pieces are now in place and we can write what is, in fact, a very simple proof.

Proof

Let $\mathbf{A}$ be any matrix. Then

$$\begin{aligned}(\mathbf{A}^T\mathbf{A})^T &= \mathbf{A}^T(\mathbf{A}^T)^T \quad (\text{since } (\mathbf{AB})^T = \mathbf{B}^T\mathbf{A}^T)\\ &= \mathbf{A}^T\mathbf{A} \qquad (\text{since } (\mathbf{A}^T)^T = \mathbf{A}).\end{aligned}$$

Since $\mathbf{A}^T\mathbf{A}$ equals its own transpose, $\mathbf{A}^T\mathbf{A}$ is symmetric.

□

2. It is often in courses in analysis where we are first required to produce rigorous proofs—and are tested on them. When they are first encountered, proofs of convergence, continuity, differentiability and the like often present profound difficulties. Therefore we present in some detail the reasoning which might go into the construction of a typical such proof.

Theorem: *Let $\{a_n\}$ and $\{b_n\}$ be two convergent sequences of real numbers with limits a and b respectively. Then the sequence $\{a_n + b_n\}$ is also convergent with limit $a + b$.*

As usual, before even thinking about the proof, we must understand the terms used in the theorem. A sequence $\{a_n\}$ **converges** to a **limit** a if, given any $\varepsilon > 0$ there exists a positive real number[3] N such that:

$$n > N \Rightarrow |a_n - a| < \varepsilon.$$

This definition is the mathematical way of formulating the intuitive notion that we can make the distance between a_n and the limit a as small as we like ($|a_n - a| < \varepsilon$) provided we take n sufficiently large ($n > N$). Put more colloquially, by travelling far enough down the sequence, the difference between a_n and the limit becomes arbitrarily small.

Now that we have (hopefully) understood the terms employed in the theorem, we must unravel its structure. The theorem is a conditional

[3] Some authors require N to be a positive integer. However, this is not necessary and the proofs are slightly simpler without this requirement.

where the antecedent is the conjunction of

$$\{a_n\} \quad \text{is a real sequence which converges to } a$$

and

$$\{b_n\} \quad \text{is a real sequence which converges to } b$$

and the consequent is

$$\text{the sequence } \{a_n + b_n\} \text{ converges to } a + b.$$

Thus, in the proof, we assume that $\{a_n\}$ is a real sequence which converges to a and we assume that $\{b_n\}$ is a real sequence which converges to b. From these assumptions, we need to deduce that the sequence $\{a_n + b_n\}$ converges to $a + b$.

Working forwards, we know that whatever positive real numbers ε_1 and ε_2 we care to choose, there exist positive real numbers N_1 and N_2 such that

$$n > N_1 \Rightarrow |a_n - a| < \varepsilon_1 \quad \text{and} \quad n > N_2 \Rightarrow |b_n - b| < \varepsilon_2.$$

Working backwards, we must show that given any positive real number ε we should be able to find a positive real number N such that

$$n > N \Rightarrow |(a_n + b_n) - (a + b)| < \varepsilon.$$

Now to show $|(a_n + b_n) - (a + b)| < \varepsilon$ we must surely need to use the inequalities $|a_n - a| < \varepsilon_1$ and $|b_n - b| < \varepsilon_2$ (given in the forward step) so we try splitting up the term $|(a_n + b_n) - (a + b)|$. We have

$$|(a_n + b_n) - (a + b)| = |a_n + b_n - a - b| = |(a_n - a) + (b_n - b)|$$

and, using the result of Example 5.3,

$$|(a_n - a) + (b_n - b)| \leq |a_n - a| + |b_n - b|.$$

Therefore

$$|(a_n + b_n) - (a + b)| \leq |a_n - a| + |b_n - b|.$$

From our forwards step, we know that we can control the size of each of the terms $|a_n - a|$ and $|b_n - b|$ on the right-hand side of this inequality. To make their sum less than ε it would be sufficient to make each of these terms less than $\varepsilon/2$. So, working forwards, we take $\varepsilon_1 = \varepsilon/2 = \varepsilon_2$.

Then there exist positive real numbers N_1 and N_2 such that

$$n > N_1 \Rightarrow |a_n - a| < \frac{\varepsilon}{2} \quad \text{and} \quad n > N_2 \Rightarrow |b_n - b| < \frac{\varepsilon}{2}.$$

We have almost joined the forward and backward processes together. The only remaining hurdle is that these two inequalities must be true simultaneously. This can be achieved by taking n to be greater than the larger of the two numbers N_1 and N_2.

All the pieces for the proof are now in place, but our forwards and backwards approach has left a rather messy trail of disjointed pieces of reasoning. In the finished proof, we need to organise these into a coherent path from beginning to end.

First proof

Suppose that $\{a_n\}$ and $\{b_n\}$ are two convergent sequences of real numbers with limits a and b respectively.

Let ε be any positive real number.

Then $\varepsilon/2 > 0$ so, by the definition of convergence for sequences, there exist positive real numbers N_1 and N_2 such that

$$n > N_1 \Rightarrow |a_n - a| < \frac{\varepsilon}{2} \quad \text{and} \quad n > N_2 \Rightarrow |b_n - b| < \frac{\varepsilon}{2}.$$

Define $N = \max\{N_1, N_2\}$. Then, provided $n > N$ we have both $n > N_1$ and $n > N_2$, so that $|a_n - a| < \varepsilon/2$ and $|b_n - b| < \varepsilon/2$.

If $n > N$ then

$$\begin{aligned} |(a_n + b_n) - (a + b)| &= |(a_n - a) + (b_n - b)| \\ &\leq |a_n - a| + |b_n - b| \qquad \text{(from Example 5.3)} \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Therefore, by definition, $\{a_n + b_n\}$ converges to limit $a + b$.

□

The proof as presented is the standard one which would be found in most introductory books on analysis. However, it does not really reflect the discovery process. The following version of the proof is structured in a more top-down manner. Although slightly longer than the first proof, it could be argued that in the second version it is easier

to understand the structure of the proof and how the definition of convergence is being used.

Second proof

Suppose that $\{a_n\}$ and $\{b_n\}$ are two convergent sequences of real numbers with limits a and b respectively.

We need to show that $\{a_n + b_n\}$ converges to limit $a + b$. In other words, given any positive real number ε, we must find a positive real number N such that

$$n > N \Rightarrow |(a_n + b_n) - (a + b)| < \varepsilon.$$

Now

$$\begin{aligned} |(a_n + b_n) - (a + b)| &= |(a_n - a) + (b_n - b)| \\ &\leq |a_n - a| + |b_n - b| \qquad \text{(from Example 5.3).} \end{aligned}$$

Therefore

$$|(a_n + b_n) - (a + b)| < \varepsilon \text{ provided } |a_n - a| < \frac{\varepsilon}{2} \text{ and } |b_n - b| < \frac{\varepsilon}{2} \quad (1)$$

Since $\{a_n\}$ converges to a, there exists a positive real number N_1 such that $n > N_1 \Rightarrow |a_n - a| < \varepsilon/2$. Similarly, since $\{b_n\}$ converges to b, there exists a positive real number N_2 such that $n > N_2 \Rightarrow |b_n - b| < \varepsilon/2$.

Let $N = \max\{N_1, N_2\}$.

Then $$\begin{aligned} n > N &\Rightarrow n > N_1 \text{ and } n > N_2 \\ &\Rightarrow |a_n - a| < \frac{\varepsilon}{2} \text{ and } |b_n - b| < \frac{\varepsilon}{2} \\ &\Rightarrow |(a_n + b_n) - (a + b)| < \varepsilon \quad \text{(from (1)).} \end{aligned}$$

□

3. Our last example in this section comes from group theory. (The basic terminology of group theory is given in the appendix.)

Theorem: *Let G be any group. For all $x, y \in G$, $(xy)^{-1} = y^{-1}x^{-1}$.*

Learning from our experience with Example 1 above, we shall not begin this time with a consideration of examples. Instead, let's first

try to understand clearly what the theorem is saying. Since x and y are elements of the group, so too is xy. The theorem is concerned with inverses, so we shall need to use axiom G3. This gives the defining property of inverses: $h = g^{-1}$ if and only if $hg = e = gh$. In other words, in order to show one element of a group is an inverse of another element, we need to show that their product (both ways round) is the identity e. In the theorem, to show $y^{-1}x^{-1}$ is an inverse of xy we need to verify

$$(xy)(y^{-1}x^{-1}) = e \text{ and } (y^{-1}x^{-1})(xy) = e,$$

We consider one of these expressions: $(xy)(y^{-1}x^{-1})$. If we could ignore the brackets, then we could proceed as follows:

$$\begin{aligned} xyy^{-1}x^{-1} &= xex^{-1} && \text{(since } yy^{-1} = e \text{ by G3)} \\ &= xx^{-1} && \text{(since } xe = x \text{ by G2)} \\ &= e && \text{(since } xx^{-1} = e \text{ by G3).} \end{aligned}$$

This is precisely what we wanted to show. However, we have just assumed we may ignore the brackets and combine pairs of elements in any sequence we find convenient. In order to deal properly with the brackets, we need to make use of G1. We are ready to write down our proof.

Proof

Let $x, y \in G$. To show $(xy)^{-1} = y^{-1}x^{-1}$ we need to verify

$$(xy)(y^{-1}x^{-1}) = e \text{ and } (y^{-1}x^{-1})(xy) = e.$$

For the first of these:

$$\begin{aligned} (xy)(y^{-1}x^{-1}) &= ((xy)y^{-1})x^{-1} && \text{(by G1)} \\ &= (x(yy^{-1}))x^{-1} && \text{(by G1)} \\ &= (xe)x^{-1} && \text{(by G3)} \\ &= xx^{-1} && \text{(by G2)} \\ &= e && \text{(by G3).} \end{aligned}$$

The second equation $(y^{-1}x^{-1})(xy) = e$ is verified in an entirely similar manner. The details are left as an exercise.

Since we have shown $(xy)(y^{-1}x^{-1}) = e$ and $(y^{-1}x^{-1})(xy) = e$, it follows from G3 that

$$(xy)^{-1} = y^{-1}x^{-1}.$$

□

Our proof is more-or-less the standard one given in most introductory texts of group theory. Most books would omit the brackets, however, and present the simplified argument given prior to our proof. This is justifiable provided it is realised that a product $x_1x_2 \ldots x_n$ in a group is not ambiguous as any way of bracketing the terms produces the same element of the group. (This can be proved using the second principle of mathematical induction—see Section 9.2—although the proof is somewhat messy and it is rarely, if ever, given.)

To conclude, we summarise some of the tips offered in the course of the chapter (which are not listed in any particular order).

Summary of important points

1. Try some examples, but remember that an example does not prove a general result.
2. Try specialising to a particular case which can be more fully understood, then generalise to the more general situation.
3. Try to think of similar or analogous theorems the method of whose proof is known.
4. If the theorem is a conditional, try working backwards from the consequent as well as forwards from the antecedent.
5. Where appropriate, draw a diagram.
6. When writing a proof, explain the steps using words as well as symbols. It is better to give too much explanation than not enough.
7. When writing a proof, consider a top-down approach.

Exercises 5.3

1. Two elements x, y of a group G are said to **commute** if $xy = yx$. Prove that, if x and y commute then:

(i) x^{-1} and y^{-1} commute.

(ii) $g^{-1}xg$ and $g^{-1}yg$ commute for all elements g of the group G.

2. Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices and define $\mathbf{A} * \mathbf{B} = \mathbf{AB} - \mathbf{BA}$. Prove that, for all $n \times n$ matrices:

(i) $\mathbf{A} * \mathbf{B} = -\mathbf{B} * \mathbf{A}$.

(ii) $\mathbf{A} * (\mathbf{B} + \mathbf{C}) = (\mathbf{A} * \mathbf{B}) + (\mathbf{A} * \mathbf{C})$.

(iii) $\mathbf{A} * (\mathbf{BC}) = (\mathbf{A} * \mathbf{B})\mathbf{C} + \mathbf{B}(\mathbf{A} * \mathbf{C})$.

3. (a) Let G be a group and x an element of G. Show that, if $|x| = 6$ then $|x^2| = 3$, $|x^3| = 2$, $|x^4| = 3$ and $|x^5| = 6$.

(b) Let G be a group and x and y be elements of G. Show that, if $x \neq e$, $y \neq e$, $x^6 = e$, $x^{28} = e$ and $xyx = y^2$ then $|x| = 2$ and $|y| = 3$.

(See the appendix for the definition of the order, $|x|$, of $x \in G$.)

4. An $n \times n$ matrix $\mathbf{B}$ is said to be **anti-symmetric** if $\mathbf{B}^{\mathrm{T}} = -\mathbf{B}$. Prove that, if $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{P}$ are $n \times n$ matrices such that $\mathbf{A}$ is symmetric and $\mathbf{B}$ is anti-symmetric, then:

(i) $\mathbf{A}^2$ is symmetric.

(ii) $\mathbf{B}^2$ is symmetric.

(iii) $\mathbf{A} * \mathbf{B} = \mathbf{AB} - \mathbf{BA}$ is symmetric (see Exercise 2, above).

(iv) $\mathbf{P}^{\mathrm{T}}\mathbf{AP}$ is symmetric.

(v) $\mathbf{P}^{\mathrm{T}}\mathbf{BP}$ is anti-symmetric.

5. Let $\{a_n\}$ and $\{b_n\}$ be two convergent sequences of real numbers with limits a and b respectively. Prove each of the following.

(i) The sequence $\{2a_n\}$ converges to limit $2a$.

(ii) More generally, if k is any real number then the sequence $\{ka_n\}$ converges to limit ka.

Note: the case $k = 0$ needs to be treated as a special case. Why?

(iii) The sequence $\{a_n - b_n\}$ converges to limit $a - b$.

(iv) If k and l are real numbers then the sequence $\{ka_n + lb_n\}$ converges to limit $ka + lb$.

Note: remember that you can use any previously proved theorems. In particular, Example 5.6.2 and part (ii) may be useful here.

(v) The sequence $\{a_n b_n\}$ converges to limit ab.

(vi) If $b \neq 0$ then the sequence $\{1/b_n\}$ converges to limit $1/b$.

(vii) If $b \neq 0$ then the sequence $\{a_n/b_n\}$ converges to limit a/b.

Hint: use parts (v) and (vi).

6. Let x and y be elements of a group G such that $y^{-1}x^2y = x^3$ and $x^{-1}y^2x = y^3$. Show that $x = y = e$.

7. An $n \times n$ matrix $\mathbf{A}$ is **orthogonal** if $\mathbf{A}^{\mathrm{T}} = \mathbf{A}^{-1}$ or, equivalently, $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \mathbf{I}_n$, where $\mathbf{I}_n$ is the $n \times n$ identity matrix. Show that if $\mathbf{A}$ and $\mathbf{B}$ are orthogonal $n \times n$ matrices, then $\mathbf{A}^{\mathrm{T}}\mathbf{B}$ is also orthogonal.

8. Let X be a non-empty set. A **metric** on X is a distance function d, i.e. for all $x, y \in X$, $d(x,y)$ is a real number such that the following four axioms are satisfied.

M1. $d(x,y) \geq 0$ for all $x, y \in X$.

M2. $d(x,y) = 0 \Leftrightarrow x = y$ for all $x, y \in X$.

M3. $d(x,y) = d(y,x)$ for all $x, y \in X$.

M4. $d(x,z) \leq d(x,y) + d(y,z)$ for all $x, y, z \in X$.

(a) Try to understand what each of these axioms is saying in the case of the usual distance between points in the plane $\mathbb{R}^2$.

(The set $\mathbb{R}^2$ together with usual distance function is a model of the axiom system.)

(b) Prove that, for all $x, y, z, t \in X$,
(i) $|d(x,z) - d(y,z)| \leq d(x,y)$.
(ii) $d(x,z) + d(y,t) \geq |d(x,y) - d(z,t)|$.

(c) Prove that axiom M1 is redundant. In other words, show that M1 follows from the other axioms: $(M2 \wedge M3 \wedge M4) \Rightarrow M1$.

Hint: use M4 with $x = z$.

(d) Show that $d(x,y) = |x - y|$ defines a metric on $\mathbb{R}$.

(e) Let X be any non-empty set and let d be defined by:

$$d(x,y) = \begin{cases} 0 \text{ if } x = y \\ 1 \text{ if } x \neq y. \end{cases}$$

Show that d is a metric on X. (This metric is called the **discrete metric** on the set X.)

9. Given two $n \times n$ matrices **A** and **B**, we say that **A** is **similar** to **B** if there exists a non-singular (invertible) matrix **P** such that $\mathbf{B} = \mathbf{P}^{-1}\mathbf{AP}$. Prove the following for all $n \times n$ matrices **A**, **B** and **C**.

(i) **A** is similar to itself.
(ii) If **A** is similar to **B** then **B** is similar to **A**.
(iii) If **A** is similar to **B** and **B** is similar to **C**, then **A** is similar to **C**.

Note: These three results together show that the relation of similarity on the set of $n \times n$ matrices is an equivalence relation.

10. The completeness axiom for $\mathbb{R}$.

Let S be a non-empty subset of the real numbers $\mathbb{R}$. A **supremum** for S is a real number α which satisfies the following two conditions:

S1. For all $s \in S, \alpha \geq s$.

S2. If β is any real number such that $\beta \geq s$ for all $s \in S$, then $\alpha \leq \beta$.

The property S1 says that α is at least as large as every element of S and the property S2 says that α is the smallest real number with the property S1. If α is the supremum of S, we write $\alpha = \sup S$.

A non-empty subset S of $\mathbb{R}$ is **bounded above** if there exists $\alpha \in \mathbb{R}$ satisfying S1. The **completeness axiom** for $\mathbb{R}$ states that every non-empty subset of $\mathbb{R}$ which is bounded above has a supremum.

(a) Show that $\sup\{1 - 1/n : n \in \mathbb{Z}^+\} = 1$.

Prove each of the following for all non-empty subsets A and B of $\mathbb{R}$ which are bounded above.

(b) If $A \subseteq B$ then $\sup A \leq \sup B$.

(c) If $x \in \mathbb{R}$ and $B = \{x + a : a \in \mathbb{R}\}$ then $\sup B = x + \sup A$.

(d) If $x \in \mathbb{R}$, $x \geq 0$ and $B = \{xa : a \in \mathbb{R}\}$ then $\sup B = x \sup A$.

The **infimum** of a non-empty subset S of $\mathbb{R}$ denoted $\inf S$, is defined by interchanging $\geq$ and $\leq$ in the definition of supremum.

(e) Let $A \subseteq \mathbb{R}$ be non-empty and bounded above and let $B = \{-a : a \in A\}$. Show that $\sup B = -\inf A$.

Deduce that every non-empty subset of $\mathbb{R}$ which is bounded below has an infimum.

6 Direct Proof: Variations

6.1 Introduction

In Chapter 5 we examined how we might construct a direct proof of a theorem expressible as a conditional proposition of the form $P \rightarrow Q$. We also saw how the proof design could be applied to theorems of the form $\forall x[P(x) \rightarrow Q(x)]$. However, there are conditional theorems where P (or $P(a)$) adds nothing useful to our background knowledge. In other words, the assumption of P (or $P(a)$) is not helpful in our attempt to construct a logical chain of propositions culminating in the consequent of the theorem. In such cases we must look for an alternative to the method of direct proof as described in the last chapter.

In the next section of this chapter we look at another technique for proving conditional theorems. In the following section, we will examine an important method of proof which can be applied to a variety of theorems, whether or not expressed in conditional form. In Section 6.4 we will look at proofs of theorems expressed as biconditionals. Whilst these three types of proof differ in fundamental ways, each will use the method of direct proof just as described in Chapter 5. However, this will be used to produce a proof, not of the theorem as stated, but of a proposition whose underlying propositional form is logically equivalent to that of the theorem. In other words, we use it to produce a proof of an equivalent theorem.

6.2 Proof using the Contrapositive

Recall that the replacement rule known as 'transposition' states that the conditional propositional form $p \rightarrow q$ is logically equivalent to its contrapositive $\overline{q} \rightarrow \overline{p}$ (see also Exercise 2.3.4). This means that, if we can provide a formal proof of the validity of an argument with conclusion $\overline{Q} \rightarrow \overline{P}$, then we can also prove the validity of the argument

with the same premises but with conclusion $P \to Q$. The proofs will be identical except that the latter will have $P \to Q$ appended, justified by the transposition rule.

This suggests a method by which we may prove conditional theorems of the form $P \to Q$. We simply prove $\overline{Q} \to \overline{P}$ and then infer the equivalent proposition $P \to Q$. We proceed similarly for theorems which take the form of universally quantified conditional propositional functions, i.e. theorems which can be written $\forall x[P(x) \to Q(x)]$. We prove $\neg Q(a) \to \neg P(a)$ for an arbitrary a in the universe of discourse by the direct method and infer $P(a) \to Q(a)$ by applying the transposition rule. Finally, universal generalisation allows us to infer $\forall x[P(x) \to Q(x)]$ and the theorem is proved. The structure of the underlying formal proof for theorems of each type is shown below.

Formal proof using the contrapositive

Proof of $P \to Q$		Proof of $\forall x[P(x) \to Q(x)]$	
1.	A_1 } axioms	1.	A_1 } axioms
⋮		⋮	
n.	A_n	n.	A_n
$n+1$.	T_1 } theorems	$n+1$.	T_1 } theorems
⋮		⋮	
$n+m$.	T_m	$n+m$.	T_m
$n+m+1$.	$\overline{Q}$ (CP)	$n+m+1$.	$\neg Q(a)$ (CP)
⋮		⋮	
r.	$\overline{P}$	r.	$\neg P(a)$
$r+1$.	$\overline{Q} \to \overline{P}$ $((n+m+1)-r.$ CP)	$r+1$.	$\neg Q(a) \to \neg P(a)$ $((n+m+1)-r.$ CP)
$r+2$.	$P \to Q$ $(r+1.$ Trans)	$r+2$.	$P(a) \to Q(a)$ $(r+1.$ Trans)
		$r+3$.	$\forall x[P(x) \to Q(x)]$ $(r+2.$ UG)

Proving that $P \to Q$ (or $P(a) \to Q(a)$) is a theorem via a proof of $\overline{Q} \to \overline{P}$ (or $\neg Q(a) \to \neg P(a)$) is usually thought of as an indirect method of proof. However, to prove the contrapositive, we use the method

of direct proof exactly as described in the last chapter. We add $\overline{Q}$ (or $\neg Q(a)$) to our background knowledge (axioms and theorems) and show that we can infer $\overline{P}$ (or $\neg P(a)$).

Examples 6.1

1. **Theorem:** *For every integer n, if n^2 is even, then n is even.*

(Note that this is the converse of the theorem proved in Example 5.2.2.)

The theorem may be stated $\forall x[E(x^2) \rightarrow E(x)]$ where

$E(x)$: x is even

and the universe of discourse is the integers. As usual we prove $E(n^2) \rightarrow E(n)$ where n is an arbitrary integer. Taking our cue from Example 5.2.2, we might try a direct proof of the theorem. This would commence:

Let n^2 be an even integer.
Then $n^2 = 2k$ for some integer k.

In an attempt to find out something useful about n, we might proceed with:

Hence

$$\begin{aligned} n &= \pm\sqrt{2k} \\ &= \pm\sqrt{2}\sqrt{k}. \end{aligned}$$

Now we have a problem because we cannot deduce that n has a factor 2 from this expression nor is there any obvious way of re-writing it which would reveal that it has 2 as a factor.

Our attempt at a direct proof has not been successful (although a direct proof *does* exist—see Exercise 6.1.8.). We now try and see if it is possible to prove the contrapositive, $\neg E(n) \rightarrow \neg E(n^2)$, i.e. if n is *not* even, then n^2 is *not* even. ('Not even' of course is equivalent to 'odd'.) We employ the method of direct proof: we add $\neg E(n)$ to our list of assumptions and show that we can infer $\neg E(n^2)$. The proof (which is very similar to that used in Example 5.2.2) proceeds as follows.

Proof

Let n be an odd integer.

Then

$$n = 2m + 1 \quad \text{for some integer } m$$

$$\Rightarrow \quad n^2 = (2m+1)^2$$

$$= 4m^2 + 4m + 1$$

$$= 2(2m^2 + 2m) + 1$$

$$= 2M + 1 \quad \text{where } M \text{ is an integer}$$

$$\Rightarrow \quad n^2 \text{ is odd.}$$

This completes the proof of the contrapositive. We can therefore deduce that, if n is an arbitrary integer such that n^2 is even, then n is even. It follows that, for every integer n, if n^2 is even, then n is even.

□

2. **Theorem:** *For any positive integers m and n, if $m + n$ is odd, then either m is odd or n is odd.*

Again we might commence by attempting a direct proof as follows.

Let m and n be integers such that $m + n$ is odd.
Then $m + n = 2k + 1$ for some integer k.

Here we encounter the same sort of problem as in the previous example—there is no obvious deduction to be made about the individual integers m and n. So we try instead to prove the contrapositive.

We define the following propositional functions on the universe $\mathbb{Z}^+$, the set of positive integers:

$P(m,n)$: $m + n$ is odd,
$Q(m)$: m is odd.

Then the theorem may be written: $P(m,n) \rightarrow (Q(m) \vee Q(n))$ for arbitrary integers m and n.

The consequent of the theorem is $Q(m) \vee Q(n)$. The antecedent of the contrapositive is therefore $\neg(Q(m) \vee Q(n))$ and it is this proposition which we add to our assumptions. However, in this form it is not

particularly useful because it tells us nothing about the integers m and n individually. Applying De Morgan's replacement rule, we find that this proposition is equivalent to $\neg Q(m) \wedge \neg R(n)$. Since both of $\neg Q(m)$ (m is even) and $\neg R(n)$ (n is even) can be inferred from this conjunction, we may commence our proof by assuming each of these. We then show that we can infer $\neg P(m,n) : m + n$ is even. The proof is as follows.

Proof

Suppose that m and n are even so that $m = 2r$ and $n = 2s$ for some positive integers r and s.

Then

$$\begin{aligned} m + n &= 2r + 2s \\ &= 2(r + s) \\ &= 2t \qquad \text{where } t \text{ is an integer} \\ \Rightarrow \quad & m + n \text{ is even.} \end{aligned}$$

This proves the contrapositive from which we can deduce that, for arbitrary positive integers m and n, if $m + n$ is odd, then m is odd or n is odd.

□

Exercises 6.1

Prove each of the theorems 1–7 by proving the contrapositive. For each one, also attempt a direct proof.

1. For any integer n, if n^2 is not divisible by 7, then n is not divisible by 7.

2. For any integers m and n, if mn is even, then m is even or n is even.

3. For any integers m and n, if mn is odd then m is odd and n is odd.

4. If m and n are positive integers and $mn = 100$, then either $m \leq 10$ or $n \leq 10$.

5. If a is an odd integer, then the quadratic equation $x^2 - x - a = 0$ has no roots which are integers.

6. If x is any real number such that $0 < x < 1$, then $x > x^2$.

7. If $n \in \mathbb{N}$ and $2^n - 1$ is prime, then n is prime.

8. Use the prime factorisation theorem (see Section 4.2) as background knowledge to give a direct proof of the theorem in Example 6.1.1.

6.3 Proof by Contradiction

Suppose we assume the truth of some proposition P and in so doing we find that this forces us to accept the truth of another proposition Q which is in fact known to be false. Our only option would be to re-examine our assumption that P was true. Since this led us to deduce a falsehood, we would have no alternative but to conclude that it was an incorrect assumption and that P must therefore be false. This is the basis of a proof by contradiction.

As an illustration of the method, consider the following simple example. Suppose we have the proposition:

In any group of thirteen people, there must be at least two born under the same star sign.

To prove that this is true we might argue as follows. Suppose everyone in the group is born under a *different* star sign. This implies that there are at least thirteen star signs. However we know that this is not the case—there are exactly twelve. So it cannot be that everyone is born under a different star sign and we must conclude that at least two members of the group have the same star sign.

To prove a theorem T (not necessarily a conditional) using the method of contradiction, we begin by assuming that the theorem is false and add $\overline{T}$ to our background knowledge. We then show that this leads to the deduction of a proposition which is patently false. Usually this takes the form $R \wedge \overline{R}$ for some proposition R, i.e. adding $\overline{T}$ to our axioms and theorems allows us to deduce both R and $\overline{R}$. Note that the proposition $R \wedge \overline{R}$ is a substitution instance of the propositional form $p \wedge \overline{p}$. This form is a contradiction—it is false no matter what proposition is substituted for p. If our assumption that T is false turns out to support the deduction of a proposition which is always false, then we have no alternative but to reject that assumption. We must therefore accept the truth of the theorem.

A proof by contradiction feels rather different from the methods of proof which we have described so far and it is often referred to as a 'method of indirect proof'. However, it can be shown to be another form of direct proof—again, not of the theorem as stated, but of another with

a logically equivalent underlying propositional form. The following shows the logical equivalence of $\overline{p} \to p$ and p:

$$\begin{aligned} \overline{p} \to p &\equiv \overline{\overline{p}} \vee p \quad \text{(Impl)} \\ &\equiv p \vee p \quad \text{(DN)} \\ &\equiv p \quad \text{(Taut)} \end{aligned}$$

Hence, to prove a theorem T, we may instead prove $\overline{T} \to T$. This can be achieved using a direct proof. We add $\overline{T}$, the negation of the theorem, to our axioms and theorems and show that we can deduce T. Now we can deduce a proposition T from a list of assumptions which includes its negation if we can, *en route*, deduce propositions R and $\overline{R}$. (Remember that we can deduce any proposition whatsoever in these circumstances—see Section 2.5 and Example 2.8.4.) Once we have obtained these contradictory propositions, we can deduce T and this completes the proof.

If the theorem is a universally quantified propositional function of the form $\forall x\, T(x)$ we proceed, as always, with the proof of $T(a)$ for an arbitrary a. This is achieved as described above, by proving $\neg T(a) \to T(a)$ via the deduction of a proposition together with its negation. The structure of the underlying formal proof for each of the two forms of theorem is given below.

In practice an informal proof by contradiction does not include the steps $s+1$ to $s+6$ (or $s+7$) and the proof terminates once it has been shown that it is possible to deduce the contradictory propositions R and $\overline{R}$.

In showing how this method may be used to prove a theorem, we have made no assumptions about the forms of either the proposition T or that of the propositional function $T(x)$. These may or may not be conditionals. However, it is important to note that in a proof of T by contradiction, the negation of the whole theorem is added to the list of assumptions. For example, if the theorem is of the form $P \to Q$, then the proposition to be added to the axioms and theorems is $\overline{P \to Q}$. Of course we may, if we wish, use the replacement rules and from $\overline{P \to Q}$ deduce in turn the equivalent propositions $\overline{\overline{P} \vee Q}$ (Impl), $\overline{\overline{P}} \wedge \overline{Q}$ (De M) and $P \wedge \overline{Q}$ (DN). Similarly, if the theorem is of the form $\forall x[P(x) \wedge Q(x)]$ (so that we are aiming to prove $P(a) \wedge Q(a)$ for an arbitrary a), then it is $\neg[P(a) \wedge Q(a)]$ which must be added.

Formal proof by contradiction

Proof of T			Proof of $\forall x\, T(x)$		
1.	A_1	axioms	1.	A_1	axioms
⋮			⋮		
n.	A_n		n.	A_n	
$n+1$.	T_1	theorems	$n+1$.	T_1	theorems
⋮			⋮		
$n+m$.	T_m		$n+m$.	T_m	
$n+m+1$.	$\overline{T}$ (CP)		$n+m+1$.	$\neg T(a)$ (CP)	
⋮			⋮		
r.	R		r.	R	
⋮			⋮		
s.	$\overline{R}$		s.	$\overline{R}$	
$s+1$.	$R \vee T$ (r. Add)		$s+1$.	$R \vee T(a)$ (r. Add)	
$s+2$.	T ($s, s+1$. DS)		$s+2$.	$T(a)$ ($s, s+1$. DS)	
$s+3$.	$\overline{T} \rightarrow T$ (($n+m+1$) $-(s+2)$. CP)		$s+3$.	$\neg T(a) \rightarrow T(a)$ (($n+m+1$) $-(s+2)$. CP)	
$s+4$.	$\overline{\overline{T}} \vee T$ ($s+3$. Imp)		$s+4$.	$\neg\neg T(a) \vee T(a)$ ($s+3$. Imp)	
$s+5$.	$T \vee T$ ($s+4$. DN)		$s+5$.	$T(a) \vee T(a)$ ($s+4$. DN)	
$s+6$.	T ($s+5$. Taut)		$s+6$.	$T(a)$ ($s+5$. Taut)	
			$s+7$.	$\forall x\, T(x)$ ($s+6$. UG)	

Note that, although it might appear that we have deduced the theorem at line $s+2$ of the proof, this is not the case. At this stage we are still involved in the conditional proof so that the correct deduction is $\overline{T} \rightarrow T$ or $\neg T(a) \rightarrow T(a)$.

Whilst we have justified proof by contradiction by appealing to the laws of logic, the method makes intuitive sense. We show that, if we assume that the theorem is false then 'nonsense' (in the form of a contradictory pair of propositions) follows. We therefore deduce that the theorem cannot be false. Because it necessitates the inference of an 'absurdity', the method is often known by its latin name *reductio ad absurdum*. It

was this method of proof which the great mathematician G. H. Hardy (1877–1947) viewed as '... one of a mathematician's finest weapons'. He went on to say: 'It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but the mathematician offers *the game.*'

In our first illustration of a proof by contradiction, we prove that the square root of 2 is not a rational number. This is probably one of the best known examples of this method of proof. The second example is also generally regarded as a classic example of a proof by contradiction. The theorem states that there are an infinite number of prime numbers and this particular proof is attributed to Euclid.

Examples 6.2

1. **Theorem:** *The square root of* 2 *is not rational.*

We first note that the statement of this theorem is not a conditional nor could it be converted to a conditional in any useful way. Methods of proof appropriate to conditional theorems are therefore not likely to succeed. The other problem is that it is often difficult to show that something is *not* the case. This is particularly so in this example where, to prove that $\sqrt{2}$ is not rational, we must rule out infinitely many possibilities of the form p/q $(q \neq 0)$. However, from assuming that $\sqrt{2}$ *is* rational there are things which we can deduce and, with luck, these may lead to a contradiction.

To commence our proof by contradiction, we add the negation of the theorem to our assumptions. This proposition states that $\sqrt{2}$ is rational. We can then use as background knowledge the theorem which states that any rational number can be written as m/n, where m and n are integers with no common factors and $n \neq 0$. The proof proceeds as follows. Note that it also uses as background knowledge the result proved in Example 6.1.1: if n is any integer and n^2 is even, then n is even.

Proof

Suppose that $\sqrt{2}$ is rational.

