Australian Mathematical Society Lecture Series 25

Classical Groups, Derangements and Primes

Timothy C. Burness
Michael Giudici

Australian Mathematical Society Lecture Series: 25

Classical Groups, Derangements and Primes

TIMOTHY C. BURNESS
University of Bristol

MICHAEL GIUDICI
The University of Western Australia

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

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

www.cambridge.org
Information on this title: www.cambridge.org/9781107629448

First published 2016

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

Library of Congress Cataloguing in Publication data
Burness, Timothy C., 1979–
Classical groups, derangements, and primes / Timothy C. Burness, University of Bristol,
Michael Giudici, The University of Western Australia
pages cm. – (Australian Mathematical Society lecture series ; 25)
Includes bibliographical references and index.
ISBN 978-1-107-62944-8
1. Logic, Symbolic and mathematical. 2. Group theory. 3. Algebra. 4. Numbers,
Prime. I. Giudici, Michael, 1976– II. Title.
QA9.B856 2016
512.7–dc23
2015013719

ISBN 978-1-107-62944-8 Paperback

Classical Groups, Derangements and Primes

A classical theorem of Jordan states that every nontrivial finite transitive permutation group contains a derangement. This existence result has interesting and unexpected applications in many areas of mathematics, including graph theory, number theory and topology. Various generalisations have been studied in recent years, with a particular focus on the existence of derangements with special properties.

Written for academic researchers and postgraduate students working in related areas of algebra, this introduction to the finite classical groups features a comprehensive account of the conjugacy and geometry of elements of prime order. The development is tailored towards the study of derangements in finite primitive classical groups; the basic problem is to determine when such a group G contains a derangement of order r, where r is a given prime divisor of the degree of G. This involves a detailed analysis of the conjugacy classes and subgroup structure of the finite classical groups.

AUSTRALIAN MATHEMATICAL SOCIETY LECTURE SERIES

1. Introduction to Linear and Convex Programming, N. CAMERON
2. Manifolds and Mechanics, A. JONES, A. GRAY & R. HUTTON
3. Introduction to the Analysis of Metric Spaces, J. R. GILES
4. An Introduction to Mathematical Physiology and Biology, J. MAZUMDAR
5. 2-Knots and their Groups, J. HILLMAN
6. The Mathematics of Projectiles in Sport, N. DE MESTRE
7. The Petersen Graph, D. A. HOLTON & J. SHEEHAN
8. Low Rank Representations and Graphs for Sporadic Groups, C. E. PRAEGER & L. H. SOICHER
9. Algebraic Groups and Lie Groups, G. I. LEHRER (ed.)
10. Modelling with Differential and Difference Equations, G. FULFORD, P. FORRESTER & A. JONES
11. Geometric Analysis and Lie Theory in Mathematics and Physics, A. L. CAREY & M. K. MURRAY (eds.)
12. Foundations of Convex Geometry, W. A. COPPEL
13. Introduction to the Analysis of Normed Linear Spaces, J. R. GILES
14. Integral: An Easy Approach after Kurzweil and Henstock, L. P. YEE & R. VYBORNY
15. Geometric Approaches to Differential Equations, P. J. VASSILIOU & I. G. LISLE (eds.)
16. Industrial Mathematics, G. R. FULFORD & P. BROADBRIDGE
17. A Course in Modern Analysis and its Applications, G. COHEN
18. Chaos: A Mathematical Introduction, J. BANKS, V. DRAGAN & A. JONES
19. Quantum Groups, R. STREET
20. Unitary Reflection Groups, G. I. LEHRER & D. E. TAYLOR
21. Lectures on Real Analysis, F. LÁRUSSON
22. Representations of Lie Algebras, A. HENDERSON
23. Neverending Fractions, J. BORWEIN et al.

Dedicated to the memory of our friend and colleague
Ákos Seress, 1958–2013

Preface

The theory of permutation groups is a classical area of algebra, which arises naturally in the study of symmetry in a vast range of mathematical and physical systems. Originating in the early nineteenth century, permutation group theory continues to be a very active area of current research, with far-reaching applications across the sciences and beyond. In the last thirty years, the subject has been revolutionised by the *Classification of Finite Simple Groups* (CFSG), a truly remarkable theorem that is widely recognised as one of the greatest achievements of twentieth century mathematics. This has led to many interesting problems, and the development of powerful new techniques to solve them.

