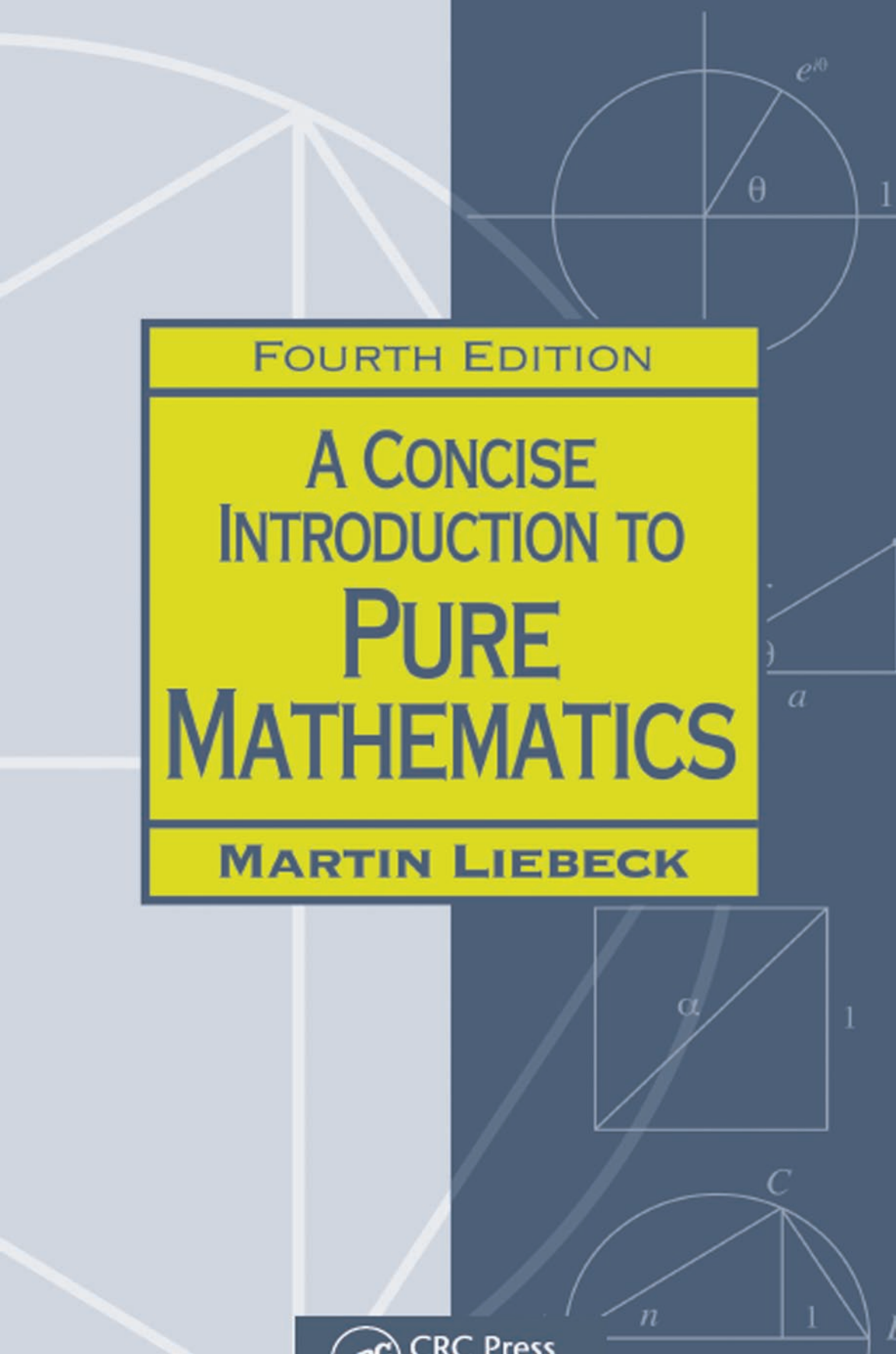

FOURTH EDITION
A CONCISE INTRODUCTION TO PURE MATHEMATICS
MARTIN LIEBECK
CRC Press

FOURTH EDITION

A CONCISE INTRODUCTION TO PURE MATHEMATICS

FOURTH EDITION

A CONCISE INTRODUCTION TO PURE MATHEMATICS

MARTIN LIEBECK

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20150825

International Standard Book Number-13: 978-1-4987-2292-6 (Paperback)

Library of Congress Cataloging-in-Publication Data

Liebeck, M. W. (Martin W.), 1954-
A concise introduction to pure mathematics / Martin Liebeck. -- Fourth edition.
pages cm
"A CRC title."
Includes bibliographical references and index.
ISBN 978-1-4987-2292-6 (alk. paper)
1. Logic, Symbolic and mathematical. 2. Mathematics. I. Title.

QA9.L478 2016
510--dc23 2015025649

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

To Ann, Jonny and Matthew

Contents

Foreword ix

Preface xi

1 Sets and Proofs 1

2 Number Systems 13

3 Decimals 21

4 n^{th} Roots and Rational Powers 27

5 Inequalities 31

6 Complex Numbers 39

7 Polynomial Equations 51

8 Induction 61

9 Euler's Formula and Platonic Solids 77

10 The Integers 87

11 Prime Factorization 95

12 More on Prime Numbers 103

13 Congruence of Integers 107

14 More on Congruence 117

15 Secret Codes 127

16 Counting and Choosing 133

17 More on Sets 147

18 Equivalence Relations 157

19 Functions 163

20 Permutations 173

21 Infinity 189

22 Introduction to Analysis: Bounds 199

23 More Analysis: Limits 207

24 Yet More Analysis: Continuity 217

25 Introduction to Abstract Algebra: Groups 225

26 Introduction to Abstract Algebra: More on Groups 235

Solutions to Odd-Numbered Exercises 255

Further Reading 293

Index of Symbols 295

Index 297

Foreword

One of the great difficulties in teaching undergraduate mathematics at universities in the United States is the great gap between teaching students a set of algorithms (which is very often the bulk of what is learned in calculus) and convincing students of the power, beauty and fun of the basic concepts in mathematics.

