Harvey E. Rose

UNIVERSITEXT

A Course on Finite Groups

Springer

A Course on Finite Groups

Universitext

For other titles in this series, go to
www.springer.com/series/223

H.E. Rose

A Course on Finite Groups

Springer

H.E. Rose
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW, UK
H.E.Rose@bristol.ac.uk

ISBN 978-1-84882-888-9 e-ISBN 978-1-84882-889-6
DOI 10.1007/978-1-84882-889-6
Springer London Dordrecht Heidelberg New York

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2009942898

Mathematics Subject Classification (2000): 20-01

Cover design: WMXDesign GmbH

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This book is an introduction to the remarkable range and variety of finite group theory for undergraduate and beginning graduate mathematicians, and all others with an interest in the subject. My original plan was to develop the theory to the point where I could present the proofs and supporting material for some of the main results in the subject. These were to include the theorems of Lagrange, Sylow, Burnside (Normal Complement), Jordan–Hölder, Hall and Schur–Zassenhaus amongst others, and to provide an introduction to character theory developed to the point where Burnside's $p^r q^s$-theorem could be derived and Frobenius kernels and complements could be introduced. I have come to realise that this would have resulted in a rather long book and so some material would have to go. It was at this point that modern technology came to my aid. Solutions to the problems were also to be included, but these would have taken at least 90 rather dense pages and an appendix to this book was perhaps not the best place for this material. A number of textbooks now put solutions on a web site attached to the book which is maintained jointly by the author and the publisher. Extending this idea has allowed me to fulfil my original intentions and keep the printed text to manageable proportions. So the web site now attached to this book, which can be found by going to

www.springer.com

and following the product links, includes not only the Solution Appendix but also extra sections to many of the chapters and two extra web chapters. These items are listed on the contents pages, and present work that is not basic to a chapter's topic being either slightly more specialised or slightly more challenging. Also, perhaps unfortunately, all work on character theory and applications (Chapters 13 and 14) is now on the web. As this book goes to press, about half of this web material is written and 'latexed', it is hoped that the remaining half will be available when the book is published or soon after. Of course, more web items could be added later. I attended Muchio Suzuki's graduate group theory lectures given at the University of Illinois in 1974 and 1975, and so in tribute to him and the insight he gave into modern finite group theory I have ended the extended text with a discussion of his simple groups $\mathrm{Sz}(2^n)$ as an application of the Frobenius theory.

Prerequisites

This book begins with the definition of a group, and Appendices A and B give a brief résumé of the background material from Set Theory and Number Theory that is required. So in one sense, the book needs no prerequisites, only the ability to 'think-straight' and a desire to learn the subject. On the other hand, it would help if the reader had undertaken the following.

(a) We are assuming that the reader is familiar with the material of a basic abstract algebra course, and so he or she has seen at least a few examples of groups and fields, associative and commutative operations, *et cetera*, and also has had some experience working in an abstract setting.
(b) We are also assuming that the reader is familiar with the basics of linear algebra including facts about vector spaces, matrices and determinants, and the definitions of inner and Hermitian forms. We also use the elementary operations, similarity and rational canonical forms, and related topics. Most standard one-semester linear algebra textbooks provide more than is required.
(c) It would also help if the reader had undertaken a first course on analysis which included the basic set operations, elementary properties of the standard number systems: integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$, and the standard set-theoretic methods summarised in Appendix A.
(d) Lastly, some familiarity with elementary number theory would be an asset, Appendix B summarises most that is required. The Euclidean Algorithm is used widely in this book, as are the basic congruence properties.

Plan of the Book

The author of an introductory group theory text has a problem: the theory is self-contained and coherent, many topics are interconnected, and several are needed more or less from the start. On the other hand, the material in a book has perforce to be presented linearly starting at Page 1. During the planning and writing of this book, I have assumed that most readers will not read it sequentially from cover to cover, but will occasionally 'dot-about'. Hence I have allowed some 'forward reference', mostly for examples.