Then

$$\sqrt{2} = \frac{m}{n} \qquad \text{where } m, n \text{ are integers with no common factors and } n \neq 0$$

$$\Rightarrow \quad 2 = \frac{m^2}{n^2}$$

$$\Rightarrow \quad 2n^2 = m^2$$

$$\Rightarrow \quad m^2 \text{ is even}$$

$$\Rightarrow \quad m \text{ is even} \qquad \text{(see Example 6.1.1 above)}$$

$$\Rightarrow \quad m = 2r \qquad \text{for some integer } r$$

$$\Rightarrow \quad m^2 = 4r^2$$

$$\Rightarrow \quad 2n^2 = 4r^2 \qquad \text{(since } 2n^2 = m^2\text{)}$$

$$\Rightarrow \quad n^2 = 2r^2$$

$$\Rightarrow \quad n^2 \text{ is even}$$

$$\Rightarrow \quad n \text{ is even.}$$

We have shown that both m and n are even, i.e. they have a common factor. But this contradicts our earlier deduction that m and n had no common factors. Hence the assumption that $\sqrt{2}$ is rational must be false and so $\sqrt{2}$ is irrational.

□

2. **Theorem:** *There is an infinite number of prime numbers.*

The difficulties here are associated with the need to establish the existence of an *infinite* number of primes. In the previous example there were infinitely many possibilities which needed to be 'ruled out'. Here we need to 'rule in' (to the category of prime numbers) infinitely many integers. However, from assuming that the number of primes is finite there is the possibility that we might be able to produce a chain of deductions leading to a contradiction.

Proof

We first assume the negation of the theorem, i.e. that there is a finite number of prime numbers. We can therefore list these: $p_1, p_2, \ldots, p_n$.

Now consider P, the product of all the prime numbers.

$$P = p_1 p_2 \ldots p_n$$

$$\Rightarrow \qquad P + 1 = p_1 p_2 \ldots p_n + 1.$$

Now $P + 1$ is not prime since it is different from $p_1, p_2, \ldots, p_n$ and these are the only prime numbers. Applying the prime factorisation theorem (see Section 4.2) we conclude that $P + 1$ must be divisible by one of $p_1, p_2, \ldots, p_n$ so that we can write

$$P + 1 = p_r Q \quad \text{for some } r \text{ such that } 1 \leq r \leq n.$$

But
$$\begin{aligned} P &= p_1 \ldots p_r \ldots p_n \\ &= p_r(p_1 \ldots p_{r-1} p_{r+1} \ldots p_n) \\ &= p_r S \quad \text{where } S = p_1 p_2 \ldots p_{r-1} p_{r+1} \ldots p_n \end{aligned}$$

$$\Rightarrow \qquad P + 1 = p_r S + 1.$$

Hence $P + 1$ gives a remainder of 1 when divided by p_r and so is not divisible by p_r. The contradiction has surfaced and we can therefore infer the theorem, i.e. the number of primes is infinite.

□

The method of proof by contradiction is very commonly used to prove the uniqueness of some property, i.e. that there is only one element of the universe having the given property. We shall look at such proofs in Chapter 7.

Exercises 6.2

1. In a proof by contradiction, we assume the negation of the theorem $\overline{T}$ and show that this allows us to infer a proposition with a contradiction f as its underlying propositional form. Use the replacement rules together with any of the rules established in Exercise 2.3.8(a) to show that $\overline{p} \rightarrow f \equiv p$. (This provides another justification for the method of proof by contradiction.)

Prove each of the following theorems using proof by contradiction.

2. For any integers m and n where $n \neq 0, m + \sqrt{2}n$ is not rational.

3. The smallest factor greater than 1 of any integer $n > 1$ is prime.

4. For any set $A, \varnothing \subseteq A$.

5. For any sets A and B, $(A - B) \cap B = \varnothing$.

6. Prove the theorem used in Example 5.2.1: if n is an integer greater than 1 which has no factor k where k is prime and $2 \leq k \leq \sqrt{n}$, then n is prime. (Use a proof by contradiction to prove the contrapositive.)

7. Use the probability axioms together with any of the theorems given in Exercise 4.3.4 to prove that, for any event A, $0 \leq p(A) \leq 1$.

8. Let $A_1, A_2, \ldots, A_n$ be a collection of sets and define

$$\begin{aligned} B_1 &= A_1 \\ B_2 &= A_2 - A_1 \\ B_3 &= A_3 - (A_1 \cup A_2) \\ &\vdots \\ B_n &= A_n - (A_1 \cup A_2 \cup \cdots \cup A_{n-1}). \end{aligned}$$

Prove that $B_i \cap B_j = \varnothing$ for all $i \neq j$.

9. Let $\{x_n\}$ be a real sequence with limit l. Prove that, if $x_n \geq a$ for all n, then $l \geq a$.

10. Prove that the set $\{1 - 1/n : n \in \mathbb{Z}^+\}$ has no greatest element. (Compare with Exercise 5.3.10(a).)

11. Let G be a group with 6 elements, i.e. $|G| = 6$. Prove that G has no element of order 5.

12. Let $\{a_n\}$ be the sequence defined by $a_n = (-1)^n$.

(a) Prove that $\{a_n\}$ does not converge to limit $l = 1$.
(b) Prove that $\{a_n\}$ does not converge to any limit l.
(The definition of a limit of a sequence is given on page 156.)

13. Use the completeness axiom for $\mathbb{R}$ (see Exercise 5.3.10) to prove that the set $\mathbb{N}$ of natural numbers is not bounded above. (This is called the **Archimedean property of** $\mathbb{N}$.)

6.4 Proof of a Biconditional

If we are required to provide a formal proof of a biconditional proposition of the form $P \leftrightarrow Q$ it suffices to deduce each of the two conditionals $P \rightarrow Q$ and its converse $Q \rightarrow P$. We can then use the

inference rule referred to as 'conjunction' to infer $(P \to Q) \wedge (Q \to P)$ and then 'material equivalence' to infer $P \leftrightarrow Q$. Hence to prove a biconditional theorem of the form $P \leftrightarrow Q$, we prove that $P \to Q$ and $Q \to P$ are each theorems. If the theorem is a quantified biconditional of the form $\forall x[P(x) \leftrightarrow Q(x)]$ we proceed in the usual way and prove that, for an arbitrary a in the universe, $P(a) \to Q(a)$ and $Q(a) \to P(a)$ are true propositions. The application of the same two inference rules allows us to infer $P(a) \leftrightarrow Q(a)$ and the theorem follows after applying universal generalisation. The proof of a biconditional theorem therefore involves the proof of two conditional 'sub-theorems'. Of course each of these individual conditionals may be proved by any of the methods which we have described. The structure of the formal proofs underlying the method are shown below.

Formal proof of a biconditional

Proof of $P \leftrightarrow Q$

1.	A_1	} axioms
⋮		
n.	A_n	
$n+1$.	T_1	} theorems
⋮		
$n+m$.	T_m	
⋮		
r.	$P \to Q$	
⋮		
s.	$Q \to P$	
$s+1$.	$(P \to Q) \wedge (Q \to P)$	$(r, s.$ Conj$)$
$s+2$.	$P \leftrightarrow Q$	$(s+1.$ Equiv$)$

Proof of $\forall x[P(x) \leftrightarrow Q(x)]$

1.	A_1	} axioms
⋮		
n.	A_n	
$n+1$.	T_1	} theorems
⋮		
$n+m$.	T_m	
⋮		
r.	$P(a) \to Q(a)$	
⋮		
s.	$Q(a) \to P(a)$	
$s+1$.	$(P(a) \to Q(a)) \wedge (Q(a) \to P(a))$	$(r, s.$ Conj$)$
$s+2$.	$P(a) \leftrightarrow Q(a)$	$(s+1.$ Equiv$)$
$s+3$.	$\forall x[P(x) \leftrightarrow Q(x)]$	(s+2. UG)

Biconditional theorems of the form $P \leftrightarrow Q$ are normally expressed as 'P if and only if Q' and are often abbreviated to 'P iff Q'. Recall that an alternative expression is 'P is a necessary and sufficient condition for Q'.

Examples 6.3

1. **Theorem:** *For any integer n, n^2 is even if and only if n is even.*

Proof

This theorem can be symbolised $\forall x\,[E(x^2) \leftrightarrow E(x)]$ where $E(x)$ denotes 'x is even' and the universe is the integers. In Example 5.2.2 we provided a direct proof of the theorem: for any integer n, if n is even then n^2 is even. Example 6.1.1 gives a proof (using the contrapositive) of: for any integer n, if n^2 is even then n is even.

Since we have proofs of $E(n^2) \rightarrow E(n)$ and of $E(n) \rightarrow E(n^2)$, we can splice them together to produce the proof of $E(n) \leftrightarrow E(n^2)$.

We can therefore infer the theorem: for any integer n, n^2 is even if and only if n is even.

□

2. **Theorem:** $2x^2 + 3x - 1 = x^2 + 8x - 5$ *iff* $x = 4$ *or* $x = 1$.

Proof

We first prove that, if $2x^2 + 3x - 1 = x^2 + 8x - 5$, then $x = 4$ or $x = 1$. The proof is simply a matter of showing that these two values of x are roots of the quadratic equation.

$$
\begin{aligned}
& 2x^2 + 3x - 1 = x^2 + 8x - 5 \\
\Rightarrow \quad & x^2 - 5x + 4 = 0 \\
\Rightarrow \quad & (x - 4)(x - 1) = 0 \\
\Rightarrow \quad & x = 4 \text{ or } x = 1.
\end{aligned}
$$

To complete the proof of the biconditional, we must now show that, if $x = 4$ or $x = 1$, then $2x^2 + 3x - 1 = x^2 + 8x - 5$. Of course, this could be achieved by evaluating each side of the equation for $x = 1$ and $x = 4$ and demonstrating the equality. Alternatively, we may proceed as follows:

$$
\begin{aligned}
& x = 4 \text{ or } x = 1 \\
\Rightarrow \quad & (x - 4)(x - 1) = 0
\end{aligned}
$$

$$\begin{aligned} \Rightarrow \quad & x^2 - 5x + 4 = 0 \\ \Rightarrow \quad & 2x^2 + 3x - 1 = x^2 + 8x - 5. \end{aligned}$$

□

Notice that the second part of the proof consists of exactly the same steps as the first part, but with the order reversed. We can therefore condense both parts of the proof neatly into the following alternative proof.

Proof

$$\begin{aligned} & 2x^2 + 3x - 1 = x^2 + 8x - 5 \\ \Leftrightarrow \quad & x^2 - 5x + 4 = 0 \\ \Leftrightarrow \quad & (x-4)(x-1) = 0 \\ \Leftrightarrow \quad & x = 4 \text{ or } x = 1. \end{aligned}$$

□

3. **Theorem:** *For any sets A and B, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.*

(This theorem is known as De Morgan's law for sets. Note the similarity with De Morgan's replacement rule.)

The usual way of proving that two sets X and Y are equal is to prove that $X \subseteq Y$ and that $Y \subseteq X$. As we saw in Example 5.2.3, to prove that $X \subseteq Y$ we need to show that, if x is an arbitrary element of X then $x \in Y$. To prove the theorem therefore, we must show that if $x \in \overline{A \cup B}$ then $x \in \overline{A} \cap \overline{B}$ and also that if $x \in \overline{A} \cap \overline{B}$ then $x \in \overline{A \cup B}$. In other words, we must prove the biconditional $x \in \overline{A \cup B}$ iff $x \in \overline{A} \cap \overline{B}$. As in the last example the proofs of the two conditional 'subtheorems' contain exactly the same steps but reversed. We can therefore write the proof as follows.

Proof

$$\begin{aligned} & x \in \overline{A \cup B} \\ \Leftrightarrow \quad & x \notin A \cup B \\ \Leftrightarrow \quad & x \notin A \text{ and } x \notin B \\ \Leftrightarrow \quad & x \in \overline{A} \text{ and } x \in \overline{B} \\ \Leftrightarrow \quad & x \in \overline{A} \cap \overline{B}. \end{aligned}$$

Hence $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ and $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$ so that $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

□

Of course, if a proof of $P \rightarrow Q$ can be reversed to prove $Q \rightarrow P$, then our task of producing a proof of $P \leftrightarrow Q$ is greatly simplified. However, for most biconditional theorems, this is not the case. For example, note that the proof of the theorem 'if n is an even integer, then n^2 is an even integer' (Example 5.2.2) cannot readily be reversed to produce a proof of the converse 'if n^2 is an even integer, then n is an even integer'.

Our final example of a biconditional proof is also one where we cannot easily reverse the proof of $P \rightarrow Q$ to prove $Q \rightarrow P$.

4. **Theorem:** *For all non-empty sets A and B, $A \times B = B \times A$ if and only if $A = B$.*

Proof

Suppose that A and B are non-empty sets such that $A \times B = B \times A$.

Let $a \in A$ and choose any $b \in B$.

Then $$(a, b) \in A \times B \Rightarrow (a, b) \in B \times A$$
$$\Rightarrow a \in B.$$

Since $a \in A \Rightarrow a \in B$, we have proved that $A \subseteq B$.

Now suppose $b \in B$ and choose any $a \in A$.

Then $$(a, b) \in A \times B \Rightarrow (a, b) \in B \times A$$
$$\Rightarrow b \in A.$$

Since $b \in B \Rightarrow b \in A$, we have proved that $B \subseteq A$.

We have $A \subseteq B$ and $B \subseteq A$ so that $A = B$.

We have proved that, if $A \times B = B \times A$, then $A = B$. We now prove the converse.

Suppose that $A = B$.

Then $A \times B = A \times A = B \times A$.

Hence, if $A = B$ then $A \times B = B \times A$.

This completes the proof of the theorem.

□

Exercises 6.3

1. Prove that, for all sets A, B and C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

2. Prove that, for all sets A and B, $A \subseteq B$ is a necessary and sufficient condition for $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

3. Prove that, for all integers m and n, m and n have the same remainder when divided by 5 if and only if 5 is a factor of $m - n$.

4. Prove that, for all integers m and n, if p is prime then p is a factor of mn if and only if either p is a factor of m or p is a factor of n.

5. Prove that the line $y = mx - 2$ intersects the parabola $y = 3x^2 + 1$ iff $|m| \geq 6$. (See Exercise 5.2.3.)

6. Prove that $a = cm$ is a necessary and sufficient condition for the line $y = mx + c$ to be a tangent to the parabola $y^2 = 4ax$.

7. Prove that, if a and b are non-negative real numbers, then $a^2 \geq b^2$ iff $a \geq b$. (See Exercise 5.2.1.)

8. Suppose that $x = x_1$, $y = y_1$ is a solution of the equation $ax + by = c$. Prove that the pair $x = x_1$, $y = y_1$ is a solution of the equation $a_1x + b_1y = c_1$ if and only if it is a solution of $(a + da_1)x + (b + db_1)y = c + dc_1$ (for any $d \neq 0$).

9. Prove that a necessary and sufficient condition for the quadratic equations $a_1x^2 + b_1x + c_1 = 0$ and $a_2x^2 + b_2x + c_2 = 0$ ($a_1 \neq 0$ and $a_2 \neq 0$) to have a common root is

$$(a_1b_2 - a_2b_1)(b_1c_2 - b_2c_1) = (c_1a_2 - c_2a_1)^2.$$

10. Prove that a group G is abelian if and only if

$$(ab)^{-1} = a^{-1}b^{-1} \text{ for all } a, b \in G.$$

11. Prove that, for any sets A and B, $A \subseteq \overline{B}$ if and only if $A \cap B = \varnothing$.

12. Let $\mathbf{A}$ be a 2×2 matrix with non-zero real entries. Prove that:

(i) $\mathbf{A}^2 = \mathbf{0}_{2\times 2}$ if and only if

$$\mathbf{A} = \begin{pmatrix} a & b \\ \dfrac{-a^2}{b} & -a \end{pmatrix}$$

for some non-zero real numbers a, b.

(ii) $\mathbf{A}^2 = \mathbf{A}$ if and only if

$$\mathbf{A} = \begin{pmatrix} a & b \\ \dfrac{a(1-a)}{b} & 1-a \end{pmatrix}$$

for some non-zero real numbers a, b such that $a \neq 1$.

13. Let m and n be integers. Prove that $m + n\sqrt{2}$ is rational if and only if $n = 0$.

7 Existence and Uniqueness Proofs

7.1 Introduction

So far in this book we have concerned ourselves with the proof of theorems which are propositions P or universally quantified propositional functions, $\forall x\, P(x)$. For much of the current chapter we shall turn our attention to proofs of existence theorems—that is, theorems which assert the existence within the universe of an object or objects with a certain property, P. We can symbolise such a theorem by: $\exists x\, P(x)$.

Some examples of theorems of this form are the following.

(a) Some prime numbers are of the form $32n + 1$, where n is an integer.

(b) Some quadratic equations do not have real roots.

(c) Not all real numbers are rational.

(d) There exist sets which have the same cardinality as some of their proper subsets.

(e) There exist non-abelian simple groups.

Typically, existence theorems are stated using the phraseology 'Some...' or 'There exist...'. Notice, however, that example (c) above is expressed rather differently, as the negation of a universally quantified propositional function, $\neg\forall x\, P(x)$. The rule of quantification denial, QD (see Section 3.2), states that this is logically equivalent to $\exists x \neg P(x)$, which is an existence theorem. In our example, the equivalent existentially quantified statement may be expressed as 'Some real numbers are irrational (not rational)' or 'There exist irrational real numbers'. The manner in which these theorems are expressed seems

to suggest that they are asserting the existence of several objects of the required type. However, this is merely convention and each of the theorems could be expressed in the form 'There exists at least one object with the required property'. To prove a theorem of this type it is sufficient to demonstrate the existence of a single object of the appropriate type whether or not there actually exist many such objects. (In Section 7.5 we shall consider how we might prove that there is only one object with the required property if this is the case.)

7.2 Proof by Construction

The most obvious way to prove a theorem of the form $\exists x\, P(x)$ is to find a specific object a in the universe for which $P(a)$ is true. We can then use the rule of existential generalisation (EG) to infer the theorem $\exists x\, P(x)$. This method of proof is called **proof by construction** because we construct (or find) a specific object a with the required property. How we actually go about finding or constructing the desired object a will, of course, depend on the particular theorem under consideration. The proof of $P(a)$ may employ any of the methods we have discussed in the previous two chapters.

The underlying formal proof of a proof by construction is given in the box below.

Proof by construction

1.	A_1	axioms
⋮		
n.	A_n	
$n+1$.	T_1	theorems
⋮		
$n+m$.	T_m	
⋮		
r.	$P(a)$	
$r+1$.	$\exists x\, P(x)$	(r. UG)

The following examples illustrate the method.

Examples 7.1

1. **Theorem:** *Some prime numbers are of the form* $32n + 1$, *where* n *is an integer.*

If we define the universe of discourse to be the integers and we define propositional functions $P(x) : x$ *is prime* and $Q(x) : x = 32n + 1$, *for some integer* n, then the theorem can be symbolised as $\exists x\,[P(x) \wedge Q(x)]$. We need, therefore, to find a specific integer a for which $P(a)$ and $Q(a)$ are both true propositions. The simplest approach is to list (some of) the integers a for which $Q(a)$ is true and then find one of these for which $P(a)$ is also true. (Alternatively, we could list integers a for which $P(a)$ is true—the primes—and find one of these for which $Q(a)$ is true. However, it is easier to list integers of the form $32n + 1$ than it is to list primes, so we adopt the former approach.)

The positive integers of the form $32n + 1$ are: 1, 33, 65, 97, 129, 161, 193, ... Which, if any, of these are also prime? We begin:

$$1 \text{ is not prime (by definition),}$$

$$33 = 3 \times 11, \text{ so 33 is not prime,}$$

$$65 = 5 \times 13, \text{ so 65 is not prime.}$$

However, on testing 97 for factors (see Example 5.2.1 for a way of doing this which requires only a few potential factors to be tested), we find that 97 is, indeed, prime. Therefore we have found an object with the desired properties and we can now proceed to the proof.

Proof

$97 = 32 \times 3 + 1$ and 97 is prime.

□

The proof itself is, of course, almost trivial. It is often the case with constructive proofs that the proofs themselves are relatively simple. The hard work goes into finding the required object a, but this does not show in the written proof. In our example, we have merely exhibited an object $a = 97$ with the desired properties. We have not *proved* that 97 is prime. In other words, this is taken as part of our background knowledge of the integers. If a proof of this were deemed necessary, we could follow the method given in Example 5.2.1. In Chapters 5 and 6,

we noted frequently that the use of the rule of universal generalisation was not made explicit. Similarly, in this example, the application of the rule of existential generalisation is left to the reader. The proof simply exhibits an object a for which $P(a)$ is a true proposition. The underlying formal proof has a final line, $\exists x\, P(x)$, justified by EG.

2. **Theorem:** *Not all real numbers are rational.*

We have noted that the theorem is equivalent to the proposition: *there exists a real number which is irrational.* With universe the real numbers and denoting *'x is irrational'* by $P(x)$, the theorem may be symbolised as $\exists x\, P(x)$. In Example 6.2.1 we proved (by contradiction) that $\sqrt{2}$, is irrational. In other words, we proved $P(\sqrt{2})$, which now becomes part of our background knowledge of the real numbers. Adopting the usual practice that the application of EG is left to the reader, we therefore have the following one-line proof of the theorem.

Proof

$\sqrt{2}$ is irrational, by Example 6.2.1.

□

The hard work is first discovering that $\sqrt{2}$ is a suitable real number to consider and then proving that $\sqrt{2}$ is indeed irrational. Of course, this is hidden from view in our one-line proof.

There is also a nice non-constructive proof of this theorem, that is, a proof which does not actually produce any specific irrational real numbers. See Example 8.4.2.

3. **Theorem:** *For any positive integer n, multiplication of $n \times n$ matrices is not commutative.*

The commutative law for multiplication says that the two products xy and yx are always equal: $\forall x \forall y(xy = yx)$. The given theorem is the negation of this law for matrix multiplication (so the quantification is over the universe of matrices). Using the rule of quantification denial twice (see Section 3.2), we can show that $\neg\forall x \forall y(xy = yx)$ is equivalent to $\exists x \exists y(xy \neq yx)$. Thus, to prove the theorem, we must find two square matrices of the same dimension, **A** and **B**, with the property that $\mathbf{AB} \neq \mathbf{BA}$. Two such matrices are easily found using a little trial and error.

For simplicity, we consider 2×2 matrices. Suppose we try $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} -1 & 1 \\ 3 & 2 \end{pmatrix}$.

Then $$\mathbf{AB} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 5 \\ 9 & 11 \end{pmatrix}$$

and $$\mathbf{BA} = \begin{pmatrix} -1 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 9 & 14 \end{pmatrix}$$

so $\mathbf{AB} \neq \mathbf{BA}$. Since we have found a suitable example, we can proceed directly to a proof.

Proof

Let $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} -1 & 1 \\ 3 & 2 \end{pmatrix}$.

Then $$\mathbf{AB} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 5 \\ 9 & 11 \end{pmatrix}$$

and $$\mathbf{BA} = \begin{pmatrix} -1 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 9 & 14 \end{pmatrix}$$

so $\mathbf{AB} \neq \mathbf{BA}$.

□

In this example, trial and error easily produces elements of the universe with the required property. Indeed a random choice of matrices is likely to give the desired result. However, this will not always be the case and sometimes we really do need to sit down and carefully construct a suitable example. Staying with 2×2 matrices for simplicity, we could do this here by first considering arbitrary products and then making simple choices for the entries as follows.

First note

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} u & v \\ w & x \end{pmatrix} = \begin{pmatrix} au + bw & av + bx \\ cu + dw & cv + dx \end{pmatrix}$$

and

$$\begin{pmatrix} u & v \\ w & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ua + vc & ub + vd \\ wa + xc & wb + xd \end{pmatrix}.$$

We wish to choose the entries of the two matrices so that the two products are different. Recall that two matrices are not equal if they

differ in at least one entry. Now, since $au = ua$, we can ensure that the top-left entry of the products are different if $bw \neq vc$. A simple choice would be $b = w = 0$, $v = c = 1$. With these choices and any choice of a, d, u and x, we can construct matrices with the required property. Taking $a = d = u = x = 1$ gives matrices

$$\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ and } \mathbf{B} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

such that $\mathbf{AB} \neq \mathbf{BA}$.

Exercises 7.1

1. Prove each of the following existence theorems.

(a) Not all prime numbers are odd.

(b) There exists an integer k such that k, $k + 2$ and $k + 4$ are all prime.

(c) There exist consecutive positive integers n, $n + 1$ which are both the sum of squares of two positive integers, i.e. $n = a^2 + b^2$, $n + 1 = c^2 + d^2$.

(d) There exists a triple of consecutive positive integers n, $n + 1$, $n + 2$ each of which is the sum of squares of two positive integers $a^2 + b^2$.

(e) There exists a complex number z such that $z^4 = -1$.

(f) There exists an irrational number x such that x^2 is also irrational.

(g) There exist positive integers n which can be expressed as the sum of two squares (of positive integers) in two distinct ways: $n = a^2 + b^2 = c^2 + d^2$ where $\{a, b\} \neq \{c, d\}$.

(h) There exist positive integers n which can be expressed as the sum of two *distinct* squares (of positive integers) in two distinct ways, i.e. $n = a^2 + b^2 = c^2 + d^2$ where $a \neq b$, $c \neq d$ and $\{a, b\} \neq \{c, d\}$.

(i) There exist positive integers n which are both the square of a positive integer and the cube of a positive integer: $n = a^2$ and $n = b^3$.

(j) There exist positive integers n which can be expressed as the sum of two *distinct* cubes (of positive integers) in two distinct ways, i.e. $n = a^3 + b^3 = c^3 + d^3$ where $a \neq b$, $c \neq d$ and $\{a, b\} \neq \{c, d\}$.

2. Prove each of the following existence theorems about matrices.

(i) There exists a matrix $\mathbf{A}$ not equal to $\mathbf{0}_{n\times n}$ for any n such that $\mathbf{A}^2 = \mathbf{0}_{n\times n}$.

(ii) There exists a matrix $\mathbf{A}$ not equal to $\mathbf{I}_n$ for any n such that $\mathbf{A}^2 = \mathbf{I}_n$.

(iii) There exists a matrix $\mathbf{A}$ not equal either to $\mathbf{0}_{n\times n}$ or to $\mathbf{I}_n$ for any n such that $\mathbf{A}^2 = \mathbf{A}$.

(iv) There exist matrices $\mathbf{A}$, $\mathbf{B}$ such that $\mathbf{AB} = \mathbf{I}_n$ but $\mathbf{BA} \neq \mathbf{I}_m$ for any m.

(v) Let $\mathbf{A} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. There exists a 2×2 matrix $\mathbf{B}$ such that $\mathbf{BAB} = \begin{pmatrix} 6 & 0 \\ 0 & 2 \end{pmatrix}$.

3. This question refers to the set $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with the operation of **multiplication modulo 8** defined by:

$$n \times_8 m = \text{remainder when } nm \text{ is divided by } 8.$$

For example, $2 \times_8 6 = 4, 3 \times_8 7 = 5$, etc. A **multiplicative inverse** of an element $n \in \mathbb{Z}_8$ is an element $m \in \mathbb{Z}_8$ such that $n \times_8 m = 1$.

Prove each of the following.

(i) In $\mathbb{Z}_8$ there exists a multiplicative inverse of 5.

(ii) Not all elements of $\mathbb{Z}_8$ have a multiplicative inverse.

(iii) The equation $3 \times_8 x = 2$ has a solution in $\mathbb{Z}_8$.

(iv) The equation $x \times_8 x = 1$ has a solution in $\mathbb{Z}_8$.

(v) There exist elements x and y in $\mathbb{Z}_8$, both different from 1, such that $x \times_8 y = 7$.

4. Prove each of the following existence theorems from the realm of group theory.

(a) Not all groups are cyclic.
(b) There exist non-abelian groups.
(c) There exist groups which have no proper subgroups.

7.3 Non-constructive Existence Proofs

There are methods of proof of an existence theorem $\exists x\, P(x)$ which do not identify any specific element a in the universe of discourse which

has the property defined by the predicate P. Any such proof is termed a **non-constructive existence proof** or an **indirect existence proof**.

Usually, the method used is that of proof by contradiction. We prove that the negation of the theorem, that is $\neg\exists x\, P(x)$, leads us to infer a false proposition. Now $\neg\exists x\, P(x)$ asserts that there is no element of the universe which has the property P. By the rule of quantification denial, QD (see Section 3.2), $\neg\exists x\, P(x)$ is equivalent to $\forall x \neg P(x)$. Thus, we assume $\forall x \neg P(x)$ and show that this inevitably leads to a falsehood. Using the method of proof by contradiction we can infer $\neg\forall x \neg P(x)$ which is equivalent to $\neg\neg\exists x\, P(x)$ by QD and hence to $\exists x\, P(x)$ by DN. The structure of the underlying formal proof is shown in the box below (where we have omitted the details of the proof by contradiction).

Non-constructive existence proof

1.	A_1	axioms
⋮		
n.	A_n	
$n+1$.	T_1	theorems
⋮		
m.	T_m	
$n+m+1$.	$\forall x \neg P(x)$	(CP)
$n+m+2$.	$\neg P(a)$	(UI)
⋮		
r.	Q	
⋮		
s.	$\neg Q$	
$s+1$.	$\neg\forall x \neg P(x)$	$((n+m+1)-s$. Proof by contradiction)
$s+2$.	$\neg\neg\exists x\, P(x)$	($s+1$. QD)
$s+3$.	$\exists x\, P(x)$	($s+2$. DN)

Examples 7.2

1. **Theorem:** *There exists a prime number greater than* 10^{100}.

Before embarking on a non-constructive proof, it is worth reflecting on the difficulties associated with a constructive proof. The number 10^{100} is enormous, greater than the number of atoms in the universe.

Despite the obvious difficulties, there are constructive proofs of the theorem. In other words there are specific known primes larger than 10^{100}. For example, several very large **Mersenne numbers** of the form $M_p = 2^p - 1$ (where p is prime) are known to be prime. The first of these greater than 10^{100} which is also prime is $2^{521} - 1$, which has 157 digits in its decimal notation. (The largest of the currently known primes have many thousands of digits in their decimal expansions.)

The proof that any one of these extremely large integers is prime requires a computer (a very fast supercomputer in the case of the largest) to perform all the necessary calculations. This should be contrasted with our non-constructive proof which follows readily from Euclid's theorem that there exist infinitely many primes (which we have proved in Example 6.2.2 and so becomes part of our background knowledge). It is also worth noting that Euclid's theorem itself had a non-constructive proof.

Proof

Suppose that every prime number p satisfies $2 \leq p \leq 10^{100}$. Then, since there are only finitely many integers between 2 and 10^{100}, there can be only finitely many primes. This contradicts Euclid's theorem (Example 6.2.2). Therefore our initial supposition is incorrect and hence there are prime numbers greater than 10^{100}.

□

2. **Theorem:** *In any n-sided polygon there is an interior angle θ such that*

$$\theta \leq \left(\frac{n-2}{n}\right)\pi.$$

Figure 7.1 shows an 8-sided polygon with an interior angle θ marked.

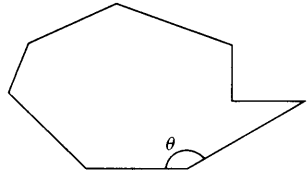


Figure 7.1

Note that this is a slightly different kind of existence theorem in that it is not simply asserting the existence of an object with a particular property. Let $T(P,\theta)$ denote the propositional function: θ *is an internal angle of* P *such that* $\theta \leq [(n-2)/n]\pi$; then the theorem can be symbolised $\forall P \exists \theta\, T(P,\theta)$. Here the universe for P is the set of all n-sided polygons. We can therefore think of the theorem as asserting the existence of a property possessed by *all* members of this universe. As explained in Chapter 5, we will prove $\exists \theta\, T(P,\theta)$ for an arbitrary n-sided polygon P and then (implicitly) apply UG at the end to obtain $\forall P \exists \theta\, T(P,\theta)$. Now $\exists \theta\, T(P,\theta)$ is a 'simple' existence theorem of the type we have been discussing.

In our proof, we shall assume as background knowledge the result: *in any* n*-sided polygon the sum of the interior angles is* $(n-2)\pi$. For a proof of this result, see Exercise 9.2.3.

Proof

Let P be an arbitrary n-sided polygon and suppose that every interior angle θ of P satisfies $\theta > [(n-2)/n]\pi$. Since P has n interior angles,

$$\text{sum of interior angles} > n\left(\frac{n-2}{n}\right)\pi = (n-2)\pi.$$

which contradicts our background knowledge result. Therefore at least one of the interior angles must satisfy

$$\theta \leq \left(\frac{n-2}{n}\right)\pi.$$

□

Exercises 7.2

Further examples of non-constructive existence proofs are given in Exercises 8.2.

1. A polygon is **convex** if every interior angle θ is such that $\theta \leq \pi$.

Prove that, in any n-sided non-convex polygon, there is an interior angle θ such that

$$\theta < \left(\frac{n-3}{n-1}\right)\pi.$$

This theorem appears to assert that every non-convex triangle has a negative internal angle. Explain this apparent contradiction.

2. (a) Let $\{a_1, a_2, \ldots, a_n\}$ be a set of non-zero integers such that $\sum_{k=1}^{n} a_k < n$. Prove that at least one of the integers in the set is negative.

   (b) Let $\{b_1, b_2, \ldots, b_n\}$ be a set of integers such that $\sum_{k=1}^{n} b_k^2 < n$. Prove that at least one of the integers in the set is zero.

3. A tennis club has $2n + 1$ members, where n is a positive integer. During one week, $n + 1$ singles matches were played between members. Prove that some member played more than once during the week.

4. The following theorem is given as background knowledge.

Theorem: *Let* $f: [a,b] \to \mathbb{R}$ *be a continuous function defined on the closed interval* $[a,b] = \{x \in \mathbb{R} : a \leq x \leq b\}$. *Then the image of* f, $\{f(x) : x \in [a,b]\}$, *is also a closed interval* $[c,d]$ *for some real numbers* $c \leq d$.

Use this theorem to prove the following existence theorem.

Intermediate value theorem: *Let* $f: [a,b] \to \mathbb{R}$ *be continuous and suppose* k *lies between* $f(a)$ *and* $f(b)$ *in the sense that* k *satisfies* $f(a) \leq k \leq f(b)$ *or* $f(b) \leq k \leq f(a)$. *Then there exists* $x \in [a,b]$ *such that* $f(x) = k$.

5. The completeness axiom for $\mathbb{R}$ (Exercise 5.3.10) can be used to establish the existence of real numbers satisfying certain properties.

Prove that there exists a positive real number x which satisfies the equation $x^2 = 2$.

Essentially, this asserts the existence of the real number $\sqrt{2}$.