Martin Liebeck's book, *A Concise Introduction to Pure Mathematics, Fourth Edition*, is one of the best I have seen at filling this gap. In addition to preparing students to go on into mathematics, it is also a wonderful choice for a student who will not necessarily go on in mathematics but wants a gentle but fascinating introduction into the culture of mathematics. Liebeck starts with the basics and introduces number systems. In particular he discusses the real numbers and complex numbers. He shows how these concepts are natural and important in solving natural problems. Various topics in analysis, geometry, number theory and combinatorics are introduced and are shown to be fun and beautiful. Starting from scratch, Liebeck develops interesting results which hopefully will intrigue the student and give encouragement to continue to study mathematics.

This book will give a student the understanding to go on to further courses in abstract algebra and analysis. The notion of a proof will no longer be foreign, but also mathematics will not be viewed as some abstract black box. At the very least, the student will have an appreciation of mathematics.

As usual, Liebeck's writing style is clear and easy to read. This is a book that could be read by a student on his or her own. There is a wide selection of problems ranging from routine to quite challenging.

While there is a difference in mathematical education between the U.K. and the U.S., this book will serve both groups of students extremely well.

Professor Robert Guralnick
Chair of Mathematics Department
University of Southern California
Los Angeles, California

Preface

I can well remember my first lecture as a mathematics undergraduate, back in the olden days. In it, we were told about something called "Russell's Paradox" — does the set consisting of all sets which do not belong to themselves belong to itself? — after which the lecturer gave us some rules called the "Axioms of Set Theory." I came out of the lecture somewhat baffled. The second lecture, in which we were informed that "a_n tends to l if, for every $\varepsilon > 0$, there exists N such that for all $n \geq N$, $|a_n - l| < \varepsilon$," was also a touch bewildering. In fact, the lecturers were pretty good, and bafflement and bewilderment eventually gave way to understanding, but nevertheless it was a fairly fierce introduction to the world of university pure mathematics.

Nowadays we university lecturers are less fierce, and mathematics courses tend to start with a much gentler introduction to pure mathematics. I gave such a course at Imperial College for several years to students in the first term of the first year of their degree (generally in mathematics, or some joint degree including mathematics). This book grew out of that course. As well as being designed for use in a first university course, the book is also suitable for self-study. It could, for example, be read by students between school and university, or indeed by anybody with a reasonable background in school mathematics.

One of my aims is to provide a robust bridge between school and university mathematics. For a number of the topics covered, students may well have studied some of the basic material on this topic at school, but this book will generally take the topic much further, in a way that is interesting and stimulating (at least to me). For example, many will have come across the method of mathematical induction, and used it to solve some simple problems, like finding a formula for the sum $1+2+3+\ldots+n$. But I doubt that many have seen how induction can be used to study solid objects whose faces all have straight edges, and to show that the only so-called regular solids are the famous five "Platonic solids" (the cube, tetrahedron, octahedron, icosahedron and dodecahedron), as is done in Chapter 9.

I generally enjoy things more if they come in bite-sized pieces, and accordingly I have divided the book into 26 short chapters. Each chapter ends with

a selection of exercises, ranging from routine calculations to some quite challenging problems.

When starting to study pure mathematics at university, students often have a refreshing sense of "beginning all over again." Basic structures, like the real numbers, the integers, the rational numbers and the complex numbers, must be defined and studied from scratch, and even simple and obvious-looking statements about them must be proved properly. For example, it probably seems obvious that if n is an integer (i.e., one of the whole numbers $0, 1, -1, 2, -2, 3, -3$ and so on), and n^2 is odd, then n must also be odd. But how can we write down a rigorous proof of this fact? Methods for writing down proofs of this and many other simple facts form one of the themes of Chapter 1, along with a basic introduction to the language of sets.

In Chapter 2, I define and begin to study three of the basic number systems referred to in the previous paragraph: the real numbers (which we start off by thinking of as points on an infinite straight line — the "real line"); the integers; and the rational numbers (which are the fractions $\frac{m}{n}$, where m and n are integers). It takes some effort to prove that there is at least one real number that is not rational — a so-called irrational number — but once this is done, one can see quite easily that there are many irrational numbers. Indeed, by Chapter 21 we shall understand the strange fact that, in a very precise sense, there are "more" irrational numbers than rational numbers (even though there are infinitely many of each).

In studying properties of the system of real numbers, it is sometimes helpful to have ways of thinking of them that are different from just "points on the real line." In Chapter 3, I introduce the familiar decimal notation for real numbers, which provides a visual way of writing them down and can be useful in their general study. Chapters 4 and 5 carry on with our basic study of the real numbers.

In Chapter 6, I bring our last important number system into the action — the complex numbers. Students may well have met these before. We begin by introducing a symbol i, and defining $i^2 = -1$. A general complex number is a symbol of the form $a + bi$, where a and b are real numbers. We soon find that using complex numbers we can write down solutions of all quadratic equations, and then proceed to study other equations like $x^n = 1$. We also find some beautiful links between complex numbers and geometry in the plane. Chapter 7 takes the theory of equations much further. Solving quadratics is probably very familiar, but much less well known is the method for solving cubic equations given in this chapter. We then look at general polynomial equations (i.e., equations of the form $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$) and explore the amazing fact that every such equation has solutions which are complex numbers (known as the Fundamental Theorem of Algebra).

