Graduate Texts in Mathematics

Robert A. Wilson

The Finite Simple Groups

Springer

Graduate Texts in Mathematics 251

For other titles published in this series, go to
http://www.springer.com/series/136

Robert A. Wilson

The Finite Simple Groups

Springer

Professor Robert A. Wilson
Queen Mary, University of London
School of Mathematical Sciences
Mile End Road
London E1 4NS
UK
R.A.Wilson@qmul.ac.uk

ISSN 0072-5285
ISBN 978-1-84800-987-5 e-ISBN 978-1-84800-988-2
DOI 10.1007/978-1-84800-988-2
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: 2009941783

Mathematics Subject Classification (2000): 20D

Cover design: SPI Publisher Services

Printed on acid-free paper

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

Preface

This book is intended as an introduction to all the finite simple groups. During the monumental struggle to classify the finite simple groups (and indeed since), a huge amount of information about these groups has been accumulated. Conveying this information to the next generation of students and researchers, not to mention those who might wish to apply this knowledge, has become a major challenge.

With the publication of the two volumes by Aschbacher and Smith [12, 13] in 2004 we can reasonably regard the proof of the Classification Theorem for Finite Simple Groups (usually abbreviated CFSG) as complete. Thus it is timely to attempt an overview of all the (non-abelian) finite simple groups in one volume. For expository purposes it is convenient to divide them into four basic types, namely the alternating, classical, exceptional and sporadic groups.

The study of alternating groups soon develops into the theory of permutation groups, which is well served by the classic text of Wielandt [170] and more modern treatments such as the comprehensive introduction by Dixon and Mortimer [53] and more specialised texts such as that of Cameron [19]. The study of classical groups via vector spaces, matrices and forms encompasses such highlights as Dickson's classic book [48] of 1901, Dieudonné's [52] of 1955, and more modern treatments such as those of Taylor [162] and Grove [72]. The complete collection of groups of Lie type (comprising the classical and exceptional groups) is beautifully exposed in Carter's book [21] using the simple complex Lie algebras as a starting point. And sporadic attempts have been made to bring the structure of the sporadic groups to a wider audience—perhaps the most successful book-length introduction being that of Griess [69]. But no attempt has been made before to bring within a single cover an introductory overview of all the finite simple groups (unless one counts the 'Atlas of finite groups' [28], which might reasonably be considered to be an overview, but is certainly not introductory).

The remit I have given myself, to cover all of the finite simple groups, gives both advantages and disadvantages over books with more restricted subject matter. On the one hand it allows me to point out connections, for example between exceptional behaviour of generic groups and the existence of sporadic groups. On the other hand it prevents me from proving everything in as much detail as the reader may desire. Thus the reader who wishes to understand everything in this book will have to do a lot of homework in filling in gaps, and following up references to more complete treatments. Some of the exercises are specifically designed to fill in gaps in the proofs, and to develop certain topics beyond the scope of the text.

One unconventional feature of this book is that Lie algebras are scarcely mentioned. The reasons for this are twofold. Firstly, it hardly seems possible to improve on Carter's exposition [21] (although this book is now out of print and secondhand copies change hands at astronomical prices). And secondly, the alternative approach to the exceptional groups of Lie type via octonions deserves to be better known: although real and complex octonions have been extensively studied by physicists, their finite analogues have been sadly neglected by mathematicians (with a few notable exceptions). Moreover, this approach yields easier access to certain key features, such as the orders of the groups, and the generic covering groups.

On the other hand, not all of the exceptional groups of Lie type have had effective constructions outside Lie theory. In the case of the family of large Ree groups I provide such a construction for the first time, and give an analogous description of the small Ree groups. The importance of the octonions in these descriptions led me also to a new octonionic description of the Leech lattice and Conway's group, and to an ambition, not yet realised, to see the octonions at the centre of the construction of all the exceptional groups of Lie type, and many of the sporadic groups, including of course the Monster.

Complete uniformity of treatment of all the finite simple groups is not possible, but my ideal (not always achieved) has been to begin by describing the appropriate geometric/algebraic/combinatorial structure, in enough detail to calculate the order of its automorphism group, and to prove simplicity of a clearly defined subquotient of this group. Then the underlying geometry/algebra/combinatorics is further developed in order to describe the subgroup structure in as much detail as space allows. Other salient features of the groups are then described in no particular order.

