Subgroups of the Symmetric Group of Degree n Containing an n -cycle

by

Joanne Charlebois, B.A.

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of
Master of Science

School of Mathematics and Statistics

Carleton University

Ottawa, Ontario

July 4, 2002

© 2002, Joanne Charlebois

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-79781-3

Canada

The undersigned recommend to
the Faculty of Graduate Studies and Research
acceptance of the thesis
**“Subgroups of the Symmetric Group
of Degree n Containing an n -cycle”**
submitted by Joanne Charlebois, B.A.
in partial fulfillment of the requirements for
the degree of Master of Science

Thesis supervisor

Director, School of Mathematics and Statistics

July 25, 2002

Abstract

This thesis addresses the question of which subgroups G of the finite symmetric group S_n contain an n -cycle.

The solution to the case $n = p$ a prime is based on a theorem of Burnside. When n is not prime, we apply a theorem based on results of Burnside and Schur to see that the groups G we are looking for are either imprimitive or 2-transitive. Using the Classification of Finite Simple Groups, we look at each possible group G and determine which do indeed contain an n -cycle.

We give a list of subgroups, maximal in S_n or in A_n , containing an n -cycle:

1. A_n , n odd;
2. $S_{n/m}wrS_m$ (with the standard action), for all m dividing n with $1 < m < n$;
3. $\text{PTL}(d, q)$, for all d, q with $n = (q^d - 1)/(q - 1)$;
4. $\text{AGL}(1, p)$, for $n = p$ a prime;
5. $\text{PSL}(2, 11)$ (in an exceptional action), for $n = 11$;
6. M_{11} , for $n = 11$;
7. M_{23} , for $n = 23$.

We also discuss some of this problem's applications.

Acknowledgements

I would like to thank my supervisor Dr. John Dixon for all the help, guidance, and support he has given me throughout my work on this thesis, my honours project, and three summer research projects.

I would also like to thank Dr. Brian Mortimer for lending me his copy of the Atlas of Finite Groups and for some helpful discussions about its contents.

And thank you to the government of Ontario for my Ontario Graduate Scholarship.

Contents

1	Introduction	1
2	The Classification of Finite Simple Groups	4
2.1	Simple groups of Lie type	5
2.1.1	Projective Special Linear Groups $\text{PSL}(d, q)$	7
2.1.2	Projective Special Unitary Groups $\text{PSU}(3, q)$	9
2.1.3	Suzuki Groups $Sz(q)$	10
2.2	Sporadic Simple Groups	12
3	The Subcases	15
3.1	The prime case $n = p$	18
4	The Imprimitive Case	21
5	The 2-Transitive Case	24
5.1	Affine Groups	24
5.2	Almost Simple Groups	26
6	Applications	35

List of Tables

2.1	The simple groups of Lie type	8
2.2	The sporadic simple groups	13
5.1	The almost simple 2-transitive groups	27

Chapter 1

Introduction

This thesis addresses the question of which subgroups of the finite symmetric group S_n contain an n -cycle.

In the case that n is odd, an n -cycle is an even permutation and so we have the rather trivial maximal subgroup A_n containing all the n -cycles of S_n . (And, of course, conversely A_n does not contain an n -cycle if n is even.)

When $n = p$ a prime, if p divides the order of the group, then the group certainly contains a p -cycle. In fact the solution to the case $n = p$ was known by Burnside, some examples of it having been discovered in the 1800's by Galois and Mathieu ([14, p. 97, p. 99]). This case is discussed further in Section 3.1.

As we shall see, when n is not prime a subgroup $G \leq S_n$ containing an n -cycle must be either imprimitive or 2-transitive. In Chapters 4 and 5 we then consider each such subgroup G to determine which contain the desired cycle.

In the 2-transitive case we assume the Classification of Finite Simple Groups (CFSG) in order to claim that our list is exhaustive. The Classification is discussed in Chapter 2.

We summarize our solution to the problem in the following theorem.

Theorem 1.1 *The subgroups G of S_n containing an n -cycle, with G maximal in*

either S_n or A_n , are:

1. A_n , n odd;
2. $S_{n/m} \text{wr} S_m$ (with the standard action), for all m dividing n with $1 < m < n$;
3. $\text{PTL}(d, q)$, for all d, q with $n = (q^d - 1)/(q - 1)$;
4. $\text{AGL}(1, p)$, for $n = p$ a prime;
5. $\text{PSL}(2, 11)$ (in an exceptional action), for $n = 11$;
6. M_{11} , for $n = 11$;
7. M_{23} , for $n = 23$.

Much of the interest of this question lies in its applications. Some of these are discussed in Chapter 6. We investigate when a subgroup of S_n generated by an n -cycle and certain elements of small order do not generate the full symmetric group. We investigate when such a subgroup can have the cyclic group $\mathbb{Z}_n$ or the dihedral group D_{2n} as a homomorphic image. We also survey some other applications that appear in the literature.

It has recently come to our attention that the primitive case of the problem considered in this thesis has been solved by Cai Heng Li in the preprint paper ([24]). Li solves the more general question of classifying finite primitive permutation groups containing an abelian regular subgroup. His results confirm ours.

We give some notational conventions followed throughout this thesis: p is a prime, q a prime power p^e , n is the degree of a representation being considered, and generally lowercase letters are integers, group elements, or polynomials. A capital Greek letter denotes a set, a lowercase Greek letter a set element, field element, or a function. Matrices are denoted by Roman capitals, and the identity matrix is denoted by I . The usual form for symmetric and alternating groups on n letters,

S_n and A_n respectively, are used, but occasionally we use $Sym(\Delta)$ and $Alt(\Delta)$ for some specific set Δ . The order of a group G is written $|G|$, and $G \rtimes H$ denotes a semidirect product of a group G by a group H . The multiplicative group of nonzero elements of a field F is written F^* .

Chapter 2

The Classification of Finite Simple Groups

The finite simple groups are important because every finite group can be obtained from successive extensions of simple groups.

According to the Classification of Finite Simple Groups (CFSG), the nonabelian simple groups can be classified as follows.

Theorem 2.1 *A non-abelian finite simple group is one of the following:*

1. *an alternating group A_n , $n \geq 5$;*
2. *a group of Lie type;*
3. *one of 26 sporadic groups.*

Though the result was announced by Gorenstein in 1979 ([11, p. 3]), the proof was not entirely complete; there were some problems with “quasi-thin groups” and “groups of Ree type” for example. The proof was about 15 000 pages of work contained in many different journals, books, even computer calculations and unpublished research notes. Currently a team of mathematicians including Richard

Lyons and Ronald Solomon are continuing the task they began with the late Daniel Gorenstein of writing a complete and self-contained proof of the CFSG. The first four volumes of their work have appeared ([17]), and it is estimated that the total length of the proof will be about 5000 pages.

The CFSG has many consequences for finite group theory. Some of these consequences are rather deep, like the Schreier conjecture, and have not yet been proved without relying on the CFSG. The Schreier conjecture states that the outer automorphism group of a nonabelian finite simple group is solvable. For more applications of the CFSG, see [4, §4.7-4.12] and W. Feit's paper [11, p.175].

The theorem concerns non-abelian simple groups; the abelian simple groups are clearly just the (cyclic) groups of prime order. The alternating groups are well known; Galois knew these were simple for $n \geq 5$.

We now discuss the groups of Lie type and the sporadic groups, focusing on several groups that will be of interest in Chapter 5.

2.1 Simple groups of Lie type

The groups of Lie type are divided into 6 infinite families of *classical groups*, each parametrized by a dimension d and a field order q , and 10 infinite families of *exceptional groups*, each parametrized by a field order q . They are listed in Table 2.1. The classical groups have been known by that name since H. Weyl's book [42] of the same name appeared in 1939. The exceptional groups behave like classical groups of fixed dimension.

The groups of Lie type can also be divided into the categories of *Chevalley groups* and *twisted Chevalley groups*, which include and generalize the classical linear, unitary, symplectic, and orthogonal groups. In 1955 Claude Chevalley discovered a way of defining bases for Lie algebras that allowed them and their corresponding Lie groups (called *adjoint Chevalley groups*) to be defined over arbitrary fields rather

than just over $\mathbb{C}$ ([7]).

The complex Lie algebras are denoted

$$A_d, B_d, C_d, D_d, G_2, F_4, E_6, E_7, E_8$$

(where we specify $d \geq 1, 2, 3, 4$ for A_d, B_d, C_d, D_d respectively to avoid repetitions).

The corresponding groups are

$$A_d(q), B_d(q), C_d(q), D_d(q), G_2(q), F_4(q), E_6(q), E_7(q), E_8(q)$$

(note that $G_2(q), F_4(q)$ were written $E_2(q), E_4(q)$ by a few authors).

Steinberg modified Chevalley's procedure in 1959 and the twisted Chevalley groups

$${}^2A_d(q), {}^2D_d(q), {}^3D_4(q), {}^2E_6(q)$$

resulted. The groups ${}^3D_4(q), {}^2E_6(q)$ had not been discovered before Steinberg's work, which was published in [37].

