Numbers, Groups and Codes

Second Edition

Numbers, Groups and Codes

Second Edition

J. F. HUMPHREYS
Senior Fellow in Mathematics, University of Liverpool

M. Y. PREST
Professor of Mathematics, University of Manchester

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9780521540506

First published 2004
8th printing 2013

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

ISBN 978-0-521-54050-6 Paperback

To Sarah, Katherine and Christopher *J. F. Humphreys*
To the memory of my parents *M. Y. Prest*

Contents

Preface to first edition

This book arose out of a one-semester course taught over a number of years both at the University of Notre Dame, Indiana, and at the University of Liverpool. The aim of the course is to introduce the concepts of algebra, especially group theory, by many examples and to relate them to some applications, particularly in computer science. The books which we considered for the course seemed to fall into two categories. Some were too elementary, proceeded at too slow a pace and had far from adequate coverage of the topics we wished to include. Others were aimed at a higher level and were more comprehensive, but had correspondingly skimpy presentation of the material. Since we could find no text which presented the material at the right level and in a way we felt appropriate, we prepared our own course notes: this book is the result. We have added some topics which are not always treated in order to increase the flexibility of the book as the basis for a course. The material in the book could be covered at an unhurried pace in about 48 lectures; alternatively, a 36-hour unit could be taught, covering Chapters 1, 2 (not Section 2.4), 4 and 5.

Preface to second edition

We have prepared this second edition bearing in mind the fact that students studying mathematics at university, at least in the UK, are less well prepared than in the past. We have taken more time to explain some points and, in particular, we have not assumed that students are comfortable reading formal statements of theorems and making sense of their proofs. Especially in the first chapter, we have added many comments designed to help the reader make sense of theorems and proofs. The more 'mathematically sophisticated' reader may, of course, read quickly through these comments. We have also added a few more straightforward exercises at the ends of some sections.

Two major changes in content have been made. In Chapter 3 we have removed material (some propositional logic, Boolean algebras and Karnaugh maps) around Boolean algebras. We have retained most of the material on propositional logic, added a section designed to help students deal with quantifiers and added a further section on proof strategies. The emphasis of this chapter is now on the use of logic within mathematics rather than on the Boolean structure behind propositional logic.

The second major change has been the inclusion of a new chapter, Chapter 6, on the algebra of polynomials. We emphasise the similarity with the arithmetic of integers, including the usefulness of the notion of congruence class, and we show how polynomials are used in constructing cyclic codes.

Introduction

'A group is a set endowed with a specified binary operation which is associative and for which there exist an identity element and inverses.' This, in effect, is how many books on group theory begin. Yet this tells us little about groups or why we should study them. In fact, the concept of a group evolved from examples in number theory, algebra and geometry and it has applications in many contexts. Our presentation of group theory in this book reflects to some extent the historical development of the subject. Indeed, the formal definition of an abstract group does not occur until the fourth chapter. We believe that, apart from being more 'honest' than the usual presentation, this approach has definite pedagogic advantages. In particular, the student is not presented with a seemingly unmotivated abstract definition but, rather, sees the sense of the definition in terms of the previously introduced special cases. Moreover, the student will realise that these concepts, which may be so glibly presented, actually evolved slowly over a period of time.

The choice of topics in the book is motivated by the wish to provide a sound, rigorous and historically based introduction to group theory. In the sense that complete proofs are given of the results, we do not depart from tradition. We have, however, tried to avoid the dryness frequently associated with a rigorous approach. We believe that by the overall organisation, the style of presentation and our frequent reference to less traditional topics we have been able to overcome this problem. In pursuit of this aim we have included many examples and have emphasised the historical development of the ideas, both to motivate and to illustrate. The choice of applications is directed more towards 'finite mathematics' and computer science than towards applications arising out of the natural sciences.

Group theory is the central topic of the book but the formal definition of a group does not appear until the fourth chapter, by which time the reader will

have had considerable practice in 'group theory'. Thus we are able to present the idea of a group as a concept that unifies many ideas and examples which the reader already will have met.

One of the objectives of the book is to enable the reader to relate disparate branches of mathematics through 'structure' (in this case group theory) and hence to recognise patterns in mathematical objects. Another objective of the book is to provide the reader with a large number of skills to acquire, such as solving linear congruences, calculating the sign of a permutation and correcting binary codes. The mastery of straightforward clearly defined tasks provides a motivation to understand theorems and also reveals patterns. The text has many worked examples and contains straightforward exercises (as well as more interesting ones) to help the student build this confidence and acquire these skills.