This book may be read in sequence as a story of all the finite simple groups, or it may be read piecemeal by a reader who wants an introduction to a particular group or family of groups. The latter reader must however be prepared to chase up references to earlier parts of the book if necessary, and/or make use of the index. Chapters 4 and 5 are largely (but not entirely) independent of each other, but both rely heavily on Chapters 2 and 3. The sections of Chapter 4 are arranged in what I believe to be the most appropriate order pedagogically, rather than logically or historically, but could be read in a different order. For example, one could begin with Section 4.3 on $G_2(q)$ and proceed via triality (Section 4.7) to $F_4(q)$ (Section 4.8) and $E_6(q)$ (Section 4.10), postponing the twisted groups until later. The ordering of sections in Chapter 5 is traditional, but a more avant-garde approach might begin with J_1 (Section 5.9.1), and follow this with the exotic incarnation of (the double cover of) J_2 as a quaternionic reflection group (in the first few parts of Section 5.6), and/or the octonionic Leech lattice (Section 5.6.12). But one cannot go far in the study of the sporadic groups without a thorough understanding of M_{24}.

I was introduced to the weird and wonderful world of finite simple groups by a course of lectures on the sporadic simple groups given by John Conway in Cambridge in the academic year 1978–9. During that course, and the following three years when he was my Ph.D. supervisor, he taught me most of what subsequently appeared in the 'Atlas of finite groups' [28], and a large part of what now appears in this book. I am of course extremely indebted to him for this thorough initiation.

Especial thanks go also to my former colleague at the University of Birmingham, Chris Parker, who, early in 2003, fuelled by a couple of pints of beer, persuaded me there was a need for a book of this kind, and volunteered to write half of it; who persuaded the Head of School to let us teach a two-semester course on finite simple groups in 2003–4; who developed the original idea into a detailed project plan; and who then quietly left me to get on and write the book. It is not entirely his fault that the book which you now have in your hands bears only a superficial resemblance to that original plan: I excised the chapters which he was going to write, on Lie algebras and algebraic groups, and shovelled far more into the other chapters than we ever anticipated. At the same time the planned 150 pages grew to nearly 300. Indeed, the more I wrote, the more I became aware of how much I had left out. I would need at least another 300 pages to do justice to the material, but one has to stop somewhere. I apologise to those readers who find that I stopped just at the point where they started to get interested.

Several colleagues have read substantial parts of various drafts of this book, and made many valuable comments. I particularly thank John Bray, whose keen nose for errors and assiduousness in sorting out some of the finer points has improved the accuracy and reliability of the text enormously; John Bradley, whose refusal to accept woolly arguments helped me tighten up the exposition in many places; and Peter Cameron whose comments on some early draft chapters have led to significant improvements, and whose encouragement has helped to keep me working on this book.

I owe a great deal also to my students for their careful reading of various versions of parts of the text, and their uncovering of countless errors, some minor, some serious. I used to tell them that if they had not found any errors, it was because they had not read it properly. I hope that this is now less true than it used to be. I thank in particular Jonathan Ward, Johanna Rämö, Simon Nickerson, Nicholas Krempel, and Richard Barraclough, and apologise to any whose names I have inadvertently omitted.

It is a truism that errors remain, and the fault (if fault there be), human nature. By convention, the responsibility is mine, but in fact that is unrealistic.

As Gauss himself said, "In science and mathematics we do not appeal to authority, but rather *you are responsible for what you believe*." Nevertheless, I shall endeavour to maintain a web-site of corrections that have been brought to my attention, and will be grateful for notification of any further errors that you may find.

Thanks go also to Karen Borthwick at Springer-Verlag London for her gentle but persistent pressure, and to the anonymous referees for their enthusiasm for this project and their many helpful suggestions. I am grateful to Queen Mary, University of London, for their initially relatively light demands on me when I moved there in September 2004, which left me time to indulge in the pleasures of writing. It is entirely my own fault that I did not finish the book before those demands increased to the point where only a sabbatical would suffice to bring this project to a conclusion. I am therefore grateful to Jianbei An and the University of Auckland, and John Cannon and the University of Sydney, for providing me with time, space, and financial support during the last six months which enabled me, among other things, to sign off this book.

