SYMMETRIC GENERATION OF GROUPS

Some of the most beautiful mathematical objects found in the last forty years are the sporadic simple groups, but gaining familiarity with these groups presents problems for two reasons. Firstly, they were discovered in many different ways, so to understand their constructions in depth one needs to study lots of different techniques. Secondly, since each of them is, in a sense, recording some exceptional symmetry in space of certain dimensions, they are by their nature highly complicated objects with a rich underlying combinatorial structure.

Motivated by initial results on the Mathieu groups which showed that these groups can be generated by highly symmetrical sets of elements, the author develops the notion of symmetric generation from scratch and exploits this technique by applying it to many of the sporadic simple groups, including the Janko groups and the Higman–Sims group.

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

40 N. White (ed.) *Matroid Applications*
41 S. Sakai *Operator Algebras in Dynamical Systems*
42 W. Hodges *Basic Model Theory*
43 H. Stahl and V. Totik *General Orthogonal Polynomials*
45 G. Da Prato and J. Zabczyk *Stochastic Equations in Infinite Dimensions*
46 A. Björner *et al. Oriented Matroids*
47 G. Edgar and L. Sucheston *Stopping Times and Directed Processes*
48 C. Sims *Computation with Finitely Presented Groups*
49 T. Palmer *Banach Algebras and the General Theory of *-Algebras I*
50 F. Borceux *Handbook of Categorical Algebra I*
51 F. Borceux *Handbook of Categorical Algebra II*
52 F. Borceux *Handbook of Categorical Algebra III*
53 V. F. Kolchin *Random Graphs*
54 A. Katok and B. Hasselblatt *Introduction to the Modern Theory of Dynamical Systems*
55 V. N. Sachkov *Combinatorial Methods in Discrete Mathematics*
56 V. N. Sachkov *Probabilistic Methods in Discrete Mathematics*
57 P. M. Cohn *Skew Fields*
58 R. Gardner *Geometric Tomography*
59 G. A. Baker, Jr., and P. Graves-Morris *Padé Approximants, 2nd edn*
60 J. Krajicek *Bounded Arithmetic, Propositional Logic, and Complexity Theory*
61 H. Groemer *Geometric Applications of Fourier Series and Spherical Harmonics*
62 H. O. Fattorini *Infinite Dimensional Optimization and Control Theory*
63 A. C. Thompson *Minkowski Geometry*
64 R. B. Bapat and T. E. S. Raghavan *Nonnegative Matrices with Applications*
65 K. Engel *Sperner Theory*
66 D. Cvetkovic, P. Rowlinson and S. Simic *Eigenspaces of Graphs*
67 F. Bergeron, G. Labelle and P. Leroux *Combinatorial Species and Tree-Like Structures*
68 R. Goodman and N. Wallach *Representations and Invariants of the Classical Groups*
69 T. Beth, D. Jungnickel, and H. Lenz *Design Theory I, 2nd edn*
70 A. Pietsch and J. Wenzel *Orthonormal Systems for Banach Space Geometry*
71 G. E. Andrews, R. Askey and R. Roy *Special Functions*
72 R. Ticciati *Quantum Field Theory for Mathematicians*
73 M. Stern *Semimodular Lattices*
74 I. Lasiecka and R. Triggiani *Control Theory for Partial Differential Equations I*
75 I. Lasiecka and R. Triggiani *Control Theory for Partial Differential Equations II*
76 A. A. Ivanov *Geometry of Sporadic Groups I*
77 A. Schinzel *Polymomials with Special Regard to Reducibility*
78 H. Lenz, T. Beth, and D. Jungnickel *Design Theory II, 2nd edn*
79 T. Palmer *Banach Algebras and the General Theory of *-Algebras II*
80 O. Stormark *Lie's Structural Approach to PDE Systems*
81 C. F. Dunkl and Y. Xu *Orthogonal Polynomials of Several Variables*
82 J. P. Mayberry *The Foundations of Mathematics in the Theory of Sets*
83 C. Foias *et al. Navier–Stokes Equations and Turbulence*
84 B. Polster and G. Steinke *Geometries on Surfaces*
85 R. B. Paris and D. Kaminski *Asymptotics and Mellin–Barnes Integrals*
86 R. McEliece *The Theory of Information and Coding, 2nd edn*
87 B. Magurn *Algebraic Introduction to K-Theory*
88 T. Mora *Solving Polynomial Equation Systems I*
89 K. Bichteler *Stochastic Integration with Jumps*
90 M. Lothaire *Algebraic Combinatorics on Words*
91 A. A. Ivanov and S. V. Shpectorov *Geometry of Sporadic Groups II*
92 P. McMullen and E. Schulte *Abstract Regular Polytopes*
93 G. Gierz *et al. Continuous Lattices and Domains*
94 S. Finch *Mathematical Constants*
95 Y. Jabri *The Mountain Pass Theorem*
96 G. Gasper and M. Rahman *Basic Hypergeometric Series, 2nd edn*
97 M. C. Pedicchio and W. Tholen (eds.) *Categorical Foundations*
98 M. E. H. Ismail *Classical and Quantum Orthogonal Polynomials in One Variable*
99 T. Mora *Solving Polynomial Equation Systems II*
100 E. Olivieri and M. Eulália Vares *Large Deviations and Metastability*
102 L. W. Beineke *et al.* (eds.) *Topics in Algebraic Graph Theory*
103 O. Staffans *Well-Posed Linear Systems*
105 M. Lothaire *Applied Combinatorics on Words*
106 A. Markoe *Analytic Tomography*
107 P. A. Martin *Multiple Scattering*
108 R. A. Brualdi *Combinatorial Matrix Classes*
110 M.-J. Lai, L. L. Schumaker *Spline Functions on Triangulations*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Symmetric Generation of Groups