The first chapter of the book gives an account of elementary number theory, with emphasis on the additive and multiplicative properties of sets of congruence classes. In Chapter 2 we introduce the fundamental notions of sets, functions and relations, treating formally ideas that we have already used in an informal way. These fundamental concepts recur throughout the book. We also include a section on finite state machines. Chapter 3 is an introduction to the logic of mathematical reasoning, beginning with a detailed discussion of propositional logic. Then we discuss the use of quantifiers and we also give an overview of some proof strategies. The later chapters do not formally depend on this one. Chapter 4 is the central chapter of the book. We begin with a discussion of permutations as yet another motivation for group theory. The definition of a group is followed by many examples drawn from a variety of areas of mathematics. The elementary theory of groups is presented in Chapter 5, leading up to Lagrange's Theorem and the classification of groups of small order. At the end of Chapter 5, we describe applications to error-detecting and error-correcting codes. Chapter 6 introduces the arithmetic of polynomials, in particular the division algorithm and various results analogous to those in Chapter 1. These ideas are applied in the final section, which depends on Chapter 5, to the construction of cyclic codes.

Every section contains many worked examples and closes with a set of exercises. Some of these are routine, designed to allow the reader to test his or her understanding of the basic ideas and methods; others are more challenging and point the way to further developments.

The dependences between chapters are mostly in terms of examples drawn from earlier material and the development of certain ideas. The main dependences are that Chapter 5 requires Chapter 1 and the early part of Section 4.3

and, also, the examples in Section 4.3 draw on some of Chapter 1 (as well as Sections 4.1 and 4.2).

The material on group theory could be introduced at an early stage but this would not be in the spirit of the book, which emphasises the development of the concept. The formal material of the book could probably be presented in a book of considerably shorter length. We have adopted a more leisurely presentation in the interests of motivation and widening the potential readership.

We have tried to cater for a wide range in ability and degree of preparation in students. We hope that the less well prepared student will find that our exposition is sufficiently clear and detailed. A diligent reader will acquire a sound basic knowledge of a branch of mathematics which is fundamental to many later developments in mathematics. All students should find extra interest and motivation in our relatively historical approach. The better prepared student also should derive long-term benefit from the widening of the material, will discover many challenging exercises and will perhaps be tempted to develop a number of points that we just touch upon. To assist the student who wishes to learn more about a topic, we have made some recommendations for further reading.

Changes in teaching and examining mathematics in secondary schools in the UK have resulted in first-year students of mathematics having rather different skills than in the past. We believe that our approach is well suited to such students. We do not assume a great deal of background yet we do not expect the reader to be an uncritical and passive consumer of information.

One last word: in our examples and exercises we touch on a variety of further developments (for example, normal subgroups and homomorphisms) that could, with a little supplementary material, be introduced explicitly.

Advice to the reader

Mathematics cannot be learned well in a passive way. When you read this book, have paper and pen(cil) to hand: there are bound to be places where you cannot see all the details in your head, so be prepared to stop reading and start writing. Ideally, you should proceed as follows. When you come to the statement of a theorem, pause before reading the proof: do you find the statement of the result plausible? If not, why not? (try to disprove it). If so, then why is it true? How would you set about showing that it is true? Write down a sketch proof if you can: now try to turn that into a detailed proof. Then read the proof we give.

Exercises The exercises at the end of each section are not arranged in order of difficulty, but loosely follow the order of presentation of the topics. It is essential that you should attempt a good portion of these.

Understanding the proofs of the results in this book is very important but so also is doing the exercises. The second-best way to check that you understand a topic is to attempt the exercises. (The best way is to try to explain it to someone else.) It may be quite easy to convince yourself that you understand the material: but attempting the relevant exercises may well expose weak points in your comprehension. You should find that wrestling with the exercises, particularly the more difficult ones, helps you to develop your understanding. You should also find that exercises and proofs illuminate each other.

Proofs Although the emphasis of this text is on examples and applications, we have included proofs of almost all the results that we use. Since students often find difficulty with formal proofs, we will now discuss these at some length. Attitudes towards the need for proofs in mathematics have changed over the centuries.