I have already mentioned the method of proof by mathematical induction, which is introduced in Chapter 8. This is a technique for proving statements

involving a general positive integer n, such as "the sum of the first n odd positive integers is equal to n^2," or "the number of regions formed by n straight lines drawn in the plane, no two parallel and no three going through the same point, is equal to $\frac{1}{2}(n^2+n+2)$." The method of induction is actually rather more powerful than first meets the eye, and Chapter 9 is devoted to the proof by induction of an elegant result, known as Euler's formula, about the relationship between the numbers of corners, edges and faces of a solid object, whose faces all have straight edges. Euler's formula has all sorts of uses. For example, if you want to make a football by sewing together hexagonal and pentagonal pieces of leather, in such a way that each corner lies on three edges, then the formula implies that you will need exactly 12 pentagonal pieces, no more and no less. I could not resist going further in this chapter and showing how to use Euler's formula to study the famous Platonic solids mentioned earlier.

Chapters 10 through 14 are all about possibly the most fascinating number system of all: the integers. Students will know what a prime number is — an integer greater than 1 that is only divisible by 1 and itself — and are quite likely aware of the fact that every integer greater than 1 is equal to a product of prime numbers, although this fact requires a careful proof. Much more subtle is the fact that such a prime factorization is unique — in other words, given an integer greater than 1, we can express it as a product of prime numbers in only one way. "Big deal! So what?" I hear you say. Well, yes, it is a big deal (so big that this result has acquired the grandiose title of "The Fundamental Theorem of Arithmetic"), and after proving it I try to show its significance by using it in the study of a number of problems; for instance, apart from 1 and 0, are there any squares that differ from a cube by just 1?

Chapter 15 contains an amazing application of some of the theory of prime numbers developed in the previous chapters. This application concerns some very clever secret codes that are used every day for the secure electronic transmission of sensitive information — one of today's most spectacular "real-world" applications of pure mathematics.

Chapter 16 is about methods of counting things. For example, suppose I have given the same lecture course for the last 16 years, and tell 3 jokes each year. I never tell the same set of 3 jokes twice. At least how many jokes do I know? To solve this and other important counting problems, we introduce binomial coefficients, which leads us into the binomial and multinomial theorems.

After a little formal theory of sets and relations in Chapters 17 and 18, I introduce functions in Chapter 19, and develop some of the delights of the theory of an especially interesting and important class of functions called "permutations" in Chapter 20. Then comes Chapter 21, in which I address some fascinating questions about infinite sets. When can we say that two infinite sets have the same "size"? Can we ever say that one infinite set has bigger "size" than another? These questions are answered in a precise and rigorous

way, and some of the answers may appear strange at first sight; for example, the set of all integers and the set of all rational numbers have the same size, but the set of all real numbers has greater size than these. Chapter 21 closes with a beautifully subtle result that tells us that an infinite set always has smaller size than the set of all its subsets. The proof of this is based on the argument of Russell's Paradox — which brings me back to where I started ....

The next three chapters have a somewhat different flavour to the rest of the book. In them I introduce a topic known as mathematical analysis, which is the study of the real numbers and functions defined on them. Of course I can't cover very much of the subject — that would require several more books — but I do enough to prove several interesting results and to fill in one or two gaps in the preceding chapters. The point is that with our somewhat naive understanding of the real numbers up to here, it is difficult to see how to prove even such basic properties as the fact that every positive real number has a square root, a cube root and so on. The material in Chapters 22–24 is sufficient at least to prove this fact, and also to do some other interesting things, such as proving a special case of the famous Fundamental Theorem of Algebra.

In the final two chapters of the book I introduce another very different kind of mathematics — the theory of groups, which is part of a huge area known as abstract algebra. Groups are defined as sets of objects (they could be numbers, or functions, or anything really), together with a rule for combining any two objects to get another one, and this rule is subject to four clearly defined assumptions, called the "axioms" of group theory. The game is to see what one can deduce just using the axioms. Fortunately the subject is more than just a game, and there are many beautiful examples and applications.

Let me now offer some comments on designing a course based on the book. Crudely speaking, the book can be divided into six fairly independent sections, with the following "core" chapters:

Introduction to number systems: Chapters 1, 2, 3, 4, 5, 6, 8

Theory of the integers: Chapters 10, 11, 13, 14

Introduction to discrete mathematics: Chapters 16, 17, 19, 20

Functions, relations and countability: Chapters 18, 19, 21

Introduction to analysis: Chapters 22, 23, 24

Introduction to abstract algebra: Chapters 25, 26

One could design a one- or two-semester course in a number of ways. For example, if the emphasis is to be on discrete mathematics, the core chapters to use from the first section would be 1, 2 and 8, and all the other sections except the last two would be core; the last section on abstract algebra would also be a natural addition to such a course. On the other hand, if the course is intended to prepare students more for a future course in analysis, one should use all the

chapters in the first, fourth and fifth sections. Overall, I would recommend incorporating at least the first four sections into your course — it works well!

I would like to express my thanks to my late father, Dr. Hans Liebeck, who read the entire manuscripts of the first two editions and suggested many improvements, as well as saving me from a number of embarrassing errors. Sadly, I can no longer claim that any errors that remain are his responsibility. And, finally, I thank generations of students at Imperial who have sat through my lectures and have helped me to hone the course into the sleek monster that has grown into this book.

New Features of the Fourth Edition

This fourth edition contains several substantial additions to the third edition. First, I have included two new chapters at the end to serve as an introduction to the topic of abstract algebra. This is a big subject which is often introduced in a course of its own at the undergraduate level, but I believe it fits quite well into the framework of this book. For one thing, it is a topic that one can begin to read about from scratch, without needing to know too much other stuff; on the other hand, many of the examples and applications are closely connected with other parts of the book, particularly the chapters on number systems, prime numbers, congruence and permutations. It also gives an introduction to "abstract" reasoning in mathematics, where one is allowed only to use a set of axioms and nothing else, and often students find this a new and exciting challenge.