Hint: let $S = \{x \in \mathbb{R} : x > 0 \text{ and } x^2 < 2\}$. Prove that S is (a) non-empty and (b) bounded above. Use the completeness axiom to deduce the existence of a supremum α for S. Finally prove that $\alpha^2 = 2$.

7.4 Use of Counter-examples

So far in this book, we have been concerned with finding and understanding proofs of theorems. Of course, given a particular proposition, we will not know whether it really is a theorem until a proof has been found. Suppose we are presented with a proposition of the form $\forall x\, P(x)$ which may or may not be a theorem. If it turns out that the

proposition is not a theorem then all our techniques and strategies for finding a proof are bound to fail for the glaringly obvious reason that no proof exists! Unfortunately, there is no way of showing that a proposition is a theorem *in advance* of finding a proof—finding a proof is precisely how a proposition is shown to be a theorem.

Consider, for example, the proposition:

For all non-negative integers n, the integer $F_n = 2^{2^n} + 1$ is prime.

In 1640, Fermat asserted his belief that this proposition was a theorem, although he was unable to supply a proof. Was Fermat correct in his belief? The first stage in investigating the question is to look at some of the smaller examples.

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65\,537$$

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294\,967\,297^1$$

$$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 18\,446\,744\,073\,709\,551\,617$$

It is clear that F_0, F_1 and F_2 are prime and we can fairly quickly verify that F_3 is prime (see Example 5.2.1). With rather more work, F_4 can be shown to be prime. (Even with a standard scientific calculator, this would be a lengthy and tedious task.) Beyond F_4 these so-called **Fermat numbers** grow very rapidly indeed. We cannot imagine anyone wishing to use the method of Example 5.2.1 to test whether or not F_5 is prime aided only by a pocket calculator. Indeed, it was not until 1732, nearly one hundred years after Fermat proposed the conjecture, that Euler established that F_5 is composite by showing that

$$F_5 = 4294\,967\,297 = 641 \times 6\,700\,417.$$

Of course, this factorisation of F_5 shows that Fermat's conjecture is not a theorem. The factorisation provides a 'counter-example' to the proposition.

[1] A word of warning! Some pocket calculators will evaluate F_5 incorrectly as 4294 967 296 due to the method they employ to evaluate powers.

As an aside, it is interesting to note that what took the mathematical community nearly 100 years to achieve now takes a modest desktop computer just a few seconds. There are various computer algebra packages which will obtain these factors in under a second. Indeed the factorisation of the next Fermat number $F_6 = 274\,177 \times 67\,280\,421\,310\,721$ is also achieved by some such packages in a second or two. Lest we become too complacent about their ability, two different computer algebra packages each running on a personal computer for over 100 hours failed to find the (known) factorisation of F_7.

Let us consider again the general situation: suppose we are presented with a proposition which is a universally quantified propositional function $\forall x\, P(x)$. If we can find a single specific member a of the universe such that $P(a)$ is false, then $\forall x\, P(x)$ is not a theorem. Any element a in the universe such that $P(a)$ is false is called a **counter-example** to the proposition $\forall x\, P(x)$. The method of finding the appropriate element a and showing $P(a)$ is false is often called **proof by counter-example**. Since the existence of a counter-example establishes that $\forall x\, P(x)$ is *not* a theorem, perhaps *'disproof* by counter-example' would be a better term. It should be noted that the existence of a counter-example does prove the proposition $\neg\forall x\, P(x)$ or its equivalent (by the rule of quantification denial) $\exists x \neg P(x)$. The formal proof underlying the method is given in the box below.

Proof by counter-example

1.	A_1	axioms
⋮		
n.	A_n	
$n+1$.	T_1	theorems
⋮		
$n+m$.	T_m	
⋮		
r.	$\neg P(a)$	(where a is a specific element of the universe)
$r+1$.	$\exists x \neg P(x)$	(r. EG)
$r+2$.	$\neg\forall x\, P(x)$	(r+1. QD)

Given a proposition $\forall x\, P(x)$ which may or may not be a theorem, we are faced with a dilemma. Do we search for a proof or do we try to find

a counter-example? If $\forall x\, P(x)$ is a theorem and we opt to search for a counter-example, then our quest is bound to fail. On the other hand, if $\forall x\, P(x)$ is not a theorem then any search for a proof will inevitably be unsuccessful. The choice of which path to take—proof or counter-example—is often based on experience, intuition or pure instinct. In practice the situation is not as bad as it appears. The first step in the search for a proof is frequently to look at some examples and during this initial phase we may come across a counter-example anyway.

Actually, there is a third possibility which is rather disturbing. It may be impossible to find a proof of, or a counter-example to, the proposition $\forall x\, P(x)$. Essentially, we have defined a theorem to be a proposition which is provable from the axioms. There are some situations when neither $\forall x\, P(x)$ nor $\neg\forall x\, P(x)$ is provable from the axioms. In other words, the given axiom system is not sufficiently powerful to determine the 'truth' of $\forall x\, P(x)$. In this case, we say that $\forall x\, P(x)$ is **undecidable** from the given axioms. Fortunately, such situations are rare and tend to crop up only in the more esoteric areas of mathematics.

Examples 7.3

1. Find a counter-example to the proposition: *for all real numbers x and y, if $x \leq y$ then $|x| \leq |y|$.*

The proposition can be symbolised as $\forall x \forall y[(x \leq y) \rightarrow (|x| \leq |y|)]$, where the universe for x and y is the set of real numbers. For a counter-example, we need to find real numbers a and b such that $(a \leq b) \rightarrow (|a| \leq |b|)$ is false. This is a conditional proposition of the form $P \rightarrow Q$ which is false only when P is true and Q is false. Thus a counter-example will be such that $a \leq b$ is true and $|a| \leq |b|$ is false. Since $|x| = x$ for all non-negative real numbers x, any counter-example must be such that at least one of the real numbers a or b is negative. An example where $a \leq b$ is true is $a = -2, b = -1$. In this case, $|a| = |-2| = 2$ and $|b| = |-1| = 1$ so the statement $|a| \leq |b|$ becomes $2 \leq 1$, which is clearly false. We have found our counter-example.

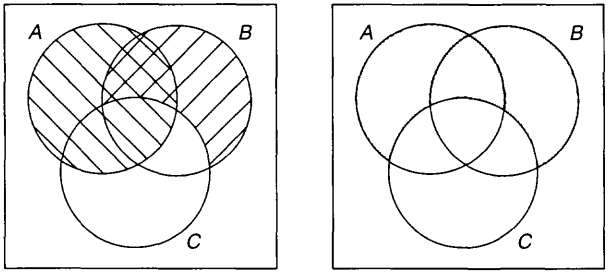
2. Find a counter-example to the proposition: *for all sets A, B and C,*

$$A \cup (B - C) = (A \cup B) - C.$$

Recall (or see the appendix) that for sets X and Y, the set $X - Y$ contains all those elements of X which do not belong to Y:

$$X - Y = \{x: x \in X \text{ and } x \notin Y\}.$$

Although one or more Venn diagrams will not constitute a proof of a theorem, they can be extremely useful in pointing the way towards a proof or counter-example. Figure 7.2 represents the sets $A \cup (B - C)$ and $(A \cup B) - C$ on two Venn diagrams.



$A \cup (B-C)$ $(A \cup B)-C$

Figure 7.2

From the diagrams, we can see that the 'difference' between the two sets is that $A \cup (B - C)$ contains $A \cap C$ as a subset whereas $(A \cup B) - C$ does not. This indicates that a counter-example will require the set $A \cap C$ to be non-empty.

Counter-example

Let $A = \{1,2,3,4,5\}$, $B = \{2,4,6\}$ and $C = \{2,3,5\}$.

Then $B - C = \{4,6\}$ so $A \cup (B - C) = \{1,2,3,4,5,6\}$.

However $A \cup B = \{1,2,3,4,5,6\}$ so $(A \cup B) - C = \{1,4,6\}$.

Therefore $A \cup (B - C) \neq (A \cup B) - C$ for these sets.

□

In terms of proving a particular proposition to be false, any counter-example is as good as any other. However, simpler counter-examples are to be preferred to more complicated ones. A complicated example may be difficult to understand and can obscure the real reason why the particular proposition is false. A simpler example is more likely to come close to the heart of why the proposition is false and thus provide greater insight. For instance, another counter-example

to the proposition '$A \cup (B - C) = (A \cup B) - C$ for all sets A, B, C' is provided by $A =$ {positive real numbers}, $B =$ {integers} and $C =$ {irrational real numbers}. (We leave it as an exercise to verify that these sets do, indeed, provide a counter-example—see Exercise 7.3.3.) However, it is more difficult to evaluate the various sets involved here and we may wonder whether the reason that $A \cup (B - C) \neq (A \cup B) - C$ has something to do with the fact that the sets are infinite or involve irrational numbers.

Exercises 7.3

1. Let $f(n) = n^2 + n + 41$. Then $f(0) = 41$, $f(1) = 43$, $f(2) = 47$, $f(3) = 53$, $f(4) = 61, \ldots$ are all prime. Find a counter-example to the proposition:

for all non-negative integers n, f(n) is prime.

(This formula, which does produce a long sequence of primes, was discovered by Euler. In fact, amongst all expressions of the form $n^2 + an + b$ where a and b are non-negative integers less than 10 000, there is none which produces a longer sequence of primes.)

2. Find a counter-example to each of the following propositions.

(a) For all real numbers a, b, c and d, if $a > b$ and $c > d$ then $(a - c) > (b - d)$.

(b) For all positive integers a, b and c, if c is a factor of $a + b$ then c is a factor of a or c is a factor of b.

(c) $f(n) = n^2 - n + 17$ is prime for all positive integers n.

(d) $6^n + 4n^4$ is divisible by 5 for all positive integers n.

(e) $3^n < 4n^4$ for all even positive integers n.

(f) $n^4 + 1$ is prime for all even positive integers n.

3. Verify that the sets $A =$ {positive real numbers}, $B =$ {integers} and $C =$ {irrational real numbers} provide a counter-example to the proposition: $A \cup (B - C) = (A \cup B) - C$ for all sets A, B, C as claimed in Example 7.3.2.

4. Find a counter-example to each of the following propositions defined over the universe of all 2×2 matrices with real number entries.

(i) If $\mathbf{AB} = \mathbf{AC}$ and $\mathbf{A} \neq \mathbf{0}_{2\times 2}$, then $\mathbf{B} = \mathbf{C}$.

(ii) The only matrices satisfying the equation $\mathbf{A}^2 = \mathbf{A}$ are $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(iii) If $\mathbf{A}^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ then $\mathbf{A}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(iv) If $\mathbf{A}$ and $\mathbf{B}$ are distinct (i.e. non-equal) matrices such that $\mathbf{AB} = \mathbf{BA}$ then either $\mathbf{A}$ or $\mathbf{B}$ is equal to $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

5. Prove or disprove each of the following propositions.

(i) If a and b are rational numbers, then ab is a rational number.
(ii) If a and b are irrational numbers, then ab is an irrational number.
(iii) If a and b are rational numbers and $b \neq 0$, then a/b is a rational number.
(iv) If a and b are irrational numbers, then a/b is an irrational number.

6. Find a counter-example to each of the following propositions.

(a) Every continuous function $f\colon \mathbb{R} \to \mathbb{R}$ is differentiable.
(b) Every continuous function $f\colon (a,b) \to \mathbb{R}$ is bounded.
Here (a,b) is the open interval $\{x \in \mathbb{R} : a < x < b\}$. A function is **bounded** if there exists a positive real number M such that $|f(x)| \leq M$ for all x in its domain.
Note: there is a theorem which states that every continuous function $f\colon [a,b] \to \mathbb{R}$ is bounded, where $[a,b]$ denotes the closed interval $\{x \in \mathbf{R} : a \leq x \leq b\}$. Your counter-example shows that this theorem does not extend to open intervals.
(c) If $f\colon \mathbb{R} \to \mathbb{R}$ is twice differentiable and f has a local maximum at $x = a$ then $f''(a) < 0$.
If $g\colon \mathbb{R} \to \mathbb{R}$ is twice differentiable and g has a local minimum at $x = b$ then $g''(a) > 0$.
Note: your counter-examples indicate the limitations of the second derivative test for local maxima and minima.

7. Prove or disprove each of the following propositions.

(a) If A, B and C are sets such that $A \subseteq B$, $B \subseteq C$ then $A \subseteq C$.
(b) If A, B and C are sets such that $A \not\subseteq B$, $B \not\subseteq C$ then $A \not\subseteq C$. (The symbol $\not\subseteq$ means 'is not a subset of.')

(c) If **A** and **B** are $n \times n$ matrices such that both **A** and **AB** are symmetric, then **B** is symmetric.

(d) If G is a group and $a, b \in G$ then $(ab)^n = a^n b^n$ for all positive integers n.

(e) If A, B and C are sets such that $C \subseteq A \times B$, then $C = X \times Y$ for some $X \subseteq A$ and $Y \subseteq B$. (Informally, this says that every subset of a Cartesian product is itself a Cartesian product.)

7.5 Uniqueness Proofs

Sometimes in mathematics, we wish to prove not only that an object with certain properties exists but also that there is only one such object, i.e. that the object is unique. The existence part of such a proof was discussed in Sections 7.2 and 7.3. Here we focus on the uniqueness part. To see what is required in such a proof, suppose we define the natural number N to be the number of objects with the required property. An existence proof amounts to showing $N \geq 1$; in other words, that there is at least one such object. Given this, to establish uniqueness as well we must show that $N = 1$ so that there is exactly one object of the required type.

The method of proving that $N = 1$ is essentially the method of proof by contradiction, although it is frequently phrased in a slightly different manner, as we shall explain. We suppose that existence has been established, so that we know $N \geq 1$. Since N is an integer and $N \geq 1$, the negation of $N = 1$ is $N \geq 2$. Thus we suppose that there are at least two different objects in the universe satisfying the required conditions. We can therefore choose two such objects and deduce a false proposition.

To investigate the structure of the proof more closely, we need to introduce some notation. Let $P(x)$ denote the propositional function: x *is an object with the required properties.* Then $N \geq 2$ is equivalent to the proposition $\exists x \exists y[P(x) \wedge P(y) \wedge (x \neq y)]$ which asserts that there exist two distinct objects with the required property. Using existential instantiation (EI) twice we deduce $P(a) \wedge P(b) \wedge (a \neq b)$ for specific elements a and b of the universe. The false conclusion which is generally obtained from this assumption is $a = b$.

Now uniqueness proofs are often not expressed as proofs by contradiction but rather as direct proofs. It is possible to prove $\neg(N \geq 2)$ directly. It is not too difficult to show (see Exercise 7.4.8) that

$$\neg[\exists x \exists y (P(x) \wedge P(y) \wedge (x \neq y))]$$

is equivalent to

$$\forall x \forall y [(P(x) \wedge P(y)) \rightarrow (x = y)].$$

This means that uniqueness can be proved directly using the method of conditional proof. We need to prove $P(a) \wedge P(b) \rightarrow (a = b)$ for arbitrary a and b in the universe and then (implicitly) use UG twice. Thus we add $P(a)$ and $P(b)$ to our assumptions and infer $a = b$. (Strictly, it is $P(a) \wedge P(b)$ which is added to the assumptions, but this is equivalent to adding both $P(a)$ and $P(b)$.) In other words, we suppose that a and b are objects of the required type and deduce that $a = b$.

In practice, the difference between the two versions of a uniqueness proof is minimal. Both assume a and b are objects in the universe with the required property. In the proof by contradiction it is additionally assumed that the two objects are distinct, $a \neq b$. The 'contradiction' which arises is almost always $a = b$. The direct proof version is slightly simpler as the additional assumption that a and b are distinct is not made. The formal proof underlying the direct proof version is given below. We leave as an exercise to construct the formal proof underlying the proof by contradiction version.

Direct proof of uniqueness of x satisfying $P(x)$

1.	A_1	axioms
⋮		
n.	A_n	
$n+1$.	T_1	theorems
⋮		
$n+m$.	T_m	
$n+m+1$.	$P(a) \wedge P(b)$ (CP)	(where a and b are arbitrary elements of the universe)
⋮		
r.	$a = b$	
$r+1$.	$(P(a) \wedge P(b)) \rightarrow (a = b)$	$((n+m+1)-r$. CP)
$r+2$.	$\forall x \forall y [(P(x) \wedge P(y)) \rightarrow (x = y)]$	$(r+1$. UG)

Examples 7.4

1. **Theorem:** *For every real number a, the equation $x^3 = a$ has a unique real solution.*

The existence part of the proof is both subtle and difficult—it amounts to proving that every real number a has a cube root $\sqrt[3]{a}$. How can we prove, for example, that the real number $\sqrt[3]{2}$ exists? The existence part uses the completeness axiom for the real numbers—see Exercises 5.3.10 and 7.2.5.

Proof

We shall assume the existence part of the theorem (as background knowledge!) and prove only the uniqueness part.

Suppose x and y are real numbers such that $x^3 = a$ and $y^3 = a$. Then

$$\begin{aligned} x^3 = y^3 &\Rightarrow x^3 - y^3 = 0 \\ &\Rightarrow (x - y)(x^2 + xy + y^2) = 0 \\ &\Rightarrow x - y = 0 \quad \text{or} \quad x^2 + xy + y^2 = 0 \\ &\Rightarrow x = y \quad \text{or} \quad x^2 + xy + y^2 = 0. \end{aligned}$$

We are required to show that $x = y$. This would now follow (using commutation and disjunctive syllogism) if we could show that $x^2 + xy + y^2 \neq 0$. Unfortunately, we cannot! However, from Exercise 5.2.5,

$$(x \neq 0 \text{ or } y \neq 0) \Rightarrow x^2 + xy + y^2 \neq 0.$$

The contrapositive relation is:

$$x^2 + xy + y^2 = 0 \Rightarrow (x = 0 \text{ and } y = 0).$$

In particular, $x^2 + xy + y^2 = 0 \Rightarrow x = y$.

From the argument above, it now follows that:

$$\begin{aligned} (x - y)(x^2 + xy + y^2) = 0 &\Rightarrow x = y \quad \text{or} \quad x^2 + xy + y^2 = 0 \\ &\Rightarrow x = y. \end{aligned}$$

Therefore the equation $x^3 = a$ has a unique real solution.

□

2. **Theorem:** *Let* $\mathbf{A}$ *be a* 2×2 *matrix. If* $\det \mathbf{A} \neq 0$ *then* $\mathbf{A}$ *has a unique inverse.*

This time we shall prove both the existence and uniqueness part of the theorem. The existence part is proved by construction, that is, given $\mathbf{A}$ we find a matrix $\mathbf{B}$ such that $\mathbf{AB} = \mathbf{BA} = \mathbf{I}_2$. We shall simply define the matrix $\mathbf{B}$ and show that it is the inverse of $\mathbf{A}$. (For an explanation of where the matrix $\mathbf{B}$ comes from, a textbook covering basic matrix theory can be consulted.)

Proof

Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and suppose $\det \mathbf{A} = ad - bc \neq 0$. Define $\mathbf{B}$ to be the 2×2 matrix

$$\mathbf{B} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} \dfrac{d}{ad - bc} & \dfrac{-b}{ad - bc} \\ \dfrac{-c}{ad - bc} & \dfrac{a}{ad - bc} \end{pmatrix}.$$

Then

$$\begin{aligned} \mathbf{AB} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \frac{1}{ad - bc} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= \frac{1}{ad - bc} \begin{pmatrix} ad - bc & -ab + ab \\ cd - cd & ad - bc \end{pmatrix} \\ &= \frac{1}{ad - bc} \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}_2. \end{aligned}$$

Therefore $\mathbf{AB} = \mathbf{I}_2$. Verifying that $\mathbf{BA} = \mathbf{I}_2$ is similar. Hence $\mathbf{B}$ is an inverse of $\mathbf{A}$.

We now turn to the uniqueness part of the theorem. We shall need to assume, as background knowledge, the associative property of multiplication of 2×2 matrices which states that $\mathbf{X}(\mathbf{YZ}) = (\mathbf{XY})\mathbf{Z}$ for all 2×2 matrices $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$.

Suppose that $\mathbf{B}$ and $\mathbf{C}$ are 2×2 matrices such that $\mathbf{AB} = \mathbf{BA} = \mathbf{I}_2$ and $\mathbf{AC} = \mathbf{CA} = \mathbf{I}_2$. Then

$$\begin{aligned}
\mathbf{B} &= \mathbf{BI}_2 && \text{(property of } \mathbf{I}_2\text{)} \\
&= \mathbf{B}(\mathbf{AC}) && \text{(since } \mathbf{AC} = \mathbf{I}_2\text{)} \\
&= (\mathbf{BA})\mathbf{C} && \text{(associative law for matrix multiplication)} \\
&= \mathbf{I}_2\mathbf{C} && \text{(since } \mathbf{BA} = \mathbf{I}_2\text{)} \\
&= \mathbf{C} && \text{(property of } \mathbf{I}_2\text{).}
\end{aligned}$$

Therefore the inverse of $\mathbf{A}$ is unique.

□

The proof of uniqueness clearly relies on the associative law for matrix multiplication. In fact the proof is valid for any associative binary operation (with an identity element). In particular, the proof can be used to show that in any group the inverse of each element is unique.

3. For our last example, we prove the uniqueness part of the fundamental theorem of arithmetic. The proof of the existence part was outlined in Section 4.2 and will be dealt with more rigorously in Chapter 9.

Fundamental theorem of arithmetic: *Every integer greater than* 1 *can be expressed as a product of prime numbers in a manner which is unique apart from the ordering of the prime factors.*

Proof of uniqueness

Let a be an integer greater than 1 and let

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \qquad (*)$$

be two factorisations of a into prime factors. Without loss of generality we may suppose that $n \geq m$.

Now q_m is a factor of a so q_m divides the product $p_1 p_2 \cdots p_n$. If a prime number divides a product, it must divide one of the factors (see Exercises 6.3.4 and 9.1.12 (a)—the first of these is $p|ab \Rightarrow p|a \vee p|b$, the second is the extension to several factors) so q_m divides one of the p's, p_k say. But p_k is prime so it has no factors other than 1 and p_k; therefore $q_m = p_k$.

Dividing $(*)$ by $q_m = p_k$ and renumbering the p's (if necessary) gives

$$p_1 p_2 \cdots p_{n-1} = q_1 q_2 \cdots q_{m-1}.$$

Repeat the argument above using $q_{m-1}, \cdots, q_2$ in turn. This produces:

$$p_1 p_2 \cdots p_l = q_1 \qquad (**)$$

where $l = n - m + 1 \geq 1$. As before q_1 divides $p_1 p_2 \cdots p_l$ so must divide one of the ps. However, if $l > 1$ so that there is more than one factor on the left-hand side of $(**)$, then dividing by q_1 would give a product of prime numbers equal to 1. This is impossible since every prime is strictly greater than 1. Therefore $l = 1$ so $n = m$ and $(**)$ is just $p_1 = q_1$.

In summary, we have shown that with a suitable re-numbering of the p's if necessary,

$$n = m \text{ and } p_1 = q_1, p_2 = q_2, \ldots, p_n = q_m$$

so the prime factorisation is unique apart from the ordering of the factors.

□

Exercises 7.4

1. Prove that the equation $ax = b$, where a and b are fixed real numbers and $a \neq 0$, has a unique solution.

2. Prove that, if $a > 0$ then the equation $x^2 = a$ has a unique positive solution. (As in Example 7.4.1, you may assume the existence of $\sqrt{a}$ for $a > 0$.)

3. Prove that, for every real number a, the equation $x^5 = a$ has a unique solution. (Again, assume the necessary existence theorem and concentrate on the uniqueness part of the proof.)

4. Prove that, if a, b, c, d are real numbers such that $ad - bc \neq 0$, then for all real numbers s, t there exists a unique solution (x, y) to the simultaneous equations

$$ax + by = s$$
$$cx + dy = t.$$

5. Prove that every integer $a > 2$ can be expressed uniquely as $a = 2^n b$ where n is an integer and b is an odd integer.

6. Let G be a group. Prove that:

(i) the identity element e is unique.

(ii) for each $x \in G$ the inverse of x is unique.

(iii) for all $a, b \in G$, the equation $ax = b$ has a unique solution in G.

7. The completeness axiom for $\mathbb{R}$ states that every non-empty subset of $\mathbb{R}$ which is bounded above has a supremum. (See Exercise 5.3.10.)

Let A be a non-empty subset of $\mathbb{R}$ which is bounded above. Prove that the supremum of A is unique.

8. Prove the result used on page 203 that

$$\neg[\exists x \exists y (P(x) \wedge P(y) \wedge (x \neq y))]$$

is equivalent to

$$\forall x \forall y [(P(x) \wedge P(y)) \rightarrow (x = y)].$$

8 Further Proof Techniques

8.1 Introduction

In the previous three chapters we have described some general methods and techniques of proof. In doing so we have not made any specific assumptions about the nature of the assumed background knowledge, the axioms and previously proved theorems. Of course, when considering particular examples we do need some detailed knowledge of the system, but as far as the general proof techniques are concerned no specific background knowledge was assumed. In this chapter and the next we explore some proof techniques based upon specific axioms or theorems which must therefore be part of the background knowledge of the system within which the theorems are proved.

It should be emphasised that it is *techniques* based on particular axioms or theorems which are of interest here. For example, we are not dealing with situations such as the following (see Example 5.4.):

background knowledge: *for all real numbers* x, $x^2 > 0$;

theorem: *for all non-negative real numbers* x *and* y, $\dfrac{x+y}{2} \geq \sqrt{xy}$.

The point here is that the theorem, and therefore its proof, relates directly in content to the given background knowledge. Instead, we shall consider situations where a theorem provides a *framework* for proofs in many different contexts. Of necessity any theorem which serves such a purpose must be very general in nature. For convenience, we call the theorem on which a particular proof technique is based the 'special theorem' for that technique.

In each of the cases we shall consider the special theorem is a universally quantified conditional propositional function, $\forall x[P(x) \rightarrow Q(x)]$.

The universe of discourse of the variable x needs to be sufficiently general to allow the theorem to have wide applicability. One possibility, for instance, would be the case where x is defined over the universe of sets. Since theorems in many different contexts can be phrased in terms of set theory, such a theorem is likely to be applicable in many different situations. The proof technique based on a special theorem of the form $\forall x[P(x) \rightarrow Q(x)]$ is summarised below. The method is used to prove a theorem of the form $\forall x\, Q(x)$. Provided $\forall x[P(x) \rightarrow Q(x)]$ is part of our background knowledge, universal instantiation gives $P(a) \rightarrow Q(a)$ where a is an arbitrary element of the universe. The main body of the proof establishes $P(a)$ from which we may infer $Q(a)$, by modus ponens, and then $\forall x\, Q(x)$, by universal generalisation.

Proof technique based on a special theorem

$1.$	A_1	axioms
$\vdots$		
$n.$	A_n	
$n+1.$	T_1	theorems
$\vdots$		
$n+m.$	T_m	
$n+m+1.$	$\forall x[P(x) \rightarrow Q(x)]$	special theorem
$n+m+2.$	$P(a) \rightarrow Q(a)$	$(n+m+1.$ UI$)$
$\vdots$		
$r.$	$P(a)$	
$r+1.$	$Q(a)$	$(n+m+2, r.$ MP$)$
$r+2.$	$\forall x\, Q(x)$	$(r+1.$ UG$)$

Before considering particular instances of proof techniques based on special theorems, a word of caution is in order. As we shall see, our special theorems are frequently very simple, almost trivial, to state. This does not mean, however, that particular proofs based on the corresponding technique are trivial! A given special theorem provides the structure for a corresponding proof. Even when the structure of a proof is relatively straightforward, the detailed arguments involved need not be.

8.2 Proofs of Identities

Consider the two equations:

$$(x+1)^2 = x^2 + 2x + 1$$

and

$$x^2 - 2x - 3 = 0.$$

The first of these is true for all real numbers x, whereas the second has two real number solutions, $x = -1$ and $x = 3$. When an equation is true for all elements in the universe, we refer to it as an **identity**. For the equations above, we can regard the identity $(x+1)^2 = x^2 + 2x + 1$, which is true for all real x, as telling us something about the algebraic properties of the real numbers. By contrast, the equation $x^2 - 2x - 3 = 0$ is telling us something about the real number x. It is equations of the first kind, the identities, which are of principal concern to us in this section.

Some authors use a different symbol for identities and write $(x+1)^2 \equiv x^2 + 2x + 1$, where the symbol $\equiv$ is interpreted as meaning 'is identically equal to'. We may regard $(x+1)^2 \equiv x^2 + 2x + 1$ as an abbreviation for: *for all* x, $(x+1)^2 = x^2 + 2x + 1$.

Crucial in proving identities (and solving equations) is the **transitive property** of equality: if $a = b$ and $b = c$ then $a = c$. Although this appears to be an almost trivial property, some care needs to be exercised when applying it—see Example 8.2.4 below, for instance.

Example 8.1

To illustrate the use of the transitive property consider the following simple theorem.

Theorem: *For all real numbers* x, $(x+1)^3 = (x^3 + 1) + 3x(x+1)$.

Proof

Let x be a real number. Then:

$$\begin{aligned}(x+1)^3 &= x^3 + 3x^2 + 3x + 1 \\ &= (x^3 + 1) + (3x^2 + 3x) \\ &= (x^3 + 1) + 3x(x+1).\end{aligned}$$

□

Analysing the proof in Example 8.1, we see that it comprises the following three steps.

1. $(x+1)^3 = x^3 + 3x^2 + 3x + 1$
2. $x^3 + 3x^2 + 3x + 1 = (x^3 + 1) + 3x(x+1)$
3. $(x+1)^3 = (x^3 + 1) + 3x(x+1)$ (from 1 and 2).

The justification of line 3 is the transitive property. More generally, a proof of an identity will involve many steps. In order to avoid having to appeal to the transitive property at each stage, it is convenient to prove a theorem which will cover proofs with several steps. The following theorem will be the special theorem for the proof technique used in Example 8.1.

Theorem of identities: *If $a_1, a_2, \ldots, a_n$ are members of some universe such that $a_1 = a_2, a_2 = a_3, \ldots, a_{n-1} = a_n$ then $a_1 = a_n$.*

Proof

We shall give a somewhat informal proof. For a more rigorous version of the argument, we would need to use the method of proof by induction—see Chapter 9.

Suppose that $a_1, a_2, \ldots, a_n$ are such that $a_1 = a_2, a_2 = a_3, \ldots, a_{n-1} = a_n$.

Since $a_1 = a_2$ and $a_2 = a_3$ it follows from the transitive property that $a_1 = a_3$. We therefore have $a_1 = a_3$ and $a_3 = a_4$ so $a_1 = a_4$, again by the transitive property.

Continuing in this way we eventually obtain $a_1 = a_n$ as required.

□

With the theorem of identities as the special theorem, the proof technique given on page 210 gives the following method for proving identities.

Proof of identities

Suppose that $a_1, a_2, \ldots, a_n$ are members of some universe such that the following are true propositions:

1. $a_1 = a_2$, 2. $a_2 = a_3$, ..., $n-1$. $a_{n-1} = a_n$.

Then $a_1 = a_n$ is a true proposition.

Sometimes it is not convenient to organise the proof of an identity $a_1 = a_n$ as an unbroken chain $a_1 = a_2 = \cdots = a_n$ from the left-hand side a_1 to the right-hand side a_n. Instead, it may be easier to construct two chains, one from the left-hand side to some element b and the other from the right-hand side also to the same element b:

$$a_1 = a_2 = \cdots = b \quad \text{and} \quad a_n = a_{n-1} = \cdots = b.$$

From these, we may deduce $a_1 = b$ and $a_n = b$ using the theorem of identities. We now need to appeal to the **commutative property** of equality: if $a = b$ then $b = a$. Using this, we may now deduce $a_1 = b$ and $b = a_n$. Finally, we apply the transitive property to obtain $a_1 = a_n$. Which of the two structures to adopt in a given proof is frequently a matter of taste, although sometimes one version is easier to explain than the other.

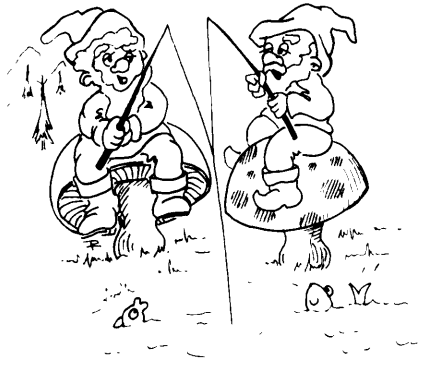
Examples 8.2

1. The **binomial coefficients** $\binom{n}{k}$ are defined for all non-negative integers n and k such that $k \leq n$ by:

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$$

where $n! = n(n-1)(n-2)\cdots 2 \times 1$ for $n \geq 1$ (and $0! = 1$).

The binomial coefficients are also denoted by $C(n,k)$, ${}_nC_k$ or ${}^nC_k$. There are various identities which can be proved involving the binomial coefficients. The following is a typical example.



Binomial coefficient

Theorem: *If n and k are positive integers such that $k < n$, then*

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

To prove the identity, we consider one side of the equation and, using algebraic manipulation, construct a chain of equal expressions ending with the other side of the equation. Usually in mathematics, it is easier to combine two terms and simplify than to divide a single term in two. Thus it is sensible to begin with the left-hand side of the equation and work towards the right-hand side.

Proof

Suppose that n and k are positive integers such that $k \leq n$. Then

$$\begin{aligned}
&\binom{n}{k} + \binom{n}{k-1} \\
&= \frac{n!}{(n-k)!\,k!} + \frac{n!}{(n-(k-1))!(k-1)!} && \text{(using the definitions)} \\
&= \frac{n!}{(n-k)!\,k!} + \frac{n!}{(n-k+1)!(k-1)!} \\
&= \frac{n!(n-k+1)}{(n-k+1)(n-k)!\,k!} + \frac{n!\,k}{(n-k+1)!\,k(k-1)!} \\
&= \frac{n!(n-k+1)}{(n-k+1)!\,k!} + \frac{n!\,k}{(n-k+1)!\,k!} && \text{(since } (n-k+1)\times(n-k)! = (n-k+1)! \\
& && \text{and } k\times(k-1)! = k!) \\
&= \frac{n!(n-k+1+k)}{(n-k+1)!\,k!} \\
&= \frac{n!(n+1)}{(n-k+1)!\,k!} \\
&= \frac{(n+1)!}{((n+1)-k)!\,k!} && \text{(since } n!\times(n+1) = (n+1)!) \\
&= \binom{n+1}{k} && \text{(using the definition).}
\end{aligned}$$

□

2. The following 'proof' claims to establish a similar kind of identity for the so-called **falling factorial**

$$(n)_k = \frac{n!}{(n-k)!}$$

also denoted variously by $P(n,k)$, ${}_nP_k$ or ${}^nP_k$. However the 'proof' exhibits an error common in the construction of proofs of identities. What is wrong with it?