The essential topics that the reader should 'get to grips with' first include the basic facts about groups and subgroups, homomorphisms and isomorphisms, direct products and solubility. Also some aspects of the theory of *actions*—conjugacy, the centraliser and the normaliser—are not far behind. Of course, as noted above, although the material has to be presented linearly, it need not be read linearly, and there are considerable advantages in presenting the basic facts of a topic—homomorphisms, for example—in one place. One consequence of this fact is that the order of the chapters has some flexibility. So Chapter 7 could be read before Chapters 5 and 6 with only a small amount of back-reference in the examples. Some group-theorists may consider it essential for students to have a good grounding in the Abelian theory before the non-Abelian theory is tackled. Similarly, Chapters 10 and 11 can be read in either order with little back-reference required. So a possible non-linear reading of the text is

> Sections 2.1, 2.3, 2.4 and 4.1—the basic core of the subject, then the rest of Chapter 2, Sections 4.2, 4.3, 7.1 and 11.1 in this order,

then the following sections where the reading order might be varied

> Part or all of Chapters 3 and 5, Sections 7.2, 7.3, and 9.1, and Chapters 6 and 10.

Following this the remaining printed sections or possibly some of the web sections could be tackled. In the text, I have sometimes introduced topics ‘early’ and out of their logical order, for example, isomorphisms in Chapter 2, to deal with this point. Also, as a general rule, the ‘easier’ and/or more elementary parts of a topic come near the beginning of the chapter, and so the final sections often contain more specialised and/or challenging material.

Further Reading

The reader would do not harm studying any of the books listed in the bibliography, we suggest a few concentrating on the more recent titles. For a general further development of the finite theory try:

> Robinson (1982), Suzuki (1982, 1986), Aschbacher (1986), Kurzweil and Stellmacher (2004), and Isaacs (2008).

Also the three volume Huppert and Blackburn (1967, 1982a, 1982b) is very comprehensive and deals with many topics not found elsewhere. For more specialised topics, the following should be read:

> Doerk and Hawkes (1992) for soluble groups,
> Carter (1972), the ATLAS (1985), and Conway and Sloane (1993) for finite simple groups,
> James and Liebeck (1993), Huppert (1998) and Isaacs (2006) for character theory, and
> Kaplansky (1969), Fuchs (1970, 1973), and Rotman (1994) for infinite Abelian groups.

Of course, some of the older books still have much to offer, these include

> Burnside (1911, reprinted 2004), Kurosh (1955), Scott (1964) and Rose (1978)—no relation!

Although 45 years old, in my opinion, Scott’s book remains one of the best introductions to the subject.

All errors and omissions that are still present in the text and/or web pages are entirely my fault, please contact me with details at

h.e.rose@bris.ac.uk

General comments, including comments on the correctness and/or clarity of the text, or shorter, clearer or better solutions to the problems (which could be added to the web site), are also welcome.

Acknowledgements I have received a considerable amount of assistance during the writing of this book for which I am extremely grateful. First, from my family (especially from my wife Rita), from colleagues, both academic and computational (especially Richard Lewis and Peter Burton), at the University of Bristol, and from the staff (both editorial and 'Latex' specialist) at Springer Verlag. I have given courses based on preliminary versions of this book many times in Bristol, my students have helped me to clarify many points and I thank them for this. But my main debt of gratitude goes to those who read a final draft of the text and cleared up many inconsistencies and errors on my part. These include the referees appointed by Springer Verlag, John Bowers (formally of the University of Leeds), Robin Chapman (Universities of Bristol and Exeter), Robert Curtis for Chapter 12 (University of Birmingham), and Ben Fairbairn (University of Birmingham). These last four spent many hours going through the manuscript, and improved it greatly—they are forever in my debt.

Bristol Harvey Rose

Contents

Web Contents

Chapter 1
Introduction—The Group Concept

Groups are all-pervasive in mathematics, there is hardly a branch of the subject that does not use them in one way or another. They are also widely used in many branches of the physical sciences. In one sense, this is to be expected because groups are quite often formed when an operation like multiplication or composition is applied to a set or system. Groups occur as number systems or collections of matrices, in permutation theory, as the symmetries of geometrical objects or as sets of maps, and in many other guises. Also the theory contains many elegant, dramatic and illuminating theorems.