London — *Robert Wilson*
June 2009

Contents

1

Introduction

1.1 A brief history of simple groups

The study of (non-abelian) finite simple groups can be traced back at least as far as Galois, who around 1830 understood their fundamental significance as obstacles to the solution of polynomial equations by radicals (square roots, cube roots, etc.). From the very beginning, Galois realised the importance of classifying the finite simple groups, and knew that the alternating groups A_n are simple for $n \geqslant 5$, and he constructed (at least) the simple groups $\mathrm{PSL}_2(p)$ for primes $p \geqslant 5$.

Every finite group G has a *composition series*

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{n-1} \lhd G_n = G \tag{1.1}$$

where each group is normal in the next, and the series cannot be refined any further: in other words, each G_i/G_{i-1} is *simple*. The Jordan–Hölder theorem states that the set of *composition factors* G_i/G_{i-1} (counting multiplicities) is independent of the choice of composition series. Thus if any composition series contains a non-abelian composition factor then they all do. Galois's theorem states that a polynomial equation in one variable has a solution by radicals if and only if the corresponding 'Galois group' has a composition series with cyclic factors.

The 19th century saw slow progress in finite group theory until 1870, in which year appeared Camille Jordan's 'Traité des substitutions' [104], followed in 1872 by the publication of Sylow's theorems. The former contains constructions of the simple groups we now call $\mathrm{PSL}_n(p)$, while the latter provides the first tools for classifying simple groups. And we must not forget the extraordinary paper of Mathieu [131] from 1861 in which he constructs the groups we now know as the sporadic groups M_{11} and M_{12}, and which was followed by another paper [132] in 1873 constructing M_{22}, M_{23} and M_{24}.

It was not until the dawn of the 20th century that a well-developed theory of the finite classical groups began to emerge, most notably in the work of

R.A. Wilson, *The Finite Simple Groups*,
Graduate Texts in Mathematics 251,

L. E. Dickson. In large part this work was inspired by Killing's classification of complex simple Lie algebras (if that is not an oxymoron) into the types $\mathtt{A}_n$, $\mathtt{B}_n$, $\mathtt{C}_n$, $\mathtt{D}_n$, $\mathtt{G}_2$, $\mathtt{F}_4$, $\mathtt{E}_6$, $\mathtt{E}_7$ and $\mathtt{E}_8$. Dickson constructed finite simple groups analogous to all of these except $\mathtt{F}_4$, $\mathtt{E}_7$ and $\mathtt{E}_8$, for every finite field (with a small number of exceptions which are not simple).

One wonders why Dickson did not go on to construct finite simple groups of the remaining three types. It seems extraordinary that it was another fifty years before Chevalley provided a uniform construction of all these groups, in his famous 1955 paper [23]. The types $\mathtt{A}_n$, $\mathtt{B}_n$, $\mathtt{C}_n$ and $\mathtt{D}_n$ give rise to the classical groups $\mathrm{PSL}_{n+1}(q)$ (linear), $\mathrm{P}\Omega_{2n+1}(q)$ (orthogonal, odd dimension), $\mathrm{PSp}_{2n}(q)$ (symplectic) and $\mathrm{P}\Omega^+_{2n}(q)$ (orthogonal, even dimension, plus type). But where were the unitary groups, and $\mathrm{P}\Omega^-_{2n}(q)$? Very soon it was realised that these could be obtained by 'twisting' the Chevalley construction. Using the unitary groups as a model, Steinberg, Tits and Hertzig independently constructed two new families ${}^3D_4(q)$ and ${}^2E_6(q)$.

Soon afterwards, Suzuki and Ree saw how to 'twist' the groups of types $\mathtt{B}_2$, $\mathtt{G}_2$ and $\mathtt{F}_4$, provided the characteristic of the field was 2, 3, or 2 respectively. And that seemed to be that. There was a feeling in the early 1960s (or so I am told) that probably all the finite simple groups had been discovered, and all that remained was to prove this.