Theorem: *If r and n are positive integers such that $r < n+1$ then*

$$(n+1)_r = (n)_r + r(n)_{r-1}.$$

'Proof.'

Suppose n and r are positive integers such that $r < n+1$. Then

$$\begin{aligned}
& (n+1)_r = (n)_r + r(n)_{r-1} \\
\Rightarrow \quad & \frac{(n+1)!}{((n+1)-r)!} = \frac{n!}{(n-r)!} + r \times \frac{n!}{(n-(r-1))!} \\
\Rightarrow \quad & \frac{(n+1)!}{(n+1-r)!} = \frac{n!}{(n-r)!} + r \times \frac{n!}{(n-r+1)!} \\
\Rightarrow \quad & \frac{(n+1)!}{(n+1-r)!} = \frac{n!(n-r+1)}{(n-r+1)(n-r)!} + \frac{r \times n!}{(n-r+1)!} \\
\Rightarrow \quad & \frac{(n+1)!}{(n+1-r)!} = \frac{n!(n-r+1)}{(n-r+1)!} + \frac{r \times n!}{(n-r+1)!} \\
\Rightarrow \quad & \frac{(n+1)!}{(n+1-r)!} = \frac{n!(n-r+1+r)}{(n-r+1)!} \\
\Rightarrow \quad & \frac{(n+1)!}{(n+1-r)!} = \frac{n!(n+1)}{(n-r+1)!} \\
\Rightarrow \quad & \frac{(n+1)!}{(n+1-r)!} = \frac{(n+1)!}{(n-r+1)!}.
\end{aligned}$$

Since this is clearly true, it follows that $(n+1)_r = (n)_r + r(n)_{r-1}$.

□

It could be argued, with some justification, that the proof is flawed because it fails to justify or explain the steps. However, each step follows from the previous one by a little algebraic manipulation in a similar manner to the proof given in the previous example.

In fact, there is a serious *structural*, rather than stylistic, problem with the claimed proof. In the first line, the identity to be proved is written down; subsequent lines are consequences of this until, at the end, a statement is deduced which is clearly true. This means that the structure of the 'proof' is to assume the identity and then deduce an obviously true proposition:

(proposition to be proved) $\Rightarrow$ (obviously true proposition).

However, we know from the method of direct proof that we should proceed *from* what is known (background knowledge) *to* the proposition being proved. In other words, the *direction* of the argument in the claimed proof is wrong.

Using this invalid method of 'proof,' it is easy to produce 'proofs' of obviously false propositions. A simple example is the following, which claims to prove that $1 = -1$.

$1 = -1 \Rightarrow 1 = 1$ (by squaring both sides).

Since $1 = 1$ is true, we deduce $1 = -1$.

This shows clearly what is wrong with the method. Although $1 = -1 \Rightarrow 1 = 1$ is a valid implication, the converse $1 = 1 \Rightarrow 1 = -1$ is not.

Returning to the theorem about falling factorials, it is a simple matter to re-organise the given argument into a correct proof. We simply need to restructure the argument to obtain a chain of equal expressions linking one side of the equation to the other. As in the previous example, it is easiest to work from the expression with two terms towards the expression with a single term.

Correct proof

Suppose n and r are positive integers such that $r < n + 1$. Then

$$\begin{aligned}(n)_r + r(n)_{r-1} &= \frac{n!}{(n-r)!} + r \times \frac{n!}{(n-(r-1))!} \\ &= \frac{n!}{(n-r)!} + r \times \frac{n!}{(n-r+1)!} \\ &= \frac{n!(n-r+1)}{(n-r+1)(n-r)!} + \frac{r \times n!}{(n-r+1)!}\end{aligned}$$

$$
\begin{aligned}
&= \frac{n!(n-r+1)}{(n-r+1)!} + \frac{r \times n!}{(n-r+1)!} \\
&= \frac{n!(n-r+1+r)}{(n-r+1)!} \\
&= \frac{n!(n+1)}{(n-r+1)!} \\
&= \frac{(n+1)!}{(n-r+1)!} \\
&= (n+1)_r.
\end{aligned}
$$

□

3. Another realm in which identities frequently appear is set theory. The basic laws for the algebra of sets are given in the appendix. We shall assume these laws as background knowledge in much the same way that we assume the basic algebraic properties of the real numbers as background knowledge.

The 'standard' method of proving that two sets A and B are equal is to show each is a subset of the other: $A \subseteq B$ and $B \subseteq A$. In a situation where $A = B$ is actually an identity, i.e. it is true for all sets, then using the laws for the algebra of sets often provides a simpler proof. The following example illustrates a proof using the laws. We leave as an exercise to construct an alternative proof by showing that each set is a subset of the other—it is longer and more involved.

Theorem: *For all sets A, B and C, $A - (B \cup C) = (A - B) - C$.*

Proof

Let A, B, and C be arbitrary sets. Then

$$
\begin{aligned}
A - (B \cup C) &= A \cap \overline{(B \cup C)} && \text{(definition of set difference)} \\
&= A \cap (\overline{B} \cap \overline{C}) && \text{(De Morgan's law)} \\
&= (A \cap \overline{B}) \cap \overline{C} && \text{(associative law)} \\
&= (A - B) \cap \overline{C} && \text{(definition of set difference)} \\
&= (A - B) - C && \text{(definition of set difference).}
\end{aligned}
$$

□

4. Consider the following 'solution' of a pair of simultaneous quadratic equations:

$$x^2 + 3x + 2 = 0 \quad \text{(a)}$$
$$2x^2 - 5x + 2 = 0 \quad \text{(b)}$$

'Solution'

From (a) and (b) $\quad x^2 + 3x + 2 = 2x^2 - 5x + 2$

$\Rightarrow \quad x^2 - 8x = 0$

$\Rightarrow \quad x(x - 8) = 0.$

Hence $x = 0$ or $x = 8$.

□

There is clearly a problem here because the 'solutions' $x = 0$ and $x = 8$ satisfy neither of the original equations (a) and (b). So what is wrong with our argument? In fact, there is nothing wrong with the argument itself which establishes the conditional proposition:

if x is a real number such that $x^2 + 3x + 2 = 0$ and $2x^2 - 5x + 2 = 0$ then $x = 0$ or $x = 8$. (*)

The equation $x^2 + 3x + 2 = 0$ has solutions $x = -1, -2$ and the equation $2x^2 - 5x + 2 = 0$ has solutions $x = \frac{1}{2}, 2$. This means that the antecedent, *x is a real number such that $x^2 + 3x + 2 = 0$ and $2x^2 - 5x + 2 = 0$*, is true for no real number x. Therefore the conditional proposition (*) is true for every real number x since it has a false antecedent. This situation will not arise when we are manipulating identities (rather than solving equations) because identities are true for all elements of the appropriate universe.

There is a rule in formal logic (sometimes called the substitution rule) which governs when it is appropriate to add $a = c$ to a formal proof which already contains the lines $a = b$ and $b = c$. The precise statement of the rule is beyond the scope of this text—it involves the notion of free and bound variables. Provided we are careful to interpret an argument which involves the use of the transitive property of equality we can avoid proving true but unhelpful propositions such as (*) above.

Exercises 8.1

Prove each of the following identities.

1. For all real $x \neq 1$, $\dfrac{x^4 - 1}{x - 1} = x^3 + x^2 + x + 1$.

2. For all real numbers x and y, $(x + y)^4 - (x - y)^4 = 8xy(x^2 + y^2)$.

3. For all positive integers k, n such that $k \leq n$,

$$\binom{n}{k} = \frac{n - k + 1}{k} \times \binom{n}{k - 1}.$$

4. For all positive integers n, m, k such that $k \leq m \leq n$,

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n - k}{m - k}.$$

5. For all positive integers n, m, k such that $k \leq m$, $k \leq n$,

$$\binom{n}{k}(m)_k = \binom{m}{k}(n)_k.$$

6. For all positive integers m, n such that $m \geq 2$, $n \geq 2$,

$$\binom{n}{2} + \binom{m}{2} + mn = \binom{m + n}{2}.$$

7. For all positive integers m, n, r such that $m \geq 3$, $n \geq 3$, $r \geq 3$,

$$\binom{n}{3} + \binom{m}{3} + \binom{r}{3} + \binom{n + m + r}{3} = \binom{m + n}{3} + \binom{m + r}{3} + \binom{r + n}{3} + mnr.$$

8. For all positive integers n, r such that $r \leq n + 2$.

$$(n + 2)_r = (n)_r + 2r(n)_{r-1} + r(r - 1)(n)_{r-2}.$$

Give two proofs: (i) using direct algebraic manipulation;
(ii) using the theorem in Example 8.2.2.

9. For all positive integers $m \geq 3$, $n \geq 3$,

$$(m + n)_3 = (m)_3 + 3(m)_2(n)_1 + 3(m)_1(n)_2 + (n)_3.$$

10. For all sets A, B, C which are subsets of some universe $\mathcal{U}$:

(i) $(A \cup B) - C = (A - C) \cup (B - C)$.

(ii) $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$.

(iii) $(A - B) \cap C = (A \cap C) - B$.

(iv) $A - (B \cap C) = (A - B) \cup (A - C)$.

8.3 Use of Counting Arguments

Although counting is apparently an 'elementary' activity, many quite advanced theorems can be proved using counting arguments. In fact, counting can be a complex task and there is a branch of mathematics, called enumeration theory, devoted to techniques of counting. Our aim in this section is to present some simple counting theorems which form the basis of proof techniques.

The first technique provides another method of proving identities. The basic idea is very simple. Suppose the elements of a finite set can be counted in two different ways, providing two expressions for the number of elements of the set. Then, by the transitive and commutative properties of equality, the two expressions must be equal.

The identity counting theorem: *Let A be a finite set such that $|A| = n$ and $|A| = m$, then $n = m$.*

□

Although this theorem is the basis for proofs in many and varied situations, we shall illustrate the technique using an identity involving binomial coefficients $\binom{n}{r}$ and falling factorials $(n)_r$. The reason that such an identity may be proved using a counting argument is that both $\binom{n}{r}$ and $(n)_r$ can be interpreted as the number of ways certain selections can be made from a collection of objects. For completeness, we describe (without justification) the basic results about binomial coefficients and falling factorials below.

Suppose we are given a collection of n distinguishable objects and we wish to select r of the objects. If the order in which the objects are selected is significant in the sense that we count different orderings of a given collection of objects as different selections, then the number of ways of selecting r of the n objects is $(n)_r$. We can think of an ordered

selection as producing a list of objects: $A_1, A_2, \ldots, A_r$. If, on the other hand, the order in which the objects are selected is not significant, the number of ways of selecting r of the n objects is $\binom{n}{r}$. We can think of an unordered selection as producing a set of objects: $\{A_1, A_2, \ldots, A_r\}$.

In summary:

- The number of different lists of length r which can be formed from a collection of n distinguishable objects is $(n)_r$.
- The number of different sets of r elements which can be formed from a collection of n distinguishable objects is $\binom{n}{r}$.

Example 8.3

The following theorem generalises the identities given in Example 8.2.2 and Exercises 8.1.8 and 8.1.9.

Theorem: *Let m, n and r be positive integers such that $r \leq m$ and $r \leq n$. Then*

$$(m+n)_r = \sum_{k=0}^{r} \binom{r}{k} (m)_k \, (n)_{r-k}.$$

Before embarking on the proof, it may be worth reflecting on the difficulty of proving the identity using direct algebraic manipulation. The right-hand side is the sum of $r+1$ terms:

$$\binom{r}{0}(m)_0 \, (n)_r + \binom{r}{1}(m)_1 \, (n)_{r-1} + \binom{r}{2}(m)_2 \, (n)_{r-2} + \cdots + \binom{r}{r}(m)_r \, (n)_0.$$

Clearly, to manipulate this expression with general values of m, n and r would be a fearsome task with a high probability of error.

The key to the proof is to interpret the expressions as the number of ways of counting certain selections.

Proof

Let $S = \{A_1, A_2, \ldots, A_m, B_1, B_2, \ldots, B_n\}$ be a set of $m+n$ distinguishable objects of two different types—the A's and the B's. Suppose we

are to make an ordered selection of r objects from S. Since there are $m+n$ objects in S, this can be done in $(m+n)_r$ ways, which is the left-hand side of the identity. If we can also interpret the right-hand side of the identity as the number of possible ordered selections of r objects from S, the proof will be complete.

Any selection of r objects from S contains k objects of type A and $r-k$ objects of type B for some $k = 0, 1, \ldots, r$. Therefore adding the number of selections with k objects of type A for all values of $k = 0, 1, \ldots, r$ will give the total number of selections. Hence:

$$(m+n)_r = \sum_{k=0}^{r} \left(\begin{array}{l} \text{number of selections with } k \text{ objects of} \\ \text{type } A \text{ and } r-k \text{ objects of type } B. \end{array} \right) \qquad (*)$$

For any particular value of k, an ordered selection of r objects containing k objects of type A and $r-k$ objects of type B can be made as follows.

First make an ordered selection of k objects from $\{A_1, A_2, \ldots, A_m\}$; this can be done in $(m)_k$ different ways.

Next make an ordered selection of $r-k$ objects from $\{B_1, B_2, \ldots, B_n\}$; this can be done in $(n)_{r-k}$ different ways.

Finally we need to 'splice together' these two selections. At this stage, we have two ordered lists:

$A_{i_1}, A_{i_2}, \ldots, A_{i_k}$ (the ordered selection of A's)

and $B_{j_1}, B_{j_2}, \ldots, B_{j_{r-k}}$ (the ordered selection of B's).

Imagine that these $r = k + (r-k)$ objects are to be placed into a row of r boxes, one object per box. To do this we simply need to select k of the boxes to take the A's in order; the remaining $r-k$ boxes will take the B's in order. The number of selections of the k boxes is $\binom{r}{k}$ which represents the number of ways of splicing together the selections of the A's and the B's.

Therefore, the number of ordered selections of r objects containing k objects of type A and $r-k$ objects of type B for any particular value of k is:

$$\binom{r}{k}(m)_k\,(n)_{r-k}.$$

Hence, from equation $(*)$ we have, as required,

$$(m+n)_r = \sum_{k=0}^{r}\binom{r}{k}(m)_k\,(n)_{r-k}.$$

□

Although the detailed explanations given in the proof are somewhat lengthy, this should not obscure its simple structure based on the identity counting theorem. We calculate the number of ways of making a certain selection of objects from a set in two different ways. Since the two expressions are counting the same thing, they must be equal.

Non-constructive Existence Proofs Based on Counting Arguments

Counting the elements of finite sets can also be used to give non-constructive proofs of existence theorems. The method is based on the following simple theorem.

The subset counting theorem: *If A and B are finite sets such that $A \subseteq B$ and $|A| \neq |B|$ then $A \subset B$. Therefore there exists an element of B which does not belong to A.*

Proof

It is clear that, for all finite sets A and B, $A = B \Rightarrow |A| = |B|$. The contrapositive is: $|A| \neq |B| \Rightarrow A \neq B$.

Now suppose that A and B are finite sets such that $A \subseteq B$ and $|A| \neq |B|$. Using the result above, this implies that $A \subseteq B$ and $A \neq B$. Hence A is a proper subset of B, $A \subset B$, so there exists at least one element of B which does not belong to A.

□

With this theorem as the special theorem, the formal proof given on page 210 gives rise to the following method of proof. Note that proofs which follow the method will be non-constructive existence proofs—we can be sure that there exists at least one element of B which is not an element of A without actually finding such an element.

A counting argument for non-constructive existence proofs

Suppose that A and B are finite sets such that the following are true propositions:

1. $A \subseteq B$, 2. $|A| \neq |B|$.

Then there exists at least one element of B which does not belong to A.

This argument may be interpreted in terms of predicates. Let P and Q be predicates such that every object x (in a finite universe) which has property P also has property Q. In other words, $\forall x[P(x) \rightarrow Q(x)]$ is a true proposition. Let $A = \{x : P(x)\}$ and $B = \{x : Q(x)\}$; then $A \subseteq B$. Suppose we can show that the sets A and B have different numbers of elements. It follows that there is at least one element of B which does not belong to A. This means that there exists at least one object x which has property Q but does not have property P, i.e. $\exists x[\neg P(x) \wedge Q(x)]$.

Examples 8.4

1. **Theorem:** *Let G be a finite group with an even number of elements. Then there exists an element $x \in G$ such that $x \neq e$ and $x^{-1} = x$.*

The idea of the proof is to compare the set G with its subset consisting of the identity e together with all those elements for which $g^{-1} \neq g$. We then show that the subset contains a different number of elements from G. Hence there exists at least one element x in G not belonging to the subset and this element satisfies the required conditions: $x \neq e$ and $x^{-1} = x$.

Proof

Let G be a finite group with an even number of elements. Let S be the subset of G comprising the identity element e together with all those elements g such that $g^{-1} \neq g$.

Apart from the identity element (which satisfies $e^{-1} = e$), all the other elements of S may be grouped together in pairs g, g^{-1}. (We are using here the fact that each element of a group has a *unique* inverse—see Exercise 7.4.6). There are clearly an even number of elements which

may be grouped together in pairs like this. Since S also contains the identity element, S has an odd number of elements. But $|G|$ is even, so $|G| \neq |S|$. Therefore there exists an element x belonging to G which does not belong to S and x satisfies the conditions $x \neq e$ and $x^{-1} = x$.

□

2. **Theorem:** *There exist irrational real numbers.*

The non-constructive proof we shall give is due to Georg Cantor[1]. In fact Cantor's method can be used to prove rather more than the existence of a (single) irrational real number, as we shall explain. In the 1870s and 1880s, Cantor developed a theory of infinite sets which allows comparison between the sizes of different infinite sets. At the core of Cantor's theory was his extension of the notion of cardinality to infinite sets. If two finite sets have the same cardinality, then their elements can be placed in **one-to-one correspondence**: each element of the first set can be paired with a unique element of the second and *vice versa*. Extending this idea to arbitrary sets, we say that any two sets have the **same cardinality** if their elements can be placed in one-to-one correspondence. This gives a well-defined notion of cardinality for arbitrary sets. (By 'well-defined' we mean that it satisfies: $A = B \Rightarrow |A| = |B|$.) However, some of the cardinality properties of infinite sets are rather different from the corresponding properties of finite sets. For instance, a finite set cannot have the same cardinality as a proper subset (see Exercise 9.2.8). Surprisingly perhaps, the same is not true for infinite sets. It can be shown, for example, that the set of integers $\mathbb{Z}$ has the same cardinality as the set of rational numbers $\mathbb{Q}$, even though $\mathbb{Z}$ is a proper subset of $\mathbb{Q}$, $\mathbb{Z} \subset \mathbb{Q}$.

To prove our theorem we need a comparison between the sets of rational numbers $\mathbb{Q}$ and real numbers $\mathbb{R}$. Using a clever argument (using the method of proof by contradiction), Cantor showed that these two sets have different cardinalities, that is, $|\mathbb{Q}| \neq |\mathbb{R}|$. (See Garnier and Taylor (1992), for example.)

With this result as part of our background knowledge, we can now use the counting argument for finite sets in Example 1 above as a model for our proof. Of course, we need to assume that, with cardinality defined

[1] Georg Cantor, born in St Petersberg in 1845, trod the fine line between genius and mental illness, especially in his later years when he was plagued by self-doubt. His theory of the infinite, which aroused intense controversy in its day, is now regarded as one of the jewels of modern mathematics.

as above, the subset counting theorem extends from the universe of finite sets to that of arbitrary sets. However, our proof of the subset counting theorem does not refer to the finite nature of the sets and is valid for arbitrary sets.

Proof (of **Theorem:** *There exist irrational real numbers*)

Since every rational number is a real number, we have $\mathbb{Q} \subseteq \mathbb{R}$. However, $|\mathbb{Q}| \neq |\mathbb{R}|$ (Cantor's theorem). Therefore there exists at least one element of $\mathbb{R}$ which is not an element of $\mathbb{Q}$. In other words, there exists at least one real number which is not rational.

□

Although the structure of this proof is simple, it does assume a considerable amount of background knowledge. We have only sketched the bare bones of Cantor's theory and have taken a great deal for granted. For example, Cantor's proof that $|\mathbb{Q}| \neq |\mathbb{R}|$ is quite sophisticated. However, this non-constructive proof gives rather more than the existence of a (single) irrational real number. It can be shown that adding a finite number of elements to an infinite set does not change its cardinality. Since $|\mathbb{Q}| \neq |\mathbb{R}|$, it follows that we cannot add a finite number of elements to $\mathbb{Q}$ and obtain $\mathbb{R}$. Thus there are infinitely many irrational real numbers.

Pigeon hole principle

The pigeon hole principle is a simple observation which is the basis for many existence proofs. To illustrate the principle, suppose seven letters are to be distributed in a rack containing six pigeon holes. Then clearly at least one of the pigeon holes must receive more than one letter. We will shortly state the principle in more mathematical terms. However, the following non-mathematical statement is more memorable and comprehensible than its mathematical counterpart.

The pigeon hole principle

If k objects are placed in n pigeon holes where $k > n$ then some pigeon hole contains more than one object.

It should be clear that the pigeon hole principle is well suited to non-constructive proofs which assert the existence of more than one object of a given type. In mathematical proofs, we do not have actual pigeon holes, of course. The principle is similar to the Subset Counting Theorem in that it compares two finite sets (pigeon holes and objects to be placed in them) containing different numbers of elements. In the pigeon hole principle, however, one of the sets is not a subset of the other. To express the principle more formally in mathematical terms, we need a way of linking the set of pigeon holes with the set of objects. Let A denote the set of objects and B the set of pigeon holes. Define a function

$$f: A \to B \text{ by } f(\textit{object}) = \textit{pigeon hole in which it is placed.}$$

To say that some pigeon hole contains more than one object is equivalent to saying that there exist two objects, *object* 1 and *object* 2, such that

$$f(\textit{object } 1) = f(\textit{object } 2).$$

A function with this property is said to be **not injective**. We can therefore state the pigeon hole principle in mathematical terms as follows.

Pigeon hole theorem: *If $f: A \to B$ is a function between finite sets where $|A| > |B|$, then f is not injective. Hence there exist $a_1, a_2 \in A$ such that $a_1 \neq a_2$ and $f(a_1) = f(a_2)$.*

Proof

Let $f : A \to B$ be a function between finite sets such that $|A| > |B|$.

The proof uses the subset counting theorem. Define a subset C of A by

$$C = \{a \in A : f(a) \neq f(x) \text{ for any } x \in A\}.$$

Informally, C is the subset of those objects which are placed in a pigeon hole by themselves. The set C certainly has no more elements than B itself. Since $|C| \leq |B|$ and, by hypothesis, $|A| > |B|$, we have $|C| < |A|$ so $|C| \neq |A|$. This shows that C and A satisfy the hypotheses of the subset counting theorem. Therefore there exists an element a of A not belonging to C. Since a does not belong to C,

there exists an $x \in A - \{a\}$ such that $f(x) = f(a)$, so f is not injective, as required.

□

Examples 8.5

1. **Theorem:** *In any set containing 6 distinct positive integers there exists a pair whose difference is a multiple of 5.*

Proof

Let $\{a_1, a_2, a_3, a_4, a_5, a_6\}$ be a set of six distinct positive integers and let $r_1, r_2, r_3, r_4, r_5, r_6$ be their respective remainders after division by 5. Since there are only five possible values for the remainders (0, 1, 2, 3 or 4), it follows by the pigeon hole principle that at least two of the remainders are equal, say $r_i = r_j$. Therefore $a_i - a_j$ has remainder 0 after division by 5, so that $a_i - a_j$ is a multiple of 5.

□

The role of the pigeon holes in this example is played by the potential remainders after division by 5. Each of the elements of the set is 'placed' in the pigeon hole labelled by its remainder. In the proof itself the analogy between the possible remainders and pigeon holes is not made explicitly.

Using the mathematical formulation, we could write the proof as follows.

Proof

Let $S = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ be a set of six positive integers and define a function

$$f: S \to \{0, 1, 2, 3, 4, 5\}$$

$$f(a_i) = \text{remainder when } a_i \text{ is divided by 5.}$$

Since $|\{a_1, a_2, a_3, a_4, a_5, a_6\}| > |\{0, 1, 2, 3, 4\}|$, the pigeon hole theorem implies that f is not injective. Therefore, there exist elements $a_i \neq a_j$ of S such that $f(a_i) = f(a_j)$. In other words, there exist two distinct elements of S with the same remainder after division by 5. The difference between these two elements is therefore a multiple of 5.

□

2. The following example is, in fact, a theorem in graph theory. We have formulated the statement of the theorem here in non-graph-

theoretic terms. For the graph theory version of the theorem, see Exercise 8.2.2(iv).

Theorem: *Let S be a network of bus stations connected by various bus routes. Suppose, further, that there are n bus stations and m bus routes connecting them, where each route connects exactly two stations. If $m > \frac{1}{2}n(n-1)$ then there exists a pair of bus stations connected by at least two distinct bus routes.*

Proof

Since each bus route connects exactly two stations, we need to compare the number of bus routes with the number of *pairs* of bus stations.

To define a pair of bus stations we need to select 2 stations from the n given. This can be done in $\binom{n}{2} = \frac{1}{2}n(n-1)$ ways—see page 221. Therefore there are $\frac{1}{2}n(n-1)$ pairs of bus stations. Since $m > \frac{1}{2}n(n-1)$, the number of routes m is greater than the number of pairs of stations. Therefore, there exists a pair of stations connected by more than one route, by the pigeon hole principle.

□

In the proof, the role of the pigeon holes is taken by the set of *pairs* of bus stations and the role of the objects is taken by the bus routes. Each bus route is 'placed in' the pigeon hole corresponding to the bus stations which it connects. In the mathematical formulation, define sets $A = \{\text{bus routes}\}$, $B = \{\text{pairs of bus stations}\}$ and define a function

$$f : A \to B,$$

$f(\textit{bus route}) = \textit{the pair of bus stations which the route connects.}$

Exercises 8.2

1. Use counting arguments to prove each of the following identities.

(i) For all positive integers n, k such that $k \leq n$,

$$(n)_k = \binom{n}{k} (k)_k.$$

(ii) For all positive integers m, n and r such that $r \leq m$, $r \leq n$,

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}.$$

(iii) For all positive integers n, r such that $1 < r < n+1$,

$$(n+1)_r = (n)_r + r(n)_{r-1}.$$

(This identity was proved using algebraic manipulation in Example 8.2.2.)

(iv) The identity given in Exercise 8.1.6.

2. A **graph** is a mathematical object which comprises a set of **vertices** and a set of **edges** such that each edge connects either a pair of distinct vertices or a vertex with itself. Graphs can be represented by diagrams such as Figure 8.1. (For further details, see Garnier and Taylor (1992), for example.)

First some terminology: A **loop** is an edge connecting a vertex to itself. If v is a vertex of a graph, its **degree** is the number of edges connecting it except that each loop contributes 2 towards the degree of the vertex which it connects to itself.

Prove each of the following theorems about graphs, using counting arguments.

(i) In any graph, the sum of all the vertex degrees is twice the number of edges.

This result is known as the **handshaking lemma**—why?

(ii) In any graph, the number of vertices which have odd degree is even.

(iii) A graph is **regular of degree r** if every vertex has degree r.

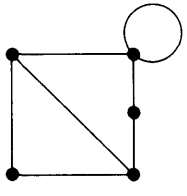


Figure 8.1

A graph which has n vertices and is regular of degree r has $\frac{1}{2}nr$ edges.

(iv) If a graph has no loops, n vertices and m edges, where $m > \frac{1}{2}n(n-1)$, then there exists a pair of vertices which is connected by more than one edge.
(This is the graph-theoretic version of the theorem proved in Example 8.5.2.)

3. (i) Prove the identity

$$3^n = 2^n + \binom{n}{1}2^{n-1} + \binom{n}{2}2^{n-2} + \cdots + \binom{n}{n-1}2 + 1$$

$$= \sum_{k=0}^{n} \binom{n}{k} 2^{n-k}.$$

Hint: Consider the number of sequences of length n which can be constructed from the letters a, b, c; then consider the number of times the letter a occurs in such a sequence.

(ii) By considering the number of sequences in part (i) where a occurs an even number of times, prove the identity

$$\frac{3^n + 1}{2} = 2^n + \binom{n}{2}2^{n-2} + \binom{n}{4}2^{n-4} + \cdots + \binom{n}{q}2^{n-q}$$

where $q = \begin{cases} n & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd.} \end{cases}$

(iii) Generalise your argument from part (i) to prove the identity

$$r^n = (r-1)^n + \binom{n}{1}(r-1)^{n-1} + \binom{n}{2}(r-1)^{n-2} +$$

$$\cdots + \binom{n}{n-1}(r-1) + 1 = \sum_{k=0}^{n} \binom{n}{k} (r-1)^{n-k}.$$

4. (a) Prove that, for any set of five points located in a rectangle of dimensions 6 units by 8 units, there exists a pair which are no more than 5 units apart.

(b) Prove that, for any set of $n^2 + 1$ points in a square of side n, there exists a pair which are no more than $\sqrt{2}$ units apart.

(c) Prove that, for any set of $n^2 + 1$ points in an equilateral triangle of side n, there exists a pair which are no more than 1 unit apart.

5. Prove that in any collection of 12 distinct integers chosen from the set $\{1, 2, 3, \ldots, 30\}$ there exists a pair with common factor greater than 1.

6. Let G be a finite group with $|G| = n$ and let g be an element of G. Prove that $g^k = e$ for some positive integer $k \leq n$.

7. Prove the following **generalised pigeon hole principle**.

If k objects are placed in n pigeon holes where $k > rn$ (and r is a positive integer) then some pigeon hole contains more than r objects.

8. Use the generalised pigeon hole principle (see Exercise 7) to prove each of the following theorems.

(a) In any set of 750 people there exist three people with the same birthday (day and month, but not necessarily year, of birth).

(b) If a pair of dice are thrown 45 times there exists a score which occurred (at least) five times.

(c) In a certain lottery, six numbers are drawn at random each week from the set $\{1, 2, 3, \ldots, 49\}$ to determine a winner. Prove that, in a year of lottery draws, some number was drawn on at least seven occasions.

8.4 The Method of Exhaustion

Suppose a universally quantified propositional function $\forall x\, P(x)$ is defined over a finite universe $A = \{a_1, a_2, \ldots, a_n\}$. Then the proposition $\forall x\, P(x)$ is equivalent to $P(a_1) \wedge P(a_2) \wedge \cdots \wedge P(a_n)$. So to prove $\forall x\, P(x)$, it is sufficient to prove each of the propositions $P(a_1), P(a_2), \ldots, P(a_n)$ separately. A proof of $\forall x\, P(x)$ which follows this approach is called a 'proof by exhaustion' because it exhausts each of the elements of the universe $a_1, a_2, \ldots, a_n$ in turn. We leave it as an exercise to construct the formal proof underlying this method.

Note that the inference

$$P(a_1) \wedge P(a_2) \wedge \cdots \wedge P(a_n) \Rightarrow \forall x\, P(x)$$

Proof by exhaustion

is not quite the same as an inference justified by universal generalisation, UG. In the case of UG, we prove $P(a)$ where a is an arbitrary element of the universe and then infer $\forall x\, P(x)$. In other words, $P(a)$ is proved for a single, arbitrary element of the universe, rather than for each and every element of the universe as is the case with a proof by exhaustion.

The method of proof by exhaustion outlined above is not very widely used. It is really feasible to use the technique only if the finite universe $A = \{a_1, a_2, \ldots, a_n\}$ is reasonably small. If n is large, the work involved in proving $P(a_i)$ for every element a_i is formidable. However, it is more often feasible to prove $P(a)$ for each of several possible *cases* rather than for each of many elements. (We saw this technique used in Example 5.3.) We could refer to this as *exhaustion of cases* rather than *exhaustion of elements* as described above. There is the added advantage that, even if the universe A is infinite (so that exhaustion of elements would be impossible) there may still be only finitely many cases to consider. This was the situation in Example 5.3. As we shall explain, exhaustion of elements is, in fact, a special case of exhaustion of cases, so we concentrate our attention on the latter.

The following theorem is the special theorem for the method of proof by exhaustion of cases. It is essentially a re-statement of the definition of the union of n sets (see the appendix).

Union theorem: *Suppose* $A = A_1 \cup A_2 \cup \cdots \cup A_n$. *Then* $x \in A$ *if and only if* $x \in A_i$ *for some* $i = 1, 2, \ldots, n$.

Let $\forall x\, P(x)$ be a quantified propositional function where x is defined over a universe A and let $A = A_1 \cup A_2 \cup \cdots \cup A_n$. We regard the subsets

$A_1, A_2, \ldots, A_n$ as defining separate cases. Suppose we can prove the theorem $\forall x\, P(x)$ when x is defined over each of the 'sub-universes' A_i in turn. Then, by the union theorem, it follows that $\forall x\, P(x)$ is a true proposition for x defined over the whole universe A.

Note that the condition $A = A_1 \cup A_2 \cup \cdots \cup A_n$ does not imply that the cases are mutually exclusive. In other words, we may have $A_i \cap A_j \neq \varnothing$ for some i and j. Most frequently, however, we would consider mutually exclusive cases. For example, to prove a theorem about the real numbers we would probably not consider $x \geq 0$ and $x \leq 0$ as separate cases since they both include the case $x = 0$. It would, of course, be sufficient to prove the theorem for $x \geq 0$ and $x \leq 0$ but the mutually exclusive cases $x \geq 0$ and $x < 0$ would also suffice.

A collection of non-empty subsets $A_1, A_2, \ldots, A_n$ of a set A which satisfy the conditions

- $A = A_1 \cup A_2 \cup \cdots \cup A_n$
- $A_i \cap A_j = \varnothing$ for all $i \neq j$

is called a (finite) **partition** of the set A. In this situation we may strengthen the conclusion of the union theorem to state that: $x \in A$ *if and only if* $x \in A_i$ *for a unique* $i \in \{1, 2, \ldots, n\}$. In terms of cases, this is the situation where the cases are mutually exclusive and, although this is not necessary for the method summarised below, it is usual.

Proof by exhaustion

Suppose that $\forall x\, P(x)$ is defined over the universe A where

$$A = A_1 \cup A_2 \cup \cdots \cup A_n.$$

If $\forall x\, P(x)$ is a true proposition when x is defined over each universe $A_1, A_2, \ldots, A_n$ in turn, then $\forall x\, P(x)$ is a true proposition when x is defined over the universe A.

As we have mentioned, a universe A such that $A = A_1 \cup A_2 \cup \cdots \cup A_n$ can be thought of as defining separate cases and thus gives rise to the method of proof by exhaustion of cases. How does the method of proof by exhaustion of elements, considered at the beginning of the section, fit into this framework? Suppose $A = \{a_1, a_2, \ldots, a_n\}$ is a finite universe. Then the sets $A_1 = \{a_1\}$, $A_2 = \{a_2\}, \ldots, A_n = \{a_n\}$ define a partition of A

and, for each subset A_i, the theorem $\forall x\, P(x)$ defined over universe A_i is equivalent to the proposition $P(a_i)$. Therefore, proving $\forall x\, P(x)$ for each sub-universe amounts to proving propositions $P(a_1), P(a_2), \ldots, P(a_n)$ and we recover the original proof by exhaustion of elements. In other words, proof by exhaustion of elements is simply a special case of our method of proof by exhaustion (of cases).