With Applications to Many of the Sporadic Finite Simple Groups

ROBERT T. CURTIS
University of Birmingham, UK

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India

103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

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/9780521857215

First published 2007

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

ISBN 978-0-521-85721-5 Hardback

This book is dedicated to my mother, Doreen Hannah (née Heard), 1912–2006, and to my wife, Ahlam.

Contents

Preface

The book is aimed at postgraduate students and researchers into finite groups, although most of the material covered will be comprehensible to fourth year undergraduates who have taken two modules of group theory. It is based on the author's technique of symmetric generation, which seems able to present many difficult group-theoretic constructions in a more elementary manner. It is thus the aim of the book to make these beautiful, but combinatorially complicated, objects accessible to a wider audience.

The stimulus for the investigations which led to the contents of the book was a question from a colleague of mine, Tony Gardiner, who asked me if the Mathieu group M_{24} could contain two copies of the linear group $\mathrm{L}_3(2)$ which intersect in a subgroup isomorphic to the symmetric group S_4. He needed such a configuration in order to construct a graph with certain desirable properties. I assured him that the answer was almost certainly yes, but that I would work out the details. I decided to use copies of $\mathrm{L}_3(2)$ which are maximal in M_{24} and found that the required intersection occurred in the nicest possible way, in that one could find subgroups $H \cong K \cong \mathrm{L}_3(2)$, with $H \cap K \cong \mathrm{S}_4$, and an involution t such that $\mathrm{C}_{\mathrm{M}_{24}}(H \cap K) = \langle t \rangle$ and $H^t = K$. This means that t has seven images under conjugation by H, and the maximality of H together with the simplicity of M_{24} mean that these seven involutions must generate M_{24}. The symmetry of the whole set-up enables one to write down seven corresponding involutory permutations on 24 letters directly from a consideration of the action of $\mathrm{L}_3(2)$ on 24 points.

Applying the same ideas with $\mathrm{L}_3(2)$ replaced by the alternating group A_5, or more revealingly the projective special linear group $\mathrm{PSL}_2(7)$ replaced by $\mathrm{PSL}_2(5)$, I found that in an analogous manner the smaller Mathieu group M_{12} is generated by five elements of order 3 which can be permuted under conjugation within the large group by a subgroup isomorphic to A_5.

From here the generalization to other groups became clear and many of the sporadic simple groups revealed themselves in a pleasing manner. This book concentrates on groups of moderate size, and it is satisfying to see how the symmetry of the generating sets enables one to verify by hand claims that would appear to be beyond one's scope. With groups such as the smallest Janko group J_1, the Higman–Sims group HS and the second Janko group HJ, I have included the full manual verification, so that the reader can appreciate what can be achieved. However, in writing the book I have come more and more to make use of the double coset enumerator which was produced by John Bray and myself specifically for groups defined by what we now call a *symmetric presentation*. The program implementing this algorithm is written in MAGMA, which has the advantage that it is very easy to read what the code is asking the machine to do. Thus, even when a hand calculation is possible, and indeed has been completed, I have often preferred to spare the reader the gory details and simply include the MAGMA output. Of course, some of the groups which are dealt with in this manner are out of range for all but the doughtiest reckoner!