I have also added new material in a number of other chapters: on inequalities in Chapters 5 and 8; on counting methods in Chapter 16; and on the Inclusion–Exclusion Principle and Euler's ϕ-function in Chapter 17. There are also lots of new exercises, and, as in the previous edition, I have included solutions to the odd-numbered ones.

Chapter 1

Sets and Proofs

This chapter contains some introductory notions concerning the language of sets, and methods for writing proofs of mathematical statements.

Sets

We shall think of a *set* as simply a collection of objects, which are called the *elements* or *members* of the set. There are a number of ways of describing a set. Sometimes the most convenient way is to make a list of all the objects in the set and put curly brackets around the list. Thus, for example,

$\{1,3,5\}$ is the set consisting of the objects 1, 3 and 5.

$\{\text{Fred}, \text{dog}, 1.47\}$ is the set consisting of the objects Fred, dog and 1.47.

$\{1,\{2\}\}$ is the set consisting of two objects, one being the number 1 and the other being the set $\{2\}$.

Often, however, this is not a convenient way to describe our set. For example, the set consisting of all the people who live in Denmark is for most purposes best described by precisely this phrase (i.e., "the set of all people who live in Denmark"); it is unlikely to be useful to describe this set in list form $\{\text{Sven}, \text{Inge}, \text{Jesper}, \ldots\}$. As another example, the set of all real numbers whose square is less than 2 is neatly described by the notation

$$\{x \,|\, x \text{ a real number}, x^2 < 2\}.$$

(This is to be read: "the set of all x such that x is a real number and $x^2 < 2$." The symbol "|" is the "such that" part of the phrase.) Likewise,

$$\{x \,|\, x \text{ a real number}, x^2 - 2x + 1 = 0\}$$

denotes the set consisting of all real numbers x such that $x^2 - 2x + 1 = 0$.

As a convention, we define the *empty set* to be the set consisting of no objects at all, and denote the empty set by the symbol $\emptyset$.

If S is a set, and s is an element of S (i.e., an object that belongs to S), we write

$$s \in S$$

and say *s belongs to S*. If some other object t does not belong to S, we write

$$t \notin S.$$

For example,

$$1 \in \{1,3,5\} \text{ but } 2 \notin \{1,3,5\},$$

$$\text{if } S = \{x \,|\, x \text{ a real number}, 0 \leq x \leq 1\}, \text{ then } 1 \in S \text{ but Fred} \notin S,$$

$$\{2\} \in \{1,\{2\}\} \text{ but } 2 \notin \{1,\{2\}\},$$

$$1 \notin \emptyset.$$

Two sets are defined to be equal when they consist of exactly the same elements; for example,

$$\{1,3,5\} = \{3,5,1\} = \{1,5,1,3\},$$

$$\{x \,|\, x \text{ a real number}, x^2 - 2x + 1 = 0\} = \{1\},$$

$$\{x \,|\, x \text{ a real number}, x^2 + 1 = 0\} = \text{the set of female popes} = \emptyset.$$

We say a set T is a *subset* of a set S if every element of T also belongs to S (i.e., T consists of some of the elements of S). We write $T \subseteq S$ if T is a subset of S, and $T \not\subseteq S$ if not. For example, if $S = \{1,\{2\},\text{cat}\}$, then

$$\{\text{cat}\} \subseteq S, \;\; \{\{2\}\} \subseteq S, \;\; \{2\} \not\subseteq S.$$

As another example, the subsets of $\{1,2\}$ are

$$\{1,2\}, \{1\}, \{2\}, \emptyset.$$

(By convention, $\emptyset$ is a subset of every set.)

This is all we shall need about sets for the time being. This topic will be covered somewhat more formally in Chapter 17.

Proofs

Consider the following mathematical statements:

(1) The square of an odd integer is odd. (By an *integer* we mean a whole number, i.e., one of the numbers $\ldots, -2, -1, 0, 1, 2, \ldots$.)

(2) No real number has square equal to -1.

(3) Every positive integer is equal to the sum of two integer squares. (The integer squares are $0, 1, 4, 9, 16, 25$, and so on.)

Each of these statements is either true or false. Probably you have quickly formed an opinion on the truth or falsity of each, and regard this as "obvious" in some sense. Nevertheless, to be totally convincing, you must provide clear, logical proofs to justify your opinions.

To clarify what constitutes a proof, we need to introduce a little notation. If P and Q are statements, we write

$$P \Rightarrow Q$$

to mean that statement P implies statement Q. For example,

$x = 2 \Rightarrow x^2 < 6$,

it is raining $\Rightarrow$ the sky is cloudy.

Other ways of saying $P \Rightarrow Q$ are:

if P then Q (e.g., if $x = 2$ then $x^2 < 6$);

Q if P (e.g., the sky is cloudy if it is raining);

P only if Q (e.g., $x = 2$ only if $x^2 < 6$; it rains only if the sky is cloudy).

Notice that $P \Rightarrow Q$ does *not* mean that also $Q \Rightarrow P$; for example, $x^2 < 6 \not\Rightarrow x = 2$ (where $\not\Rightarrow$ means "does not imply"). However, for some statements P, Q, it *is* the case that both $P \Rightarrow Q$ and $Q \Rightarrow P$; in such a case we write $P \Leftrightarrow Q$, and say "P if and only if Q." For example,

$x = 2 \Leftrightarrow x^3 = 8$,

you are my wife if and only if I am your husband.

The *negation* of a statement P is the opposite statement, "not P," written as the symbol $\bar{P}$. Notice that if $P \Rightarrow Q$ then also $\bar{Q} \Rightarrow \bar{P}$ (since if $\bar{Q}$ is true then P cannot be true, as $P \Rightarrow Q$).