Meanwhile, other parts of group theory had been developing by leaps and bounds. The Feit–Thompson paper [59] of 1963 proved the monumental result that every finite group of odd order is soluble, or to put it another way, every non-abelian finite simple group has even order. Thus every nonabelian finite simple group contains an element of order 2 (an *involution*) and soon the seemingly outrageous notion began to take root, that one could prove by induction that all finite simple groups were known. Thompson again provided the base case for the induction by classifying the minimal simple groups.

And so, in the early 1960s, the attempt to get a complete classification of the finite simple groups began in earnest. But it turned out to be a lot harder than some people had predicted. More or less the first case to try to eliminate after Thompson's work (at least logically, if not historically) was the case of a simple group with involution centraliser $C_2 \times A_5$. Janko's construction of such a group in 1964 sent shock-waves throughout the group theory community. Suddenly it seemed that the classification project might not be so easy after all. Maybe there were still hundreds, thousands, infinitely many simple groups left to find?

In the decade that followed, a further twenty 'sporadic' (the term originally used by Burnside to describe the Mathieu groups) simple groups were discovered, and then the supply suddenly dried up. By 1980 there was a general feeling that the classification of finite simple groups was almost complete, and there were probably no more finite simple groups to find. Not that that has stopped some people from continuing to look. Announcements were made that the proof was almost complete, and (premature) predictions of the imminent death of group theory filled the air.

1.2 The Classification Theorem

The *Classification Theorem for Finite Simple Groups* (traditionally abbreviated CFSG, conveniently forgetting that what is important is not so much the *Classification*, as the *Theorem*) states that every finite simple group is isomorphic to one of the following:

(i) a cyclic group C_p of prime order p;
(ii) an alternating group A_n, for $n \geqslant 5$;
(iii) a classical group:

linear:	$\mathrm{PSL}_n(q)$, $n \geqslant 2$, except $\mathrm{PSL}_2(2)$ and $\mathrm{PSL}_2(3)$;
unitary:	$\mathrm{PSU}_n(q)$, $n \geqslant 3$, except $\mathrm{PSU}_3(2)$;
symplectic:	$\mathrm{PSp}_{2n}(q)$, $n \geqslant 2$, except $\mathrm{PSp}_4(2)$;
orthogonal:	$\mathrm{P}\Omega_{2n+1}(q)$, $n \geqslant 3$, q odd;
	$\mathrm{P}\Omega^+_{2n}(q)$, $n \geqslant 4$;
	$\mathrm{P}\Omega^-_{2n}(q)$, $n \geqslant 4$

where q is a power p^a of a prime p;
(iv) an exceptional group of Lie type:

$$G_2(q), q \geqslant 3; F_4(q); E_6(q); {}^2E_6(q); {}^3D_4(q); E_7(q); E_8(q)$$

where q is a prime power, or

$${}^2B_2(2^{2n+1}), n \geqslant 1; {}^2G_2(3^{2n+1}), n \geqslant 1; {}^2F_4(2^{2n+1}), n \geqslant 1$$

or the Tits group ${}^2F_4(2)'$;
(v) one of 26 sporadic simple groups:
- the five Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24};
- the seven Leech lattice groups Co_1, Co_2, Co_3, McL, HS, Suz, J_2;
- the three Fischer groups Fi_{22}, Fi_{23}, Fi'_{24};
- the five Monstrous groups $\mathbb{M}$, $\mathbb{B}$, Th, HN, He;
- the six pariahs J_1, J_3, J_4, O'N, Ly, Ru.

Conversely, every group in this list is simple, and the only repetitions in this list are:

$$\begin{aligned} \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) &\cong A_5; \\ \mathrm{PSL}_2(7) &\cong \mathrm{PSL}_3(2); \\ \mathrm{PSL}_2(9) &\cong A_6; \\ \mathrm{PSL}_4(2) &\cong A_8; \\ \mathrm{PSU}_4(2) &\cong \mathrm{PSp}_4(3). \end{aligned} \tag{1.2}$$

It is the chief aim of this book to explain, as far as space allows, the *statement* of CFSG. Thus we seek to introduce all the finite simple groups, to provide concrete constructions whenever possible, to calculate the orders of the groups, prove simplicity, and study their actions on various natural geometrical or combinatorial objects to the point where much of the subgroup structure is revealed. In so doing, we prove a substantial part (though by no means all) of the converse part of CFSG, that is, we prove the existence of many of the finite simple groups. (In the literature on CFSG the word 'construction' is generally used in this technical sense of 'existence proof', but in this book I shall often use it in the weaker sense of building, possibly without proof, an object which is in fact the group in question.) On the other hand, there is nothing at all here about the proof of the main part of CFSG, that is, the non-existence of any other finite simple groups.