Examples 8.6

1. Recall from Exercise 7.1.3 that the operation of multiplication modulo 8 is defined on the set $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ by:

$$n \times_8 m = \text{remainder when } nm \text{ is divided by 8.}$$

Theorem: *The equation $x^2 = 5$ has no solution in $\mathbb{Z}_8$.*

Note that we use x^2 as shorthand for $x \times_8 x$. Since the universe $\mathbb{Z}_8$ is finite (and, indeed, not too large) the method of proof by exhaustion of elements seems to be an appropriate strategy.

Proof

In $\mathbb{Z}_8$ we have:

$$0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 1,\ 4^2 = 0,\ 5^2 = 1,\ 6^2 = 4,\ 7^2 = 1.$$

(For example, $5^2 = 5 \times_8 5 =$ (remainder when 25 is divided by 8) $= 1$.)

Therefore each $x \in \mathbb{Z}_8$ satisfies $x^2 \neq 5$, and the theorem is proved, by exhaustion.

□

2. (Example 5.3 revisited.)

Theorem: *For all real numbers x and y, $|x + y| \leq |x| + |y|$.*

In Example 5.3, we gave two proofs of this theorem, both based on a consideration of cases. It is not our intention to re-prove the theorem here, but to show how the proofs in Example 5.3 fit into the framework outlined above.

The first proof given in Example 5.3 split the proof into the following four cases:

1. $x \geq 0, \quad y \geq 0.$
2. $x \geq 0, \quad y < 0.$
3. $x < 0, \quad y \geq 0.$
4. $x < 0, \quad y < 0.$

The theorem is of the form of a doubly quantified propositional function $\forall x \forall y\, P(x,y)$ where x and y are defined over the universe of real numbers. Since the cases deal with x and y separately, it is not immediately clear how to fit the four cases into our framework. One approach is to regard the theorem as having the form $\forall (x,y)\, P(x,y)$ defined over the universe $\mathbb{R}^2$ of all ordered pairs of real numbers (x,y). Let A_1, A_2, A_3, A_4 be the following subsets of $\mathbb{R}^2$:

$$A_1 = \{(x,y) \in \mathbb{R}^2 : x \geq 0, y \geq 0\}$$
$$A_2 = \{(x,y) \in \mathbb{R}^2 : x \geq 0, y < 0\}$$
$$A_3 = \{(x,y) \in \mathbb{R}^2 : x < 0, y \geq 0\}$$
$$A_4 = \{(x,y) \in \mathbb{R}^2 : x < 0, y < 0\}.$$

These subsets A_1, A_2, A_3, A_4 form a partition of the universe $\mathbb{R}^2$. Each of the cases given in the first proof of Example 5.3 is the proof of the proposition $\forall (x,y)\, P(x,y)$ over one of the sub-universes A_i.

The second proof given in Example 5.3 has a slightly different structure. First the mini-theorem, *for all real numbers* a, $a \leq |a|$, was proved; using this, the main theorem was then proved. Recall that a theorem proved before a 'main' theorem in order to assist in its proof is often called a lemma. To prove the lemma, two cases were considered corresponding to the partition of the universe $\mathbb{R}$ into two subsets $\{x \in \mathbb{R} : x \geq 0\}$ and $\{x \in \mathbb{R} : x < 0\}$. Having proved the lemma, by exhaustion of cases, the main theorem was then proved by a direct argument without having to resort to cases.

Exercises 8.3

1. Prove each of the following theorems about multiplication modulo 8 defined on the universe $\mathbb{Z}_8$.

Hint: it may help to draw up a multiplication table showing all the possible products $n \times_8 m$ in $\mathbb{Z}_8$.

(i) If $x \times_8 y = 2$ then either x or y is equal to 2 or 6.

(ii) For all $x \in \mathbb{Z}_8$, $x^3 = 0$ or $x^3 = x$.

(iii) For all integers $n \geq 2$, $4^n = 0$ in $\mathbb{Z}_8$.

(iv) For all $b \in \mathbb{Z}_8$, the equation $3 \times_8 x = b$ has a unique solution for x.

(v) If $x \neq 0$, then $x = 3 \times_8 x$ if and only if $x = 4$.

(vi) If $x \neq 0$, then $2 \times_8 x = 6 \times_8 x$ if and only $x = 2, 4$ or 6.

2. Prove each of the following considering cases where necessary.

(a) For all integers n, if n is not a multiple of 3 then n^2 has remainder 1 after division by 3.

(b) For all integers n, n^2 has remainder 0 or 1 after division by 4.

(c) For all integers n, if n is not a multiple of 5 then n^4 has remainder 1 after division by 5.

3. By considering cases when appropriate, prove each of the following theorems.

(a) For all real numbers x and y, $|xy| = |x||y|$.

(b) For all real numbers x and y, $|x - y| \geq ||x| - |y||$.

(c) For all real numbers x and y, $\max\{x, y\} = \frac{1}{2}(x + y + |x - y|)$ where $\max\{x, y\}$ is the larger of x and y.

(d) For all real numbers x and y, $\min\{x, y\} = \frac{1}{2}(x + y - |x - y|)$ where $\min\{x, y\}$ is the smaller of x and y.

4. By considering the possible remainders after division by 12, prove each of the following.

(i) If k is an integer such that $k - 1$ is divisible by 3 and $k(k - 1)$ is divisible by 12, then $k = 12n + 1$ or $k = 12n + 4$ for some integer n.

(ii) If k is an integer such that $k - 1$ is divisible by 4 and $k(k - 1)$ is divisible by 12, then $k = 12n + 1$ or $k = 12n + 9$ for some integer n.

(iii) For every integer k, k^2 is of the form $12n, 12n + 1, 12n + 4$ or $12n + 9$ for some integer n.

5. Prove each of the following theorems over the universe of sets.

(a) If $A \subseteq X$ and $B \subseteq X$ then $(A \cup B) \subseteq X$.
(b) For all sets $A, B, X, (A \cup B) \times X = (A \times X) \cup (B \times X)$.

9 Mathematical Induction

9.1 The Principle of Mathematical Induction

In this chapter, we consider a method of proof which is important because of its applicability to a large family of useful theorems. As with the proof techniques considered in the last chapter, this one relies upon a special theorem which constitutes essential background knowledge. This theorem is generally known as 'the principle of mathematical induction' and the method of proof which it sanctions is referred to as 'proof by mathematical induction'. (However, note that, despite its misleading title, this is nevertheless a deductive method of proof. As we pointed out in Chapter 1, inductive reasoning is not acceptable as a mathematical proof.)

There are many mathematical theorems which can be formulated as $\forall n\, P(n)$ where the universe of discourse for n is $\mathbb{N}$, the set of natural numbers. Consider, for example, the following:

(a) The sum of the first $n+1$ natural numbers is $n(n+1)/2$,

$$\text{i.e. } \sum_{i=0}^{n} i = 0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ for all } n \in \mathbb{N}.$$

(b) For every natural number n, $2^{n+2} + 3^{2n+1}$ is divisible by 7.

(c) For all natural numbers n, a set with cardinality n has power set with cardinality 2^n, i.e. if A is a set such that $|A| = n$, then $|\mathcal{P}(A)| = 2^n$ for all $n \in \mathbb{N}$.

What these theorems have in common is that each can be expressed as a universally quantified propositional function with the natural numbers as the universe of discourse. For instance, if we define the following propositional functions on the universe $\mathbb{N}$:

$P(n)$: $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$;

$Q(n)$: $2^{n+2} + 3^{2n+1}$ is divisible by 7;

$R(n)$: $|A| = n$ (where A denotes a set);

$S(n)$: $|\mathcal{P}(A)| = 2^n$ (where $\mathcal{P}(A)$ denotes the power set of the set A);

the three theorems above may then be written:

(a) $\forall n\, P(n)$;
(b) $\forall n\, Q(n)$;
(c) $\forall n[R(n) \rightarrow S(n)]$.

Note that a theorem which can be expressed as a propositional function universally quantified over the natural numbers may not be asserting some property of the set $\mathbb{N}$ itself. Of the three theorems above, the first states that some property is shared by all natural numbers. It is therefore a theorem *about* natural numbers. However, the second theorem is about integers of the form $2^{n+2} + 3^{2n+1}$ (where $n \in \mathbb{N}$) and the third theorem concerns sets. Nevertheless both of these can be expressed in the form $\forall n\, T(n)$ where the universe is $\mathbb{N}$ and they are therefore members of the family of theorems which concern us in this chapter.

The difficulty with proving theorems of this type is that we must show that the appropriate propositional function is true for all values of n within the universe of discourse, i.e. for all natural numbers. Verifying that the propositional functions are true for particular values of n is not usually a problem. For instance, substituting $n = 4$ in $2^{n+2} + 3^{2n+1}$ gives $2^6 + 3^9 = 64 + 19683 = 19747 = 2821 \times 7$, so that $Q(n)$ is true when $n = 4$, i.e. $Q(4)$ is a true proposition. In a similar way, we can check that $P(n)$ is true for, say, $n = 10$: $0 + 1 + 2 + \cdots + 9 + 10 = 55 = (10 \times 11)/2$. This verifies that $P(10)$ is a true proposition. However, no matter how many natural numbers we substitute for n, this will not constitute a proof that the propositional function is true for *all* values in the universe. All it can show is that the propositional function is a theorem for the specific values of n which we have checked.

The method of proof known as 'mathematical induction' gives us an alternative to direct proof in the case where the universe of discourse is $\mathbb{N}$. It depends upon an axiom of the natural numbers which can be stated as follows.

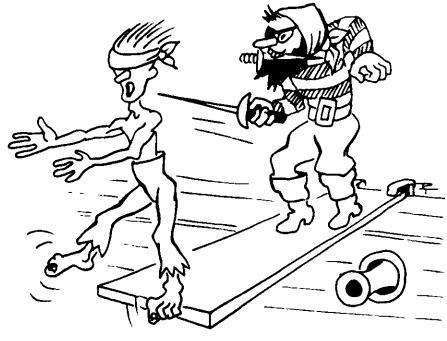
Axiom of induction

Suppose that S is a subset of $\mathbb{N}$ and that the following are true propositions:

(a) $0 \in S$,
(b) $\forall n[n \in S \rightarrow (n + 1) \in S]$.

Then S contains all the natural numbers, i.e. $S = \mathbb{N}$.

If we consider for a moment exactly what this axiom is saying, we shall see that it has an intuitive appeal. Proposition (b) (strictly, the proposition obtained by applying UI to proposition (b)) states that the set S is such that, if it contains any particular natural number, k say, then it also contains the natural number which follows k, that is $k + 1$. Proposition (a) states that 0 belongs to S. Hence, from the truth of (b), we can conclude that $0 + 1 = 1$ also belongs to S. Since 1 is a member of S, we deduce that $1 + 1 = 2$ is an element of S. Since this chain of deduction can (in theory at least) be continued indefinitely, we can conclude that all the natural numbers belong to S. Of course, this line of reasoning does not constitute a proof of what is stated in the axiom, although it could be used to prove that $k \in S$ for any specific k, no matter how large. Extending the argument to prove that $k \in S$ for any natural number would necessitate an infinite number of steps and therefore no such proof could be constructed. (Indeed, proofs are *defined* as having only a finite number of steps.) Hence the necessity for the axiom.



A finite number of steps

Suppose that, given a theorem such as one of the three stated at the beginning of this section, we define S to be the subset of the natural numbers for which the associated propositional function is a true proposition. This means that, if the theorem can be stated as the quantified propositional function $\forall n\, F(n)$, then S contains all those natural numbers for which $F(n)$ is true. Hence we can write $S = \{n \in \mathbb{N} : F(n) \text{ is true}\}$. With this interpretation, the truth of '$0 \in S$' ((a) in the axiom above) is equivalent to '$F(0)$ is true', and proposition (b) in the axiom, $\forall n[n \in S \rightarrow (n+1) \in S]$, is equivalent to $\forall n[F(n) \rightarrow F(n+1)]$. If $F(0)$ and $\forall n[F(n) \rightarrow F(n+1)]$ are both true propositions, the final part of the axiom will then allow us to deduce that $S = \mathbb{N}$. For the set S which we have defined, this is equivalent to saying that $F(n)$ is true for all natural numbers n, i.e. $\forall n\, F(n)$ is a true proposition. This interpretation of the axiom is a theorem known as **the principle of mathematical induction**. We state this formally below.

Principle of mathematical induction

Suppose that $F(n)$ is a propositional function with universe of discourse $\mathbb{N}$ and that the following are true propositions:

(a) $F(0)$,
(b) $\forall n[F(n) \rightarrow F(n+1)]$.

Then $\forall n\, F(n)$ is a true proposition.

The principle of mathematical induction points to a method whereby we may prove theorems which can be stated in the form $\forall n\, F(n)$ where $n \in \mathbb{N}$. We first show that the conditions stated in the principle are satisfied. This necessitates verifying that:

(a) $F(0)$ is a true proposition, and
(b) $\forall n[F(n) \rightarrow F(n+1)]$ is a true proposition.

These two stages are essential to any proof which appeals to the principle of mathematical induction. They amount to proving two 'sub-theorems'—$F(0)$ and $\forall n[F(n) \rightarrow F(n+1)]$. Proving the first (that is, checking that $F(0)$ is true) is referred to as the **initial step** or **basis of induction**. This is usually a simple matter. The proof of the second sub-theorem is known as the **inductive step**. This is carried out in the usual

way by proving that $F(k) \rightarrow F(k+1)$ is a true proposition when k is an arbitrary member of the universe $\mathbb{N}$. The sub-theorem follows from applying universal generalisation (UG) to this result. However, explicit mention of the application of UG is nearly always omitted in more informal proofs and the inductive step often terminates once the truth of $F(k) \rightarrow F(k+1)$ is established. Usually, the proof of $F(k) \rightarrow F(k+1)$ will be achieved using the method of conditional proof. We add $F(k)$, referred to as the **induction hypothesis**, to our set of assumptions and we show that the truth of $F(k+1)$ necessarily follows. Once the initial and inductive steps have been completed, we can then use the principle of mathematical induction to deduce the theorem $\forall n\, F(n)$. A proof which has this overall structure is often referred to informally as a 'proof by induction' although it is nevertheless a deductive proof.

For a proof which utilises mathematical induction, the underlying formal proof will include the axiom of induction along with other axioms of the system and the principle of mathematical induction as a theorem. The general structure of the underlying formal proof is shown below.

Proof by mathematical induction

1.	A_1		axioms (including the axiom of induction)
⋮			
n.	A_n		
$n+1$.	T_1		theorems (including the principle of mathematical induction)
⋮			
$n+m$.	T_n		
⋮			Initial step
r.	$F(0)$		
$r+1$.	$F(k)$	(CP—induction hypothesis)	Inductive step
⋮			
s.	$F(k+1)$		
$s+1$.	$F(k) \rightarrow F(k+1)$	$((r+1) - s.$ CP)	
$s+2$.	$\forall n[F(n) \rightarrow F(n+1)]$	$(s+1.$ UG)	
$s+3$.	$\forall n\, F(n)$	$(r, s+2.$ Principle of mathematical induction.)	

There is an analogy which may be useful in clarifying the structure of a proof by mathematical induction. Consider an infinite row of fireworks numbered 0, 1, 2, ... connected together so that each is ignited by its immediate predecessor in the line. The process of arranging the set-up so that the firework numbered k will ignite that numbered $k + 1$ is analogous to the inductive step. However, nothing happens until the first firework in the line is ignited. This stage corresponds to the initial step which is necessary to set the whole process into operation. Once the initial step is carried out and firework number 0 is lit, it sets off the second (numbered 1) which sets off the third and so on to the 'end' of the infinite line. What the axiom of induction tells us is that, under certain conditions, we can be sure that all the fireworks will light even if we don't actually observe them. If we know that they are set up properly (analogous to the inductive step) and that the first has been lit (analogous to the initial step) then we can be secure in the knowledge that every one in the line will ignite.

Proof by induction

We now illustrate the method by proving the theorems (a), (b) and (c) stated at the beginning of this section.

Examples 9.1

1. **Theorem**: *The sum of the first* $n + 1$ *natural numbers is* $n(n + 1)/2$.

Proof

Defining $P(n): \sum_{i=0}^{n} i = n(n+1)/2$ as before, we commence with the initial step and show that $P(0)$ is a true proposition. Taking the left hand side of the equation and substituting $n = 0$ gives:

$$\sum_{i=0}^{0} i = 0.$$

Substituting $n = 0$ in the right hand side gives:

$$\frac{0(0+1)}{2} = 0.$$

Hence the equation holds for $n = 0$ so that $P(0)$ is true. This completes the initial step.

We now proceed to the inductive step. We add the induction hypothesis, $P(k)$ (where k is an arbitrary member of the universe), to our list of assumptions, i.e. we assume that the sum of the first $k+1$ natural numbers, $0+1+2+\cdots+k$, is $k(k+1)/2$. The sum of the first $k+2$ natural numbers, $0+1+2+\cdots+k+(k+1)$, is then obtained by adding $k+1$ to $k(k+1)/2$. In this way we show that the truth of $P(k)$ guarantees the truth of $P(k+1)$. It helps to bear in mind that $P(k+1)$ is obtained from $P(n)$ by replacing n by $k+1$. Hence $P(k+1)$ is

$$\sum_{i=0}^{k+1} i = [(k+1)(k+1+1)]/2$$

or equivalently,

$$\sum_{i=0}^{k+1} i = [(k+1)(k+2)]/2.$$

The inductive step proceeds as follows:

$$\text{Suppose} \quad \sum_{i=0}^{k} i = 0+1+2+\cdots+k$$

$$= \frac{k(k+1)}{2} \quad \text{(induction hypothesis).}$$

$$\text{Then} \quad \sum_{i=0}^{k+1} i = 0+1+2+\cdots+k+(k+1)$$

$$= \left(\sum_{i=0}^{k} i\right) + (k+1)$$

$$= \frac{k(k+1)}{2} + k + 1 \quad \text{(from the induction hypothesis)}$$
$$= \frac{k^2 + k + 2k + 2}{2}$$
$$= \frac{k^2 + 3k + 2}{2}$$
$$= \frac{(k+1)(k+2)}{2}.$$

We have established the truth of $P(k+1)$ and hence of $P(k) \rightarrow P(k+1)$ for an arbitrary natural number k. This completes the inductive step and we deduce that $\forall n[P(n) \rightarrow P(n+1)]$ is a true proposition through the tacit application of UG.

We have now proved conditions (a) and (b) of the principle of mathematical induction. It follows that $\forall n\, P(n)$ is a theorem, i.e. that $\sum_{i=0}^{n} i = n(n+1)/2$ where n is any natural number.

□

Our proof as presented contains much more in the way of detailed explanation than would normally be given and something along the following lines would be acceptable as a proof of the theorem.

Proof

Define $P(n)$: $\displaystyle\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$

Then $\displaystyle\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}.$

Hence $P(0)$ is true.

Suppose that $P(k)$ is true for an arbitrary $k \in \mathbb{N}$,

i.e. $\displaystyle\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$ (induction hypothesis).

Then $\displaystyle\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + (k+1)$

$$= \frac{k(k+1)}{2} + k + 1 \quad \text{(by the induction hypothesis)}$$

$$= \frac{k^2 + k + 2k + 2}{2}$$
$$= \frac{k^2 + 3k + 2}{2}$$
$$= \frac{(k+1)(k+2)}{2}.$$

Hence $P(k) \Rightarrow P(k+1)$ for an arbitrary $k \in \mathbb{N}$ and therefore it follows by mathematical induction that $\sum_{i=0}^{n} i = n(n+1)/2$ for all $n \in \mathbb{N}$.

□

2. **Theorem**: *For every natural number* n, $2^{n+2} + 3^{2n+1}$ *is divisible by* 7.

Proof

As before, we define $Q(n)$ to be the propositional function '$2^{n+2} + 3^{2n+1}$ is divisible by 7'. The condition that the expression $2^{n+2} + 3^{2n+1}$ is divisible by 7 simply means that it can be written as 7 multiplied by some integer. Hence, an equivalent but more convenient interpretation for this propositional function is $Q(n) : 2^{n+2} + 3^{2n+1} = 7a$ for some integer a.

We commence with the initial step and show that $Q(0)$ is true, i.e. we show that when we substitute $n = 0$ in the expression $2^{n+2} + 3^{2n+1}$, the result is divisible by 7.

$$2^{0+2} + 3^{(2\times 0+1)} = 2^2 + 3^1$$
$$= 4 + 3$$
$$= 7$$
$$= 7 \times 1.$$

Hence $Q(0)$ is true and we have completed the initial step.

We now proceed with the inductive step. The induction hypothesis is $Q(k) : 2^{k+2} + 3^{2k+1}$ is divisible by 7. We start by assuming that this is true. Now $Q(k+1)$ is the proposition '$2^{k+1+2} + 3^{2(k+1)+1}$ is divisible by 7'; in other words, '$2^{k+3} + 3^{2k+3} = 7b$ for some integer b'. Hence the inductive step consists of using the fact that $2^{k+2} + 3^{2k+1}$ is divisible by 7 to show that $2^{k+3} + 3^{2k+3}$ also has a factor 7.

Assume $2^{k+2} + 3^{2k+1} = 7c$ for some integer c (induction hypothesis).

Now $$\begin{aligned} 2^{k+3} + 3^{2k+3} &= 2 \times 2^{k+2} + 3^2 \times 3^{2k+1} \\ &= 2 \times 2^{k+2} + 9 \times 3^{2k+1}. \end{aligned}$$

We now make use of the induction hypothesis and substitute $7c - 3^{2k+1}$ for 2^{k+2} in the last equation. (We could equally well use the induction hypothesis to substitute for 3^{2k+1}.)

We have $$\begin{aligned} 2^{k+3} + 3^{2k+3} &= 2 \times 2^{k+2} + 9 \times 3^{2k+1} \\ &= 2(7c - 3^{2k+1}) + 9 \times 3^{2k+1} \quad \text{(from the induction hypothesis)} \\ &= 14c - 2 \times 3^{2k+1} + 9 \times 3^{2k+1} \\ &= 14c + 7 \times 3^{2k+1} \\ &= 7(2c + 3^{2k+1}). \end{aligned}$$

Now, since c is an integer, then so is $2c + 3^{2k+1}$. Hence we have completed the inductive step. We have shown $Q(k) \Rightarrow Q(k+1)$ for an arbitrary k in the universe so that $\forall n[Q(n) \rightarrow Q(n+1)]$ is a true proposition.

Finally, the principle of mathematical induction allows us to deduce that $\forall n\, Q(n)$ is a theorem, i.e. for every natural number n, $2^{n+2} + 3^{2n+1}$ is divisible by 7.

□

The proof with extraneous explanations omitted might be written as follows.

Proof

Define $Q(n)$: $2^{n+2} + 3^{2n+1} = 7a$ for some integer a.

We have $$\begin{aligned} 2^{0+2} + 3^{2\times 0+1} &= 2^2 + 3^1 \\ &= 7 \\ &= 7 \times 1. \end{aligned}$$

Hence $Q(0)$ is true.

Assume that for an arbitrary $k \in \mathbb{N}$,

$$2^{k+2} + 3^{2k+1} = 7c \text{ for some integer } c \quad \text{(induction hypothesis)}.$$

Then

$$\begin{aligned} 2^{k+3} + 3^{2k+3} &= 2 \times 2^{k+2} + 3^2 \times 3^{2k+1} \\ &= 2 \times 2^{k+2} + 9 \times 3^{2k+1} \\ &= 2(7c - 3^{2k+1}) + 9 \times 3^{2k+1} \text{ (by the induction hypothesis)} \\ &= 14c - 2 \times 3^{2k+1} + 9 \times 3^{2k+1} \\ &= 14c + 7 \times 3^{2k+1} \\ &= 7(2c + 3^{2k+1}) \\ &= 7b \text{ where } b \text{ is an integer.} \end{aligned}$$

Hence $Q(k) \Rightarrow Q(k+1)$ for an arbitrary natural number k. Therefore, for all $n \in \mathbb{N}$, $2^{n+2} + 3^{2n+1}$ is divisible by 7.

□

3. **Theorem**: *If A is a set such that $|A| = n$, then $|\mathcal{P}(n)| = 2^n$ for all $n \in \mathbb{N}$.*

Proof

As before we define the propositional functions $R(n) : |A| = n$ and $S(n) : |\mathcal{P}(n)| = 2^n$. We also define $T(n) : R(n) \rightarrow S(n)$ so that the theorem can be written $\forall n\, T(n)$.

We first establish the truth of $T(0)$, i.e. the truth of $R(0) \rightarrow S(0)$. We therefore add $R(0)$ to our assumptions. This corresponds to assuming the truth of the proposition $|A| = 0$. It follows that $A = \varnothing$, the empty set, in which case $\mathcal{P}(A) = \{\varnothing\}$ and $|\mathcal{P}(A)| = 1 = 2^0$. The last proposition is $S(0)$ and the proof of $R(0) \rightarrow S(0)$ is complete. We can write this more succinctly as follows:

$$\begin{aligned} & |A| = 0 \\ \Rightarrow \quad & A = \varnothing \\ \Rightarrow \quad & \mathcal{P}(A) = \{\varnothing\} \\ \Rightarrow \quad & |\mathcal{P}(A)| = 1 \\ & = 2^0. \end{aligned}$$

We have shown that, if $R(0)$ is true, then so is $S(0)$ and we can therefore conclude that the conditional $T(0) : R(0) \rightarrow S(0)$ is a true proposition. This constitutes the initial step.

We now move to the inductive step. This entails proving that $T(k) \Rightarrow T(k+1)$, i.e. that

$$[R(k) \rightarrow S(k)] \Rightarrow [R(k+1) \rightarrow S(k+1)].$$

The induction hypothesis is $T(k)$, i.e. $R(k) \rightarrow S(k)$. With this as an assumption, our task is to deduce the truth of $R(k+1) \rightarrow S(k+1)$. Since this is a conditional proposition we shall, as usual, employ the method of conditional proof. We add $R(k+1)$ to our list of assumptions (which now includes the induction hypothesis) and show that this implies the truth of $S(k+1)$. The truth of $T(k+1) : R(k+1) \rightarrow S(k+1)$ follows. A further application of conditional proof allows us to deduce the truth of $T(k) \rightarrow T(k+1)$. The structure of this part of the proof is summarised below.

$$\left.\begin{array}{rll} T(k): & R(k) \rightarrow S(k) & \text{(induction hypothesis)} \\ & \left.\begin{array}{l} R(k+1) \\ \vdots \\ S(k+1) \end{array}\right\} \text{CP} & \\ T(k+1): & R(k+1) \rightarrow S(k+1) & \\ T(k) \rightarrow T(k+1): & [R(k) \rightarrow S(k)] \rightarrow [R(k+1) \rightarrow S(k+1)] & \end{array}\right\} \text{CP}$$

Proceeding with the first step, we add to our assumptions the induction hypothesis. This is the conditional $(|A| = k) \rightarrow (|\mathcal{P}(A)| = 2^k)$, i.e. we assume that, if an arbitrary set A has k elements, then its power set $\mathcal{P}(A)$ has 2^k elements. The conditional $R(k+1) \rightarrow S(k+1)$ is equivalent to $(|B| = k+1) \rightarrow (|\mathcal{P}(B)| = 2^{k+1})$, i.e. that an arbitrary set with $k+1$ elements is such that its power set has 2^{k+1} elements. (We use a different symbol for each of the two sets involved since clearly a set with k elements cannot be the same set as one with $k+1$ elements.) We add to our list of assumptions $R(k+1) : |B| = k+1$. We then infer $S(k+1) : |\mathcal{P}(B)| = 2^{k+1}$.

We have $(|A| = k) \rightarrow (|\mathcal{P}(A)| = 2^k)$ (induction hypothesis) and $|B| = k+1$. Now a set B which has $k+1$ elements can be written as the union of two disjoint sets, one with k elements and one with 1 element. Let us call these sets C and D respectively. We then have $B = C \cup D$ where $|C| = k$ and $|D| = 1$. (Of course the sets C and D

are not unique. For example, denoting $B = \{b_1, b_2, \ldots, b_k, b_{k+1}\}$, we could have $C = \{b_1, b_2, \ldots, b_k\}$ and $D = \{b_{k+1}\}$ or $C = \{b_2, \ldots, b_k, b_{k+1}\}$ and $D = \{b_1\}$. In fact, there are $k+1$ different ways of choosing the sets C and D.)

Now what about $\mathcal{P}(B)$, the power set of B—how many elements does it contain? Consider, for example the sets B, C and D where $B = \{b_1, b_2, b_3\}, C = \{b_1, b_2\}$ and $D = \{b_3\}$. Now $\mathcal{P}(C) = \{\varnothing, \{b_1\}, \{b_2\}, \{b_1, b_2\}\}$ and, since $C \subset B$, each subset of C is also a subset of B. In other words, each element of $\mathcal{P}(C)$ is also a member of $\mathcal{P}(B)$ so that $\mathcal{P}(C) \subset \mathcal{P}(B)$. What additional elements are included in $\mathcal{P}(B)$? We have not yet considered those subsets of B which contain the single element of D, namely b_3. These can be obtained by taking each subset of C and adding b_3 as an additional element. Hence $\mathcal{P}(B)$ contains all 4 elements in $\mathcal{P}(C)$ together with the additional 4 elements listed below:

$$\varnothing \cup \{b_3\} = \{b_3\},$$

$$\{b_1\} \cup \{b_3\} = \{b_1, b_3\},$$

$$\{b_2\} \cup \{b_3\} = \{b_2, b_3\}$$

and

$$\{b_1, b_2\} \cup \{b_3\} = \{b_1, b_2, b_3\}.$$

In general, if $\mathcal{P}(C)$ contains n elements, $\mathcal{P}(B)$ contains these n elements together with an additional n elements formed by taking the union of the single element set D with each set in $\mathcal{P}(C)$. The set $\mathcal{P}(B)$ therefore contains $2n$ elements.

We have

$$\begin{aligned} |\mathcal{P}(B)| &= 2 \times |\mathcal{P}(C)| \\ &= 2 \times 2^k \quad \text{(applying the induction hypothesis to the set } C \text{ which has } k \text{ elements)} \\ &= 2^{k+1}. \end{aligned}$$

We have established the truth of $S(k+1)$ and hence (by CP) of $T(k+1)$. This in turn guarantees the truth of $T(k) \rightarrow T(k+1)$ (again using CP) and the truth of $\forall n[T(n) \rightarrow T(n+1)]$ follows as usual by universal generalisation. This completes the inductive step and the principle of mathematical induction allows us to infer that $\forall n[R(n) \rightarrow S(n)]$ is a theorem, i.e. that, if A is a set such that $|A| = n$, then $|\mathcal{P}(A)| = 2^n$ for all $n \in \mathbb{N}$.

□

Once again, this proof contains more explanation than is really necessary. We leave it as an exercise to present an acceptable shortened, less wordy version.

It is useful to return to our firework analogy for a moment and to consider what would happen if we lit, say, the fifth firework (numbered 4) in the line rather than the first. If the fireworks are linked so that each ignites only its successor (not its predecessor), only the fifth and subsequent fireworks would ignite leaving the first four intact. This is analogous to commencing the initial step, not at $n = 0$, but at $n = 4$.

This leads us to a rather more general statement of the principle of mathematical induction. It may be that the propositional function $F(n)$ is false or meaningless for values of n less than some natural number m. In this case we wish to prove that $F(n)$ is true for all integers $n \geq m$. Suppose we alter the initial step and show that the associated propositional function $F(n)$ is true for $n = m$. Having established the inductive step for $n \geq m$, the principle of mathematical induction will allow us to infer that $F(n)$ is a true proposition for all natural numbers greater than or equal to m. In other words, to prove that $\forall n\, F(n)$ is true for the universe of discourse $\{m, m+1, m+2, \ldots\}$, we show that $F(m)$ is true and that within this universe $\forall n[F(n) \rightarrow F(n+1)]$ is also true. We state this formally below.

Principle of mathematical induction

Suppose that $F(n)$ is a propositional function with universe of discourse $\mathbb{N} - \{0, 1, 2, \ldots, m-1\}$ and that the following are true propositions:

(a) $F(m)$,
(b) $\forall n[F(n) \rightarrow F(n+1)]$.

Then $\forall n\, F(n)$ is a true proposition.

This, of course, includes the previous principle where $m = 0$.

Examples 9.2

1. **Theorem**: *For all integers* $n \geq 4$, $n! > 2^n$.

Proof

As we saw in Section 5.1, this theorem may be expressed in two alternative forms. We may state it as the universally quantified conditional propositional function $\forall n[P(n) \rightarrow F(n)]$ where $P(n)$ is 'n is greater than or equal to 4', $F(n)$ is '$n! > 2^n$' and the universe is the integers. Alternatively, we may restrict the universe to integers greater than or equal to 4 and symbolise the theorem simply as $\forall n\, F(n)$. Taking our cue from the statement of the principle of mathematical induction above, we choose the second alternative. The initial step then consists of showing that $F(4)$ is a true proposition.

Now

$$\begin{aligned} 4! &= 4 \times 3 \times 2 \times 1 \\ &= 24 \\ &> 16 \\ &= 2^4. \end{aligned}$$

We have shown that $4! > 2^4$. This establishes the truth of $F(4)$ and completes the initial step.

We now tackle the inductive step. The induction hypothesis is $k! > 2^k$ where k is an arbitrary member of the set of integers greater than or equal to 4. We add this to our list of assumptions and we then proceed with the intention of inferring $(k+1)! > 2^{k+1}$.

$$\begin{aligned} (k+1)! &= (k+1) \times k! \\ &> (k+1) \times 2^k \quad \text{(applying the induction hypothesis)} \\ &> 2 \times 2^k \quad \text{(since } k \geq 4\text{)} \\ &= 2^{k+1}. \end{aligned}$$

We have shown that, for an arbitrary integer $k \geq 4, F(k) \rightarrow F(k+1)$ is a true proposition so that $\forall n[F(n) \rightarrow F(n+1)]$ is true for the universe of integers greater than or equal to 4. This completes the inductive step. Applying the principle of mathematical induction, we conclude that $\forall n\, F(n)$ is a true proposition for this universe or, equivalently, $n! > 2^n$ for all integers n such that $n \geq 4$.

□

2. What is wrong with the following 'proof by mathematical induction'?

Conjecture: *All triangles have the same area.*

'Proof'

Let $S(n)$ denote the proposition 'Any set of n triangles ($n \geq 1$) is such that all n triangles have the same area'. The theorem can then be stated $\forall n\, S(n)$.