Group theory has developed sometimes slowly but at other times by great leaps and bounds over the past two centuries. Often ideas and results appeared first implicitly before they were explicitly written down. For example, it is thought that Galois, in the 1820s, was the first to write down the axioms of a group, but some forty years earlier Lagrange was working with permutations of the roots of equations and proved a result which led to the famous theorem that now bears his name, the comments on actions given in the Introduction to Chapter 5 also apply here. Galois introduced a number of other basic notions including, for example, simple groups and normal subgroups. In 1850, Cayley showed that every group can be represented as a permutation group, and much of the nineteenth century work dealt with this aspect of the theory. Results started to appear more quickly, Sylow produced his ground-breaking work on p-subgroups in 1872, characters and representation theory were introduced around the turn of the century, and Hall's extensions of Sylow's work appeared in the 1920s and 1930s—to mention only a few of the many major developments. Another surge began around 1950 and led in the early 1980s to the completion of the classification problem for finite simple group, hereafter referred to as CFSG, which must surely rank amongst the greatest achievements in all mathematics. A number of important corollaries have followed from this work, for example, the positive solution of the Restricted Burnside Problem (page 27).

The purpose of this book is to introduce the reader to the fine branch of mathematics called *group theory*—there is a 'great story' to tell, and we hope that it will encourage you, the reader, to develop an abiding interest in the subject, and a desire to look further and deeper into the theory.

H.E. Rose, *A Course on Finite Groups,*
Universitext,
DOI 10.1007/978-1-84882-889-6_1,

Group Examples

A group is a mathematical system (or set) with a single operation. We begin by considering two familiar examples; the first is the integers $\mathbb{Z}$. The elements are

$$\ldots, -2, -1, 0, 1, 2, 3, \ldots,$$

and the operation is standard addition '$+$'. There are a number of basic axioms from which almost all additive properties follow. The first and in some ways the most important is *closure*, or being *well-defined*; that is,

$$\text{if } a, b \in \mathbb{Z}, \quad \text{then} \quad a + b \in \mathbb{Z}.$$

This is equivalent to stating that $+$ is an operation (Appendix A). Some so-called *partial* systems have been studied, but all systems considered in this book satisfy an axiom of this type. The next property is *associativity*; that is,

$$\text{for all } a, b, c \in \mathbb{Z} \quad \text{we have} \quad (a + b) + c = a + (b + c).$$

When forming this sequence of additions, we obtain the same answer if we first add a to b, and then add the result of this addition to c, or if we first add b to c and then form the sum of a and the result of this last addition. Some algebraic systems lack this property but, in general, non-associative systems have limited uses unless some more complex rule is applied—for example, in Lie algebras—and again we shall not consider such systems in this book.

In $\mathbb{Z}$, a natural question to ask is: Does the equation

$$a + x = b \tag{1.1}$$

have a solution x? In ancient times mathematicians only 'allowed' this equation to have a solution if $b > a$, that is, if x is positive. But this is very restrictive, and in the group $\mathbb{Z}$ Equation (1.1) is always uniquely soluble, and so we need to introduce the 'zero' and 'negative' integers. The zero 0 satisfies

$$a + 0 = 0 + a = a \quad \text{for all } a \in \mathbb{Z};$$

in the sequel, we use the term *neutral element* for the entity 0; see the discussion on page 4. Further, we introduce the *negative integers* by