1.3 Applications of the Classification Theorem

If one has (or if many people have) spent decades classifying certain objects, one is apt to forget just why one started the project in the first place. Predictions of the death of group theory in 1980 were the pronouncements of just such amnesiacs. But group theorists did not spend such an enormous amount of effort classifying simple groups just in order to put them in a glass case and admire them.

The first serious applications of CFSG were in permutation group theory. For example, the classical problem of classifying multiply-transitive groups, which had led Mathieu to the discovery of the first five sporadic groups, was easily solved: essentially, there are no others. With more work, one can classify 2-transitive groups. The O'Nan–Scott Theorem was the first result aimed towards a classification of primitive permutation groups. It reduced this problem (for a fixed degree n) to the problem of classifying maximal subgroups of index n in the almost simple groups, rather than in arbitrary groups.

This emphasised the need which was already felt, to have a good classification of the maximal subgroups of the simple groups. For individual groups it is possible to obtain complete explicit lists of maximal subgroups. For example, the maximal subgroups of the sporadic groups can be obtained by (often formidable) calculations: all except the Monster have been completed in this way. For families of groups it is not always possible to obtain such an explicit answer. In the case of the alternating groups, the O'Nan–Scott theorem lists some maximal subgroups explicitly, and says that any other maximal subgroup is almost simple, acting primitively. A theorem of Liebeck, Praeger and Saxl [120] tells us exactly when a subgroup of the latter type is *not* maximal, but it is impossible to give an explicit list of the rest.

A similar programme for classifying the maximal subgroups of the classical groups began with the publication of Aschbacher's paper [5] on the subject in 1984. For small dimensions explicit lists of all the maximal subgroups are known, going back to the classification of the maximal subgroups of $\mathrm{PSL}_2(q)$ more than a century ago by L. E. Dickson and others [48]. With the benefit of exhaustive lists of representations of quasisimple groups in dimensions up to 250, due to Hiss and Malle [79] and Lübeck [124], there is some prospect that eventually there will be explicit lists of maximal subgroups for classical groups in these dimensions. Similarly, one would hope to be able to do the same for the exceptional groups of Lie type: so far, complete lists are available for five of the ten families.

1.4 Remarks on the proof of the Classification Theorem

There has been much debate about whether CFSG deserves to be called a theorem, and this debate has contributed to the philosophical arguments about what a theorem is, what a proof is, what mathematics is (or are) and how we recognise them when we see them. I believe most mathematicians are pragmatic in their daily professional lives, and do not expect to reach the Platonic ideal of a perfect proof which confers absolute certainty on a result. Certainly some mathematicians who argue most vociferously for the absolute nature of proof are amongst those whose own proofs often fall short of this ideal. Thus my own point of view is that it is ultimately meaningless to argue about whether a written (or spoken) argument 'is' or 'is not' a 'proof'. One can only really argue about the degree of certainty we derive from the argument.

The twentieth century saw announcements of solutions of many long-standing difficult problems in mathematics, including besides the CFSG, also the four-colour problem, Fermat's Last Theorem, the Poincaré conjecture, and others. It is natural, and necessary, to greet these announcements with a healthy degree of scepticism, as not all of them have stood up to the test of time. But in most cases a gradual process of expert scrutiny, tidying up and correcting minor (or major) errors leads eventually to a general acceptance that the problem in question has indeed been solved. On the other hand, it is impossible in practice to satisfy the mathematician's desire for absolute certainty. After all, we are only human and therefore fallible. We make mistakes, which sometimes lie hidden for years.