We establish the initial step for $n = 1$. Clearly any set containing a single triangle is such that all triangles within the set have the same number of elements. Hence $S(1)$ is a true proposition.

The induction hypothesis is 'Any set of k triangles ($k \geq 1$) is such that all k triangles within the set have the same area'. To establish the inductive step we must show that this implies that any set of $k + 1$ triangles is such that all have the same area.

Consider the arbitrary set of $k + 1$ triangles with elements denoted by $A_1, A_2, \ldots, A_k, A_{k+1}$. Now the set $\{A_1, A_2, \ldots, A_k\}$ contains k triangles and, by the induction hypothesis, these all have the same area. Similarly the set $\{A_2, A_3, \ldots, A_k, A_{k+1}\}$ contains k triangles and so these too must have the same area.

Therefore it follows that all of the triangles $A_1, A_2, \ldots, A_k, A_{k+1}$ have the same area and, by mathematical induction, we deduce that $\forall n\, S(n)$ is true. Hence any set of n triangles is such that all have the same area and so all triangles have the same area.

□

Solution

Since the theorem is clearly preposterous, there must be some flaw in what appears to be its proof. But where is the error? The argument used in the initial step is clearly valid. It is therefore the inductive step which must be scrutinised for some fallacious reasoning.

The inductive step relies implicitly on the two sets of triangles $\{A_1, A_2, \ldots, A_k\}$ and $\{A_2, A_3, \ldots, A_k, A_{k+1}\}$ having elements in common so that the 'same area' property can be transferred from the first set to the second. This is indeed the case so long as $k \geq 2$. The problem lies in the assumption that the truth of $S(1)$ implies the truth of $S(2)$. A set containing the two triangles, A_1 and A_2 say, can be split into two sets each containing one triangle. Within each of these sets all triangles certainly have the same area. However, we cannot deduce from this that the single triangle in the set $\{A_1\}$ has the same area as that in the set

$\{A_2\}$. The proof is therefore not valid because we have not established the inductive step for *every* integer $k \geq 1$.

(A subtle but important point is that, even if it did not contain this flaw, the above would not constitute a proof of the conjecture as stated. What it would prove is the weaker proposition: Any *finite* set of triangles is such that all have the same area. The 'theorem' claims that *all* triangles have the same area and, since there are uncountably many triangles, the set containing them all is not finite.)

Exercises 9.1

1. Prove that $n < 2^n$ for all $n \in \mathbb{N}$.

2. Prove that:

(a) the sum of the squares of the first $n+1$ natural numbers is $\dfrac{n(n+1)(2n+1)}{6}$.

(b) the sum of the cubes of the first $n+1$ natural numbers is $\left[\dfrac{n(n+1)}{2}\right]^2$.

3. Prove that, for all natural numbers n, $4^{2n+1} + 3^{n+2}$ is divisible by 13.

4. Prove that, for all $n \in \mathbb{N}$, if x is a real number and $x \neq 1$,

$$\sum_{i=0}^{n} x^i = \frac{x^{n+1} - 1}{x - 1}$$

5. Prove that:

(i) for all integers $n \geq 4$, $n^3 < 3^n$.
(ii) for all integers $n \geq 5$, $n^2 < 2^n$.

6. (i) Use mathematical induction to show that, for all $n \in \mathbb{Z}^+$, the nth odd positive integer is $2n - 1$.

(ii) Use (ordinary) induction to formulate a conjecture for the sum of the first n odd integers. Attempt to prove that your conjecture is a theorem using mathematical induction.

7. Use mathematical induction to prove that $x + 1$ is a factor of $x^{2n-1} + 1$ for all $n \in \mathbb{Z}^+$.

8. Prove by mathematical induction that $13^n - 5^n$ is divisible by 8 for all $n \in \mathbb{Z}^+$.

9. Prove that, for all positive integers n,

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

10. Prove that, for all positive integers n,

$$\cos\theta + \cos 2\theta + \cdots + \cos n\theta = \frac{\sin(n + \frac{1}{2})\theta}{2\sin\frac{1}{2}\theta} - \frac{1}{2}.$$

11. Prove that if $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ are non-singular $m \times m$ matrices, then

$$(\mathbf{A}_1\mathbf{A}_2 \cdots \mathbf{A}_n)^{-1} = \mathbf{A}_n^{-1}\mathbf{A}_{n-1}^{-1} \cdots \mathbf{A}_1^{-1}$$

for any integer $n \geq 2$.

12. (a) Prove that, if $a_1, \ldots, a_n$ are positive integers and p is a prime number such that $p|(a_1 \cdots a_n)$, then p divides one of the integers $a_i, i = 1, \ldots, n$. (See page 206.)

(b) Prove the theorem of identities (see page 212): If $a_1, a_2, \ldots, a_n$ are members of some universe such that $a_1 = a_2, a_2 = a_3, \ldots, a_{n-1} = a_n$, then $a_1 = a_n$.

13. In Example 5.2.2 we proved that the square of an even integer is even. Suppose that we define the following propositional functions on the universe of positive integers:

$E(n)$: n is even
$T(n)$: $E(n) \rightarrow E(n^2)$.

This theorem can then be written in the form $\forall n[E(n) \rightarrow E(n^2)]$ or $\forall n\, T(n)$. This suggests that mathematical induction may be a suitable method of proof. Attempt to prove the theorem by mathematical induction. What goes wrong?

9.2 The Second Principle of Mathematical Induction

In Section 4.2 we referred to the prime factorisation theorem which states that every integer greater than 1 can be expressed as the product

of prime numbers. If we define the propositional function:

$$P(n) : n \text{ can be expressed as the product of prime numbers}$$

on the universe of positive integers, then proving the theorem amounts to showing that $P(n)$ is true for all integers n such that $n > 1$. This therefore falls into the class of theorems for which mathematical induction may be an appropriate method of proof.

The initial step for the inductive proof is simple enough. Clearly $P(2)$ is a true proposition since 2 is already expressed as the product of prime numbers, albeit in a rather trivial way. The inductive step is a little more problematic. We assume the truth of $P(k)$ (the induction hypothesis) so that

$$k = p_1 p_2 \cdots p_m, \text{ where } p_1, p_2, \ldots, p_m \text{ are prime numbers.}$$

We must now establish the truth of $P(k+1)$, that is, we must show that the integer $k+1$ can be expressed as the product of prime numbers. However, the factorisation of k above does not help us to determine whether $k+1$ can be factorised and, if so, how.

Now clearly the integer $k+1$ must be either prime or composite. If it is prime then $P(k+1)$ is a true proposition. On the other hand, if $k+1$ is composite then it can be expressed as

$$k + 1 = q_1 q_2 \quad \text{where} \quad 2 \leq q_1, q_2 \leq k.$$

Now we have a problem. Whilst our induction hypothesis allows us to assume that k can be expressed as the product of prime numbers, it does not allow us to assume that this is the case for integers less than k, in particular q_1 and q_2. What we need is an induction hypothesis which allows us to assume $P(q_1)$ and $P(q_2)$ as well as $P(k)$. If we had an induction hypothesis which stated that $P(n)$ was true for all $n \leq k$, this would entitle us to express q_1 and q_2 as the product of prime numbers and thereby to complete the inductive step.

In fact we can modify our principle of induction to accommodate proofs wherein the inductive step depends upon an induction hypothesis that $F(n)$ is true, not just for $n = k$, but for each $n \leq k$. Suppose that we are given a theorem of the type described in Section 9.1, i.e. one which can be stated as the universally quantified propositional form $\forall n\, F(n)$ with $\mathbb{N}$ as the universe of discourse. Recall that we previously defined the set S in the axiom of induction to be $\{n \in \mathbb{N} : F(n) \text{ is true}\}$. Suppose

instead that we define $S = \{m \in \mathbb{N} : F(n) \text{ is true for all } n \leq m\}$. This means that S contains all natural numbers m which are such that $F(n)$ is true for $n = 0, 1, \ldots, m$. Now we can re-interpret parts (a) and (b) of the axiom and arrive at what appears to be a slightly different principle of mathematical induction.

Part (a) of the axiom requires the truth of $0 \in S$, which is equivalent to the truth of $F(0)$ exactly as before. Hence the initial step is identical to that described previously. Part (b) of the axiom requires us to establish the truth of the conditional $(k \in S) \rightarrow ((k+1) \in S)$ where k is an arbitrary element of $\mathbb{N}$. The induction hypothesis is $k \in S$ where k is an arbitrary natural number. In our new interpretation this is equivalent to the assumption '$F(n)$ is true for all $n \leq k$' or to '$F(0) \wedge F(1) \wedge \cdots \wedge F(k)$ is a true proposition'. The inductive step involves showing that the truth of $(k+1) \in S$ necessarily follows. The proposition $(k+1) \in S$ is now equivalent to '$F(n)$ is true for all $n \leq k+1$' or '$F(0) \wedge F(1) \wedge \cdots \wedge F(k) \wedge F(k+1)$ is a true proposition'. Clearly, to show the truth of this proposition, all that is necessary is to establish the truth of $F(k+1)$. The truth of $F(n)$ for all values of n less than $k+1$ is incorporated within the induction hypothesis. Having successfully carried out the initial and inductive steps, we may conclude that $\forall n\, F(n)$ is a true proposition as before.

This modified principle of mathematical induction is often referred to as the 'second principle of mathematical induction' (or 'the strong principle of mathematical induction'). We state it formally below.

Second principle of mathematical induction

Suppose that $F(n)$ is a propositional function with universe of discourse $\mathbb{N}$ and that the following are true propositions:

(a) $F(0)$,
(b) $\forall n[(F(0) \wedge F(1) \wedge \cdots \wedge F(n)) \rightarrow F(n+1)]$.

Then $\forall n\, F(n)$ is a true proposition.

It is possible to derive the second principle of induction directly from the original principle rather than from the axiom of induction. We leave this as an exercise (Exercise 9.2.1).

Of course, the second principle of mathematical induction can be modified as before so that it can be used to show that $F(n)$ is true for all $n \geq m$. This again involves restating the principle for a propositional function $F(n)$ defined on the universe of discourse $\{m, m+1, m+2, \ldots\}$.

Second principle of mathematical induction

Suppose that $F(n)$ is a propositional function with universe of discourse $\mathbb{N} - \{0, 1, \ldots, m-1\}$ and that the following are true propositions:

(a) $F(m)$,
(b) $\forall n\,[(F(m) \wedge F(m+1) \wedge \cdots \wedge F(n)) \rightarrow F(n+1)]$.

Then $\forall n\, F(n)$ is a true proposition.

We are now in a position to prove the 'prime factorisation theorem' referred to earlier. We do this in the example below.

Examples 9.3

1. **Theorem**: *Every integer greater than* 1 *can be expressed as the product of prime numbers.*

Proof

We define $P(n)$: n can be expressed as the product of prime numbers. Since we have to prove that $P(n)$ is true for $n \geq 2$, we shall be using the more general of the two statements of the second principle of mathematical induction with $m = 2$.

Initial step: Since 2 is an expression of the product of prime numbers, $P(2)$ is true.

Inductive step: The induction hypothesis is $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$ for an arbitrary $k \in \mathbb{N}$, i.e. each integer from 2 to k can be expressed as a product of prime numbers. As usual, we add this to our assumptions.

Now $k+1$ is either prime or composite. If it is prime then the inductive step is complete. If $k+1$ is composite, then

$$k+1 = q_1 q_2 \quad \text{where} \quad 2 \leq q_1, q_2 \leq k.$$

By the induction hypothesis, q_1 and q_2 can each be expressed as the product of prime numbers so that

$$q_1 = a_1 a_2 \cdots a_r \qquad \text{and} \qquad q_2 = b_1 b_2 \cdots b_s$$

where a_i, $i = 1, 2, \ldots, r$ and b_j, $j = 1, 2, \ldots, s$ are prime numbers.

Hence

$$k+1 = a_1 a_2 \cdots a_r b_1 b_2 \cdots b_s$$

where a_i, $i = 1, 2, \cdots, r$ and b_j, $j = 1, 2, \cdots, s$ are prime numbers.

Since $k+1$ can be expressed as the product of prime numbers, we have established the truth of $[P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$ and therefore of $\forall n[(P(2) \wedge \cdots \wedge P(n)) \rightarrow P(n+1)]$. Applying the second principle of mathematical induction, we conclude that $P(n)$ is true for all $n \geq 2$.

□

2. **Theorem**: *Suppose that a_n, the nth term in an infinite sequence, is defined as follows:*

$$a_1 = 0, \quad a_2 = 1$$

and

$$a_n = 3a_{n-1} - 2a_{n-2} \text{ for } n \geq 3.$$

Then

$$a_n = 2^{n-1} - 1 \text{ for all } n \in \mathbb{Z}^+.$$

(Note that, apart from the first two terms of the sequence, the definition of the general term incorporates the two preceding terms. Any sequence where each term is defined using previous terms in the sequence is said to be **recursively defined**.)

Suppose that we define $F(n) : a_n = 2^{n-1} - 1$. We are required to prove that $F(n)$ is true for all positive integers. However, the definition $a_n = 3a_{n-1} - 2a_{n-2}$ holds only for $n \geq 3$ and it is this equation which we shall need to use in the inductive step. Hence we shall use mathematical induction to prove that $F(n)$ is true for positive integers greater than or equal to 3 so that our starting step will need to establish the truth of $F(3)$. To complete the proof that $F(n)$ is true for all positive integers, we must also establish the truth of $F(1)$ and $F(2)$.

The proof is as follows.

Proof

We have

$$a_n = 3a_{n-1} - 2a_{n-2} \quad \text{for } n \geq 3$$

so that

$$\begin{aligned} a_3 &= 3a_2 - 2a_1 \\ &= 3 \times 1 - 2 \times 0 \\ &= 3 \\ &= 2^{3-1} - 1. \end{aligned}$$

Hence $F(3)$ is true.

Suppose that, for some arbitrary integer $k \geq 3$, $F(3), F(4), \ldots, F(k)$ are all true propositions, i.e. $a_n = 2^{n-1} - 1$ for $n = 3, 4, \ldots, k$. (This is the induction hypothesis.)

Then

$$\begin{aligned} a_{k+1} &= 3a_k - 2a_{k-1} \\ &= 3(2^{k-1} - 1) - 2(2^{k-2} - 1) \quad \text{(by the induction hypothesis)} \\ &= 3 \times 2^{k-1} - 3 - 2^{k-1} + 2 \\ &= 2 \times 2^{k-1} - 1 \\ &= 2^k - 1. \end{aligned}$$

Hence, for an arbitrary integer $k \geq 3$, $F(3) \wedge F(4) \wedge \cdots \wedge F(k) \Rightarrow F(k+1)$ and, by the second principle of mathematical induction, we conclude that $a_n = 2^{n-1} - 1$ is true for all $n \geq 3$.

Also

$$\begin{aligned} a_1 &= 0 \\ &= 2^{1-1} - 1 \end{aligned}$$

$\Rightarrow$ $F(1)$ is true

and

$$\begin{aligned} a_2 &= 1 \\ &= 2^{2-1} - 1 \end{aligned}$$

$\Rightarrow$ $F(2)$ is true.

Hence $F(n)$ is true for all $n \geq 1$ and the result is proved.

□

Note that an induction hypothesis which assumed only $a_k = 2^{k-1} - 1$ would not have been sufficient. To complete the inductive step, we also needed $a_{k-1} = 2^{k-2} - 1$ and hence the second principle of induction.

There is a modification of the second principle of induction by which $F(1)$ and $F(2)$ are incorporated into the main proof and which does not therefore require $F(3)$ to be verified directly—see Exercise 9.2.2.

Exercises 9.2

1. Show that the second principle of induction can be derived directly from the original principle of induction as follows. Given a theorem of the form $\forall n\, F(n)$ (where $F(n)$ is defined on the universe of natural numbers), define $G(n) : F(0) \wedge F(1) \wedge \cdots \wedge F(n)$. Show that the conditions (a) and (b) of the principle applied to $G(n)$ are equivalent to those of the second principle applied to $F(n)$.

2. For inductive proofs involving recursively defined sequences, it is often convenient to include the checking of the truth of the proposition for the first few explicitly defined terms as part of the initial step rather than separating them from the inductive proof itself. There is a modification of the second principle which allows us to achieve this.

(i) Establish the following principle of induction.

Let $F(n)$ be a propositional function with universe of discourse $\mathbb{N} - \{0, \ldots, m\}$ and let r be a fixed element of the universe (i.e. $r \geq m$). Suppose the following are true propositions:

(a) $F(m) \wedge \cdots \wedge F(r)$,
(b) $\forall n[((n \geq r) \wedge F(m) \wedge \cdots \wedge F(n)) \rightarrow F(n+1)]$

Then $\forall n\, F(n)$ is a true proposition.

Condition (b) is often written less formally as

$$(\forall n \geq r)[(F(m) \wedge \cdots \wedge F(n)) \rightarrow F(n+1)].$$

(ii) Re-write the proof given in Example 9.3.2 using this principle. The initial step must establish the truth of $F(1) \wedge F(2)$. The inductive step then consists of showing that $(F(1) \wedge F(2) \wedge \cdots \wedge F(k)) \Rightarrow F(k+1)$.

For each of the following, prove the theorem given using either the first or second principle of induction as appropriate.

3. In any n-sided polygon ($n \geq 3$), the sum of the interior angles is $(n-2)\pi$.

4. The following is an infinite sequence known as 'the sequence of Fibonacci numbers':

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

Each term in the sequence after the first two is defined recursively as the sum of the two preceding terms. Therefore, denoting the nth term in the sequence by f_n, we can define f_n for $n \in \mathbb{Z}^+$ as follows:

$$f_1 = 1, \quad f_2 = 1$$
$$\text{and} \quad f_n = f_{n-1} + f_{n-2} \quad \text{for } n \geq 3.$$

Prove each of the following:

(i) $f_n < 2^n$ for all $n \in \mathbb{Z}^+$;

(ii) $f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$ for all $n \in \mathbb{Z}^+$

5. Suppose that a_n, the nth term in an infinite sequence, is defined recursively as follows:

$$a_1 = 3,$$
$$\text{and} \quad a_n = a_{n-1} + 3 \quad \text{for } n \geq 2.$$

Prove that $a_n = 3n$.

6. Suppose that a_n, the nth term in an infinite sequence, is defined recursively as follows:

$$a_1 = 6, \quad a_2 = 11$$
$$\text{and} \quad a_n = 3a_{n-1} - 2a_{n-2} \quad \text{for } n \geq 3.$$

Prove that, for $n \geq 1, a_n = 5 \times 2^{n-1} + 1$.

7. Suppose that a_n, the nth term in an infinite sequence, is defined recursively as follows:

$$a_1 = 1, a_2 = 2, a_3 = 3$$

and $\quad a_n = a_{n-1} + a_{n-2} + a_{n-3} \quad$ for all $n \geq 4$.

Prove that $a_n < 2^n$ for all $n \in \mathbb{Z}^+$.

8. Prove that, for all finite sets A and B, if $B \subset A$, then $|B| < |A|$. *Hint*: use induction on $|A|$.

9. Prove the **binomial theorem**: for all $x, y \in \mathbb{R}, n \in \mathbb{Z}^+$

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1}y + \binom{n}{2} x^{n-2}y^2 + \cdots + y^n$$

$$= \sum_{i=0}^{n} \binom{n}{i} x^{n-i}y^i.$$

Hint: the identity $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ might be useful—see Example 8.2.1.

10. Suppose that $P(n)$ is defined over the universe $\mathbb{N}$ and that the following are true propositions:

(a) $P(1)$;
(b) $\forall n[P(n) \rightarrow P(2n)]$;
(c) $\forall n[P(n+1) \rightarrow P(n)]$.

Prove that $\forall n\, P(n)$ is a true proposition.

Appendix: Some Definitions and Terminology

Logic

Replacement Rules	
Commutation (Com)	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$
Association (Assoc)	$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
Distribution (Dist)	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
De Morgan's laws (De M)	$\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$ $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$
Double negation (DN)	$p \equiv \overline{\overline{p}}$
Transposition (Trans)	$p \rightarrow q \equiv \overline{q} \rightarrow \overline{p}$
Material implication (Impl)	$p \rightarrow q \equiv \overline{p} \vee q$
Material equivalence (Equiv)	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$ $p \leftrightarrow q \equiv (p \wedge q) \vee (\overline{p} \wedge \overline{q})$
Tautology (Taut)	$p \wedge p \equiv p$ $p \vee p \equiv p$
Exportation (Exp)	$(p \wedge q) \rightarrow r \equiv p \rightarrow (q \rightarrow r)$

Rules of inference for constructing formal proofs

Name of rule	Premises	Conclusion
Simplification (Simp)	$p \wedge q$	p
Addition (Add)	p	$p \vee q$
Conjunction (Conj)	p, q	$p \wedge q$
Disjunctive syllogism (DS)	$p \vee q, \overline{p}$	q
Modus ponens (MP)	$p \rightarrow q, p$	q
Modus tollens (MT)	$p \rightarrow q, \overline{q}$	$\overline{p}$
Hypothetical syllogism (HS)	$p \rightarrow q, q \rightarrow r$	$p \rightarrow r$
Absorption (Abs)	$p \rightarrow q$	$p \rightarrow (p \wedge q)$
Constructive dilemma (CD)	$(p \rightarrow q) \wedge (r \rightarrow s), p \vee r$	$q \vee s$

Rules for quantification denial (QD)

Suppose that a universe of discourse is defined for the variable x. Then, for any propositional function Fx:

$\neg \forall x\, Fx$ is equivalent to $\exists x \neg Fx$,

and $\neg \exists x\, Fx$ is equivalent to $\forall x \neg Fx$.

Rules of instantiation and generalisation

Universal instantiation (UI)	Given any propositional function Fx, from the truth of $\forall x\, Fx$, we can infer the truth of Fa for any individual a in the universe of discourse.
Existential instantiation (EI)	Given any propositional function Fx, from the truth of $\exists x\, Fx$, we can infer that there is at least one individual a in the universe of discourse for which Fa is true.
Universal generalisation (UG)	If the proposition Fa is true for an arbitrary member a of the universe of discourse, then $\forall x\, Fx$ is true.
Existential generalisation (EG)	If the proposition Fa is true for some particular individual a in the universe of discourse, then $\exists x\, Fx$ is true.

Set Theory

A **set** is to be thought of as any collection of objects whatsoever[1]. If an object x belongs to a set A we say 'x is an **element** of A' and write this as $x \in A$. If x does not belong to A, we write $x \notin A$. The **empty set**, $\varnothing$, is the set which contains no elements at all.

A set A is a **subset** of a set B, written $A \subseteq B$, if and only if every element of A is also an element of B. Symbolically, $A \subseteq B$ if and only if $x \in A \Rightarrow x \in B$. A set A is a **proper subset** of a set B, written $A \subset B$, if and only if $A \subseteq B$ and $A \neq B$.

One way to avoid the problems alluded to in the footnote is to insist that all sets are subsets of some **universal set** $\mathcal{U}$. This set $\mathcal{U}$ plays a similar role to the universe of discourse in predicate logic. In particular, the universal set is not fixed for all time so that different universal sets may be defined for different tasks.

Given a set A, we define:

- its **complement**, $\overline{A}$, to be the set of all elements (in the universal set $\mathcal{U}$) which do not belong to A, $\overline{A} = \{x: x \notin A\}$.
- its **power set**, $\mathcal{P}(A)$, to be the set containing all the subsets of A, $\mathcal{P}(A) = \{B: B \subseteq A\}$. Thus $B \in \mathcal{P}(A) \Leftrightarrow B \subseteq A$.

The **intersection** of two sets A, B is the set containing all the elements which belong both to A and to B; the intersection is denoted $A \cap B$. Symbolically, $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$. The **union** of two sets A, B is the set containing all the elements which belong to A or to B or to both; the union is denoted $A \cup B$. Symbolically, $x \in A \cup B \Leftrightarrow (x \in A) \vee (x \in B)$. The definitions of intersection and union generalise to more than two sets:

$$A_1 \cap A_2 \cap \cdots \cap A_n = \{x : x \in A_i \text{ for each } i = 1, 2, \ldots, n\},$$

$$A_1 \cup A_2 \cup \cdots \cup A_n = \{x : x \in A_i \text{ for some } i = 1, 2, \ldots, n\}.$$

Two sets A and B are said to be **disjoint** if they have no elements in common, i.e. if $A \cap B = \varnothing$.

[1] In fact, there are difficulties which arise from such a general definition of a set, such as Russell's paradox—see Garnier and Taylor (1992), for example. To avoid the difficulties, we would need to take an axiomatic approach to set theory, which is beyond the scope of this text.

The **difference** between two sets A and B is the set containing all the elements which belong to A but not to B; the difference is denoted $A - B$. Symbolically, $x \in A - B \Leftrightarrow (x \in A) \wedge (x \notin B)$. Note that the complement of A may be defined as the difference $\overline{A} = \mathcal{U} - A$.

The **cardinality** of a finite set A, denoted $|A|$, is the number of (distinct) elements belonging to A.

An **ordered pair** (a, b) where $a \in A$ and $b \in B$ satisfies the property: $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. The **Cartesian product** of two sets A and B is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$; the Cartesian product is denoted $A \times B$. Symbolically,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.$$

These definitions generalise to the case of more than two sets as follows. An **ordered *n*-tuple** $(a_1, a_2, \ldots, a_n)$ such that $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$ satisfies the property: $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ if and only if $a_1 = b_1$ and $a_2 = b_2, \ldots,$ and $a_n = b_n$. The **Cartesian product** of n sets $A_1, A_2, \ldots, A_n$ is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ such that $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$; the Cartesian product is denoted $A_1 \times A_2 \times \cdots \times A_n$. Symbolically,

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

The Algebra of Sets

The following identities are satisfied for all sets A, B and C which are subsets of some universal set $\mathcal{U}$.

Idempotent laws	$A \cap A = A$	$A \cup A = A$
Commutative laws	$A \cap B = B \cap A$	$A \cup B = B \cup A$
Associative laws	$A \cap (B \cap C) = (A \cap B) \cap C$	
	$A \cup (B \cup C) = (A \cup B) \cup C$	
Absorption laws	$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$
Distributive laws	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
Involution law	$\overline{\overline{A}} = A$	
De Morgan's laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Identity laws	$A \cup \varnothing = A$	$A \cap \varnothing = \varnothing$
	$A \cup \mathcal{U} = \mathcal{U}$	$A \cap \mathcal{U} = A$

Complement laws $A \cup \overline{A} = \mathcal{U}$ $A \cap \overline{A} = \varnothing$
$\overline{\varnothing} = \mathcal{U}$ $\overline{\mathcal{U}} = \varnothing$

Some Commonly Used Sets

The set of **natural numbers** is $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

The set of **integers** is $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$= \{0, 1, -1, 2, -2, 3, -3, \ldots\}$.

The set of **rational numbers** is the set of numbers which can be expressed as fractions, $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z} \text{ and } q \neq 0\}$.

The set $\mathbb{R}$ of **real numbers** is harder to define precisely, but we may think of a real number as a number which can be expressed as a decimal which may be infinite. Examples of real numbers (which do not belong to the sets above) are $\pi = 3.141\,592\,65\ldots$, $\sqrt{2} = 1.414\,213\,56\ldots$, and $\log_{10} 3 = 0.477\,121\,25\ldots$.

These sets are related as follows: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

The set of positive integers is $\mathbb{Z}^+ = \{n \in \mathbb{Z} : n > 0\} = \{1, 2, 3, 4, \ldots\}$. Similarly, the sets of positive rational numbers and positive real numbers are, respectively, $\mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$ and $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$.

Matrices

An $n \times m$ **matrix A** is a rectangular array of numbers or symbols which has n rows and m columns. The entry in row i and column j is called the **(i,j)-entry** and is denoted a_{ij}.

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{pmatrix}.$$

Let **A** be an $n \times m$ matrix and **B** be a $p \times q$ matrix.

The sum $\mathbf{A} + \mathbf{B}$ is defined if and only if $n = p$ and $m = q$. If this is the case then $\mathbf{A} + \mathbf{B}$ is an $n \times m$ $(= p \times q)$ matrix whose (i,j)-entry is $a_{ij} + b_{ij}$:

$$\begin{matrix}\mathbf{A}\end{matrix}\qquad\qquad\begin{matrix}\mathbf{B}\end{matrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nm} \end{pmatrix}$$

$$\begin{matrix}\mathbf{A}+\mathbf{B}\end{matrix}$$

$$= \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1m}+b_{1m} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2m}+b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \dots & a_{nm}+b_{nm} \end{pmatrix}.$$

The product **AB** is defined if and only if $m = p$. If this is the case then **AB** is an $n \times q$ matrix whose (i,j)-entry is $\sum_{k=1}^{m} a_{ik}b_{kj}$:

$$\begin{matrix}\mathbf{A}\end{matrix}\qquad\qquad\begin{matrix}\mathbf{B}\end{matrix}\qquad\qquad\begin{matrix}\mathbf{AB}\end{matrix}$$

$$\begin{pmatrix} \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{im} \\ \vdots & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} \dots & b_{1j} & \dots \\ \dots & b_{2j} & \dots \\ & \vdots & \\ \dots & b_{mj} & \dots \end{pmatrix} = \begin{pmatrix} & \vdots & \\ \dots & c_{ij} & \dots \\ & \vdots & \end{pmatrix}$$

where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{im}b_{mj} = \sum_{k=1}^{m} a_{ik}b_{kj}.$$

The $m \times n$ **zero matrix** $\mathbf{0}_{m\times n}$ has (i,j)-entry equal to 0 for all $1 \le i \le m$ and $1 \le j \le n$. The $m \times n$ zero matrix $\mathbf{0}_{m\times n}$ satisfies the property that $\mathbf{A} + \mathbf{0}_{m\times n} = \mathbf{A} = \mathbf{0}_{m\times n} + \mathbf{A}$ for all $m \times n$ matrices **A**.

The $n \times n$ **identity matrix** $\mathbf{I}_n$ has (i,i)-entry equal to 1 for all i and (i,j)-entry equal to 0 for all $i \neq j$:

$$\mathbf{I}_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

The $n \times n$ identity matrix $\mathbf{I}_n$ satisfies the property that $\mathbf{AI}_n = \mathbf{A} = \mathbf{I}_n\mathbf{A}$ for all $n \times n$ matrices **A**.

The **inverse** of an $n \times n$ matrix $\mathbf{A}$ is an $n \times n$ matrix $\mathbf{A}^{-1}$ such that $\mathbf{A}\mathbf{A}^{-1} = \mathbf{I}_n = \mathbf{A}^{-1}\mathbf{A}$. Not all $n \times n$ matrices have inverses. If $\mathbf{A}$ has an inverse it is said to be **non-singular** or **invertible.**

The **transpose** of an $n \times m$ matrix $\mathbf{A}$ is the $m \times n$ matrix $\mathbf{A}^{\mathrm{T}}$ obtained by interchanging the rows and columns of $\mathbf{A}$:

$$\text{if } \mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} \text{ then } \mathbf{A}^{\mathrm{T}} = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1m} & a_{2m} & \dots & a_{nm} \end{pmatrix}.$$

For example, if $\mathbf{A} = \begin{pmatrix} -1 & 2 \\ 3 & -6 \\ 10 & \frac{1}{2} \end{pmatrix}$ then $\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} -1 & 3 & 10 \\ 2 & -6 & \frac{1}{2} \end{pmatrix}$.

The transpose satisfies the following properties:

1. For all matrices, $\mathbf{A}$, $(\mathbf{A}^{\mathrm{T}})^{\mathrm{T}} = \mathbf{A}$.
2. For all matrices such that $\mathbf{A} + \mathbf{B}$ is defined, $(\mathbf{A} + \mathbf{B})^{\mathrm{T}} = \mathbf{A}^{\mathrm{T}} + \mathbf{B}^{\mathrm{T}}$.
3. For all matrices such that $\mathbf{AB}$ is defined, $(\mathbf{AB})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}$.

The **determinant**, $\det \mathbf{A}$, of a 2×2 matrix is defined by $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.

An $n \times n$ matrix $\mathbf{A}$ is **symmetric** if $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$. Intuitively, to say $\mathbf{A}^{\mathrm{T}} = \mathbf{A}$ for a square matrix means that $\mathbf{A}$ is symmetric about its 'leading diagonal' which runs from top-left to bottom-right.

For example, if $\mathbf{A} = \begin{pmatrix} 5 & 14 & -2 \\ 14 & -1 & \frac{2}{3} \\ -2 & \frac{2}{3} & 9 \end{pmatrix}$ then $\mathbf{A}^{\mathrm{T}} = \begin{pmatrix} 5 & 14 & -2 \\ 14 & -1 & \frac{2}{3} \\ -2 & \frac{2}{3} & 9 \end{pmatrix} = \mathbf{A}$.

Group Theory

A **group** is a set G together with a binary operation which we will write multiplicatively, so that $ab \in G$ for all $a, b \in G$, satisfying the following three axioms:

G1. For all $a, b, c \in G$, $a(bc) = (ab)c$.

G2. There exists an element $e \in G$, called an **identity**, such that, for all $a \in G$, $ea = a = ae$.

G3. For each $a \in G$ there exists an element $a^{-1} \in G$, called an **inverse** of a, such that $aa^{-1} = e = a^{-1}a$.

Furthermore, the group is said to be **abelian**[2] if, in addition, for all $a, b \in G$, $ab = ba$.

The **order** of a group G is $|G|$, the cardinality of G as a set.

The **order** of an element x of a group G, denoted $|x|$, is the smallest positive integer n such that $x^n = e$ (where $x^n = \underbrace{xx \cdots x}_{\leftarrow n \text{ times} \rightarrow}$). If no such positive integer exists, then x has **infinite order.**

A group G is **cyclic** if there exists an element $x \in G$ such that every $g \in G$ can be expressed as $g = x^n$ for some $n \in \mathbb{Z}$.

A subset H of a group G is a **subgroup** of G if H is itself a group under the same binary operation as that defined in G. Further, H is a **proper subgroup** of G if it is a subgroup different from $\{e\}$ and G itself.

[2] Named after the Norwegian mathematician Niels Henrik Abel (1802-29) who contributed to the theory of equations and infinite series. Abel showed that there is no formula giving the roots of a general quintic (fifth power) equation. A year after his early death from tuberculosis he was awarded the Grand Prize in mathematics by the Royal Academy of France.

References and Further Reading

Andrews G E (1994) The death of proof? Semi-rigorous mathematics? You've got to be kidding, *The Mathematical Intelligencer*, **16**, 16-18.

Aschbacher M (1981) The classification of finite simple groups, *The Mathematical Intelligencer*, **3**, 59-65.

Benacerraf P and Putnam H (eds) (1983) *Philosophy of Mathematics, Selected Readings* (2nd edn), Cambridge University Press, Cambridge.