For example, if P is the statement $x = 2$ and Q the statement $x^2 < 6$, then $P \Rightarrow Q$ says "$x = 2 \Rightarrow x^2 < 6$," while $\bar{Q} \Rightarrow \bar{P}$ says "$x^2 \geq 6 \Rightarrow x \neq 2$." Likewise, for the other example above we have "the sky is not cloudy $\Rightarrow$ it is not raining."

Perhaps labouring the obvious, let us now make a list of the deductions that can be made from the implication "it is raining $\Rightarrow$ the sky is cloudy," given various assumptions:

Assumption	Deduction
it is raining	sky is cloudy
it is not raining	no deduction possible
sky is cloudy	no deduction possible
sky is not cloudy	it is not raining

Now let us put together some examples of proofs. In general, a proof will consist of a series of implications, proceeding from given assumptions, until the desired conclusion is reached. As we shall see, the logic behind a proof can take several different forms.

Example 1.1

Suppose we are given the following three facts:

(a) I will be admitted to Greatmath University only if I am clever.

(b) If I am clever then I do not have to work hard.

(c) I have to work hard.

What can be deduced?

Answer Write G for the statement "I will be admitted to Greatmath University," C for the statement "I am clever," and W for the statement "I have to work hard." Then (a) says $G \Rightarrow C$, and (b) says $C \Rightarrow \bar{W}$. Hence,

$$W \Rightarrow \bar{C} \quad \text{and} \quad \bar{C} \Rightarrow \bar{G}.$$

Since W is true by (c), we deduce that $\bar{G}$ is true, i.e., I will not be admitted to Greatmath University (thank goodness).

Example 1.2

In this example we prove statement (1) from the previous page: the square of an odd integer is odd.

PROOF Let n be an odd integer. Then n is 1 more than an even integer, so $n = 1 + 2m$ for some integer m. Therefore, $n^2 = (1 + 2m)^2 = 1 + 4m + 4m^2 = 1 + 4(m + m^2)$. This is 1 more than $4(m + m^2)$, an even number, hence n^2 is odd. ∎

Formally, we could have written this proof as the following series of implications:

$$n \text{ odd} \Rightarrow n = 1 + 2m \Rightarrow n^2 = 1 + 4(m + m^2) \Rightarrow n^2 \text{ odd}.$$

However, this is evidently somewhat terse, and such an approach with more complicated proofs quickly leads to unreadable mathematics; so, as in the above proof, we insert words of English to make the proof readable, including words like "hence," "therefore," "then" and so on, to take the place of implication symbols.

Note The above proof shows rather more than just the oddness of n^2: it shows that the square of an odd number is always 1 more than a multiple of 4, i.e., is of the form $1 + 4k$ for some integer k.

The proofs given for Examples 1.1 and 1.2 could be described as *direct* proofs in that they proceed from the given assumptions directly to the conclusion via a series of implications. We now discuss two other types of proof, both very commonly used.

The first is *proof by contradiction*. Suppose we wish to prove the truth of a statement P. A proof by contradiction would proceed by first assuming that P is false — in other words, assuming $\bar{P}$. We would try to deduce from this a statement Q that is palpably false (for example, Q could be the statement "$0 = 1$" or "Liebeck is the pope"). Having done this, we have shown

$$\bar{P} \Rightarrow Q.$$

Hence also $\bar{Q} \Rightarrow P$. Since we know Q is false, $\bar{Q}$ is true, and hence so is P, so we have proved P, as desired.

The next three examples illustrate the method of proof by contradiction.

Example 1.3

Let n be an integer such that n^2 is a multiple of 3. Then n is also a multiple of 3.

PROOF Suppose n is not a multiple of 3. Then when we divide n by 3, we get a remainder of either 1 or 2; in other words, n is either 1 or 2 more than a multiple of 3. If the remainder is 1, then $n = 1 + 3k$ for some integer k, so

$$n^2 = (1 + 3k)^2 = 1 + 6k + 9k^2 = 1 + 3\left(2k + 3k^2\right).$$

But this means that n^2 is 1 more than a multiple of 3, which is false, as we are given that n^2 is a multiple of 3. And if the remainder is 2, then $n = 2 + 3k$ for some integer k, so

$$n^2 = (2 + 3k)^2 = 4 + 12k + 9k^2 = 1 + 3\left(1 + 4k + 3k^2\right),$$

which is again false as n^2 is a multiple of 3.

Thus we have shown that assuming n is not a multiple of 3 leads to a false statement. Hence, as explained above, we have proved that n is a multiple of 3. ∎

Usually in a proof by contradiction, when we arrive at our false statement Q, we simply write something like "this is a contradiction" and stop. We do this in the next proof.

Example 1.4
No real number has square equal to -1.

PROOF Suppose the statement is false. This means that there *is* a real number, say x, such that $x^2 = -1$. However, it is a general fact about real numbers that the square of any real number is greater than or equal to 0 (see Chapter 5, Example 5.2). Hence $x^2 \geq 0$, which implies that $-1 \geq 0$. This is a contradiction. ∎

Example 1.5
Prove that $\sqrt{2}+\sqrt{6} < \sqrt{15}$.

PROOF Let me start by giving a non-proof:

$$\sqrt{2}+\sqrt{6} < \sqrt{15} \Rightarrow \left(\sqrt{2}+\sqrt{6}\right)^2 < 15$$
$$\Rightarrow 8+2\sqrt{12} < 15 \Rightarrow 2\sqrt{12} < 7 \Rightarrow 48 < 49.$$

The last statement $(48 < 49)$ is true, so why is this not a proof? Because the implication is going the wrong way — we have shown that if P is the statement we want to prove, and Q is the statement that $48 < 49$, then $P \Rightarrow Q$; but this tells us nothing about the truth or otherwise of P.