So what of the CFSG? Has it indeed been proved? Certainly the process of collating the various parts of the proof, filling in the gaps and correcting errors, has taken longer than anyone expected when the imminent completion of the proof was announced around 1980. The project by Gorenstein, Lyons and Solomon [66] to write down the whole proof in one place is still in progress: six of a projected eleven volumes have been published so far. The so-called 'quasithin' case is not included in this series, but has been dealt with in two volumes, totalling some 1200 pages, by Aschbacher and Smith [12, 13]. Nor do they consider the problem of existence and uniqueness of the 26 sporadic simple groups: fortunately this is not in the slightest doubt. So by now most parts of the proof have been gone over by many people, and re-proved in different ways. Thus the likelihood of catastrophic errors is much reduced, though not completely eliminated.

1.5 Prerequisites

I have tried in this book to keep the prerequisites to a minimum, but I do assume a familiarity with abstract group theory up to the level of Sylow's theorems and the Jordan–Hölder theorem, as well as the basics of linear algebra, such as can be found in Kaye and Wilson [105], and a reasonable mathematical maturity. In a few of the proofs I also need to assume a basic knowledge of representation theory, such as can be found in James and Liebeck [98], although this is not necessary for most of the text. In the chapter on sporadic groups I shall from time to time use basic properties of graphs, codes, lattices and other mathematical objects, but I hope that these can be picked up from the context. For the record, here is a summary of roughly what I assume as background in group theory. (Don't read this unless you need to!)

Groups, subgroups and cosets

A *group* is a (finite) set G with an *identity* element 1, a (binary) *multiplication* $x.y$ (or xy) and a (unary) *inverse* x^{-1} satisfying the *associative law* $(xy)z = x(yz)$, the *identity laws* $x1 = 1x = x$ and the *inverse laws* $xx^{-1} = x^{-1}x = 1$ for all $x, y, z \in G$ (and the *closure laws* $xy \in G$ and $x^{-1} \in G$ which we take for granted). It is *abelian* if $xy = yx$ for all $x, y \in G$, *non-abelian* otherwise. A *subgroup* is a subset H closed under multiplication and inverses. (It is sufficient to check $xy^{-1} \in H$ for all $x, y \in H$.) *Left cosets* of H in G are subsets $gH = \{gh \mid h \in H\}$ and *right cosets* are $Hg = \{hg \mid h \in H\}$. The left (or right) cosets all have the same size, and partition G, so that $|G| = |H||G : H|$ (*Lagrange's Theorem*), where $|G|$ is the *order* of G, i.e. the number of elements in G, and $|G : H|$ is the *index* of H in G, i.e. the number of left (or right) cosets. The *order* of an element $g \in G$ is the order n of the *cyclic group* $\langle g\rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ (denoted C_n) that it *generates*, and the *exponent* of G is the lowest common multiple of the orders of the elements, that is the smallest positive integer e such that $g^e = 1$ for all $g \in G$.

Homomorphisms and quotient groups

A *homomorphism* is a map $\phi : G \to H$ which preserves the multiplication, $\phi(xy) = \phi(x)\phi(y)$ (from which it follows that $\phi(1) = 1$ and $\phi(x^{-1}) = \phi(x)^{-1}$). The *kernel* of ϕ is $\ker\phi = \{g \in G \mid \phi(g) = 1\}$, and is a subgroup which satisfies $g(\ker\phi) = (\ker\phi)g$, i.e. its left and right cosets are equal (such a subgroup N is called *normal*, written $N \trianglelefteq G$, or $N \triangleleft G$ if also $N \neq G$). An *isomorphism* is a bijective homomorphism, i.e. one satisfying $\ker\phi = \{1\}$ and $\phi(G) = H$: in this case we write $G \cong H$.

If N is a normal subgroup of G, the *quotient* group G/N has elements xN (for all $x \in G$) and group operations $(xN)(yN) = (xy)N$, and $(xN)^{-1} = x^{-1}N$. The *first isomorphism theorem* states that if $\phi : G \to H$ is a homomorphism then the image of ϕ, $\phi(G) \cong G/\ker\phi$ (and the isomorphism is given by $\phi(x) \mapsto x(\ker\phi)$).