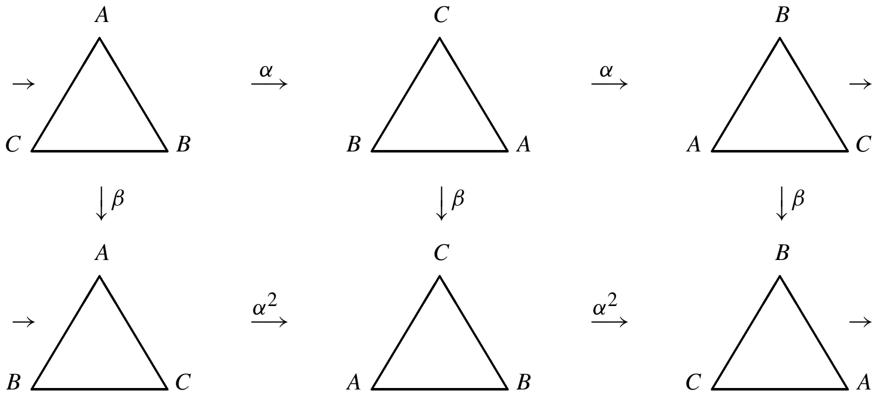
$$\text{for all } a \in \mathbb{Z} \quad \text{there exists a unique } c \in \mathbb{Z} \quad \text{that satisfies} \quad a + c = 0.$$

We usually write $-a$ for c (and a^{-1} for c if we are using a multiplicative notation as is the case for almost all groups discussed in this book), and we call it the *inverse* of a. It is now easy to show that (1.1) always has a unique solution. The system $\mathbb{Z}$ has one extra basic property not shared by all groups: it is *commutative*, or *Abelian*. This is given by

$$\text{for all } a, b \in \mathbb{Z} \quad \text{we have} \quad a + b = b + a,$$

the result of several additions does not depend on the order of the terms in the sum. To recap, $\mathbb{Z}$ has the four basic properties: Closure, associativity, a neutral element and inverses, and it has the extra property of Abelianness. Note also it is a countably infinite system.

For our second example, we consider another familiar system—symmetries of an equilateral triangle. Groups of symmetries provide a good range of examples, they are widely used in both mathematical and physical systems, for example, by chemists when they are studying the crystal structure of matter. The group of symmetries of a triangle has two aspects which are different from those in our first example: It is finite, and it is not Abelian, but as we shall see below it shares the four basic properties with $\mathbb{Z}$. Consider an equilateral triangle with vertices labelled A, B, C. This geometric object has a number of *symmetries*, that is, transformations (rotations and reflections) that give another copy of the original triangle. We work in the standard Euclidean plane.



The elements of the group are the six rotations and reflections of the triangle illustrated above, and the operation is composition; that is, do one rotation or reflection, and then do another on the result of the first. We take the basic rotation α to be clockwise about the centre of the triangle by the angle $2\pi/3$, see the top row of the diagram above. Note that three applications of α (that is, α^3, a rotation by 2π) maps the triangle to itself identically, and so can be taken as the neutral element. This also shows that the inverse of α is α^2; see the bottom row in the diagram. The triangle has three reflections, they are mirror transformations about a line through a vertex and the centre of the corresponding opposite edge. One, labelled β (three times) in the diagram, is about a vertical line through the top vertex of the corresponding triangle and the centre of its base. The other two reflections can be generated as follows. If we first apply α to the top-left triangle and then apply β to the result, we obtain the middle triangle in the bottom row. This gives the second reflection of the top-left triangle, now about a line through the bottom right-hand vertex B and the centre of the opposite edge AC. Note that we would obtain the same result if we first applied β to the top-left triangle, and then applied α^2 to the result. We can obtain the third reflection if we repeat this construction but begin by applying α^2 instead of α to the top-left triangle. Incidentally, this shows that the group is not Abelian (that is, not commutative as $\beta\alpha = \alpha^2\beta \neq \alpha\beta$). The inverse of a reflection is itself: Two applications of a reflection gives the neutral element. We call a group element of this type an *involution*, and we shall see later that these elements play an important role in the theory. It is straightforward to check that this system is closed and has the associativity property (reader, try a few cases). Hence the system contains the six symmetries of the triangle: Neutral element (where a triangle is mapped to itself identically), α, α^2, β, $\alpha\beta$, and $\alpha^2\beta$, and it satisfies the four basic group axioms (closure, associativity, and possession of a neutral element and inverses for all of its elements) as in our first example. It is also finite and not Abelian. Later we shall call this system the *dihedral group* of the triangle and denote it by D_3.