As is made clear in the text, every finite simple group possesses definitions of the type used in this book. However, I have not seen fit to include those groups which are plainly out of range of mechanical enumeration, or where a description of the construction introduces additional complicated ideas. Nonetheless, 19 of the 26 sporadic groups are mentioned explicitly and it is hoped that the definitions given are quite easily understood. The book is in three Parts.

Part I: Motivation

Part I, which assumes a rather stronger background than Part II and which could, and perhaps should, be omitted at a first reading, explains where the ideas behind symmetric generation of groups came from. In particular, it explains how generators for the famous Mathieu groups M_{12} and M_{24} can be obtained from easily described permutations of the faces of the dodecahedron and Klein map, respectively. This not only ties the approach in with classical mathematics, but demonstrates a hitherto unrecognized link with early algebraic geometry. Although Part I is, in a sense, independent of what follows, the way in which combinatorial, algebraic and geometric constructions complement one another gives an accurate flavour of the rest of the book.

Part I is essentially background and does not contain exercises.

Part II: Involutory symmetric generators

Part II begins by developing the basic ideas of symmetric generation of finite groups in the most straightforward case: when the generators have order 2. The preliminary topics of *free products of cyclic groups* and *double cosets* are defined before the notions of *symmetric generating sets, control subgroup, progenitor, Cayley diagrams* and *coset stabilizing subgroups* are introduced and fully explained through elementary but important examples. It is shown that every finite simple group can be obtained in the manner described, as a quotient of a progenitor. Through these elementary examples the reader becomes adept at handling groups defined in terms of highly symmetric sets of elements of order 2.

At this stage we demonstrate how the algebraic structure can be used to do the combinatorial work for us. The Fano plane emerges as a by-product of the method, and the famous isomorphisms $A_5 \cong PSL_2(5)$ and $PSL_2(7) \cong PSL_3(2)$ are proved. Further, $PSL_2(11)$ emerges in its exceptional Galois action on 11 points, and the 11-point biplane is revealed. An easy example produces the symmetric group S_6 acting non-permutation identically on two sets of six letters, and the outer automorphism of S_6 reveals itself more readily than in other constructions known to the author; the isomorphism $\mathrm{Aut}A_6 \cong P\Gamma L_2(9)$ follows. The method is also used to exhibit the exceptional triple covers of A_6 and A_7.

There follows a systematic computerized investigation of groups generated by small, highly symmetrical sets of involutory generators, and it is seen that classical and sporadic groups emerge alongside one another. The results of this investigation are presented in convenient tabular form, as in Curtis, Hammas and Bray [36].

Having familiarized the reader with the methods of symmetric generation, we now move on to more dramatic applications. Several sporadic simple groups are defined, and in many cases constructed by hand, in terms of generating sets of elements of order 2.

Part II concludes by describing how the methods of symmetric generation afford a concise and amenable way of representing an element of a group as a permutation followed by a short word in the symmetric generators. Thus an element of the smallest Janko group J_1 can be written as a permutation of eleven letters, in fact an element of $L_2(11)$, followed by a word of length at most four in the eleven involutory symmetric generators. A manual algorithm for multiplying elements represented in this manner, and for reducing them to canonical form, has been computerized in Curtis and Hasan [37].

Part III: Symmetric generators of higher order

In Part III we extend our investigations to symmetric generators of order greater than 2. It soon becomes apparent that this leads us into a consideration of monomial representations of our so-called control subgroup over finite fields. The resulting progenitors are slightly more subtle objects than those in Part II, and they reward our efforts by producing a fresh crop of sporadic simple groups.

Nor is it necessary to restrict our attention to finite fields of prime order. A monomial representation over, say, the field of order 4 may be used to define a progenitor in which each 'symmetric generator' is a Klein fourgroup. It turns out that this is a natural way to obtain the Conway group Co_1 and other sporadic groups.