The other twisted Chevalley groups, the Suzuki groups ${}^2B_2(q)$ and the Ree groups ${}^2G_2(q), {}^2F_4(q)$, arise from a different modification of Chevalley's technique. These groups were discovered in 1960 and 1961 ([38], [32], [33]). Note the first Ree group ${}^2F_4(2)$ is not simple; it is ${}^2F_4(2) = T \rtimes 2$ where $T = {}^2F'_4(2)$ is a simple group not appearing elsewhere in Table 2.1. The group T is known as Tits' group after Jacques Tits who originally discovered it.

The term "twisted" refers to how these groups arise from automorphisms of the *Dynkin diagrams* corresponding to each adjoint Chevalley group; for more information on Chevalley theory see [7], [8], [5], [6], [17].

The groups listed in Table 2.1 are simple except that $\text{PSU}(3, 2)$ is solvable, and $\text{PSL}(2, 2) \cong S_3$, $\text{PSL}(2, 3) \cong A_4$. The other groups are nonisomorphic, nonabelian simple groups not isomorphic to alternating groups with the following exceptions: $\text{PSL}(2, 4) \cong \text{PSL}(2, 5) \cong A_5$, $\text{PSL}(2, 7) \cong \text{PSL}(3, 2)$, $\text{PSL}(2, 9) \cong A_6$, $\text{PSL}(4, 2) \cong A_8$, $\text{PSp}(4, 2) \cong S_6$, $\text{PSU}(4, 2) \cong \text{PSp}(4, 3)$. In Table 2.1 we use the convention

started by Artin that families of (generally) simple groups such as $\text{PSU}(d, q)$ be given single-letter names, hence $U_d(q)$. A few authors do not use this convention and may use $U_d(q)$ to denote $\text{GU}(d, q)$ for example.

For the orders of the groups in Table 2.1, see e.g. [17, Vol. 1], [9], [19], or [4, p. 191].

We now describe the groups $\text{PSL}(d, q)$, $\text{PSU}(3, q)$, and $Sz(q)$ in more detail, as we need some details about them in Chapter 5.

2.1.1 Projective Special Linear Groups $\text{PSL}(d, q)$

The *general linear group* $\text{GL}(d, q)$ is the familiar group of invertible $d \times d$ matrices with entries in the field $\mathbb{F}_q$. Its subgroup of matrices with determinant 1 is the *special linear group* $\text{SL}(d, q)$. The projective groups $\text{PGL}(d, q)$ and $\text{PSL}(d, q)$ are obtained by factoring $\text{GL}(d, q)$ and $\text{SL}(d, q)$ by their respective centres, which consist of the scalar matrices of each group.

As mentioned earlier, the groups $\text{PSL}(d, q)$ for $d \geq 2$ are simple except for the cases $(d, q) = (2, 2), (2, 3)$ (isomorphic to S_3 and A_4 respectively), and a few of these projective linear groups are isomorphic. The group $\text{PSL}(d, q)$ is also sometimes called $L_d(q)$ following Artin's convention of giving single-letter names to groups that are generally simple, and in Chevalley's notation is written $A_{d-1}(q)$.

For $d \geq 3$ the projective groups act naturally on the projective geometry $\text{PG}(d-1, q)$ which is constructed as follows using the linear action of $\text{GL}(d, q)$. When the group $\text{GL}(d, q)$ acts on the set $(\mathbb{F}_q)^d$ of row vectors by right multiplication it has two orbits, $\{0\}$ and $\Omega = (\mathbb{F}_q)^d \setminus \{0\}$. The action on Ω is imprimitive; the blocks consist of all nonzero multiples of a given vector. (The definition of *imprimitive* is recalled in Chapter 3.) Each such block is a *projective point* of the projective geometry $\text{PG}(d-1, q)$, and the point containing the vector $(\alpha_1, \dots, \alpha_d)$ is written $[\alpha_1, \dots, \alpha_d]$. (These coordinates, where a scalar multiple denotes the same point, and there is no point with all coordinates zero, are called *homogeneous coordinates*.) The group

Chevalley groups	Common name	Notation(s)	Condition
Classical	Projective special linear	$\mathrm{PSL}(d+1, q) = A_d(q)$ $= L_{d+1}(q)$	$d \geq 1$
Classical	Orthogonal	$\mathrm{P}\Omega(2d+1, q) = B_d(q)$ $= O_{2d+1}(q)$	$d \geq 2$
Classical	Symplectic	$\mathrm{PSp}(2d, q) = C_d(q)$ $= S_{2d}(q)$	$d \geq 3, q$ odd
Classical	Orthogonal	$\mathrm{P}\Omega^+(2d, q) = D_d(q)$ $= O_{2d}^+(q)$	$d \geq 4$
Exceptional		$E_6(q)$	
Exceptional		$E_7(q)$	
Exceptional		$E_8(q)$	
Exceptional		$F_4(q)$	
Exceptional		$G_2(q)$	
Steinberg groups			
Classical	Projective special unitary	$\mathrm{PSU}(d+1, q) = {}^2A_d(q^2)$ $= U_{d+1}(q)$	$d \geq 2$
Classical	Orthogonal	$\mathrm{P}\Omega^-(2d, q) = {}^2D_d(q^2)$ $= O_{2d}^-(q)$	$d \geq 4$
Exceptional		${}^2E_6(q^2)$	
Exceptional		${}^3D_4(q^3)$	
Suzuki & Ree groups			
Exceptional	Suzuki	$Sz(q) = {}^2B_2(q)$	$q = 2^{2d+1}$
Exceptional	Ree	$R_1(q) = R(q) = {}^2G_2(q)$	$q = 3^{2d+1}$
Exceptional	Ree	$R_2(q) = R(q) = {}^2F_4(q)$	$q = 2^{2d+1}$

Table 2.1: The simple groups of Lie type

$\mathrm{GL}(d, q)$ has a permutation action on the set of projective points since these form a set of blocks for the group. The kernel of this action is the subgroup Z of scalars in $\mathrm{GL}(d, q)$. Thus the image of the action on the blocks (i.e. on the projective points of $\mathrm{PG}(d-1, q)$) is the group $\mathrm{GL}(d, q)/Z = \mathrm{PGL}(d, q)$, which therefore acts faithfully on the blocks. The number of blocks, that is the degree of the action, is $n = (q^d - 1)/(q - 1)$. For $d \geq 3$, the group $\mathrm{PGL}(d, q)$ is 2-transitive on the set of points of $\mathrm{PG}(d-1, q)$.

The full automorphism group of $\mathrm{PG}(d-1, q)$ ($d \geq 3$) is larger, in general, than $\mathrm{PGL}(d, q)$. This automorphism group is the normalizer in S_n of $\mathrm{PSL}(d, q)$; it is the *projective special linear group* $\mathrm{P\Gamma L}(d, q)$ (see [1, Thm. 2.26]). It is generated by two types of automorphisms: those induced by each element of $\mathrm{GL}(d, q)$ in the action described above, and those induced by each field automorphism σ of $\mathbb{F}_q$, via $[\alpha_1, \dots, \alpha_d] \mapsto [\alpha_1^\sigma, \dots, \alpha_d^\sigma]$. (So when $q = p$ a prime, $\mathrm{P\Gamma L}(d, q)$ coincides with $\mathrm{PGL}(d, q)$.)

2.1.2 Projective Special Unitary Groups $\mathrm{PSU}(3, q)$

This group is actually a subgroup of $\mathrm{PGL}(3, q^2)$ (and by a few authors it is denoted $\mathrm{PSU}(3, q^2)$ instead of $\mathrm{PSU}(3, q)$).

Let V be the 3-dimensional vector space over $\mathbb{F}_{q^2}$. The automorphism $\bar{\cdot} : \xi \mapsto \xi^q$ of $\mathbb{F}_{q^2}$ has order 2 and gives us a hermitian form $\phi : V \times V \rightarrow \mathbb{F}_{q^2}$. (Recall *hermitian* means that for all $u, v \in V$ and all $\alpha, \beta \in \mathbb{F}_{q^2}$,

$$\phi(\alpha u, \beta v) = \alpha \beta^q \phi(u, v) \text{ and } \phi(u, v) = \phi(v, u)^q.)$$

The elements of $\mathrm{GL}(3, q^2)$ preserving the given hermitian form make up a subgroup $\mathrm{GU}(3, q)$, the *general unitary group*. (So $A \in \mathrm{GL}(3, q^2)$ belongs to $\mathrm{GU}(3, q)$ if and only if $\phi(u, v) = \phi(u^A, v^A)$ for all $u, v \in V$; equivalently $A^{-1} = \bar{A}^T$.) The *special unitary group* $\mathrm{SU}(3, q)$ consists of those matrices in $\mathrm{GU}(3, q)$ having determinant 1.