Abstract Groups and Representations

With these and other examples in mind, we define a group as a system with a single operation satisfying the four basic properties (axioms) described above, the formal definition is given at the beginning of Chapter 2. Also, Section 2.2 provides a substantial list of examples. The following point is important. In both cases, the examples given above are particular 'instances' of the group in question; we call them *representations* of the group. Referring to the second example, another representation is given by considering the set of permutations of the set $\{1, 2, 3\}$ with composition as the operation; see page 19 and Section 3.1. A third representation using 2×2 matrices is given in Problem 4.2. Each group example given in this book is a representation of its corresponding *abstract group*, see the discussion in the Introduction to Chapter 3. *Right from the start this is a characteristic feature that the reader should note, and we use a corresponding nomenclature.* So when discussing a group in the abstract we call it a 'group', but when discussing a particular example or representation, say using permutations or matrices or some analogous construction, we call it a 'permutation group' or a 'matrix group' or analogous group. Similarly, the 'neutral element' which we always denote by e is the element in the abstract group satisfying the relevant axiom, and it has many instances or representations in particular groups. In the examples given in Section 2.2, it is 0, or 1, or -3, or a matrix, or a collection of maps, or the point at infinity on a curve, *et cetera*. The term 'neutral element' is not standard, nor is it 'new'; for example, it occurs in Cohn (1965), page 50. Some authors use either 'identity' or 'trivial element'; the first only really applies to an 'operation of multiplicative type', whilst the second gives the wrong impression—this element is an important one in the group, and certainly not trivial in the usual sense of this word. We have extended this nomenclature to the single element (sub)group $\langle e \rangle$ which we call the *neutral (sub)group*, see Definition 2.12. Also an 'inverse' can be an additive inverse, or a multiplicative inverse, or an inverse matrix, *et cetera*.

Classes of Groups

The class of all groups is a large one. Set-theorists call it a *proper class* as opposed to a *set*, but as we are taking the usual naive view of set theory (Appendix A) we shall treat sets and classes synonymously. We shall see that it is convenient to consider subclasses defined by some of the basic properties. For example, groups can be finite or infinite, and Abelian or non-Abelian; these distinctions are fundamental. We shall study further distinctions later, for instance, in Chapter 11 between 'soluble' and 'non-soluble' groups. Here we divide the class of all groups into four subclasses and, as we shall see, both the theory and the actual groups in each subclass have distinct characteristics.

The first subclass contains the

Finite Abelian Groups In Chapter 7, we show that groups in this class can be characterised completely, and they have a particularly simple form—that is, as 'products of cyclic groups'. So in one sense they are 'a bit boring'; but in an application, if we know *a priori* that the group or groups under discussion are in this subclass, then we can be sure that they take this simple form which can have a major influence on the result. A good example occurs in the theory of rational points on elliptic curves discussed on page 22. Amongst our four subclasses, this is the only one for which we have a complete description of all of the groups involved.

The second subclass contains the

Finite Non-Abelian Groups Most of the work in this book deals with groups in this class. For finite groups in general, there is a strong interplay between the 'group theory' and the 'number theory' of the group in question. In part this is a consequence of Lagrange's Theorem which states that the order (number of elements) of a subgroup H of a group G must divide the order of G; so the prime factorisation of the order of a finite group is an important invariant of the group. One major development from this is the Sylow theory discussed in Chapter 6 which asserts the existence of subgroups with prime power order. Another important distinction in the theory is between the so-called 'simple' and 'non-simple' groups; see the definition on page 33. The Jordan–Hölder Theorem states, roughly speaking, that all finite (and some infinite) groups can be 'built up' from simple groups using 'extensions'; this will be discussed in Chapter 9—note that one of the main aims our work is to describe all groups. A theory of extensions has been developed, but a considerable amount of work and many new ideas will be needed before it can be described as finished; see Section 9.2. On the other hand, a complete list of finite simple groups is now known, much of the development work was undertaken between 1955 and 1985 and, as noted above, it forms one of the crowning achievements of twentieth century mathematics. We give a brief introduction to this topic in Chapter 12. Hence considerable progress has been made in the theory of finite non-Abelian groups and this will be discussed in the following chapters and web appendices, but work still needs to be done.