The classification of finite simple groups is one of the most extraordinary intellectual achievements in the twentieth century. It states that there are just 26 finite simple groups which do not fit into one of the known infinite families. These groups, which range in size from the smallest Mathieu group of order 7920 to the Monster group of order around 10^{53}, were discovered in a number of unrelated ways and no systematic way of constructing them has as yet been discovered. Symmetric generation provides a uniform concise definition which can be used to construct surprisingly large groups in a revealing manner. Many of the smaller sporadic groups are constructed by hand in Parts II and III of this book, and computerized methods for constructing several of the larger sporadics are described. It is our aim in the next few years to complete the task of providing an analogous definition and construction of each of the sporadic finite simple groups.

Acknowledgements

I should first of all like to thank John Conway for introducing me to those beautiful objects the Mathieu groups, and for the many hours we spent together studying other finite groups as we commenced work on the ATLAS [25]. In many ways, all that I came to understand at that time has fed into the present work. I am also indebted to my colleague, Tony Gardiner, for asking me the question mentioned in the Preface which sparked the central ideas in this book.

Since that time, several of my research students have worked on topics arising out of these ideas and have thus contributed to the contents of this book. I shall say a few words about each of them in the chronological order in which they submitted their dissertations.

Ahmed Hammas (1991) from Medina in Saudi Arabia carried out the first systematic search for images of progenitors with small control subgroups. Perhaps his most startling and satisfying discovery was the isomorphism

$$\frac{2^{\star 5} : \mathrm{A}_5}{[(0\ 1\ 2\ 3\ 4)t_0]^7} \cong \mathrm{J}_1,$$

the smallest Janko group. **Abdul Jabbar** (1992) from Lahore in Pakistan also joined the project early on, having worked with Donald Livingstone on (2,3,7)-groups. He concentrated on symmetric presentations of subgroups of the Conway group and, in particular, those groups in the Suzuki chain. **Michelle Ashworth**, in her Masters thesis (1997), explored the manner in which the hexads of the Steiner system $S(5,6,12)$ can be seen on the faces of a dodecahedron, and how the octads of the Steiner system $S(5,8,24)$ appear on the faces of the Klein map. **John Bray** (1998), who now works at Queen Mary, University of London, made a massive contribution to the project, both as my research student and later as an EPSRC research fellow. His thesis contains many results which I have not included in this book and far more details than would be appropriate in a text of this nature. His formidable computational skills came to fruition in his programming and improvement of the *double coset enumerator* which had evolved out of my early hand calculations. **Stephen Stanley** (1998), who now works for a software company in Cambridge, UK, was mainly concerned with monomial representations of finite groups and their connection with symmetric generation. One of his most interesting achievements was a faithful 56-dimensional representation of the covering group $2^{2\cdot}L_3(4)$ over $\mathbb{Z}_8$, the integers modulo 8. **Mohamed Sayed** (1998) from Alexandria in Egypt produced an early version of the double coset enumerator, which worked well in some circumstances but was probably too complicated to cope with larger groups. **Sean Bolt** (2002) works for the Open University in Coventry; he made a comprehensive study of a symmetric presentation of the largest Janko group J_4, which eventually led us to the definition described in Part II of this book. **John Bradley** (2005), who is presently teaching in the University of Rwanda, verified by hand the symmetric presentations we had for the McLaughlin group McL and the Janko group J_3. This brings us up to the present day with **Sophie Whyte** (2006), who has just graduated having followed on from the work of Stephen Stanley. In particular she has identified all faithful irreducible monomial representations of the covering groups of the alternating groups, and has used them as control subgroups in interesting progenitors.

I should also like to thank my colleague **Chris Parker** for his collaboration with me on a very successful project to extend symmetric generation to the larger sporadic groups, and I should like to thank the EPSRC for supporting that project. Chris's commitment and infectious enthusiasm for mathematics made it a pleasure to work with him. The School of Mathematics is to be thanked for providing additional funding which enabled us to take on two research assistants: John Bray and **Corinna Wiedorn**. Corinna came to us from Imperial College, where she had been working with Sasha Ivanov. She possessed geometric skills which proved invaluable as we dealt with larger and larger objects. Among her many achievements was a verification by hand of the symmetric presentation for J_1 mentioned above as being found by Ahmed Hammas. The skills of the four people involved meshed perfectly and led to a very productive period. Sadly Corinna died in 2005, and her exceptional talent is lost to mathematics.