The unitary group $\mathrm{GU}(3, q)$ induces an action on the set of 1-dimensional subspaces of V . Letting Z denote the scalar matrices of $\mathrm{GU}(3, q)$, the induced group is $\mathrm{PGU}(3, q) = \mathrm{GU}(3, q)/Z$, the *projective general unitary group*. The group $\mathrm{PGU}(3, q)$ has a subgroup $\mathrm{PSU}(3, q) = \mathrm{PGU}(3, q) \cap \mathrm{PSL}(3, q^2)$, the *projective special unitary group* consisting of elements with determinant 1. Similarly to $\mathrm{PGL}(d, q) \leq \mathrm{P}\Gamma\mathrm{L}(d, q)$, $\mathrm{PGU}(3, q)$ is a subgroup of $\mathrm{P}\Gamma\mathrm{U}(3, q)$ which is obtained by adding in the field automorphisms of $\mathbb{F}_{q^2}$. The group $\mathrm{PSU}(3, q)$ has index $\gcd(3, q+1)$ in $\mathrm{PGU}(3, q)$, and $[\mathrm{P}\Gamma\mathrm{U}(3, q) : \mathrm{PGU}(3, q)] = 2e$ where $q = p^e$. For $q > 2$, $\mathrm{PSU}(3, q)$ is simple; hence it is also denoted by $U_3(q)$. In the Chevalley notation based on the underlying Lie algebra, it is denoted by ${}^2A_2(q^2)$. As noted earlier, $\mathrm{PSU}(3, 2)$ is solvable.

The projective unitary groups act on a set Ω of $q^3 + 1$ 1-dimensional subspaces of the set of isotropic vectors in V . A vector $v \in V$ is *isotropic* if $\phi(v, v) = 0$. A scalar multiple of an isotropic vector is also isotropic so we get the set of 1-dimensional subspaces $\Omega = \{\langle v \rangle \mid \phi(v, v) = 0\}$. The set Ω is left invariant by elements of the projective unitary groups and the action on Ω is 2-transitive (see e.g. [14, p. 249]).

2.1.3 Suzuki Groups $Sz(q)$

Michio Suzuki discovered this family of groups in 1959 while trying to characterize *Zassenhaus groups*, which are permutation groups G with the following properties:

1. G is 2-transitive;
2. every non-identity element of G has at most two fixed points;
3. G has no regular normal subgroup.

(Recall a permutation group is *regular* if only the identity fixes any point.)

The only known Zassenhaus groups before Suzuki made his discovery were the groups $\mathrm{PGL}(2, q)$ with $q \geq 3$. It is now known that these groups and the Suzuki

groups $Sz(q)$ are all the Zassenhaus groups ([21, p. 163]).

Let $q = 2^{2d+1}$, $d > 0$, and let π be the automorphism of $\mathbb{F}_q$ given by $\xi^\pi = \xi^{2^{d+1}}$ (so that $\xi^{\pi^2} = \xi^2$). The Suzuki group $Sz(q)$ is a subgroup of $GL(4, q)$ ([21, pp. 183-184]), defined as follows:

$$Sz(q) := \langle S(\alpha, \beta), M(\xi), T \mid \alpha, \beta \in \mathbb{F}_q, \xi \in \mathbb{F}_q^* \rangle$$

where the generators are

$$S(\alpha, \beta) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 1 & 0 & 0 \\ \beta & \alpha^\pi & 1 & 0 \\ \alpha^2(\alpha^\pi) + \alpha\beta + \beta^\pi & \alpha(\alpha^\pi) + \beta & \alpha & 1 \end{pmatrix},$$

$$M(\xi) := \begin{pmatrix} \xi^{1+2^d} & 0 & 0 & 0 \\ 0 & \xi^{2^d} & 0 & 0 \\ 0 & 0 & \xi^{-2^d} & 0 \\ 0 & 0 & 0 & \xi^{-1-2^d} \end{pmatrix}, \text{ and}$$

$$T := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The group $Sz(q)$ acts on the set $\mathcal{O}$, defined as follows. In the projective space $PG(3, q)$, denote

$$p_\infty = [1, 0, 0, 0], \quad p(\xi, \zeta) = [\xi\zeta + (\xi^\pi)\xi^2 + \zeta^\pi, \zeta, \xi, 1]$$

in homogeneous coordinates. Then

$$\mathcal{O} = \{p_\infty, p(\xi, \zeta) \mid \xi, \zeta \in \mathbb{F}_q\}.$$

The group $Sz(q)$ is simple and is faithfully represented and 2-transitive on the set $\mathcal{O}$ ([21, pp. 185, 188]).

2.2 Sporadic Simple Groups

These groups are finite simple groups that are not members of infinite families. They are listed in Table 2.2. The “Date” column refers to the date the group was predicted to exist, for some of these groups were not proven to exist until several years after their existence was conjectured.

The first-known sporadic groups were the Mathieu groups discovered by E. Mathieu in the 1800’s. All the smaller Mathieu groups are contained in M_{24} . Mathieu did not know that M_{12} was contained in M_{24} ; it was Frobenius who first realized this, and who first calculated the character table for M_{24} . The largest of the Mathieu groups is quite important; many properties of larger sporadic groups reduce to properties of M_{24} .

The group Co_1 , named after its discoverer J.H. Conway, is the automorphism group of the *Leech lattice*. The Leech lattice is a lattice in 24-dimensional real space (it can be described in terms of M_{24}). The groups Co_2 , Co_3 , McL , HS , Suz , HJ can also be obtained from the Leech lattice.

B. Fischer discovered his groups Fi_n , $n = 22, 23, 24$, while classifying all 3-*transposition groups*, groups generated by a conjugacy class of involutions whose pairwise products have orders less than or equal to 3.

The Monster, also called the Friendly Giant, is the largest sporadic group and was discovered independently by Fischer and R. Griess. Many of the other sporadic groups can be described in terms of the Monster, for example as the nonabelian composition factors of the centralizers of certain Monster elements. (The groups in Table 2.2 with alternate notations F_i are some of these groups.) The structure of the Monster, like that of many of the other sporadic groups, is related to M_{24} .

The groups J_1 , J_3 , J_4 , Ru , ON , Ly can be most easily constructed as matrix groups of dimension d over finite fields of order f with $(d, f) = (7, 11), (9, 4), (112, 2), (28, 2), (45, 7), (111, 5)$ respectively.

Group	Notation(s)	Order	Date
Mathieu	M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	1861
Mathieu	M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	1861
Mathieu	M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	1873
Mathieu	M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	1873
Mathieu	M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	1873
Janko	J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	1964
Hall-Janko	$J_2 = HJ$	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	1967
Suzuki	Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1967
Higman-Sims	HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	1967
McLaughlin	$McL = Mc$	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	1967
Conway	$Co_3 = .3$	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	1968
Conway	$Co_2 = .2$	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	1968
Conway	$Co_1 = .1$	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	1968
Janko	J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	1968
Fischer	Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1968
Held	$He = F_7$	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	1969
Fischer	Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	1969
Fischer	Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	1969
Lyons	Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	1971
Rudvalis	Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	1972
O'Nan	$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	1973
Harada-Norton	$HN = F_5$	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	1974
Thompson	$Th = F_3$	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	1974
Baby Monster	$B = BM = F_2$	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ $\cdot 31 \cdot 47$	1975
Monster	$M = FG = F_1$	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23$ $\cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	1975
Janko	J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	1975

Table 2.2: The sporadic simple groups

For more information on the sporadic groups, see [10], [9], [40].

We shall see later that the only groups from Table 2.2 that we are concerned with are the Mathieu groups M_{11} , M_{22} , M_{23} . We now describe these.

The groups M_{11} and M_{23} have their natural actions of prime degrees 11 and 23 respectively (these groups are mentioned in Section 3.1 in addition to in Chapter 5). The former is a point stabilizer of M_{12} , the latter of M_{24} . The group M_{22} has its natural action of degree 22, and is a point stabilizer of M_{23} , i.e. it is a 2-point stabilizer of M_{24} .

In order to describe these groups we first define Steiner systems. A *Steiner system* $S(t, k, v)$ is a finite set Ω of size v , with a set $\mathcal{B}$ of subsets of Ω called *blocks* (not to be confused with blocks of imprimitivity), each of size k , such that for the integer t (with $t < k < v$), each subset of Ω of size t lies in exactly one block of $\mathcal{B}$.

The Mathieu groups arise as automorphism groups of certain Steiner systems; M_{11} acts 4-transitively on an $S(4, 5, 11)$ Steiner system denoted by W_{11} , M_{23} acts 4-transitively on an $S(4, 7, 23)$ Steiner system denoted by W_{23} , and M_{22} acts 3-transitively on an $S(3, 6, 22)$ Steiner system denoted by W_{22} . (These systems are also called *Witt geometries*.) In fact W_{11} , W_{23} , and W_{22} are the unique $S(4, 5, 11)$, $S(4, 7, 23)$, and $S(3, 6, 22)$ Steiner systems respectively ([14, p. 190, p.202]). We have $M_{11} = \text{Aut}(W_{11})$, $M_{23} = \text{Aut}(W_{23})$, and $[\text{Aut}(W_{22}) : M_{22}] = 2$.

Chapter 3

The Subcases

In this chapter we break the problem down into subcases by applying several theorems. We also discuss the case when the degree is prime.

Suppose we have $G \leq S_n$ containing an n -cycle x . We begin by noting some observations about the subgroup $R = \langle x \rangle$ generated by the n -cycle. The cyclic subgroup R is clearly regular and abelian, and has a Sylow p -subgroup for primes p dividing n . When n is not a prime we can apply the following theorem from [14, p. 95], which is based on results of Burnside and Schur ([3] and [36] respectively) which were generalized by Wielandt (see [43]).