The third subclass contains the

Infinite Abelian Groups For infinite groups in general, number theory only plays a small role, but questions concerning cardinality can be important. The so-called finitely-generated Abelian groups are similar to those in the first subclass as they can be represented as products of cyclic groups. But many groups in this class are not finitely generated, for example, the rational numbers with addition or the positive reals with multiplication. Apart from a brief survey in `Web Section` 7.5 we shall not deal with these groups in this book. Much of the work develops ideas from linear algebra, and good introductions to this topic are given in Kaplansky (1969), and Fuchs (1970, 1973).

The final subclass contains the

Infinite Non-Abelian Groups This is perhaps the least well-understood part of the theory. A number of extensions of the finite theory have been studied, but no general classification is known, and it seems unlikely that one will be found in the near future. One approach is to use topology. For example, the reals have a natural (metric) topology, and the interplay between the group theory and the topology of this system can be exploited to gain new insights. Since 1950 a number of long-standing problems have been solved, often showing that these groups are more complicated than previously thought; for example, see Problem 6.7. A good introduction is given in Kurosh (1955), also Robinson (1982) discusses a number of aspects of this part of the theory. Infinite groups with some kind of 'finiteness condition', such as being 'finitely generated' or 'finitely presented', have also been widely studied.

Summary of the Book

Below we give a brief summary of the contents of the printed Chapters 2 to 12, Appendices A to E, the `Web Chapters` 13 and 14, and the `Web Appendices`.

Chapter 2—Elementary Group Properties The basic entities—semigroups, groups, subgroups, cosets, normal subgroups and simple groups—are defined, Lagrange's Theorem is derived, and the second section lists a number of standard examples.

Chapter 3—Group Construction and Representation The main construction methods and group representations are discussed. Firstly, permutations are introduced, the symmetric and alternating groups are defined, and an elementary proof of the simplicity of A_n for $n > 4$ is given. Secondly, matrix groups are briefly considered, and lastly group presentations are introduced (this topic is completed in `Web Section` 4.7 once the First Isomorphism Theorem has been proved). `Web Section` 3.6 discusses some of the various representations of the alternating group A_5 to illustrate the fact that groups can have a wide range of representations.

Chapter 4—Homomorphisms The natural maps, called Homomorphisms (and Isomorphisms when the map is a bijection), and factor groups are introduced, and the four fundamental Isomorphism and Correspondence Theorems are derived. Cyclic groups and the basic properties of the automorphism group of a group are described. There are two `Web Sections` 4.6 and 4.7. The first introduces the 'transfer' which provides a useful example of a 'real' homomorphism, and the second completes the work on group presentations begun in Chapter 3.

Chapter 5—Action and the Orbit-stabiliser Theorem This chapter, the last giving the basic material, introduces 'actions' which bring together a number of useful constructions, and gives a proof of the Orbit-stabiliser Theorem. It also describes three important particular actions: the coset action, the conjugate element action leading to centralisers and the Class Equations, and the conjugate subgroup action leading to normalisers and the N/C-theorem. `Web Section` 5.5 extends the work on permutation theory begun in Chapter 3, and includes a discussion of 'transitive' and 'primitive' permutation groups, and Iwasawa's simplicity lemma.

Chapter 6—p-Groups and Sylow Theory The basic theory of p-groups (where all elements have order a power of p) is discussed, and the five Sylow theorems are derived—these results form one of the most important aspects of the finite theory. There are then two sections of applications, the first gives (a) some facts about groups whose orders have a small number of factors, (b) proves the so-called Frattini Argument, and (c) introduces nilpotent groups. The second is `Web Section` 6.5 which gives some more substantial applications including a proof of Burnside's Normal Complement Theorem and a discussion of groups all of whose Sylow subgroups are cyclic.