The first mathematics was concerned with computations using particular numbers, and so the question of proof, as opposed to correctness of a

computation, never arose. Later, however, in arithmetic and geometry, people saw patterns and relationships that appeared to hold irrespective of the particular numbers or dimensions involved, so they began to make general assertions about numbers and geometrical figures. But then a problem arose: how may one be certain of the truth of a general assertion? One may make a general statement, say about numbers, and check that it is true for various particular cases, but this does not imply that it is always true.

To illustrate. You may already have been told that every positive integer greater than 1 is a product of primes, for instance $12 = 2 \cdot 2 \cdot 3$, $35 = 5 \cdot 7$, and so on. But since there are infinitely many positive integers it is impossible, by considering each number in turn, to check the truth of the assertion for every positive integer. So we have the assertion: 'every positive integer greater than 1 is a product of primes'. The evidence of particular examples backs up this assertion, but how can we be justifiably certain that it is true?

Well, we may give a proof of the assertion. A proof is a sequence of logically justified steps which takes us from what we already know to be true to what we suspect (and, after a proof has been found, know) to be true.

It is unreasonable to expect to conjure something from nothing, so we do need to make some assumptions to begin with (and we should also be clear about what we mean by a valid logical deduction). In the case of the assertion above, all we need to assume are the ordinary arithmetic properties of the integers, and the principle of induction (see Section 1.2 for the latter). It is also necessary to have defined precisely the terms that we use, so we need a clear definition of what is meant by 'prime'. We may then build on these foundations and construct a proof of the assertion. (We give one on p. 28.)

It should be understood that current mathematics employs a very rigorous standard of what constitutes a valid proof. Certainly what passed for a proof in earlier centuries would often not stand up to present-day criteria. There are many good reasons for employing such strict criteria but there are some drawbacks, particularly for the student.
A formal proof is something that is constructed 'after the event'. When a mathematician proves a result he or she will almost certainly have some 'picture' of what is going on. This 'picture' may have suggested the result in the first place and probably guided attempts to find a proof. In writing down a formal proof, however, it often is the case that the original insight is lost, or at least becomes embedded in an obscuring mass of detail.

Therefore one should not try to read proofs in a naive way. Some proofs are merely verifications in which one 'follows one's nose', but you will probably be able to recognise such a proof when you come across one and find no great

trouble with it – provided that you have the relevant definitions clear in your mind and have understood what is being assumed and what is to be proved. But there are other proofs where you may find that, even if you can follow the individual steps, you have no overview of the structure or direction of the proof. You may feel rather discouraged to find yourself in this situation, but the first thing to bear in mind is that you probably will understand the proof sometime, if not now, then later. You should also bear in mind that there is some insight or idea behind the proof, even if it is obscured. You should therefore try to gain an overview of the proof: first of all, be clear in your mind about what is being assumed and what is to be proved. Then try to identify the key points in the proof – there are no recipes for this, indeed even experienced mathematicians may find difficulty in sorting out proofs that are not well presented, but with practice you will find the process easier.

If you still find that you cannot see what is 'going on' in the proof, you may find it helpful to go through the proof for particular cases (say replacing letters with numbers if that is appropriate). It is often useful to ignore the given proof (or even not to read it in the first place) but to think how *you* would try to prove the result – you may well find that your idea is essentially the same as that behind the proof given (or is even better!).

In any event, do not allow yourself to become 'stuck' at a proof. If you have made a serious attempt to understand it, but to little avail, then *go on*: read through what comes next, try the examples, and maybe when you come back to the proof (and you should make a point of coming back to it) you will wonder why you found any difficulty. Remember that if you can do the 'routine' examples then you are getting something out of this text: understanding (the ideas behind) the proofs will deepen your understanding and allow you to tackle less routine and more interesting problems.

Background assumed We have tried to minimise the prerequisites for successfully using this book. In theory it would be enough to be familiar with just the basic arithmetic and order-related properties of the integers, but a reader with no more preparation than this would, no doubt, find the going rather tough to begin with. The reader that we had in mind when writing this book has also seen a bit about sets and functions, knows a little elementary algebra and geometry, and does know how to add and multiply matrices. A few examples and exercises refer to more advanced topics such as vectors, but these may safely be omitted.