Davis P J and Hersh R (1981) Proof, In: Davis P J and Hersh R (1981) *The Mathematical Experience*, Birkhäuser, Boston, pp. 147-151.

Franklin J and Daoud A (1988) *Introduction to Proofs in Mathematics*, Prentice Hall, Englewood Cliffs, N.J.

Friske M (1985) Teaching proof: a lesson from software engineering, *American Mathematical Monthly*, **92**, 142-144.

Garnier R and Taylor J (1992) *Discrete Mathematics for New Technology*, Adam Hilger, Bristol.

Goodstein R L (1965) The axiomatic method, in: Goodstein R L (1965) *Essays in the Philosophy of Mathematics*, Leicester University Press, Leicester, pp. 116-125.

Horgan J (1993) The death of proof, *Scientific American*, **269**, 74-82.

Leron U (1983) Structuring mathematical proofs, *American Mathematical Monthly*, **90**, 174-185.

Polya G (1957) *How to Solve It. A New Aspect of Mathematical Method* (2nd edn), Doubleday, New York.

Solow D (1990) *How To Read and Do Proofs: An Introduction to Mathematical Thought Processes* (2nd edn), Wiley, New York.

Tieszen R (1992) What is a proof? in: Detlefsen M (1992) *Proof, Logic and Formalisation*, Routledge, London & New York.

Velleman D J (1994) *How to Prove it, a Structured Approach*, Cambridge University Press, Cambridge.

Wells D (1986) *The Penguin Dictionary of Curious and Interesting Numbers*, Penguin, Harmondsworth.

Wheeler R F (1981) *Rethinking Mathematical Concepts*, Ellis Horwood, Chichester.

Zeilberger D (1993) Theorems for a price: tomorrow's semi-rigorous mathematical culture, *Notices of the American Mathematical Society*, **48**, 978-981.

Hints and Solutions to Selected Exercises

Exercises 2.1

1. (i) If the wind blows then the sun doesn't shine or the rain falls (or both).

(ii) The wind blows and the rain falls if and only if the sun doesn't shine.

(v) If the rain doesn't fall or the temperature rises (but not both) then the sun shines and the wind doesn't blow.

2. (i) $T \leftrightarrow (S \wedge \overline{R})$.
(iii) $(S \wedge T) \vee (W \wedge R)$.
(v) $[\overline{S} \vee (W \wedge R)] \rightarrow \overline{T}$.

3. (i) False. (ii) False. (iv) True.

4. (i) False. (iii) True. (iv) True.

5. (iii)

p	q	r	$p \rightarrow r$	$r \rightarrow q$	$(p \rightarrow r) \wedge (r \rightarrow q)$
T	T	T	T	T	T
T	T	F	F	T	F
T	F	T	T	F	F
T	F	F	F	T	F
F	T	T	T	T	T
F	T	F	T	T	T
F	F	T	T	F	F
F	F	F	T	T	T

(iv)

p	q	r	$r \wedge p$	$\overline{q}$	$\overline{p}$	$(\overline{q} \wedge \overline{p})$	$(r \wedge p) \vee (\overline{q} \wedge \overline{p})$
T	T	T	T	F	F	F	T
T	T	F	F	F	F	F	F
T	F	T	T	T	F	F	T
T	F	F	F	T	F	F	F
F	T	T	F	F	T	F	F
F	T	F	F	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

Exercises 2.2

1. Contradiction.
3. Tautology.
5. Contradiction.
9. Neither.
12. Neither.

Exercises 2.3

1. (i) $p_1 \vdash p_2, p_2 \vdash p_1, p_1 \equiv p_2$.
   (ii) None.
   (iii) $p_2 \vdash p_1$.
   (vi) $p_1 \vdash p_2, p_2 \vdash p_1, p_1 \equiv p_2$.
   (viii) $p_1 \vdash p_2, p_2 \vdash p_1, p_1 \equiv p_2$.

2. (ii) True. (iii) Nothing.
   (v) True.

3. (i) Yes. (iii) No.
   (vii) Yes. (ix) Yes.

4.

p	q	$p \to q$	$q \to p$	$\overline{p}$	$\overline{q}$	$\overline{p} \to \overline{q}$	$\overline{q} \to \overline{p}$
T	T	T	T	F	F	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

From the truth table, we have: $(p \to q) \equiv (\overline{q} \to \overline{p}), (\overline{p} \to \overline{q}) \equiv q \to p$ and no other logical equivalences.

6.

p	q	r	$p \to q$	$p \wedge q$	$(p \wedge q) \to r$	$(p \to q) \wedge [(p \wedge q) \to r]$	$p \to r$
T	T	T	T	T	T	T	T
T	T	F	T	T	F	F	F
T	F	T	F	F	T	F	T
T	F	F	F	F	T	F	F
F	T	T	T	F	T	T	T
F	T	F	T	F	T	T	T
F	F	T	T	F	T	T	T
F	F	F	T	F	T	T	T

Whenever $(p \wedge q) \wedge [(p \wedge q) \to r]$ is true (rows 1 and 5-8), $p \to r$ is true. Therefore $(p \wedge q) \wedge [(p \wedge q) \to r]$ logically implies $p \to r$.

7. (i) Yes.
(iv) No.

8. (b)

(i) $\overline{p} \vee (p \wedge q) \equiv (\overline{p} \vee p) \wedge (\overline{p} \vee q)$ (Dist)
$\equiv (p \vee \overline{p}) \wedge (\overline{p} \vee q)$ (Com)
$\equiv t \wedge (\overline{p} \vee q)$ (Complement law)
$\equiv (\overline{p} \vee q) \wedge t$ (Com)
$\equiv \overline{p} \vee q$ (Identity law)

(iii) $(\overline{\overline{p} \wedge q}) \wedge (p \vee \overline{q}) \equiv (\overline{\overline{p}} \vee \overline{q}) \wedge (p \vee \overline{q})$ (De M)
$\equiv (p \vee \overline{q}) \wedge (p \vee \overline{q})$ (DN)
$\equiv p \vee \overline{q}$ (Taut)

(v) $p \wedge [(p \wedge q) \vee \overline{p}] \equiv [p \wedge (p \wedge q)] \vee (p \wedge \overline{p})$ (Dist)
$\equiv [p \wedge (p \wedge q)] \vee f$ (Complement law)
$\equiv p \wedge (p \wedge q)$ (Identity law)
$\equiv (p \wedge p) \wedge q$ (Assoc)
$\equiv p \wedge q$ (Taut)

Exercises 2.4

1. Argument form: premises: $p \to q, \overline{q}$; conclusion $\overline{p}$.

p	q	$p \to q$	$\overline{q}$	$(p \to q) \wedge \overline{q}$	$\overline{p}$
T	T	T	F	F	F
T	F	F	T	F	F
F	T	T	F	F	T
F	F	T	T	T	T

Whenever the conjunction of the premises is true (row 4 only), the conclusion is true also. Hence the argument is valid.

4. Argument form: premises: $p \leftrightarrow \overline{q}, \overline{p} \to \overline{r}$; conclusion: $r \veebar q$

p	q	r	$\overline{p}$	$\overline{q}$	$\overline{r}$	$p \leftrightarrow \overline{q}$	$\overline{p} \to \overline{r}$	$(p \leftrightarrow \overline{q}) \wedge (\overline{p} \to \overline{r})$	$r \veebar q$
T	T	T	F	F	F	F	T	F	F
T	T	F	F	F	T	F	T	F	T
T	F	T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T	T	F
F	T	T	T	F	F	T	F	F	F
F	T	F	T	F	T	T	T	T	T
F	F	T	T	T	F	F	F	F	T
F	F	F	T	T	T	F	T	F	F

In row 4, the conjunction of the premises is true but the conclusion is false. Hence the argument is invalid.

5. Argument form: premises: $p \leftrightarrow q$, $\overline{q} \wedge r$, $r \to p$;
conclusion: $\overline{s}$.

The truth table shows the conjunction of the premises to be a contradiction so that the premises are inconsistent. Hence the argument is valid.

7. Argument form: premises: $p \veebar q$, $p \to \overline{r}$;
conclusion: $r \to q$.

The argument is valid.

9. Argument form: premises $p \vee q$, $\overline{p} \to r$;
conclusion: $q \to \overline{r}$.

The argument is invalid.

Exercises 2.5

1. We define: G: I shall play golf.
H: I shall stay at home.
R: I shall read.

1.	$G \vee (H \wedge R)$	(premise)
2.	$(G \vee H) \wedge (G \vee R)$	(1. Dist)
3.	$G \vee H$	(2. Simp)

5. We define: H: People are happy.
C: People are charitable.

1.	$H \leftrightarrow C$	(premise)
2.	$\overline{H \wedge C}$	(premise)
3.	$(H \wedge C) \vee (\overline{H} \wedge \overline{C})$	(2. Equiv)
4.	$(\overline{H} \wedge \overline{C})$	(2, 3. DS)

7. We define: W: You will win the game.
R: You follow the rules.
C: You are conventional.
S: You are always successful.

1.	$W \leftrightarrow R$	(premise)
2.	$R \rightarrow C$	(premise)
3.	$\overline{C} \wedge S$	(premise)
4.	$S \rightarrow W$	(premise)
5.	$S \wedge \overline{C}$	(3. Com)
6.	S	(5. Simp)
7.	W	(4, 6. MP)

(It is worth noting that this argument has inconsistent premises so that *any* conclusion could be substituted for W, for example $\overline{W}$, and the resulting argument would also be valid.)

10. Define: V: Peter is brave.
N: Peter is brainy.
L: Peter is bald.

1.	$(V \vee N) \wedge (N \vee L)$	(premise)
2.	$\overline{N}$	(premise)
3.	$V \vee N$	(1. Simp)

4.	$N \vee V$	(3. Com)
5.	V	(2, 4. DS)
6.	$(N \vee L) \wedge (V \vee N)$	(1. Com)
7.	$N \vee L$	(6. Simp)
8.	L	(2, 7. DS)
9.	$V \wedge L$	(5, 8. Conj)

14. Define: G: Ghosts are a reality.
S: There are spirits roaming the earth.
D: We fear the dark.
I: We have an imagination.

1.	$(G \rightarrow S) \wedge (\overline{G} \rightarrow \overline{D})$	(premise)
2.	$D \vee \overline{I}$	(premise)
3.	$I \wedge \overline{G}$	(premise)
4.	I	(3. Simp)
5.	$\overline{I} \vee D$	(2. Com)
6.	$\overline{\overline{I}}$	(4. DN)
7.	D	(5, 6. DS)
8.	$(\overline{G} \rightarrow \overline{D}) \wedge (G \rightarrow S)$	(1. Com)
9.	$\overline{G} \rightarrow \overline{D}$	(8. Simp)
10.	$\overline{G} \wedge I$	(3. Com)
11.	$\overline{G}$	(10. Simp)
12.	$\overline{D}$	(9, 11. MP)
13.	$D \vee S$	(7. Add)
14.	S	(12, 13. DS)

Exercises 2.6

1. We define: C: You confront him.
Y: You're a coward.
F: You're a fool.

(a)	1.	$\overline{C} \rightarrow Y$	(premise)
	2.	$\overline{C}$	(CP)
	3.	Y	(1, 2. MP)
	4.	$Y \vee F$	(3. Add)
	5.	$\overline{C} \rightarrow (Y \vee F)$	(2-4. CP)

(b)

1.	$\overline{C} \rightarrow Y$	(premise)
2.	$\overline{\overline{C}} \vee Y$	(1. Impl)
3.	$(\overline{\overline{C}} \vee Y) \vee F$	(2. Add)
4.	$\overline{\overline{C}} \vee (Y \vee F)$	(3. Assoc)
5.	$\overline{C} \rightarrow (Y \vee F)$	(4. Impl)

5. (a) We define: M: You mow the lawn.
C: You clean the car.
P: You'll get pocket money.
S: You'll stay at home this evening.

1.	$(M \wedge C) \vee \overline{P}$	(premise)
2.	$\overline{P} \rightarrow S$	(premise)
3.	$\overline{C}$	(CP)
4.	$\overline{C} \vee \overline{M}$	(3. Add)
5.	$\overline{M} \vee \overline{C}$	(4. Com)
6.	$\overline{(M \wedge C)}$	(5. De M)
7.	$\overline{P}$	(1, 6. DS)
8.	S	(2, 7. MP)
9.	$\overline{C} \rightarrow S$	(3–8. CP)
10.	$\overline{\overline{C}} \vee S$	(9. Impl)
11.	$C \vee S$	(10. DN)

(b)

1.	$(M \wedge C) \vee \overline{P}$	(premise)
2.	$\overline{P} \rightarrow S$	(premise)
3.	$\overline{\overline{(M \wedge C)}} \vee \overline{P}$	(1. DN)
4.	$\overline{(M \wedge C)} \rightarrow \overline{P}$	(3. Impl)
5.	$\overline{(M \wedge C)} \rightarrow S$	(2, 4. HS)
6.	$\overline{\overline{(M \wedge C)}} \vee S$	(5. Impl)
7.	$(M \wedge C) \vee S$	(6. DN)
8.	$S \vee (M \wedge C)$	(7. Com)
9.	$S \vee (C \wedge M)$	(8. Com)
10.	$(S \vee C) \wedge (S \vee M)$	(9. Dist)
11.	$S \vee C$	(10. Simp)
12.	$C \vee S$	(11. Com)

Exercises 3.1

2. (There are acceptable alternatives to each of the following.)

(i) $Pp \wedge Df$
(iii) $(Pp \vee Dp) \wedge \neg Cf$
(v) $\forall x\,[Px \rightarrow (Dx \vee Cx)]$
(vii) $\exists x\,(Px \wedge Dx \wedge \neg Cx)$

3. (i) Everyone who is dishonest is not to be trusted.
(iii) Everyone who values success is honest and can be trusted.
(v) If there are people who are dishonest and value success, then no-one can be trusted.
(vii) Not everyone who values success is to be trusted and some people who value success are honest.

4. (i)	(a)	F	(b)	F	(c)	F	(d) F
(iii)	(a)	T	(b)	T	(c)	T	(d) T
(vi)	(a)	F	(b)	F	(c)	T	(d) F

Exercises 3.2

1. (Once again, there are acceptable alternatives to each of the following. For instance, other variables may be used within each expression.)

(i) $\forall y\,(Tcy \rightarrow Pcy)$
(iii) $\exists x\,(Txs \wedge \neg Pxs)$
(v) $\exists x\,\forall y\,(Txy \rightarrow Pxy)$
(vii) $\forall x \exists y\,(Txy \wedge \neg Exy) \rightarrow \forall x \forall y\,(\neg Pxy)$

With no universes of discourse defined:

(i) $\forall y\,[Cy \rightarrow (Tcy \rightarrow Pcy)]$
(iii) $\exists x\,(Sx \wedge Txs \wedge \neg Pxs)$
(v) $\exists x \forall y\,[(Sx \wedge Cy \wedge Txy) \rightarrow Pxy]$
(vii) $\forall x \exists y\,(Sx \wedge Cy \wedge Txy \wedge \neg Exy) \rightarrow \forall x \forall y\,[(Sx \wedge Cy) \rightarrow \neg Pxy]$

2. (i) No sports cars are motorcycles.
(iii) Any motorcycle is more economical than any sports car.
(v) There are sports cars which are slower than any motorcycle.

3. (i) Rx: x is rich,
Hx: x is always happy.

$\exists x\,(Rx \wedge \neg Hx)$

(iii) Ax: x went to the auction,
Bx: x bought something.

$\forall x\,(Ax \rightarrow Bx)$

(v) Wx: x spends all his or her time working.

$\neg\exists x\,Wx$

(vii) Cx: x is courageous,
Axy: x applauds y.

$\forall x \forall x\,(Cx \rightarrow Ayx)$ or $\forall x\,(Cx \rightarrow \forall y\,Ayx)$

Exercises 3.3

1. We define the following propositional functions on the universe of 'people':

Gx: x is good-looking,
Rx: x is rich,
Dx: x is dishonest.

1.	$\exists x\,(Gx \wedge Rx)$	(premise)
2.	$\forall x\,(Rx \rightarrow Dx)$	(premise)
3.	$Ga \wedge Ra$	(1. EI)
4.	$Ra \rightarrow Da$	(2. UI)
5.	$Ra \wedge Ga$	(3. Com)
6.	Ra	(5. Simp)
7.	Da	(4, 6. MP)
8.	Ga	(3. Simp)
9.	$Ga \wedge Da$	(7, 8. Conj)
10.	$\exists x\,(Gx \wedge Dx)$	(9. EG)

3. We define the following on the universe of 'numbers':

Ex: x is an even number,
Rx: x is rational,

Tx: x is divisible by two,
Fx: x is divisible by four.

1.	$\forall x\,[Ex \rightarrow (Rx \wedge Tx)]$	(premise)
2.	$\exists x\,(Ex \wedge Fx)$	(premise)
3.	$Ea \wedge Fa$	(2. EI)
4.	$Ea \rightarrow (Ra \wedge Ta)$	(1. UI)
5.	Ea	(3. Simp)
6.	$Ra \wedge Ta$	(4, 5. MP)
7.	$Fa \wedge Ea$	(3. Com)
8.	Fa	(7. Simp)
9.	$Ta \wedge Ra$	(6. Com)
10.	Ta	(9. Simp)
11.	$Ta \wedge Fa$	(8, 10. Conj)
12.	$\exists x\,(Tx \wedge Fx)$	(11. EG)

7. We define the following on the universe of 'people':

Dx: x is a doctor,
Lx: x is a lawyer,
Rx: x commands the respect of the community,
Hx: x earns a high salary.

1.	$\forall x\,[(Dx \vee Lx) \rightarrow (Rx \wedge Hx)]$	(premise)
2.	$(Da \vee La) \rightarrow (Ra \wedge Ha)$	(1. UI)
3.	La	(CP)
4.	$La \vee Da$	(3. Add)
5.	$Da \vee La$	(4. Com)
6.	$Ra \wedge Ha$	(2, 5. MP)
7.	Ra	(6. Simp)
8.	$La \rightarrow Ra$	(3-8. CP)
9.	$\forall x\,(Lx \rightarrow Rx)$	(8. UG)

9. We define the following on the universe of 'functions':

Px: x is a polynomial,
Dx: x is differentiable,
Cx: x is continuous.

1.	$\neg\exists x\,(Px \wedge \neg Dx)$	(premise)
2.	$\forall x\,(Dx \rightarrow Cx)$	(premise)

3.	$\forall x \neg(Px \wedge \neg Dx)$	(1. QD)
4.	$Da \rightarrow Ca$	(2. UI)
5.	$\neg(Pa \wedge \neg Da)$	(3. UI)
6.	$\neg Pa \vee \neg\neg Da$	(5. De M)
7.	$\neg Pa \vee Da$	(6. DN)
8.	$Pa \rightarrow Da$	(7. Imp)
9.	$Pa \rightarrow Ca$	(4, 8. HS)
10.	$\forall x\,(Px \rightarrow Cx)$	(9. UG)

Exercises 4.1

2. Any two great circles intersect at two antipodal points on the sphere. Therefore given a 'line' l and a point P not on l, there is no 'line' containing P which is parallel to l.

3. Under the given interpretation, each of the axioms is an 'elementary property' of the set of natural numbers.

4. Axiom A2 is false in the interpretation: $0 = (n - 1) + 1$.
The remaining axioms are true in the interpretation.

5. Since we know that $\mathbb{N}$ is a model of the axiom system, we need only consider how the axioms 'apply to' ω. For example:

A5. If $x = \omega$ then, for all $y \in \mathbb{N}$,

$$x + y' = \omega + y' = \omega = \omega' = (\omega + y)' = (x + y)'.$$

If $y = \omega$ then, for all $x \in \mathbb{N}$,

$$x + y' = x + \omega' = x + \omega = \omega = \omega' = (x + \omega)' = (x + y)'.$$

Exercises 4.2

1. (i)

	Statement	**Justification**
1.	$\forall x \forall x\,(x + y' = (x + y)')$	(axiom)
2.	$\forall x\,(x + \mathbf{0} = x)$	(axiom)
3.	$\forall x\,(\mathbf{1} + y' = (\mathbf{1} + y)')$	(1. UI)
4.	$\mathbf{1} + \mathbf{0}' = (\mathbf{1} + \mathbf{0})'$	(3. UI)

5.	$\mathbf{1}+\mathbf{0}=\mathbf{1}$	(2. UI)
6.	$\mathbf{1}+\mathbf{0}'=\mathbf{1}'$	(4, 5. substitution)
7.	$\mathbf{1}+\mathbf{1}=\mathbf{1}'$	(6. definition of **1**)
8.	$\mathbf{1}+\mathbf{1}=\mathbf{2}$	(7. definition of **2**)

(iv)

	Statement	**Justification**
1.	$\forall x \forall x\,(x+y'=(x+y)')$	(axiom)
2.	$\forall y\,(\mathbf{1}+y'=(\mathbf{1}+y)')$	(1. UI)
3.	$\mathbf{1}+\mathbf{1}'=(\mathbf{1}+\mathbf{1})'$	(3. UI)
4.	$\mathbf{1}+\mathbf{1}=\mathbf{2}$	(theorem: part (i) above)
5.	$\mathbf{1}+\mathbf{1}'=\mathbf{2}'$	(3, 4. substitution)
6.	$\mathbf{1}+\mathbf{1}'=\mathbf{3}$	(5. definition of **3**)
7.	$\mathbf{1}+\mathbf{2}=\mathbf{3}$	(6. definition of **2**)

Exercises 4.3

1. (ii) By A4 there exist three distinct points such that no line contains all three points. Suppose the points A, B and C satisfy this property. Let l_{PQ} denote the unique line containing points P and Q. Then l_{AB} does not contain C so $l_{AC} \neq l_{AB}$ and $l_{BC} \neq l_{AB}$. Similarly l_{BC} does not contain A so $l_{AC} \neq l_{BC}$. Therefore the three lines l_{AB}, l_{AC} and l_{BC} are distinct.

It is not possible for D to lie on more than one of these lines. (For example, if l_{AB} and l_{AC} both contain D then these are two distinct lines both containing A and D, contradicting the uniqueness part of A3.) Therefore there exists a pair of these lines, say l_1 and l_2, neither of which contains D. Now l_1 and l_2 have a point, P say, in common and none of the lines l_{AB}, l_{AC} and l_{BC} contain both D and P. Therefore there exists a fourth line containing these points.

Therefore, there exist at least four distinct lines.

2. The number of lines is now at least 5 and at most 10.

3. (a) (i) Since a and ab are strings (axioms 1 and 2) we can use axiom 4 to deduce that aba is a string and then axiom 3 to deduce that $abab$ is a string. Repeated use of axioms 4 and 3 in this way has the effect of adding ab to the end of the 'current' string. Therefore $abab\ldots ab$ (where ab is repeated n times) is a string for any positive integer n.

(ii) If a string ends in b then it must end in either ab (by axioms 2 and 3) or bbb (by axiom 4). Therefore, it is not possible for a string to end in abb.

4. (i) Define an infinite collection of events $A_1 = S$, $A_2 = \varnothing$, $A_3 = \varnothing$, $A_4 = \varnothing, \ldots$. These events are clearly pairwise disjoint and $\bigcup_{n=1}^{\infty} A_n = S$. Therefore, from axioms A2 and A3, we have $1 = 1 + p(\varnothing) + p(\varnothing) + p(\varnothing) + \cdots$ which implies $p(\varnothing) = 0$.

(ii) Suppose that $A_1, A_2, A_3, \ldots, A_N$ is a finite collection of pairwise disjoint events. Extend this to an infinite collection of pairwise disjoint events by defining $A_i = \varnothing$ for all $i > N$. Then

$$\bigcup_{n=1}^{\infty} A_n = \left(\bigcup_{n=1}^{N} A_n\right) \cup \left(\bigcup_{n=N+1}^{\infty} A_n\right) = \left(\bigcup_{n=1}^{N} A_n\right) \cup \varnothing = \left(\bigcup_{n=1}^{N} A_n\right)$$

and, using part (i),

$$\sum_{n=1}^{\infty} p(A_n) = \sum_{n=1}^{N} p(A_n) + \sum_{n=N+1}^{\infty} p(A_n) = \sum_{n=1}^{N} p(A_n) + 0 = \sum_{n=1}^{N} p(A_n).$$

Therefore axiom A3 now gives,

$$p\left(\bigcup_{n=1}^{N} A_n\right) = p\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} p(A_n) = \sum_{n=1}^{N} p(A_n).$$

The remaining parts of the exercise rely on part (ii) with suitably chosen pairwise disjoint families.

Exercises 5.1

1. (b) (i) Universe = {integers of the form $4^{2n+1} + 3^{n+2}$}, $Q(x)$: x is divisible by 13.

   (ii) $P(x)$: x is an integer of the form $4^{2n+1} + 3^{n+2}$.

   (d) (i) Universe = {rectangles}, $Q(x)$: x is a parallelogram.

   (ii) $P(x)$: x is a rectangle.

2. (b) $437 = 19 \times 23$ so 437 is composite (not prime).

(d) We assume, as background knowledge, the following result: *if a triangle has sides a, b and c then the area A satisfies* $A =$

$\sqrt{s(s-a)(s-b)(s-c)}$ *where* $s = \frac{1}{2}(a+b+c)$. Then direct calculation gives $A = 66$ cm^2.

4. (b) $$\frac{1}{500} - \frac{1}{700} = \frac{200}{500 \times 700} > \frac{200}{700 \times 700}$$

and $$\frac{1}{500} - \frac{1}{700} = \frac{200}{500 \times 700} < \frac{200}{500 \times 500};$$

hence $$\frac{200}{700^2} < \frac{1}{500} - \frac{1}{700} < \frac{200}{500^2}.$$

6. (b) Suppose that n and m are positive integers such that m is a factor of n and n is a factor of m. Since m is a factor of n, it follows that $m \leq n$; similarly, since n is a factor of m, it follows that $n \leq m$. From $m \leq n$ and $n \leq m$ we deduce $n = m$. (For an alternative proof, see Exercise 5.2.6.)

(d) Let A, B and C be sets. Then

$$\begin{aligned}(A \cap B) - C &= (A \cap B) \cap \overline{C} && \text{(definition of set difference)}\\ &= A \cap (B \cap \overline{C}) && \text{(associative law)}\\ &= A \cap (B - C) && \text{(definition of set difference).}\end{aligned}$$

7. (b) The problem is in the step

$$x(x-2) = x - 2 \quad \Rightarrow \quad \frac{x(x-2)}{x-2} = \frac{x-2}{x-2}.$$

Since $x = 2$ (from the first line of the proof), we are attempting to divide by 0 which is meaningless. In general, for real numbers a, b and c, we have $a = b$ and $c \neq 0 \Rightarrow a/c = b/c$.

Exercises 5.2

1. (a) Let a and b be non-negative real numbers and suppose that $a^2 \geq b^2$. Then $a^2 - b^2 = (a-b)(a+b) \geq 0$. If $a + b = 0$ then $a = b = 0$ so $a \geq b$. Otherwise $a + b > 0$ so $(a-b)(a+b) \geq 0$ implies $a - b \geq 0$ and thus $a \geq b$.

2. (b) Let the roots be α and β. Then $\alpha + \beta = -a$ and $\alpha\beta = b$. Therefore, if α and β are even integers then so, too, are $a = -(\alpha + \beta)$ and $b = \alpha\beta$.

3. (i) If the line $y = mx - 2$ intersects the parabola $y = 3x^2 + 1$, then the pair of simultaneous equations

$$y = mx - 2$$
$$y = 3x^2 + 1$$

has real solutions for x and y. Now

$$\left.\begin{aligned} y &= mx - 2 \\ y &= 3x^2 + 1 \end{aligned}\right\} \quad \Rightarrow \quad 3x^2 + 1 = mx - 2 \quad \Rightarrow \quad 3x^2 - mx + 3 = 0.$$

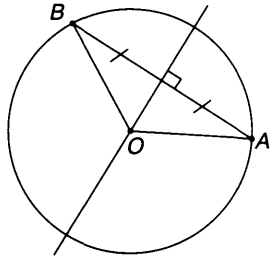
If the quadratic equation $3x^2 - mx + 3 = 0$ has a real solution then its discriminant $(-m)^2 - 4 \times 3 \times 3 \geq 0$. This implies $m^2 \geq 36$ so $|m| \geq 6$.

5. Let x and y be real numbers which are not both zero. Then

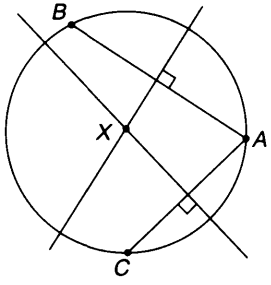
$$x^2 + xy + y^2 = \left(x^2 + xy + \frac{1}{4}y^2\right) + \frac{3}{4}y^2 = \left(x + \frac{1}{2}y\right)^2 + \frac{3}{4}y^2 > 0.$$

6. (ii) Let m and n be positive integers such that $m|n$ and $n|m$. Then there exist positive integers k_1 and k_2 such that $n = k_1 m$ and $m = k_2 n$. Therefore $k_1 k_2 = 1$. Since k_1 and k_2 are positive integers, this implies $k_1 = k_2 = 1$. Hence $m = n$.

7. Suppose two points A and B lie on a circle. Then the centre O of the circle lies on the perpendicular bisector of AB (because $OA = OB$).



Now, let A, B and C be three points in the plane which do not lie on a straight line. Consider the perpendicular bisectors of AB and AC. Since A, B and C do not lie on a straight line, AB and AC are not parallel and hence their perpendicular bisectors are also not parallel. Therefore the perpendicular bisectors of AB and AC intersect at a point, X say.



Now the circle with centre X and radius XA passes through B (since $XA = XB$ as X lies on the perpendicular bisector of AB) and passes through C (since $XA = XC$ as X lies on the perpendicular bisector of AC). Therefore all three points lie on the circle with centre X and radius XA.

8. (i) Let x and y be positive real numbers such that $x + y = 1$.

$$
\begin{aligned}
& (x-y)^2 \geq 0 \\
\Rightarrow \quad & x^2 - 2xy + y^2 \geq 0 \\
\Rightarrow \quad & x^2 + y^2 \geq 2xy \\
\Rightarrow \quad & x^2 + 2xy + y^2 \geq 4xy \\
\Rightarrow \quad & (x+y)^2 \geq 4xy. \\
\Rightarrow \quad & 1 \geq 4xy \qquad \text{(since } x + y = 1\text{)} \\
\Rightarrow \quad & xy \leq \frac{1}{4}.
\end{aligned}
$$

Exercises 5.3

1. (ii) Let G be a group and let $x, y \in G$ be two elements which commute.

Let $g \in G$. Then (using the associativity property of groups (group axiom 1) to bracket expressions as we please), we have:

$$
\begin{aligned}
& xy = yx \\
\Rightarrow \quad & g^{-1}xyg = g^{-1}yxg \\
\Rightarrow \quad & g^{-1}x(gg^{-1})yg = g^{-1}y(gg^{-1})xg
\end{aligned}
$$

$$\Rightarrow \qquad (g^{-1}xg)(g^{-1}yg) = (g^{-1}yg)(g^{-1}xg)$$

so $g^{-1}xg$ and $g^{-1}yg$ commute.

2. (ii) Let $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ be $n \times n$ matrices.

$$\begin{aligned}\mathbf{A} * (\mathbf{B} + \mathbf{C}) &= \mathbf{A}(\mathbf{B} + \mathbf{C}) - (\mathbf{B} + \mathbf{C})\mathbf{A} \\ &= \mathbf{AB} + \mathbf{AC} - \mathbf{BA} - \mathbf{CA} \\ &= \mathbf{AB} - \mathbf{BA} + \mathbf{AC} - \mathbf{CA} \\ &= (\mathbf{A} * \mathbf{B}) + (\mathbf{A} * \mathbf{C}).\end{aligned}$$

3. (b) Let x and y be elements of a group G such that $x \neq e$, $y \neq e$, $x^6 = e$, $x^{28} = e$ and $xyx = y^2$.

First note that $x^{24} = (x^6)^4 = e^4 = e$. Hence $x^{28} = e \Rightarrow x^4x^{24} = x^4 = e$.

Therefore $x^6 = e \Rightarrow x^2x^4 = e \Rightarrow x^2 = e$, so $|x| = 2$.

Now $xyx = y^2 \Rightarrow (xyx)(xyx) = y^4 \Rightarrow xyx^2yx = y^4 \Rightarrow xy^2x = y^4$.

But $y^2 = xyx$ so, substituting for y^2 in the equation $xy^2x = y^4$ gives $y^4 = x^2yx^2$. Since $x^2 = e$, we have $y = y^4$ so $y^3 = e$.

Since $y^3 = e$ and $y \neq e$, it follows that $|y| = 3$. (To prove this rigorously, we must also show that $y^2 \neq e$. This can be proved quite simply using the method of proof by contradiction—see Section 6.3.)

4. (ii) Let $\mathbf{A}$ and $\mathbf{B}$ be $n \times n$ matrices such that $\mathbf{A}$ is symmetric and $\mathbf{B}$ is anti-symmetric.

$$\begin{aligned}(\mathbf{B}^2)^{\mathrm{T}} &= (\mathbf{BB})^{\mathrm{T}} \\ &= \mathbf{B}^{\mathrm{T}}\mathbf{B}^{\mathrm{T}} && \text{(since, in general, } (\mathbf{AB})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}\text{)} \\ &= (-\mathbf{B})(-\mathbf{B}) && \text{(since } \mathbf{B} \text{ is anti-symmetric)} \\ &= \mathbf{B}^2.\end{aligned}$$

Since $(\mathbf{B}^2)^{\mathrm{T}} = \mathbf{B}^2$, it follows that $\mathbf{B}^2$ is symmetric, by definition.

7. Let $\mathbf{A}$ and $\mathbf{B}$ be orthogonal $n \times n$ matrices. Then $\mathbf{A}^{\mathrm{T}}\mathbf{A} = \mathbf{I}_n$ so $\mathbf{A} = (\mathbf{A}^{\mathrm{T}})^{-1}$. Hence

$$(\mathbf{A}^{\mathrm{T}}\mathbf{B})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}(\mathbf{A}^{\mathrm{T}})^{\mathrm{T}} = \mathbf{B}^{\mathrm{T}}\mathbf{A} = \mathbf{B}^{-1}(\mathbf{A}^{\mathrm{T}})^{-1} = (\mathbf{A}^{\mathrm{T}}\mathbf{B})^{-1}.$$

Therefore $\mathbf{A}^{\mathrm{T}}\mathbf{B}$ is also orthogonal.

8. (c) Assume d satisfies M2, M3 and M4. Then, for all $x, y \in X$, we have:

$$d(x,x) \leq d(x,y) + d(y,x) \quad \text{(from M4 with } z = x\text{)}$$

$$\Rightarrow \quad 0 \leq d(x,y) + d(y,x) \quad \text{(from M2)}$$

$$\Rightarrow \quad 0 \leq d(x,y) + d(x,y) \quad \text{(from M3)}$$

$$\Rightarrow \quad 0 \leq d(x,y).$$

Hence d satisfies M1.