Chapter 7—Products and Abelian Groups Direct products are introduced, and two proofs of the Fundamental Theorem of Abelian Groups are presented; see page 5. The third section discusses 'semi-direct products', a variant of the direct product construction, and the groups of order 12 are described (they can all be treated as semi-direct products). Some basic facts, but no proofs, concerning infinite Abelian groups are given in `Web Section` 7.5. Except for some problems, this is the only point where specifically infinite groups are considered in any detail.

Chapter 8—Groups of Order 24, Three Examples No new theory is presented in this chapter, but three groups of order 24 are discussed in some detail. The work constructs their subgroups including those of Frattini and Fitting, the subgroup lattice, series and some of their representations. Appendix C, see pages 289 to 292, gives data on the remaining twelve groups of order 24. The purpose of this chapter is to challenge the reader to think more about the objects he or she is studying, and to ask questions. For example: can the centre of a group equal its derived subgroup or its Frattini subgroup? This chapter is also intended to motivate the remaining topics, that is series, simple groups and (on the web) representation theory.

Chapters 9—Series, Jordan–Hölder Theorem and the Extension Problem This is the first of three shorter chapters dealing with series and the normal subgroup structure of groups. In the first of these, we prove the theorem of Jordan and Hölder on composition series—this demonstrates the importance of simple groups to the theory. Secondly, we present a brief introduction to extension theory—that is the construction of complex groups using some of their subgroups as components, and we discuss one substantial example.

Chapter 10—Nilpotency Nilpotent groups lie between Abelian and soluble groups, and this second shorter chapter continues the work on these groups begun earlier. There is a surprising number of equivalent definitions which shows the importance of the notion. The second section discusses two 'special' subgroups of a group—the Frattini and Fitting subgroups; they have some remarkable properties (including being nilpotent), and extensions of the latter have proved useful in the completion of CFSG.

Chapter 11—Solubility After a brief historical introduction the last of the shorter chapters introduces the basic facts about soluble groups, and discusses a number of equivalent conditions. The most important is due to Philip Hall and extends the Sylow theory in the soluble case.

Chapter 12—Simple Groups of Order Less than 10000 This is another 'descriptive' chapter giving an account of simple groups with order less than 10000. We introduce Steiner systems—their automorphisms provide a new way to construct groups, prove the simplicity of the linear (matrix) groups $L_n(q)$, and discuss one 'classical' ($U_3(3)$, a *unitary group*) and one 'sporadic' (M_{11}, the first *Mathieu group*) group in detail. Some numerical data is also given but many proofs are omitted. Appendix E, see page 295, gives data on the groups $L_2(q)$, and an appendix at `Web Section` 12.6 provides more information about Steiner systems for Mathieu groups, and data on simple groups of order less than 10^6.

Appendix A—Set Theory and Appendix B—Number Theory These two appendices give the basic definitions and results for the work on sets and number theory which underlie all the material in the book.

Appendices C, D and E These appendices provide data on several aspects of the theory. The first, C, lists properties of groups of order 24 (this is an appendix to Chapter 8), D details the number of groups with order up to 520, and E provides some representations of the linear groups $L_2(q)$ (this is an appendix to Chapter 12).

`Web Chapter` 13—Representation and Characters A brief introduction to representation and character theory is presented sufficient for the applications given in `Web Chapter` 14. This theory includes the basic definitions, Schur's Lemma and Maschke's theorem, the orthogonality relations, and 'lifts', *et cetera*. This chapter is entirely theoretical except for the examples.

`Web Chapter` 14—Character Tables, and Theorems of Burnside and Frobenius We give three applications of the work in `Web Chapter` 13 which have strong connections with the earlier material. First, we construct some character tables including those for most of the groups of order 12 or less, and some others including several of order 24 discussed in Chapter 8. These character tables provide a surprising amount of information concerning the groups in question. Second, we prove Burnside's $p^r q^s$-theorem (this completes the proof of Hall's Theorem given in Chapter 11). The third section introduces the Frobenius 'kernel' and 'complement', gives a proof of Frobenius's Theorem concerning these notions, and finally it provides some applications of this theorem including a discussion of Suzuki groups.