A cunning change to the above false proof gives a correct proof, by contradiction. So assume the result is false; i.e., assume that $\sqrt{2}+\sqrt{6} \geq \sqrt{15}$. Then

$$\sqrt{2}+\sqrt{6} \geq \sqrt{15} \Rightarrow \left(\sqrt{2}+\sqrt{6}\right)^2 \geq 15$$
$$\Rightarrow 8+2\sqrt{12} \geq 15 \Rightarrow 2\sqrt{12} \geq 7 \Rightarrow 48 \geq 49,$$

which is a contradiction. Hence we have proved that $\sqrt{2}+\sqrt{6} < \sqrt{15}$. ∎

The other method of proof we shall discuss is actually a way of proving statements are false — in other words, *disproving* them. We call the method *disproof by counterexample*. It is best explained by examples.

Example 1.6
Consider the following two statements:

(a) All men are Chinese.

(b) Every positive integer is equal to the sum of two integer squares.

As the reader will have cleverly spotted, both these statements are false. To disprove (a), we need to prove the negation, which is "not all men are Chinese," or equivalently, "there exists a man who is not Chinese"; this is readily done by simply displaying one man who is not Chinese — this man will then be a *counterexample* to statement (a). The point is that to disprove (a), we do not need to consider *all* men, we just need to produce a single counterexample.

Likewise, to disprove (b) we just need to provide a single counterexample — that is, a positive integer that is *not* equal to the sum of two squares. The number 3 fits the bill nicely.

Quantifiers

I will conclude the chapter by slightly formalising some of the discussion we have already had about proofs.

Consider the following statements:

(1) There is an integer n such that $n^3 = -27$.

(2) For some integer x, $x^2 = -1$.

(3) There exists a positive integer that is not equal to the sum of three integer squares.

Each of these statements has the form: "there exists some integer with a certain property." This type of statement is so common in mathematics that we represent the phrase "there exists" by a special symbol, namely $\exists$. So, writing $\mathbb{Z}$ for the set of all integers, the above statements can be rewritten as follows:

(1) $\exists n \in \mathbb{Z}$ such that $n^3 = -27$.

(2) $\exists x \in \mathbb{Z}$ such that $x^2 = -1$.

(3) $\exists x \in \mathbb{Z}$ such that x is positive and is not equal to the sum of three integer squares.

The symbol $\exists$ is called the *existential quantifier*. To prove that an existence statement is true, it is enough to find just one object satisfying the required property. So (1) is true, since $n = -3$ has the required property; and (3) is true since $x = 7$ is not the sum of three squares (of course there are many other values of x having this property, but only one value is required to demonstrate the truth of (3)).

Now consider the following statements:

(4) For all integers n, $n^2 \geq 0$.

(5) The cube of any integer is positive.

(6) Every integer is equal to the difference of two positive integers.

All these statements are of the form: "for all integers, a certain property is true." Again, this type of statement is very common in mathematics, and we represent the phrase "for all" by a special symbol, namely $\forall$. So the above statements can be rewritten as follows:

(4) $\forall n \in \mathbb{Z}$, $n^2 \geq 0$.

(5) $\forall n \in \mathbb{Z}$, $n^3 > 0$.

(6) $\forall x \in \mathbb{Z}$, x is equal to the difference of two positive integers.

The symbol $\forall$ is called the *universal quantifier*. To show that a "for all" statement is true, a general argument is required; to show it is false, a single counterexample is all that is needed (this is just proof by counterexample, discussed in the previous section). I will leave you to show that (4) and (6) are true, while (5) is false.

Many mathematical statements involve more than one quantifier. For example, statement (6) above can be rewritten as

(6) $\forall x \in \mathbb{Z}$, $\exists m, n \in \mathbb{Z}$ such that $m > 0, n > 0$ and $x = m - n$.

Here's another example: the statement "for any integer a, there is an integer b such that $a + b = 0$" can be rewritten as "$\forall a \in \mathbb{Z}, \exists b \in \mathbb{Z}$ such that $a + b = 0$." Notice that the order of quantifiers is important: the statement "$\exists b \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}$, $a + b = 0$" means something quite different.

Let's finish by seeing how to find the negation of a statement involving quantifiers. Consider statement (1) above: $\exists n \in \mathbb{Z}$ such that $n^3 = -27$. The negation of this is the statement "there does not exist an integer n such that $n^3 = -27$" — in other words, "every integer has cube not equal to -27," or more succinctly, "$\forall n \in \mathbb{Z}$, $n^3 \neq -27$." So to form the negation of the original statement,

we have changed $\exists$ to $\forall$ and negated the conclusion (i.e., changed $n^3 = -27$ to $n^3 \neq -27$).

Now consider statement (5): $\forall n \in \mathbb{Z}$, $n^3 > 0$. The negation of this is "not all integers have a positive cube" — in other words, "there is an integer having a non-positive cube," or more succinctly, "$\exists n \in \mathbb{Z}$ such that $n^3 \leq 0$." This time, to form the negation we have replaced $\forall$ by $\exists$ and negated the conclusion.

To summarise: when forming the negation of a statement involving quantifiers, we change $\exists$ to $\forall$, change $\forall$ to $\exists$ and negate the conclusion.

Let's do another example, and negate the following statement:

(7) For any integers x and y, there is an integer z such that $x^2 + y^2 = z^2$.

We can rewrite this as: $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}$, $\exists z \in \mathbb{Z}$ such that $x^2 + y^2 = z^2$. Hence the negation is

$$\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, \text{ such that } \forall z \in \mathbb{Z},\ x^2 + y^2 \neq z^2.$$

In other words: there exist integers x, y such that for all integers z, $x^2 + y^2 \neq z^2$. I'm sure you can pretty quickly decide whether (7) or its negation is true.