The normal subgroups of G/N are in one-to-one correspondence with the normal subgroups K of G which contain N, and the *second isomorphism theorem* is $(G/N)/(K/N) \cong G/K$. If H is any subgroup of G, and N is any normal subgroup of G, then $HN = \{xy \mid x \in H, y \in N\}$ is a subgroup of G and $N \cap H$ is a normal subgroup of H, and the *third isomorphism theorem* is $HN/N \cong H/(N \cap H)$.

Simple groups and composition series

A group S is *simple* if it has exactly two normal subgroups (1 and S). In particular, an abelian group is simple if and only if it has prime order. A series

$$1 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{n-1} \lhd G_n = G \tag{1.3}$$

for a group G is called a *composition series* if all the factors G_i/G_{i-1} are simple (and they are then called *composition factors*).

The *fourth isomorphism theorem* (or *Zassenhaus's butterfly lemma*) states that if $X \lhd Y \leqslant G$ and $A \lhd B \leqslant G$ then

$$\frac{(Y \cap B)X}{(Y \cap A)X} \cong \frac{(Y \cap B)}{(Y \cap A)(X \cap B)} \cong \frac{(Y \cap B)A}{(X \cap B)A}.$$

Hence any two series for G have isomorphic *refinements*, and by induction on the length of a composition series, any two composition series for a finite group have the same composition factors, counted with multiplicities (the *Jordan–Hölder Theorem*). A *normal series* is one in which all terms G_i are normal in G, and if it has no proper refinements it is called a *chief series*, and its factors G_i/G_{i-1} *chief factors*.

Soluble groups

A group is *soluble* if it has a composition series with abelian (hence cyclic of prime order) composition factors. A *commutator* is an element $x^{-1}y^{-1}xy$, denoted $[x, y]$, and the subgroup generated by all commutators $[x, y]$ of elements $x, y \in G$ is the *commutator subgroup* (or *derived subgroup*), written $[G, G]$ or G'. Writing $G^{(0)} = G$ and $G^{(n)} = (G^{(n-1)})'$, it follows that G is soluble if and only if $G^{(n)} = 1$ for some n. Also G/N is abelian if and only if N contains G', so G/G' is the *largest abelian quotient* of G.

Group actions and conjugacy classes

The *right regular representation* of a group G is the identification of each element $g \in G$ with the permutation $x \mapsto xg$ of the elements of G. This shows that every finite group is isomorphic to a group of permutations (*Cayley's theorem*). If G is a group of permutations on a set Ω, and $a \in \Omega$, the *stabiliser* of a is the subgroup H consisting of all permutations in G which map a to itself. Then Lagrange's theorem can be re-interpreted as the *orbit–stabiliser theorem*, that $|G|/|H|$ equals the number of images of a under G (i.e. the *length* of the *orbit* of a).

Now let G act on itself by conjugation, $g : x \mapsto g^{-1}xg$, so that the orbits are the *conjugacy classes* $[x] = \{g^{-1}xg \mid g \in G\}$, and the stabiliser of x is the *centraliser* of x, $C_G(x) = \{g \in G \mid g^{-1}xg = x\}$. In particular, the conjugacy classes partition G, and their sizes divide the order of G. An element x is in a conjugacy class of size 1 if and only if x *commutes* with every element of G, i.e. $x \in Z(G) = \{y \in G \mid g^{-1}yg = y \text{ for all } g \in G\}$, the *centre* of G, which is a normal subgroup of G.

p-groups and nilpotent groups

A finite group is called a *p-group* if its order is a power of the prime p (and so by Lagrange's Theorem all its elements have order some power of p). Every conjugacy class in G has p^a elements for some a, and $\{1\}$ is a conjugacy class, so there are at least p conjugacy classes of size 1, and $Z(G)$ has order at least p. Define $Z_1(G) = Z(G)$ and $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$, so that if G is a p-group then $Z_n(G) = G$ for some n. A group with this property is called *nilpotent* (of *class* at most n), and the series

$$1 = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd \cdots$$

is called the *upper central series*.

The *direct product* $G_1 \times \cdots \times G_k$ of groups $G_1, \ldots, G_k$ is defined on the set $\{(g_1, \ldots, g_k) \mid g_i \in G_i\}$ by the group operations $(g_1, \ldots, g_k)(h_1, \ldots, h_k) = (g_1h_1, \ldots, g_kh_k)$ and $(g_1, \ldots, g_k)^{-1} = ({g_1}^{-1}, \ldots, {g_k}^{-1})$. A finite group is nilpotent if and only if it is a direct product of p-groups.