Let G be a transitive permutation group on a finite set Ω of size at least 2. By a classical theorem of Jordan [82], G contains an element that acts fixed-point-freely on Ω; such elements are called *derangements*. The existence of derangements has interesting and unexpected applications in many other areas of mathematics, such as graph theory, number theory and topology (we will briefly discuss some of these applications in Chapter 1).

The study of derangements can be traced all the way back to the origins of probability theory over three centuries ago. Indeed, in 1708 Pierre de Montmort [106] studied the proportion of derangements in the symmetric group S_n in its natural action on n points. Montmort obtained a precise formula, which shows that this proportion tends to the constant $1/e$ as n tends to infinity. This work played an important role in his pioneering mathematical analysis of various games of chance that were popular in the salons and gambling dens of early eighteenth century Paris. As we will see in Chapter 1, a wide range of related problems concerning derangements has been studied in more recent years.

One of the main motivations for our work stems from a theorem of Fein, Kantor and Schacher that provides a powerful extension of Jordan's aforementioned existence result. The main theorem in [52] states that every transitive group G as above contains a derangement of *prime power* order. It is interesting to note that the only known proof of this theorem requires CFSG. Naturally, we can ask whether or not G always contains a derangement of *prime* order. It turns out that this is false in general, although examples with no such elements appear to be somewhat rare, which explains why the permutation groups with this property are called *elusive* groups. For example, a theorem of Giudici [61] implies that the smallest Mathieu group M_{11} is the only almost simple primitive elusive group (with respect to its 3-transitive action on 12 points).

This observation raises several natural and intriguing questions. Clearly, if r is a prime number then G contains a derangement x of order r only if r divides $|\Omega|$ (every cycle in the disjoint cycle decomposition of x has to have length r). This leads naturally to a *local* notion of elusivity: for a prime r we say that G is *r-elusive* if r divides $|\Omega|$ and G does not contain a derangement of order r. In particular, G is elusive if and only if G is r-elusive for every prime divisor r of $|\Omega|$. Given a non-elusive group G, we can ask whether or not G contains a derangement of order r for *every* prime divisor r of $|\Omega|$, or whether G contains a derangement of order 2 (when $|\Omega|$ is even), or a derangement of order r for the largest prime divisor r of $|\Omega|$, and so on.

In this book we will address questions of this nature for a particularly important family of finite permutation groups. Recall that a transitive group G as above is *primitive* if Ω is indecomposable, in the sense that there are no G-invariant partitions of Ω (except for the two trivial partitions $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$). The primitive permutation groups are the basic building blocks of all finite permutation groups, and they play a central role in permutation group theory. The structure of such a group is described by the O'Nan–Scott Theorem, which classifies the finite primitive permutation groups according to their socle and the action of a point stabiliser (see [94], for example). This theorem can often be used to reduce a general problem concerning primitive groups G to the so-called *almost simple* case, where

$$T \leqslant G \leqslant \mathrm{Aut}(T)$$

for a nonabelian simple group T (the socle of G). At this point, CFSG can be invoked to describe the possibilities for T (and thus G), and this can be combined with detailed information on the subgroup structure, conjugacy classes and representation theory of almost simple groups. When applicable, this reduction strategy is an extremely powerful tool in permutation group theory.

In [23], the O'Nan–Scott Theorem is used to reduce the problem of determining the r-elusive primitive permutation groups to the almost simple case. Now, according to CFSG, there are three possibilities for the socle T of an almost simple group:

(i) T is an alternating group A_n of degree $n \geqslant 5$;
(ii) T is one of 26 sporadic simple groups;
(iii) T is a simple group of Lie type.

All the r-elusive primitive groups arising in cases (i) and (ii) are determined in [23], so it remains to deal with the almost simple groups of Lie type, which are either *classical* or *exceptional*. Recall that the classical groups arise naturally from groups of invertible matrices defined over finite fields, and the exceptional groups can be constructed from the exceptional simple Lie algebras over $\mathbb{C}$, of type E_6, E_7, E_8, F_4 and G_2.

The purpose of this book is to provide a detailed analysis of derangements of prime order in primitive almost simple classical groups. In a strong sense, 'most' almost simple groups are classical, so our work is a major contribution to the project initiated in [23]. A summary of our main results will be presented in Chapter 1 (see Section 1.5), with more detailed statements available later in the text. In order to do this, we require detailed information on the subgroup structure and conjugacy classes of elements (of prime order) in finite almost simple classical groups. Indeed, observe that if G is a primitive permutation group with point stabiliser H, then H is a maximal subgroup of G, and an element $x \in G$ is a derangement if and only if the conjugacy class of x in G fails to meet H.