`Web Solution Appendix` This includes answers, hints on solutions, and in some cases full solutions, for all of the problems given in Chapters 2 to 12, and Appendices A and B.

Developing the theory and proving results are of course important, but two other aspects are also important.

Problems Each chapter ends with a sequence of problems for the reader to try of varying difficulty partly as indicated with a star $\star$ suggesting a greater challenge. Some readers may find it difficult to decide which problems start with and which are the most important, so some of these have been marked with the symbol ⧫. These are all fairly straightforward, theoretical, and contain minor results that are used in the main part of the text. Other problems ask for examples to be constructed, these have no indication mark but should also be tackled early. As noted above, hints, sketch solutions, or in some cases detailed treatments of problems, are given in `Web Solution Appendix` on the web site attached to this book.

'Actual groups' We are studying groups, and so it seems essential to us that the reader 'sees' and 'experiences' as many 'actual' or 'concrete' groups as possible. This will, we hope, illuminate the theory and so induce a greater understanding in general. Some parts of the text and a number of the problems are given over to this aspect including the whole of Chapter 8.

Computers in Group Theory

During the past thirty years, and more so recently, computers have become an increasingly useful tool in pure mathematics, as well as in most other branches of mathematics, many branches of the physical sciences, and beyond. In group theory, they are particularly useful for doing matrix and permutation calculations, and for producing examples. But they can also be used for more sophisticated constructions, for example, looking for subgroups of a group or constructing homomorphisms. A number of computer algebra packages, some 'free' and some commercially available, have been developed over the past decade or so, and the reader is encouraged to make use of at least one of these while reading this book. Also a number of the problems are best tackled using one of these packages.

While writing this book, we have made extensive use of the computer algebra package called GAP—Groups, Algorithms, and Programming. This package has many authors based in Aachen in Germany, St. Andrews in Scotland, and at many other sites; we would like to take this opportunity to compliment these authors on the excellence of their product. It is available free from the St. Andrews web site at

http://www-gap.dcs.st-and.ac.uk/~gap

We have also made some use of the commercially available package called MAGMA which incorporates many aspects of the GAP program.

One point should be borne in mind whilst working with any of these packages, and it is one that we emphasise several times in this book. In a particular calculation, the program can only deal with a specified representation of the group under discussion, say as a permutation group or as a matrix group. The package GAP is particularly good when working with permutation groups, but it also deals well with matrix groups defined over a specific field and with presentations.

Chapter 2
Elementary Group Properties

In this chapter, we introduce our main objects of study—groups. A general overview including some historical comments was given in Chapter 1. More detail on the history of the theory can be found in Wussing (1984), van der Waerden (1985), and at www-gap.dcs.st-andrews.ac.uk/~history/. Here we give the basic definitions and an extensive list of examples, introduce subgroups and cosets, normal subgroups and simple groups, and prove the first major result in the theory—Lagrange's Theorem.

2.1 Basic Definitions

We begin by defining the group concept. Maps between groups will be discussed in Chapter 4. As a preliminary to this we introduce *semigroups* as follows.

Definition 2.1 A *semigroup* is a non-empty set $X = \{\dots, x, y, z, \dots\}$ together with a binary operation $\odot$ (page 281) which satisfies the following two conditions (axioms):

(i) it is *closed*, or *well-defined*: for all $x, y \in X$, we can perform the operation $x \odot y$ and

$$x \odot y \in X,$$

(ii) it is *associative*: for all $x, y, z \in X$,

$$x \odot (y \odot z) = (x \odot y) \odot z.$$

Note that (i) is implied by the definition of the operation $\odot$; see the comments below Definition 2.2.

H.E. Rose, *A Course on Finite Groups*,
Universitext,

DOI 10.1007/978-1-84882-889-6_2,