Finally, let me make an observation for you to be wary of or amused by (or both). Here are a couple of strange statements involving the empty set:

(8) $\forall a \in \{x \,|\, x \text{ a real number}, x^2 + 1 = 0\}$, we have $a^{17} - 72a^{12} + 39 = 0$.

(9) $\exists b \in \{x \,|\, x \text{ a real number}, x^2 + 1 = 0\}$ such that $b^2 \geq 0$.

You will have noticed that the set $\{x \,|\, x \text{ a real number}, x^2 + 1 = 0\}$ is equal to the empty set. Hence the statement in (8) says that all elements of the empty set have a certain property; this is true, since there are no elements in the empty set! Likewise, any similar "for all" statement involving the empty set is true. On the other hand, the statement (9) says that there exists an element of the empty set with a certain property; this must be false, since there are no elements in the empty set.

Exercises for Chapter 1

1. Let A be the set $\{\alpha, \{1, \alpha\}, \{3\}, \{\{1,3\}\}, 3\}$. Which of the following statements are true and which are false?

   (a) $\alpha \in A$.
   (b) $\{\alpha\} \notin A$.
   (c) $\{1, \alpha\} \subseteq A$.
   (d) $\{3, \{3\}\} \subseteq A$.
   (e) $\{1,3\} \in A$.
   (f) $\{\{1,3\}\} \subseteq A$.
   (g) $\{\{1, \alpha\}\} \subseteq A$.
   (h) $\{1, \alpha\} \notin A$.
   (i) $\emptyset \subseteq A$.

2. Let B, C, D, E be the following sets:

$$B = \{x \mid x \text{ a real number}, x^2 < 4\},$$

$$C = \{x \mid x \text{ a real number}, 0 \leq x < 2\},$$

$$D = \{x \mid x \in \mathbb{Z}, x^2 < 1\},$$

$$E = \{1\}.$$

   (a) Which pair of these sets has the property that neither is contained in the other?

   (b) You are given that X is one of the sets B, C, D, E, but you do not know which one. You are also given that $E \subseteq X$ and $X \subseteq B$. What can you deduce about X?

3. Which of the following arguments are valid? For the valid ones, write down the argument symbolically.

   (a) I eat chocolate if I am depressed. I am not depressed. Therefore I am not eating chocolate.

   (b) I eat chocolate only if I am depressed. I am not depressed. Therefore I am not eating chocolate.

   (c) If a movie is not worth seeing, then it was not made in England. A movie is worth seeing only if critic Ivor Smallbrain reviews it. The movie *Cat on a Hot Tin Proof* was not reviewed by Ivor Smallbrain. Therefore *Cat on a Hot Tin Proof* was not made in England.

4. A and B are two statements. Which of the following statements about A and B implies one or more of the other statements?

   (a) Either A is true or B is true.

   (b) $A \Rightarrow B$.

   (c) $B \Rightarrow A$.

   (d) $\bar{A} \Rightarrow B$.

   (e) $\bar{B} \Rightarrow A$.

5. Which of the following statements are true, and which are false?

   (a) $n = 3$ only if $n^2 - 2n - 3 = 0$.

   (b) $n^2 - 2n - 3 = 0$ only if $n = 3$.

   (c) If $n^2 - 2n - 3 = 0$ then $n = 3$.

   (d) For integers a and b, ab is a square only if both a and b are squares.

   (e) For integers a and b, ab is a square if both a and b are squares.

6. Write down careful proofs of the following statements:
   (a) $\sqrt{6}-\sqrt{2}>1$.
   (b) If n is an integer such that n^2 is even, then n is even.
   (c) If $n=m^3-m$ for some integer m, then n is a multiple of 6.

7. Disprove the following statements:
   (a) If n and k are positive integers, then n^k-n is always divisible by k.
   (b) Every positive integer is the sum of three squares (the squares being 0, 1, 4, 9, 16, etc.).

8. Given that the number 8881 is not a prime number, prove that it has a prime factor that is at most 89. (*Hint: Don't try to factorize 8881! Try to be a bit more clever and prove it by contradiction.*)

9. In this question I am assuming you know what a prime number is; if not, take a look at the definition on page 69.

   For each of the following statements, form its negation and either prove that the statement is true or prove that its negation is true:
   (a) $\forall n\in\mathbb{Z}$ such that n is a prime number, n is odd.
   (b) $\forall n\in\mathbb{Z}$, $\exists a,b,c,d,e,f,g,h\in\mathbb{Z}$ such that
   $$n=a^3+b^3+c^3+d^3+e^3+f^3+g^3+h^3.$$
   (c) $\exists x\in\mathbb{Z}$ such that $\forall n\in\mathbb{Z}$, $x\neq n^2+2$.
   (d) $\exists x\in\mathbb{Z}$ such that $\forall n\in\mathbb{Z}$, $x\neq n+2$.
   (e) $\forall y\in\{x\,|\,x\in\mathbb{Z},x\geq 1\}$, $5y^2+5y+1$ is a prime number.
   (f) $\forall y\in\{x\,|\,x\in\mathbb{Z},x^2<0\}$, $5y^2+5y+1$ is a prime number.

10. Prove by contradiction that a real number that is less than every positive real number cannot be positive.

11. Critic Ivor Smallbrain (see Exercise 3(c)) has been keeping a careful account of the number of chocolate bars he has eaten during film screenings over his career. For each positive integer n he denotes by a_n the total number of bars he consumed during the first n films. One evening, during a screening of the Christmas epic *It's a Wonderful Proof*, he notices that the sequence $a_1,a_2,a_3,\ldots,a_n,\ldots$ obeys the following rules for all $n\geq 1$:
   $$a_{n+1}>a_n, \text{ and } a_{a_n}=3n.$$
   Also $a_1>0$.

(a) Find a_1. (*Hint:* Let $x = a_1$. Then what is a_x?)

(b) Find $a_2, a_3, \ldots, a_9$.

(c) Find a_{100}.