The study of the subgroup structure of an almost simple classical group G, and in particular its maximal subgroups, can be traced all the way back to Galois and his letter to Chevalier written on the eve of his fatal duel in 1832 [59]. More recently, in particular post-CFSG, there have been great advances in this area.

The main result is a theorem of Aschbacher from 1984. In [3], eight collections of 'natural', or *geometric*, subgroups of G are defined in terms of the underlying geometry of the natural (projective) module V for the socle of G. These subgroup collections include the stabilisers of appropriate subspaces and direct sum decompositions of V, for example. Given a subgroup H of G, Aschbacher proves that either H is contained in a member of one of these geometric collections, or H is almost simple and the socle of H acts absolutely irreducibly on V (and satisfies several additional conditions). Detailed information on the subgroups in the geometric collections (in terms of existence, structure, maximality and conjugacy) is given by Kleidman and Liebeck [86], and further details for the low-dimensional classical groups can be found in the recent book [13] by Bray, Holt and Roney-Dougal.

In this book, our analysis of derangements for geometric actions of classical groups is organised according to the subgroup collections arising in Aschbacher's theorem. Rather different methods are needed to study the remaining *non-geometric* actions of classical groups, and a detailed analysis of derangements in this situation will be given in a future paper.

In Chapters 2 and 3 we aim to provide the reader with an accessible introduction to the finite classical groups and their underlying geometry, with a particular focus on the conjugacy classes of elements of prime order. Our treatment is inevitably tailored towards the application to derangements, and we make no attempt to give a comprehensive introduction.

We start with a discussion of forms, standard bases and automorphisms, and we describe some specific classical group embeddings that will be useful later. A brief description of the subgroup collections arising in Aschbacher's theorem is provided in Section 2.6. Chapter 3 is dedicated to the study of conjugacy classes of elements of prime order in almost simple classical groups. Our main aim is to bring together a wide range of results on conjugacy classes that are somewhat scattered through the literature in this area. In particular, we provide a detailed analysis of involutions (both semisimple, unipotent and outer automorphisms), which complements important earlier work of Aschbacher and Seitz [5], and Gorenstein, Lyons and Solomon [67]. Of course, we require this information for the application to derangements given in Chapters 4, 5 and 6, but we hope that our treatment will be useful more generally, in a wide range of problems concerning finite permutation groups. For example, this sort of information has been essential in recent work on fixed point ratios and bases for primitive permutation groups (see [17, 18, 19, 20] and [21, 25, 26, 27, 28]), in the classification of almost simple extremely primitive groups and $\frac{3}{2}$-transitive groups (see [6, 29, 30]), and in a wide range of problems concerning the generation and random generation of finite simple groups (see [14, 24, 70], for example). In Chapter 5 we also determine the precise structure of some specific geometric maximal subgroups of classical groups, extending the analysis given in [86] (see Sections 5.3.2 and 5.5.1).

We hope that this book will be useful to graduate students and researchers who work with finite classical groups. Indeed, the background material in Chapters 2 and 3 will be accessible to graduate students with a basic understanding of linear algebra and group theory. In particular, we hope that our detailed treatment of conjugacy classes of elements of prime order will serve as a useful general reference. Our study of derangements of prime order in almost simple classical groups provides an immediate application, building naturally on the material presented in Chapters 2 and 3. We anticipate that the content of Chapters 4, 5 and 6 will appeal to researchers working in permutation group theory.

Finally, some words on the organisation of this book. Chapter 1 serves as a general introduction. Here we provide a brief survey of earlier work on derangements, we describe several applications and we present a summary of our main results on derangements in finite classical groups. The next two chapters provide a brief introduction to the finite classical groups, giving the necessary background information that we will need for the application to derangements investigated in Chapters 4, 5 and 6.

Our analysis of derangements of prime order in finite classical groups begins in Chapter 4, where we handle the so-called *subspace actions*. Guided by Aschbacher's structure theorem, the remaining geometric subgroup collections are studied in Chapter 5, together with a small additional collection of *novelty* subgroups that arises when G has socle $\mathrm{Sp}_4(q)'$ (q even) or $\mathrm{P}\Omega_8^+(q)$. Finally, in Chapter 6 we use our earlier work to present detailed results on derangements in the low-dimensional classical groups, including both geometric and non-geometric actions.