Abelian groups

If m and n are coprime, then $C_m \times C_n \cong C_{mn}$. Hence in any finite abelian group there is an element whose order is equal to the exponent of the group. Indeed, every finite abelian group is isomorphic to a group $C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ with n_i dividing n_{i-1} for all $2 \leqslant i \leqslant r$. Conversely, the integers n_i are uniquely determined by the group.

Sylow's theorems

If G is a finite group of order $p^k n$, where p is prime and n is not divisible by p, then the *Sylow theorems* state that

(i) G has subgroups of order p^k;
(ii) these *Sylow p-subgroups* are all conjugate; and
(iii) the number s_p of Sylow p-subgroups satisfies $s_p \equiv 1 \bmod p$. (Note also that, by the orbit–stabiliser theorem, s_p is a divisor of n).

To prove the first statement, let G act by right multiplication on all subsets of G of size p^k: since the number of these subsets is not divisible by p, there is a stabiliser of order divisible by p^k, and therefore equal to p^k. To prove the second statement, and also to prove that any p-subgroup is contained in a Sylow p-subgroup, let any p-subgroup Q act on the right cosets Pg of any Sylow p-subgroup P by right multiplication: since the number of cosets is not divisible by p, there is an orbit $\{Pg\}$ of length 1, so $PgQ = Pg$ and gQg^{-1} lies inside P. To prove the third statement, let a Sylow p-subgroup P act by conjugation on the set of all the other Sylow p-subgroups: the orbits have length divisible by p, for otherwise P and Q are distinct Sylow p-subgroups of $N_G(Q)$, which is a contradiction.

An important corollary of Sylow's theorems is the *Frattini argument*: if $N \lhd G$ and P is a Sylow p-subgroup of N, then $G = N_G(P)N$.

Automorphism groups

An *automorphism* of a group G is an isomorphism of G with itself. The set of all automorphisms of G forms a group under composition, and is denoted $\mathrm{Aut}(G)$. The *inner* automorphisms are the automorphisms $\phi_g : x \mapsto g^{-1}xg$, for $g \in G$. These form a subgroup $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$. Indeed, if $\alpha \in \mathrm{Aut}(G)$, then $\alpha^{-1}\phi_g\alpha = \phi_{g^\alpha}$, so that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. Now $\phi_{gh} = \phi_g\phi_h$, and $\phi_g = \phi_h$ if and only if $gh^{-1} \in Z(G)$, so the map ϕ defined by $\phi : g \mapsto \phi_g$ is a homomorphism from G onto $\mathrm{Inn}(G)$ with kernel $Z(G)$. Therefore $\mathrm{Inn}(G) \cong G/Z(G)$ and, in particular, if $Z(G) = 1$ then $G \cong \mathrm{Inn}(G)$. The *outer automorphism group* of G is $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

1.6 Notation

Unfortunately there is no general consensus on notation for simple groups, extensions of groups, and so on. In this book I shall usually, but not always, follow the notation of the 'Atlas of finite groups' [28]. The main exception is for orthogonal groups, where Atlas notation is most likely to be misunderstood, and I prefer to follow Dieudonné [52]. Notation for simple groups is given in Section 1.2. Extensions of groups are written in one of the following ways: $A \times B$ denotes a direct product, with normal subgroups A and B; also $A{:}B$ denotes a semidirect product (or split extension), with a normal subgroup A and a subgroup B; and $A{}^{\cdot}B$ denotes a non-split extension, with a normal subgroup A and quotient B, but no subgroup B; finally $A.B$ or just AB denotes an unspecified extension.

The expression $[n]$ denotes an (unspecified) group of order n, while n or C_n denotes (usually) a cyclic group of order n. If p is prime, p^n denotes an elementary abelian group of order p^n, i.e. a direct product of n copies of C_p. Often I shall use q^n (where q is a power of p) also to denote an elementary abelian p-group, although this is not standard Atlas notation. This includes the case $n = 1$.