Theorem 3.1 *Let G be a permutation group of degree n containing a regular subgroup R . Suppose that R is abelian and has a cyclic Sylow p -subgroup for some prime p with $p < n$. Then G is either imprimitive or 2-transitive.*

So we see that the groups in which we are interested are either imprimitive or 2-transitive. Recall that a transitive permutation group G is *imprimitive* if the set Ω on which it acts has a partition into equal-sized subsets (each of size greater than 1)

$$\Omega = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_m$$

with $m > 1$ and with the following property: for every i and every $x \in G$, $\Omega_i^x = \Omega_j$ for some j . Otherwise G is *primitive*. Recall that a permutation group is *2-transitive* if for every $\alpha, \beta, \gamma, \delta \in \Omega$, with $\alpha \neq \gamma$, $\beta \neq \delta$, there exists $x \in G$ such that $\alpha^x = \beta$, $\gamma^x = \delta$.

These two properties are mutually exclusive; indeed, in a 2-transitive group, for any partition $\Omega = \cup_i \Omega_i$, take $\alpha, \gamma \in \Omega_i, \beta \in \Omega_j, \delta \in \Omega_k$ with $j \neq k$ and take $x \in G$ such that $\alpha^x = \beta$, $\gamma^x = \delta$. Clearly the group is primitive.

Now we approach the question from a different perspective: we want to look for maximal subgroups of S_n . The following theorem from [4, p. 107] is actually the original form of the famous O’Nan-Scott Theorem which was announced in 1979 ([11, p. 319]).

Theorem 3.2 *A maximal subgroup of S_n is one of the following;*

1. *intransitive, $S_k \times S_l$, $k + l = n$;*
2. *transitive imprimitive, $S_k wr S_l$ (with the standard action), $kl = n$;*
3. *primitive non-basic, $S_k wr S_l$ (with the product action), $k^l = n, k \neq 2$;*
4. *affine, $AGL(d, p)$, $p^d = n$;*
5. *diagonal, $T^k \rtimes (\text{Out}(T) \times S_k)$, T non-abelian simple, $|T|^{k-1} = n$;*
6. *almost simple.*

For the definitions of the terms basic, diagonal, and product action, see [4, §4.3-4.4].

Note that a maximal subgroup of A_n is the intersection of one of the above groups with A_n . This theorem gives necessary but not sufficient conditions for maximality; Liebeck, Praeger, and Saxl have listed all the exceptions to maximality in [26].

An earlier theorem which appears as a special case (the 2-transitive case) of the full O’Nan-Scott Theorem is the following theorem of Burnside ([3]). Recall that

the *socle* $\text{soc}(G)$ of a group G is the subgroup generated by its minimal normal subgroups (a normal subgroup N of G is *minimal* if $N \neq 1$ and N does not properly contain any other nontrivial normal subgroup of G). Clearly every finite group $G \neq 1$ has $\text{soc}(G) \neq 1$.

Theorem 3.3 *The socle of a finite 2-transitive permutation group is either a regular elementary abelian p -group, or a nonregular, nonabelian simple group acting primitively.*

Now the groups in Theorem 3.2 that are also either imprimitive or 2-transitive are those groups we want to consider.

Clearly the groups in case 1 of Theorem 3.2 do not have n -cycles; these groups are intransitive.

Case 2 of the theorem gives the imprimitive groups; we will be looking at this case in Chapter 4. This is the only case where the groups are imprimitive: if G is imprimitive of degree n with blocks $\Omega_1, \dots, \Omega_l$ of size k , then G is maximal imprimitive with respect to these blocks if and only if it contains all the permutations that either individually fix each of the blocks or interchange the blocks setwise. In this case G is permutation isomorphic to $S_k \wr S_l$ with the standard action.

Case 3 gives primitive non-basic groups; 2-transitive groups must be basic ([4, p. 110]) so these groups are not under consideration.

The affine groups of case 4 have elementary abelian socle and make up one case of Theorem 3.3. We study affine groups in Section 5.1.

The diagonal groups of case 5 are not 2-transitive ([4, p. 110]) and they are primitive by construction ([14, §4.5]), so we need not consider them.

Case 6 gives the almost simple groups. A group G is *almost simple* if it is of the form $T \leq G \leq \text{Aut}(T)$ for some simple group T . (Equivalently G has simple socle.) The almost simple 2-transitive groups make up the other case of Theorem 3.3 and are studied in Section 5.2.

We now conclude this chapter with a description of the $n = p$ prime degree case.

3.1 The prime case $n = p$

For convenience we consider G to be acting on the finite field $\mathbb{F}_p$ so that the permutations of $\text{Sym}(\mathbb{F}_p)$ are just polynomial functions, and in particular a p -cycle is (conjugate to) the function $\phi : \xi \mapsto \xi + 1$.

We have the following theorem due to Burnside, from [14, p. 97].

Theorem 3.4 *Let G be a subgroup of $\text{Sym}(\mathbb{F}_p)$ containing the p -cycle $\phi : \xi \mapsto \xi + 1$. Then G is either 2-transitive or $G \leq \text{AGL}(1, p)$.*

Clearly every transitive permutation group of prime degree p contains a p -cycle; indeed the degree of the (irreducible) representation divides the order of the group, so when that degree is a prime p we get an element of order p in the group (necessarily a cycle as p is prime).

The group $\text{AGL}(1, p)$ is a subgroup of $\text{Sym}(\mathbb{F}_p)$ consisting of the permutations of the form

$$t_{\alpha, \beta} : \xi \mapsto \alpha\xi + \beta$$

for $\alpha, \beta \in \mathbb{F}_p$ with $\alpha \neq 0$. It is easy to see that this is indeed a subgroup; it is called the 1-dimensional *affine group* over $\mathbb{F}_p$. The order of $\text{AGL}(1, p)$ is $p(p - 1)$ since there are p choices for the element β and $p - 1$ choices for the element α . The group $\text{AGL}(1, p)$ is 2-transitive but has no 2-transitive proper subgroup.

Using the CFSG the finite 2-transitive groups have been determined (see Chapter 5) and consequently the above theorem implies that a transitive group of degree p is one of the following groups ([14, p. 99]):

1. the symmetric group S_p or the alternating group A_p ;
2. a subgroup of $\text{AGL}(1, p)$;

3. the exceptional permutation representation of $\text{PSL}(2, 11)$ of degree 11;
4. the Mathieu groups M_{11} or M_{23} in their natural representations of degrees 11 and 23, respectively;
5. a projective group G with $\text{PSL}(d, q) \leq G \leq \text{PFL}(d, q)$ when the degree $(q^d - 1)/(q - 1)$ is prime.

The groups listed, being transitive, always contain a p -cycle.

For the projective groups in the list, it is conjectured that there are infinitely many primes p of the form $(q^d - 1)/(q - 1)$, but this has never been proved. (Note every Mersenne prime is of this form.) The group $\text{PSL}(d, q)$ was described in Section 2.1, and the projective linear case of our problem, when the degree need not be prime, is discussed in Section 5.2.

We conclude this section by describing the exceptional representation of degree 11 of the group $\text{PSL}(2, 11)$; note that M_{11} and M_{23} were described in Section 2.2.

The natural action of $\text{PSL}(2, 11)$ is of degree 12. Its action of degree 11 arises from the exceptional 3-transitive action of the Mathieu group M_{11} on 12 points. The point stabilizers here are isomorphic to $\text{PSL}(2, 11)$; hence the exceptional 2-transitive action of degree 11 of $\text{PSL}(2, 11)$. This action can be constructed as follows (see [14, p. 231] for more details). Let $\Delta := \{\alpha, \beta, \gamma, \delta, \varepsilon\}$ and look at the action of $\text{Alt}(\Delta)$ on the set

$$\begin{aligned} \Omega := \{ & 0 := \{\delta, \varepsilon\}, 1 := \{\alpha, \varepsilon\}, 2 := \{\alpha, \beta\}, 3 := \{\beta, \gamma\}, 4 := \{\gamma, \delta\}, \\ & 5 := \{\alpha, \gamma\}, 6 := \{\beta, \delta\}, 7 := \{\gamma, \varepsilon\}, 8 := \{\alpha, \delta\}, 9 := \{\beta, \varepsilon\} \}. \end{aligned}$$

Observe the images of the following elements of $\text{Alt}(\Delta)$ under this action:

$$\begin{aligned} (\beta\gamma)(\varepsilon\delta) &\mapsto x := (18)(25)(49)(67) \\ (\alpha\delta)(\beta\gamma) &\mapsto y := (01)(24)(56)(79). \end{aligned}$$

Then we have $H := \langle x, y \rangle \cong \text{Alt}(\Delta)$. Let ∞ be a point not in Ω and put $z := (\infty 0)(35)(48)(79)$. Then $G := \langle H, z \rangle$ is a 2-transitive group of degree 11 and order $11 \cdot 10 \cdot 6$; it is isomorphic to $\text{PSL}(2, 11)$.

Chapter 4

The Imprimitve Case

We begin this section by recalling some definitions and basic concepts. The definition of *imprimitve* was recalled in Chapter 3.