We also include two appendices. In Appendix A we record several number-theoretical results that will be needed in our analysis of conjugacy classes and derangements. Finally, in Appendix B we present various tables that conveniently summarise some of the information on conjugacy classes in finite classical groups discussed in Chapter 3.

Tim Burness and Michael Giudici, March 2015

Acknowledgements

Burness was supported by Engineering and Physical Sciences Research Council grant EP/I019545/1 and the Royal Society of London. He thanks the Centre for the Mathematics of Symmetry and Computation at the University of Western Australia for their generous hospitality during several visits.

Giudici was supported by Australian Research Council Discovery Project grant DP0770915, and he thanks the Schools of Mathematics at the University of Southampton and the University of Bristol for their generous hospitality.

Both authors thank Robert Guralnick and Martin Liebeck for their encouragement and helpful comments. They also thank Martin Liebeck and Gary Seitz for providing advanced access to their book [96] on unipotent and nilpotent classes, and they thank John Bray, Derek Holt and Colva Roney-Dougal for providing numerous details (pre-publication) from their book [13] on the subgroup structure of the low-dimensional finite classical groups.

Notational conventions

Group-theoretic notation

Let G and H be groups, n a positive integer, p a prime number.

$\lvert G\rvert$	order of G
G'	derived subgroup of G
$Z(G)$	centre of G
$\mathrm{soc}(G)$	socle of G (subgroup of G generated by its minimal normal subgroups)
G^∞	last term in the derived series of G
G^n	direct product of n copies of G
$H \leqslant G$	H is a subgroup of G
$H < G$	H is a proper subgroup of G
$\lvert G : H\rvert$	index of a subgroup H of G
$G.H$	an extension of G by H
$G{:}H$	a split extension of G by H
$G \wr H$	wreath product of G and H, $H \leqslant S_n$
$N_G(H)$	normaliser in G of H
$C_G(x)$	centraliser in G of x
x^G	G-conjugacy class of x
$\lvert x\rvert$	order of x
C_n or just n	cyclic group of order n
C_p^n or just p^n	elementary abelian group of order p^n
D_n	dihedral group of order n
S_n	symmetric group of degree n
A_n	alternating group of degree n
$[n]$	unspecified soluble group of order n

Other notation

$\mathbb{F}_q$	field of size q
$\mathbb{F}^\times$	nonzero elements of a field $\mathbb{F}$
$\overline{\mathbb{F}}$	algebraic closure of a field $\mathbb{F}$
$\mathbb{E}/\mathbb{F}$	$\mathbb{E}$ is a field extension of $\mathbb{F}$
$\mathscr{S}_r$	set of all nontrivial rth roots of unity in a field
$D(Q)$	discriminant of a quadratic form Q
$\Phi(r,q)$	smallest $i \in \mathbb{N}$ such that r divides $q^i - 1$
$\delta_{i,j}$	Kronecker delta
$(a_1,\ldots,a_t)$	greatest common divisor of integers $a_1,\ldots,a_t$
$[a_1,\ldots,a_t]$	least common multiple of integers $a_1,\ldots,a_t$
$(a)_b$	highest power of b dividing a, for integers a,b
a'	largest odd divisor of the integer a
$\mathbb{N}_0$	$\mathbb{N} \cup \{0\}$
A^T	transpose of a matrix A
$\lfloor x \rfloor$	largest integer $n \leqslant x$ ($x \in \mathbb{R}$)
$x - \varepsilon$	$x - \varepsilon 1$ with $\varepsilon = \pm$ ($x \in \mathbb{R}$)

Classical group notation

Our notation for classical groups is fairly standard, and we closely follow the notation used by Kleidman and Liebeck [86]. In particular, we write

$$\mathrm{PSL}_n^+(q) = \mathrm{PSL}_n(q), \;\; \mathrm{PSL}_n^-(q) = \mathrm{PSU}_n(q)$$

for the projective special linear and unitary groups of dimension n over $\mathbb{F}_q$, respectively. Specific notation for orthogonal groups will be defined in Section 2.5. We write $x = [x_1,\ldots,x_k]$ to denote a block-diagonal matrix $x \in \mathrm{GL}_n(q)$ with blocks $x_1,\ldots,x_k$. Furthermore, if the x_i are all equal then we write $x = [x_1^k]$. We use I_n for the identity matrix in $\mathrm{GL}_n(q)$, and we write J_n for the standard (lower-triangular) unipotent Jordan block of size n in $\mathrm{GL}_n(q)$. Further notation will be introduced as and when needed in the text.

Contents