(d) Verify that d satisfies M1, M2, M3 and M4.

10. (a) Verify that $\alpha = 1$ satisfies the conditions S1 and S2.

(b) Let A and B be non-empty subsets of $\mathbb{R}$ which are bounded above. Suppose $A \subseteq B$. Then $x \in A \Rightarrow x \in B \Rightarrow x \leq \sup B$, so $\sup B$ is an upper bound for A. Therefore $\sup A \leq \sup B$, by property S2 applied to $\sup A$.

(c) Let A be a non-empty subset of $\mathbb{R}$, which is bounded above, $x \in \mathbb{R}$ and $B = \{x + a : a \in \mathbb{R}\}$.

Let $b \in B$. Then $b = x + a$ for some $a \in A$. But $a \leq \sup A$ so $x + a \leq x + \sup A$. Therefore $x + \sup A$ is an upper bound for B, so $\sup B \leq x + \sup A$ by property S2 applied to $\sup B$.

Now $a \in A \Leftrightarrow x + a \in B$ so $a \in A \Leftrightarrow a = (-x) + b$ for some $b \in B$. Therefore $A = \{(-x) + b : b \in B\}$. Reversing the roles of A and B in the argument above, we obtain $\sup A \leq (-x) + \sup B$ so $\sup B \geq x + \sup A$.

Since $\sup B \leq x + \sup A$ and $\sup B \geq x + \sup A$ we have $\sup B = x + \sup A$, as required.

(d) Similar to (c).

Exercises 6.1

1. The contrapositive is 'if n is divisible by 7, then n^2 is divisible by 7' where n is any integer. The proof is similar to Example 5.2.2.

2. The negation of the (inclusive) disjunction 'm is even or n is even' is the conjunction 'm and n are both odd'. (This follows from De Morgan's

replacement rule.) The contrapositive is therefore 'if m and n are odd, then mn is odd' where m and n are any integers. This is proved using the fact that an integer p is odd if and only if $p = 2k + 1$ for some integer k.

3. The contrapositive is 'if m is even or n is even (or both), then mn is even'. This can be proved by considering the two cases:

(a) m is even regardless of n;
(b) n is even regardless of m.

(Of course these two cases overlap when both m and n are even but this does not affect the proof.)

5. The contrapositive is 'if $x^2 - x - a = 0$ has at least one integer root, then a is not an odd integer'.

An outline of the proof is given below.

Suppose that $x^2 - x - a = 0$ has roots x_1 and x_2 and that x_1 is an integer.

Then $x^2 - x - a = 0$

$\Rightarrow \quad x_1 + x_2 = 1$ and $x_1 x_2 = -a$.

The first of these equations implies that x_2 is also an integer. We can then show that $x_1 x_2$ is even (using $x_1 + x_2 = 1$) and hence that a is not an odd integer.

Exercises 6.2

2. Suppose that $m + \sqrt{2}n$ is rational, where m and n are integers and $n \neq 0$ and show that this implies that $\sqrt{2}$ is rational.

3. Suppose that there is some integer $n > 1$ for which the smallest factor, $k > 1$, is not prime.

Then $n = kl$ for some integer l.

But k is not prime so that $k = k_1 k_2$ for some integers k_1 and k_2 where $1 < k_1, k_2 < k$.

Hence $n = k_1 k_2 l$

$\Rightarrow k$ is not the smallest factor of n.

This contradiction allows us to conclude that the smallest factor greater than one of any integer greater than one must be prime.

5. Suppose there exist sets A and B such that $(A - B) \cap B \neq \varnothing$. Then there exists an element a such that

$$\begin{aligned} & a \in A - B \text{ and } a \in B \\ \Rightarrow\ & a \in A \cap \overline{B} \text{ and } a \in B \\ \Rightarrow\ & a \in A \text{ and } a \in \overline{B} \text{ and } a \in B. \end{aligned}$$

Clearly there is a contradiction here. We cannot have $a \in \overline{B}$ and $a \in B$. Hence the theorem is proved.

6. Assume a universe for n of integers greater than 1. The contrapositive of the theorem is then 'for any n, if n is not prime, then n has a prime factor k where $2 \leq k \leq \sqrt{n}$'. From Exercise 3 above, we do know that the smallest factor of n is prime. Suppose that this factor is l and that $l > \sqrt{n}$ (i.e l is *not* in the range $2 \leq l \leq \sqrt{n}$) and deduce a contradiction.

8. Suppose that the sets $A_1, \ldots, A_n, B_1, \ldots, B_n$ are as given in the exercise and suppose $B_i \cap B_j \neq \varnothing$ for some $i < j$.

$$\begin{aligned} \text{Choose}\quad & x \in B_i \cap B_j. \\ \text{Then}\quad & x \in B_i \\ \text{i.e.}\quad & x \in A_i - (A_1 \cup \cdots \cup A_{i-1}) \\ \Rightarrow\quad & x \in A_i. \\ \text{Also}\quad & x \in B_j \\ \text{i.e.}\quad & x \in A_j - (A_1 \cup \cdots \cup A_{j-1}) \\ \Rightarrow\quad & x \notin (A_1 \cup \cdots \cup A_{j-1}) \\ \Rightarrow\quad & x \notin A_i. \end{aligned}$$

We've proved $x \in A_i$ and $x \notin A_i$, a contradiction.

Hence $B_i \cap B_j = \varnothing$ for all $i \neq j$.

9. Let $\{x_n\}$ be a real sequence with limit l and suppose $x_n \geq a$ for all n but $l < a$.

Then $\varepsilon = a - l > 0$.

Therefore there exists $N > 0$ such that $|x_n - l| < \varepsilon$ for all $n > N$.

Show that this implies that $x_n < a$ for all $n > N$.

11. Suppose that G is a group with 6 elements and that $g \in G$ has order 5.

Then e, g, g^2, g^3, g^4 are distinct elements of G (and $g^5 = e$).

Therefore $G = \{e, g, g^2, g^3, g^4, h\}$ where $h \neq g^n$ for any n.

Consider $gh \in G$. Since $h \neq g^n$, it follows that $gh \neq g^n$ for any n.

Therefore $gh = h$, so $g = e$, a contradiction.

12. (a) Suppose that $\{a_n\}$ converges to limit 1.

Let $\varepsilon = \frac{1}{2}$. Since $\varepsilon > 0$, there exists an $N > 0$ such that

$$|a_n - 1| < \varepsilon = \tfrac{1}{2} \text{ for all } n > N.$$

But if n is odd and $n > N$, then

$$\begin{aligned} |a_n - 1| &= |(-1)^n - 1| \\ &= |-2| \\ &> \frac{1}{2}. \end{aligned}$$

This is a contradiction.

(b) Suppose $\{a_n\}$ converges to a limit l.

Let $\varepsilon = 1$. Since $\varepsilon > 0$, there exists an $N > 0$ such that

$$|a_n - l| < 1 \text{ for all } n > N.$$

Choose n, m such that $n > N, m > N$ and n is even, m is odd. By writing $2 = |2| = |(1 - l) + (1 + l)|$, show that this leads to the contradiction $2 < 2$.

Exercises 6.3

1. $x \in A \cup (B \cap C)$

   $\Leftrightarrow$ $x \in A$ or $x \in B \cap C$

   $\Leftrightarrow$ $x \in A$ or ($x \in B$ and $x \in C$)

   $\Leftrightarrow$ ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$) (see note below)

   $\Leftrightarrow$ $x \in A \cup B$ and $x \in A \cup C$

   $\Leftrightarrow$ $x \in (A \cup B) \cap (A \cup C)$.

Therefore $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Note: We can think of the statement in the third line of the proof as being the disjunction of two propositions. One is '$x \in A$' and the other is the conjunction of '$x \in B$' and '$x \in C$', where x is an arbitrary element of $A \cup (B \cap C)$. By the distribution replacement rule, $(x \in A) \vee [(x \in B) \wedge (x \in C)]$ is equivalent to $[(x \in A) \vee (x \in B)] \wedge [(x \in A) \vee (x \in C)]$ and hence to the fourth line of the proof.

3. Suppose that m and n are integers which have the same remainder after division by 5 and show that this implies that $m - n = 5(k - l)$ for some integers k and l.

Then suppose that 5 is a factor of $m - n$. Let m have remainder r_1 and let n have remainder r_2 after division by 5. Then consider $m - n$ and show that $r_1 = r_2$.

4. Suppose that p is a prime factor of mn and use the fact that m and n can each be expressed uniquely (apart from ordering) as a product of prime factors (see Section 4.2) to show that p is a factor of m or of n.

The converse is straightforward.

5. $y = mx - 2$ and $y = 3x^2 + 1$ intersect

   $\Leftrightarrow$ $mx - 2 = 3x^2 + 1$ has real roots

   $\Leftrightarrow$ $3x^2 - mx + 3 = 0$ has real roots

   $\Leftrightarrow$ $b^2 \geq 4ac$ where $a = 3, b = -m, c = 3$

   $\Leftrightarrow$ $m^2 \geq 36$

   $\Leftrightarrow$ $|m| \geq 6$.

Hence $y = mx - 2$ and $y = 3x^2 + 1$ intersect if and only if $|m| \geq 6$.

9. Suppose that the two quadratic equations have a common root x_1. Then $a_1x_1^2 + b_1x_1 + c_1 = 0$ and $a_2x_1^2 + b_2x_1 + c_2 = 0$. Subtracting a_2 times the first equation from a_1 times the second gives

$$x_1(a_1b_2 - a_2b_1) + a_1c_2 - a_2c_1 = 0$$

$$\Rightarrow \qquad x_1 = \frac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1}.$$

Similarly, subtracting b_2 times the first equation from b_1 times the second, we have (after a little algebra)

$$x_1^2 = \frac{b_2c_1 - c_2b_1}{a_2b_1 - a_1b_2}.$$

Putting these together gives

$$\left(\frac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1}\right)^2 = \frac{b_2c_1 - c_2b_1}{a_2b_1 - a_1b_2}.$$

The result follows after a little algebra.

Now suppose that $(a_1b_2 - a_2b_1)(b_1c_2 - b_2c_1) = (c_1a_2 - c_2a_1)^2$. Taking our cue from the first part of the proof, we write

$x = \dfrac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1}$. Then we show that $a_1x^2 + b_1x + c_1 = 0$.

Hence $x = \dfrac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1}$ is a root of $a_1x^2 + b_1x + c_1 = 0$.

In a similar way we can show that $x = \dfrac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1}$ is also a root of $a_2x^2 + b_2x + c_2 = 0$.

This shows that the two quadratic equations have a common root and completes the proof of the theorem.

10. Suppose that G is abelian and let $a, b \in G$.

Then $$(ab)^{-1} = b^{-1}a^{-1} \quad \text{(see Example 5.6.3)}$$

$$= a^{-1}b^{-1} \quad \text{(since } G \text{ is abelian).}$$

Now suppose that $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$.

If $a, b \in G$, then $b^{-1}, a^{-1} \in G$.

Hence $(a^{-1}b^{-1})^{-1} = (a^{-1})^{-1}(b^{-1})^{-1}$ (by the assumption)

$$\Rightarrow \quad (a^{-1}b^{-1})^{-1} = ab$$
$$\Rightarrow \quad (b^{-1})^{-1}(a^{-1})^{-1} = ab$$
$$\Rightarrow \quad ba = ab.$$

Therefore G is abelian.

12. (i) Let $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c and d are non-zero real numbers.

Then $\mathbf{A}^2 = \mathbf{0}_{2\times 2} \Rightarrow$

$$a^2 + bc = 0 \quad (1)$$
$$b(a+d) = 0 \quad (2)$$
$$c(a+d) = 0 \quad (3)$$
$$bc + d^2 = 0 \quad (4)$$

Now, (2) $\Rightarrow a = -d$ (as does (3)) and (1) $\Rightarrow c = \dfrac{-a^2}{b}$.

Hence $\mathbf{A} = \begin{pmatrix} a & b \\ \dfrac{a^2}{b} & -a \end{pmatrix}$.

The converse is proved directly by evaluating $\mathbf{A}^2$,

where $\mathbf{A} = \begin{pmatrix} a & b \\ \dfrac{a^2}{b} & -a \end{pmatrix}$.

(ii) $\mathbf{A}^2 = \mathbf{A} \Rightarrow$

$$a^2 + bc = a \quad (1)$$
$$b(a+d) = b \quad (2)$$
$$c(a+d) = c \quad (3)$$
$$bc + d^2 = d \quad (4)$$

These equations give $d = 1 - a$ and $c = \dfrac{a(1-a)}{b} \quad (a \neq 1)$.

The converse is proved by direct calculation.

13. To prove that, if $m + n\sqrt{2}$ is rational, then $n = 0$ (see Exercise 6.2.2 which is the contrapositive of this theorem).

If $n = 0$, then $m + n\sqrt{2} = m$, which is clearly rational since it is an integer.

Exercises 7.1

1. (b) 3, 5 and 7 are all prime.

   (d) $72 = 6^2 + 6^2, 73 = 3^2 + 8^2$ and $74 = 5^2 + 7^2$.

   (f) $\sqrt[4]{2}$ and $\sqrt{2}$ are both irrational.

   (h) $65 = 1^2 + 8^2 = 4^2 + 7^2$.

   (j) $1729 = 1^3 + 12^3 = 9^3 + 10^3$.

There is a famous story associated with this example. G. H. Hardy was visiting his protégé, the brilliant and largely self-taught Indian mathematician Srinivasa Ramanujan, who was ill. In his book about Ramanujan[1], Hardy recalls:

It was Littlewood who said that every positive integer was one of Ramanujan's personal friends. I remember going to see him once when he was lying ill in Putney. I had ridden in a taxi-cab No. 1729, and had remarked that the number seemed to me a rather dull one, and that I hoped it was not an unfavourable omen. 'No,' he reflected, 'it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways.'

2. (ii) If $A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ then $\mathbf{A}^2 = \mathbf{I}_2$.

   (iv) If $\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$

   then $\mathbf{AB} = \mathbf{I}_2$ but $\mathbf{BA} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

3. (ii) 2 has no multiplicative inverse.

   (*Proof*: for all $x \in \mathbb{Z}_8, 2 \times_8 x$ is even and so cannot be equal to 1.)

   (iv) $x = 5$ is a solution.

[1] G.H. Hardy, *Ramanujan: Twelve Lectures on Subjects Suggested by his Life and Works*, Chelsea, New York, 1959, page 12. (Reprint of 1940 Cambridge University Press edition.)

Exercises 7.2

1. Let P be an n-sided non-convex polygon and suppose that every interior angle satisfies $\theta \geq (n-3)\pi/(n-1)$. Since P is non-convex there exists an interior angle, $\phi > \pi$. Then:

$$\text{sum of interior angles} = \phi + \text{sum of remaining interior angles}$$
$$> \pi + (n-1)\left(\frac{n-3}{n-1}\right)\pi = (n-2)\pi.$$

This contradicts the theorem given as background knowledge in Example 7.2.2. Therefore there exists an interior angle satisfying $\theta < (n-3)\pi/(n-1)$.

There is no contradiction since every triangle is convex. (The angle-sum in a triangle is π, so every interior angle satisfies $\theta \leq \pi$.)

3. Suppose that $n+1$ matches were played and that no-one played more than once. Since each match has two players, there were $2n+2$ different members involved in the matches. However the club has only $2n+1$ members. Therefore some member played more than once.

5. Let $S = \{x \in \mathbb{R} : x > 0 \text{ and } x^2 < 2\}$. Clearly $S \neq \emptyset$, since $1 \in S$ for example. Note also that if $x > 3$ then $x^2 > 9$ so $x \notin S$. Hence if $x \in S$ then $x \leq 3$ so S is bounded above (by 3).

By the completeness axiom for $\mathbb{R}$, the bounded, non-empty set S has a supremum, α say. We can prove that $\alpha^2 = 2$ using the method of proof by contradiction. (Show that $\alpha^2 < 2$ and $\alpha^2 > 2$ each leads to a contradiction.)

Exercises 7.3

2. (b) $a = 5, \quad b = 4, \quad c = 3.$

   (d) $n = 5: \quad 6^5 + 4 \times 5^4 = 10276.$

   (f) $n = 8: \quad 8^4 + 1 = 4097 = 17 \times 241.$

3. $\sqrt{2} \in A \cup (B - C)$ but $\sqrt{2} \notin (A \cup B) - C$.
   Hence $A \cup (B - C) \neq (A \cup B) - C$.

4. (ii) $\mathbf{A} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$. (iv) $\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$.

5. (i) *Proof.* Suppose a and b are rational numbers. Then there exist integers m, n, p, q such that $n \neq 0, q \neq 0, a = m/n$ and $b = p/q$. Now

$$ab = \frac{m}{n} \times \frac{p}{q} = \frac{mp}{nq}$$

where mp and nq are integers and $nq \neq 0$. Therefore ab is rational. □

(ii) *Counter-example.* Let $a = \sqrt{2} = b$; then a and b are irrational but $ab = 2$ is rational.

6. (c) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = -x^4$, is twice differentiable, has a local maximum at $x = 0$ but $f''(0) = 0$. Similarly $g\colon \mathbb{R} \to \mathbb{R}$, $g(x) = x^4$, is twice differentiable, has a local minimum at $x = 0$ but $g''(0) = 0$.

7. (b) *Counter-example.* $A = \{1, 2\}$, $B = \{2, 4\}$ and $C = \{1, 2, 3\}$.

(c) *Counter-example.* $\mathbf{A} = \begin{pmatrix} 4 & 2 \\ 2 & 1 \end{pmatrix}$ and $\mathbf{B} = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$.

Exercises 7.4

4. Suppose $ad - bc \neq 0$.

Existence. A solution is $x = \dfrac{ds - bt}{ad - bc}$, $y = \dfrac{at - cs}{ad - bc}$.

Uniqueness. Suppose that:

$$\begin{aligned} ax_1 + by_1 &= s \quad (1) \\ cx_1 + dy_1 &= t \quad (2) \end{aligned} \qquad \text{and} \qquad \begin{aligned} ax_2 + by_2 &= s \quad (3) \\ cx_2 + dy_2 &= t \quad (4) \end{aligned}$$

Subtracting (3) from (1) and subtracting (4) from (2) gives:

$$a(x_1 - x_2) + b(y_1 - y_2) = 0 \quad (5)$$
$$c(x_1 - x_2) + d(y_1 - y_2) = 0 \quad (6)$$

Now subtract $b \times (6)$ from $d \times (5)$:

$$(ad - bc)(x_1 - x_2) = 0.$$

Since $ad - bc \neq 0$, it now follows that $x_1 - x_2 = 0$ so $x_1 = x_2$. Equations (5) and (6) now simplify to

$$b(y_1 - y_2) = 0$$
$$d(y_1 - y_2) = 0$$

Since b and d cannot *both* be zero (otherwise $ad - bc$ would be zero), one of these equations (at least) implies $y_1 - y_2 = 0$ so $y_1 = y_2$.

Therefore the solution is unique.

6. (ii) Suppose a and b are inverses of x. Then

$$\begin{aligned} a &= (bx)a && \text{(since } bx = e \text{ because } b \text{ is an inverse of } x\text{)} \\ &= b(xa) && \text{(associativity)} \\ &= b && \text{(since } xa = e \text{ because } a \text{ is an inverse of } x\text{).} \end{aligned}$$

7. Let S be a non-empty subset of $\mathbb{R}$ which is bounded above and let α and $\overline{\alpha}$ be suprema for S.

Since $\overline{\alpha}$ is an upper bound for S, the supremum property S2 for α (see Exercise 5.3.10) implies $\alpha \leq \overline{\alpha}$. Similarly, since α is an upper bound for S, the supremum property S2 for $\overline{\alpha}$ implies $\overline{\alpha} \leq \alpha$. Hence $\overline{\alpha} = \alpha$.

Exercises 8.1

2. For all real numbers x and y,

$$\begin{aligned} (x+y)^4 - (x-y)^4 &= (x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4) \\ &\quad - (x^4 - 4x^3y + 6x^2y^2 - 4xy^3 + y^4) \\ &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \\ &\quad - x^4 + 4x^3y - 6x^2y^2 + 4xy^3 - y^4 \\ &= 8x^3y + 8xy^3 \\ &= 8xy(x^2 + y^2). \end{aligned}$$

3. Let k and n be positive integers such that $k \leq n$. Then

$$\begin{aligned} \frac{n-k+1}{k} \times \binom{n}{k-1} &= \frac{n-k+1}{k} \times \frac{n!}{(n-(k-1))!(k-1)!} \\ &= \frac{n-k+1}{k} \times \frac{n!}{(n-k+1)!(k-1)!} \end{aligned}$$

$$= \frac{(n-k+1) \times n!}{(n-k+1)(n-k)! \times k(k-1)!}$$
$$= \frac{n!}{(n-k)!k!}$$
$$= \binom{n}{k}.$$

8. (i) Let n and r be positive integers such that $r \leq n+2$. Then

$$(n)_r + 2r(n)_{r-1} + r(r-1)(n)_{r-2}$$
$$= \frac{n!}{(n-r)!} + 2r\frac{n!}{(n-r+1)!} + r(r-1)\frac{n!}{(n-r+2)!}$$
$$= \frac{n!}{(n-r+2)!}((n-r+2)(n-r+1) + 2r(n-r+2) + r(r-1))$$
$$= \frac{n!}{(n-r+2)!}(n^2 - 2nr + r^2 + 3n - 3r + 2 + 2nr - 2r^2 + 4r + r^2 - r)$$
$$= \frac{n!}{(n-r+2)!}(n^2 + 3n + 2)$$
$$= \frac{n!}{(n-r+2)!}(n+2)(n+1)$$
$$= \frac{(n+2)!}{(n-r+2)!}$$
$$= (n+2)_r.$$

(ii) Let n and r be positive integers such that $r \leq n+2$. Using the theorem in Example 8.2.2. we have:

$$(n+2)_r = (n+1)_r + r(n+1)_{r-1}$$
$$= (n)_r + r(n)_{r-1} + r((n)_{r-1} + (r-1)(n)_{r-2})$$
$$= (n)_r + 2r(n)_{r-1} + r(r-1)(n)_{r-2}.$$

10. (i) For all sets A, B and C belonging to $\mathcal{U}$,

$$(A \cup B) - C = (A \cup B) \cap \overline{C} \qquad \text{(definition of set difference)}$$
$$= \overline{C} \cap (A \cup B) \qquad \text{(commutative law)}$$
$$= (\overline{C} \cap A) \cup (\overline{C} \cap B) \qquad \text{(distributive law)}$$

$$= (A \cap \overline{C}) \cup (B \cap \overline{C}) \quad \text{(commutative law)}$$
$$= (A - C) \cup (B - C) \quad \text{(definition of set difference)}.$$

Exercises 8.2

1. (i) $(n)_k$ is the number of lists of length k chosen from a set of n distinguishable objects. Such a list may be constructed in two stages as follows.

First choose a *set* of k objects from the n given. This can be done in $\binom{n}{k}$ ways.

Then order the chosen k objects in a list. This can be done in $k! = (k)_k$ ways.

Therefore, the total number of lists is $\binom{n}{k}(k)_k$.

We have counted the number of lists in two different ways so $(n)_k = \binom{n}{k}(k)_k$.

3. (i) Consider a sequence $x_1 x_2 \ldots x_n$ of length n constructed from the letters a, b and c. Since there are 3 choices for each letter x_i, the total number of such sequences is 3^n.

Next, we count the number of such sequences in which the letter a appears exactly k times, for some fixed value of k where $0 \leq k \leq n$. We can construct such a sequence by first selecting k positions in the sequence to take the letter a. This amounts to choosing k members of the 'set of positions' $\{1, 2, \ldots, n\}$, so there are $\binom{n}{k}$ such choices. The remaining $n - k$ positions form a sequence constructed from the letters b and c, so there are 2^{n-k} such sequences (using a similar argument to that in the previous paragraph). Therefore the number of sequences containing exactly k a's is

$$\binom{n}{k} 2^{n-k}.$$

Since there must be k a's for *some* value of $k = 0, 1, 2, \ldots, n$,

$$3^n = \text{total number of sequences}$$

$$= \sum_{k=0}^{n} (\text{number of sequences with } k \text{ letter } a\text{'s})$$

$$= \sum_{k=0}^{n} \binom{n}{k} 2^{n-k}.$$

4. (a) Divide the rectangle into four equally sized sub-rectangles, as shown.

3	R3	R4
3	R1	R2
	4	4

By the pigeon hole principle, if five points are located in the rectangle then at least two of them are situated in one of the sub-rectangles. The maximum distance apart of two points in one of the sub-rectangles is the length of a diagonal which is $\sqrt{3^2 + 4^2} = 5$ units, by Pythagoras' theorem. Therefore there exists a pair of points which are no more than 5 units apart.

5. There are 10 prime numbers less that 30, namely 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Suppose that 12 distinct integers are chosen from the set $\{1, 2, 3, \ldots, 30\}$. At least 11 of the chosen integers are different from 1. For each such integer, consider its smallest prime factor. Since there are only 10 possible distinct prime factors, at least one pair has a common (smallest prime) factor greater than 1, by the pigeon hole principle.

Exercises 8.3

2. (a) If n is not a multiple of 3 then $n = 3k + 1$ or $n = 3k + 2$ for some integer k. Now consider n^2 in each case.

(c) The multiplication table for $\{0, 1, 2, 3, 4\}$ under multiplication modulo 5 is:

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

If n is not a multiple of 5, then $n \neq 0$ modulo 5. Considering the top-left to bottom-right diagonal of the table, we see that n^2 is 1 or 4 modulo 5. Therefore $n^4 = 1^2 = 1$ or $n^4 = 4^2 = 1$ modulo 5. Hence if n is not a multiple of 5, then n^4 has remainder 1 after division by 5.

3. (b) We use the inequality $|x + y| \leq |x| + |y|$ (see Example 8.6.2.) Using this, we have

$$|x| = |(x - y) + y| \leq |x - y| + |y| \text{ so } |x - y| \geq |x| - |y|.$$

Hence $|x - y| = |y - x| \geq |y| - |x|$.

Since $|x - y|$ is at least as large as both $|x| - |y|$ and $|y| - |x| = -(|x| - |y|)$, it follows that $|x - y| \geq ||x| - |y||$ as required.

4. (i) Let k be an integer such that $k - 1$ is divisible by 3 and $k(k - 1)$ is divisible by 12. Since $k - 1$ is divisible by 3, it follows that $k = 1, 4, 7$ or 10 modulo 12.

If $k = 1$ or 4 modulo 12 then $k(k - 1) = 0$ modulo 12 so $k(k - 1)$ is divisible by 12.

If $k = 7$ or 10 modulo 12 then $k(k - 1) = 6$ modulo 12 so $k(k - 1)$ is not divisible by 12.

Therefore $k = 1$ or 4 modulo 12 so $k = 12n + 1$ or $k = 12n + 4$ for some integer n.

5. (a) Let A, B and X be sets such that $A \subseteq X$ and $B \subseteq X$ and let $x \in A \cup B$. Then $x \in A$ or $x \in B$ (or both). If $x \in A$ then $x \in X$ since $A \subseteq X$; if $x \in B$ then $x \in X$ since $B \subseteq X$. We have proved $x \in A \cup B \Rightarrow x \in X$ so $(A \cup B) \subseteq X$.

Exercises 9.1

1. Clearly $0 < 2^0$ so that $n < 2^n$ holds for $n = 0$.

Suppose that $k < 2^k$ for some arbitrary natural number k. (This is the induction hypothesis.)

Now $\quad k < 2^k$

$\Rightarrow \quad k + 1 < 2^k + 1$

$\leq 2^k + 2^k \quad$ (since $2^k \geq 1$ for all $k \in \mathbb{N}$)

$$= 2 \times 2^k$$
$$= 2^{k+1}.$$

This completes the inductive step. So, by mathematical induction, we can conclude that $n < 2^n$ for all $n \in \mathbb{N}$.

4. If $n = 0$, we have

$$\frac{x^{n+1} - 1}{x - 1} = \frac{x - 1}{x - 1}$$
$$= 1$$
$$= \sum_{i=0}^{0} x^i.$$

This completes the initial step.

The induction hypothesis is

$$\sum_{i=0}^{k} x^i = \frac{x^{k+1} - 1}{x - 1}.$$

Then

$$\sum_{i=0}^{k+1} x^i = \frac{x^{k+1} - 1}{x - 1} + x^{k+1}$$
$$= \frac{x^{k+1} - 1 + x^{k+1}(x - 1)}{x - 1}$$
$$= \frac{x^{k+2} - 1}{x - 1}.$$

This completes the inductive step and the theorem follows by mathematical induction.

5. (i) If $n = 4, n^3 = 64$ and $3^n = 81$. Hence $n^3 < 3^n$ for $n = 4$.

Induction hypothesis: $k^3 < 3^k$ for some arbitrary integer $k \geq 4$.

We have

$$(k + 1)^3 = k^3 + 3k^2 + 3k + 1.$$

Now $3k^2 < k \times k^2 = k^3$ since $k \geq 4$

and

$$\begin{aligned} 3k+1 &< k \times 3k \\ &= 3k^2 \\ &< k^3 \qquad \text{from the result above.} \end{aligned}$$

So

$$\begin{aligned} (k+1)^3 &< k^3 + k^3 + k^3 \\ &= 3k^3 \\ &< 3 \times 3^k \qquad \text{by the induction hypothesis} \\ &= 3^{k+1}. \end{aligned}$$

This completes the inductive step and the theorem follows by mathematical induction.

6. (ii) The conjecture is $\sum_{i=1}^{n}(2i-1) = n^2$.

7. If $n = 1, x^{2n-1} + 1 = x + 1$. Hence, for $n = 1, (x+1)$ is a factor of $x^{2n-1} + 1$.

Suppose that for some positive integer k, $(x+1)$ is a factor of $x^{2k-1} + 1$, i.e. $x^{2k-1} + 1 = (x+1)f(x)$ where $f(x)$ is a polynomial of degree $2k-2$.

Then show that $x^{2(k+1)-1} + 1 = (x+1)[x^2 f(x) - (x-1)]$ where $x^2 f(x) - (x-1)$ is a polynomial of degree $2k$.

9. Initial step:

$$\begin{aligned} \sum_{i=1}^{1} \frac{1}{i(i+1)} &= \frac{1}{1(1+1)} \\ &= \frac{1}{1+1}. \end{aligned}$$

Induction hypothesis:

$$\sum_{i=1}^{k} \frac{1}{i(i+1)} = \frac{k}{k+1}.$$

Inductive step:

$$\begin{aligned} \sum_{i=1}^{k+1} \frac{1}{i(i+1)} &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k(k+2)+1}{(k+1)(k+2)} \end{aligned}$$

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

The theorem follows by mathematical induction.

12. (a) The initial step is trivial.

Induction hypothesis: suppose that, for some positive integer k, if p is prime and $a_1, a_2, \ldots, a_k$ are positive integers such that $p|(a_1 \ldots a_k)$, then p divides one of the positive integers $a_1, \ldots, a_k$.

Inductive step: Let $p|(a_1 \ldots a_k a_{k+1})$.

Then $p|(a_1 \ldots a_k)$ or $p|a_{k+1}$ (see Exercise 6.3.4).

So $p|a_1$ or $p|a_2$ or ... or $p|a_k$ or $p|a_{k+1}$ (by the induction hypothesis).

The result follows by mathematical induction.

(b) The initial step is trivial.

Induction hypothesis: suppose that, for some positive integer k, if $a_1, a_2, \ldots, a_k$ are members of some universe such that $a_1 = a_2, a_2 = a_3, \ldots, a_{k-1} = a_k$, then $a_1 = a_k$.

Inductive step: suppose that $a_1 = a_2, a_2 = a_3, \ldots, a_{k-1} = a_k, a_k = a_{k+1}$.

Then $a_1 = a_k$ and $a_k = a_{k+1}$ (by the induction hypothesis).

So $a_1 = a_{k+1}$ by the transitive property of equality (see page 211).

The result follows by mathematical induction.

Exercises 9.2

3. To effect the inductive step, consider dividing the $(k+1)$-sided polygon into a k-sided polygon and a triangle.

4. (i) We have $f_3 = f_2 + f_1 = 1 + 1 = 2$, so that $f_3 < 2^3$.

Suppose that there is a $k \in \mathbb{Z}^+$ such that $f_n < 2^n$ for all $n \in \mathbb{Z}^+$ such that $3 \leq n \leq k$.

Now

$$\begin{aligned} f_{k+1} &= f_k + f_{k-1} \\ &< 2^k + 2^{k-1} \quad \text{(by the induction hypothesis)} \\ &= 2^{k+1}\left(\frac{1}{2} + \frac{1}{4}\right) \\ &= \frac{3}{4}\, 2^{k+1} \\ &< 2^{k+1}. \end{aligned}$$

Hence we have shown by mathematical induction that $f_n < 2^n$ for all $n \geq 3$.

However, $f_1 < 2^1$ and $f_2 < 2^2$ so that $f_n < 2^n$ for all positive integers n.

7. The inductive step is achieved in a similar way to that of Exercise 4(i) above.

8. Define $P(n)$: If A and B are sets such that $|A| = n$ and $B \subset A$, then $|B| < |A|$.

Then $P(0)$ is true since its antecedent is false.

Assume that $P(k)$ is true for some positive integer k.

Let A be a set with $k + 1$ elements and let $B \subset A$.

If $B = \varnothing$ then $|B| = 0 \Rightarrow |B| < k + 1 = |A|$.

If $B \neq \varnothing$ then choose $x \in B$.

Then $x \in A$ and $(B - \{x\}) \subset (A - \{x\})$.

But $|A - \{x\}| = k$ so, by the induction hypothesis,

$$\begin{aligned} & |B - \{x\}| < |A - \{x\}| \\ \Rightarrow \quad & |B - \{x\}| < k. \end{aligned}$$

Now $|B - \{x\}| = |B| - 1$

$\Rightarrow \quad |B| - 1 < k$

$\Rightarrow \quad |B| < k + 1$

$\Rightarrow \quad |B| < |A|$.

This completes the inductive step and the result follows by mathematical induction.

10. Suppose that $P(n)$ satisfies the conditions given.

Initial step: $P(2)$ is true (from condition (a))

$\Rightarrow \quad P(1)$ is true (from condition (c))

Inductive step: Suppose $P(k)$ is true.

Then $P(2k)$ is true (from (b))

$\Rightarrow \quad P(2k-1)$ is true (from (c))

$\Rightarrow \quad P(2k-2)$ is true (from (c))

.

.

.

$\Rightarrow \quad P(2k-(k-1)) = P(k+1)$ is true (from (c)).

The theorem follows by mathematical induction.