Consider two groups H and K and a group action of H on K (denoted by $k \mapsto k^h$ where $k, k^h \in K$ and $h \in H$) which respects the group structure of K . Then the *semidirect product* of K by H is the group

$$G = K \rtimes H = \{(k, h) \mid k \in K, h \in H\}$$

with the product on G given by

$$(k, h)(l, g) := (kl^{h^{-1}}, hg)$$

for all $(k, h), (l, g) \in G$.

For a non-empty set Γ and a group K we consider the set $F = \text{Fun}(\Gamma, K)$ of all functions from Γ to K . We define a pointwise product to turn F into a group as follows:

$$(fg)(\gamma) = f(\gamma)g(\gamma) \text{ for all } f, g \in F \text{ and } \gamma \in \Gamma.$$

Now suppose we also have a group H which acts on Γ . Then the *wreath product* $Kwr_\Gamma H$ is the semidirect product $F \rtimes H$, where H acts on F by the action

$$f^h(\gamma) := f(\gamma^{h^{-1}}) \text{ for all } f \in F, \gamma \in \Gamma, \text{ and } h \in H.$$

When $G = Kwr_{\Gamma}H$ and K acts on a set Δ , then we define an action of G on $\Delta \times \Gamma$ by

$$(\delta, \gamma)^{(f, h)} := (\delta^{f(\gamma)}, \gamma^h)$$

for all $(\delta, \gamma) \in \Delta \times \Gamma$ and $(f, h) \in \text{Fun}(\Gamma, K) \rtimes H = Kwr_{\Gamma}H$. This action is used in the theorem below.

With these definitions recalled, we turn to the theorem of this chapter.

Theorem 3.2 shows that the maximal imprimitive subgroups of S_n have the form $S_{n/m}wrS_m$ with the standard action and $m \mid n$, $1 < m < n$.

Theorem 4.1 *Every subgroup of the form $S_{n/m}wrS_m$ with the standard action contains an n -cycle.*

Proof: Put $d := n/m$.

Let $\phi : \{1, 2, \dots, m\} \rightarrow S_d$ be such that

$$\begin{aligned} \phi(1) &= (12 \dots d) \text{ and} \\ \phi(\gamma) &= () \text{ for } \gamma \neq 1, \end{aligned}$$

where $()$ denotes the identity permutation of S_d . Let $x = (12 \dots m)$ in S_m .

Then we claim $(\phi, x) \in S_dwrS_m$ is an n -cycle on the elements of $\Omega := \{1, \dots, d\} \times$

$\{1, \dots, m\}$. Indeed, writing $((\alpha, \beta))$ for an element of Ω , we have

$$\begin{aligned}
 ((1, 1))^{(\phi, x)} &= ((2, 2)) \\
 ((2, 2))^{(\phi, x)} &= ((2, 3)) \\
 &\vdots \\
 ((2, m))^{(\phi, x)} &= ((2, 1)) \\
 ((2, 1))^{(\phi, x)} &= ((3, 2)) \\
 ((3, 2))^{(\phi, x)} &= ((3, 3)) \\
 &\vdots \\
 ((d, m))^{(\phi, x)} &= ((d, 1)) \\
 ((d, 1))^{(\phi, x)} &= ((1, 2)) \\
 ((1, 2))^{(\phi, x)} &= ((1, 3)) \\
 &\vdots \\
 ((1, m))^{(\phi, x)} &= ((1, 1))
 \end{aligned}$$

which shows that (ϕ, x) cycles through all n points of Ω . $\square$

This completes the solution in the imprimitive case. The 2-transitive case is more complicated, as we see in the next chapter.

Chapter 5

The 2-Transitive Case

As we saw in Chapter 3, the 2-transitive maximal subgroups of S_n are either affine, $\text{AGL}(d, p)$ with p prime and $p^d = n$, or are almost simple (i.e. have simple socle). This chapter classifies the groups from each of these two cases that have an n -cycle.

5.1 Affine Groups

Theorem 3.2 tells us that a maximal affine subgroup of S_n looks like $\text{AGL}(d, p)$ where $p^d = n$.

We begin by describing the affine group $\text{AGL}(d, q)$ where $q = p^e$ for a prime p . This group acts on the *affine geometry* $\text{AG}(d, q)$ which consists of points and affine subspaces. The points of this geometry are the elements of the vector space $V := (\mathbb{F}_q)^d$, and the affine subspaces are the sets of translates of m -dimensional subspaces of V for each $m \leq d$. That is, if S is an m -dimensional subspace of V , then $S + v := \{u + v \mid u \in S\}$ is an m -dimensional affine subspace for each $v \in V$. An affine automorphism is a permutation of the points such that each affine subspace is mapped to an affine subspace of the same dimension.

The *affine general linear group* $\text{AGL}(d, q)$ consists of the affine automorphisms

of the form

$$t_{A,v} : u \mapsto uA + v, \text{ for all } A \in \text{GL}(d, q), v \in V.$$

(The automorphisms of this form are called *affine transformations*.) This group is 2-transitive on the points of $\text{AG}(d, q)$. We have $\text{AGL}(d, q) \cong P \rtimes \text{GL}(d, q)$, a semidirect product of the elementary abelian p -subgroup $P = \{t_{I,v} \mid v \in V\}$ of order q^d by a subgroup isomorphic to $\text{GL}(d, q)$.

The group $\text{AGL}(d, q)$ is isomorphic in a natural way to the subgroup of $\text{GL}(d+1, q)$ consisting of all matrices of the form

$$\begin{pmatrix} A & 0 \\ v & 1 \end{pmatrix}$$

where $A \in \text{GL}(d, q)$ and $v \in V$.

The general affine group has a subgroup $\text{ASL}(d, q)$, the *affine special linear group*, consisting of those elements $t_{A,v}$ with $\det(A) = 1$. $\text{AGL}(d, q)$ is in turn a subgroup of $\text{AFL}(d, q)$, the *affine semilinear group*, which is obtained by adding in the automorphisms of $\mathbb{F}_q$. The elements of $\text{AFL}(d, q)$ are the transformations of the form

$$t_{A,v,\sigma} : u \mapsto u^\sigma A + v \text{ for } A \in \text{GL}(d, q), v \in V, \sigma \in \text{Aut}(\mathbb{F}_q)$$

(where σ acts componentwise on a vector u). Note that when $q = p$ (the case we need to look at), we have $\text{AFL}(d, q) = \text{AGL}(d, q)$.

Theorem 5.1 *A group $G = \text{AGL}(d, p)$ with $p^d = n$ contains an n -cycle if and only if $d = 1$ (or $G = \text{AGL}(2, 2) \cong S_4$).*

Proof: It is clear that $d = 1$ is sufficient to get an n -cycle (see Section 3.1).

Now suppose $d \geq 2$.

As noted above, the group $\text{AGL}(d, p)$ is contained in $\text{GL}(d+1, p)$ as a group of lower triangular block matrices. In fact $\text{AGL}(d, p)$ contains a Sylow p -subgroup P of $\text{GL}(d+1, p)$ consisting of the lower triangular matrices with all 1's on the diagonal.

We claim that any element of P has order at most p^k where $p^{k-1} < d+1 \leq p^k$. Indeed, $X \in P$ implies that $(X - I)^{d+1} = 0$ (since $X - I$ has only zeros on and above the diagonal) and so

$$0 = (X - I)^{p^k} = X^{p^k} - I$$

with this last equality occurring because the field has characteristic p .

An element of order p^d would of course be contained in P , and so to get such an element we need $p^{d-1} < d+1$. It is easy to check that this implies $(d, p) = (2, 2)$.

We have $\text{AGL}(2, 2) \cong S_4$ and so this group does contain a 4-cycle. This completes the proof. $\square$

5.2 Almost Simple Groups

The finite 2-transitive groups G with simple socle N are given in Table 5.1, adapted from [4, Table 7.4, p. 197]. Recall that $q = p^e$ is a prime power; n and d are positive integers, where n is always the degree of the representation of the group being considered. The fourth column gives the index $[G : N]$ for the largest possible G where G is the normalizer of N in S_n .

As noted in Chapter 3, the groups in rows 8, 9, 14 do indeed contain n -cycles.

Lemma 5.1 *The groups $N = G$ in rows 3, 4, 10, 11, 15, 17, and 18 of Table 5.1 do not contain n -cycles. In rows 7 and 16 neither the groups nor their normalizers G contain an n -cycle.*

Proof: In all these cases, the degree of the representation is even, and so an n -cycle is an odd permutation. Since $N \cap A_n$ is normal in N , the simple group N must be contained in A_n and so cannot contain an n -cycle. In particular, none of the groups in the list contain an n -cycle.

For the groups in the second part of the list we have that $[G : N]$ is odd in both cases. Since $[S_n : A_n] = 2$ and $N \leq A_n$, we conclude $G \leq A_n$. Hence G does not

Row	Degree	Condition	N	Max. $[G : N]$
1.	n	$n \geq 5$	A_n	2
2.	$(q^d - 1)/(q - 1)$	$d \geq 2$	$\text{PSL}(d, q)$	$\gcd(d, q - 1)e$
3.	$2^{2d-1} + 2^{d-1}$	$d \geq 3$	$\text{Sp}(2d, 2)$	1
4.	$2^{2d-1} - 2^{d-1}$	$d \geq 3$	$\text{Sp}(2d, 2)$	1
5.	$q^3 + 1$	$q \geq 3$	$\text{PSU}(3, q)$	$\gcd(3, q + 1)e$
6.	$q^2 + 1$	$q = 2^{2d+1} > 2$	$\text{Sz}(q)$	$2d + 1$
7.	$q^3 + 1$	$q = 3^{2d+1} > 3$	$R_1(q)$	$2d + 1$
8.	11		$\text{PSL}(2, 11)$	1
9.	11		M_{11}	1
10.	12		M_{11}	1
11.	12		M_{12}	1
12.	15		A_7	1
13.	22		M_{22}	2
14.	23		M_{23}	1
15.	24		M_{24}	1
16.	28		$\text{PSL}(2, 8)$	3
17.	176		HS	1
18.	276		Co_3	1

Table 5.1: The almost simple 2-transitive groups

contain an n -cycle in either of these cases. $\square$

Lemma 5.2 *The group in row 12 (A_7 represented as a group of degree 15) does not contain an n -cycle.*

Proof: It is enough to show that A_7 has no element of order 15.

An element of order 15 can be written in disjoint cycle notation as a set of cycles whose lengths have the property that their least common multiple is 15. An element of this order moving the smallest number of points is conjugate (in the symmetric group) to $(123)(45678)$. Such an element cannot belong to A_7 as it acts on more than 7 points; hence A_7 cannot have an element of order 15. $\square$

Lemma 5.3 *The group in row 13, M_{22} , does not contain a 22-cycle; nor does its normalizer.*

Proof: Since 22 is even, a 22-cycle is an odd permutation and so cannot be contained in the simple group M_{22} . The group has index 2 in its normalizer, so this normalizer could contain odd permutations. As mentioned in Section 2.2, this normalizer is $\text{Aut}(W_{22})$. It does not contain a 22-cycle as the Atlas shows us that the normalizer $G.2 = \text{Aut}(W_{22})$ of $G = M_{22}$ does not contain an element of order 22 ([9, p. 40]). $\square$

Note that the next three groups considered were described in Section 2.1.

Lemma 5.4 *The group $N = \text{Sz}(q)$ and its normalizer G of row 6 of Table 5.1 do not contain a $(q^2 + 1)$ -cycle.*

Proof: When $q = 8$, the Atlas shows that $\text{Sz}(8)$ does not contain an element of order $q^2 + 1 = 65$ ([9, p. 28]). The index of $\text{Sz}(8)$ in its normalizer N is $2d + 1 = 3$ and so an element of order 65 in G would have to lie in N .

When $q > 8$, we use the following facts from [21].

Let $r = 2^d$ and recall that $q = 2^{2d+1}$. Then $N = Sz(q)$ has particular subgroups H_0 ([21, p. 183]) and H_1, H_2 ([21, p. 213]) of orders $q - 1$, $q + 2r + 1$, $q - 2r + 1$ respectively.

The conjugacy classes of N are ([21, p. 269]):

1. $\{1\}$;
2. the class of involutions;
3. $\frac{1}{2}q - 1$ classes in $\cup_{y \in N} (H_0 \setminus \{1\})^y$;
4. $\frac{1}{4}(q + 2r)$ classes in $\cup_{y \in N} (H_1 \setminus \{1\})^y$;
5. $\frac{1}{4}(q - 2r)$ classes in $\cup_{y \in N} (H_2 \setminus \{1\})^y$;
6. two classes of elements of order 4.

Thus the elements of N have order 1, 2, 4, or order dividing $q - 1$, $q + 2r + 1$, or $q - 2r + 1$, all of which are smaller than $q^2 + 1$. This proves that N does not contain a $q^2 + 1$ -cycle.

The index of N in G is $2d + 1$ and so if G contains a $q^2 + 1$ -cycle x , then x^{2d+1} is an element of order at least $(q^2 + 1)/(2d + 1)$. However $(q^2 + 1)/(2d + 1)$ is larger than the orders of the elements of N . Indeed, note the largest possible order of an element of N is

$$q + 2r + 1 = 2^{2d+1} + 2^{d+1} + 1$$

and compare $q + 2r + 1$ to $(q^2 + 1)/(2d + 1)$ as follows. Consider

$$f(d) = ((q + 2r + 1)(2d + 1) - 1)/q^2.$$

We have

$$\begin{aligned} f(d) &= 2(d(2^{2d+1} + 2^{d+1} + 1) + 2^{2d} + 2^d)/2^{4d+2} \\ &= d(2^{-2d} + 2^{-3d} + 2^{-4d-1}) + 2^{-2d-1} + 2^{-3d-1}. \end{aligned}$$

We see that $f(d)$ for positive integers d clearly reaches its maximum at $d = 1$. The value at $d = 1$ is

$$f(1) = 1/4 + 1/8 + 1/32 + 1/8 + 1/16 = 19/32$$

and so $f(d) < 1$ for all d . This proves the claim that $(q^2 + 1)/(2d + 1)$ is larger than the order of an element of N .

Hence the normalizer G does not contain an element of order $q^2 + 1$. $\square$

Lemma 5.5 *The group $N = \text{PSU}(3, q)$ of row 5 of Table 5.1 and its normalizer G do not contain $q^3 + 1$ -cycles.*

Proof: Recall that $\text{PSU}(3, q)$ was described in Section 2.1.2.

We first show that if an element in $\text{PGU}(3, q)$ has order h where h divides $q^3 + 1$, then $h \leq m := q^2 - q + 1$. Suppose that for some (minimal) h dividing $q^3 + 1$, the matrix $A \in \text{GU}(3, q) \leq \text{GL}(3, q^2)$ has the property that A^h is in the centre Z of $\text{GU}(3, q)$.

Because $|Z| = q - 1$, the hypothesis shows that the order of A divides $(q^3 + 1)(q - 1)$. Since the polynomial $g(t) := t^{(q^3+1)(q-1)} - 1 \in \mathbb{F}_{q^2}[t]$ satisfies $\gcd(g(t), g'(t)) = 1$, $g(t)$ splits into distinct linear factors in some finite extension of $\mathbb{F}_{q^2}$. Thus the minimal polynomial for A has distinct roots, and so A is similar to a diagonal matrix over some extension of $\mathbb{F}_{q^2}$. Thus A^k is scalar if and only if all eigenvalues of A^k are equal. Hence h is the least integer such that the h th powers of all eigenvalues of A are equal to one another.

We have to consider three cases:

- (i) the eigenvalues ξ, η, ζ of A all lie in $\mathbb{F}_{q^2}$;
- (ii) one eigenvalue ξ lies in $\mathbb{F}_{q^2}$ and two (Galois conjugate) eigenvalues η, η^{q^2} lie in $\mathbb{F}_{q^4}$;
- (iii) the three eigenvalues are Galois conjugates $\xi, \xi^{q^2}, \xi^{q^4}$ in $\mathbb{F}_{q^6}$.

(i) If the eigenvalues ξ, η, ζ of A all lie in $\mathbb{F}_{q^2}$, then since $A^h \in Z$ and $h|q^3 + 1$, we have $\xi^{q^3+1} = \eta^{q^3+1} = \zeta^{q^3+1}$. But this implies $\xi^{q+1} = \eta^{q+1} = \zeta^{q+1}$ since elements of $\mathbb{F}_{q^2}$ are fixed under the Galois map $\theta \mapsto \theta^{q^2}$. Therefore $h|q + 1$ which is less than m since $q > 2$.

(ii) If one of the eigenvalues is $\xi \in \mathbb{F}_{q^2}$ and the other two are $\eta, \eta^{q^2} \in \mathbb{F}_{q^4}$, then the order of ξ divides $q + 1$ (as above) and the orders of η, η^{q^2} divide $q^4 - 1$. Thus the order of A divides $\text{lcm}(q^4 - 1, q + 1) = q^4 - 1$. But this implies that h divides

$$\gcd(q^4 - 1, q^3 + 1) = \gcd(q^4 + q^3, q^3 + 1) = q + 1 < m.$$

(iii) Now suppose the three eigenvalues are $\xi, \xi^{q^2}, \xi^{q^4}$, and assume $h > q + 1$.

Since A is unitary, $A^{-1} = \bar{A}^T$. As $\bar{\xi} = \xi^q$ (see Section 2.1.2), these latter two matrices have eigenvalues $\xi^{-1}, \xi^{-q^2}, \xi^{-q^4}$ and $\xi^q, \xi^{q^3}, \xi^{q^5}$ respectively. We cannot have $\xi^{-1} = \xi^q$ because $h > q + 1$. Similarly if $\xi^{-1} = \xi^{q^5}$ then h divides $\gcd(q^3 + 1, q^5 + 1) = q + 1$ contrary to $h > q + 1$. Therefore $\xi^{-1} = \xi^{q^3}$ and so $\xi^{q^3+1} = 1$. Thus the eigenvalues have order dividing $q^3 + 1$.

Now consider A^m , where $m = q^2 - q + 1$. We have

$$\begin{aligned} \xi^{m(q^2-1)} &= \xi^{(q^4-q^3+q-1)} \\ &= \xi^{(q^3+1)(q-1)} \\ &= 1 \end{aligned}$$

and so $\xi^m = \xi^{q^2m}$. Similarly $\xi^m = \xi^{q^4m}$. Since $\xi^m = \xi^{q^2m} = \xi^{q^4m}$, A^m is a scalar matrix in the centre Z of $\text{GU}(3, q)$. But $\text{PGU}(3, q) = \text{GU}(3, q)/Z$, so $A^m = I$ in $\text{PGU}(3, q)$; hence A is not a $q^3 + 1$ -cycle in this group.

Now the normalizer of $N = \text{PSU}(3, q)$ is $G = \text{PTU}(3, q)$, in which $\text{PGU}(3, q)$ has index $2e$ where $q = p^e$.

Now by the above we know that $\text{PGU}(3, q)$ does not contain a $q^3 + 1$ -cycle, and that an element A in $\text{GU}(3, q)$ with eigenvalues of order dividing $q^3 + 1$ would drop into the centre when raised to the power $q^2 - q + 1$. Therefore in order to have a

$q^3 + 1$ -cycle in $\text{PTU}(3, q)$ we would need $[\text{PTU}(3, q) : \text{PGU}(3, q)]$ to be a multiple of $q + 1 = (q^3 + 1)/(q^2 - q + 1)$. But it is impossible to have $2e \geq p^e + 1$ for positive integers e , and so $G = \text{PTU}(3, q)$ cannot contain a $q^3 + 1$ -cycle. $\square$

Lemma 5.6 *The group $\text{PSL}(d, q)$ of row 2 of Table 5.1 does not contain a $(q^d - 1)/(q - 1)$ -cycle unless $\gcd(d, q - 1) = 1$. The group $\text{PGL}(d, q)$ always contains such a cycle.*

Proof: Note that $[\text{PGL}(d, q) : \text{PSL}(d, q)] = \gcd(d, q - 1)$ so a statement equivalent to the first assertion of the theorem is that $\text{PSL}(d, q)$ does not contain an n -cycle unless $\text{PSL}(d, q) = \text{PGL}(d, q)$.

We begin by explaining why $\text{PGL}(d, q)$ does contain an n -cycle.

The field $V := \mathbb{F}_{q^d}$ is d -dimensional as a vector space over $\mathbb{F}_q$. It can therefore be embedded in the ring $\text{Mat}(d, q)$ of $d \times d$ matrices over $\mathbb{F}_q$ in an obvious way using the linear action of right multiplication of V on itself. In this way we can construct a cyclic subgroup (of order $q^d - 1$) of $\text{GL}(d, q)$ isomorphic to $\mathbb{F}_{q^d}^*$. A matrix A which generates this cyclic subgroup is called a *Singer cycle*. Since A represents a generator of $\mathbb{F}_{q^d}^*$, clearly A permutes the nonzero vectors of the underlying vector space V in a single cycle. Since the centre Z of $\text{GL}(d, q)$ has order $q - 1$, A induces an element of $\text{PGL}(d, q)$ which acts as a $(q^d - 1)/(q - 1)$ -cycle on the 1-dimensional subspaces of V .

Therefore any group G of degree $n = (q^d - 1)/(q - 1)$ with $\text{PGL}(d, q) \leq G \leq \text{PTL}(d, q)$ contains an n -cycle.

Now suppose that $A \in \text{SL}(d, q)$ is a Singer cycle. Then A has order $n(q - 1)$ and its characteristic polynomial is the minimal polynomial g of V over $\mathbb{F}_q$. If one of the roots of g is $\eta \in V$, then the set of roots is $\{\eta, \eta^q, \eta^{q^2}, \dots, \eta^{q^{d-1}}\}$, which forms a basis for V over $\mathbb{F}_q$. The matrix A is similar to a diagonal matrix over V , so A^k is scalar if and only if all eigenvalues of A^k are equal.

Now we also have $\det(A) = 1$ as $A \in \text{SL}(d, q)$. Therefore the product of the eigenvalues is

$$1 = \eta \cdot \eta^q \cdots \eta^{q^{d-1}} = \eta^{q^{d-1} + \cdots + q + 1} = \eta^n.$$

Suppose $r \mid \gcd(d, q-1)$ and $r > 1$. Then $d \equiv 0 \pmod{r}$ and $q \equiv 1 \pmod{r}$ imply that

$$\begin{aligned} n = q^{d-1} + \cdots + q + 1 &\equiv d(1) \pmod{r} \\ &\equiv 0 \pmod{r}. \end{aligned}$$

Hence r divides n . (Note it must be that $r < n$.)

Then

$$\begin{aligned} 1 &= \eta^{n((q-1)/r)} \\ \eta^{n/r} &= \eta^{nq/r} \end{aligned}$$

and similarly, $\eta^{n/r} = \eta^{nq^i/r}$ for each i , $1 \leq i \leq d-1$. Therefore $A^{n/r}$ has all its eigenvalues equal. Hence the matrix $A^{n/r}$ is scalar, and so when we pass to the quotient $\text{SL}(d, q)/Z = \text{PSL}(d, q)$, $A^{n/r} = I$. Thus A is not a Singer cycle in $\text{PSL}(d, q)$.

Recall that in Section 3.1 we had the degree $(q^d - 1)/(q - 1)$ equal to a prime p . If $r \mid \gcd(d, q-1)$ and $r > 1$ then, as above, $r \mid n$ and so $n = (q^d - 1)/(q - 1)$ is not prime. Hence in the case where $(q^d - 1)/(q - 1) = p$, we must have $\gcd(d, q-1) = 1$, i.e. we must have $\text{PSL}(d, q) = \text{PGL}(d, q)$. $\square$

This section's results are summarized in the following theorem.

Theorem 5.2 *An almost simple 2-transitive permutation group G of degree n contains an n -cycle if and only if $G = A_n$ with n odd, $G = M_{11}$ of degree 11, $G = M_{23}$ of degree 23, $G = \text{PSL}(2, 11)$ of degree 11, or $\text{PGL}(d, q) \leq G \leq \text{PTL}(d, q)$ of degree $n = (q^d - 1)/(q - 1)$.*

Proof: The theorem follows immediately from the lemmas and Table 5.1. $\square$

That a nonsolvable 2-transitive group containing an n -cycle is necessarily one of the above groups was in fact deduced by W. Feit ([11, p. 179]) from the CFSG and the work of Curtis, Kantor, and Seitz ([12]).

Chapter 6

Applications

As mentioned in the introduction, this problem has some interesting applications. We first look at when we can have a permutation group G of degree n containing an n -cycle and certain elements of small order, with G not equal to S_n or A_n .

For groups containing an n -cycle and a 2-cycle or a 3-cycle, the following well-known theorem (see e.g. [14, p. 77]) reduces the question to the imprimitive case.

Theorem 6.1 *If G is a primitive subgroup of S_n , then G contains a 3-cycle if and only if $G = A_n$ or S_n ($n \geq 3$), and G contains a 2-cycle if and only if $G = S_n$ ($n \geq 2$).*

It is easy to see that an imprimitive group $S_{n/m} \wr S_m$, $1 < m < n$, contains a 2-cycle and a 3-cycle. Put $d := n/m$. We may consider the set Ω this group acts on to be $\Omega = \{1, 2, \dots, n\}$ in the following form:

1	2	...	d
$d+1$	$d+2$	...	$2d$
$\vdots$	$\vdots$		$\vdots$
$n-d+1$	$n-d+2$	...	n

where each of the m rows is a block of imprimitivity. The group $S_d wr S_m$ consists of all permutations that interchange the m rows and permute the d elements of each row amongst themselves. (In this new notation, $((i, j))$ from Chapter 4 is now the element in the i th position within the j th row.) It is now obvious that elements such as (12) , and (123) (when $d \geq 3$), and $(12)(34)$ (when $d = 2$ or $d \geq 4$), belong to this group, since these certainly do preserve the rows.

In the case of a $(2, 2)$ -cycle the primitive case was solved by Kochetov ([23]) in the following theorem.

Theorem 6.2 *If G is a primitive subgroup of S_n generated by an n -cycle and an involution moving 4 points, then*

1. $G = S_n$;
2. $G = A_n$;
3. $n = 6$ and $G = S_5$;
4. $n = 7$ and $G = \text{PSL}(2, 7)$.

Note that S_5 is maximal in S_6 , and $\text{PSL}(2, 7)$ is maximal in S_7 (note this is an exceptional representation).

The observations above make up part of the solution to the following question considered by Alan Turing (in a previously unpublished note in [41]) in relation to a problem in cryptography: for which $x \in S_n$ does the subgroup generated by x and $(12 \dots n)$ not contain A_n ? One could obtain a full solution to this problem by studying generators of the subgroups listed in Theorem 1.1.

This question of Turing is also related to the study of chordal rings in graph theory. A *chordal ring* is a finite directed graph $\mathcal{G}$ (with no loops or multiple edges) on n vertices $v_1, v_2, \dots, v_n$ with the following properties. $\mathcal{G}$ has a “ring” of edges

(v_i, v_{i+1}) ($1 \leq i \leq n-1$) and (v_n, v_1) , and it has an automorphism $(v_1 \dots v_n)$ permuting the vertices cyclically. Since the automorphism group of $\mathcal{G}$ contains an n -cycle, we see that the results of this thesis can be applied to the study of $\text{Aut}(\mathcal{G})$. See the paper [29] for more on this topic.

A related question of interest in graph theory is the following, which was posed by Bruce Richter ([34]). When can a subgroup of S_n have $\mathbb{Z}_n$ (the cyclic group of order n) or D_{2n} (the dihedral group of order $2n$) as a homomorphic image? We give a solution for the case $n = p$ a prime.

Theorem 6.3 *If subgroup G of S_p ($p \geq 2$) has $\mathbb{Z}_p$ or D_{2p} as a homomorphic image, then $G \cong \mathbb{Z}_p$ (or $G \cong D_4$, $p = 2$), or $G \cong D_{2p}$, respectively.*

Proof: Suppose we have $K \triangleleft G$ where K is the kernel of the homomorphism, and $G/K \cong \mathbb{Z}_p$ or D_{2p} .

Since G/K has an element of order p , so does G . This element must be a p -cycle as p is prime. Therefore by Section 3.1, $G = M_{11}$, M_{23} , $\text{PSL}(2, 11)$, $G \leq \text{AGL}(1, p)$, or $\text{PGL}(d, q) \leq G \leq \text{P}\Gamma\text{L}(d, q)$ with $p = (q^d - 1)/(q - 1)$. (Note that $D_{2p} \leq \text{AGL}(1, p)$ for all p .)

We need not consider the simple groups $G = A_p$, M_{11} , M_{23} , $\text{PSL}(2, 11)$, since the kernel K is a normal subgroup of G . Thus we need only consider $G \leq \text{AGL}(1, p)$ and $\text{PGL}(d, q) \leq G \leq \text{P}\Gamma\text{L}(d, q)$ when $p = (q^d - 1)/(q - 1)$.

Now if $K \neq 1$, $K \triangleleft G$, then $K \cap \text{soc}(G) = \text{soc}(G)$. Thus if K is nontrivial, it must contain the socle of G .

In the case of $\text{AGL}(1, p)$, the socle is $\langle x \rangle$ where x is a p -cycle. The quotient group is cyclic of order $p - 1$, so this quotient group cannot have a subgroup of order p .

In the case of $\text{P}\Gamma\text{L}(d, q)$, the socle is $\text{PSL}(d, q)$ and the quotient group has order $\text{gcd}(d, q - 1)e$ where $q = r^e$ for some prime r . Since $p = (q^d - 1)/(q - 1)$ does not divide $\text{gcd}(d, q - 1)e$, the quotient group cannot have a subgroup of order p . $\square$

For composite n , this problem is more complicated since G need not contain an n -cycle. It is not even necessary that G be transitive; for example in S_6 the subgroup $G = \langle (12)(345) \rangle$ is not transitive but is cyclic of order 6. If we consider only those G that do have an n -cycle, then Theorem 1.1 can be applied; similarly to the above theorem there are no nontrivial homomorphisms for primitive groups G containing an n -cycle.

Theorem 1.1 has also been used by Li in [25] to classify certain Cayley graphs. For more on the relation between transitive groups and graph theory, see [31].

Theorem 1.1 has other applications, for example to Kronecker conjugacy of polynomials of degree n , see [28].

Bibliography

- [1] Artin, Emil. *Geometric Algebra*. Wiley-Interscience, London and New York, 1957.
- [2] Aschbacher, M. and L. Scott. Maximal subgroups of finite groups. *J. Algebra*, 92 (1985), 44-80.
- [3] Burnside, W. *Theory of Groups of Finite Order*, second edition. Cambridge University Press, 1911.
- [4] Cameron, Peter J. *Permutation Groups*. Cambridge University Press, 1999.
- [5] Carter, R.W. *Simple Groups of Lie Type*. Wiley-Interscience, London and New York, 1972.
- [6] Carter, R.W. *Finite Groups of Lie Type*. Wiley-Interscience, London and New York, 1985.
- [7] Chevalley, Claude. Sur certains groupes simples. *Tohoku Math. J. (2)*, 7 (1955), 14-66.
- [8] Chevalley, Claude. *Théorie des groupes de Lie*, Tômes I-III, Hermann et compagnie, Paris, 1955.
- [9] Conway, J.H., R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson. *The Atlas of Finite Groups*. Clarendon Press, Oxford, 1985.

- [10] Conway, J.H. and N.J.A. Sloane. *Sphere packings, Lattices and Groups*. Springer-Verlag, New York, 1988.
- [11] Cooperstein, B. and G. Mason, editors. The Santa Cruz Conference on Finite Groups. *Proceedings of Symposia in Pure Mathematics*, vol. 37, 1979.
- [12] Curtis, C.W., W.M. Kantor, and G.M. Seitz. The 2-transitive permutation representations of the finite Chevalley groups. *Trans. Amer. Math. Soc.*, 218 (1976), 1-59.
- [13] Dieudonné, Jean. *La géométrie des groupes classiques*, seconde édition. Springer-Verlag, Berlin, 1963.
- [14] Dixon, John D. and Brian Mortimer. *Permutation Groups*. Springer-Verlag, New York, 1996.
- [15] Dixon, John D. Automorphism groups of chordal rings and a problem of A.M. Turing. Unpublished, 1996.
- [16] Dynkin, E.B. Maximal subgroups of the classical groups. *Amer. Math. Soc. Transl. Ser. 2*, 6 (1957), 245-378.
- [17] Gorenstein, Daniel, Richard Lyons and Ronald Solomon. *The Classification of the Finite Simple Groups*, Volumes 1-4. American Mathematical Society, Providence, R.I., 1994, 1996, 1998, 1999.
- [18] Gorenstein, Daniel. *Finite Simple Groups*. Plenum Press, New York, 1982.
- [19] Hazewinkel, M., editor. *Encyclopaedia of Mathematics: an updated and annotated translation of the Soviet "Mathematical Encyclopaedia"*. Kluwer Academic Publishers, 10 vols., 1988-1994.
- [20] Hegedüs, P. Regular subgroups of the affine group. *J. Algebra*, 225 (2000), 740-742.

- [21] Huppert, B. and N. Blackburn. *Finite Groups III*, Springer-Verlag, Berlin, 1982.
- [22] Kleidman, P. and M.W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. London Math. Soc. Lecture Notes no. 129, Cambridge University Press, 1990.
- [23] Kochetov, Yu. Yu. Permutation groups generated by a $(2, 2)$ -cycle and an n -cycle. *Funct. Anal. Appl.*, 31 (1997), 133-135.
- [24] Li, Cai Heng. The finite primitive permutation groups containing an abelian regular subgroup. Submitted to *J. London Math. Soc.*, 2002, 21 pp.
- [25] Li, Cai Heng. On edge-transitive Cayley graphs, rotary Cayley maps on 2-manifolds and s -arc-transitive graphs. Preprint, 2002.
- [26] Liebeck, M.W., C.E. Praeger, and J. Saxl. The classification of the maximal subgroups of the finite symmetric and alternating groups. *J. Algebra*, 111 (1987), 477-516.
- [27] Liebeck, M.W., C.E. Praeger, and J. Saxl. Transitive subgroups of primitive permutation groups. *J. Algebra*, 234 (2000), 291-361.
- [28] Müller, Peter. Kronecker conjugacy of polynomials. *Trans. Amer. Math. Soc.*, 350 (1998), 1823-1850.
- [29] Pálffy, P.P. Isomorphism problem for relational structures with a cyclic automorphism. *Europ. J. Combinatorics*, 8 (1987), 35-43.
- [30] Passman, D. *Permutation Groups*. W.A. Benjamin, New York, 1968.
- [31] Praeger, C.E. Finite transitive permutation groups and vertex-transitive graphs. *Graph Symmetry: Algebraic Methods and Applications*, NATO ASI Ser. C, 497 (1997), 277-318.

- [32] Ree, R. A family of simple groups associated with the simple Lie algebra of type (G_2) . *Bull. Amer. Math. Soc.*, 66 (1960), 508-510.
- [33] Ree, R. A family of simple groups associated with the simple Lie algebra of type (F_4) . *Bull. Amer. Math. Soc.*, 67 (1961), 115-116.
- [34] Richter, Bruce. Personal correspondence, 2000.
- [35] Schönert, Martin, et al. *GAP: Groups, Algorithms, and Programming*. Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, fifth edition, 1995.
- [36] Schur, I. Zur Theorie der einfach transitiven Permutationsgruppen. *Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Klasse*, 598-623.
- [37] Steinberg, R. Variations on a theme of Chevalley. *Pacific J. Math.*, 9 (1959), 875-891.
- [38] Suzuki, M. A new type of simple groups of finite order. *Proc. Nat. Acad. Sci. U.S.A.*, 46 (1960), 868-870.
- [39] Taylor, D.E. *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics no. 9. Heldermann Verlag, Berlin, 1992.
- [40] Thompson, T.M. *From Error-Correcting Codes through Sphere Packings to Simple Groups*, Carus Mathematical Monograph no. 21. Mathematical Association of America, Washington, D.C., 1983.
- [41] Turing, A.M. *Collected Works: Pure Mathematics*. North-Holland, Amsterdam, 1992.
- [42] Weyl, H. *The Classical Groups: Their Invariants and Representations*, Princeton Mathematics Series no. 1. Princeton University Press, 1939.

- [43] Wielandt, H. *Finite Permutation Groups*. Academic Press, New York, 1964.