(d) Investigate the sequence $a_1, a_2, \ldots, a_n, \ldots$ further.

Chapter 2

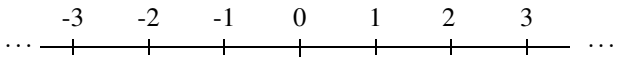
Number Systems

In this chapter we introduce three number systems: the real numbers, the integers and the rationals.

The Real Numbers

Here is an infinite straight line:

Choose a point on this line and label it as 0. Also choose a unit of length, and use it to mark off evenly spaced points on the line, labelled by the whole numbers $\ldots, -2, -1, 0, 1, 2, \ldots$ like this:



We shall think of the real numbers as the points on this line. Viewed in this way, the line is called the *real line.* Write $\mathbb{R}$ for the set of all real numbers.

The real numbers have a natural *ordering,* which we now describe. If x and y are real numbers, we write $x < y$, or equivalently $y > x$, if x is to the left of y on the real line; under these circumstances we say x is less than y, or y is greater than x. Also, $x \leq y$ indicates that x is less than or equal to y. Thus, the following statements are all true: $1 \leq 1$, $1 \geq 1$, $1 < 2$, $2 \geq 1$. A real number x is *positive* if $x > 0$ and is *negative* if $x < 0$.

The *integers* are the whole numbers, marked as above on the real line. We write $\mathbb{Z}$ for the set of all integers and $\mathbb{N}$ for the set of all positive integers $\{1, 2, 3, \ldots\}$. Positive integers are sometimes called *natural numbers.*

Fractions $\frac{m}{n}$ can also be marked on the real line. For example, $\frac{1}{2}$ is placed halfway between 0 and 1; in general, $\frac{m}{n}$ can be marked by dividing each of the unit intervals into n equal sections and counting m of these sections away from 0. A real number of the form $\frac{m}{n}$ (where m,n are integers) is called a *rational number*. We write $\mathbb{Q}$ for the set of all rational numbers.

There are of course many different fractions representing the same rational number: for example, $\frac{8}{12} = \frac{-6}{-9} = \frac{2}{3}$, and so on. We say the rational $\frac{m}{n}$ is in *lowest terms* if no cancelling is possible — that is, if m and n have no common factors (apart from 1 and -1).

Rationals can be added and multiplied according to the familiar rules:

$$\frac{m}{n} + \frac{p}{q} = \frac{mq+np}{nq}, \quad \frac{m}{n} \times \frac{p}{q} = \frac{mp}{nq}.$$

Notice that the sum and product of two rationals is again rational.

In fact, addition and multiplication of arbitrary real numbers can be defined in such a way as to obey the following rules:

RULES 2.1 *For all* $a,b,c, \in \mathbb{R}$,
(1) $a+b=b+a$ *and* $ab=ba$
(2) $a+(b+c)=(a+b)+c$ *and* $a(bc)=(ab)c$
(3) $a(b+c)=ab+ac$.

For example, (2) assures us that $(2+5)+(-3)=2+(5+(-3))$ (i.e., $7-3=2+2$), and $(2\times 5)\times(-3)=2\times(5\times(-3))$ (i.e., $10\times(-3)=2\times(-15)$).

Before proceeding, let us pause briefly to reflect on these rules. They may seem "obvious" in some sense, in that you have probably been assuming them for years without thinking. But ponder the following equation, to be solved for x:

$$x+3=5.$$

What are the steps we carry out when we solve this equation? Here they are:
Step 1. Add -3 to both sides: $(x+3)+(-3)=5+(-3)$.
Step 2. Apply rule (2): $x+(3+(-3))=5-3$.
Step 3. This gives $x+0=5-3$, hence $x=2$.
The point is that without rule (2) we would be stuck. (Indeed, there are strange systems of objects with an addition for which one does not have rule (2), and in such systems one cannot even solve simple equations like the one above.)

There are some further important rules obeyed by the real numbers, relating to the ordering described above. We postpone discussion of these until Chapter 5.

Rationals and Irrationals

We often call a rational number simply a rational. The next result shows that the rationals are densely packed on the real line.

PROPOSITION 2.1
Between any two rationals there is another rational.

PROOF Let r and s be two different rationals. Say r is the larger, so $r > s$. We claim that the real number $\frac{1}{2}(r+s)$ is a rational lying between r and s. To see this, observe that $\frac{1}{2}r > \frac{1}{2}s \Rightarrow \frac{1}{2}r + \frac{1}{2}s > \frac{1}{2}s + \frac{1}{2}s \Rightarrow \frac{1}{2}(r+s) > s$, and likewise $\frac{1}{2}r > \frac{1}{2}s \Rightarrow \frac{1}{2}r + \frac{1}{2}r > \frac{1}{2}s + \frac{1}{2}r \Rightarrow r > \frac{1}{2}(r+s)$. Thus, $\frac{1}{2}(r+s)$ lies between r and s. Finally, it is rational, since if $r = \frac{m}{n}, s = \frac{p}{q}$, then $\frac{1}{2}(r+s) = \frac{mq+np}{2nq}$. ∎

Despite its innocent statement and quick proof, this is a rather significant result. For example, it implies that in contrast to the integers, there is no smallest positive rational, since for any positive rational x there is a smaller positive rational (for example, $\frac{1}{2}x$); likewise, given any rational, there is no "next rational up." The proposition also shows that the rationals cannot be represented completely by "dots" on the real line, since between any two dots there would have to be another dot.

The proposition also raises a profound question: OK, the rationals are dense on the real line; but do they in fact fill out the whole line? In other words, is every real number a rational?

The answer is no, as we shall now demonstrate. First we need the following proposition, which is not quite as obvious as it looks.

PROPOSITION 2.2
There is a real number α such that $\alpha^2 = 2$.

PROOF Draw a square of side 1: