On Closures of Finite Permutation Groups

Jing Xu

MSc Peking University

This thesis is presented for the degree of Doctor of Philosophy of

The University of Western Australia

School of Mathematics and Statistics

2005

Abstract

In this thesis we investigate the properties of k-closures of certain finite permutation groups. Given a permutation group G on a finite set Ω, for $k \geq 1$, the k-closure $G^{(k)}$ of G is the largest subgroup of $\mathrm{Sym}(\Omega)$ with the same orbits as G on the set Ω^k of k-tuples from Ω.

The first problem in this thesis is to study the 3-closures of affine permutation groups. In 1992, Praeger and Saxl showed if G is a finite primitive group and $k \geq 2$ then either $G^{(k)}$ and G have the same socle or $(G^{(k)}, G)$ is known. In the case where the socle of G is an elementary abelian group, so that G is a primitive group of affine transformations of a finite vector space, the fact that $G^{(k)}$ has the same socle as G gives little information about the relative sizes of the two groups G and $G^{(k)}$. In this thesis we use Aschbacher's Theorem for subgroups of finite general linear groups to show that, if $G \leq \mathrm{AGL}(d, p)$ is an affine permutation group which is not 3-transitive, then for any point $\alpha \in \Omega$, G_α and $(G^{(3)} \cap \mathrm{AGL}(d, p))_\alpha$ lie in the same Aschbacher class. Our results rely on a detailed analysis of the 2-closures of subgroups of general linear groups acting on non-zero vectors and are independent of the finite simple group classification. In addition, modifying the work of Praeger and Saxl in [47], we are able to give an explicit list of affine primitive permutation groups G for which $G^{(3)}$ is not affine.

The second research problem is to give a partial positive answer to the so-called Polycirculant Conjecture, which states that every transitive 2-closed permutation group contains a semiregular element, that is, a permutation whose cycles all have the same length. This would imply that every vertex-transitive graph has a semiregular automorphism. In this thesis we make substantial progress on the Polycirculant Conjecture by proving that every vertex-transitive, locally-quasiprimitive graph has a semiregular automorphism. The main ingredient of the proof is the determination of all biquasiprimitive permutation groups with no semiregular elements.

Publications arising from this thesis are [17, 54].

Acknowledgements

This thesis would not have been possible without the support of many people.

First of all, I would like to give my sincere thanks to my supervisors: Dr. Cheryl Praeger, Dr. Cai Heng Li and Dr. Michael Giudici. Dr. Cheryl Praeger has been an inspiration to me throughout my thesis process. It was her who opened my eyes to the area of closures of permutation groups. It was her who taught me permutation groups theory as well as research skills. Dr. Cai Heng Li has always been there for me whenever I have a question in my research. In addition, he and his wife, Dr. Jian Ping Wu, have been taking care of my life in Australia since the date I arrived at Perth. Dr. Michael Giudici has been supportive and helpful over the last three years. I am grateful for his advice in research and his help in improving my written English, especially when I was studying the Polycirculant Conjecture with him.

I would also like to thank Dr. Jie Wang, my MSc supervisor at Peking University, for his continuing support and encouragement. Thanks also go to Dr. Boris Datskovsky, my supervisor at Temple University, who first taught me how to write mathematics in English and who supported me to come to Perth to study the area I am interested in, Dr. Oliver King and Dr. Tim Penttila, who gave me valuable advice on the work of the thesis.

I am greatly indebted to my parents for their constant support. My parents are both mathematical teachers. They introduced me to mathematical research, and they showed me how enjoyable the experience can be. I also thank my boyfriend Qiang Li for his love, patience and support.

Finally I acknowledge the support of the IPRS scholarship of Australia and a UPA (International students) scholarship from the University of Western Australia during the course of my PhD study.

Contents

Abstract **i**

Acknoledgements **ii**

1 Introduction **1**

1.1 Overview 1

1.2 Closures of primitive permutation groups 2

1.3 The Polycirculant Conjecture 3

1.4 Main results and organization of this thesis 6

2 Preliminary Results **9**

2.1 Permutation groups and group actions 9

2.2 Primitive groups, quasiprimitive groups and biquasiprimitive groups . . . 12

2.3 O'Nan-Scott type theorems 14

2.3.1 Centralizers and normalizers 14

2.3.2 The socle 15

2.3.3 Product actions 16

2.3.4 The direct product of groups 17

2.3.5 The O'Nan-Scott theorems 18

2.4 General results about k-closures 20

2.5 Algebraic graph theory 23

2.5.1 Basic definitions 23

2.5.2 Orbital (di)graphs 24

2.5.3 Vertex-transitive graphs 25

3 Linear Algebra and Geometries **29**

3.1 Tensor product spaces 29

3.2 Semilinear transformations 34

3.3 Projective geometry 36

3.4 The geometry of classical groups . . . 37
3.4.1 Basic definitions . . . 37
3.4.2 The orthogonal geometry . . . 38
3.4.3 The symplectic and unitary geometries . . . 42

4 Aschbacher's Classification 45
4.1 The reducible subgroups C_1 . . . 45
4.2 The imprimitive subgroups C_2 . . . 46
4.3 The field extension subgroups C_3 . . . 46
4.4 The tensor product subgroups C_4 . . . 47
4.5 The subfield subgroups C_5 . . . 47
4.6 The symplectic-type subgroups C_6 . . . 48
4.6.1 Symplectic type r-groups. . . . 48
4.6.2 The maximal C_6-subgroups $H = N_{\Gamma\mathrm{L}(d,q)}(R)$ . . . 49
4.6.3 The structure of $N_{\mathrm{GL}(d,p^e)}(R)$ when $d \geq 3$ . . . 49
4.7 The tensor product subgroups C_7 . . . 52
4.8 The classical subgroups C_8 . . . 52

5 Some Special Semilinear Subgroups 53
5.1 Dickson's theorem and Aschbacher classes in dimension 2 . . . 54
5.2 2-dimensional semilinear groups . . . 55
5.3 The case $\mathrm{SL}(d,q) \leq H \leq \Gamma\mathrm{L}(d,q) \quad (d \geq 3)$ . . . 57
5.4 The case $d = 1$ . . . 58
5.4.1 Proof of Proposition 5.4.2 . . . 58
5.4.2 Proof of Theorem 5.4.1. . . . 61

6 Closures of Semilinear Groups 63
6.1 Notations and outline . . . 63
6.2 Proof of Theorem 6.0.6 when $d = 2$ . . . 65
6.3 The case $H \in C_1$ . . . 66
6.4 The case $H \in C_2$ . . . 66
6.5 The case $H \in C_3$ with $d \geq 3$. . . . 66
6.6 The cases $H \in C_4$ and $H \in C_7$ . . . 67
6.7 The case $H \in C_5$ . . . 69
6.8 The case $H \in C_8$ . . . 71
6.8.1 The symplectic groups . . . 71
6.8.2 The orthogonal groups . . . 71

6.8.3 The unitary groups . . . 72
6.9 The case $H \in C_6$ for $d \geq 3$. . . . 72
6.9.1 The reduction . . . 73
6.9.2 Proof of Proposition 6.9.1 when R is of type 5 . . . 74
6.9.3 Proof of Proposition 6.9.1 when R is of type 1,2,3 or 4 . . . 75
6.10 The case $H \in C_9$ for $d \geq 3$. . . . 82

7 Closures of Affine Permutation Groups 83
7.1 The general result . . . 83
7.2 Closures of affine primitive groups . . . 84
7.3 Product action and the proof of Theorem 7.2.1 . . . 85

8 Elusive Permutation Groups 89
8.1 Introduction . . . 89
8.2 Some biquasiprimitive elusive groups . . . 92
8.2.1 The notation for biquasiprimitive elusive groups . . . 92
8.2.2 The examples . . . 93
8.3 Determining all biquasiprimitive elusive groups . . . 96
8.3.1 The case where G^+ acts faithfully on both orbits . . . 97
8.3.2 The case where G^+ is not faithful on its orbits. . . . 102
8.4 Proofs of Theorems 8.1.8 and 8.1.10 . . . 103

9 Concluding Remarks 105
9.1 Further questions on closures of affine permutation groups . . . 105
9.2 Future work on the Polycirculant Conjecture . . . 105

Chapter 1

Introduction

In this chapter, we introduce the research problems studied in the thesis and review the relevant history. In addition, we will introduce the main results and organization of the thesis. We refer readers to Chapter 2 and other standard texts such as [4, 10, 12, 52] for definitions and notation not fully explained in this chapter.

1.1 Overview

Permutation groups frequently arise in nature as groups of permutations of various kinds of mathematical objects which leave certain relations invariant. In 1969, Wielandt [53] set out to present a unified treatment of finite and infinite permutation groups, based on invariant relations and invariant functions. To do so he initiated the study of k-closures of permutation groups.

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on a set Ω. Let k be a positive integer. Then G has a natural action on $\Omega^k = \Omega \times \cdots \times \Omega$ (k copies). Wielandt [53] defined the *k-closure* of G to be the group

$$G^{(k)} := \{g \in Sym(\Omega) \mid \Delta^g = \Delta \text{ for each orbit } \Delta \text{ of } G \text{ on } \Omega^k\},$$

that is, $G^{(k)}$ is the largest subgroup of $\mathrm{Sym}(\Omega)$ with the same orbits as G on the set of ordered k-tuples from Ω. We say that G is *k-closed* if $G = G^{(k)}$. Also, in [53] Wielandt obtained a number of basic properties of the k-closures of permutation groups and gave some interesting applications. For example,

$$G \leq \ldots \leq G^{(k)} \leq G^{(k-1)} \leq \ldots \leq G^{(2)},$$

and if $|\Omega| = n$, then $G^{(n-1)} = G$. In fact, Wielandt [53] showed that $G = G^{(k)}$ if there are points $\alpha_1, \ldots, \alpha_{k-1}$ in Ω such that $G_{\alpha_1,\ldots,\alpha_{k-1}} = 1$, that is, if G has a base of length less than k. Major efforts have been made to obtain information about G by investigating the above inclusion, especially when G is a finite primitive group.

In this thesis, we are going to investigate the properties of k-closures of certain finite permutation groups. The first problem is to study the 3-closures of affine permutation groups. The second one is to give a partial positive answer to the so-called Polycirculant Conjecture. We will explain these two problems and review the relevant history in the following two sections.

Note that throughout this thesis, we only consider finite permutation groups acting on finite sets.

1.2 Closures of primitive permutation groups

A permutation group G acting transitively on a set Ω is called *primitive* if G preserves no nontrivial partition of Ω. One of the most important and useful theorems for studying finite permutation groups is the O'Nan-Scott Theorem (see [33]). It identifies certain types of finite primitive permutation groups according to the nature of their socles (the subgroup generated by the set of all minimal normal subgroups) and their permutation actions, and states that every finite primitive permutation group belongs to exactly one of these types.

Clearly, if G is primitive of rank r on Ω (i.e. the number of G_α-orbits on Ω is r), then so is $G^{(2)}$, and $G^{(2)}$ is the largest subgroup of $\mathrm{Sym}(\Omega)$ containing G with this property. In particular, if G is 2-transitive on Ω, then $G^{(2)}$ is the full symmetric group $\mathrm{Sym}(\Omega)$. With these in mind, the problem of determining the 2-closure of G when G is simply primitive (that is, primitive but not 2-transitive) arises naturally. However, this problem is rather difficult and is unsolved in general.

In [32], Liebeck, Praeger and Saxl began to investigate the closures of primitive groups type by type by using the O'Nan-Scott Theorem. They studied $G^{(2)}$ when G is simply primitive of almost simple type, that is, $T \trianglelefteq G \leq \mathrm{Aut}(T)$ for some non-abelian simple group T. The main result [32, Theorem 1] shows that if G is an almost simple group with $T \trianglelefteq G \leq \mathrm{Aut}(T)$ and G is simply primitive, then either $T \trianglelefteq G^{(2)} \leq \mathrm{Aut}(T)$ or $(G, G^{(2)})$ is given in an explicit list. Also, they proved that if G is an almost simple primitive permutation group of degree $n > 24$ with socle T, then for $k \geq 4$, $G^{(k)}$ also has socle T, (see [32, Corollary 2]). Actually, in [32, Theorem 2], they determined all almost simple primitive permutation groups G such that G is not k-transitive and $G^{(k)}$ is not contained in the normalizer of the socle of G, where k is an integer and $k \geq 2$. In addition, they obtained an interesting application to 2-closures of automorphism subgroups of distance transitive graphs. We will talk about the relationship between the study of 2-closures of permutation groups and the study of the automorphism groups of graphs later. This is the second main topic of the thesis.

In [47], Praeger and Saxl proved an extension of [32, Corollary 2] for all finite primitive groups: they showed that, for a finite primitive group G, the k-closure $G^{(k)}$ is close to G for fairly small values of k. The main theorem (see [47], Theorem 1) they obtained is that if G is a finite primitive permutation group, then for any integer $k \geq 6$, the k-closure $G^{(k)}$ has the same socle as G. In addition, Praeger and Saxl investigated the inclusion $G < H \leq G^{(k)}$, where G is a primitive permutation group, G and H have different socles, and $k \geq 2$. They developed a reduction method (see [47] Theorem 2) to deal with this "different socles" case and classified explicitly the groups G and H. Finally, in that paper, they posed the following question:

Question 1.2.1 [Praeger and Saxl, 1992] *Suppose G is a primitive group of affine type such that $G \leq G^{(k)} \leq \mathrm{AGL}(d,p)$, so $G = NH$ and $G^{(k)} = NK$, where $N = Z_p^d$ and $H \leq K \leq \mathrm{GL}(d,p)$. What can be said about the inclusion $H \leq K \leq \mathrm{GL}(d,p)$?*

The question arose because in the case when G and $G^{(k)}$ are both primitive groups of affine type, the fact that $G^{(k)}$ and G have the same socle provides rather weak information about the "closeness" of these two groups. In this thesis, we answer this question when $k = 3$ in terms of Aschbacher's classification [1] of subgroups of $\mathrm{GL}(d,p)$ (see Theorem 7.1.1 and Corollary 7.2.2). In fact we will investigate the 3-closures of all affine permutation groups, not just primitive affine permutation groups.

1.3 The Polycirculant Conjecture

The Polycirculant Conjecture originates from the study of vertex-transitive graphs. A *graph* is a pair (Ω, E) of sets Ω (of *vertices*) and E (of *edges*) where E is a subset of the set of unordered pairs of distinct elements of Ω. An *automorphism* of a graph (Ω, E) is a permutation of Ω which preserves the edge set E. A *vertex-transitive graph* is a graph whose automorphism group acts transitively on the set of vertices.

A *semiregular* permutation is a non-identity permutation whose cycles all have the same length. Such a permutation generates a semiregular permutation group, that is, a group such that the only element which fixes a point is the identity. Thus the existence of a semiregular permutation in a permutation group is equivalent to the existence of a fixed-point-free element of prime order.

In 1981, Marušič [34] asked if every finite vertex-transitive graph has a semiregular automorphism. The question was asked independently by Jordan [22] in 1988. Note that a vertex-transitive graph is a Cayley graph if and only if it has a regular (both transitive and semiregular) group of automorphisms. Hence we only need to look at vertex-transitive graphs which are not Cayley graphs. A lot of papers have been written about such graphs, see for example [21, 36, 37, 38].

Marušič and Scapellato [35] proved that every vertex-transitive graph of valency three has a semiregular automorphism, while Marušič [34] proved that all vertex-transitive graphs with p^k or mp vertices, where p is a prime and $m \leq p$, have semiregular automorphisms of order p. Also Marušič and Scapellato [35] proved that every vertex-transitive graph with $2p^2$ vertices, for p a prime, has a semiregular automorphism of order p.

Note that the full automorphism group of a graph is 2-closed: any permutation of the vertex set that preserves the orbits of the automorphism group on ordered pairs preserves adjacency and so is an automorphism of the graph. The converse is not true, for example, the cyclic group of order four acting on a set of size four is 2-closed but is not the full automorphism group of a graph. However every 2-closed permutation group may be viewed as the full automorphism group of an edge coloured graph. This point of view indicates the relationship between these two subjects: automorphism groups of graphs, and 2-closed permutation groups. Klin [9, Problem BCC15.12] extended the question of Marušič to the more general setting of 2-closed groups.

Conjecture 1.3.1 (Polycirculant Conjecture) *Every transitive* 2*-closed finite permutation group contains a semiregular permutation.*

This conjecture leads to the study of transitive permutation groups without semiregular elements. A permutation group $G \leq \mathrm{Sym}(\Omega)$ is called *elusive* if G is transitive and contains no nontrivial semiregular permutations (equivalently, no fixed-point-free elements of prime order). The name is intended to suggest that such groups are not easy to find.

The research on fixed-point-free elements of permutation groups has a long history. The existence of such an element in a transitive permutation group was proved by the Orbit-Counting Lemma (or Cauchy-Frobenius Lemma, see [12, Theorem 1.7A]) many years ago. Let $G \leq \mathrm{Sym}(\Omega)$, for each $g \in G$, let $\mathrm{fix}_\Omega(g)$ be the set of points of Ω fixed by the element g. The Orbit-Counting Lemma states that the number m of orbits of G is $\frac{1}{|G|}\sum_{g\in G}|\mathrm{fix}_\Omega(g)|$, that is, the average number of fixed points of the elements of G. Therefore, noting that the identity fixes every point of Ω, the Orbit-Counting Lemma implies that there must be some fixed-point-free element in G if G is a finite transitive permutation group. More recently, Fein, Kantor and Schacher [14, Theorem 1] proved in 1981 that any finite transitive permutation group with degree greater than 1 has a fixed-point-free element of prime power order. Unlike the Orbit-Counting Lemma, this result is a very deep result and was motivated by an application to Brauer groups of local fields. The only known proof of this result depends on the classification of the finite simple groups. However, we cannot replace "prime power" with "prime" in this result since elusive permutation groups do exist. For example, the Mathieu group M_{11} in its 3-transitive action of degree 12 has no fixed-point-free elements of prime order but does have fixed-point-free elements of order 4. See [7] for further examples and constructions of elusive permutation groups.

A transitive permutation group G on a set Ω is *quasiprimitive* if every nontrivial normal subgroup is transitive. In particular, every primitive permutation group is quasiprimitive. Praeger [43] proved a structure theorem for finite quasiprimitive permutation groups which is similar to the O'Nan-Scott Theorem for finite primitive permutation groups.

Giudici [16] has made substantial progress towards asserting the truth of the Polycirculant Conjecture. He determined all the quasiprimitive elusive permutation groups, and showed that none of them are 2-closed. In fact, Giudici [16] has shown that if a counterexample G exists then every minimal normal subgroup of G is intransitive. Also in his thesis [15], Giudici investigated the elusive groups with intransitive minimal normal subgroups and obtained many useful results.

In this thesis we prove the truth of the Polycirculant Conjecture for a large class of graphs, that is, all vertex-transitive locally-quasiprimitive graphs have a semiregular automorphism (see Theorem 8.1.8). We say that a graph Γ with a group G of automorphisms is *G-locally-quasiprimitive* if for each vertex α, the vertex stabiliser G_α acts quasiprimitively on the set $\Gamma(\alpha)$ of vertices adjacent to α. The class of all vertex-transitive locally-quasiprimitive graphs includes all arc-transitive graphs of prime valency and all 2-arc transitive graphs, that is, graphs for which the automorphism group acts transitively on the set of all distinct ordered triples $(\alpha_0, \alpha_1, \alpha_2)$ such that α_1 is adjacent to both α_0 and α_2.

An important ingredient in our proof of Theorem 8.1.8 is a determination of all biquasiprimitive elusive groups. A *biquasiprimitive* permutation group is a transitive permutation group for which every nontrivial normal subgroup has at most two orbits and there is some normal subgroup with precisely two orbits. This is an important class of permutation groups when studying bipartite graphs and was studied in [46]. In this thesis we determine all biquasiprimitive elusive groups.

1.4 Main results and organization of this thesis

The thesis is organized as follows. In Chapter 2 we collect some definitions and preliminary results on permutation groups and on algebraic graph theory. These results will be used frequently in this thesis.

In Chapter 3 we discuss linear algebra techniques and talk about some geometries associated with the linear vector spaces. We first give a detailed discussion about tensor product spaces and about those linear transformations that preserve a tensor decomposition. Then we define nonsingular semilinear transformations and give a geometrical explanation. In addition, we discuss projective and polar spaces. We give the basic definitions of these geometries and study the corresponding "automorphism" groups in this chapter.

In Chapter 4 we give a detailed description of Aschbacher's classification of subgroups of the general linear group and introduce Aschbacher's Theorem. We give the definitions of C_i-subgroups for each $i \in \{1, ..., 9\}$ and describe their group structures one by one.

Chapters 5,6 and 7 aim to answer Question 1.2.1 for $k = 3$. Since the best approach to studying 3-closures of affine permutation groups is first to study 2-closures of semilinear subgroups (see Lemma 2.4.1 (4)), we begin by studying 2-closures of semilinear subgroups. In detail, for $H \leq \Gamma\mathrm{L}(d, q)$, we study $H^{(2)} \cap \Gamma\mathrm{L}(d, q)$ in Chapters 5 and 6. In Chapter 5, we consider some special cases for H, that is, we suppose H is a 1- or 2- dimensional semilinear subgroup, or we suppose $H \geq \mathrm{SL}(d, q)$ with $d \geq 3$. The main result of this Chapter is Theorem 5.0.1. Chapter 6 is dedicated to the proof of Theorem 6.0.6 which is one of the main results of the thesis. Theorem 6.0.6 deals with the 2-closures of semilinear subgroups that do not contain $\mathrm{SL}(d, q)$ in terms of Aschbacher's classification. This theorem is proved by elementary methods.

Theorem 6.0.6 *Suppose H is a subgroup of $\Gamma\mathrm{L}(d, q)$ where $d \geq 2$ and $q = p^f$ is a power of a prime p. Suppose further that H does not contain $\mathrm{SL}(d, q)$ and $H \in C_i$ for some $i = 1, 2, ..., 8, 9$. Then in its action on $V(d, q) \setminus \{0\}$ either*

(a) *$d = 4, q = 2$ and $H = A_7$ is 2-transitive, or*

(b) *$H^{(2)} \cap \Gamma\mathrm{L}(d, q) \in C_i$.*

Finally in Chapter 7 we give the main result (Theorem 7.1.1) concerning 3-closures of affine permutation groups. We state this theorem here.

Theorem 7.1.1 *Suppose G is an affine permutation group such that $G = NH$, where $N = Z_p^d$, $H \leq \mathrm{GL}(d, p)$, $d \geq 1$ and p is a prime.*

1. *If $d = 1$ then $G^{(2)} = G^{(3)} = G$ for proper subgroups G of* $\mathrm{AGL}(1,p)$*, while* $\mathrm{AGL}(1,p)^{(2)} = S_p$ *and* $\mathrm{AGL}(1,p)^{(3)} = \mathrm{AGL}(1,p)$.

2. *If $d = 2$, then $G^{(3)} \cap \mathrm{AGL}(2,p) = G$.*

3. *If $d \geq 3$ and H contains $\mathrm{SL}(d,p)$, then $\mathrm{AGL}(d,p) \leq G^{(3)}$.*

4. *If $d \geq 3$, $\mathrm{SL}(d,p) \not\leq H$ and $H \in C_i$ for $i = 1, 2, ..., 8, 9$, then either $G = Z_2^4 A_7 < \mathrm{AGL}(4,2)$ and $G^{(2)} = G^{(3)} = S_{16}$, or $G^{(3)} \cap \mathrm{AGL}(d,p) = NK$ with $K \in C_i$.*

Moreover, modifying [47, Lemma 4.1], we are able to give an explicit list of affine primitive permutation groups G for which $G^{(3)}$ is not affine.

Theorem 7.2.1 *Suppose $G \leq \mathrm{AGL}(d,p)$ is an affine primitive group of degree p^d where p is a prime and $d \geq 1$. Suppose also that $G < L \leq G^{(3)}$ with $L \not\leq \mathrm{AGL}(d,p)$. Then $p = 2$ and either*

(a) *$L \geq A_{2^d}$ and $G = \mathrm{AGL}(d,2)$ (with $d \geq 3$) or $G = Z_2^4 \rtimes A_7$ (with $d = 4$), or*

(b) *G and L preserve a product decomposition Γ^m, where $|\Gamma| = 2^{d'}, m \geq 2$, and $d = d'm$. Moreover, $(A_{2^{d'}})^m \leq L \leq S_{2^{d'}} \wr S_m$ and $G = G_0 \wr D$, where D is a transitive subgroup of S_m and $G_0 = \mathrm{AGL}(d',2)$ (with $d' \geq 3$) or $Z_2^4 \rtimes A_7$ (with $d' = 4$).*

We then have the following corollary which answers Question 1.2.1 for $k = 3$.

Corollary 7.2.2 *Suppose that G is a primitive affine permutation group such that $G = NH$, where $N = Z_p^d$, $H \leq \mathrm{GL}(d,p)$, p is a prime, and $d \geq 2$.*

(a) *If $d = 2$ then $G^{(3)} = G$.*

(b) *If $d \geq 3$ and H contains $\mathrm{SL}(d,p)$, then $G^{(3)} = \mathrm{AGL}(d,p)$ when p is odd and $G^{(3)} = S_{2^d}$ when $p = 2$.*

(c) *If $G = Z_2^4.A_7 < \mathrm{AGL}(4,2)$ then $G^{(2)} = G^{(3)} = S_{16}$.*

(d) *If $d \geq 3, \mathrm{SL}(d,p) \not\leq H$ and $G \neq Z_2^4.A_7$, then either $G^{(3)} = NK$ where H, K lie in C_i for the same i, where $1 \leq i \leq 9$, or $G^{(3)}$ and G are given by Theorem 7.2.1 (b).*

The results concerning the 3-closures of affine groups have been written up for publication in [54].

In Chapter 8 we study the Polycirculant Conjecture. We first discuss the basic definitions and the known results. Then we prove the following theorem which determines all elusive biquasiprimitive permutation groups.

Theorem 8.1.11 *Let G be a finite biquasiprimitive elusive permutation group on Ω and let $\alpha \in \Omega$. Then one of the following holds:*

1. $G = M_{10}$ *and* $|\Omega| = 12$*;*
2. $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ *and* $G_\alpha \cong \mathrm{PSL}(2,11)^k \rtimes K'$*, where* $K' \leq K \leq S_k$ *such that* K *is transitive,* $|K : K'| = 2$*, and* $K \backslash K'$ *contains no elements of order* 2*;*
3. $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ *and* $G_\alpha \cong (\mathrm{PSL}(2,11)^{k/2} \times M_{11}^{k/2}) \rtimes K'$*, where* k *is even,* $K' \leq K \leq S_k$ *such that* K *is transitive and* K' *is intransitive,* $|K : K'| = 2$ *and* $K \backslash K'$ *contains no elements of order* 2*.*

Moreover, each group G *in* (1)-(3) *is biquasiprimitive and elusive,* G *is not* 2*-closed, and* $G^{(2)}$ *contains a fixed-point-free element of order* 3*.*

Finally we prove the following.

Theorem 8.1.8 *Let* Γ *be a finite graph with a group* G *of automorphisms such that* G *is vertex-transitive and locally-quasiprimitive. Then* Γ *has a semiregular automorphism.*

The results in Chapter 8 have been written up for publication in [17].

We finish the thesis by discussing some further problems related to these two problems in Chapter 9.

Chapter 2

Preliminary Results

This chapter presents a collection of basic definitions and well known results on permutation groups and from algebraic graph theory. The results and notation contained here are often standard and can be found in texts such as [4, 10, 12, 52].

2.1 Permutation groups and group actions

Let Ω be a finite nonempty set. A bijection (a one-to-one and onto mapping) from Ω to Ω is called a *permutation* of Ω. The set of all permutations of Ω forms a group under composition of mappings called the *symmetric group* on Ω. We denote this group by $\mathrm{Sym}(\Omega)$, and write S_n to denote $\mathrm{Sym}(\Omega)$ when $\Omega = \{1, 2, ..., n\}$ for some positive integer n. A *permutation group* is a subgroup of some symmetric group. The *degree* of a permutation group on a set Ω is the cardinality of Ω.

Permutation groups are usually induced by the actions of groups on specified sets. Let G be a group and Ω be a nonempty set, an *action* of G on Ω is a map $\Omega \times G \to \Omega$, written $(\alpha, g) \mapsto \alpha^g$, such that:

(i) $\alpha^1 = \alpha$ for all $\alpha \in \Omega$ where 1 denotes the identity element of G; and

(ii) $(\alpha^x)^y = (\alpha)^{xy}$ for all $\alpha \in \Omega$ and all $x, y \in G$.

The *kernel* of the action of G on Ω is defined to be the subgroup of all elements of G which fix each point of Ω. If this kernel is trivial, then we say that G acts *faithfully* on Ω, and hence identifying each element $g \in G$ with the corresponding bijection $g : \alpha \mapsto \alpha^g$ we have $G \leq \mathrm{Sym}(\Omega)$ is a permutation group on Ω. Otherwise G is said to act on Ω *unfaithfully*, and the quotient group G/K, where K is the kernel, is called the permutation group on Ω induced by G. We denote this induced permutation group by G^Ω.

Let G be a group acting on a set Ω, and let $\alpha \in \Omega$. The *orbit* of α under G is defined to be the set $\alpha^G := \{\alpha^g \mid g \in G\}$. We also call the set of elements in G which fix the point

α, the *stabilizer* of α in G, and denote it by $G_\alpha := \{g \in G \mid \alpha^g = \alpha\}$. Note that G_α is a subgroup of G. Moreover, if $\beta = \alpha^x$ for $x \in G$, then $G_\beta = x^{-1}G_\alpha x$. Similarly, for a subset $\Delta \subseteq \Omega$, the *pointwise stabilizer* of Δ in G is

$$G_\Delta := \{x \in G \mid \delta^x = \delta \text{ for all } \delta \in \Delta\},$$

and the *setwise stabilizer* of Δ in G is

$$G_{\{\Delta\}} := \{x \in G \mid \Delta^x = \Delta\}.$$

It is readily seen that G_Δ and $G_{\{\Delta\}}$ are both subgroups of G and that $G_\Delta \trianglelefteq G_{\{\Delta\}}$.

The following theorem is one of the most important tools in the theory of group actions (see for example [12, Theorem 1.4A(iii)]).

Theorem 2.1.1 (Orbit-Stabilizer Theorem). *Let G be a finite group acting on a set Ω. Then for all $\alpha \in \Omega$, $|\alpha^G| = |G : G_\alpha|$.*

A group G acting on Ω is said to be *transitive* if for any $\alpha, \beta \in \Omega$, there is some $g \in G$ such that $\alpha^g = \beta$. A group G acting on a set Ω is said to be *semiregular* if the only element fixing a point in Ω is the identity. We say that a group G acting on Ω is *regular* if G is both transitive and semiregular on Ω. The following two fundamental results can be found in texts such as [12, 52].

Lemma 2.1.2 *Let G be a group acting transitively on a finite set Ω and let K be a subgroup of G. Then K is transitive if and only if $G = KG_\alpha$ for some $\alpha \in \Omega$.*

Proposition 2.1.3 *An abelian transitive permutation group is regular.*

Example 2.1.4 (Action on right cosets). For any group G and any subgroup H of G, let $\Gamma_H := \{Ha \mid a \in G\}$, the set of right cosets of H in G, and define an action of G on Γ_H by right multiplication: $(Ha)^x = Hax$ with Ha and Hax in Γ_H and $x \in G$.

It is easy to see that the above action is well defined and is transitive. The point stabilizer of the coset Ha is the subgroup H^a, hence the kernel of this action is the subgroup $\bigcap_{a\in G} H^a$ which is called the *core* of H in G, denoted by $\mathrm{core}_G(H)$. If $H = \{1\}$, then the action is faithful and regular, and is also called the *right regular representation* of G.

Let G be a group acting on a set Ω and let H be a group acting on a set Δ. We need the following definition to see when they are "the same" except for the labelling of the points.

Definition 2.1.5 Let G be a group acting on a set Ω and let H be a group acting on a set Δ. Then the action of G on Ω is *permutationally isomorphic* to the action of H on Δ if there is an isomorphism $\varphi : G \to H$ and a bijection $\lambda : \Omega \to \Delta$ such that for all $g \in G$ and $\alpha \in \Omega$, we have $(\alpha^g)^\lambda = (\alpha^\lambda)^{\varphi(g)}$.

In the special case where $G, H \leq \mathrm{Sym}(\Omega)$, then G is permutationally isomorphic to H (acting on Ω) if and only if there is some $\lambda \in \mathrm{Sym}(\Omega)$ such that $H = \lambda^{-1}G\lambda$, that is, H and G are conjugate in $\mathrm{Sym}(\Omega)$. (Note that if G and H are permutationally isomorphic then Definition 2.1.5 implies that $g\lambda = \lambda\varphi(g)$ as an element of $\mathrm{Sym}(\Omega)$, and hence $\varphi(g) = \lambda^{-1}g\lambda$ for all $g \in G$.)

Next we suppose that G is a group acting on Ω and Δ. We define equivalent actions as follows.

Definition 2.1.6 Let G be a group acting on Ω and Δ. Then the two actions are *equivalent* if there is a bijection $\lambda : \Omega \to \Delta$ such that for all $g \in G$ and $\alpha \in \Omega$, we have $(\alpha^g)^\lambda = (\alpha^\lambda)^g$.

Consider G acting on Ω and Δ. If the action of G on Ω is equivalent to the action of G on Δ, then the action of G on Ω is also permutationally isomorphic to the action of G on Δ as we can take φ to be identity map. However, the converse is not true, for an example, see the discussion in the paragraph below Lemma 2.1.7.

When the two actions of G are transitive there is a simple criterion for deciding whether or not they are equivalent.

Lemma 2.1.7 [12, Lemma 1.6B] *Suppose that a group G acts transitively on two sets Ω and Δ, and let H be a stabilizer of a point in Ω. Then the actions are equivalent if and only if H is the stabilizer of some point in Δ.*

Lemma 2.1.7 and Example 2.1.4 tell us that the transitive actions of G are given up to equivalence by the actions on the set of right cosets of H as H runs over a set of representatives for the conjugacy classes of subgroups of G. For example, S_6 has two conjugacy classes of subgroups of index 6, so S_6 has two inequivalent transitive actions of degree 6. However the permutation groups induced by the two actions are permutationally isomorphic, since the two actions are both faithful and there exists $\varphi \in \mathrm{Aut}(S_6)$ interchanging the two conjugacy classes of subgroups of index 6. This example indicates a big difference between the two definitions. Consider G acting transitively on Ω and Δ. If the action of G on Ω is equivalent to the action of G on Δ, then for any $\omega \in \Omega$ and $\delta \in \Delta$, G_ω and G_δ are conjugate in G. If the action of G on Ω is permutationally isomorphic to the action of

G on Δ, then for any $\omega \in \Omega$ and $\delta \in \Delta$, G_ω and G_δ are conjugate under $\mathrm{Aut}(G)$. We say that subgroups H_1 and H_2 of G are *conjugate under* $\mathrm{Aut}(G)$ if there exists $\varphi \in \mathrm{Aut}(G)$ such that $H_2 = H_1^\varphi$. We have the following lemma similar to Lemma 2.1.7.

Lemma 2.1.8 *Suppose that the group G acts transitively on the two sets Ω and Δ, and let H be a stabilizer of a point in Ω. Then the action of G on Ω is permutationally isomorphic to the action of G on Δ, if and only if for some $\varphi \in \mathrm{Aut}(G)$, H^φ is the stabilizer of some point in Δ.*

Proof. Suppose that the action of G on Ω is permutationally isomorphic to the action of G on Δ. Then there exist $\varphi \in \mathrm{Aut}(G)$ and a bijection $\lambda : \Omega \to \Delta$ such that $(\alpha^g)^\lambda = (\alpha^\lambda)^{\varphi(g)}$ for any $\alpha \in \Omega$. Let H be the stabilizer of $\alpha \in \Omega$ in the first action. Then H^φ is the point stabilizer of α^λ in the second action.

Conversely, suppose that, for H the stabilizer of a point α of Ω, there exists $\varphi \in \mathrm{Aut}(G)$, such that H^φ is the stabilizer of a point, say β in Δ. Define a map $\lambda : \Omega \to \Delta$ as follows, for any $x \in G$,

$$\lambda : \alpha^x \to \beta^{\varphi(x)}.$$

It is easy to check that λ is well defined and is a bijection, and hence the action of G on Ω is permutationally isomorphic to the action of G on Δ with respect to λ and φ. □

2.2 Primitive groups, quasiprimitive groups and biquasiprimitive groups

Let G be a group acting transitively on a set Ω. A *block* is a non-empty subset Δ of Ω such that, for all $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \varnothing$. The singleton subsets of Ω, and Ω itself, are called the *trivial blocks*. Any other block is called a *non-trivial* block. We say that the group G is *primitive* if G has no non-trivial blocks on Ω. We say that G is *imprimitive* if it is not primitive. If Δ is a block for G, then the set $\{\Delta^g \mid g \in G\}$ forms a partition of Ω called a *block system*, and so we have $|\Delta| \,\big|\, |\Omega|$. This implies that a transitive permutation group of prime degree is primitive. Conversely, we say a partition $\mathcal{P}$ of Ω is *G-invariant* if, for every $\Delta \in \mathcal{P}$ and $g \in G$, we have $\Delta^g \in \mathcal{P}$. If a partition $\mathcal{P}$ is G-invariant then any member of $\mathcal{P}$ is a block for G, and hence $\mathcal{P}$ is the corresponding block system. A G-invariant partition $\mathcal{P}$ of Ω is said to be *trivial* if either $|\mathcal{P}| = 1$ or $|\mathcal{P}| = |\Omega|$. Otherwise, $\mathcal{P}$ is called *nontrivial*. So a group G acting on Ω is primitive if there are no nontrivial G-invariant partitions of Ω.

The following theorem states the relationship between blocks and subgroups, see for example [12, Theorem 1.5A].

Theorem 2.2.1 *Let G be a group acting transitively on a set Ω and let $\alpha \in \Omega$. Then there is a bijection between the collection of subgroups of G containing the point stabilizer G_α, and the blocks of G containing α. The bijection is the map $H \mapsto \alpha^H$ defined on the set of all subgroups H of G which contain G_α.*

We have the following corollary (see [12, Corollary 1.5A]).

Corollary 2.2.2 *Let G be a group acting transitively on a set Ω, and suppose $|\Omega| \geq 2$. Then G is primitive on Ω if and only if each point stabilizer G_α is a maximal subgroup of G.*

Let k be a positive integer. We say a permutation group G acting on a set Ω is *k-transitive* if the action of G on ordered k-tuples of distinct elements of Ω defined by $(\alpha_1, ..., \alpha_k)^g = (\alpha_1^g, ..., \alpha_k^g)$ is transitive. Note that a permutation group is 1-transitive if and only if it is transitive, and that, for all positive integers k, every $(k+1)$-transitive group is also k-transitive. For example, the symmetric group S_n is n-transitive and the alternating group A_n is $(n-2)$-transitive for $n > 2$. The k-transitive groups $(k \geq 2)$ arise as examples of primitive permutation groups, that is, every 2-transitive permutation group is primitive.

The following theorem concerns the orbits of a nontrivial normal subgroup of a transitive permutation group. This result will be used frequently in our proofs later.

Theorem 2.2.3 [12, Theorem 1.6A] *Let G be a finite group acting transitively on a finite set Ω, and $N \lhd G$. Then*

1. *the orbits of N form a block system for G;*
2. *if Δ and Δ' are two N-orbits then N^Δ and $N^{\Delta'}$ are permutationally isomorphic;*
3. *the number of orbits of N divides $|G : N|$.*

Corollary 2.2.4 *Let $G \leq \mathrm{Sym}(\Omega)$ be a finite primitive permutation group. Then every non-trivial normal subgroup of G is transitive on Ω.*

We say a permutation group is *quasiprimitive* if every nontrivial normal subgroup is transitive. All primitive groups are quasiprimitive by Corollary 2.2.4, while not all quasiprimitive groups are primitive. For example, the right regular representation of a nonabelian simple group is quasiprimitive but not primitive. We say a transitive permutation group G is *biquasiprimitive* if G is not quasiprimitive and has the property that each non-trivial normal subgroup has at most two orbits. Praeger proved structure theorems (similar to the O'Nan-Scott Theorem) for both finite quasiprimitive (see [43]) and finite biquasiprimitive (see [46]) permutation groups, (see also Section 2.3). Her motivations for these two results came from the studies of non-bipartite ([43]) and bipartite ([46]) 2-arc transitive graphs respectively. Moreover, in algebraic graph theory, these two concepts have been a common technique to analyze the groups of automorphisms of symmetric graphs. See also [44, 45] for surveys of this problem.

2.3 O'Nan-Scott type theorems

As discussed in the introduction, one major breakthrough in the study of the structure of finite primitive groups came with Michael O'Nan and Leonard Scott's theorem presented at the Santa Cruz conference on "Finite Groups" in 1979. (However the original statement of the O'Nan- Scott Theorem failed to acknowledge the TW case. There are at least two correct statements of the O'Nan- Scott Theorem which were made independently, and appeared at roughly the same time. One is made by Aschbacher and Scott [3] describing the TW case via cohomology, and another is made by Kovacs [27] who first proved that in the missing TW case all groups were twisted wreath products in a fairly natural representation over their twisting subgroup.) Fourteen years later, Cheryl E. Praeger developed a similar theorem for finite quasiprimitive groups. These theorems establish connections between permutation groups and finite simple groups, so that the classification of finite simple groups can be applied extensively in the study of permutation groups. Thus, these theorems, called *O'Nan-Scott type theorems*, form an important part of modern permutation group theory.

2.3.1 Centralizers and normalizers

The *centralizer* of a subgroup H in G is $C_G(H) := \{g \in G : gh = hg \text{ for all } h \in H\}$. In particular, the *center* of G is $Z(G) := C_G(G)$. Note that if $H \trianglelefteq G$, then the centralizer $C_G(H)$ is normal in G. The *normalizer* of a subgroup H in G is $N_G(H) := \{g \in G : gH = Hg\}$. Note that for all $H \leq G$, we have $H \trianglelefteq N_G(H) \leq G$. To analyze the minimal normal subgroups of a transitive permutation group, we need the following result concerning centralizers.

Theorem 2.3.1 [12, Theorem 4.2A] *Let G be a transitive subgroup of* $\mathrm{Sym}(\Omega)$*, and α a point in Ω. Let C be the centralizer of G in* $\mathrm{Sym}(\Omega)$*. Then:*

(i) C is semiregular, and $C \cong N_G(G_\alpha)/G_\alpha$;

(ii) C is transitive if and only if G is regular;

(iii) if C is transitive, then C is conjugate to G in $\mathrm{Sym}(\Omega)$ *and hence C is regular;*

(iv) $C = 1$ if and only if G_α is self-normalizing in G (that is, $N_G(G_\alpha) = G_\alpha$).

Next we consider the normalizer of a transitive group. Let G be a transitive subgroup of $\mathrm{Sym}(\Omega)$. Then the normalizer of G in $\mathrm{Sym}(\Omega)$ acts naturally on the set G by conjugation: this gives a homomorphism

$$\Psi : N_{\mathrm{Sym}(\Omega)}(G) \to \mathrm{Aut}(G) \text{ where } \Psi(x) : u \mapsto x^{-1}ux \text{ (for each } u \in G).$$

The kernel Ker Ψ is the centralizer of G in $\mathrm{Sym}(\Omega)$, and so we have

$$N_{\mathrm{Sym}(\Omega)}(G)/C_{\mathrm{Sym}(\Omega)}(G) \leq \mathrm{Aut}(G).$$

By Theorem 2.3.1 (iv), Ψ is injective exactly when $N_G(G_\alpha) = G_\alpha$. By contrast, if G is regular (so that $G_\alpha = 1$ and $N_G(G_\alpha) = G$), then the semidirect product of G by $\mathrm{Aut}(G)$ with the natural action of $\mathrm{Aut}(G)$ on G, denoted by $G \rtimes \mathrm{Aut}(G)$, is the normalizer of G in $\mathrm{Sym}(\Omega)$. This is also called the *holomorph* of the regular group G, denoted by $\mathrm{Hol}(G)$.

2.3.2 The socle

A *minimal normal subgroup* of a nontrivial group G is a nontrivial normal subgroup M of G which does not properly contain any other nontrivial normal subgroup. The *socle* of a group G is the subgroup generated by the set of all minimal normal subgroups of G, and is denoted by $\mathrm{soc}(G)$. Every nontrivial finite group has at least one minimal normal subgroup, so has a nontrivial socle.

Theorem 2.3.2 [12, Theorem 4.3A] *Let G be a nontrivial finite group.*

(1) If N is a minimal normal subgroup of G, and L is any other normal subgroup of G, then either $N \leq L$ or $\langle N, L\rangle = N \times L$.

(2) There exist minimal normal subgroups $N_1, ..., N_m$ of G such that $\mathrm{soc}(G) = N_1 \times \cdots \times N_m$.

(3) Every minimal normal subgroup N of G is a direct product $N = T_1 \times \cdots \times T_k$ where the T_i are simple normal subgroups of N which are conjugate under G.

(4) If the subgroups N_i in (2) are all nonabelian, then $N_1, ..., N_m$ are the only minimal normal subgroups of G. Similarly, if the T_i in (3) are nonabelian, then these are the only minimal normal subgroups of N.

Lemma 2.3.3 *Let G be a quasiprimitive permutation group on Ω. Then either* $\mathrm{soc}(G)$ *is a minimal normal subgroup of G, or* $\mathrm{soc}(G) = M \times N$ *such that $M \cong N$, and both M and N are nonabelian minimal normal subgroups and are regular on Ω. In particular,* $\mathrm{soc}(G) \cong T^k$ *where T is a simple group and $k \geq 1$.*

Proof. Let M be a minimal normal subgroup of G. Let $C = C_G(M)$. By Theorem 2.3.1 (i), C is semiregular. Since $C \lhd G$, either $C = 1$ or C is regular on Ω and hence a minimal normal subgroup of G. Theorem 2.3.2 (1) shows that every minimal normal subgroup of G distinct from M is contained in C. Thus in all cases $\mathrm{soc}(G) = MC$ which equals M or $M \times C$ depending on whether or not $C \leq M$.

If $C = 1$, then M is the unique minimal normal subgroup of G. Hence Theorem 2.3.2 (3) implies that $\mathrm{soc}(G) = M = T^k$ where T is a nonabelian simple group.

If $C \cap M \neq \{1\}$, then $C = M$ is the unique minimal normal subgroup of G. Hence $\mathrm{soc}(G) = M \cong Z_p^k$ for a prime p.

In the remaining case, $C \cap M = 1$ and $C \neq 1$. So M is nonabelian. Let $N = C$. By Theorem 2.3.1 (i)(ii)(iii), $M \cong N$ are both regular and hence are nonabelian minimal normal subgroups of G. By Theorem 2.3.2 (1), M and N are the only minimal normal subgroups of G. Hence $\mathrm{soc}(G) = M \times N \cong T^k$ for some nonabelian simple group T. □

2.3.3 Product actions

A permutation group G on Ω is said to preserve a product decomposition Δ^m of Ω, $m \geq 2$, if Ω can be identified with the Cartesian product $\Delta^m = \Delta_1 \times \cdots \times \Delta_m$ (where $\Delta_i = \Delta$ for all $1 \leq i \leq m$) in such a way that G is a subgroup of the wreath product

$$W = \mathrm{Sym}(\Delta) \wr S_m = \mathrm{Sym}(\Delta)^m \rtimes S_m$$

with a product action. That is, for $g = (g_1, ..., g_m)$ in the base group $\mathrm{Sym}(\Delta)^m$,

$$(\delta_1, ..., \delta_m)^g = (\delta_1^{g_1}, ..., \delta_m^{g_m}),$$

and for t in the top group S_m,

$$(\delta_1, ..., \delta_m)^{t^{-1}} = (\delta_{1^t}, ..., \delta_{m^t}),$$

where $(\delta_1, ..., \delta_m) \in \Omega = \Delta^m$. The projection of $W = \mathrm{Sym}(\Delta)^m \rtimes S_m$ onto S_m will be denoted by π. Consider π as a permutation representation of W. Then for $1 \leq i \leq m$ the point stabilizer

$$W_i = \mathrm{Sym}(\Delta_i) \times (\mathrm{Sym}(\Delta) \wr S_{m-1})$$

is the group of all the elements of W which fix i under the action of π. And let π_i denote the projection $W_i \to \mathrm{Sym}(\Delta_i)$. The subgroup $G \cap W_i$ consists of all the elements of G which fix the i-th component Δ_i setwise. The restriction of π_i to $G \cap W_i$ is a homomorphism from $G \cap W_i$ onto a subgroup of $\mathrm{Sym}(\Delta_i)$, and we denote this homomorphism also by π_i,

$$\pi_i : G \cap W_i \to \mathrm{Sym}(\Delta_i).$$

Suppose next that $\pi(G)$ is transitive, then the groups $\pi_i(G \cap W_i) \leq \mathrm{Sym}(\Delta_i)$ are permutationally isomorphic to each other. Set $G_0 := \pi_1(G \cap W_1)$ and $\Delta = \Delta_1$ so that $G_0 \leq \mathrm{Sym}(\Delta)$. If $\pi(G)$ is transitive, then the group G_0 is called the *group induced by G on* Δ.

Below is a classical result concerning the primitive product action of a wreath product (see [12, Lemma 2.7A]).

Lemma 2.3.4 *Suppose that H and K are finite groups where H acts on a set Δ and K acts on a set of k elements. The wreath product $H \wr K$ acts primitively in product action on Δ^k if and only if K is transitive and H is primitive but not regular on Δ.*

A finite group G is said to be *almost simple* if $T \leq G \leq \mathrm{Aut}(T)$ for a nonabelian simple group T. Lemma 2.3.4 shows us how to construct new primitive permutation groups from a small primitive permutation group by using the product action.

Example 2.3.5 Product action of a primitive group G on Ω (the primitive type PA): For some $k > 1$ and almost simple primitive group H on Δ with socle T, we have $\Omega = \Delta^k$, $\mathrm{soc}(G) = T^k$, $T^k \leq G \leq H \wr S_k \leq \mathrm{Sym}(\Delta) \wr S_k$, and G acts transitively by conjugation on the set of k simple direct factors of $\mathrm{soc}(G)$, and H is induced by G on Δ.

2.3.4 The direct product of groups

Let $H = H_1 \times \cdots \times H_k$ be a direct product of groups. For each $i \in \{1, ..., k\}$, we denote the natural projection map from H to H_i by π_i.

Definition 2.3.6 Suppose that G is a subgroup of $H = \Pi_{i=1}^k H_i$.

1. We say that G is a *subdirect subgroup* of H if for each i the projection map $\pi_i : G \to H_i$ is surjective.

2. We say that G is a *diagonal subgroup* of H if for each i the projection map $\pi_i : G \to H_i$ is injective.

3. We say that G is a *full diagonal subgroup* of H if G is both a subdirect and diagonal subgroup of H.

The following lemma plays a key role in the proofs of the O'Nan-Scott theorems. The first part of the following lemma appears in [12, Lemma 4.5B], the second part can be found in [48, Lemma, p. 328] and the third part can be found in [26, Proposition 5.2.5(i)].

Lemma 2.3.7 *Let H be a finite direct product $\Pi_{i=1}^{k} T_i$ of isomorphic finite nonabelian simple groups, and let M be a subgroup of H.*

1. *If M is a full diagonal subgroup of H, then M is self normalizing in H.*
2. *If M is a subdirect subgroup of H, then there exists a partition $\{I_1, ..., I_l\}$ of $\{1, ..., k\}$ such that M is the direct product $\Pi_{j=1}^{l} M_j$, where for each j, M_j is a full diagonal subgroup of $\Pi_{i \in I_j} T_i$.*
3. *If M is a normal subgroup of H, then $M = \Pi_{j \in J} T_j$ where J is a nonempty subset of $\{1, ..., k\}$.*

2.3.5 The O'Nan-Scott theorems

In this subsection, we begin by giving a brief description of the class of finite quasiprimitive permutation groups. Note that the eight types of finite quasiprimitive permutation groups described below are in a fashion very similar to the description given by the O'Nan-Scott Theorem for finite primitive permutation groups, so we will also talk about the corresponding primitive types by indicating the difference between quasiprimitive groups and primitive groups type by type. For a detailed description, see [44, 45].

Let G be a finite quasiprimitive permutation group, and let $\alpha \in \Omega$. Then by Lemma 2.3.3, either $\mathrm{soc}(G)$ is a minimal normal subgroup of G, or $\mathrm{soc}(G)$ contains exactly two minimal normal subgroups of G.

Assume first $\mathrm{soc}(G) = M \times N$, where M and N are two minimal normal subgroups of G. By Lemma 2.3.3, $M \cong N$, and M, N are nonabelian and regular. Identify Ω with $M = T^k$. Then G is contained in the holomorph of M, that is $G \leq M \rtimes \mathrm{Aut}(M)$. We subdivide these groups into two types as follows.

HS (holomorph of a simple group): $\Omega = T$, a finite nonabelian simple group, and we have $T \rtimes \mathrm{Inn}(T) \leq G \leq \mathrm{Hol}(T) = T \rtimes \mathrm{Aut}(T)$.

HC (holomorph of a compound group): $\Omega = T^k$, where $k > 1$ and T is a finite nonabelian simple group, and $M \rtimes \mathrm{Inn}(M) \leq G \leq \mathrm{Hol}(M) = M \rtimes \mathrm{Aut}(M)$. Further, G_α acts transitively by conjugation on the set of k simple direct factors of M.

Assume next that $\mathrm{soc}(G) = M$ is an abelian minimal normal subgroup. Then we may identify Ω with $M = Z_p^d$ which may be viewed as a d-dimensional vector space over a field of prime order p. Choosing α as the zero vector, we have that G_α is an irreducible subgroup of nonsingular linear transformations of M. We obtain the following type, which is also called the *affine* type.

HA (holomorph of an abelian group): $\Omega = Z_p^d$ for a prime p and positive integer d and G is the semidirect product $G = MG_0$, a subgroup of the affine group $\mathrm{AGL}(d, p) = Z_p^d \rtimes \mathrm{GL}(d, p)$ on Ω, where M is the group of translations and G_0 is an irreducible subgroup of $\mathrm{GL}(d, p)$.

There are five further types and for each type, $M = \mathrm{soc}(G) = T_1 \times \cdots \times T_k$, for some positive integer k, and M is the unique minimal normal subgroup, where each $T_i \cong T$, a nonabelian simple group.

AS (almost simple): $\mathrm{soc}(G) = T$ is a finite nonabelian simple group. $T \leq G \leq \mathrm{Aut}(T)$ and $G = TG_\alpha$. That is, G is almost simple.

SD (simple diagonal): $\mathrm{soc}(G) = M = T^k$ with $k \geq 2$ and T nonabelian simple, and $M_\alpha = \{(t, ..., t) : t \in T\} \cong T$, a full diagonal subgroup of M. Further G acts transitively by conjugation on the set of k simple direct factors of $\mathrm{soc}(G)$.

CD (compound diagonal): $\mathrm{soc}(G) = M = T^k$ with $k \geq 4$ and T nonabelian simple, and $M_\alpha \cong T^l$ with $2 \leq l < k$ and $l \mid k$. Further, G acts transitively by conjugation on the set of k simple direct factors of $\mathrm{soc}(G)$.

TW (twisted wreath product): $\mathrm{soc}(G)$ is nonabelian, non-simple and minimal normal in G and $\mathrm{soc}(G)$ acts regularly on Ω.

PA (product action): G preserves a product structure Δ^k where $k \geq 2$ on a G-invariant partition of Ω (possibly with parts of size 1) and the subgroup of $\mathrm{Sym}(\Delta)$ induced by G is quasiprimitive of type AS with socle T.

The following theorem is the O'Nan-Scott Theorem for finite quasiprimitive permutation groups which was proved by Praeger in 1993.

Theorem 2.3.8 [43, Theorem 1] *Each finite quasiprimitive permutation group is permutationally isomorphic to a quasiprimitive group of exactly one of the quasiprimitive types HA, HS, HC, AS, SD, CD, TW, PA.*

Note that groups of the three types HA, HS and HC are always primitive. For types AS, SD, CD, TW, we need more strict conditions to guarantee primitivity. The last type PA is the furthest from the corresponding primitive type; primitive groups of product action type were introduced in Example 2.3.5. Now we state the O'Nan-Scott Theorem for primitive permutation groups.

Theorem 2.3.9 [33, 48] *Each finite primitive permutation group is permutationally isomorphic to a primitive group of exactly one of the primitive types HA, HS, HC, AS, SD, CD, TW, PA.*

The following result, due to Burnside, is also a structure theorem for one special class of primitive permutation groups (see [12, Section 3.5]). We will need this result later.

Theorem 2.3.10 [Burnside] *Let G be a transitive permutation group of prime degree p. Then either G is 2-transitive or G is permutationally isomorphic to a subgroup of the affine group* $\mathrm{AGL}(1, p)$.

Finally, we would like to mention that Praeger has proved a structure theorem [46, Theorem 1.1] for biquasiprimitive permutation groups. The theorem is also analogous to the O'Nan-Scott Theorem for finite primitive permutation groups.

2.4 General results about k-closures

First, we repeat the basic definitions about k-closures since the main theme of this thesis is the study of k-closures. Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group on a set Ω, and let k be a positive integer. Then G has a natural action on $\Omega^k = \Omega \times \cdots \times \Omega$ (k copies), given by $(\alpha_1, ..., \alpha_k)^g = (\alpha_1^g, ..., \alpha_k^g)$. In 1969, Wielandt [53] defined the *k-closure* of G to be the group

$$G^{(k)} := \{g \in \mathrm{Sym}(\Omega) \mid \Delta^g = \Delta \text{ for each orbit } \Delta \text{ of } G \text{ on } \Omega^k\},$$

that is, $G^{(k)}$ is the largest subgroup of $\mathrm{Sym}(\Omega)$ with the same set of orbits on Ω^k as G. For example, if G is k-transitive on Ω, then $G^{(k)}$ is the full symmetric group $\mathrm{Sym}(\Omega)$. We say that G is *k-closed* if $G = G^{(k)}$. A *k-relation* on Ω is a subset of $\Omega^k = \Omega \times \cdots \times \Omega$ (k copies). We say that Δ is a G-invariant k-relation if Δ is a k-relation on Ω and $\Delta^g = \Delta$ for all $g \in G$, and we denote the set of all G-invariant k-relations by k-rel G. Let $L \leq \mathrm{Sym}(\Omega)$ be another permutation group on Ω. We say G is *k-equivalent* to L if k-rel $G = k$-rel L. This condition is equivalent to the condition that G and L have the same orbit set on Ω^k. Thus, G is k-equivalent to $G^{(k)}$.

Wielandt [53] began a systematic study of k-closures of groups. Often knowledge of $G^{(k)}$ provides information about G. We collect some useful fundamental results here. The proofs of Lemma 2.4.1 (1), (2), (3) and (4) can be found in Theorems 5.8, 5.7, 5.12, 4.3, 5.9 and Lemma 4.12 of [53] respectively.

Lemma 2.4.1 [53, Wielandt] *Let $k \geq 1$ and let G and L be permutation groups on a set Ω. Then*

(1) $G \leq G^{(k+1)} \leq G^{(k)}$.

(2) If $G \leq L$, then $G^{(k)} \leq L^{(k)}$.

(3) If there exist $\alpha_1, ..., \alpha_k \in \Omega$ such that $G_{\alpha_1,...,\alpha_k} = 1$, then $G^{(k+1)} = G$.

(4) If G is $(k+1)$-equivalent to L, then G is k-equivalent to L and for any $\alpha \in \Omega$, G_α is k-equivalent to L_α.

(5) $(G^{(k)})^{(k)} = G^{(k)}$.

The following is Wielandt's Dissection Theorem [53, Theorem 6.5] and will be very useful for us in determining 2-closures. Note that Wielandt's Dissection Theorem is also valid when G is an infinite permutation group.

Theorem 2.4.2 (Wielandt's Dissection Theorem) *Let G be a permutation group on Ω and let Γ and Δ be disjoint subsets of Ω invariant under G such that $\Omega = \Gamma \cup \Delta$. Then the following are equivalent:*

1. $G^\Gamma \times G^\Delta \leq G^{(2)}$.

2. $G = G_\delta G_\gamma$ for each $\delta \in \Delta$ and $\gamma \in \Gamma$.

3. G_δ is transitive on γ^G and G_γ is transitive on δ^G for each $\delta \in \Delta$ and $\gamma \in \Gamma$.

Proposition 2.4.3 [7, Theorem 5.1] *Let $G_1 \leq \mathrm{Sym}(\Omega_1)$ and $G_2 \leq \mathrm{Sym}(\Omega_2)$ be transitive permutation groups. Then in the action of $G_1 \times G_2$ on $\Omega_1 \times \Omega_2$, given by $(\alpha, \beta)^{(g_1,g_2)} = (\alpha^{g_1}, \beta^{g_2})$, we have $(G_1 \times G_2)^{(2)} = G_1^{(2)} \times G_2^{(2)}$.*

The next proposition, due to Praeger and Saxl, concerns the 2-closure of the product action of the wreath product.

Proposition 2.4.4 *Let $G \leq \mathrm{Sym}(\Omega)$ and $K \leq S_k$. Then in the product action on Ω^k we have that $G^{(2)} \wr K \leq (G \wr K)^{(2)}$.*

Proof. This is proved by Praeger and Saxl [47, Propositon 3.1] where they assumed that K is transitive. However the argument of their proof does not require this assumption. □

Lemma 2.4.5 *Suppose $k \geq 1$ and G_1, G_2, L_1, L_2 are permutation groups on Ω such that $\langle G_1, G_2\rangle = G_1G_2$ and $\langle L_1, L_2\rangle = L_1L_2$. Suppose also that G_i is k-equivalent to L_i for $i = 1, 2$. Then G_1G_2 is k-equivalent to L_1L_2.*

Proof. Suppose $(\alpha_1, ..., \alpha_k) \in \Omega^k$ and $x_1x_2 \in L_1L_2$ where $x_i \in L_i$ for $i = 1, 2$. Since G_i is k-equivalent to L_i for $i = 1, 2$, there exist $g_i \in G_i$ for $i = 1, 2$, such that

$$(\alpha_1, ..., \alpha_k)^{x_1} = (\alpha_1, ..., \alpha_k)^{g_1},$$

and

$$(\alpha_1^{x_1}, ..., \alpha_k^{x_1})^{x_2} = (\alpha_1^{g_1}, ..., \alpha_k^{g_1})^{x_2} = (\alpha_1^{g_1}, ..., \alpha_k^{g_1})^{g_2}.$$

Hence

$$(\alpha_1, ..., \alpha_k)^{x_1x_2} = (\alpha_1, ..., \alpha_k)^{g_1g_2}.$$

Thus each L_1L_2-orbit in Ω^k is invariant under G_1G_2, and similarly each G_1G_2-orbit in Ω^k is invariant under L_1L_2. Therefore G_1G_2 is k-equivalent to L_1L_2 on Ω. □

The following lemma is an easy result about the k-closure of an induced quotient action.

Lemma 2.4.6 *Suppose $k \geq 1$ and $G, L \leq \mathrm{Sym}(\Omega)$. Suppose further that G is k-equivalent to L on Ω. Let $N \leq G \cap L$ such that N is intransitive and normal in both G and L. Let $\overline{\Omega}$ be the set of N-orbits. Then $G^{\overline{\Omega}}$ is k-equivalent to $L^{\overline{\Omega}}$ on $\overline{\Omega}$.*

Remark: The kernels of G and L on $\overline{\Omega}$ both contain N.

Proof. Set $\overline{G} = G^{\overline{\Omega}}$ and $\overline{L} = L^{\overline{\Omega}}$. For $\alpha \in \Omega$, let $[\alpha]$ denote the N-orbit containing α. Suppose $([\alpha_1], ..., [\alpha_k]) \in \overline{\Omega}^k$. For any $\bar{x} = x^{\overline{\Omega}} \in \overline{L}$ where $x \in L$, the normality of N implies that

$$([\alpha_1], ..., [\alpha_k])^{\bar{x}} = ([\alpha_1^x], ..., [\alpha_k^x]).$$

Since G is k-equivalent to L on Ω, there exists an element $g \in G$ such that

$$(\alpha_1^x, ..., \alpha_k^x) = (\alpha_1^g, ..., \alpha_k^g).$$

Hence

$$([\alpha_1], ..., [\alpha_k])^{\bar{x}} = ([\alpha_1], ..., [\alpha_k])^{\bar{g}} \text{ where } \bar{g} = g^{\overline{\Omega}} \in \overline{G}.$$

Thus each $\overline{L}$-orbit in $\overline{\Omega}^k$ is $\overline{G}$-invariant and similarly each $\overline{G}$-orbit in $\overline{\Omega}^k$ is $\overline{L}$-invariant. Therefore $\overline{G}$ is k-equivalent to $\overline{L}$ on $\overline{\Omega}$. □

2.5 Algebraic graph theory

2.5.1 Basic definitions

A *digraph* (or *directed graph*) is a pair $\Gamma = (\Omega, E)$ where Ω is a set whose elements are called the *vertices* of Γ, and E is a subset of $\Omega \times \Omega$ whose elements are called *edges* or *arcs* of Γ. For any vertex α of the digraph $\Gamma = (\Omega, E)$, we define the *neighbourhood* of the vertex α to be $\Gamma(\alpha) := \{\beta \,|\, (\alpha, \beta) \in E\}$. Similarly a *graph* is a pair $\Gamma = (\Omega, E)$ where Ω is the set of *vertices* of Γ, and E is a subset of unordered pairs of distinct vertices which are called the *edges* of Γ; the ordered pairs (α, β) of adjacent vertices (that is, $\{\alpha, \beta\} \in E$) are called the *arcs* of Γ. Thus, for a digraph, edges and arcs are the same, but this is not the case for a graph. Note that, according to our definition, a digraph may or may not have *loops* (edges of the form (α, α)), but a graph does not have any loops. Also for any vertex α of the graph $\Gamma = (\Omega, E)$, we define the *neighbourhood* of the vertex α to be $\Gamma(\alpha) := \{\beta \,|\, \{\alpha, \beta\} \in E\}$. Again, all (di)graphs $\Gamma = (\Omega, E)$ considered in this thesis are finite, that is, the vertex set Ω is a finite set.

If α and β are vertices of a digraph Γ, then a *directed path* in Γ from α to β of length d is a list of $d + 1$ vertices

$$\alpha_0 = \alpha, \alpha_1, ..., \alpha_d = \beta$$

such that $(\alpha_{i-1}, \alpha_i) \in E$ for $i = 1, ..., d$. If we only assume that, for each i, either (α_{i-1}, α_i) or (α_i, α_{i-1}) lies in E, then the path is called *undirected.* We say that a digraph Γ is *connected* if for every pair of vertices α and β there is an undirected path from α to β, and that Γ is *strongly connected* if this path can always be chosen to be directed. In a graph, we clearly do not have to distinguish between directed and undirected paths. So we say a graph Γ is *connected* if for every pair of vertices α and β there is a path from α to β.

An *automorphism* of a graph or a digraph $\Gamma = (\Omega, E)$ is an element g of $\mathrm{Sym}(\Omega)$ such that $e^g \in E$ if and only if $e \in E$. The set of all automorphisms forms a subgroup $\mathrm{Aut}(\Gamma)$ of $\mathrm{Sym}(\Omega)$, called the *automorphism group* of Γ. If a subgroup G of $\mathrm{Aut}(\Gamma)$ is transitive on the vertex set Ω, the edge set E, or the set of arcs of Γ, we say that Γ is G-vertex-transitive, G-edge-transitive, or G-arc-transitive respectively. Often we omit the prefix "G ".

The full automorphism group of a (di)graph is 2-closed since any permutation of the vertex set which preserves the orbits of $\mathrm{Aut}(\Gamma)$ on ordered pairs preserves adjacency. However, not every 2-closed permutation group is the full automorphism group of some digraph or graph. For example, let $G = \{1, (12)(34), (13)(24), (14)(23)\}$ be a permutation group acting on the set $\Omega = \{1, 2, 3, 4\}$. Since G is regular, G is 2-closed by Lemma 2.4.1

(3). However, G is not the full automorphism group of any graph or digraph.

Next we define s-arc transitive graphs. They are very important families of highly symmetric graphs and the study of s-arc transitive graphs became the motivation of the study of quasiprimitive permutation groups by Praeger [43]. For a positive integer s, an *s-arc* in a graph $\Gamma = (\Omega, E)$ is an $(s+1)$-tuple $(\alpha_0, ..., \alpha_s)$ of vertices such that $(\alpha_{i-1}, \alpha_i) \in E$ for $1 \leq i \leq s$ and $\alpha_{i-1} \neq \alpha_{i+1}$ for $1 \leq i \leq s-1$. Further, Γ is said to be (G, s)-arc transitive (or simply *s-arc transitive*) if $G \leq \mathrm{Aut}(\Gamma)$ and G is transitive on the s-arcs of Γ. Note that a 1-arc transitive graph is just an arc-transitive graph.

Finally, we define bipartite graphs. A graph $\Gamma = (\Omega, E)$ is said to be *bipartite* if its vertex set Ω can be partitioned into two parts, say Δ_1, Δ_2, in such a way that every edge of Γ joins a vertex of Δ_1 to a vertex of Δ_2. The study of vertex transitive connected bipartite graphs leads to the study of biquasiprimitive permutation groups, see Praeger's paper [46]. These tell us that the theory of vertex transitive graphs has developed in parallel with the theory of transitive permutation groups and that these two theories have influenced each other deeply and grow together fast.

2.5.2 Orbital (di)graphs

Let G be a transitive permutation group on Ω. We will construct a natural family of digraphs for G, (see for example [39]).

We begin with the natural action of G on the set $\Omega \times \Omega$:

$$(\alpha, \beta)^g = (\alpha^g, \beta^g) \text{ for all } \alpha, \beta \in \Omega, g \in G.$$

The G-orbits in $\Omega \times \Omega$ are called the *G-orbitals* on Ω (or simply orbitals). A *generalized orbital* is a non-empty union of G-orbitals. The orbital $\Delta_0 := \{(\alpha, \alpha) \mid \alpha \in \Omega\}$ is called the *trivial* G-orbital, and the other orbitals are called *nontrivial*. For each (generalized) orbital Δ there is a *paired* (generalized) orbital Δ^*, namely, $\Delta^* = \{(\beta, \alpha) \mid (\alpha, \beta) \in \Delta\}$. If $\Delta = \Delta^*$, we say that the (generalized) orbital Δ is *self-paired*.

Let Δ be a (generalized) G-orbital. Then the associated *(generalized) orbital digraph* is the digraph (Ω, Δ). As it will seldom cause confusion, we shall denote this digraph also by Δ. Note that if Δ is self-paired and $\Delta_0 \not\subseteq \Delta$, then the digraph Δ contains no loops and the edges occur in pairs of the form $\{(\alpha, \beta), (\beta, \alpha)\}$. Thus we may replace each such pair by the unordered pair $\{\alpha, \beta\}$ and thereby obtain a graph, called the *(generalized) orbital graph* associated with Δ.

Let Δ be a generalized orbital digraph (or graph) of G. The following properties follow from the definition directly.

1. $G \leq \mathrm{Aut}(\Delta)$.

2. G is transitive on the vertices of Δ, and so Δ is vertex-transitive.

3. G is transitive on the arcs of the digraph Δ if and only if Δ is a G-orbital.

4. G is transitive on arcs of the graph Δ if and only if Δ is a self-paired nontrivial G-orbital.

5. $G \leq G^{(2)} \leq \mathrm{Aut}(\Delta)$ since $G^{(2)}$ and G have the same orbitals. Hence we may obtain information about $G^{(2)}$ by studying the orbital (di)graphs of G.

There is a 1-1 correspondence between the orbitals of G and the orbits in Ω of the stabilizer G_α of a point α. If Δ is a G-orbital then the corresponding G_α-orbit in Ω is $\Delta(\alpha) := \{\beta \in \Omega \,|\, (\alpha, \beta) \in \Delta\}$, the neighbourhood of α in the orbital digraph Δ. The number of G-orbitals, or equivalently the number of G_α-orbits in Ω, is called the *rank* of G.

2.5.3 Vertex-transitive graphs

First we make a few general elementary but important observations about a finite G-vertex-transitive graph $\Gamma = (\Omega, E)$. The following all hold.

1. If Γ is not connected, then all of its connected components are isomorphic, and are themselves vertex-transitive. This enables us to reduce various research problems concerning vertex-transitive graphs to the case of connected graphs.

2. The graph Γ is *regular*, that is, there is a constant k such that every vertex α is adjacent to exactly k other vertices. The constant k is called the *valency* of Γ.

3. For $\alpha, \beta \in \Omega$, $G_\alpha^{\Gamma(\alpha)}$ is permutationally isomorphic to $G_\beta^{\Gamma(\beta)}$. This enables us to add certain group theoretic "local conditions" to the permutation group $G_\alpha^{\Gamma(\alpha)}$, for some fixed α, and have these conditions satisfied for all vertices.

4. Γ is a generalized orbital graph for G, for the self-paired generalized orbital $\Delta := \{(\alpha, \beta) \,|\, \{\alpha, \beta\} \in E\}$.

5. Γ is G-arc-transitive if and only if Γ is an orbital graph for G, namely for the self-paired orbital $\Delta := \{(\alpha, \beta) \,|\, \{\alpha, \beta\} \in E\}$.

An important family of vertex-transitive graphs is the family of Cayley graphs.

Definition 2.5.1 Let G be a finite group, and let $S \subseteq G$ such that $1_G \notin S$. The *Cayley digraph* $\mathrm{Cay}(G, S)$ of G relative to S is the digraph with vertex set G such that, for $x, y \in G$, the pair (x, y) is an arc if and only if $xy^{-1} \in S$. Further, if $S = S^{-1} := \{s^{-1} \mid s \in S\}$, then (x, y) is an arc if and only if (y, x) is an arc, and we define the *Cayley graph* of G relative to S as the graph with vertex set G such that $\{x, y\}$ is an edge if and only if $xy^{-1} \in S$. We denote this undirected graph also by $\mathrm{Cay}(G, S)$, as its meaning will be clear from the context.

A Cayley (di)graph $\mathrm{Cay}(G, S)$ is (strongly) connected if and only if $\langle S \rangle = G$. Moreover, the group G acting on itself in its right regular representation is a subgroup of the automorphism group of $\mathrm{Cay}(G, S)$ and acts transitively on G. Thus all Cayley (di)graphs are vertex-transitive. The existence of a subgroup of $\mathrm{Aut}(\Gamma)$ acting regularly on vertices characterizes Cayley (di)graphs. We may compare the following lemma with the Polycirculant Conjecture (Conjecture 1.3.1).

Lemma 2.5.2 [4, Lemma 16.3] *A (di)graph $\Gamma = (\Omega, E)$ is isomorphic to a Cayley (di)graph for a group G if and only if $\mathrm{Aut}(\Gamma)$ has a subgroup $\overline{G}$ isomorphic to G such that $\overline{G}$ is regular on Ω.*

When we consider finite G-vertex-transitive, $(G, 2)$-arc transitive graphs, the property of 2-arc transitivity for vertex-transitive graphs is equivalent to a condition on the vertex stabilizer G_α, that is, $G_\alpha^{\Gamma(\alpha)}$ is 2-transitive, a so-called "local condition" on Γ. A more general class of vertex-transitive graphs defined by a local property is the following.

Definition 2.5.3 A G-vertex-transitive graph $\Gamma = (\Omega, E)$ is said to be *G-locally quasiprimitive* if, for $\alpha \in \Omega$, G_α is quasiprimitive on $\Gamma(\alpha)$.

We give some examples of G-vertex-transitive and G-locally quasiprimitive graphs.

Example 2.5.4 Let Γ be a G-vertex-transitive graph.

1. Suppose also that Γ is $(G, 2)$-arc transitive. Then Γ is G-locally quasiprimitive since G_α is 2-transitive (and hence quasiprimitive) on $\Gamma(\alpha)$ for each $\alpha \in \Omega$.

2. Suppose also that Γ is G-arc transitive with valency p for a prime p. Then Γ is G-locally quasiprimitive, since G_α is primitive on $\Gamma(\alpha)$ for each $\alpha \in \Omega$.

We finish this section by stating the following theorem which was proved by Praeger [40]. This theorem is very important for our proof of Theorem 8.1.8, see also [30, Theorem 1.3].

Theorem 2.5.5 [40, Section 1] *Let $\Gamma = (\Omega, E)$ be a finite connected G-vertex-transitive, G-locally quasiprimitive graph, and let N be a normal subgroup of G. Then one of the following holds.*

1. *N is transitive on Ω; or*

2. *Γ is bipartite and the N-orbits in Ω are the two parts of the bipartition of Γ; or*

3. *N has more than two orbits in Ω, and N is semiregular on Ω.*

Chapter 3

Linear Algebra and Geometries

Our first research problem is to investigate the 3-closures of affine permutation groups, see Question 1.2.1. Let $V(d,p)$ be a vector space of dimension d over a finite field F_p with $d \geq 1$ and p a prime. We say that G is an *affine* permutation group if $G = NH$ acting on the vector space $V(d,p)$ where $N = Z_p^d$ is the group of translations and $H \leq \mathrm{GL}(d,p)$ is the stabilizer of the zero vector. In this chapter, we discuss linear algebra techniques we will use in our proof and talk about some geometries associated with the vector spaces.

3.1 Tensor product spaces

In this section, we discuss tensor product spaces. We begin by giving definitions and basic properties, for a detailed description see for example [19, 29].

Let U, V be finite dimensional vector spaces over F_q. Let $\{u_1, ..., u_n\}$ be a basis of U, and let $\{v_1, ..., v_m\}$ be a basis of V. For each pair (i,j) with $1 \leq i \leq n$ and $1 \leq j \leq m$, let t_{ij} be a letter. We may define a vector space W over F_q that is generated by the set $\{t_{ij} \,|\, 1 \leq i \leq n \text{ and } 1 \leq j \leq m\}$, that is to say, W is all the F_q-linear combinations of the t_{ij}. We denote W by $U \otimes V$, the *tensor product* space of U and V. Then W is a vector space of dimension nm with an F_q-basis $\{t_{ij} \,|\, 1 \leq i \leq n \text{ and } 1 \leq j \leq m\}$. If $u = x_1u_1 + \cdots + x_nu_n$ and $v = y_1v_1 + \cdots + y_mv_m$, with x_i, y_j in F_q, then we define the *tensor product* of u and v, denoted by $u \otimes v$, to be the element

$$u \otimes v = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i y_j t_{ij}$$

of W. In particular, $u_i \otimes v_j = t_{ij}$. In this way, we can define a map from $U \times V$ to W by

$$(u,v) \mapsto u \otimes v.$$

Note that the map is not onto.

The following theorem can be found in [19, §1.4, §1.13], which proves that the above map is a bilinear map, and that the definition of $U \otimes V$ is independent of the choice of the bases of U and V.

Theorem 3.1.1 *With the notation above, let U, V be finite dimensional vector spaces over F_q. And let $W = U \otimes V$. Then*

1. *If $u, u' \in U$ and $v \in V$, then $(u + u') \otimes v = u \otimes v + u' \otimes v$.*
2. *If $u \in U$ and $v, v' \in V$, then $u \otimes (v + v') = u \otimes v + u \otimes v'$.*
3. *If $\lambda \in F_q$, $u \in U$ and $v \in V$, then $(\lambda u) \otimes v = u \otimes (\lambda v) = \lambda(u \otimes v)$.*
4. *Let $\{u'_1, ..., u'_n\}$ be any basis of U, and let $\{v'_1, ..., v'_m\}$ be any basis of V. Then $\{u'_i \otimes v'_j \mid i \in \{1, ..., n\}, j \in \{1, ..., m\}\}$ forms a basis of W.*

Naturally, we wish to take a tensor product of more than two spaces. We have associativity for this product, see for example [29, Chapter XVI, §1, Proposition 1].

Theorem 3.1.2 *Let V_1, V_2, V_3 be finite dimensional vector spaces over F_q. Then there is a unique isomorphism*

$$V_1 \otimes (V_2 \otimes V_3) \to (V_1 \otimes V_2) \otimes V_3$$

such that

$$v_1 \otimes (v_2 \otimes v_3) \to (v_1 \otimes v_2) \otimes v_3$$

for all $v_1 \in V_1, v_2 \in V_2$ and $v_3 \in V_3$.

Theorem 3.1.2 allows us to omit the parentheses in the tensor product of several factors. For $1 \leq i \leq t$ and $t \geq 2$, let V_i be an n_i-dimensional vector space over the finite field F_q where $n_i \geq 2$ and $q = p^f$. Then we may form the tensor product vector space $W = V_1 \otimes \cdots \otimes V_t$, and the tensor product of elements $u_i \in V_i$ for $i = 1, ..., t$, denoted by $u_1 \otimes \cdots \otimes u_t$. By definition, the operation of tensor product satisfies the following multilinear property. Let $\lambda \in F_q$, and let $e_j \in V_j$ for $j = 1, ..., t$. Then for each $i \in \{1, ...t\}$,

1. $e_1 \otimes \cdots \otimes e_{i-1} \otimes (v_1 + v_2) \otimes e_{i+1} \otimes \cdots \otimes e_t$
   $= (e_1 \otimes \cdots \otimes e_{i-1} \otimes v_1 \otimes e_{i+1} \otimes \cdots \otimes e_t) + (e_1 \otimes \cdots \otimes e_{i-1} \otimes v_2 \otimes e_{i+1} \otimes \cdots \otimes e_t)$,
   where $v_1, v_2 \in V_i$.
2. $(\lambda e_1) \otimes \cdots \otimes e_t = e_1 \otimes \cdots \otimes e_{i-1} \otimes (\lambda e_i) \otimes e_{i+1} \otimes \cdots \otimes e_t = \lambda(e_1 \otimes \cdots \otimes e_t)$.

Suppose that $\{x_{ij} \,|\, 1 \le j \le n_i\}$ is a basis of V_i for each i. The following lemma is a corollary of Theorem 3.1.1 (4), which constructs a special basis for W, called the *tensor product basis* in this thesis.

Lemma 3.1.3 *With the above notation, suppose that* $\{x_{ij} \,|\, 1 \le j \le n_i\}$ *is a basis of* V_i*. Then* $B = \{x_{1j_1} \otimes \cdots \otimes x_{tj_t} |\ 1 \le j_i \le n_i$ *for* $1 \le i \le t\}$ *is a basis for* $W = V_1 \otimes \cdots \otimes V_t$*.*

We call an element w of W *simple* if there exist $v_i \in V_i$, for $i = 1, ..., t$, such that $w = v_1 \otimes \cdots \otimes v_t$. Suppose that $v_i = \sum_{j=1}^{n_i} \lambda_{ij} x_{ij}$. Then

$$v_1 \otimes \cdots \otimes v_t = \sum_{\substack{1 \le j_i \le n_i \\ 1 \le i \le t}} (\lambda_{1j_1} \cdots \lambda_{tj_t}) x_{1j_1} \otimes \cdots \otimes x_{tj_t}.$$

Note that there exist many vectors in W that are not simple.

For each $g_i \in \mathrm{GL}(V_i)$, we define the element $g_1 \otimes \cdots \otimes g_t \in \mathrm{GL}(W)$ by setting

$$(v_1 \otimes \cdots \otimes v_t)^{(g_1 \otimes \cdots \otimes g_t)} = v_1^{g_1} \otimes \cdots \otimes v_t^{g_t} \text{ for any } v_i \in V_i,$$

and then extending linearly. Thus under the multiplication of $\mathrm{GL}(W)$ we have $(g_1 \otimes \cdots \otimes g_t)(h_1 \otimes \cdots \otimes h_t) = (g_1 h_1) \otimes \cdots \otimes (g_t h_t)$ and $(g_1 \otimes \cdots \otimes g_t)^{-1} = g_1^{-1} \otimes \cdots \otimes g_t^{-1}$ where $g_i, h_i \in \mathrm{GL}(V_i)$. Now we define

$$\mathrm{GL}(V_1) \otimes \mathrm{GL}(V_2) \otimes \cdots \otimes \mathrm{GL}(V_t) := \{g_1 \otimes g_2 \otimes \cdots \otimes g_t \,|\, g_i \in \mathrm{GL}(V_i)\}.$$

Then $\mathrm{GL}(V_1) \otimes \mathrm{GL}(V_2) \otimes \cdots \otimes \mathrm{GL}(V_t)$ is a subgroup of $\mathrm{GL}(W)$. (It is possible for different $g_1 \otimes \cdots \otimes g_t$ to give the same element of $\mathrm{GL}(W)$.)

We say that G is a *central product* of subgroups H and K if $G = HK$ with $H \cap K \subseteq Z(G)$ such that H centralizes K. If $H \cap K = Z(G)$ then we write $G = H \circ K$. Note that, $\mathrm{GL}(V_1) \otimes \cdots \otimes \mathrm{GL}(V_t)$ is actually the central product $\mathrm{GL}(V_1) \circ \cdots \circ \mathrm{GL}(V_t)$, we will use both notations for this subgroup later.

Further, we suppose that $W = V_1 \otimes \cdots \otimes V_t$ where $V_i = V$ for each i. Let $\rho \in S_t$. Then ρ induces an element of $\mathrm{GL}(W)$ naturally, namely, the action of ρ on simple vectors (in particular, on a tensor product basis of W) is given by

$$(v_1 \otimes \cdots \otimes v_t)^{\rho^{-1}} = v_{1^\rho} \otimes \cdots \otimes v_{t^\rho}.$$

Hence the semidirect product $(\mathrm{GL}(V) \otimes \cdots \otimes \mathrm{GL}(V)) \rtimes S_t$, which we will often write as $\mathrm{GL}(V) \wr_{\otimes} S_t$ in this thesis, is a subgroup of $\mathrm{GL}(W)$.

The next three technical lemmas concern those linear transformations that leave invariant the set of simple vectors.

Lemma 3.1.4 *With the notation after Theorem 3.1.2, let* $w_1 = v_1 \otimes \cdots \otimes v_t$ *and* $w_2 = u_1 \otimes \cdots \otimes u_t$ *be two nonzero simple elements of* W*. Then* $w_1 + w_2$ *is simple if and only if* u_i *is a scalar multiple of* v_i *for all but at most one* i*.*

Proof. Suppose u_i is a scalar multiple of v_i for all but at most one i. Without loss of generality we may assume that there exist $\lambda_2, ..., \lambda_t \in F_q$ such that $u_2 = \lambda_2 v_2$,..., $u_t = \lambda_t v_t$. Set $\lambda = \lambda_2\lambda_3...\lambda_t$. Then $w_1 + w_2 = (v_1 + \lambda u_1) \otimes v_2 \otimes \cdots \otimes v_t$ is simple.

Conversely, suppose $w_1 + w_2$ is simple. If $w_1 + w_2 = 0$, then $w_1 = -w_2$. This implies that u_i is a scalar multiple of v_i for all i.

Now suppose that $w_1 + w_2 \neq 0$. Let $U_i = \text{Span}(u_i, v_i)$ for each i. Suppose that $\{u_1, v_1\}$ and $\{u_2, v_2\}$ are linearly independent sets. Note that $w_1 + w_2 \in U_1 \otimes \cdots \otimes U_t$. Then since $w_1 + w_2$ is simple, there exist $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in F_q$ and $e_i \in U_i$ for $3 \leq i \leq t$ such that

$$\begin{aligned} w_1 + w_2 &= (u_1 \otimes \cdots \otimes u_t) + (v_1 \otimes \cdots \otimes v_t) \\ &= (\lambda_1 u_1 + \lambda_2 v_1) \otimes (\lambda_3 u_2 + \lambda_4 v_2) \otimes e_3 \otimes \cdots \otimes e_t \\ &= \lambda_1\lambda_3(u_1 \otimes u_2 \otimes e_3 \otimes \cdots \otimes e_t) + \lambda_1\lambda_4(u_1 \otimes v_2 \otimes e_3 \otimes \cdots \otimes e_t) \\ &\quad +\lambda_2\lambda_3(v_1 \otimes u_2 \otimes e_3 \otimes \cdots \otimes e_t) + \lambda_2\lambda_4(v_1 \otimes v_2 \otimes e_3 \otimes \cdots \otimes e_t). \end{aligned}$$

Hence when $t = 2$, we have:

$$u_1 \otimes u_2 + v_1 \otimes v_2 = \lambda_1\lambda_3(u_1 \otimes u_2) + \lambda_1\lambda_4(u_1 \otimes v_2) + \lambda_2\lambda_3(v_1 \otimes u_2) + \lambda_2\lambda_4(v_1 \otimes v_2).$$

Since $u_1 \otimes u_2, u_1 \otimes v_2, v_1 \otimes u_2$ and $v_1 \otimes v_2$ are linearly independent, we have $\lambda_1\lambda_3 = \lambda_2\lambda_4 = 1$ and $\lambda_1\lambda_4 = \lambda_2\lambda_3 = 0$, which is impossible. When $t \geq 3$,

$$\begin{aligned} 0 &= u_1 \otimes u_2 \otimes ((u_3 \otimes \cdots \otimes u_t) - (\lambda_1\lambda_3 e_3 \otimes \cdots \otimes e_t)) \\ &\quad +v_1 \otimes v_2 \otimes ((v_3 \otimes \cdots \otimes v_t) - (\lambda_2\lambda_4 e_3 \otimes \cdots \otimes e_t)) \\ &\quad -u_1 \otimes v_2 \otimes \lambda_1\lambda_4 e_3 \otimes \cdots \otimes e_t \\ &\quad -v_1 \otimes u_2 \otimes \lambda_2\lambda_3 e_3 \otimes \cdots \otimes e_t \end{aligned}$$

If any of the four summands is nonzero, then it is linearly independent of the sum of the other three summands, and we have a contradiction. Hence each of the summands is 0. Since $w_1, w_2, w_1 + w_2$ are all nonzero, it follows that all the u_i, v_i, e_i are nonzero and hence we must have $\lambda_1\lambda_3 \neq 0, \lambda_2\lambda_4 \neq 0$ and $\lambda_1\lambda_4 = \lambda_2\lambda_3 = 0$, which is impossible.

Therefore u_i is a scalar multiple of v_i for all but at most one i. □

For each i, choose e_i, a nonzero element of V_i. Write $e = e_1 \otimes e_2 \otimes \cdots \otimes e_t$ and

$$W_i := \{e_1 \otimes \cdots \otimes e_{i-1} \otimes v_i \otimes e_{i+1} \otimes \cdots \otimes e_t \mid v_i \in V_i\}.$$

Note that we also write $W_i = e_1 \otimes \cdots \otimes e_{i-1} \otimes V_i \otimes e_{i+1} \otimes \cdots \otimes e_t$ which is isomorphic to the vector space V_i.

Lemma 3.1.5 *With the notation as above, let $g \in \mathrm{GL}(W)$ be a linear transformation such that $e^g = e$ and, for each simple $w \in W$, w^g is also simple. Then for each $i = 1, ..., t$, there exists j, such that $1 \le j \le t$ and $W_i^g \subseteq W_j$.*

Proof. Without loss of generality, we may assume that $i = 1$. Note that $\dim V_1 \ge 2$. Let $v \in V_1 \setminus \langle e_1 \rangle$. Since g preserves the set of simple vectors,

$$(v \otimes e_2 \otimes \cdots \otimes e_t)^g = u_1 \otimes \cdots \otimes u_t$$

for some $u_i \in V_i$, $1 \le i \le t$. Since $(e_1 \otimes e_2 \otimes \cdots \otimes e_t) + (v \otimes e_2 \otimes \cdots \otimes e_t)$ is simple, its image $(e_1 \otimes \cdots \otimes e_t) + (u_1 \otimes \cdots \otimes u_t)$ under g is also simple. By Lemma 3.1.4, u_i is a scalar multiple of e_i for all but at most one i. Moreover, since $e_1 \otimes \cdots \otimes e_t$ and $v \otimes e_2 \otimes \cdots \otimes e_t$ are linearly independent, $e_1 \otimes \cdots \otimes e_t$ and $u_1 \otimes \cdots \otimes u_t$ are linearly independent. Thus there exists precisely one j such that $u_j \notin \langle e_j \rangle$. If $v' \in V_1 \setminus \langle e_1 \rangle$ and

$$(v' \otimes e_2 \otimes \cdots \otimes e_t)^g = u'_1 \otimes \cdots \otimes u'_t,$$

then the same argument gives that u'_i is a scalar multiple of e_i for all but one i, say $u'_l \notin \langle e_l \rangle$. Using the fact that $(v \otimes e_2 \otimes \cdots \otimes e_t) + (v' \otimes e_2 \otimes \cdots \otimes e_t)$ is simple, we deduce that u'_i is a scalar multiple of u_i for all but one i. However, if $j \ne l$, then this means that $u'_j \in \langle e_j \rangle \cap \langle u_j \rangle = \{0\}$ which is not the case. Hence $l = j$, and so $u'_i \in \langle e_i \rangle$ for all $i \ne j$. Thus

$$(v' \otimes e_2 \otimes \cdots \otimes e_t)^g \in W_j$$

for each $v' \in V_1 \setminus \langle e_1 \rangle$. Since also $e^g = e \in W_j$, it follows that $W_1^g \subseteq W_j$. □

Lemma 3.1.6 *Let $g \in \mathrm{GL}(W)$ such that g leaves invariant the set of simple vectors, and g fixes each W_i pointwise. Then $g = 1$.*

Proof. We claim that for any simple $w \in W$, w^g is a scalar multiple of w. Let $w = v_1 \otimes v_2 \otimes \cdots \otimes v_t$, and let l be the number of i such that $v_i \notin \langle e_i \rangle$. We prove the claim by induction on l. By assumption, for $l = 0$ and $l = 1$, $w^g = w$. Now assume inductively that the claim is true for $l = m$ where $1 \le m < t$. We will show that it is true for $l = m + 1$.

Without loss of generality, we may suppose that

$$w = v_1 \otimes \cdots \otimes v_{m+1} \otimes e_{m+2} \cdots \otimes e_t$$

where for $i = 1, ..., m+1$, $v_i \notin \langle e_i \rangle$. Let

$$w^g = u_1 \otimes \cdots \otimes u_t.$$

Set

$$w_1 = e_1 \otimes v_2 \otimes \cdots \otimes v_{m+1} \otimes e_{m+2} \cdots \otimes e_t$$

and

$$w_2 = v_1 \otimes \cdots \otimes v_m \otimes e_{m+1} \otimes e_{m+2} \cdots \otimes e_t.$$

Then $w_1 + w$ and $w_2 + w$ are simple and hence $(w_1 + w)^g$ and $(w_2 + w)^g$ are simple. Also, by induction, $w_1^g = \lambda_1 w_1$ and $w_2^g = \lambda_2 w_2$ for some $\lambda_1, \lambda_2 \in F_q$.

Thus $(w_1 + w)^g = \lambda_1 w_1 + w^g$, and this is a simple vector. So by Lemma 3.1.4, u_i is a scalar multiple of the ith component of w_1 for all but one i. Likewise, u_i is a scalar multiple of the ith component of w_2 for all but one i. But u_1 cannot be a scalar multiple of both e_1 and v_1, and u_{m+1} cannot be a scalar multiple of both e_{m+1} and v_{m+1}. Therefore for all $i \notin \{1, m+1\}$, u_i is a scalar multiple of the ith component of w. Thus $w^g \in \langle u_1 \otimes v_2 \otimes \cdots \otimes v_m \otimes u_{m+1} \otimes e_{m+2} \otimes \cdots \otimes e_t \rangle$. Also, u_1 is a scalar multiple of either e_1 or v_1 and u_{m+1} is a scalar multiple of either e_{m+1} or v_{m+1}. If $u_1 \in \langle e_1 \rangle$, then by induction, $w^g \in \langle (e_1 \otimes v_2 \otimes \cdots \otimes v_m \otimes u_{m+1} \otimes e_{m+2} \otimes \cdots \otimes e_t)^g \rangle$, contradicting the fact that w and $e_1 \otimes v_2 \otimes \cdots \otimes v_m \otimes u_{m+1} \otimes e_{m+2} \otimes \cdots \otimes e_t$ are linearly independent. Hence $u_1 \in \langle v_1 \rangle$. Similarly, $u_{m+1} \in \langle v_{m+1} \rangle$. Thus w^g is a scalar multiple of w, and the claim is proved by induction.

Now, using induction on l once again (with l defined as above), we show that $w^g = w$ for every simple $w \in W$, and hence that $g = 1$. The case $l \leq 1$ is true by assumption. Now assume that this is true for $l = m$ where $1 \leq m < t$, and consider $w = v_1 \otimes \cdots \otimes v_{m+1} \otimes e_{m+2} \cdots \otimes e_t$ where $v_i \notin \langle e_i \rangle$ for $i = 1, ..., m+1$. Once again, set $w_1 = e_1 \otimes v_2 \otimes \cdots \otimes v_{m+1} \otimes e_{m+2} \cdots \otimes e_t$. Then both w and $w + w_1$ are simple. Hence there exist $\lambda, \mu \in F_q^*$ such that $w^g = \lambda w$ and $(w + w_1)^g = \mu(w + w_1)$. Also, by the inductive hypothesis, $(w_1)^g = w_1$. But then $(w + w_1)^g = w^g + w_1^g = \lambda w + w_1 = \mu(w + w_1)$. Since w and w_1 are linearly independent, $\mu = \lambda = 1$ and $w^g = w$. □

3.2 Semilinear transformations

Let $V = V(d, q)$ be a vector space of dimension d over a finite field F_q with $d \geq 1$ and $q = p^f$ a prime power. Throughout this thesis, we denote the *Frobenius automorphism* of F_q by τ, that is, $\tau : \lambda \to \lambda^p$ for each $\lambda \in F_q$. The full automorphism group of the field F_q is $\langle \tau \rangle$, the cyclic group of order f generated by the Frobenius automorphism. Moreover, we denote $F_q^* = F_q \setminus \{0\}$, a cyclic group of order $q-1$ with respect to the field multiplication.

Pick a basis $\{v_1, ..., v_d\}$ of V and use it to identify V with F_q^d. We can define an action of τ on V as follows: $(\lambda_1 v_1 + \cdots + \lambda_d v_d)^\tau := \lambda_1^\tau v_1 + \cdots + \lambda_d^\tau v_d = \lambda_1^p v_1 + \cdots + \lambda_d^p v_d$ for $\lambda_i \in F_q$. Then we define $\Gamma\mathrm{L}(d, q) := \mathrm{GL}(d, q) \rtimes \langle \tau \rangle$, called the *general semilinear group* of V. Note that the definition of the action of τ on V depends on the basis. However the group $\Gamma\mathrm{L}(d, q)$ is independent of the choice of basis. A non-identity element of $\Gamma\mathrm{L}(d, q)$ is called a *non-singular semilinear transformation* of V. In the following discussion, when we refer to the Frobenius automorphism $\tau \in \Gamma\mathrm{L}(d, q)$, τ will always be defined as above with respect to the basis $\{v_1, ..., v_d\}$.

Let $h \in \Gamma\mathrm{L}(d, q)$. Then there exists a field automorphism $\tau(h) \in \langle \tau \rangle$, called *the associated field automorphism* of h, such that for all $v \in V$ and $\lambda \in F_q$,

$$(\lambda v)^h = \lambda^{\tau(h)} v^h.$$

Moreover, this map from $\Gamma\mathrm{L}(d, q)$ to $\mathrm{Aut}(F_q)$ is a surjective homomorphism with kernel $\mathrm{GL}(d, q)$. That is, $\tau(h) = \tau^j$ for some integer j satisfying $0 \le j < f$, and $\tau(h_1 h_2) = \tau(h_1)\tau(h_2)$. Throughout this thesis, we use $\tau(h)$ to denote the associated field automorphism of h when h is a non-singular semilinear transformation.

Proposition 3.2.1 (Order formulae.) *Let $d \ge 1$ and $q = p^f$.*

1. $|\mathrm{GL}(d, q)| = (q^d - 1)(q^d - q) \cdots (q^d - q^{(d-1)}) = q^{d(d-1)/2} \prod_{i=1}^d (q^i - 1)$.
2. $|\mathrm{SL}(d, q)| = q^{d(d-1)/2} \prod_{i=2}^d (q^i - 1)$.
3. $|\Gamma\mathrm{L}(d, q)| = f |\mathrm{GL}(d, q)|$.

Let a, n be positive integers. A prime s is called a *primitive prime divisor* of $a^n - 1$ if s divides $a^n - 1$ but does not divide $a^i - 1$ for any $i < n$. In view of Proposition 3.2.1, the following result, proved by Zsigmondy [55], will be very useful when we consider the order of subgroups of $\Gamma\mathrm{L}(d, q)$.

Theorem 3.2.2 *Let a, n be positive integers. Then either $a^n - 1$ has a primitive prime divisor, or $(a, n) = (2^b - 1, 2)$ for some integer b, or $(a, n) = (2, 6)$.*

The next proposition, that is essentially [49, Proposition 84.1], characterizes non-singular semilinear transformations geometrically.

Proposition 3.2.3 *Suppose that $d \ge 2$ and $V = V(d, q)$ is a vector space over F_q. Then a function $f : V \to V$ is in $\Gamma\mathrm{L}(d, q)$ if and only if it has the following two properties:*

1. *f is an automorphism of the additive group of V.*

2. f sends one-dimensional subspaces of V onto one-dimensional subspaces.

Proof. By [49, Proposition 84.1], a function $f : V \to V$ is a non-singular semilinear transformation of V if and only if it has the following three properties:

1. f is an automorphism of the additive group of V.

2. f sends one-dimensional subspaces of V onto one-dimensional subspaces.

3. If u and v are linearly independent vectors of V, then the vectors $f(u)$ and $f(v)$ are also linearly independent.

Note that conditions 1 and 2 imply condition 3. Thus $f \in \Gamma\mathrm{L}(d,q)$ if and only if conditions 1 and 2 hold. □

3.3 Projective geometry

Let $V = V(d,q)$ be a d-dimensional vector space over F_q for $d \geq 2$. Then we can construct a projective geometry by "projection" of V naturally. The $(d-1)$-*dimensional projective space over* F_q, denoted by $\mathrm{PG}(d-1,q)$, is the set of all nontrivial proper subspaces of V. We call the 1-dimensional subspaces of V *points*, the 2-dimensional subspaces *lines* and the 3-dimensional subspaces *planes*. A set of points in $\mathrm{PG}(d-1,q)$ is said to be *collinear* if it is contained in a line.

An *automorphism* of a projective space is a bijection of the point set of the space such that subspaces are mapped onto subspaces of the same dimension and inclusion is preserved. In particular, an automorphism takes collinear points to collinear points. Conversely, if f is a permutation of the point set of $\mathrm{PG}(d-1,q)$ which takes collinear points to collinear points, then f is an automorphism (see [51, Chapter 3]). That means, the projective geometry is determined by the structures of its points and lines.

Recall from Section 3.2 that $\Gamma\mathrm{L}(d,q) = \mathrm{GL}(d,q) \rtimes \langle\tau\rangle$. Any element of $\Gamma\mathrm{L}(d,q)$ induces an automorphism of $\mathrm{PG}(d-1,q)$. The kernel of this action of $\Gamma\mathrm{L}(d,q)$ on the set of points of $\mathrm{PG}(d-1,q)$ is the scalar subgroup Z. We define the *projective general semilinear group* $\mathrm{P\Gamma L}(d,q)$ to be the permutation group induced on the points of the projective space $\mathrm{PG}(d-1,q)$. Thus,

$$\mathrm{P\Gamma L}(d,q) \cong \Gamma\mathrm{L}(d,q)/Z,$$

and $\mathrm{P\Gamma L}(d,q)$ is a subgroup of the full automorphism group of $\mathrm{PG}(d-1,q)$. The Fundamental Theorem of Projective Geometry (see [51, 3.1]) tells us the converse is also true when $d \geq 3$.

Theorem 3.3.1 (Fundamental Theorem of Projective Geometry) *Suppose $d \geq 3$. If f is a permutation of the point set of* $\mathrm{PG}(d-1,q)$ *which takes collinear points to collinear* *points, then* $f \in \mathrm{P\Gamma L}(d,q)$.

Next we look at the 2-transitivity of the subgroups of $\mathrm{P\Gamma L}(d,q)$ on the set of points of $\mathrm{PG}(d-1,q)$. Let $\mathrm{PGL}(d,q)$ and $\mathrm{PSL}(d,q)$ be the permutation groups induced on the points of $\mathrm{PG}(d-1,q)$ by $\mathrm{GL}(d,q)$ and $\mathrm{SL}(d,q)$ respectively. Thus,

$$\mathrm{PGL}(d,q) \cong \mathrm{GL}(d,q)/Z \text{ and } \mathrm{PSL}(d,q) \cong \mathrm{SL}(d,q)/(Z \cap \mathrm{SL}(d,q)).$$

Theorem 3.3.2 *Suppose* $d \geq 2$. *Then* $\mathrm{PSL}(d,q)$ *is* 2*-transitive on the set of points of the projective space* $\mathrm{PG}(d-1,q)$.

The next theorem determines all 2-transitive subgroups of $\mathrm{P\Gamma L}(d,q)$ on the set of points of the project space $\mathrm{PG}(d-1,q)$ when $d \geq 3$. This result was proved by Cameron and Kantor in [8].

Theorem 3.3.3 [8, Theorem 1] *Suppose that* $G \leq \Gamma\mathrm{L}(d,q)$ *with* $d \geq 3$. *Suppose further that* G *induces a* 2*-transitive subgroup on the set of points of* $\mathrm{PG}(d-1,q)$, *then either* $G \geq \mathrm{SL}(d,q)$ *or* $G = A_7 \leq \mathrm{SL}(4,2)$.

3.4 The geometry of classical groups

There are three kinds of classical groups that preserve nontrivial forms: symplectic groups, unitary groups and orthogonal groups. We begin by introducing some basic definitions and notation.

3.4.1 Basic definitions

Let $V = V(d,q)$ be a d-dimensional vector space over F_q. A map $\mathbf{f} : V \times V \to F_q$ is called a *left linear form* if, for all $u, w, v \in V$ and $\lambda \in F_q$,

$$\mathbf{f}(u+w,v) = \mathbf{f}(u,v) + \mathbf{f}(w,v) \quad \text{and} \quad \mathbf{f}(\lambda u, v) = \lambda \mathbf{f}(u,v).$$

A left linear form $\mathbf{f}$ is called a *bilinear form* if for all $u, w, v \in V$ and $\lambda \in F_q$,

$$\mathbf{f}(v,u+w) = \mathbf{f}(v,u) + \mathbf{f}(v,w) \quad \text{and} \quad \mathbf{f}(v,\lambda u) = \lambda \mathbf{f}(v,u).$$

The *radical* of a bilinear form $\mathbf{f}$ is

$$\mathrm{rad}_{\mathbf{f}}(V) = \{v \in V \mid \mathbf{f}(u,v) = 0 \text{ for all } u \in V\}.$$

For any map $\mathbf{Q} : V \to F_q$, define $\mathbf{f}_Q : V \times V \to F_q$ by

$$\mathbf{f}_Q(v,w) = \mathbf{Q}(v+w) - \mathbf{Q}(v) - \mathbf{Q}(w), \text{ for } v, w \in V. \tag{3.1}$$

Then $\mathbf{Q}$ is called a *quadratic form* if $\mathbf{Q}(\lambda v) = \lambda^2\mathbf{Q}(v)$ for all $v \in V$ and $\lambda \in F_q$ and $\mathbf{f}_Q$ is a bilinear form. When $\mathbf{Q}$ is a quadratic form, $\mathbf{f}_Q$ will be called its *associated bilinear form.*

Let $\mathbf{f} : V \times V \to F_q$ be a map. Then $\mathbf{f}$ is called *symmetric* if

$$\mathbf{f}(v,w) = \mathbf{f}(w,v) \text{ for all } v,w \in V.$$

We observe that, for any quadratic form $\mathbf{Q}$, its associated bilinear form $\mathbf{f}_Q$ is symmetric. Also, $\mathbf{f}$ is called *skew-symmetric* if

$$\mathbf{f}(v,w) = -\mathbf{f}(w,v) \text{ for all } v,w \in V.$$

Finally, if α is an automorphism of the field F_q, then $\mathbf{f}$ is *sesquilinear* with respect to α if $\mathbf{f}$ is left linear and $\mathbf{f}(v,w) = \mathbf{f}(w,v)^\alpha$ for all $v,w \in V$.

A bilinear or sesquilinear form $\mathbf{f}$ is called *non-degenerate* if $\mathbf{f}(u,v) = 0$ for all $u \in V$ implies $v = 0$, that is, $\mathrm{rad}_{\mathbf{f}}(V) = \{0\}$. A quadratic form $\mathbf{Q}$ is called *non-degenerate* if either its associated bilinear form $\mathbf{f}_Q$ is non-degenerate or $\mathbf{Q}(v) \neq 0$ for each nonzero vector $v \in \mathrm{rad}_{f_\mathbf{Q}}(V)$.

We define $\mathbf{f}$ to be *symplectic* if $\mathbf{f}$ is skew-symmetric, bilinear, non-degenerate, and $\mathbf{f}(v,v) = 0$ for all $v \in V$.

Let $q = q_0^2$. Then $F_q = F_{q_0^2}$ has an involutory field automorphism $\alpha : \lambda \to \lambda^{q_0}$. Define $\mathbf{f}$ to be *unitary* if $\mathbf{f}$ is left linear, non-degenerate, and sesquilinear with respect to α.

From now on, we assume that V is equipped with a non-degenerate quadratic form $\mathbf{Q}$, or a symplectic or unitary form $\mathbf{f}$, (written $(V,\mathbf{Q})$ and $(V,\mathbf{f})$ respectively). The corresponding geometries are an orthogonal geometry in the first case, and a symplectic or a unitary geometry in the second case.

3.4.2 The orthogonal geometry

In this subsection, we assume that $V = (V,\mathbf{Q})$ where $\mathbf{Q}$ is a non-degenerate quadratic form. An element $g \in \Gamma\mathrm{L}(d,q)$ is called a $\mathbf{Q}$-*semisimilarity* if there exist $\lambda \in F_q^*$ and $\sigma \in \mathrm{Aut}(F_q)$ such that

$$\mathbf{Q}(v^g) = \lambda\mathbf{Q}(v)^\sigma \text{ for all } v \in V.$$

In fact, one can show that $\sigma = \tau(g)$, where $\tau(g)$ is the associated field automorphism of g, see [26, Lemma 2.1.2]. The set of all $\mathbf{Q}$-semisimilarities forms a subgroup $\Gamma\mathrm{O}(V)$ of $\Gamma\mathrm{L}(d,q)$.

A non-zero vector u is called *singular* if $\mathbf{Q}(u) = 0$. A non-zero vector u is called *isotropic* if $\mathbf{f}_Q(u,u) = 0$. It follows from the definition of $\mathbf{f}_Q$, see (3.1), that

$$2\mathbf{Q}(u) = \mathbf{f}_Q(u,u) \text{ for each } u \in V. \tag{3.2}$$

Hence every singular vector is isotropic. However, when q is a power of 2, by (3.2), every non-zero vector is isotropic while some non-zero vectors are not singular. We call (e, f) a *hyperbolic pair* if $\mathbf{Q}(e) = \mathbf{Q}(f) = 0$ and $\mathbf{f}_Q(e, f) = 1$.

For a subset J of V, we define

$$J^\perp = \{v \in V \mid \ \mathbf{f}_Q(v, u) = 0 \text{ for all } u \in J\}.$$

It is easy to see that $J^\perp$ is a subspace of V. We also say that $V = U \perp W$ is the *orthogonal* direct sum of subspaces U and W if $V = U \oplus W$ and $\mathbf{f}_Q(u, w) = 0$ for all $u \in U$ and $w \in W$.

The space $(V, \mathbf{Q})$ has the following decomposition, (see [51, 11.3]):

$$V = L_1 \perp \dots \perp L_m \perp W \tag{3.3}$$

where $m \geq 0$, L_i is generated by a hyperbolic pair (e_i, f_i), and W does not contain any nonzero singular vectors. One can show that this condition on W implies that $\dim W \leq 2$, (see [51, 11.3]). Note that we allow $m = 0$, and in this case we set $V = W$.

We have to consider three cases for the group $\Gamma\mathrm{O}(V)$, depending on the dimension of the subspace of W in (3.3). In detail, the odd dimensional orthogonal groups $\Gamma\mathrm{O}(V)$ are uniquely determined up to conjugacy in $\Gamma\mathrm{L}(d, q)$, while there are two conjugacy classes of even dimensional orthogonal groups.

1. If $W = 0$, then $\dim V = 2m$. We write $\Gamma\mathrm{O}^+(2m, q)$ for $\Gamma\mathrm{O}(V)$ in this case.

2. If $\dim W = 1$, then $\Gamma\mathrm{O}(V)$ is unique up to conjugacy in $\Gamma\mathrm{L}(d, q)$. We write $\Gamma\mathrm{O}^\circ(2m+1, q)$ for $\Gamma\mathrm{O}(V)$ in this case (note that the form $\mathbf{Q}$ is not unique up to isomorphism when q is odd, although the group $\Gamma\mathrm{O}(V)$ is).

3. If $\dim W = 2$, then $\Gamma\mathrm{O}(V)$ is again unique up to conjugacy in $\Gamma\mathrm{L}(d, q)$. We denote it by $\Gamma\mathrm{O}^-(2m + 2, q)$ in this case.

Let

$$\Theta = \{v \in V \mid \ \mathbf{Q}(v) = 0\}.$$

Note that $\Theta \setminus \{0\}$ is non-empty if and only if $d \geq 3$ or $d = 2$ and $\Gamma\mathrm{O}(V) = \Gamma\mathrm{O}^+(2, q)$. We have the following theorem.

Theorem 3.4.1 *Suppose* $\Theta \setminus \{0\}$ *is non-empty. If* $g \in \Gamma\mathrm{L}(d, q)$ *fixes* Θ *setwise, then* $g \in \Gamma\mathrm{O}(V)$*.*

We are very grateful to Dr. Oliver King for providing the following proof of Theorem 3.4.1. He actually proved that $\mathrm{GO}(V)$ is the stabilizer in $\mathrm{GL}(V)$ of the set Θ when $\Theta \setminus \{0\}$

is nonempty in [25, Lemma 1]. In [25], King assumed that the field is of characteristic different from 2, although this assumption was not in fact necessary for the argument proving [25, Lemma 1].

In order to prove Theorem 3.4.1, we need to discuss some more geometry. Consider a 2-subspace $L = \langle v, u\rangle$ where $\mathbf{Q}(v) = 0$, and hence $\mathbf{f}_Q(v, v) = 0$. Then $\dim(L^\perp \cap L) = 0, 1$ or 2.

Suppose first that $L^\perp \cap L = \{0\}$. Then L is a non-degenerate subspace containing a non-zero singular vector. Thus L is generated by a hyperbolic pair (e, f). Since $\mathbf{Q}(\lambda_1 e + \lambda_2 f) = \lambda_1\lambda_2$, we have $L \cap \Theta = \langle e\rangle \cup \langle f\rangle$. Also since L is non-degenerate, it has trivial radical, and in particular, $v^\perp \cap L = \langle v\rangle$.

Suppose next that $\dim(L^\perp \cap L) = 1$ and let $L^\perp \cap L = \langle w\rangle$. Then $\mathbf{f}_Q(v, w) = \mathbf{f}_Q(v, v) = \mathbf{f}_Q(w, w) = 0$. If $L = \langle v, w\rangle$ then $L \subseteq L^\perp$, which is a contradiction. Therefore $L^\perp \cap L = \langle v\rangle$. We claim that $\mathbf{Q}(u) \neq 0$. Otherwise, $\mathbf{Q}(v) = \mathbf{Q}(u) = 0$ and $\mathbf{f}_Q(v, u) = 0$ imply that $L \subseteq L^\perp$. Thus $\mathbf{Q}(\lambda_1 v + \lambda_2 u) = \lambda_2^2\mathbf{Q}(u)$. Hence $L \cap \Theta = \langle v\rangle$ and $L \subseteq v^\perp$.

Finally suppose that $L \subseteq L^\perp$. Then in particular, $L \subseteq v^\perp$, and $\mathbf{f}_Q(u, u) = \mathbf{f}_Q(v, v) = 0$. From (3.2) we obtain $2\mathbf{Q}(u) = \mathbf{f}_Q(u, u) = 0$. If q is odd, this implies that $\mathbf{Q}(u) = 0$ and it follows that L is totally singular, that is, $L \subseteq \Theta$. When q is even, if L is not totally singular, then there exists $w \in L\setminus\langle v\rangle$ such that $\mathbf{Q}(w) \neq 0$. Then $\mathbf{Q}(\lambda_1 v+\lambda_2 w) = \lambda_2^2\mathbf{Q}(w)$. Hence $L \cap \Theta = \langle v\rangle$.

Thus we can divide the 2-subspaces L of V that contain at least one non-zero singular vector v into three types according to the number of elements in the set $L \cap \Theta$.

1. The secant type: L is generated by a hyperbolic pair and $|L \cap \Theta| = 2(q - 1) + 1$. Also $v^\perp \cap L = \langle v\rangle$.

2. The tangent type: $L \cap \Theta = \langle v\rangle$ and $|L \cap \Theta| = q$. In this case, either $L^\perp \cap L = L \cap \Theta$ or q is even and $L \subseteq L^\perp$. In particular, $L \subseteq v^\perp$.

3. The totally singular type: $L \subseteq \Theta$, thus $|L \cap \Theta| = q^2$. Also in this type we have $L \subseteq v^\perp$.

Note that if $g \in \Gamma\mathrm{L}(d, q)$ maps Θ to itself, then g preserves the above three types of 2-subspaces. That is, g maps a 2-subspace of the secant type to a 2-subspace of the secant type, a 2-subspace of the tangent type to a 2-subspace of the tangent type, and a 2-subspace of the totally singular type to a 2-subspace of the totally singular type.

This leads to the following lemma.

Lemma 3.4.2 *Suppose $g \in \Gamma\mathrm{L}(d, q)$ maps Θ to itself. Suppose also that L is a 2-subspace containing a singular vector v.*

(a) If $L = \langle v, u\rangle$ and $u \in v^\perp$ then L is not of secant type.

(b) If L is not of secant type, then $L \subseteq v^\perp$.

(c) If L is not of secant type, then $L^g \subseteq (v^g)^\perp$.

Proof. (a) If $u \in v^\perp$ then $L \subseteq v^\perp$, and so L is not of secant type.

(b) The condition $L \subseteq v^\perp$ holds when L is either of tangent type or of totally singular type.

(c) Note that since g preserves Θ, L^g is not of secant type. Thus Part (c) follows from (b) applied to L^g and v^g. □

Proof of Theorem 3.4.1: Suppose $\Theta \setminus \{0\}$ is nonempty and $g \in \Gamma\mathrm{L}(d, q)$ preserves Θ. Let $\sigma = \tau(g)$ be the associated field automorphism of g.

Since $\Theta \setminus \{0\}$ is nonempty, either $d \geq 3$, or $d = 2$ and the group is $\Gamma\mathrm{O}^+(2, q)$. In either case there exists a 2-subspace L_1 generated by a hyperbolic pair (e, f) where $\mathbf{Q}(e) = \mathbf{Q}(f) = 0$ and $\mathbf{f}_Q(e, f) = \mathbf{Q}(e + f) = 1$. It follows that $V = L_1 \perp L_1^\perp$. Set $e_1 = e^g$ and $f_1 = f^g$. Then, since g preserves Θ, $\mathbf{Q}(e_1) = \mathbf{Q}(f_1) = 0$ and L_1^g is of secant type, so $\mathbf{f}_Q(e_1, f_1) = \lambda$ for some nonzero $\lambda \in F_q$. For any $v_1 \in L_1$, we have $v_1 = \mu_1 e + \mu_2 f$ for some $\mu_1, \mu_2 \in F_q$. Then $\mathbf{Q}(v_1) = \mu_1\mu_2$, and

$$\mathbf{Q}(v_1^g) = \mathbf{Q}(\mu_1^\sigma e_1 + \mu_2^\sigma f_1) = \lambda(\mu_1\mu_2)^\sigma = \lambda\mathbf{Q}(v_1)^\sigma.$$

For $v_2 \in L_1^\perp$, by Lemma 3.4.2 (a), the 2-subspaces $\langle e, v_2\rangle$ and $\langle f, v_2\rangle$ are not of secant type. By Lemma 3.4.2 (c), we have $\langle e_1, v_2^g\rangle \subseteq \langle e_1\rangle^\perp$ and $\langle f_1, v_2^g\rangle \subseteq \langle f_1\rangle^\perp$, and hence $v_2^g \in \langle e_1, f_1\rangle^\perp$. Note that, since this holds for all $v_2 \in L_1^\perp$, we have that $(L_1^\perp)^g \subseteq (L_1^g)^\perp$, and hence that $V = L_1^g \perp (L_1^\perp)^g$.

Consider the vector $w = v_2 + e - \mathbf{Q}(v_2)f$ where $v_2 \in L_1^\perp$. Then using (3.1),

$$\mathbf{Q}(w) = \mathbf{Q}(v_2) + \mathbf{Q}(e - \mathbf{Q}(v_2)f) = 0,$$

and therefore, since g preserves Θ,

$$0 = \mathbf{Q}(w^g) = \mathbf{Q}(v_2^g) + \mathbf{Q}(e_1 - \mathbf{Q}(v_2)^\sigma f_1) = \mathbf{Q}(v_2^g) - \lambda\mathbf{Q}(v_2)^\sigma.$$

Thus $\mathbf{Q}(v_2^g) = \lambda\mathbf{Q}(v_2)^\sigma$, and this holds for any $v_2 \in L_1^\perp$.

Finally, any element of V has the form $v = v_1 + v_2$ with $v_1 \in L_1$ and $v_2 \in L_1^\perp$. For such a vector, $\mathbf{Q}(v) = \mathbf{Q}(v_1) + \mathbf{Q}(v_2)$. Also, since $(L_1^\perp)^g = (L_1^g)^\perp$, we have $\mathbf{f}_Q(v_1^g, v_2^g) = 0$, and hence

$$\mathbf{Q}(v^g) = \mathbf{Q}(v_1^g) + \mathbf{Q}(v_2^g) = \lambda\mathbf{Q}(v_1)^\sigma + \lambda\mathbf{Q}(v_2)^\sigma = \lambda\mathbf{Q}(v)^\sigma.$$

Therefore $g \in \Gamma\mathrm{O}(V)$ as required. □

3.4.3 The symplectic and unitary geometries

Suppose $V = (V, \mathbf{f})$ where $\mathbf{f}$ is symplectic or unitary. As in the orthogonal case, a non-zero vector u is called *isotropic* if $\mathbf{f}(u,u) = 0$. For a subset J of V, we set

$$J^{\perp} = \{v \in V \mid \ \mathbf{f}(v,u) = 0 \text{ for all } u \in J\},$$

and we say that $V = U \perp W$ if $V = U \oplus W$ and $\mathbf{f}(u,w) = 0$ for all $u \in U$ and $w \in W$.

Likewise, if $\mathbf{f}$ is a symplectic or unitary form on V, then $g \in \Gamma\mathrm{L}(d,q)$ is called an $\mathbf{f}$-*semisimilarity* if there exist $\lambda \in F_q^*$ and $\sigma \in \mathrm{Aut}(F_q)$ such that

$$\mathbf{f}(u^g, v^g) = \lambda \mathbf{f}(u,v)^{\sigma} \text{ for all } u, v \in V.$$

Also by [26, Lemma 2.1.2], $\sigma = \tau(g)$, the associated field automorphism of g. The set of all $\mathbf{f}$-semisimilarities forms a subgroup of $\Gamma\mathrm{L}(d,q)$, denoted by $\Gamma\mathrm{Sp}(V)$ when $\mathbf{f}$ is symplectic, and by $\Gamma\mathrm{U}(V)$ when $\mathbf{f}$ is unitary. In particular, $g \in \Gamma\mathrm{L}(d,q)$ is called an $\mathbf{f}$-*isometry* if

$$\mathbf{f}(u^g, v^g) = \mathbf{f}(u,v) \text{ for all } u, v \in V.$$

First we suppose that $V = (V, \mathbf{f})$ where $\mathbf{f}$ is a symplectic form. The following proposition (see for example [26, Proposition 2.4.1]) tells us that there is a unique symplectic geometry up to isometry for $V(d,q)$ and the dimension d must be even. Thus the group $\Gamma\mathrm{Sp}(V)$ is uniquely determined up to conjugacy in $\Gamma\mathrm{L}(d,q)$ when d is even.

Proposition 3.4.3 *Suppose that $V = (V, \mathbf{f})$ where $\mathbf{f}$ is a symplectic form. Then V has a basis $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ such that for all i, j,*

$$\mathbf{f}(e_i, e_j) = \mathbf{f}(f_i, f_j) = 0 \textit{ and } \mathbf{f}(e_i, f_j) = \delta_{ij}.$$

In particular, the dimension of V is even.

A basis described in the above proposition is called a *symplectic basis.* Consider the natural action of $\Gamma\mathrm{L}(d,q)$ on $V \times V$. Let $\Delta = \{(u,v) \mid \ \mathbf{f}(u,v) = 0\}$. The following lemma shows that $\Gamma\mathrm{Sp}(V)$ is the setwise stabilizer of Δ in $\Gamma\mathrm{L}(V)$.

Lemma 3.4.4 *Suppose that $V = (V, \mathbf{f})$ where $\mathbf{f}$ is a symplectic form. Let $\Delta = \{(u,v) \mid \mathbf{f}(u,v) = 0\}$. If $g \in \Gamma\mathrm{L}(d,q)$ fixes Δ setwise, then $g \in \Gamma\mathrm{Sp}(V)$.*

Proof. Let $\{e_1, \ldots, e_m, f_1, \ldots, f_m\}$ be a symplectic basis, thus for all i, j,

$$\mathbf{f}(e_i, e_j) = \mathbf{f}(f_i, f_j) = 0 \text{ and } \mathbf{f}(e_i, f_j) = \delta_{ij}.$$

Let $g \in \Gamma\mathrm{L}(d,q)$ such that g fixes Δ setwise. Then

$$\mathbf{f}(e_i^g, e_j^g) = \mathbf{f}(f_i^g, f_j^g) = 0 \text{ for all } i, j, \text{ and } \mathbf{f}(e_i^g, f_j^g) = 0 \text{ when } i \neq j.$$

Since $\mathbf{f}(e_1, f_1) = 1$, the pair $(e_1, f_1) \notin \Delta$ and hence $(e_1^g, f_1^g) \notin \Delta$. Thus $\lambda := \mathbf{f}(e_1^g, f_1^g) \neq 0$. Since for $i > 1$

$$\mathbf{f}(-e_1 + e_i, f_1 + f_i) = -1 + 1 = 0,$$

we have

$$0 = \mathbf{f}(-e_1^g + e_i^g, f_1^g + f_i^g) = -\mathbf{f}(e_1^g, f_1^g) + \mathbf{f}(e_i^g, f_i^g) = -\lambda + \mathbf{f}(e_i^g, f_i^g).$$

Therefore $\mathbf{f}(e_i^g, f_i^g) = \lambda$ for all i.

Now, suppose $u = \sum_{i=1}^m (\mu_i e_i + \mu_i' f_i)$ and $v = \sum_{i=1}^m (\nu_i e_i + \nu_i' f_i)$. Then since $\mathbf{f}(f_j, e_i) = -\mathbf{f}(e_i, f_j) = -\delta_{ij}$,

$$\mathbf{f}(u, v) = \sum_{i=1}^m (\mu_i \nu_i' \mathbf{f}(e_i, f_i) - \mu_i' \nu_i \mathbf{f}(e_i, f_i)) = \sum_{i=1}^m (\mu_i \nu_i' - \mu_i' \nu_i).$$

Let $\sigma = \tau(g)$, the associated field automorphism of g. Then

$$u^g = \sum_{i=1}^m (\mu_i^\sigma e_i^g + \mu_i'^\sigma f_i^g), \ v^g = \sum_{i=1}^m (\nu_i^\sigma e_i^g + \nu_i'^\sigma f_i^g),$$

and

$$\mathbf{f}(u^g, v^g) = \sum_{i=1}^m ((\mu_i \nu_i')^\sigma \mathbf{f}(e_i^g, f_i^g) - (\mu_i' \nu_i)^\sigma \mathbf{f}(e_i^g, f_i^g)) = \lambda \sum_{i=1}^m (\mu_i \nu_i' - \mu_i' \nu_i)^\sigma = \lambda \mathbf{f}(u, v)^\sigma.$$

Therefore $g \in \Gamma\mathrm{Sp}(V)$. □

Finally we suppose that $V = (V, \mathbf{f})$ where $\mathbf{f}$ is a unitary form and discuss the unitary geometry. The proof of the next proposition can be found in lots of texts, for example, [26, Propositions 2.3.1, 2.3.2]. This proposition tells us that there is a unique unitary geometry up to isometry for $V(d,q)$ and hence the group $\Gamma\mathrm{U}(V)$ is uniquely determined up to conjugacy in $\Gamma\mathrm{L}(d,q)$.

Proposition 3.4.5 *Suppose that $V = (V, \mathbf{f})$ where $\mathbf{f}$ is a unitary form. Then V has a basis $\{v_1, ..., v_d\}$ such that $\mathbf{f}(v_i, v_j) = \delta_{ij}$. Moreover, if the dimension $d \geq 2$ then there exists a nonzero vector v such that $\mathbf{f}(v, v) = 0$.*

A basis described in the above proposition is called an *orthonormal basis*. Let

$$\Phi = \{v \in V \mid \mathbf{f}(v, v) = 0\}.$$

Thus $\Phi \setminus \{0\}$ is non-empty if and only if $d \geq 2$. We define $\mathrm{GU}(V) = \Gamma\mathrm{U}(V) \cap \mathrm{GL}(V)$. King has proved the following proposition in [24].

Proposition 3.4.6 [24, Proposition 1] *Suppose* $d \geq 2$ *and let* $\Phi = \{v \in V | \mathbf{f}(v,v) = 0\}$. *If* $g \in \mathrm{GL}(d,q)$ *fixes* Φ *setwise, then* $g \in \mathrm{GU}(V)$.

We have the following corollary immediately.

Corollary 3.4.7 *Suppose* $d \geq 2$ *and let* $\Phi = \{v \in V | \mathbf{f}(v,v) = 0\}$. *If* $g \in \Gamma\mathrm{L}(d,q)$ *fixes* Φ *setwise, then* $g \in \Gamma\mathrm{U}(V)$.

Proof. Pick an orthonormal basis $\{v_1, ..., v_d\}$, then $\mathbf{f}(v_i, v_j) = \delta_{ij}$. Since $\mathrm{GL}(d,q)$ is transitive on ordered bases of V, we may assume that the Frobenius automorphism $\tau \in \Gamma\mathrm{L}(d,q)$ was defined with respect to this basis (see Section 3.2) and hence that $\tau \in \Gamma\mathrm{U}(V)$. It is easy to prove that τ fixes Φ setwise. Then for all i, $g\tau^i$ fixes Φ setwise. In particular, $g\tau(g)^{-1} \in \mathrm{GL}(V)$, and $g\tau(g)^{-1}$ also fixes Φ setwise.

It now follows from Proposition 3.4.6 that $g\tau(g)^{-1} \in \mathrm{GU}(V)$ and hence $g \in \Gamma\mathrm{U}(V)$. □

Remark Note that the notation $\Gamma\mathrm{O}(V), \Gamma\mathrm{Sp}(V)$ and $\Gamma\mathrm{U}(V)$ may differ from usage elsewhere in the literature. In particular, the groups $\Gamma\mathrm{O}(V), \Gamma\mathrm{Sp}(V)$ and $\Gamma\mathrm{U}(V)$ all contain the scalar subgroup Z and are defined relative to a certain form $\mathbf{Q}$ or $\mathbf{f}$, and we have not shown the form in the notation.

Chapter 4

Aschbacher's Classification

As we indicated in Chapter 1, our proof of the main result, Theorem 6.0.6, is based on Aschbacher's description of subgroups of $\Gamma L(d, q)$, (see [1] and [26]). In this chapter, we give a detailed description of Aschbacher's classification. As usual, suppose $q = p^f$ where p is a prime and $f \geq 1$, and let $V = V(d, q)$ be a vector space of dimension d over F_q with $d \geq 2$, and let Z denote the subgroup of scalar matrices of $\Gamma L(d, q)$.

In [1], Aschbacher defined eight families $C_1, \ldots, C_8$ of subgroups of $\Gamma L(d, q)$ that do not contain $SL(d, q)$. These families are usually defined in terms of some geometrical properties associated with the action on the underlying vector space $V(d, q)$, and in all of these cases the maximal subgroups of $\Gamma L(d, q)$ in each family can be identified. Aschbacher's Theorem states that for a subgroup H of $\Gamma L(d, q)$ which does not contain $SL(d, q)$, H is either contained in one of these eight classes or is "nearly simple" in the sense that there is a nonabelian simple group T such that $T \leq H/(H \cap Z) \leq \mathrm{Aut}(T)$.

Definition 4.0.8 Let $H \in \Gamma L(d, q)$. We say that $H \in C_i$ for $i = 1, 2, ..., 8$, if there exists a maximal C_i-subgroup M such that $H \leq M$. In addition, we say that $H \in C_9$ if H does not contain $SL(d, q)$ and is not contained in any maximal C_i-subgroup for $i = 1, 2, ..., 8$.

By Aschbacher's Theorem, if $H \in C_9$ then H is a nearly simple subgroup.

4.1 The reducible subgroups C_1

Suppose $H \in C_1$. Then H acts reducibly on V, that is, H preserves a nontrivial proper subspace of V.

Hence all the maximal C_1-subgroups have the following form. Suppose W is a nontrivial proper subspace of V. The stabilizer of W in $\Gamma L(d, q)$, denoted by $\mathrm{Stab}_{\Gamma L}(W)$, is a maximal C_1-subgroup.

4.2 The imprimitive subgroups C_2

Suppose $H \in C_2$. Then H acts irreducibly but imprimitively on V. We say that H is *imprimitive* on V if H preserves a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_t$ such that $\dim V_1 = \cdots = \dim V_t = a$ and $d = at$ for some $t > 1$.

Thus all the maximal C_2-subgroups have the following form. Suppose $V = V_1 \oplus \cdots \oplus V_t$ where $\dim V_1 = \cdots = \dim V_t = a$ and $d = at$ for some $t > 1$. The stabilizer in $\Gamma\mathrm{L}(d, q)$ of this subspace decomposition is a maximal C_2-subgroup. We denote it by $\mathrm{Stab}_{\Gamma\mathrm{L}}(\oplus V_i)$.

Next we determine the group $\mathrm{Stab}_{\Gamma\mathrm{L}}(\oplus V_i)$. It is easy to see that the stabilizer of the above subspace decomposition in $\mathrm{GL}(d, q)$ is isomorphic to $\mathrm{GL}(a, q) \wr S_t$, (see [26, Table 4.2A]). Recall from Section 3.2 that $\Gamma\mathrm{L}(d, q) = \mathrm{GL}(d, q) \rtimes \langle \tau \rangle$ and τ is defined with respect to a basis $\{v_1, ..., v_d\}$. It is sufficient to consider the case where there is a basis for each of the V_i contained in the basis $\{v_1, ..., v_d\}$. Then it is easy to see that $\tau \in \mathrm{Stab}_{\Gamma\mathrm{L}}(\oplus V_i)$. Thus

$$\mathrm{Stab}_{\Gamma\mathrm{L}}(\oplus V_i) = (\mathrm{GL}(a, q) \wr S_t) \rtimes \langle \tau \rangle.$$

4.3 The field extension subgroups C_3

Suppose $H \in C_3$. Then H preserves on V the structure of a vector space over an extension field of F_q, and a maximal C_3-subgroup is the stabilizer of a (d/b)-dimensional vector space structure on V over an extension field of F_q of degree b, where b is a prime dividing d.

Next we give a detailed description of C_3-subgroups. Suppose $d = ab$ where $b > 1$. Let $F = F_{q^b}$ be an extension field of the field F_q, and let $F = F_q[\omega]$. Then F is a vector space of dimension b over F_q and $\{1, \omega, ..., \omega^{b-1}\}$ is a basis. We may regard $V = V(d, q)$ as an a-dimensional vector space over F. Let $B = \{v_1, ..., v_a\}$ be a basis for $V(a, q^b)$ as an F-vector space. Then $B' = \{\omega^i v_j \mid \ 1 \leq j \leq a,\ 0 \leq i \leq b-1\}$ is a basis for $V(d, q)$ as an F_q-vector space. Since $\mathrm{GL}(d, q)$ is transitive on ordered F_q-bases of V, we may assume that B' is the basis used to define τ in Section 3.2.

Consider $\Gamma\mathrm{L}(a, q^b) = \langle \mathrm{GL}(a, q^b), \sigma \rangle$, where σ is the Frobenius automorphism of F_{q^b} over the prime field F_p acting on $V(a, q^b)$ with respect to the basis B, that is, $(\lambda_1 v_1 + ... + \lambda_a v_a)^\sigma = \lambda_1^p v_1 + ... + \lambda_a^p v_a$, where $\lambda_i \in F$ for $1 \leq i \leq a$. If $g \in \mathrm{GL}(a, q^b)$, then $(u + v)^g = u^g + v^g$ and $(\lambda u)^g = \lambda u^g$ for any $u, v \in V(d, q)$ and for any $\lambda \in F_q$. Thus $\mathrm{GL}(a, q^b) \leq \mathrm{GL}(d, q)$. By the definition of σ, we have

$$\sigma : \sum_{ij} \lambda_{ij} \omega^i v_j \to \sum_{ij} \lambda_{ij}^p (\omega^i)^p v_j.$$

Hence $\sigma = \tau g' \in \Gamma\mathrm{L}(d, q)$ where $g' \in \mathrm{GL}(d, q)$ is the linear transformation that acts on the basis vectors by $\omega^i v_j \mapsto (\omega^i)^p v_j$. Thus $\Gamma\mathrm{L}(a, q^b)$ is a subgroup of $\Gamma\mathrm{L}(d, q)$. Every maximal C_3-subgroup is a conjugate of this subgroup when b is a prime.

4.4 The tensor product subgroups C_4

Suppose $H \in C_4$. Then H preserves on V a tensor decomposition $V = U \otimes W$ where $\dim U \neq \dim W$ with $\dim U \geq 2$ and $\dim W \geq 2$. Thus this case only arises if d is composite, and in particular, if $d \geq 6$.

All the maximal C_4-subgroups of $\Gamma\mathrm{L}(V)$ are of the following form. Suppose that $V = U \otimes W$ where $\dim U \neq \dim W$ with $\dim U \geq 2$ and $\dim W \geq 2$. The stabilizer of this tensor decomposition in $\Gamma\mathrm{L}(d, q)$ is a maximal C_4-subgroup, denoted by $\mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$. Note that the stabilizer of $V = U \otimes W$ in $\mathrm{GL}(d, q)$ is $\mathrm{GL}(U) \otimes \mathrm{GL}(W)$, (see [26, Table 4.4A]).

Next we determine the group $\mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$. Suppose $\{x_i\}_{i\geq 1}$ is a basis of U and $\{y_j\}_{j\geq 1}$ is a basis of W. Then $\{x_i \otimes y_j\}_{i,j\geq 1}$ is a 'tensor product' basis of V, and we define the action of τ on V with respect to this basis. Then τ belongs to $\mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$. Therefore

$$\mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W) = (\mathrm{GL}(U) \otimes \mathrm{GL}(W)) \rtimes \langle \tau \rangle.$$

4.5 The subfield subgroups C_5

Suppose $H \in C_5$. Then H preserves on V the structure of a vector space over a proper subfield of F_q, (in this case, $q = p^f$ for $f > 1$). A maximal subgroup in this family is the stabilizer of a d-dimensional F_{q_0}-subspace of V where $q_0 = p^{f/b}$ for some prime b dividing f.

Next we give a detailed description of C_5-subgroups. As in Section 3.2, let $\{v_1, ..., v_d\}$ be a basis of $V(d, q)$, and define τ with respect to this basis. Let a be a divisor of f with $a < f$, set $q_0 = p^a$, and let F_{q_0} denote the proper subfield of F_q of order q_0. Let

$$V_0 = \mathrm{Span}_{F_{q_0}} \langle v_1, ..., v_d \rangle.$$

Then $\mathrm{GL}(V_0) = \mathrm{GL}(d, q_0)$ has a natural action on V and so we may regard $\mathrm{GL}(d, q_0)$ as a subgroup of $\mathrm{GL}(d, q)$. Since the field automorphism τ induces the Frobenius automorphism of the subfield F_{q_0}, the subgroup $\langle \tau \rangle$ of $\Gamma\mathrm{L}(d, q)$ normalizes $\mathrm{GL}(d, q_0)$. Also, $\mathrm{GL}(d, q_0) \rtimes \langle \tau \rangle$ is the maximal subgroup of $\Gamma\mathrm{L}(d, q)$ which fixes V_0 setwise, and the permutation group induced by $\mathrm{GL}(d, q_0) \rtimes \langle \tau \rangle$ on V_0 is $\Gamma\mathrm{L}(d, q_0)$.

Recall that Z is the subgroup of scalar matrices of $\Gamma\mathrm{L}(d,q)$. The maximal C_5-subgroups of $\Gamma\mathrm{L}(d,q)$ with respect to the divisor a of f are conjugates of the subgroup

$$\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0) = (\mathrm{GL}(d,q_0) \circ Z) \rtimes \langle \tau \rangle.$$

(This subgroup is maximal among the C_5-subgroups if and only if f/a is prime.) Note that a semilinear transformation g belongs to $\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$ if and only if g sends V_0 to λV_0 for some $\lambda \in F_q$.

4.6 The symplectic-type subgroups C_6

Suppose $H \in C_6$. Then H has as a normal subgroup an r-group of symplectic type (with prime $r \neq p$), which acts absolutely irreducibly on V, and the maximal C_6-subgroups are the normalizers in $\Gamma\mathrm{L}(d,q)$ of certain absolutely irreducible symplectic type r-groups for a prime $r \neq p$.

4.6.1 Symplectic type r-groups.

First we explain the symplectic type r-groups which appear in the definition of C_6-subgroups. We only give a brief description of these groups, for a detailed definition see [26, §4.6].

Let $r > 2$ be a prime. Define

$$R_0 = \langle x, y, z \mid x^r = y^r = z^r = [x,z] = [y,z] = 1, [y,x] = z \rangle. \tag{4.1}$$

The group R_0 is an r-group of symplectic-type. Note that the group R_0 has order r^3 and exponent r, and the center $Z(R_0) = \langle z \rangle$ is a cyclic group of order r. Let $r = 2$, the dihedral group D_8 and the quaternion group Q_8 are symplectic-type groups of order 8. The following definition tells us that all symplectic type r-groups R with exponent $r(2,r)$ can be constructed from R_0, D_8 and Q_8.

Definition 4.6.1 [26, Proposition 4.6.2] *Let R be an r-group for some prime r. Then R is of symplectic-type with exponent $r(2,r)$ if R is isomorphic to one of the following.*

1. $R = \overbrace{R_0 \circ \cdots \circ R_0}^{m}$ *where r is odd, $m \geq 1$, and R_0 is defined in (4.1).*
2. $R = \overbrace{D_8 \circ \cdots \circ D_8}^{m}$ *where $r = 2$ and $m \geq 1$.*
3. $R = \overbrace{D_8 \circ \cdots \circ D_8}^{m-1} \circ Q_8$ *where $r = 2$ and $m \geq 1$.*
4. $R = Z_4 \circ \overbrace{Q_8 \circ \cdots \circ Q_8}^{m}$ *where $r = 2$ and $m \geq 1$.*

4.6.2 The maximal C_6-subgroups $H = N_{\Gamma L(d,q)}(R)$

If we assume that H is a maximal C_6-subgroup, then

$$H = N_{\Gamma L(d,q)}(R)$$

where R is an r-group of symplectic type of exponent $r(2,r)$. By [26, pp. 150], we know that $R \leq \mathrm{GL}(d,q)$. Moreover R can be realized over the subfield F_{p^e} where e is the smallest integer for which $p^e \equiv 1 \pmod{|Z(R)|}$. If $p^e \neq q$, by [1, 3.15], the normalizer $N_{\Gamma L(d,q)}(R)$ is actually a C_5-subgroup. In more detail, defining the F_{p^e}-subspace

$$U = \mathrm{Span}_{F_{p^e}}\langle v_1, ..., v_d\rangle = U(d,p^e)$$

where $\{v_1, ..., v_d\}$ is the F_q-basis for V with respect to which τ was defined in Section 3.2, we may replace R by a conjugate in $\Gamma L(d,q)$ if necessary and obtain that $R \leq \mathrm{GL}(U) = \mathrm{GL}(d,p^e)$, R is absolutely irreducible on U and

$$N_{\Gamma L(d,q)}(R) \leq \mathrm{Stab}_{\Gamma L}(F_qU) = (\mathrm{GL}(d,p^e) \circ Z) \rtimes \langle\tau\rangle$$

(see Section 4.5 for a detailed description of $\mathrm{Stab}_{\Gamma L}(F_qU)$ in $\Gamma L(d,q)$). Therefore, by [1, Theorem A.4],

$$H = N_{\Gamma L(d,q)}(R) = (N_{\mathrm{GL}(d,p^e)}(R) \circ Z).\langle\tau\rangle. \tag{4.2}$$

When $d = 2$, by [26, Table 4.6B], the maximal C_6-subgroup H is the normalizer of $R = Q_8$ in $\Gamma L(2,q)$ with q odd. Next we assume that $d \geq 3$. We will divide H into several types according to the type of R, and explain the representations of H on $V(d,q)$ type by type and look at the corresponding group structures of H carefully in next subsection.

4.6.3 The structure of $N_{\mathrm{GL}(d,p^e)}(R)$ when $d \geq 3$

In view of (4.2), to describe the group structure of the maximal C_6-subgroup H, it is sufficient to consider the structure of $N_{\mathrm{GL}(d,p^e)}(R)$ where e is the smallest integer for which $p^e \equiv 1 \pmod{|Z(R)|}$.

Suppose that $d \geq 3$. We may divide H into the following five types depending on the type of R (see [26, Table 4.6A, 4.6B]). Note that we assume $F = F_{p^e}$ and $V = V(d,p^e)$ when we describe the following types. Hence the subgroup Z below is the center of $\mathrm{GL}(d,p^e)$.

Type 1. $R = \overbrace{R_0 \circ \cdots \circ R_0}^{m}$ where r is odd, $r \mid (p^e - 1)$, $m \geq 1$, $d = r^m$ and $R_0 = \langle x, y\rangle$ is as in (4.1). We have $|R| = r^{1+2m}$, $|Z(R)| = r$ and $N_{\mathrm{GL}(d,p^e)}(R) = (Z \circ R).\mathrm{Sp}(2m, r)$.

A faithful irreducible representation of R_0 is given as follows. Let $W_1 = V(r, p^e)$ be a vector space over F_{p^e} of dimension r. Let $\omega \in F_{p^e}^*$ be a primitive r^{th} root of unity. Pick a basis $\{e_0, e_1, ..., e_{r-1}\}$ of W_1. Let

$$x : e_i \mapsto \omega^i e_i, \ 0 \leq i \leq r-1, \tag{4.3}$$

$$y : e_i \mapsto e_{i+1}, \ \text{where } i \text{ is taken modulo } r.$$

Then x and y give rise to an absolutely irreducible representation of R_0. Thus by taking a tensor product of m copies of this representation one obtains an absolutely irreducible representation of $R = \overbrace{R_0 \circ \cdots \circ R_0}^{m}$ of degree r^m on $V = W_1 \otimes \cdots \otimes W_m$ with $W_i \cong W_1$. Here $Z(R) = \langle \omega \rangle$ acts on V by scalar transformations.

Now it is easy to see that

$$(e_0 \otimes w_2 \otimes \cdots \otimes w_m)^{x \otimes 1 \otimes \cdots \otimes 1} = e_0 \otimes w_2 \otimes \cdots \otimes w_m$$

where e_0 and x are as in (4.3) and w_i is any nonzero vector of W_i. Hence R is not semi-regular on $V \setminus \{0\}$. We will need this fact later.

Type 2. $R = Z_4 \circ \overbrace{Q_8 \circ \cdots \circ Q_8}^{m}$ where $r = 2$, $4|(p^e - 1)$ with $e = 1$ or 2, $d = 2^m \geq 3$, (hence $m \geq 2$) and

$$Q_8 \cong R_1 = \langle x, y | \ x^4 = y^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle.$$

We have $|R| = 2^{2+2m}$, $|Z(R)| = 4$ and $N_{\mathrm{GL}(d,p^e)}(R) = (Z \circ R).\mathrm{Sp}(2m, 2)$.

Let $W_1 = V(2, p^e)$ be a 2-dimensional vector space over F_{p^e}. Let $i \in F_{p^e}^*$ be a primitive 4^{th} root of unity. Pick a basis $\{e_0, e_1\}$ of W_1. Let

$$x : e_0 \rightarrow ie_0, \qquad e_1 \rightarrow (-i)e_1; \tag{4.4}$$

$$y : e_0 \rightarrow e_1, \qquad e_1 \rightarrow -e_0.$$

Then x and y give rise to an absolutely irreducible representation of $R_1 \cong Q_8$. Forming the m-fold tensor product V as before, we have $R = \langle i \rangle \circ (R_1 \otimes \cdots \otimes R_m) \leq \mathrm{GL}(V)$, where $R_j \cong R_1$, and $V = W_1 \otimes \cdots \otimes W_m$, with $W_j \cong W_1$ for $1 \leq j \leq m$. Here $Z(R) = \langle i \rangle$, where i denotes a scalar transformation of order 4. Similarly, in this type, R is not semi-regular on $V \setminus \{0\}$ since

$$(e_1 \otimes w_2 \otimes \cdots \otimes w_m)^{i(x \otimes 1 \otimes \cdots \otimes 1)} = e_1 \otimes w_2 \otimes \cdots \otimes w_m$$

where e_1 and x are as in (4.4) and w_j is any nonzero vector in W_j.

Type 3. $R = \overbrace{D_8 \circ \cdots \circ D_8}^{m}$ where $r = 2$, $e = 1$, $p \equiv -1 \pmod 4$ and $d = 2^m$ with $m \geq 3$. We have $|R| = 2^{1+2m}$, $|Z(R)| = 2$ and $N_{\mathrm{GL}(d,p)}(R) = (Z \circ R).O^+(2m, 2) \leq \mathrm{GO}^+(d, p)$.

Type 4. $R = \overbrace{D_8 \circ \cdots \circ D_8}^{m-1} \circ Q_8$ where $r = 2$, $e = 1$, $p \equiv -1 \pmod 4$ and $d = 2^m$ with $m \geq 2$. We have $|R| = 2^{1+2m}$, $|Z(R)| = 2$ and $N_{\mathrm{GL}(d,p)}(R) = (Z \circ R).O^-(2m, 2) \leq \mathrm{GSp}(d, p)$.

Type 5. $R = D_8 \circ D_8$ where $r = 2$, $e = 1$, $p \equiv -1 \pmod 4$ and $d = 4$. We have $|Z(R)| = 2$ and $N_{\mathrm{GL}(4,p)}(R) = (Z \circ R).O^+(4, 2) \leq \mathrm{GO}^+(4, p)$. This is actually the case of $m = 2$ in Type 3. We will deal with this case separately as the group $O^+(4, 2)$ has normal subgroup structure very different from the other groups $O^+(2m, 2)$ with $m \geq 3$.

We can also assume that $4 \nmid (p-1)$ in types 3, 4 and 5 for the following reason. When $4|(p-1)$, we have $Z_4 \leq Z$. It is easy to see that the normalizers of R and $Z_4 \circ R$ in $\mathrm{GL}(d, p)$ are the same, and we note that when $m \geq 2$,

$$Z_4 \circ \overbrace{D_8 \circ \cdots \circ D_8}^{m} \cong Z_4 \circ \overbrace{Q_8 \circ \cdots \circ Q_8}^{m} \cong Z_4 \circ \overbrace{D_8 \circ \cdots \circ D_8}^{m-1} \circ Q_8.$$

Hence the normalizer is of type 2. Since we are only interested in the normalizer of R in $\mathrm{GL}(d, p)$ in our proof later (Proposition 6.9.1), we may assume that $4 \nmid (p-1)$ for the types 3, 4, 5.

We next prove that if R is of type 3, 4 or 5, then R is not semi-regular on $V \setminus \{0\}$. Let

$$D_8 = \langle x, y \mid x^4 = 1, y^2 = 1, y^{-1}xy = x^{-1} \rangle.$$

Let $W_1 = V(2, p)$ be a 2-dimensional vector space over F_p. Pick a basis $\{e_0, e_1\}$ of W_1. Let

$$x : e_0 \to e_1, \qquad e_1 \to -e_0.$$

$$y : e_0 \to e_0, \qquad e_1 \to -e_1. \tag{4.5}$$

Then x and y give rise to an absolutely irreducible representation of D_8. Also, there exists an absolutely irreducible representation of Q_8 on $V(2, p)$, so that $Q_8 \leq \mathrm{GL}(2, p)$ (see [26, p. 154]).

Each group R of type 3, 4 or 5 is obtained as a tensor product (see [26, p. 154]), namely $R = R_1 \otimes \cdots \otimes R_{m-1} \otimes R_\varepsilon \leq \mathrm{GL}(V)$ where $\varepsilon = \pm$, $R_- \cong Q_8$ and $R_j \cong D_8$ for $j = +, 1, 2, ..., m-1$, and $V = W_1 \otimes \cdots \otimes W_m$, where $W_j \cong W_1$ for $1 \leq j \leq m$. The subgroup R is not semi-regular on $V \setminus \{0\}$ as

$$(e_0 \otimes w_2 \otimes \cdots \otimes w_m)^{y \otimes 1 \otimes \cdots \otimes 1} = e_0 \otimes w_2 \otimes \cdots \otimes w_m$$

where e_0 and y are as in (4.5) and for $2 \leq j \leq m$, w_j is any nonzero vector in W_j.

We summarize this result and our discussion of types 1 and 2 in a lemma.

Lemma 4.6.2 *Suppose $d \geq 3$. For all types, R is not semi-regular on $V(d, p^e) \setminus \{0\}$.*

4.7 The tensor product subgroups C_7

Suppose $H \in C_7$. Then H preserves on V a tensor decomposition $V = \otimes_{i=1}^{t} W_i$ with $\dim W_i = c \geq 2$. Thus this case only arises if d is composite, and in particular, if $d \geq 4$.

All the maximal C_7-subgroups of $\Gamma\mathrm{L}(V)$ are of the following form. Suppose that $V = W_1 \otimes \cdots \otimes W_t$ is the tensor product of $t \geq 2$ copies $W_1, ..., W_t$ of a vector space W of dimension $c \geq 2$, where $d = \dim V = c^t$. The stabilizer of this tensor decomposition is a maximal C_7-subgroup, denoted by $\mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$. Note that the stabilizer of $V = W_1 \otimes \cdots \otimes W_t$ in $\mathrm{GL}(d, q)$ is $\mathrm{GL}(W) \wr_{\otimes} S_t$ (see [26, Table 4.7A]), where

$$\mathrm{GL}(W) \wr_{\otimes} S_t = (\mathrm{GL}(W) \otimes \cdots \otimes \mathrm{GL}(W)) \rtimes S_t.$$

Next we determine the group $\mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$. Pick a typical tensor product basis of V as in case C_4, and define the action of τ on V with respect to this basis. Then τ belongs to $\mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$. Therefore

$$\mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i) = (\mathrm{GL}(W) \wr_{\otimes} S_t) \rtimes \langle \tau \rangle.$$

4.8 The classical subgroups C_8

Suppose $H \in C_8$. Then H is a subgroup of $\Gamma\mathrm{O}(V), \Gamma\mathrm{Sp}(V)$ or $\Gamma\mathrm{U}(V)$. Also the classical groups $\Gamma\mathrm{O}(V), \Gamma\mathrm{Sp}(V)$ and $\Gamma\mathrm{U}(V)$ are the maximal C_8-subgroups. We have defined these subgroups in Section 3.4.

Remark: In this thesis, we define the classes C_i $(i = 1, ..., 8)$ as subgroups which have a particular property as above. Hence there exist some subgroups which belong to more than one class. For example, we include the subgroups $\Gamma\mathrm{O}(2m + 1, 2^f)$ as maximal C_8 subgroups as they are classical groups. On the other hand, $\Gamma\mathrm{O}(2m + 1, 2^f)$ are also C_1-subgroups as they are reducible.

Chapter 5

Some Special Semilinear Subgroups

In this chapter, we begin to answer Question 1.2.1 for $k = 3$. The best approach to study 3-closures of affine permutation groups is first to study 2-closures of semilinear subgroups of $\Gamma\mathrm{L}(d, q)$ where $q = p^f$ is a power of a prime p (see Lemma 2.4.1 (4)).

Suppose that $H \leq \Gamma\mathrm{L}(d, q)$ where $d \geq 1$ and $q = p^f$. In this chapter, we study the 2-closures of H in some special cases. Our results in this chapter are independent of the Classification of Finite Simple Groups. The main result of this chapter is the following theorem which deals with subgroups H of $\Gamma\mathrm{L}(d, q)$ containing $\mathrm{SL}(d, q)$, (this includes the case $d = 1, H \leq \Gamma\mathrm{L}(1, q)$). The notation has been explained in Section 3.2.

Theorem 5.0.1 *Suppose* $\mathrm{SL}(d, q) \leq H \leq \Gamma\mathrm{L}(d, q) = \mathrm{GL}(d, q) \rtimes \langle\tau\rangle$ *where* τ *is the Frobenius automorphism of* F_q *and* $q = p^f$*. Consider the action of* H *on* $V(d, q) \setminus \{0\}$*,*

(1) *If* $d = 1$*, then every subgroup* H *of* $\Gamma\mathrm{L}(1, q)$ *is* 2*-closed.*

(2) *If* $d = 2$*, then* $H^{(2)} \cap \Gamma\mathrm{L}(2, q) \leq H\langle\tau^i\rangle$ *where* i *satisfies* $\langle\tau^i\rangle = \{\tau(h) |\ h \in H\}$ *and* $\tau(h)$ *is the associated field automorphism of* h*. In particular, if either* $H \leq \mathrm{GL}(2, q)$ *or* $\tau^i \in H$*, then* $H^{(2)} \cap \Gamma\mathrm{L}(2, q) = H$*.*

(3) *If* $d \geq 3$*, then* $H^{(2)} \cap \Gamma\mathrm{L}(d, q) = \mathrm{GL}(d, q) \rtimes \langle\tau^i\rangle$ *where* i *satisfies* $\langle\tau^i\rangle = \{\tau(h) |\ h \in H\}$*.*

Remark: We prove more than this, namely, that Part (2) holds for all subgroups H of $\Gamma\mathrm{L}(2, q)$ (see Proposition 5.2.1). Also we note that the condition $d \geq 3$ in Part (3) cannot be omitted. (Consider the groups $\mathrm{SL}(d, q).\langle\tau^i\rangle$ with $d \leq 2$.)

The outline of this chapter is as follows. First we suppose that $d = 2$, we discuss Aschbacher classes in dimension 2 (Lemma 5.1.2) and obtain Proposition 5.2.1 proving Theorem 5.0.1(2). Secondly, we study the 2-closure of H where $\mathrm{SL}(d, q) \leq H \leq \Gamma\mathrm{L}(d, q)$

and $d \geq 3$, and obtain Proposition 5.3.1 proving Theorem 5.0.1(3). Lastly, we suppose that $d = 1$ and obtain Theorem 5.4.1 which proves Theorem 5.0.1(1). We also determine 3-closures of 1-dimensional affine permutation groups in Theorem 5.4.1(2).

5.1 Dickson's theorem and Aschbacher classes in dimension 2

Dickson [11] classified all the subgroups of $\mathrm{PSL}(2, q)$ by an elementary method (see [50, Chapter 3, §6] or [20, Chaper 2, §8] for a proof). When we handle the 2-dimensional case, Dickson's Theorem is one of our main tools.

Theorem 5.1.1 [Dickson] *Let $q = p^f$ be a power of a prime and let $s = (2, q-1)$. Also let z be an integer that divides $\frac{q+1}{s}$ or $\frac{q-1}{s}$. Then a subgroup of $\mathrm{PSL}(2, q)$ is isomorphic to one of the following groups.*

1. *An elementary abelian p-group Z_p^m where $m \leq f$.*
2. *A cyclic group of order z.*
3. *A dihedral group of order $2z$.*
4. *A_4 if $p > 2$, or $p = 2$ and $f \equiv 0$ (mod 2).*
5. *S_4 if $p^{2f} - 1 \equiv 0$ (mod 16).*
6. *A_5 if $p = 5$ or $p^{2f} - 1 \equiv 0$ (mod 5).*
7. *$Z_p^m \rtimes Z_t$ where $m \leq f$, $t | \frac{p^m-1}{s}$ and $t|(p^f - 1)$.*
8. *$\mathrm{PSL}(2, p^m)$ with $m|f$ or $\mathrm{PGL}(2, p^m)$ with $2m|f$.*

Next we consider the 2-dimensional maximal C_i-subgroups for $1 \leq i \leq 8$, (see Chapter 4 for the definition of C_i-subgroups). Recall from Section 3.2 that the Frobenius automorphism $\tau \in \Gamma\mathrm{L}(2, q)$ is the map $\lambda_1 v_1 + \lambda_2 v_2 \to \lambda_1^p v_1 + \lambda_2^p v_2$ where $\{v_1, v_2\}$ is a chosen basis for $V = V(2, q)$.

Lemma 5.1.2 *Suppose $V = V(2, q)$ and $M \leq \Gamma\mathrm{L}(2, q)$ where q is not a prime. Suppose also that $M \not\geq \mathrm{SL}(2, q)$ and M is a maximal C_i-subgroup for some $i = 1, ..., 8$. Then $i \neq 4, 7$, and either $i = 3$ and M is conjugate to $\Gamma\mathrm{L}(1, q^2)$, or $\tau^g \in M$ for some $g \in \mathrm{GL}(2, q)$.*

Proof. Since the dimension $d = 2$, there are no C_4 or C_7-subgroups.

Now suppose M is a maximal C_1-subgroup. Then M stabilizes a 1-subspace $\langle v\rangle$. If $g \in \mathrm{GL}(2,q)$ is such that $v_1^g = v$ (such a g exists), then τ^g fixes v as τ fixes v_1. So $\tau^g \in M$.

Suppose M is a maximal C_2-subgroup. Then M is the stabilizer of a decomposition $V = \langle v\rangle \oplus \langle w\rangle$. Since τ fixes (v_1, v_2) and there is an element $g \in \mathrm{GL}(2,q)$ such that $(v_1^g, v_2^g) = (v, w)$, we have $\tau^g \in M$ for such a g.

Suppose M is a maximal C_3-subgroup. Then $V = V(2,q)$ may be regarded as a 1-dimensional vector space over F_{q^2} in such a way that $M = \Gamma\mathrm{L}(1, q^2)$.

Suppose M is a maximal C_5-subgroup. Then there exist an F_q-basis $\{v, w\}$ and a proper subfield F_{q_0}, such that M leaves $\mathrm{Span}_{F_{q_0}}\langle v, w\rangle$ invariant modulo the scalars of F_q. Now τ^g fixes $\mathrm{Span}_{F_{q_0}}\langle v, w\rangle$ where $g \in \mathrm{GL}(2,q)$ maps (v_1, v_2) to (v, w). Hence $\tau^g \in M$.

Suppose M is a maximal C_6-subgroup. Then by [26, Table 4.6B], M is the normalizer of $R = Q_8$ in $\Gamma\mathrm{L}(2,q)$ with q odd. By [1, Theorem A (4)], M contains a conjugate of τ.

Finally, suppose M is a maximal C_8-subgroup. Then $V(2,q)$ is equipped with a non-degenerate symplectic, unitary or quadratic form. So $M = \Gamma\mathrm{Sp}(V), \Gamma\mathrm{U}(V)$ or $\Gamma\mathrm{O}^{\pm}(V)$. Since $M \not\geq \mathrm{SL}(2,q)$ and since $\mathrm{Sp}(2,q) = \mathrm{SL}(2,q)$, the first case does not arise. In the case of a unitary form, $q = q_0^2$ and $\mathrm{SU}(V) \cong \mathrm{SL}(2,q_0)$. Then M is a maximal C_5-subgroup (see [26, Remarks, p. 165]), and so has already been dealt with. Finally, we consider $\Gamma\mathrm{O}^{\pm}(V)$. Now, by [26, Remarks, p. 165], $\Gamma\mathrm{O}^{+}(V)$ is a C_2-subgroup and $\Gamma\mathrm{O}^{-}(V)$ is a C_3-subgroup. So these cases have already been considered. The proof is now complete. □

5.2 2-dimensional semilinear groups

Let $\Gamma\mathrm{L}(2,q) = \mathrm{GL}(2,q) \rtimes \langle\tau\rangle$. We use the notation introduced in Section 3.2. Let $\{v_1, v_2\}$ be a basis of $V(2,q)$, and let $\Omega = V(2,q) \setminus \{0\}$. The action of τ on V is then given by: $(\lambda v_1 + \mu v_2)^\tau = \lambda^p v_1 + \mu^p v_2$, for $\lambda, \mu \in F_q$. Then the stabilizer $\Gamma\mathrm{L}(2,q)_{(v_1,v_2)} = \langle\tau\rangle$.

Let

$$\Delta = \{(w_1, w_2)|\ w_1, w_2 \in \Omega \text{ and } w_1 \notin \langle w_2\rangle\}.$$

Then $\mathrm{GL}(2,q)$ is regular on Δ. Thus for any pair $(w_1, w_2) \in \Delta$, there exists exactly one $g \in \mathrm{GL}(2,q)$ such that $(w_1, w_2) = (v_1^g, v_2^g)$, and hence $\Gamma\mathrm{L}(2,q)_{(w_1,w_2)} = \langle g^{-1}\tau g\rangle = \langle g_1\rangle$ is a cyclic group generated by an element g_1 with $\tau(g_1) = \tau$.

The following proposition, which reduces to Part (2) of Theorem 5.0.1 in the special case where $H \geq \mathrm{SL}(2,q)$, is valid for any $H \leq \Gamma\mathrm{L}(2,q)$.

Proposition 5.2.1 *Suppose $H \leq \Gamma\mathrm{L}(2,q)$ and $K = H^{(2)} \cap \Gamma\mathrm{L}(2,q)$. Then $K \leq H\langle\tau^i\rangle$ where i satisfies $\langle\tau^i\rangle = \{\tau(h)|\ h \in H\}$. In particular, if either $H \leq \mathrm{GL}(2,q)$ or $\tau^i \in H$, then $H = K$.*

Proof. Let $\langle \xi \rangle = F_q^*$ and let $v \in \Omega$. Since

$$(v, \xi v)^H = (v, \xi v)^K,$$

for any $g \in K$, there exists $h \in H$ such that

$$(v^h, (\xi v)^h) = (v^g, (\xi v)^g).$$

Thus

$$\xi^{\tau(h)} v^h = (\xi v)^h = (\xi v)^g = \xi^{\tau(g)} v^g = \xi^{\tau(g)} v^h.$$

Therefore, $\tau(g) = \tau(h)$, and $gh^{-1} \in K \cap \mathrm{GL}(2, q)$. Then $K = H(K \cap \mathrm{GL}(2, q))$. Thus if $H \leq \mathrm{GL}(2, q)$, then $K \leq \mathrm{GL}(2, q)$.

Now for any $g \in \mathrm{GL}(2, q) \cap K$, g is determined by the images of the basis vectors v_1 and v_2 under g. Since

$$(v_1, v_2)^H = (v_1, v_2)^K,$$

there exists $h \in H$ such that

$$(v_1^g, v_2^g) = (v_1^h, v_2^h).$$

Thus $h = \tau^j g$ for some j such that $i|j$, and $\tau^j \in K$. Therefore $K \leq H\langle \tau^i \rangle$ where i satisfies $\langle \tau^i \rangle = \{\tau(h) |\ h \in H\}$. Finally, if $H \leq \mathrm{GL}(2, q)$ or $\tau^i \in H$ then $K = H$. □

We have following corollary concerning 3-closures of affine permutation groups.

Corollary 5.2.2 *Let $G = Z_p^2 \cdot H$ be a 2-dimensional affine group with $H \leq \mathrm{GL}(2, p)$. Then $G^{(3)} \cap \mathrm{AGL}(2, p) = G$.*

Proof. Suppose $G^{(3)} \cap \mathrm{AGL}(2, p) = Z_p^2 \cdot K$ where $H \leq K \leq \mathrm{GL}(2, p)$. By Lemma 2.4.1 (4), $K \leq H^{(2)} \cap \mathrm{GL}(2, p)$. By Proposition 5.2.1, $H^{(2)} \cap \mathrm{GL}(2, p) = H$ and so $K = H$. Hence $G^{(3)} \cap \mathrm{AGL}(2, p) = G$ as required. □

Finally, we will look at a small example which indicates that even if in Theorem 5.0.1 (2) we assume that $H \geq \mathrm{SL}(2, q)$, $H^{(2)} \cap \Gamma\mathrm{L}(2, q)$ may still be strictly greater than H. Thus Proposition 5.2.1 is the best result we can get even in the case where $H \geq \mathrm{SL}(2, q)$.

Let $F = F_{5^2}$, $V = V(2, 5^2)$ and $\Omega = V \setminus \{0\}$. Let $\{v_1, v_2\}$ be a basis of V and let τ be the Frobenius automorphism with respect to this basis. For $g \in \mathrm{GL}(2, 5^2)$, suppose that $v_1^g = \lambda_1 v_1 + \lambda_2 v_2$ and $v_2^g = \lambda_3 v_1 + \lambda_4 v_2$ where $\lambda_i \in F$, then the matrix representation for g with respect to the basis $\{v_1, v_2\}$ is $g = \begin{pmatrix} \lambda_1 & \lambda_3 \\ \lambda_2 & \lambda_4 \end{pmatrix}$, and we have

$$g^\tau = \begin{pmatrix} \lambda_1^\tau & \lambda_3^\tau \\ \lambda_2^\tau & \lambda_4^\tau \end{pmatrix} = \begin{pmatrix} \lambda_1^5 & \lambda_3^5 \\ \lambda_2^5 & \lambda_4^5 \end{pmatrix}.$$

We will denote the determinant of $g \in \mathrm{GL}(2,5^2)$ by $\det(g)$. Then $\det : g \to \det(g)$ is a map from $\mathrm{GL}(2,5^2)$ to F^*. Let $\langle \xi \rangle = F^* \cong Z_{24}$, and let

$$H = \langle \mathrm{SL}(2,5^2), \tau g_1, g_2 \rangle \quad \text{where } g_1 = \begin{pmatrix} \xi^3 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } g_2 = \begin{pmatrix} \xi^8 & 0 \\ 0 & 1 \end{pmatrix}.$$

We show in the next lemma that $H^{(2)} \cap \Gamma\mathrm{L}(2,5^2)$ properly contains H.

Lemma 5.2.3 *1.* $\Gamma\mathrm{L}(2,5^2) = \langle \mathrm{SL}(2,5^2), g_1, g_2, \tau \rangle$ *and* $|\Gamma\mathrm{L}(2,5^2) : H| = 2$.

2. In the action on Ω, $\Gamma\mathrm{L}(2,5^2) \le H^{(2)}$.

Proof. (1) Note that $o(g_1) = 8$, $o(g_2) = 3$ and $[g_1, g_2] = 1$. Hence $\langle g_1, g_2 \rangle = \langle g_1 g_2 \rangle \cong Z_{24}$ and $\det(\langle g_1, g_2 \rangle) = F^*$. Therefore $\langle \mathrm{SL}(2,5^2), g_1, g_2 \rangle = \mathrm{GL}(2,5^2)$ and hence $\Gamma\mathrm{L}(2,5^2) = \langle \mathrm{SL}(2,5^2), g_1, g_2, \tau \rangle$. Also, $\tau g_1 \tau g_1 = g_1^\tau g_1 = \begin{pmatrix} \xi^{18} & 0 \\ 0 & 1 \end{pmatrix} = g_1^6$, so $\langle (\tau g_1)^2 \rangle = \langle g_1^2 \rangle$ and $H \cap \mathrm{GL}(2,5^2) = \langle \mathrm{SL}(2,5^2), g_1^2, g_2 \rangle$. Thus $|H| = 2|H \cap \mathrm{GL}(2,5^2)| = 2(|\mathrm{SL}(2,5^2)| \cdot 12) = |\Gamma\mathrm{L}(2,5^2)|/2$.

(2) Recall that $\{v_1, v_2\}$ is a basis of V, and let $K = \Gamma\mathrm{L}(2,5^2)$. Consider $\Delta = (v_1, v_2)^K$. Then the stabilizer $K_{(v_1,v_2)} = \langle \tau \rangle$, and

$$\Delta = \{(w_1, w_2) |\ w_1, w_2 \in \Omega \text{ and } w_1 \notin \langle w_2 \rangle\}.$$

Observe that $|\Delta| = |\mathrm{GL}(2,5^2)|$. Now since $\tau \notin H$, $|(v_1, v_2)^H| = |H| = |\Delta|$. Hence Δ is also an orbit of H. Also if

$$\Delta_\lambda = \{(v, \lambda v) |\ v \in \Omega\}, \text{ where } \lambda \in F^*,$$

then

$$\Delta_\lambda^H = \Delta_\lambda^K = \Delta_\lambda \cup \Delta_{\lambda^5}.$$

Therefore, K is 2-equivalent to H on Ω as required. □

5.3 The case $\mathrm{SL}(d,q) \le H \le \Gamma\mathrm{L}(d,q)$ $(d \ge 3)$

The following proposition is Part (3) of Theorem 5.0.1, the notation is introduced in Section 3.2.

Proposition 5.3.1 *Suppose* $\mathrm{SL}(d,q) \le H \le \Gamma\mathrm{L}(d,q)$ *with* $d \ge 3$ *and suppose* $K = H^{(2)} \cap \Gamma\mathrm{L}(d,q)$. *Then* $K = \mathrm{GL}(d,q) \rtimes \langle \tau^i \rangle$ *where* i *satisfies* $\langle \tau^i \rangle = \{\tau(h) |\ h \in H\}$.

Proof. Note that $\mathrm{SL}(d,q)$ $(d \ge 2)$ is transitive on $\Omega = V \setminus \{0\}$. When $d \ge 3$, $\mathrm{SL}(d,q)$ is actually 2-equivalent to $\mathrm{GL}(d,q)$ as these two groups have the same orbit sets on $\Omega \times \Omega$. These orbits are

$$\Delta = \{(v, w) |\ v, w \in \Omega \text{ and } v \notin \langle w \rangle\},$$

and

$$\Delta_\lambda = \{(v, \lambda v)|\ v \in \Omega\}, \text{ where } \lambda \in F_q^*.$$

Since each H-orbit in $\Omega \times \Omega$ is a union of $\mathrm{SL}(d,q)$-orbits, $\mathrm{GL}(d,q) \leq H^{(2)}$. Thus $\mathrm{GL}(d,q) \leq K \leq \Gamma\mathrm{L}(d,q) = \mathrm{GL}(d,q) \rtimes \langle\tau\rangle$, and so $K = \mathrm{GL}(d,q) \rtimes \langle\tau^j\rangle$ for some integer j.

Suppose $\langle\tau^i\rangle = \{\tau(h)|\ h \in H\}$. Then

$$\Delta^H = \Delta^{\langle\tau^i\rangle} = \Delta \quad \text{and} \quad (\Delta_\lambda)^H = (\Delta_\lambda)^{\langle\tau^i\rangle} = \cup_{\mu \in \{\lambda^{\langle\tau^i\rangle}\}} \Delta_\mu.$$

But if $\langle\tau^i\rangle \neq \langle\tau^j\rangle$, then there exists $\lambda \in F_q^*$ such that $\lambda^{\langle\tau^i\rangle} \neq \lambda^{\langle\tau^j\rangle}$. This would imply that H is not 2-equivalent to $K = \mathrm{GL}(d,q) \rtimes \langle\tau^j\rangle$, which would be a contradiction. Hence $\langle\tau^i\rangle = \langle\tau^j\rangle$ and the result follows. □

5.4 The case $d = 1$

In this section we treat the 1-dimensional case and prove Theorem 5.4.1. Theorem 5.4.1(1) is Part (1) of Theorem 5.0.1, and Theorem 5.4.1(2) is Part (1) of Theorem 7.1.1.

Theorem 5.4.1 *1. Every subgroup H of $\Gamma\mathrm{L}(1,q)$ is 2-closed in its action on F_q^*.*

2. Let $G \leq \mathrm{AGL}(1,p)$ be a 1-dimensional affine permutation group. Then $G^{(2)} = G^{(3)} = G$ for all proper subgroups G of $\mathrm{AGL}(1,p)$, while $\mathrm{AGL}(1,p)^{(2)} = S_p$ and $\mathrm{AGL}(1,p)^{(3)} = \mathrm{AGL}(1,p)$.

We use the following notation to prove the above theorem,

$$\Gamma\mathrm{L}(1,p^f) = \mathrm{GL}(1,p^f) \rtimes \langle\tau\rangle = \langle\xi\rangle \rtimes \langle\tau\rangle \cong Z_{p^f-1} \rtimes Z_f$$

where $\langle\xi\rangle = F_{p^f}^*$ and $\tau : \xi \to \xi^p$. The main ingredient of the proof is the proof of the following proposition.

Proposition 5.4.2 *$\Gamma\mathrm{L}(1,q)$ is 2-closed in its action on F_q^*.*

5.4.1 Proof of Proposition 5.4.2

First note that when $f = 1$, $\Gamma\mathrm{L}(1,p) = Z_{p-1}$ is regular on F_p^*. By Lemma 2.4.1(3), $\Gamma\mathrm{L}(1,p)$ is 2-closed on F_p^*. Thus we may suppose that $H = \Gamma\mathrm{L}(1,p^f) = \langle\xi\rangle \rtimes \langle\tau\rangle \leq L \leq S_{p^f-1}$ where $f > 1$. To prove that H is 2-closed we need to show that if H is 2-equivalent to L then $L = H$.

We need the following technical lemma.

Lemma 5.4.3 *Suppose $\langle\xi\rangle = F_{p^f}^*$. Suppose further that $\xi^{p^i+p^t} = \xi^{p^j+p^s}$ where $i,j,s,t \in \{0,...,f-1\}$ and $i \neq j$. Then $t = j$ and $s = i$.*

Proof. Since $o(\xi) = p^f - 1$ and

$$2 \leq p^i + p^t, p^j + p^s \leq p^f,$$

we have

$$p^i + p^t = p^j + p^s.$$

Without loss of generality, we may assume that $i < j$. Then $t > s$ and $p^t - p^s = p^j - p^i$. But the highest power of p that divides $p^t - p^s$ is p^s, and the highest power of p that divides $p^j - p^i$ is p^i. Hence $s = i$ and $t = j$ as asserted. □

Recall that $H = \Gamma\mathrm{L}(1, p^f)$ acts on $F_{p^f}^*$ transitively. Consider the orbital directed graph Γ of H which has vertex set $F_{p^f}^*$, and edge set $(1, \xi)^H$ (this is actually the Cayley digraph $\mathrm{Cay}(F_{p^f}^*, \xi^{\langle\tau\rangle})$, see Definition 2.5.1 and Lemma 2.5.2). It is easy to see that the neighbourhood of the point 1 (the H_1-orbit containing ξ) is

$$\Delta = \xi^{\langle\tau\rangle} = \{\xi, \xi^p, ..., \xi^{p^{(f-1)}}\},$$

and $H_1^\Delta \cong H_1 = \langle\tau\rangle \cong Z_f$. Also, as ξ generates $F_{p^f}^*$, the digraph Γ is strongly connected. Since H is 2-equivalent to L, L is also a subgroup of the automorphism group $\mathrm{Aut}(\Gamma)$ of Γ. We obtain information about L by studying $\mathrm{Aut}(\Gamma)$.

Lemma 5.4.4 *$L_1^\Delta = H_1^\Delta$ is a regular permutation group on Δ.*

Proof. If $|\Delta| = f = 2$, then $L_1^\Delta = H_1^\Delta = S_2$ is regular.

Next suppose $f \geq 3$. If $L_1^\Delta > H_1^\Delta$, then the point stabilizer $(L_1^\Delta)_\xi$ must be nontrivial since $L_1^\Delta = H_1^\Delta (L_1^\Delta)_\xi$ and H_1^Δ is regular on Δ. Let $g \in L_{1\xi}$ such that $g^\Delta \neq 1$. (Note that since L_1 has same orbits as H_1 and g fixes 1, it follows that g fixes Δ setwise.) Hence there exists i such that $1 \leq i \leq f - 1$ and g does not fix ξ^{p^i}, say

$$g : (\xi, \xi^{p^i}) \to (\xi, \xi^{p^j}) \quad \text{for some } j \neq i \text{ with } 1 \leq j \leq f - 1.$$

Now the fact that H is 2-equivalent to L implies that there exists $1 \neq h \in H$ such that

$$h : (\xi, \xi^{p^i}) \to (\xi, \xi^{p^j}).$$

Since $H = \Gamma\mathrm{L}(1, p^f)$, we can write h as

$$h = \tau^t h_\lambda \quad \text{where } 0 \leq t \leq f - 1 \text{ and } h_\lambda \text{ acts on } F_{p^f}^* \text{ as multiplication by } \lambda.$$

Note that, since $j \neq i$ we have $h \neq 1$, and hence $(t, \lambda) \neq (0, 1)$.

Since $\xi = \xi^h = (\xi^{p^t})\lambda$, we have $\lambda = \xi^{1-p^t}$, and, in particular, $t \neq 0$. Thus $1 \leq t \leq f-1$. Applying h to ξ^{p^i}, we obtain

$$\xi^{p^j} = (\xi^{p^i})^h = (\xi^{p^{i+t}})\xi^{1-p^t}.$$

That is,

$$\xi^{1+p^{i+t}} = \xi^{p^t+p^j}, \text{ where } i, j, t \in \{1, ..., f-1\} \text{ and } i \neq j.$$

Let $i + t \equiv i' \pmod{f}$ where $0 \leq i' \leq f-1$, so that $\xi^{p^{i+t}} = \xi^{p^{i'}}$. Also, note that $\xi^1 = \xi^{p^s}$ with $s = 0$, and $t \neq 0$. It follows from Lemma 5.4.3 that $j = s = 0$. But this contradicts the fact that $j \geq 1$. Therefore $L_1^\Delta = H_1^\Delta$. $\square$

Next we will show that the action of L_1 on Δ is faithful.

Lemma 5.4.5 $L_1 \cong L_1^\Delta$.

Proof. Since the directed graph Γ is strongly connected, to show that the action of L_1 on Δ is faithful, we only need to show that if $g \in L_1$ fixes $\Delta = \{\xi, \xi^p, ..., \xi^{p^{f-1}}\}$ pointwise, (that is, $g \in (L_1)_\Delta$), then g fixes pointwise the neighbourhoods of each of the points $\{\xi, \xi^p, ..., \xi^{p^{f-1}}\}$. Note that for any $h \in L$, $h^{-1}(L_1)_\Delta h = (L_{1^h})_{\Delta^h}$, then since Γ is connected and L is vertex-transitive, g fixes all the points of Γ.

Denote by $\Delta_{\xi^{p^i}}$ the neighbourhood of the point ξ^{p^i}. Then

$$\Delta_\xi = \xi\Delta = \{\xi^2, \xi^{1+p}, ..., \xi^{1+p^{(f-1)}}\}$$

$$\Delta_{\xi^p} = \xi^p\Delta = \{\xi^{p+1}, \xi^{2p}, ..., \xi^{p+p^{f-1}}\}$$

$$\vdots$$

$$\Delta_{\xi^{p^{f-1}}} = \xi^{p^{f-1}}\Delta = \{\xi^{p^{f-1}+1}, \xi^{p^{f-1}+p}, ..., \xi^{p^{f-1}+p^{f-1}}\}.$$

First we claim that $\Delta_{\xi^{p^i}} \cap \Delta_{\xi^{p^j}} = \{\xi^{p^i+p^j}\}$ where $0 \leq i \neq j \leq f-1$. This is true because if $y \in \Delta_{\xi^{p^i}} \cap \Delta_{\xi^{p^j}}$, then $y = \xi^{p^i+p^t} = \xi^{p^j+p^s}$ for some $0 \leq t, s \leq f-1$. By Lemma 5.4.3, we have $s = i$ and $t = j$, and $y = \xi^{p^i+p^j}$.

Now, since g fixes $\Delta = \{\xi, \xi^p, ..., \xi^{p^{f-1}}\}$ pointwise, g fixes $\Delta_\xi \cap \Delta_{\xi^{p^i}} = \{\xi^{1+p^i}\}$ for every i such that $1 \leq i \leq f-1$. Then g fixes $f-1$ points in Δ_ξ and hence also fixes the f^{th} point in Δ_ξ. In the same way, we can prove g fixes pointwise the neighbourhoods of each of the points $\{\xi, \xi^p, ..., \xi^{p^{f-1}}\}$ as required. $\square$

Now by Lemmas 5.4.4 and 5.4.5, $L_1 \cong L_1^\Delta \cong Z_f$. Thus $L = \mathrm{GL}(1, p^f)L_1 = H$, proving Proposition 5.4.2.

5.4.2 Proof of Theorem 5.4.1.

Proof of Theorem 5.4.1: (1) Let $H \leq \Gamma\mathrm{L}(1, q)$. By Lemma 2.4.1(2) and Proposition 5.4.2,

$$H^{(2)} \leq \Gamma\mathrm{L}(1, q)^{(2)} = \Gamma\mathrm{L}(1, q).$$

Set $K = H^{(2)}$. Then $H \leq K \leq \Gamma\mathrm{L}(1, q)$ and H is 2-equivalent to K. Note that the point stabilizer $\Gamma\mathrm{L}(1, q)_1 = \langle \tau \rangle$. By Lemma 2.4.1(4), the point stabilizers $H_1 \leq K_1 \leq \langle \tau \rangle$, and H_1 is 1-equivalent to K_1. Thus $\xi^{H_1} = \xi^{K_1}$. This implies that $H_1 = K_1$. Now note that

$$|H : H_1| = |1^H| = |1^K| = |K : K_1|.$$

Hence $K = H$ and H is 2-closed.

(2) First, let $G = \mathrm{AGL}(1, p)$. Then G is 2-transitive, and therefore $G^{(2)} = S_p$. Also taking $\alpha_1 = 0$ and $\alpha_2 = 1$ we have $G_{\alpha_1, \alpha_2} = 1$ and so by Lemma 2.4.1(3), $G^{(3)} = G$.

Next we assume $G < \mathrm{AGL}(1, p)$. Since G is not 2-transitive, neither is $G^{(2)}$. Now by Theorem 2.3.10 (Burnside's Theorem), $G^{(2)}$ is a subgroup of $\mathrm{AGL}(1, p)$, that is, $G = Z_p \rtimes H \leq G^{(2)} = Z_p \rtimes K$ where $H \leq K \leq Z_{p-1}$. By Lemma 2.4.1(4), H is 1-equivalent to K, so we have $1^H = 1^K$. Hence $H = K$, and $G = G^{(2)}$.

This completes the proof. □

Chapter 6

Closures of Semilinear Groups

One of our main results is Theorem 6.0.6 dealing with the 2-closures of semilinear subgroups which do not contain $\mathrm{SL}(d,q)$. We follow Aschbacher's description (see Chapter 4 for definitions) of various types of maximal subgroups of $\Gamma\mathrm{L}(d,q)$ to organize our analysis and present our results. In this chapter, we prove Theorem 6.0.6 by elementary methods, that is, by methods which are independent of the Classification of Finite Simple Groups.

Theorem 6.0.6 *Suppose H is a subgroup of $\Gamma\mathrm{L}(d,q)$ where $d \geq 2$ and $q = p^f$ is a power of a prime p. Suppose further that H does not contain $\mathrm{SL}(d,q)$ and $H \in C_i$ for some $i = 1, 2, ..., 8, 9$. Then in its action on $V(d,q) \setminus \{0\}$ either*

(a) *$d = 4, q = 2$ and $H = A_7$ is 2-transitive, or*

(b) *$H^{(2)} \cap \Gamma\mathrm{L}(d,q) \in C_i$.*

Remark: We prove a little more in this chapter, namely, under the conditions of Theorem 6.0.6, if $H \in C_i$ for $i = 1, 2, 4, 5, 7$, then $H^{(1)} \cap \Gamma\mathrm{L}(d,q) \in C_i$. Moreover, when $H \in C_8$, we have $H^{(1)} \cap \Gamma\mathrm{L}(d,q) \in C_8$ if $H \leq \Gamma\mathrm{U}(d,q^{1/2})$, $H \leq \Gamma\mathrm{O}^+(d,q)$ with $d \geq 2$, $H \leq \Gamma\mathrm{O}^-(d,q)$ with $d \geq 4$, or $H \leq \Gamma\mathrm{O}^\circ(d,q)$ with $d \geq 3$. Hence in these cases, we can answer Question 1.2.1 even for $k = 2$. But this stronger result fails when H is a maximal C_3-subgroup or $H = \Gamma\mathrm{Sp}(d,q)(d \geq 2)$ as such a subgroup is transitive on $V \setminus \{0\}$. Hence Question 1.2.1 posed by Praeger and Saxl is still open for $k = 2$.

6.1 Notations and outline

Throughout this chapter, we use the notation fixed here. Let $V = V(d,q)$ be a vector space of dimension d over a finite field F_q with $d \geq 2$ and $q = p^f$, and let $\Omega = V \setminus \{0\}$. Let τ be the Frobenius automorphism defined with respect to a basis $\{v_1, ..., v_d\}$ of V as in Section 3.2. Suppose $H \leq \Gamma\mathrm{L}(d,q) = \mathrm{GL}(d,q) \rtimes \langle\tau\rangle$ and $H \not\geq \mathrm{SL}(d,q)$. Then H acts on Ω faithfully. Set

$$K = H^{(2)} \cap \Gamma\mathrm{L}(d,q)$$

and

$$X = H^{(1)} \cap \Gamma\mathrm{L}(d,q).$$

By Lemma 2.4.1(1), $H \leq H^{(2)} \leq H^{(1)}$ and hence

$$H \leq K \leq X \leq \Gamma\mathrm{L}(d,q).$$

Also, K is 2-equivalent to H and X is 1-equivalent to H. In order to show that $K \in C_i$, it is sufficient to prove that $X \in C_i$. We will prove this for $i = 1, 2, 4, 5, 7$, and when H belongs to some subclasses of C_8, using geometric methods.

Recall that Z denotes the subgroup of scalar matrices in $\mathrm{GL}(d,q)$. Set $\overline{H} = HZ/Z$, $\overline{K} = KZ/Z$ and $\overline{X} = XZ/Z$. Then

$$\overline{H} \leq \overline{K} \leq \overline{X} \leq \mathrm{P}\Gamma\mathrm{L}(d,q),$$

and $\overline{H}$, $\overline{K}$ and $\overline{X}$ act faithfully on $\overline{\Omega}$ where $\overline{\Omega}$ is the set of 1-dimensional subspaces of V. The next result follows immediately from Lemmas 2.4.5 and 2.4.6.

Lemma 6.1.1 *With the notation as above, $\overline{H}$ is 1-equivalent to $\overline{X}$ on $\overline{\Omega}$ and $\overline{H}$ is 2-equivalent to $\overline{K}$ on $\overline{\Omega}$.*

Next, suppose $H \in C_i$ for some i. The lemma below contains another useful observation. This lemma is actually an immediate corollary of Lemma 2.4.1(2).

Lemma 6.1.2 *Let $H \leq M \leq \Gamma\mathrm{L}(d,q)$. Suppose that for a positive integer k, $M^{(k)} \cap \Gamma\mathrm{L}(d,q) = M$. Then $H^{(k)} \cap \Gamma\mathrm{L}(d,q) \leq M$.*

Now we take M to be a maximal C_i-subgroup containing H. If we can show that $M^{(k)} \cap \Gamma\mathrm{L}(d,q) = M$ for $k = 1$ or 2, then Lemma 6.1.2 implies that $H^{(k)} \cap \Gamma\mathrm{L}(d,q) \leq M$, and hence that $X \in C_i$ when $k = 1$ or $K \in C_i$ when $k = 2$.

Thus to show that $X \in C_i$ or $K \in C_i$ when $H \in C_i$, it is sufficient to prove that, if H is a maximal C_i-subgroup, then $X = H$ or $K = H$ respectively.

We summarize these observations in a lemma.

Lemma 6.1.3 *Let H, K, X be as above and suppose that $H \in C_i$. Let M be a maximal C_i-subgroup containing H. Then any one of the following conditions implies that $K \in C_i$.*

(a) $X \in C_i$.

(b) $M^{(1)} \cap \Gamma\mathrm{L}(d, q) = M$.

(c) $M^{(2)} \cap \Gamma\mathrm{L}(d, q) = M$.

6.2 Proof of Theorem 6.0.6 when $d = 2$

In this section, we use Lemma 5.1.2 and Proposition 5.2.1 to prove Theorem 6.0.6 when $d = 2$.

Proposition 6.2.1 *Suppose $H \leq \Gamma\mathrm{L}(2, q)$ and H does not contain* $\mathrm{SL}(2, q)$. *If $H \in C_i$ for some $i = 1, ..., 9$, then $K = H^{(2)} \cap \Gamma\mathrm{L}(2, q) \in C_i$.*

Proof. If $q = p$ is a prime then $H \leq \mathrm{GL}(2, p)$ and hence by Proposition 5.2.1, $K = H$. Therefore we may assume that q is not a prime.

First we suppose that $1 \leq i \leq 8$. In view of Lemma 6.1.3 (c), it is sufficient to assume that H is a maximal C_i-subgroup. Now Lemma 5.1.2 implies that, replacing H by a conjugate if necessary, either H contains the Frobenius automorphism τ or $H = \Gamma\mathrm{L}(1, q^2)$. In the first case, since $\tau \in H$, Proposition 5.2.1 implies that $K = H$. In the second case, Theorem 5.4.1 (1) implies that H is 2-closed and in particular, $K = H$.

This leaves the case $H \in C_9$. Note that by the definition of the class C_9, $K \in C_9$ or $K \geq \mathrm{SL}(2, q)$. We argue by contradiction. Assume that $K \geq \mathrm{SL}(2, q)$. By Lemma 6.1.1, $\overline{H} = HZ/Z$ is 2-equivalent to $\overline{K} = KZ/Z$ on $\overline{\Omega}$ where $\overline{\Omega}$ is the set of 1-subspaces of V. Since $K \geq \mathrm{SL}(2, q)$, $\overline{K} \geq \mathrm{PSL}(2, q)$ is 2-transitive on $\overline{\Omega}$ (Theorem 3.3.2). Thus $\overline{H}$ is 2-transitive on $\overline{\Omega}$. Since $H \in C_9$, Dickson's theorem implies that

$$\mathrm{SL}(2, 5) \trianglelefteq H \quad \text{where } q > 5 \text{ and } q^2 - 1 \equiv 0 \pmod 5.$$

Thus $\overline{H}$ is almost simple with socle A_5, that is, $A_5 \trianglelefteq \overline{H} \leq S_5$. Since $\overline{H}$ is 2-transitive on $\overline{\Omega}$, $(q + 1)q | 120$. But $q > 5$, so no such q exists. Therefore, $K \in C_9$. The proof is now complete. □

Remark: As explained before, our goal is to try to prove $X = H^{(1)} \cap \Gamma\mathrm{L}(d, q) \in C_i$, (hence to solve Question 1.2.1 for $k = 2$), not just $K \in C_i$. So in the following sections we still have to handle the $d = 2$ case if we can actually prove $X \in C_i$.

6.3 The case $H \in C_1$

Suppose $H \in C_1$ (see Section 4.1 for the definition), then $H \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(W)$ where W is a nontrivial proper subspace of V. We will show that $X \in C_1$. Then by Lemma 6.1.3 (a), $K \in C_1$.

Proposition 6.3.1 *Suppose $d \geq 2$ and H is a subgroup of* $\mathrm{Stab}_{\Gamma\mathrm{L}}(W)$ *as above. Then so is $X = H^{(1)} \cap \Gamma\mathrm{L}(d,q)$.*

Proof. By definition of $\mathrm{Stab}_{\Gamma\mathrm{L}}(W)$, $W \setminus \{0\}$ is an H-invariant 1-relation in Ω and hence also an X-invariant 1-relation. This implies that X preserves the subspace W. Therefore $X \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(W)$. □

6.4 The case $H \in C_2$

Suppose $H \in C_2$. Then $V = V_1 \oplus \cdots \oplus V_t$ where $\mathrm{dim}V_1 = \cdots = \mathrm{dim}V_t = a$ and $d = at$ for some $t > 1$ and $H \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(\oplus V_i)$ (see Section 4.2). We will show that $X \in C_2$, and hence by Lemma 6.1.3 (a), $K \in C_2$.

Proposition 6.4.1 *Suppose $d \geq 2$ and H is a subgroup of* $\mathrm{Stab}_{\Gamma\mathrm{L}}(\oplus V_i)$ *with the V_i as above. Then so is $X = H^{(1)} \cap \Gamma\mathrm{L}(d,q)$.*

Proof. Let $\Delta = (V_1 \cup ... \cup V_t) \setminus \{0\}$. Then Δ is an H-invariant 1-relation in Ω and hence also an X-invariant 1-relation.

For any $v \in V_i \setminus \{0\}$ and for any $g \in X$, we have $v \in \Delta$ and hence $v^g \in \Delta$, so that $v^g \in V_j$ for some j. We claim that $V_i^g = V_j$.

Let $w \in V_i \setminus \{0, v\}$. Then $v - w \in V_i \setminus \{0\}$ and so $w^g \in V_m \setminus \{0\}$ and $(v-w)^g \in V_l \setminus \{0\}$ for some m, l. Thus

$$(v-w)^g = v^g - w^g \in (V_j + V_m) \cap V_l$$

and is nonzero. Because the subspace decomposition is a direct sum, we must have $j = m = l$. Thus $w^g \in V_j$ and since this holds for all $w \in V_i$, g maps V_i to V_j. It follows that each g in X preserves the above subspace decomposition of V, and hence $X \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(\oplus V_i)$. □

6.5 The case $H \in C_3$ with $d \geq 3$.

Suppose $H \in C_3$. Then $H \leq \Gamma\mathrm{L}(a, q^b)$ where $d = ab$ and $b > 1$ (see Section 4.3). In this section, we will prove Proposition 6.5.1 which only concerns 2-closures of H. Since

$\Gamma\mathrm{L}(a, q^b)$ is transitive on Ω, $\Gamma\mathrm{L}(a, q^b)^{(1)} = \mathrm{Sym}(\Omega)$. Hence the following result is not true if we replace K by X.

Proposition 6.5.1 *Suppose $H \leq \Gamma\mathrm{L}(a, q^b)$ where $d = ab$ and $b > 1$. Then $K \leq \Gamma\mathrm{L}(a, q^b)$.*

The proof uses the following corollary that follows directly from Proposition 3.2.3.

Corollary 6.5.2 *With the above notation, assume that $a \geq 2$, and let $g \in \Gamma\mathrm{L}(d, q)$. Then $g \in \Gamma\mathrm{L}(a, q^b)$ if and only if g preserves the partition $\{\langle v\rangle_{F_{q^b}} \setminus \{0\} \,|\, v \in \Omega\}$, that is, g permutes the 1-dimensional subspaces in $V(a, q^b)$.*

Proof. Let $F = F_{q^b}$ be an extension field of the field F_q. By Proposition 3.2.3, for $V = V(a, F)$ with $a \geq 2$, a function $f : V \to V$ is a semilinear transformation of $V(a, F)$ if and only if it has the following two properties:

1. f is an automorphism of the additive group of $V(a, F)$.
2. f sends one-dimensional subspaces of $V(a, F)$ onto one-dimensional subspaces.

Now let $g \in \Gamma\mathrm{L}(d, q)$. Then condition 1 holds. Thus $g \in \Gamma\mathrm{L}(a, F)$ if and only if condition 2 holds. We have the required result. □

Proof of Proposition 6.5.1: Let $F = F_{q^b}$ be an extension field of the field F_q. Suppose first that $a \geq 2$, and let $\Delta = \{(\lambda v, v) |\ v \in \Omega,\ \lambda \in F = F_{q^b}\}$. This is an H-invariant 2-relation, and hence also a K-invariant 2-relation. Let $g \in K$. Then for $v \in V(a, F)$ and $\lambda \in F$, $(\lambda v, v) \in \Delta$ and hence $(\lambda v, v)^g \in \Delta$. Thus

$$(\lambda v, v)^g = (\mu w, w) \text{ for some } \mu \in F \text{ and } w \in \Omega.$$

This implies that $(\lambda v)^g = \mu w = \mu v^g$. Letting λ vary over F we conclude that $\langle v\rangle_F^g = \langle w\rangle_F$. Therefore K preserves the set of 1-dimensional subspaces in $V(a, F)$. Hence by Corollary 6.5.2, $K \leq \Gamma\mathrm{L}(a, F)$.

Finally we consider the case $a = 1$. By Theorem 5.4.1 (1), $H^{(2)} = H$. Thus $K = H^{(2)} \cap \Gamma\mathrm{L}(d, q) = H \leq \Gamma\mathrm{L}(1, q^d)$.

The proof of Proposition 6.5.1 is now complete. □

6.6 The cases $H \in C_4$ and $H \in C_7$

These two cases are tensor product subgroups of the general semilinear group, (see Section 3.1 for the basic definitions and notation of tensor product spaces).

First suppose that $H \in C_4$. Then $V = U \otimes W$ where $\dim U \neq \dim W$, with $\dim U \geq 2, \dim W \geq 2$, and $H \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$. Recall from Section 4.4 that we define τ with respect to a tensor product basis constructed from bases of U and W, and $v \in V$ is called *simple* if there exist $u \in U$ and $w \in W$ such that $v = u \otimes w$. We also denote by τ the Frobenius automorphisms in $\Gamma\mathrm{L}(U)$ and $\Gamma\mathrm{L}(W)$ with respect to bases of U and W corresponding to the tensor product basis of V. Then we have $v^\tau = u^\tau \otimes w^\tau$. Thus τ maps simple elements to simple elements, and

$$\mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W) = (\mathrm{GL}(U) \otimes \mathrm{GL}(W)) \rtimes \langle\tau\rangle.$$

Secondly, suppose that $H \in C_7$. Then $V = W_1 \otimes \cdots \otimes W_t$ is the tensor product of $t \geq 2$ copies $W_1, ..., W_t$ of a vector space W of dimension $c \geq 2$, where $d = \mathrm{dim}V = c^t$, and $H \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$. Pick a typical tensor product basis of V, and define the action of τ on V with respect to this basis (see Section 4.7). Similarly, we also have that τ maps simple elements to simple elements, and

$$\mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i) = (\mathrm{GL}(W) \wr_{\otimes} S_t) \rtimes \langle\tau\rangle.$$

Using the technical lemmas in Section 3.1, we prove:

Theorem 6.6.1 *With the above notation, let* $g \in \Gamma\mathrm{L}(V) = \mathrm{GL}(V) \rtimes \langle\tau\rangle$.

1. *Suppose* $V = U \otimes W$, *with* $\mathrm{dim}U \geq 2$, $\mathrm{dim}W \geq 2$, $\mathrm{dim}U \neq \mathrm{dim}W$, *and bases of* U, W *chosen so that* $\tau \in \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$. *If* g *leaves invariant the set of simple vectors, then* $g \in \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$.

2. *Suppose* $V = W_1 \otimes \cdots \otimes W_t$ *is the tensor product of* $t \geq 2$ *copies* $W_1, ..., W_t$ *of a vector space* W, *with bases of the* W_i *chosen so that* $\tau \in \mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$. *If* g *leaves invariant the set of simple vectors, then* $g \in \mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$.

Proof. (1) By assumption, $\tau \in \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$ and maps simple elements to simple elements. Thus replacing g by $g\tau^i$ for some i, we may assume that $g \in \mathrm{GL}(V)$.

Let $e_1 \in U, e_2 \in W$ be any nonzero elements of U and W respectively. Replacing g by gh_1 for an appropriate $h_1 \in \mathrm{GL}(U) \otimes \mathrm{GL}(W)$ we may assume further that $(e_1 \otimes e_2)^g = e_1 \otimes e_2$. Since $\dim U \neq \dim W$ and $g \in \mathrm{GL}(V)$, Lemma 3.1.5 implies that $(e_1 \otimes W)^g = e_1 \otimes W$ and $(U \otimes e_2)^g = U \otimes e_2$. Thus g induces linear transformations on $e_1 \otimes W$ and $U \otimes e_2$, so replacing g by gh_2 for an appropriate $h_2 \in \mathrm{GL}(U) \otimes \mathrm{GL}(W)$, we may assume in addition that g fixes $e_1 \otimes w$ and $u \otimes e_2$ for all $u \in U, w \in W$. Then by Lemma 3.1.6, $g = 1$. Thus we deduce that our original element g was in $\mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$.

(2) Again by assumption, $\tau \in \mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$ where each $W_i = W$, and τ maps simple elements to simple elements. Thus we can replace g by $g\tau^i$ for some i and assume $g \in \mathrm{GL}(V)$.

Let $e_1, ..., e_t$ be any nonzero elements of W. Replacing g by gh_1 for an appropriate $h_1 \in \mathrm{GL}(W) \otimes \cdots \otimes \mathrm{GL}(W)$ we may assume that $(e_1 \otimes \cdots \otimes e_t)^g = e_1 \otimes \cdots \otimes e_t$. By Lemma 3.1.5, we then have that, for any $i = 1, ..., t$, there exists a j_i, such that $1 \le j_i \le t$ and $(e_1 \otimes \cdots \otimes e_{i-1} \otimes W_i \otimes e_{i+1} \otimes \cdots \otimes e_t)^g \subseteq e_1 \otimes \cdots \otimes W_{j_i} \otimes \cdots \otimes e_t$. Since $g : V \to V$ is bijective, the map $i \to j_i$ defines an element of S_t.

Thus we can further replace the above g by gh_2 for an appropriate $h_2 \in \mathrm{GL}(W) \wr_{\otimes} S_t$, and assume that $j_i = i$ for each i, and that g fixes $e_1 \otimes \cdots \otimes e_{i-1} \otimes w \otimes e_{i+1} \otimes \cdots \otimes e_t$ for every $w \in W_i$ and every i with $1 \le i \le t$. Then an application of Lemma 3.1.6 concludes the proof. □

Returning to the proof of Theorem 6.0.6, assume $H \in C_4$ or C_7. We will show that $X \in C_4$ or C_7 (Proposition 6.6.2), hence $K \in C_4$ or C_7 respectively as required.

Proposition 6.6.2 *With the notation as above, suppose that $H \le \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$ or $H \le \mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$, then $X \le \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$ or $X \le \mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$ respectively.*

Proof. Recall that $V = V(d, q)$ is a d-dimensional vector space over a finite field F_q. For the Case C_4 where $H \le \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$, the space V has a tensor decomposition $V = U \otimes W$ where $\dim U = b \ge 2$ and $\dim W = c \ge 2$ with $d = bc, b \ne c$. For the Case C_7 where $H \le \mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$, the space V has a tensor decomposition $V = \otimes_{i=1}^t W_i$ where each $\dim W_i = c \ge 2$ and $d = c^t$. Thus in each case H preserves the set of simple elements of the corresponding tensor product vector space V. Since H is 1-equivalent to X, X also takes simple elements of V to simple elements. Thus by Theorem 6.6.1, $X \le \mathrm{Stab}_{\Gamma\mathrm{L}}(U \otimes W)$ or $\mathrm{Stab}_{\Gamma\mathrm{L}}(\otimes W_i)$ respectively. □

6.7 The case $H \in C_5$

Suppose that $H \in C_5$. Then H is a subgroup of a maximal C_5-subgroup with respect to a divisor a of f. Recall that Z denotes the subgroup of scalar matrices in $\mathrm{GL}(d, q)$ and the action of τ on V is defined with respect to the F_q-basis $\{v_1, ..., v_d\}$ of V. Let a be a proper divisor of f, set $q_0 = p^a$, and let F_{q_0} denote the proper subfield of F_q of order q_0. Let

$$V_0 = \mathrm{Span}_{F_{q_0}} \langle v_1, ..., v_d \rangle.$$

By Section 4.5, $H \le \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$ where

$$\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0) = (\mathrm{GL}(d, q_0) \circ Z) \rtimes \langle \tau \rangle.$$

We will show that $X \le \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$ and hence $K \le X \le \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$.

Recall that $\overline{H} = HZ/Z$, $\overline{X} = XZ/Z$ and $\overline{\tau} = \tau Z$. By Lemma 6.1.1, $\overline{H}$ is 1-equivalent to $\overline{X}$ on $\overline{\Omega}$, where $\overline{\Omega}$ is the set of all 1-subspaces of V.

For $d \geq 3$, regard $\overline{\Omega}$ as the set of points of the projective geometry $\mathrm{PG}(d-1, q)$. The Fundamental Theorem of Projective Geometry (see Theorem 3.3.1) tells us: if f is a permutation of the points of $\mathrm{PG}(d-1, q)$ with $d \geq 3$ that takes collinear points to collinear points, then $f \in \mathrm{P\Gamma L}(d, q)$. Recall from Section 3.3 that a set of points in $\mathrm{PG}(d-1, q)$ is said to be collinear if it is contained in a line (a 2-subspace of V).

Proposition 6.7.1 *Suppose $d \geq 2$ and H is a subgroup of* $\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$*. Then so is $X = H^{(1)} \cap \Gamma\mathrm{L}(d, q)$, and hence $K = H^{(2)} \cap \Gamma\mathrm{L}(d, q)$ is a subgroup of* $\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$.

Proof. Note that

$$\overline{\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)} = \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)/Z = \mathrm{PGL}(d, q_0).\langle \overline{\tau} \rangle.$$

To show that $X \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$, it is sufficient to show that $\overline{X} \leq \mathrm{PGL}(d, q_0).\langle \overline{\tau} \rangle$ since $\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$ contains Z.

Let

$$\overline{\Omega}_0 = \{\langle v \rangle_{F_q} \mid v \in V_0\} \subset \overline{\Omega}.$$

Then $\overline{H}$ fixes $\overline{\Omega}_0$ setwise. By Lemma 6.1.1, $\overline{X} \leq \overline{H}^{(1)}$, so $\overline{X}$ fixes $\overline{\Omega}_0$ setwise too.

First we suppose that $d \geq 3$. We can view $\overline{\Omega}_0$ as the set of points of the projective geometry $\mathrm{PG}(d-1, q_0)$, and collinear points of $\mathrm{PG}(d-1, q_0)$ are also collinear in the geometry of $\mathrm{PG}(d-1, q)$.

For any $\bar{g} \in \overline{X} \leq \mathrm{P\Gamma L}(d, q)$, the map $\bar{g} : \overline{\Omega}_0 \to \overline{\Omega}_0$ is a bijection that takes collinear points to collinear points. By the Fundamental Theorem of Projective Geometry, $\bar{g}|_{\overline{\Omega}_0} \in \mathrm{P\Gamma L}(d, q_0)$, say $\bar{g}|_{\overline{\Omega}_0} = \bar{h}$. As explained in Section 4.5, from the definition of $\mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$, there exists $h \in \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$ such that $hZ = \bar{h}$. Hence $(gh^{-1})Z = \bar{g}\bar{h}^{-1}$ fixes each element of $\overline{\Omega}_0$, and so gh^{-1} fixes setwise each 1-subspace in $\overline{\Omega}_0$. Thus $gh^{-1} \in Z.\langle \tau^a \rangle \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$, and since $h \in \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$, $g \in \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$ as well.

Next we suppose $d = 2$. By Lemma 6.1.3 (b), it is sufficient to show that $X = H$ in the case where $H = \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$. That is, it is sufficient to show that $\overline{X} = \overline{H} = \mathrm{PGL}(2, q_0).\langle \overline{\tau} \rangle$ when $H = \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$. Consider the natural action of $\overline{X} \geq \overline{H} = \mathrm{PGL}(2, q_0).\langle \overline{\tau} \rangle$ on $\overline{\Omega}_0$. Since $\{v_1, v_2\}$ is a basis of both $V(2, q)$ and $V(2, q_0)$ and $\overline{\tau}^a$ fixes $\overline{\Omega}_0$ pointwise where $q_0 = p^a$, the kernel of the action of $\overline{X}$ on $\overline{\Omega}_0$ is $\langle \overline{\tau}^a \rangle$.

Suppose $q_0 = 2$. Then $\overline{H} = S_3.\langle \overline{\tau} \rangle \leq \overline{X}$, and $\overline{X}$ acts on $\overline{\Omega}_0$ with the kernel $\langle \overline{\tau} \rangle$. Thus $|\overline{\Omega}_0| = 3$ implies that $|\overline{X}| = |\overline{H}|$, hence $X = H$. Suppose $q_0 = 3$. Then $\overline{H} = S_4.\langle \overline{\tau} \rangle$ and $|\overline{\Omega}_0| = 4$. The same argument shows that $X = H$. Finally, suppose $q_0 > 3$. By Dickson's

Theorem, $\overline{H} \leq \overline{X} \leq \mathrm{P\Gamma L}(2,q)$ implies that $\overline{X} = \mathrm{PGL}(2,q_1).\langle\bar{\tau}\rangle$ or $\mathrm{PSL}(2,q_1).\langle\bar{\tau}\rangle$ where $q_0|q_1$ and $q_1|q$. Now the fact that $\overline{X}$ fixes $\overline{\Omega}_0$ implies that $\overline{X} = \overline{H}$, and hence $X = H$.

Since $H \leq K \leq X$, we also have $K \leq \mathrm{Stab}_{\Gamma\mathrm{L}}(F_q V_0)$, and so the proof is complete. □

6.8 The case $H \in C_8$

Suppose $H \in C_8$. Then H is a subgroup of $\Gamma\mathrm{O}(V), \Gamma\mathrm{Sp}(V)$ or $\Gamma\mathrm{U}(V)$, (for detailed descriptions see Section 3.4). Also the classical groups $\Gamma\mathrm{O}(V), \Gamma\mathrm{Sp}(V)$ and $\Gamma\mathrm{U}(V)$ are the maximal C_8-subgroups. Theorem 6.0.6 for the C_8-subgroups follows from the following proposition.

Proposition 6.8.1 *Let M be a maximal C_8-subgroup of $\Gamma\mathrm{L}(V)$ acting on $\Omega = V \setminus \{0\}$, and suppose that $H \leq M$. Then $K = H^{(2)} \cap \Gamma\mathrm{L}(V) \leq M$. Moreover, either*

(a) $X = H^{(1)} \cap \Gamma\mathrm{L}(V) \leq M$, or

(b) $M = \Gamma\mathrm{Sp}(V)$, or $d = 2$ and $M = \Gamma\mathrm{O}^-(V)$, and in these cases, $M^{(1)} = \mathrm{Sym}(\Omega)$.

This proposition will be proved in the following subsections for the different types of classical groups separately, namely it follows from Lemmas 6.8.2, 6.8.3, and 6.8.4.

6.8.1 The symplectic groups

Suppose $V = (V, \mathbf{f})$ where $\mathbf{f}$ is a symplectic form. Then by Proposition 3.4.3, the dimension $d = 2m$ is even, and V has a symplectic basis. The following Lemma is a corollary of Lemma 3.4.4.

Lemma 6.8.2 *Proposition 6.8.1 holds if $M = \Gamma\mathrm{Sp}(V)$ with $d \geq 2$.*

Proof. By assumption, $H \leq \Gamma\mathrm{Sp}(V)$. Let $\Delta = \{(u,v) \in \Omega \times \Omega |\ \mathbf{f}(u,v) = 0\} \subseteq \Omega \times \Omega$. Then Δ is an H-invariant 2-relation and hence also a K-invariant 2-relation. By Lemma 3.4.4, $K \leq \Gamma\mathrm{Sp}(V)$.

Finally, since $\mathrm{Sp}(V)$ is transitive on Ω, $\mathrm{Sp}(V)^{(1)} = \mathrm{Sym}(\Omega)$. Hence $\Gamma\mathrm{Sp}(V)^{(1)} = \mathrm{Sym}(\Omega)$. □

6.8.2 The orthogonal groups

Suppose $V = (V, \mathbf{Q})$ where $\mathbf{Q}$ is a non-degenerate quadratic form. Recall from Section 3.4.2 that there are three cases for the group $\Gamma\mathrm{O}(V)$. In detail, the odd dimensional orthogonal groups $\Gamma\mathrm{O}^\circ(V)$ are uniquely determined up to conjugacy in $\Gamma\mathrm{L}(d,q)$, while there are two conjugacy classes of even dimensional orthogonal groups, denoted by $\Gamma\mathrm{O}^{\pm}(V)$ respectively. Let

$$\Theta = \{v \in V |\ \mathbf{Q}(v) = 0\}.$$

Then $\Theta \setminus \{0\}$ is a non-empty subset of Ω if and only if $d \geq 3$ or $d = 2$ and $\Gamma\mathrm{O}(V) = \Gamma\mathrm{O}^{+}(2, q)$.

Lemma 6.8.3 *Proposition 6.8.1 holds if $M = \Gamma\mathrm{O}(V)$ with $d \geq 2$.*

Proof. If $H \leq \Gamma\mathrm{O}^{-}(2, q)$ with $d = 2$, then Proposition 6.2.1 shows that $K \leq \Gamma\mathrm{O}^{-}(2, q)$, but since $\Gamma\mathrm{O}^{-}(2, q)$ is transitive on Ω, we have $\Gamma\mathrm{O}^{-}(2, q)^{(1)} = \mathrm{Sym}(\Omega)$. In all other cases, the subset $\Theta \setminus \{0\}$ is non-empty and is an H-invariant 1-relation. Thus Θ is also X-invariant, and so the fact that $X \leq \Gamma\mathrm{O}(V)$ follows from Theorem 3.4.1. Finally in these cases we also have $K \leq X \leq \Gamma\mathrm{O}(V)$ by Lemma 6.1.3 (a). □

6.8.3 The unitary groups

Suppose $V = (V, \mathbf{f})$ where $\mathbf{f}$ is a unitary form and $d = \dim V \geq 2$. Let

$$\Phi = \{v \in V |\ \mathbf{f}(v, v) = 0\}.$$

Since $d \geq 2$, $\Phi \setminus \{0\}$ is non-empty.

Lemma 6.8.4 *Proposition 6.8.1 holds if $M = \Gamma\mathrm{U}(V)$ with $d \geq 2$.*

Proof. Since $\Phi \setminus \{0\}$ is an H-invariant 1-relation, $\Phi \setminus \{0\}$ is also X-invariant. Then the fact that $X \leq \Gamma\mathrm{U}(V)$ follows from Corollary 3.4.7. Also we have $K \leq X \leq \Gamma\mathrm{U}(V)$. □

6.9 The case $H \in C_6$ for $d \geq 3$.

In this section we will prove that if $H \in C_6$ then $K \in C_6$. By Proposition 6.2.1, we know that this is true when $d = 2$. Thus we can suppose $d \geq 3$ in the following discussion. In view of Lemma 6.1.3 (c), we may also assume that H is a maximal C_6-subgroup. Recall from Section 4.6 that the maximal C_6-subgroups are the normalizers in $\Gamma\mathrm{L}(d, q)$ of certain absolutely irreducible symplectic type r-groups R for a prime $r \neq p$. Our aim in this section is to prove the following proposition. Theorem 6.0.6 for C_6-groups follows from this.

Proposition 6.9.1 *Suppose $d \geq 3$ and suppose H is a maximal C_6-subgroup, that is, $H = N_{\Gamma\mathrm{L}(d,q)}(R)$ where R is an r-group of symplectic type of exponent $r(2, r)$. Then $K = H$.*

6.9.1 The reduction

Suppose H is a maximal C_6-subgroup. Then $H = N_{\Gamma L(d,q)}(R)$ where R is an r-group of symplectic type of exponent $r(2,r)$. Let e be the smallest integer for which $p^e \equiv 1 \pmod{|Z(R)|}$, then R can be realized over the subfield F_{p^e}, and so if $p^e \neq q$ then H is also a C_5-subgroup (see Section 4.6.2). In order to state and prove the following lemma, we explain the notation again. Recall that $\{v_1, ..., v_d\}$ is the F_q-basis for V with respect to which τ was defined. Define the F_{p^e}-subspace

$$U = \mathrm{Span}_{F_{p^e}}\langle v_1, ..., v_d\rangle = U(d, p^e). \tag{6.1}$$

As explained in Section 4.6.2, we may assume that $R \leq \mathrm{GL}(U) = \mathrm{GL}(d, p^e)$ and R is absolutely irreducible on U. Therefore,

$$H = N_{\Gamma L(d,q)}(R) = (N_{\mathrm{GL}(d,p^e)}(R) \circ Z).\langle\tau\rangle. \tag{6.2}$$

Lemma 6.9.2 *With the above notation, suppose $H = N_{\Gamma L(d,q)}(R) = (N_{\mathrm{GL}(d,p^e)}(R) \circ Z).\langle\tau\rangle$ and $K = H^{(2)} \cap \Gamma L(d,q)$. Then*

(1) H and K map R-orbits on $V(d,q)$ to R-orbits on $V(d,q)$.

(2) $K = (K_1 \circ Z).\langle\tau\rangle$ where $N_{\mathrm{GL}(d,p^e)}(R) \leq K_1 \leq \mathrm{GL}(d,p^e)$.

(3) K_1 maps R-orbits on $U(d,p^e)$ to R-orbits on $U(d,p^e)$.

(4) $K_1.\langle\tau\rangle$ is 2-equivalent to $N_{\mathrm{GL}(d,p^e)}(R).\langle\tau\rangle$ in the induced action on U.

Proof. (1) Let $\Gamma_1 = v^R$ be an orbit of R in V where $v \in V$, and let Γ be the orbit of H containing Γ_1. Since $R \trianglelefteq H$, for each $h \in H$, we have $(v^R)^h = (v^h)^R$ and hence H maps R-orbits to R-orbits. Thus

$$\Gamma = \Gamma_1 \cup \Gamma_2 \cup ... \cup \Gamma_s \text{ for some } s \geq 1$$

where Γ_i are the R-orbits contained in Γ, and $|\Gamma_1| = \cdots = |\Gamma_s|$. Now define

$$\Delta = \{(u^h, v^h)|\ u, v \in \Gamma_1, h \in H\},$$

and observe that $\Delta = \cup_{i=1}^s (\Gamma_i \times \Gamma_i)$ and $\Delta \in$ 2-rel H. As K is 2-equivalent to H, K also preserves Δ. Let $u, v \in \Gamma_i$ and $x \in K$. Since $(u, v) \in \Delta$, also $(u^x, v^x) \in \Delta$. Thus u^x, v^x lie in the same R-orbit Γ_j for some j. Hence K also maps R-orbits to R-orbits.

(2) If $p^e = q$ then the statement is trivially true. If $p^e \neq q$ then H is a C_5-subgroup, and so K is also a C_5-subgroup by Proposition 6.7.1, preserving the same subfield structure as H. Then, since H contains both Z and τ, see (6.2),

$$H \leq K = (K_1 \circ Z).\langle\tau\rangle \text{ where } N_{\mathrm{GL}(d,p^e)}(R) \leq K_1 \leq \mathrm{GL}(d,p^e).$$

(3) Since both $\langle\tau\rangle$ and Z are subgroups of H which map R-orbits to R-orbits, (1) implies that K_1 maps R-orbits on V to R-orbits on V. In particular, since $R \leq K_1 \leq \mathrm{GL}(d, p^e)$, K_1 maps R-orbits on U to R-orbits on U too.

(4) For any $(u_1, u_2) \in U \times U$, we have

$$(u_1, u_2)^K = (\bigcup_{\lambda \notin F_{p^e}} \lambda(u_1, u_2)^{K_1.\langle\tau\rangle}) \bigcup (u_1, u_2)^{K_1.\langle\tau\rangle}$$

and

$$(u_1, u_2)^H = (\bigcup_{\lambda \notin F_{p^e}} \lambda(u_1, u_2)^{H_1.\langle\tau\rangle}) \bigcup (u_1, u_2)^{H_1.\langle\tau\rangle} \text{ where } H_1 = N_{\mathrm{GL}(d,p^e)}(R).$$

Since H is 2-equivalent to K on $V(d, q)$, we have

$$(u_1, u_2)^K = (u_1, u_2)^H.$$

Now the fact that $(u_1, u_2)^{K_1.\langle\tau\rangle} \subseteq U \times U$ and $(\lambda(u_1, u_2)^{K_1.\langle\tau\rangle}) \cap (U \times U) = \phi$ for each $\lambda \notin F_{p^e}$, implies that

$$(u_1, u_2)^{K_1.\langle\tau\rangle} = (u_1, u_2)^{H_1.\langle\tau\rangle} \subseteq U \times U.$$

Therefore, $K_1.\langle\tau\rangle$ is 2-equivalent to $N_{\mathrm{GL}(d,p^e)}(R).\langle\tau\rangle$. □

Lemma 6.9.2 allows us to reduce the proof of Proposition 6.9.1 to prove that K_1 is equal to $N_{\mathrm{GL}(d,p^e)}(R)$, that is, to the case where $q = p^e$. We have discussed the group structures of $N_{\mathrm{GL}(d,p^e)}(R)$ when $d \geq 3$ and divided them into five types according to the types of R in Section 4.6.3. Therefore, we will prove Proposition 6.9.1 type by type in the following subsections.

6.9.2 Proof of Proposition 6.9.1 when R is of type 5

Suppose R is of type 5 (see Section 4.6.3 for definition). Then $R = D_8 \circ D_8$, $d = 4$, $e = 1$, $p \equiv -1 \pmod 4$, and $H = N_{\Gamma\mathrm{L}(4,q)}(R) = (N_{\mathrm{GL}(4,p)}(R) \circ Z).\langle\tau\rangle$. By Lemma 6.9.2 (2), $K = (K_1 \circ Z)\langle\tau\rangle$ where $N_{\mathrm{GL}(4,p)}(R) \leq K_1 \leq \mathrm{GL}(4, p)$. To prove $K = H$, it is sufficient to prove that $N_{\mathrm{GL}(4,p)}(R) = K_1$. Since $e = 1$, Lemma 6.9.2 (4) implies that $N_{\mathrm{GL}(4,p)}(R)$ is 2-equivalent to K_1 on the F_p-space $U(4, p)$ defined in (6.1). Hence in this case we may assume that $q = p$, $V = V(4, p)$, and $H = N_{\mathrm{GL}(4,p)}(R)$ is a maximal C_6-subgroup in $\mathrm{GL}(4, p)$. Thus the following lemma proves that Proposition 6.9.1 holds when R is of type 5. Note that, in the following lemma, Z denotes the scalar subgroup of $\mathrm{GL}(4, p)$.

Lemma 6.9.3 *Suppose $q = p$, R is of type 5, $H = N_{\mathrm{GL}(4,p)}(R) \leq K \leq \mathrm{GL}(4, p)$ and K is 2-equivalent to H on $V = V(4, p)$. Then $H = K$.*

Proof. Since R is of type 5, $R = D_8 \circ D_8$ and $H = (Z \circ R).O^+(4,2) \leq \mathrm{GO}^+(4,p)$ is a C_8-subgroup. Hence by Lemma 6.8.3, $K \leq \mathrm{GO}^+(4,p)$. Note that, writing $\overline{L} = LZ/Z$ for subgroups L of $\mathrm{GL}(4,p)$,

$$\overline{R} = Z_2 \times Z_2 \times Z_2 \times Z_2,$$

$$\overline{H} = \overline{R} \rtimes O^+(4,2) = (Z_2^2.S_3 \times Z_2^2.S_3).2 = (S_4 \times S_4).2$$

and

$$\mathrm{PGO}^+(4,p) = (\mathrm{PGL}(2,p) \times \mathrm{PGL}(2,p)).2.$$

Hence we have

$$Z_2 \times Z_2 \times Z_2 \times Z_2 \leq (S_4 \times S_4).2 \leq \overline{K} \leq (\mathrm{PGL}(2,p) \times \mathrm{PGL}(2,p)).2.$$

To show $H = K$, it is sufficient to prove that $\overline{H} = \overline{K}$.

If $p = 3$, then $|\mathrm{PGL}(2,3)| = 24$ implies that $\overline{H} = \overline{K}$, and hence $H = K$ as required. So we may assume that $p > 3$. Since $p \equiv 3 \pmod 4$, this means $p \geq 7$.

By Dickson's Theorem, we know that S_4 is contained in $\mathrm{PSL}(2,p)$ and is maximal in $\mathrm{PSL}(2,p)$ (there are two conjugacy classes interchanged by $\mathrm{PGL}(2,p)$). Therefore $\overline{K} = \overline{H}$ or $\overline{K} \geq (\mathrm{PSL}(2,p) \times \mathrm{PSL}(2,p)).2$. (Since $\overline{H}$ and hence also $\overline{K}$ interchanges the two factors $\mathrm{PGL}(2,p)$ of $\mathrm{PGO}^+(4,p)$.)

Suppose $\overline{K} \geq (\mathrm{PSL}(2,p) \times \mathrm{PSL}(2,p)).2$. Then $K \geq Z \circ (\mathrm{SL}(2,p) \circ \mathrm{SL}(2,p)).2$. We view $V(4,p)$ as $V(4,p) = V(2,p) \otimes V(2,p)$. For any nonzero vector $w \in V(4,p)$, let $\overline{w}$ denote the 1-subspace spanned by w. Note that $\mathrm{PSL}(2,p)$ is 2-transitive on the set of 1-subspaces of $V(2,p)$, and hence for linearly independent vectors $u, v \in V(2,p) \setminus \{0\}$, we have $(\overline{v \otimes v}, \overline{u \otimes u})^{(\mathrm{PSL}(2,p) \times \mathrm{PSL}(2,p)).2} = \Psi$ where

$$\Psi = \{(\overline{v_1 \otimes v_2}, \overline{u_1 \otimes u_2}) |\ v_1, v_2, u_1, u_2 \in V(2,p) \setminus \{0\}, v_1 \notin \langle u_1 \rangle, v_2 \notin \langle u_2 \rangle\}.$$

By Lemma 6.1.1, $\overline{H}$ is 2-equivalent to $\overline{K}$ on $\overline{\Omega}$, and hence

$$(\overline{v \otimes v}, \overline{u \otimes u})^{\overline{H}} = (\overline{v \otimes v}, \overline{u \otimes u})^{\overline{K}} = \Psi.$$

Thus S_4 is 2-transitive on the set of 1-subspaces of $V(2,p)$, and this is a contradiction. Hence if $p \geq 7$, the only possibility for $\overline{K}$ is $\overline{K} = \overline{H}$, and hence $K = H$ as required. □

6.9.3 Proof of Proposition 6.9.1 when R is of type 1,2,3 or 4

Suppose R is of type 1, 2, 3 or 4 (see Section 4.6.3 for definition), and e is the smallest integer for which $p^e \equiv 1 \pmod{|Z(R)|}$. Then F_{p^e} is a subfield of F_q and $H = N_{\Gamma\mathrm{L}(d,q)}(R) = (N_{\mathrm{GL}(d,p^e)}(R) \circ Z).\langle\tau\rangle$ is a maximal C_6-subgroup. By Lemma 6.9.2 (2), $K = (K_1 \circ Z).\langle\tau\rangle$

where $N_{\mathrm{GL}(d,p^e)}(R) \le K_1 \le \mathrm{GL}(d,p^e)$. To show that $K = H$, it is sufficient to prove that $N_{\mathrm{GL}(d,p^e)}(R) = K_1$. Also by Lemma 6.9.2 (3), K_1 maps R-orbits on $U(d,p^e)$ to R-orbits on $U(d,p^e)$. Hence the following proposition will imply Proposition 6.9.1 when R is of type 1,2,3 or 4.

Proposition 6.9.4 *Suppose R is of type $1,2,3$ or 4 and $q = p^e$. Suppose also that $H = N_{\mathrm{GL}(d,p^e)}(R) \le K \le \mathrm{GL}(d,p^e)$, and K maps R-orbits to R-orbits in $V(d,p^e)$. Then $H = K$.*

Thus the proof of Proposition 6.9.4 will complete the entire proof of Proposition 6.9.1. Hence from now on, we assume that R is of type 1,2,3 or 4, and $q = p^e$. Also we assume $H = N_{\mathrm{GL}(d,p^e)}(R)$ and

$$R \lhd H \le K \le \mathrm{GL}(d,p^e)$$

such that K maps R-orbits to R-orbits. We will prove Proposition 6.9.4 by dealing with R type by type.

Recall that Z denotes the center of $\mathrm{GL}(d,p^e)$, and $\Omega = V(d,p^e) \setminus \{0\}$. Since $Z \le H$, the groups H and K (and $\mathrm{GL}(d,p^e)$) act naturally on $\overline{\Omega}$ where $\overline{\Omega}$ is the set of Z-orbits in Ω, and the kernel of each of these actions is Z. For a subgroup S of $\mathrm{GL}(d,p^e)$, denote by $\overline{S}$ the factor group SZ/Z. Then

$$\overline{R} \lhd \overline{H} \le \overline{K} \le \mathrm{PGL}(d,p^e) \ \text{ and these groups act faithfully on } \overline{\Omega}.$$

Also, both $\overline{H}$ and $\overline{K}$ preserve the set of $\overline{R}$-orbits in $\overline{\Omega}$.

Let $\mathcal{B}$ be the set of $\overline{R}$-orbits in $\overline{\Omega}$. Then both $\overline{H}$ and $\overline{K}$ act naturally on $\mathcal{B}$.

Lemma 6.9.5 *If R is of type $1,2,3$ or 4, then*

(1) For every $B \in \mathcal{B}$, $|B|$ is a power of r greater than 1.

(2) $\overline{R}$ is not semi-regular on $\overline{\Omega}$.

Proof. (1) Note that the representation of R on $V(d,p^e)$ is irreducible. Hence R fixes no 1-spaces, that is to say, $\overline{R}$ has no fixed points in $\overline{\Omega}$. Then for every $B \in \mathcal{B}$, $|B|$ is a power of r and is greater than 1.

(2) By Lemma 4.6.2, we know that R is not semi-regular on Ω. Let $x \in R$ such that $x \ne 1$ and x fixes a nonzero vector v. Since $R \cap Z = Z(R)$ acts on Ω by scalar transformations which do not fix any points in Ω, it follows that $x \notin Z(R)$ and so $\bar{x} \in \overline{R} \setminus \{1\}$ fixes $\bar{v} \in \overline{\Omega}$. Hence $\overline{R}$ is not semi-regular on $\overline{\Omega}$. □

Note that $\overline{R} = RZ/Z \cong R/(R \cap Z) = R/Z(R) \cong \overbrace{Z_r \times \cdots \times Z_r}^{2m}$. Hence $\overline{R}$ is an elementary abelian r-group and

$$\overline{H} = \begin{cases} \overline{R} \rtimes \mathrm{Sp}(2m, r), & m \geq 1, & \text{if } R \text{ is either of type 1 or type 2,} \\ \overline{R} \rtimes O^{+}(2m, 2), & m \geq 3, & \text{if } R \text{ is of type 3,} \\ \overline{R} \rtimes O^{-}(2m, 2), & m \geq 2, & \text{if } R \text{ is of type 4,} \end{cases}$$

where $\mathrm{Sp}(2m, r)$ and $O^{\pm}(2m, 2)$ act naturally on $\overline{R}$.

Lemma 6.9.6 *Suppose R is of type $1, 2, 3$ or 4. Then $\overline{R}$ is the unique minimal normal subgroup of $\overline{H}$.*

Proof. By the definition of $\overline{H}$, we have $\overline{R} \lhd \overline{H}$. Now, by [26, Proposition 2.10.6], $\mathrm{Sp}(2m, r)$, $O^{-}(2m, 2)$ and $O^{+}(2m, 2)$ (where in the last case $m \geq 2$), are irreducible on the underlying $2m$-dimensional space. Thus $\overline{R}$ is a minimal normal subgroup of $\overline{H}$. Also note that the actions of $\mathrm{Sp}(2m, r)$ and $O^{\pm}(2m, 2)$ on $\overline{R}$ are faithful, and therefore $C_{\overline{H}}(\overline{R}) = \overline{R}$. Hence $\overline{R}$ is the unique minimal normal subgroup of $\overline{H}$. □

Both $\overline{H}$ and $\overline{K}$ act on $\mathcal{B}$ (the set of $\overline{R}$-orbits in $\overline{\Omega}$). Let M be the kernel of the action of $\overline{K}$ on $\mathcal{B}$. Then

$$\overline{R} \leq M \lhd \overline{K}$$

and $\mathcal{B}$ is also the set of M-orbits in $\overline{\Omega}$. Let

$$A = N_M(\overline{R}).$$

We will investigate the group structure of A. Then for each possibility of A, we will prove that $K = H$.

Lemma 6.9.7 *Suppose R is of type $1, 2, 3$ or 4. Then $\overline{R}$ is not a minimal normal subgroup of A.*

Proof. Let $B \in \mathcal{B}$. By Lemma 6.9.5 (1), $|B| > 1$. Since $A \leq M$, A fixes B setwise.

Suppose $\overline{R}$ is a minimal normal subgroup of A. Let A_0 be the kernel of the action of A on B. Then A_0 and $\overline{R}$ are normal in A, and so $A_0 \cap \overline{R} \trianglelefteq A$. By Lemma 6.9.5 (1), $\overline{R}$ is nontrivial on B, and hence $A_0 \cap \overline{R} \neq \overline{R}$. Therefore by the minimality of $\overline{R}$, $A_0 \cap \overline{R} = 1$. Thus $\overline{R}$ is faithful on B, and since $\overline{R}$ is abelian, it follows that $\overline{R}$ is regular on B. Since this holds for each $B \in \mathcal{B}$, $\overline{R}$ is semi-regular on $\overline{\Omega}$, which contradicts Lemma 6.9.5 (2). Hence $\overline{R}$ is not a minimal normal subgroup of A. □

Lemma 6.9.8 *If R is of type $1, 2, 3$ or 4, then $\overline{R} \trianglelefteq A = N_M(\overline{R}) \trianglelefteq N_{\overline{\mathrm{GL}(d,p^e)}}(\overline{R}) = \overline{H}$.*

Proof. First we show that $N_{\overline{\mathrm{GL}(d,p^e)}}(\overline{R}) = \overline{H}$. By definition, $\overline{H} = \overline{N_{\mathrm{GL}(d,p^e)}(R)}$. Hence $\overline{H} \le N_{\overline{\mathrm{GL}(d,p^e)}}(\overline{R})$. On the other hand, to show that $N_{\overline{\mathrm{GL}(d,p^e)}}(\overline{R}) \le \overline{H}$, it is enough to show that if $x \in \mathrm{GL}(d,p^e)$ satisfies $x^{-1}Rx \le RZ$, then $x \in N_{\mathrm{GL}(d,p^e)}(R)$. Now, suppose $x^{-1}Rx \le RZ$. Then for any $y \in R$, there exist $r_1 \in R$ and $z_1 \in Z$ such that

$$x^{-1}yx = r_1 z_1.$$

The exponent of R is $c = r(2,r)$, and hence

$$1 = x^{-1}y^c x = r_1^c z_1^c = z_1^c.$$

Now Z is a cyclic group of order $p^e - 1$. Also, when R is either of type 1 or type 2, we have $c = |Z(R)|$. Since $Z(R)$ is the unique subgroup of Z of order c, $z_1 \in Z(R) \le R$, and it follows that $x^{-1}Rx \le R$.

When R is either of type 3 or type 4, we have $|Z(R)| = 2$, $c = 4$, and $p = p^e \equiv -1 \pmod 4$. Thus $|Z| = p^e - 1 \equiv 2 \pmod 4$, and so $z_1^4 = 1$ implies that $z_1^2 = 1$. Therefore, once again $z_1 \in Z(R) \le R$, so that $x^{-1}Rx \le R$, and hence $N_{\overline{\mathrm{GL}(d,p^e)}}(\overline{R}) = \overline{H}$ as required.

Note that since $\overline{H} = N_{\overline{\mathrm{GL}(d,p^e)}}(\overline{R})$, it follows that $A \le \overline{H}$. The only thing remaining is to prove that $A \trianglelefteq \overline{H}$. Let $n \in A = N_M(\overline{R})$ and $h \in \overline{H}$. Since $M \trianglelefteq \overline{K}$ and $h \in \overline{K}$, we have $h^{-1}nh \in M$. Also since $\overline{H}$ normalizes $\overline{R}$, it follows that $h^{-1}nh$ also normalizes $\overline{R}$, and therefore $h^{-1}nh \in A$. □

By Lemma 6.9.8,

$$A/\overline{R} \trianglelefteq \overline{H}/\overline{R} = \begin{cases} \mathrm{Sp}(2m,r) & \text{if } R \text{ is either of type 1 or type 2,} \\ O^{\pm}(2m,2) & \text{if } R \text{ is either of type 3 or type 4.} \end{cases}$$

Lemma 6.9.9 *(1) Suppose R is either of type 1 or type 2. Then $A/\overline{R}$ is contained in the center $Z(\mathrm{Sp}(2m,r)) = Z_{(r-1,2)}$.*

(2) Suppose R is either of type 3 or type 4. Then $A = \overline{R}$.

Proof. (1) Set $I = Z(\mathrm{Sp}(2m,r))$, and suppose that $A/\overline{R} \not\le I$. Lemma 6.9.6 and Lemma 6.9.7 imply that $A \ne \overline{H}$. Hence $\frac{(A/\overline{R})I}{I}$ is a proper, nontrivial normal subgroup of $\frac{\overline{H}/\overline{R}}{I} = \mathrm{PSp}(2m,r)$, and in particular, $\mathrm{PSp}(2m,r)$ is not simple. This implies that $(2m,r) = (2,3)$ or $(2m,r) = (4,2)$.

If $(2m,r) = (2,3)$, we have $\mathrm{Sp}(2,3) = Q_8 \rtimes Z_3$ where

$$Z_3 = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$$

and

$$Q_8 = \langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \rangle.$$

The only normal subgroups of $\mathrm{Sp}(2,3)$ are 1, $Z(\mathrm{Sp}(2m,3)) = \langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$, Q_8 and $\mathrm{Sp}(2,3)$. Since $A/\overline{R} \neq 1, I$ or $\overline{H}/\overline{R}$, we must have $A = \overline{R} \rtimes Q_8$. But the fact that Q_8 is transitive on $\overline{R} \backslash \{1\}$ implies that $\overline{R}$ is a minimal normal subgroup of A, which is impossible by Lemma 6.9.7.

If $(2m, r) = (4, 2)$, we have $\mathrm{Sp}(4, 2) = S_6$, and $Z(S_6) = 1$. The only normal subgroups of S_6 are 1, A_6 and S_6, and since $A/\overline{R} \neq 1$ or $\overline{H}/\overline{R}$, we have $A = \overline{R} \rtimes A_6$. Note that A_6 fixes no element of $\overline{R} \setminus \{1\}$ and the only degrees of transitive permutation representations of A_6 less than $|\overline{R}| = 16$ are 6, 10 and 15. Hence A_6 must be transitive on $\overline{R} \setminus \{1\}$. It follows that $\overline{R}$ is a minimal normal subgroup of A, which is again impossible.

The proof of (1) is now complete.

(2) In this case, we have $A/\overline{R} \trianglelefteq \overline{H}/\overline{R} = O^{\pm}(2m, 2)$ with $m \geq 3$ or $O^{-}(4, 2)$. Note that the only normal subgroups of $O^{+}(2m, 2)$ with $m \geq 3$ or of $O^{-}(2m, 2)$ with $m \geq 2$ are $1, \Omega^{\pm}(2m, 2)$ and $O^{\pm}(2m, 2)$. By Lemma 6.9.6 and Lemma 6.9.7, $A \neq \overline{H}$. Now suppose $A = \overline{R} \rtimes \Omega^{\pm}(2m, 2)$. By [26, Proposition 2.10.6], the natural action of $\Omega^{\pm}(2m, 2)$ on $\overline{R}$ is irreducible. But then $\overline{R}$ is the unique minimal normal subgroup of A, which contradicts Lemma 6.9.7. Hence $A = \overline{R}$ as required. □

We have now determined that, for each type, there are at most 2 possibilities for A. Next we will show that $K = H$ for each possibility for A. To do this, we need the following theorem of Burnside (see [20, Kapital IV, Hauptsatz 2.6, p. 419]). Let p be a prime. We denote by $\mathrm{Syl}_p(G)$ the set of Sylow-p subgroups of a finite group G.

Definition 6.9.10 Let G be a finite group, p a prime, and $P \in \mathrm{Syl}_p(G)$. We say that G is *p-nilpotent* if there exists $N \trianglelefteq G$ such that $N \cap P = 1$ and $NP = G$.

Theorem 6.9.11 [Burnside] *Let G be a finite group and $P \in \mathrm{Syl}_p(G)$. If $N_G(P) = C_G(P)$, then G is p-nilpotent.*

Now recall that $\mathcal{B}$ is the set of $\overline{R}$-orbits in $\overline{\Omega}$ and M is the kernel of $\overline{K}$ acting on $\mathcal{B}$. Hence $\mathcal{B}$ is also the set of M-orbits in $\overline{\Omega}$.

Lemma 6.9.12 *If $1 \neq Q \trianglelefteq M$, then the sizes of all nontrivial Q-orbits in $\overline{\Omega}$ are powers of r. In particular, r divides $|Q|$. Moreover, if Q is r-nilpotent, then Q is an r-group.*

Proof. By Lemma 6.9.5, for every $B \in \mathcal{B}$, the size $|B|$ is a power of r greater than 1. Since $1 \neq Q$, there exist nontrivial Q-orbits in $\overline{\Omega}$. Now pick any nontrivial Q-orbit. Then it is contained in some $B \in \mathcal{B}$ (since $\mathcal{B}$ is the set of M-orbits in $\overline{\Omega}$). Since $Q \trianglelefteq M$, it follows that Q is half-transitive on B, (that is, all Q-orbits in B have the same size). As $|B|$ is a power of r, the size of each Q-orbit in B is also a power of r. Hence we have proved that the sizes of all nontrivial Q-orbits in $\overline{\Omega}$ are powers of r.

Next, we also assume that Q is r-nilpotent. Let $P \in \mathrm{Syl}_r(Q)$. Then there exists $S \trianglelefteq Q$ such that $Q = SP$ and $r \nmid |S|$. We claim that $S = 1$. If not, then S acts nontrivially and half-transitively on at least one of the nontrivial orbits of Q. The same argument as in the previous paragraph proves that r divides $|S|$, which is a contradiction. Therefore, $S = 1$ and $Q = P$ is an r-group. □

We now return to consider $A = N_M(\overline{R})$. We will show that $K = H$ for each possibility for A.

Lemma 6.9.13 *Suppose R is of type $1, 2, 3$ or 4. If $A = \overline{R}$, then $K = H$.*

Proof. Since $A = N_M(\overline{R}) = \overline{R}$ and $\overline{R}$ is abelian, it follows that $N_M(\overline{R}) = C_M(\overline{R})$. Then $\overline{R}$ is a Sylow r-subgroup of M (to show this, let $L \in \mathrm{Syl}_r(M)$ and $L > \overline{R}$. Then $N_M(\overline{R}) \geq N_L(\overline{R}) > \overline{R}$). By Theorem 6.9.11, M is r-nilpotent. Hence by Lemma 6.9.12, $\overline{R} = M$. Now $\overline{R} = M \trianglelefteq \overline{K}$. Hence for any $x \in K$, we have $x^{-1}Rx \leq RZ$. The argument in the proof of Lemma 6.9.8 now shows that $x \in N_{\mathrm{GL}(d,p^e)}(R) = H$. Thus $H = K$ as required. □

Note that when R is of type 2, we have $r = 2$ and $Z(\mathrm{Sp}(2m, r)) = 1$. Hence the only case remaining now is $A/\overline{R} = Z_2 = Z(\mathrm{Sp}(2m, r))$ where r is odd and R is of type 1. Now $A = N_M(\overline{R}) = \overline{R}.Z_2$. This implies that $\overline{R} \in \mathrm{Syl}_r(M)$. Let E be a minimal normal subgroup of M, and let

$$Y = \langle E^h \mid h \in \overline{H} \rangle.$$

Lemma 6.9.14 *$\overline{R} \leq Y \trianglelefteq M$, $\overline{H} \leq N_{\overline{K}}(Y)$ and $\overline{R} \in \mathrm{Syl}_r(Y)$.*

Proof. Since $M \trianglelefteq \overline{K}, \overline{H} \leq \overline{K}$ and $E \trianglelefteq M$, it follows that $E^h \trianglelefteq M$ for all $h \in \overline{H}$. Hence $1 \neq Y \trianglelefteq M$. By Lemma 6.9.12, r divides $|Y|$. Now $\overline{R} \in \mathrm{Syl}_r(M)$ and $Y \trianglelefteq M$ imply that $1 \neq \overline{R} \cap Y \in \mathrm{Syl}_r(Y)$.

Note that $\overline{H}$ leaves $\{E^h, h \in \overline{H}\}$ invariant. Hence $\overline{H} \leq N_{\overline{K}}(Y)$. By Lemma 6.9.6, $\overline{R}$ is the unique minimal normal subgroup of $\overline{H}$. Then since $\overline{R} \cap Y$ is nontrivial and normalized by $\overline{H}$, it follows that $\overline{R} \leq Y$ and $\overline{R} \in \mathrm{Syl}_r(Y)$. □

We now have

$$\overline{R} \leq N_Y(\overline{R}) \leq N_M(\overline{R}) = \overline{R}.Z_2,$$

and by the definition of Y,

$$Y = T^l$$

for some simple group T and $l \geq 1$. Recall that in this remaining case R has type 1.

Lemma 6.9.15 *Suppose R is of type 1, and $A = N_M(\overline{R}) = \overline{R}.Z_2$. Then $K = H$.*

Proof. If T is abelian, then $\overline{R} \leq Y$ implies that $T = Z_r$. Also, $\overline{R} \in \mathrm{Syl}_r(Y)$ implies that $\overline{R} = Y \trianglelefteq M$ and $\overline{R}$ is the unique Sylow-r subgroup of M. Thus we have $\overline{R}$ *char* $M \trianglelefteq \overline{K}$. Hence $\overline{R} \trianglelefteq \overline{K}$, and we get $H = K$ as required.

Now suppose T is nonabelian and $N_Y(\overline{R}) = \overline{R}$. Then $\overline{R} = N_Y(\overline{R}) = C_Y(\overline{R})$. By Theorem 6.9.11, Y is r-nilpotent. Since $1 \neq Y \trianglelefteq M$, Lemma 6.9.12 implies that $Y = \overline{R}$, which contradicts the fact that T is nonabelian.

Lastly, suppose T is nonabelian and $N_Y(\overline{R}) = \overline{R}.Z_2$. Assume that

$$Y = T^l = T_1 \times \cdots \times T_l, \quad \text{and each } T_i \cong T.$$

Now r divides $|Y|$ implies that r divides $|T_i|$. Also, $\overline{R} \in \mathrm{Syl}_r(Y)$ and $T_i \trianglelefteq Y$ imply that $\overline{R} \cap T_i \in \mathrm{Syl}_r(T_i)$. Thus by comparing the orders

$$\overline{R} = (\overline{R} \cap T_1) \times \cdots \times (\overline{R} \cap T_l).$$

Hence

$$\overline{R}.Z_2 = N_Y(\overline{R}) = N_{T_1}(\overline{R} \cap T_1) \times \cdots \times N_{T_l}(\overline{R} \cap T_l).$$

Thus $l = 1$, $Y = T$ and $N_T(\overline{R} \cap T) = (\overline{R} \cap T).Z_2$. Now we have $\overline{R} \leq T = Y \leq M$ and T is simple. Let $B \in \mathcal{B}$. Since $T \leq M$, B is T-invariant. Since T is simple and $\overline{R}$ is transitive on B, it follows that T is faithful on B. Hence $\overline{R}$ is faithful on B. Then, as $\overline{R}$ is abelian and transitive on B we have that $\overline{R}$ is regular on B. It follows that $\overline{R}$ is semi-regular on $\overline{\Omega}$, which is impossible by Lemma 6.9.5.

This completes the proof. □

Now Lemmas 6.9.9, 6.9.13, and 6.9.15 conclude the proof of Proposition 6.9.4.

6.10 The case $H \in C_9$ for $d \geq 3$.

Recall that $H \in C_9$ if H does not contain $\mathrm{SL}(d, q)$ and is not contained in any maximal C_i-subgroup for $i = 1, 2, ..., 8$. In view of Proposition 6.2.1, we suppose $d \geq 3$ in this section.

Proposition 6.10.1 *Suppose $d \geq 3$ and $H \in C_9$. Then either $d = 4, q = 2$ and $H = A_7$ is 2-transitive on Ω, or $K \in C_9$.*

Proof. Note that by the definition of the class C_9, $H \notin \cup_{i=1}^{8} C_i$, and hence $K \notin \cup_{i=1}^{8} C_i$. Therefore $K \in C_9$ or $K \geq \mathrm{SL}(d, q)$.

Assume that $K \geq \mathrm{SL}(d, q)$. We will show that in this case $d = 4, q = 2$ and $H = A_7$. Consider the natural action of $\mathrm{P\Gamma L}(d, q)$ on $\overline{\Omega}$ where $\overline{\Omega}$ is the set of 1-subspaces of V. By Lemma 6.1.1, $\overline{H} = HZ/Z$ is 2-equivalent to $\overline{K} = KZ/Z$ on $\overline{\Omega}$. Since $K \geq \mathrm{SL}(d, q)$, $\overline{K} \geq \mathrm{PSL}(d, q)$ is 2-transitive on $\overline{\Omega}$. Thus $\overline{H}$ is 2-transitive on $\overline{\Omega}$. Note that $d \geq 3$. By Theorem 3.3.3, either $d = 4, q = 2$ and $H = A_7$ is 2-transitive on Ω, or $H \geq \mathrm{SL}(d, q)$. But the latter case contradicts the definition of $H \in C_9$.

Thus we get the desired result. □

Theorem 6.0.6 now follows from Proposition 6.2.1 for the case $d = 2$. For $d \geq 3$, it follows from Proposition 6.3.1 (for $H \in C_1$), Proposition 6.4.1 (for $H \in C_2$), Proposition 6.5.1 (for $H \in C_3$), Proposition 6.6.2 (for $H \in C_4$ or C_7), Proposition 6.7.1 (for $H \in C_5$), Proposition 6.8.1 (for $H \in C_8$), Proposition 6.9.1 (for $H \in C_6$), and Proposition 6.10.1 (for $H \in C_9$).

Chapter 7

Closures of Affine Permutation Groups

In this chapter we state and prove our main results concerning 3-closures of affine permutation groups. These results (Theorem 7.1.1, Theorem 7.2.1, Corollary 7.2.2) answer Question 1.2.1 for $k = 3$ in terms of Aschbacher's classification.

7.1 The general result

We have already studied the 2-closures of the subgroups of general semilinear groups in Chapter 5 and Chapter 6. The main results we have obtained are Theorem 5.0.1 and Theorem 6.0.6. In this section, we draw together Theorem 5.0.1 and Theorem 6.0.6 in the light of Lemma 2.4.1 (4) to obtain Theorem 7.1.1. Note that this theorem is also independent of the simple group classification and is valid for all affine permutation groups, not only the primitive ones.

Theorem 7.1.1 *Suppose G is an affine permutation group such that $G = NH$, where $N = Z_p^d$, $H \leq \mathrm{GL}(d, p)$, $d \geq 1$ and p is a prime.*

1. *If $d = 1$ then $G^{(2)} = G^{(3)} = G$ for proper subgroups G of $\mathrm{AGL}(1, p)$, while $\mathrm{AGL}(1, p)^{(2)} = S_p$ and $\mathrm{AGL}(1, p)^{(3)} = \mathrm{AGL}(1, p)$.*
2. *If $d = 2$, then $G^{(3)} \cap \mathrm{AGL}(2, p) = G$.*
3. *If $d \geq 3$ and H contains $\mathrm{SL}(d, p)$, then $\mathrm{AGL}(d, p) \leq G^{(3)}$.*
4. *If $d \geq 3$, $\mathrm{SL}(d, p) \not\leq H$ and $H \in C_i$ for $i = 1, 2, ..., 8, 9$, then either $G = Z_2^4 A_7 < \mathrm{AGL}(4, 2)$ and $G^{(2)} = G^{(3)} = S_{16}$, or $G^{(3)} \cap \mathrm{AGL}(d, p) = NK$ with $K \in C_i$.*

Proof. We have proved Part (1) in Section 5.4 (Theorem 5.4.1(2)), and proved Part (2) in Section 5.2 (Corollary 5.2.2). For Parts (3) and (4), note that if $G^{(3)} \cap \mathrm{AGL}(d, p) = NK$, then Lemma 2.4.1 (4) implies that $K \leq H^{(2)} \cap \mathrm{GL}(d,p)$. Thus Parts (3) and (4) follow from Theorems 5.0.1 and 6.0.6 respectively. $\square$

7.2 Closures of affine primitive groups

Our second major result, however, does depend on the simple group classification, as does the result [47, Lemma 4.1] that it strengthens. It describes those affine primitive groups G for which the 3-closure has socle different from the socle of G. Our improvement lies in the explicit classification of G in part (b).

Theorem 7.2.1 *Suppose $G \leq \mathrm{AGL}(d,p)$ is an affine primitive group of degree p^d where p is a prime and $d \geq 1$. Suppose also that $G < L \leq G^{(3)}$ with $L \not\leq \mathrm{AGL}(d,p)$. Then $p = 2$ and either*

(a) *$L \geq A_{2^d}$ and $G = \mathrm{AGL}(d,2)$ (with $d \geq 3$) or $G = Z_2^4 \rtimes A_7$ (with $d = 4$), or*

(b) *G and L preserve a product decomposition Γ^m, where $|\Gamma| = 2^{d'}, m \geq 2$, and $d = d'm$. Moreover, $(A_{2^{d'}})^m \leq L \leq S_{2^{d'}} \wr S_m$ and $G = G_0 \wr D$, where D is a transitive subgroup of S_m and $G_0 = \mathrm{AGL}(d',2)$ (with $d' \geq 3$) or $Z_2^4 \rtimes A_7$ (with $d' = 4$).*

We will give the proof of the above theorem in the next section. Note that we can apply Theorem 7.2.1 to strengthen Theorem 7.1.1 (2),(3) by determining $G^{(3)}$ instead of only $G^{(3)} \cap \mathrm{AGL}(d,p)$, in the case where G is primitive.

Corollary 7.2.2 *Suppose that G is a primitive affine permutation group such that $G = NH$, where $N = Z_p^d$, $H \leq \mathrm{GL}(d,p)$, p is a prime, and $d \geq 2$.*

(a) *If $d = 2$ then $G^{(3)} = G$.*

(b) *If $d \geq 3$ and H contains $\mathrm{SL}(d,p)$, then $G^{(3)} = \mathrm{AGL}(d,p)$ when p is odd and $G^{(3)} = S_{2^d}$ when $p = 2$.*

(c) *If $G = Z_2^4.A_7 < \mathrm{AGL}(4,2)$ then $G^{(2)} = G^{(3)} = S_{16}$.*

(d) *If $d \geq 3, \mathrm{SL}(d,p) \not\leq H$ and $G \neq Z_2^4.A_7$, then either $G^{(3)} = NK$ where H, K lie in C_i for the same i, where $1 \leq i \leq 9$, or $G^{(3)}$ and G are given by Theorem 7.2.1 (b).*

Proof. (a) Theorem 7.2.1 implies that when $d = 2$, $G^{(3)} \leq \mathrm{AGL}(2,p)$. Thus the result follows from Theorem 7.1.1(2) immediately.

(b) Suppose p is odd, then $G^{(3)} \leq \mathrm{AGL}(d,p)$ by Theorem 7.2.1. Therefore $G^{(3)} = \mathrm{AGL}(d,p)$ follows from Theorem 7.1.1(3). Next suppose $p = 2$. Theorem 7.1.1(3) and

Lemma 2.4.1 (2)(5) imply that $\mathrm{AGL}(d,2)^{(3)} \le G^{(3)}$. Thus $G^{(3)} = S_{2^d}$ as $\mathrm{AGL}(d,2)$ is 3-transitive on $V(d,2)$.

(c) It follows from the fact that $G = Z_2^4.A_7$ is 3-transitive on $V(4,2)$.

(d) It follows from Theorem 7.1.1 (4) when $G^{(3)} \le \mathrm{AGL}(d,p)$ and follows from Theorem 7.2.1 otherwise. □

7.3 Product action and the proof of Theorem 7.2.1

As we defined in Section 2.3.3, a permutation group G on Ω is said to preserve a product decomposition Γ^m of Ω, $m \ge 2$, if Ω can be identified with the Cartesian product $\Gamma^m = \Gamma_1 \times \cdots \times \Gamma_m$ (where $\Gamma_i = \Gamma$ for all $1 \le i \le m$) in such a way that G is a subgroup of the wreath product

$$W = \mathrm{Sym}(\Gamma) \wr S_m = \mathrm{Sym}(\Gamma)^m \rtimes S_m$$

with a natural product action.

Recall that we denote the projection of $W = \mathrm{Sym}(\Gamma)^m \rtimes S_m$ onto S_m by π, and for $1 \le i \le m$,

$$W_i = \mathrm{Sym}(\Gamma_i) \times (\mathrm{Sym}(\Gamma) \wr S_{m-1})$$

is the subgroup of all the elements of W which fix i under the action of π.

Now, we assume G is primitive and preserves a product decomposition Γ^m. Thus $G \le W = \mathrm{Sym}(\Gamma) \wr S_m$. By primitivity of G (Lemma 2.3.4), $\pi(G) = D \le S_m$ is transitive.

Recall that we denote by π_i the projection from $G \cap W_i$ to $\mathrm{Sym}(\Gamma_i)$,

$$\pi_i : G \cap W_i \to \mathrm{Sym}(\Gamma_i),$$

where the subgroup $G \cap W_i$ consists of all the elements of G which fix the i-th component Γ_i setwise.

Since $\pi(G)$ is transitive, set $\Gamma = \Gamma_1$, we can define the *group induced by G on Γ* (see Section 2.3.3) to be $G_0 := \pi_1(G \cap W_1)$, so that $G_0 \le \mathrm{Sym}(\Gamma)$.

Praeger and Saxl proved the following lemma in [47].

Lemma 7.3.1 [47, Lemma 4.1] *Suppose $G \le \mathrm{AGL}(d,p)$ is an affine primitive group of degree p^d where p is a prime and $d \ge 1$. Suppose also that $G < L \le G^{(3)}$ where G and L have different socles. Then $p = 2$ and either*

(a) $L \ge A_{2^d}$ and $G = Z_2^4 \rtimes A_7$ (with $d = 4$), or $G = \mathrm{AGL}(d,2)$ (with $d \ge 3$), or

(b) G and L preserve a product decomposition Γ^m, where $|\Gamma| = 2^{d'}$, $d = d'm$, $m \ge 2$, and the permutation group G_0 induced by G on Γ is $Z_2^4 \rtimes A_7$ (with $d' = 4$) or $\mathrm{AGL}(d',2)$

(with $d' \geq 3$). Moreover, the group induced by L on Γ contains $A_{2^{d'}}$ and

$$\mathrm{soc}(L) = \mathrm{soc}(G^{(3)}) \cong \overbrace{A_{2^{d'}} \times \cdots \times A_{2^{d'}}}^{m}.$$

Next we assume that case (b) of the above lemma holds. By a result of Kovacs [28, 2.2], after replacing G by a conjugate of G under an element of $S_{2^{d'}} \wr S_m$, if necessary, we may assume that

$$G \leq G_0 \wr S_m.$$

Now to complete the proof of Theorem 7.2.1, we need to show that G contains the base group $\overbrace{G_0 \times \cdots \times G_0}^{m}$, and hence

$$G_0^m \trianglelefteq G = G_0 \wr \pi(G) = G_0 \wr D.$$

Consider the stabilizer G_α of the point $\alpha = (\delta, ..., \delta) \in \Gamma^m$. Then

$$G_\alpha \leq (G_0)_\delta \wr S_m,$$

where the point stabilizer is $(G_0)_\delta \cong \mathrm{GL}(d', 2)$ (with $2^{d'} \geq 8$) or A_7 (with $d' = 4$). Hence $(G_0)_\delta$ is a nonabelian simple group.

Lemma 7.3.2 $(2^{d'} - 1)^m (2^{d'} - 2)^m$ *divides* $|G_\alpha|$ *where* $\alpha = (\delta, ..., \delta) \in \Gamma^m$.

Proof. First, consider the action of $G^{(3)}$. By Lemma 7.3.1,

$$\mathrm{soc}(G^{(3)}) = \overbrace{A_{2^{d'}} \times \cdots \times A_{2^{d'}}}^{m} \leq G^{(3)}.$$

Then the point stabilizer

$$(G^{(3)})_\alpha \geq (A_{2^{d'}-1})^m.$$

Recall that $|\Gamma| = 2^{d'} \geq 8$. Let μ, ν be distinct points in $\Gamma \setminus \{\delta\}$, let $\beta = (\mu, ..., \mu) \in \Gamma^m$ and $\gamma = (\nu, ..., \nu) \in \Gamma^m$. Let Δ be the orbit of $(A_{2^{d'}-1})^m$ containing the pair $(\beta, \gamma) = ((\mu, ..., \mu), (\nu, ..., \nu))$. Since $A_{2^{d'}-1}$ is 2-transitive on $\Gamma \setminus \{\delta\}$, we have

$$\Delta = \{((\mu_1, ..., \mu_m), (\nu_1, ..., \nu_m)) \mid \mu_i, \nu_i \in \Gamma \setminus \{\delta\} \text{ and } \mu_i \neq \nu_i \text{ for all } i \leq m\}.$$

Also, since Δ is invariant under $(G^{(3)})_\alpha$, we know that Δ is actually a $(G^{(3)})_\alpha$-orbit. By Lemma 2.4.1 (4), G_α is 2-equivalent to $(G^{(3)})_\alpha$, and so Δ is also a G_α-orbit. Finally $|\Delta| = (2^{d'} - 1)^m (2^{d'} - 2)^m$, and $|\Delta|$ divides $|G_\alpha|$. □

Recall from Section 3.2, a prime s dividing $2^{d'} - 1$ is said to be a *primitive prime divisor* of $2^{d'} - 1$ if s does not divide $2^i - 1$ for any i such that $1 \leq i < d'$. It was proved by

Zsigmondy (Theorem 3.2.2) in 1892 that for $d' \geq 2$, $2^{d'} - 1$ has a primitive prime divisor unless $d' = 6$.

When $d' \neq 6$, pick s to be a primitive prime divisor of $2^{d'} - 1$. When $d' = 6$, we set $s = 31 = 2^5 - 1$. It is easy to see that 31 does not divide $2^i - 1$ for $i = 1, 2, 3, 4, 6$. By the choice of s, s must be an odd prime. Now, for any $2^{d'} \geq 8$, let $s^a || (2^{d'} - 1)(2^{d'-1} - 1)$. Then $a \geq 1$. By Lemma 7.3.2, s^{am} divides $|G_\alpha|$.

Let

$$M = G_\alpha \cap \overbrace{((G_0)_\delta \times \cdots \times (G_0)_\delta)}^{m},$$

that is, M is the intersection of G_α with the base group of $W = \mathrm{Sym}(\Gamma) \wr S_m$. Then

$$M \trianglelefteq G_\alpha.$$

We will use the result that s^{am} divides $|G_\alpha|$ to estimate the order of M.

Lemma 7.3.3 *With the notation above, $s^{am - [\frac{m-1}{2}]}$ divides $|M|$. In particular, $M \neq \{1\}$.*

Proof. Let the s-part of $m! = |S_m|$ be s^c. Then by [12, Exercise 2.6.8],

$$c \leq [\frac{m-1}{s-1}] \leq [\frac{m-1}{2}].$$

Now G_α / M is isomorphic to a subgroup of S_m and so the highest power of s dividing $|G_\alpha / M|$ is less than or equal to s^c. Since s^{am} divides $|G_\alpha|$, it follows that $1 \neq s^{am - [\frac{m-1}{2}]}$ divides $|M|$. □

Lemma 7.3.4 *$M \cong ((G_0)_\delta)^u$, where $u | m$.*

Proof. Recall that

$$W_i = \mathrm{Sym}(\Gamma_i) \times (\mathrm{Sym}\Gamma \wr S_{m-1})$$

and

$$\pi_i : G \cap W_i \to \mathrm{Sym}\Gamma_i.$$

We have

$$\pi_i(G_\alpha \cap W_i) = (\pi_i(G \cap W_i))_\delta \cong (G_0)_\delta. \tag{7.1}$$

Write

$$(G_0)_\delta = T \text{ and } \overbrace{(G_0)_\delta \times \cdots \times (G_0)_\delta}^{m} = T_1 \times \cdots \times T_m \quad \text{where } T_i = T = (G_0)_\delta,$$

and note that, by Lemma 7.3.1, T is a nonabelian simple group (namely, either $\mathrm{GL}(d', 2)$ or A_7) and $M \leq W_i$ for all i. As $G = Z_2^d \rtimes G_\alpha$ is affine primitive, $\pi(G) = \pi(G_\alpha)$ is transitive.

Hence G_α acts on $\Sigma = \{T_1, ..., T_m\}$ transitively by conjugation. Let $i, j \in \{1, ..., m\}$. Then there exists $x \in G_\alpha$ such that $\pi(x) : i \to j$. Since $M \lhd G_\alpha$, $x^{-1}\pi_i(M)x = \pi_j(M)$. Thus $\pi_i(M) \cong \pi_j(M)$ for $1 \leq i, j \leq m$.

Now, the facts that $\{1\} \neq M \trianglelefteq G_\alpha \cap W_i$ and $(G_0)_\delta = T$ is simple together with (7.1) imply that

$$\pi_i(M) \cong (G_0)_\delta = T \quad \text{for } i = 1, 2, ..., m.$$

By Lemma 2.3.7(2), there exists a partition $\{\Lambda_1, ..., \Lambda_u\}$ of $\Sigma = \{T_1, ..., T_m\}$ such that $M = V_1 \times \cdots \times V_u$ where $V_i \cong T$ is a full diagonal subgroup of the subproduct $\prod_{j \in \Lambda_i} T_j$. Since $M \lhd G_\alpha$ and G_α acts on Σ transitively, we have $u|m$. □

In the next lemma we will prove that u must be m. Hence $M \cong ((G_0)_\delta)^m$ and $G \rhd \overbrace{G_0 \times \cdots \times G_0}^{m}$, which will conclude the proof of Theorem 7.2.1.

Lemma 7.3.5 *With the notation of Lemma 7.3.4, we have $u = m$ and $M \cong ((G_0)_\delta)^m$.*

Proof. By Lemma 7.3.3, $s^{am-[\frac{m-1}{2}]}$ divides $|M|$. By Lemma 7.3.4, $M \cong ((G_0)_\delta)^u$ where $(G_0)_\delta \leq \mathrm{GL}(d', 2)$ and u divides m. Also by Proposition 3.2.1,

$$|\mathrm{GL}(d', 2)| = 2^{\frac{d'(d'-1)}{2}} \prod_{i=1}^{d'} (2^i - 1).$$

By the choice of s, s^{au} is the highest power of s that divides $|\mathrm{GL}(d', 2)^u|$. Therefore the power of s that divides $|M|$ is less than or equal to s^{au}. Since $s^{am-[\frac{m-1}{2}]}$ divides $|M|$, $au \geq am - [\frac{m-1}{2}] > (a - \frac{1}{2})m$. But then $u > \frac{m}{2}$. Since $u|m$, $u = m$ as required. □

Chapter 8

Elusive Permutation Groups

In this chapter we first discuss some known results about elusive permutation groups and then study our second problem, the Polycirculant Conjecture. The first main result in this chapter is Theorem 8.1.8 which proves that every vertex-transitive, locally-quasiprimitive graph has a semiregular automorphism. Also we prove Theorem 8.1.11 which determines all elusive biquasiprimitive permutation groups. Recall that all groups and graphs are finite.

8.1 Introduction

A permutation group $G \leq \mathrm{Sym}(\Omega)$ is called *elusive* if G is transitive and contains no non-trivial semiregular subgroups (equivalently, no fixed-point-free elements of prime order). By definition, it is easy to see that any transitive subgroup of an elusive permutation group is also elusive.

We will make extensive use of the following lemma which indicates a fundamental property of elusive groups.

Lemma 8.1.1 [35, Lemma 2.1] *Let G be an elusive permutation group with point stabilizer G_α. Then every conjugacy class of elements of prime order in G intersects G_α non-trivially.*

We will encounter the following elusive permutation groups many times later. For more examples of elusive permutation groups, see [7].

Example 8.1.2 The following are elusive permutation groups, but their 2-closures are not elusive.

1. M_{11} with point stabilizer $\mathrm{PSL}(2, 11)$ is a 3-transitive permutation group of degree 12. This permutation group is elusive by Lemma 8.1.1 and the fact that M_{11} has

only one conjugacy class of elements of order 2 or 3, (see [6]). The 2-closure of M_{11} is the full symmetric group S_{12} since M_{11} is 2-transitive, hence $M_{11}^{(2)}$ is not elusive.

2. The transitive subgroup $M_{10} = A_6 \cdot 2$ (with point stabilizer A_5) of the above permutation group M_{11} with degree 12. This group M_{10} is elusive since it is a transitive subgroup of an elusive permutation group. In this case, the socle $T = A_6$ has two orbits of length 6. Moreover, $T = T_\alpha T_\beta$ where α and β are points in different orbits of T. Hence Wielandt's Dissection Theorem (Theorem 2.4.2) implies that $T^{(2)}$ contains $A_6 \times A_6$, and so $T^{(2)}$ contains many fixed-point-free elements of order 3. Therefore, $M_{10}^{(2)}$ is not elusive.

The next proposition shows that certain product constructions preserve the property of being elusive.

Proposition 8.1.3 [7, Theorem 4.1] *Let* $G_1 \leq \mathrm{Sym}(\Omega_1)$ *be an elusive permutation group on* Ω_1 *and let* $G_2 \leq \mathrm{Sym}(\Omega_2)$ *be an elusive permutation group on* Ω_2 *. Then*

1. $G_1 \times G_2$ *is elusive acting on* $\Omega_1 \times \Omega_2$*.*

2. $G_1 \wr S_k$ *is elusive on* Ω_1^k *in the natural product action.*

Corollary 8.1.4 *Let* $G = M_{11} \wr K$ *acting with its product action on* $\Omega = \Delta^k$ *for some* $k \geq 1$*, where* K *is a subgroup of* S_k *and* $|\Delta| = 12$*. Then the following holds.*

1. G *is elusive on* Ω*.*

2. $G^{(2)}$ *contains the subgroup* $S_{12} \wr K$*, and hence is not elusive.*

3. M_{11}^k *is elusive on* Ω *and* $(M_{11}^k)^{(2)} = S_{12}^k$ *is not elusive.*

Proof. (1) Proposition 8.1.3 (2) and Example 8.1.2 (1) imply that G is elusive on Ω.

(2) The fact that $M_{11}^{(2)} = S_{12}$ and Proposition 2.4.4 imply that $G^{(2)}$ contains the subgroup $S_{12} \wr K$. Thus $G^{(2)}$ contains many fixed-point-free elements of order 3.

(3) Since M_{11}^k is a transitive subgroup of G, M_{11}^k is elusive. Now Proposition 2.4.3 implies that $(M_{11}^k)^{(2)} = S_{12}^k$, and so $(M_{11}^k)^{(2)}$ contains many fixed-point-free elements of prime order 3. □

Giudici [16] has determined all finite elusive permutation groups with at least one transitive minimal normal subgroup. Also he determined all finite elusive almost simple permutation groups.

Theorem 8.1.5 [16, Theorem 1.1] *Let G be an elusive permutation group on a finite set Ω which has at least one transitive minimal normal subgroup. Then $G = M_{11} \wr K$ acting with its product action on $\Omega = \Delta^k$ for some $k \geq 1$, where K is transitive subgroup of S_k and $|\Delta| = 12$.*

Theorem 8.1.6 [16, Theorem 1.4] *Let G be an almost simple group acting elusively on the set Ω. Then G is either M_{11} or $M_{10} = A_6 \cdot 2$ acting on 12 points.*

The following theorem plays a central role in the proof of the above two theorems and in our further proofs as well.

Theorem 8.1.7 [16, Theorem 1.3] *Let T be a simple group with a proper subgroup H which meets every $\mathrm{Aut}(T)$-conjugacy class of elements of T of prime order. Then T is one of $A_6, M_{11}, \mathrm{P}\Omega^+(8,2)$ or $\mathrm{P}\Omega^+(8,3)$, and $H = A_5, \mathrm{PSL}(2,11)$, $\mathrm{P}\Omega(7,2)$ or $\mathrm{P}\Omega(7,3)$, respectively. Furthermore, if H meets every conjugacy class of elements of T of prime order, then $T = M_{11}$ and $H = \mathrm{PSL}(2,11)$.*

Recall that a *semiregular* permutation is a nontrivial permutation whose cycles all have the same length and that the existence of a semiregular permutation is equivalent to the existence of a fixed-point-free permutation of prime order. The Polycirculant Conjecture (Conjecture 1.3.1) states that every transitive 2-closed permutation group contains a semiregular element. This would imply that every vertex-transitive graph has a semiregular automorphism since the full automorphism group of a graph is 2-closed. See Section 2.5 for basic definitions and properties of vertex-transitive graphs. In this chapter we make substantial progress on the Polycirculant Conjecture by proving that every vertex-transitive, locally-quasiprimitive graph has a semiregular automorphism. We prove the following theorem.

Theorem 8.1.8 *Let Γ be a finite graph with a group G of automorphisms such that G is vertex-transitive and locally-quasiprimitive. Then Γ has a semiregular automorphism.*

In view of Example 2.5.4, we have the following corollary.

Corollary 8.1.9 *Every finite arc-transitive graph of prime valency has a semi-regular automorphism. Also every finite 2-arc transitive and vertex-transitive graph has a semiregular automorphism.*

Theorem 8.1.8 also has the following analogue in the 2-closed setting.

Theorem 8.1.10 *Let G be a finite transitive permutation group on Ω and suppose that for $\omega \in \Omega$ there is a self-paired orbit Σ of G_ω on $\Omega\backslash\{\omega\}$ such that G_ω^Σ is quasiprimitive. Then $G^{(2)}$ contains a semiregular permutation.*

An important ingredient in the proof of Theorem 8.1.8 is a determination of all quasiprimitive and biquasiprimitive elusive groups. All quasiprimitive elusive groups were determined in [16] and shown to be of the form $M_{11} \wr K$ acting on 12^k points, for some transitive subgroup K of S_k (Theorem 8.1.5). Recall that a *biquasiprimitive* permutation group is a transitive permutation group for which every nontrivial normal subgroup has at most two orbits and there is some normal subgroup with precisely two orbits. In this chapter we determine all biquasiprimitive elusive groups.

Theorem 8.1.11 *Let G be a finite biquasiprimitive elusive permutation group on Ω and let $\alpha \in \Omega$. Then one of the following holds:*

1. *$G = M_{10}$ and $|\Omega| = 12$;*
2. *$G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ and $G_\alpha \cong \mathrm{PSL}(2,11)^k \rtimes K'$, where $K' \leq K \leq S_k$ such that K is transitive, $|K : K'| = 2$, and $K\backslash K'$ contains no elements of order 2;*
3. *$G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ and $G_\alpha \cong (\mathrm{PSL}(2,11)^{k/2} \times M_{11}^{k/2}) \rtimes K'$, where k is even, $K' \leq K \leq S_k$ such that K is transitive and K' is intransitive, $|K : K'| = 2$ and $K\backslash K'$ contains no elements of order 2.*

Moreover, each group G in (1)-(3) is biquasiprimitive and elusive, G is not 2-closed, and $G^{(2)}$ contains a fixed-point-free element of order 3.

We note that for the examples in Theorem 8.1.11 (2), the unique minimal normal subgroup $N = M_{11}^k$ of G acts faithfully on both its orbits, while in Theorem 8.1.11 (3) the unique minimal normal subgroup $N = M_{11}^k$ of G is unfaithful on each of its orbits

8.2 Some biquasiprimitive elusive groups

8.2.1 The notation for biquasiprimitive elusive groups

First, we fix the notation for discussing biquasiprimitive permutation groups. We adopt the notation used in [46]. Suppose that G is a biquasiprimitive elusive permutation group on a finite set Ω, then there exists a non-trivial intransitive normal subgroup of G which has two orbits, say Δ_1, Δ_2. Thus there is a set Δ such that we can identify Ω with $\Delta \times \{1,2\}$ such that $\Delta_1 = \Delta \times \{1\}$ and $\Delta_2 = \Delta \times \{2\}$. Each element of G either fixes the two orbits setwise or interchanges them. The elements of G which fix Δ_1 and Δ_2 setwise form a subgroup G^+ of index 2, and G^+ induces a transitive permutation group H on Δ. By the embedding theorem for permutation groups, G is conjugate in $\mathrm{Sym}(\Omega)$ to a subgroup of the wreath product $H \wr S_2 = (H \times H) \rtimes S_2$, where for (y_1, y_2) in the base group $H \times H$, and $(12) \in S_2$,

$$(\delta, i)^{(y_1,y_2)} = (\delta^{y_i}, i) \text{ and } (\delta, i)^{(12)} = (\delta, i^{(12)}) \text{ for all } (\delta, i) \in \Omega. \tag{8.1}$$

We write the base group $B = H \times H$ as $B = H_1 \times H_2$ when we wish to distinguish the two direct factors. Note that $G^+ = G \cap B$ and by the definition of H, the group G^+ projects onto H_1 and H_2. Let $g \in G \setminus G^+$. Then $g = (x, y)(12)$ for some $x, y \in H$, and since G^+ projects onto H_2, multiplying g by an element of G^+ if necessary, we may assume that $y = 1$ and $g = (x, 1)(12)$. Hence we may assume that $G = \langle G^+, g\rangle$ where $g = (x, 1)(12)$ for some $x \in H$. Since G is elusive, there is no element of order 2 interchanging Δ_1 and Δ_2 (such an element would be fixed-point-free), and so $o(g) \neq 2$, in particular, $x \neq 1$.

We also need the following notation. Given a group M and $\varphi \in \mathrm{Aut}(M)$, we denote the full diagonal subgroup $\{(a, a^\varphi) \,|\, a \in M\}$ of $M \times M$ by $\mathrm{Diag}_\varphi(M \times M)$. Also, given $G = \langle G^+, g\rangle$ as defined above, for $M \leq H_1$ we define $\mathrm{Diag}_g(M \times M)$ as the full diagonal subgroup $\{(a, a^g) \,|\, a \in M\}$. Moreover, we need the fact that $\mathrm{Aut}(T^k) = \mathrm{Aut}(T) \wr S_k$ when T is a nonabelian simple group.

8.2.2 The examples

According to Theorem 8.1.11, there are three constructions of biquasiprimitive elusive groups. In Example 8.1.2 (2), we have seen that the biquasiprimitive group $M_{10} = A_6 \cdot 2$ acting on 12 points is an elusive group. Next we discuss the other two types given in Theorem 8.1.11. The notation is as in Subsection 8.2.1.

The following lemma concerns the second family of examples in Theorem 8.1.11.

Lemma 8.2.1 *Let $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$, where K is a transitive subgroup of S_k acting naturally on the k simple direct factors of M_{11}^k. Suppose that K contains an index 2 subgroup K' such that $K \backslash K'$ contains no elements of order 2 and let $L = \mathrm{PSL}(2, 11)^k \rtimes K'$. Then the action of G on the set of right cosets of L in G is faithful, biquasiprimitive and elusive of degree $2 \cdot (12)^k$.*

Proof. Let Ω be the set of right cosets of L in G and let N be the unique minimal normal subgroup of G. Then $N = M_{11}^k$ and $LN = M_{11}^k \rtimes K'$. Let $G^+ = LN$. Then $|G : G^+| = 2$ and so N has two orbits Δ_1 and Δ_2 on Ω, each of size 12^k. Hence every normal subgroup of G has at most two orbits on Ω and so G is a biquasiprimitive permutation group of degree $2 \cdot (12)^k$.

By Corollary 8.1.4 (1), each element of prime order in $G^+ = M_{11} \wr K'$ fixes some point of Δ_1. Since $K \setminus K'$ contains no elements of order 2, $G \setminus G^+$ contains no elements of order 2 and hence contains no elements of prime order. Thus G is elusive on Ω. $\square$

One example of (k, K, K') which satisfies the conditions of Lemma 8.2.1 is $k = 4$, $K = \langle(1234)\rangle$ and $K' = \langle(13)(24)\rangle$. Another example of (k, K, K') in this case is $k = 5$, $K = Z_5 \rtimes Z_4 = \mathrm{AGL}(1,5)$ and $K' = Z_5 \rtimes Z_2 \cong D_{10}$. Note that there is no requirement of transitivity for K'.

Next we look at the 2-closure of G when G is of the above type.

Lemma 8.2.2 *Suppose $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ is a biquasiprimitive elusive group given by Lemma 8.2.1. Then the 2-closure of G contains a fixed-point-free element of order 3.*

Proof. With the notation in Subsection 8.2.1, we may identify $\Omega = [G : L]$ with $\Delta \times \{1, 2\}$ where $\Delta \times \{i\} = \Delta_i$. Let $N = M_{11}^k$. We observe that N acts faithfully on each Δ_i. Let $M = N^{\Delta_1} \cong N$. Then $N = \mathrm{Diag}_\varphi(M \times M)$ where $\varphi = (\tau_1, ..., \tau_k).\sigma \in \mathrm{Aut}(M)$ for some $\tau_i \in M_{11}$ and $\sigma \in S_k$, and N acts on $\Omega = \Delta \times \{1, 2\}$ via $(\delta, 1)^{(g, g^\varphi)} = (\delta^g, 1)$ and $(\delta, 2)^{(g, g^\varphi)} = (\delta^{g^\varphi}, 2)$. Also note that $M = M_{11}^k$ induces a product action on Δ with $\Delta = \Phi^k$ where $\Phi = [M_{11} : \mathrm{PSL}(2, 11)]$ and $|\Phi| = 12$. First we look at the orbits of $N = \mathrm{Diag}_\varphi(M \times M)$ on the set $\Omega \times \Omega$ and see that they are of the following form.

1. $\{((\alpha, 1), (\beta, 1)) : (\alpha, \beta) \in \mathcal{O}\}$, for each orbit $\mathcal{O}$ of M on $\Delta \times \Delta$.

2. $\{((\alpha, 2), (\beta, 2)) : (\alpha, \beta) \in \mathcal{O}\}$, for each orbit $\mathcal{O}$ of M on $\Delta \times \Delta$.

3. $\{((\alpha, 1), (\beta, 2)) : (\alpha, \beta) \in \mathcal{O}'_{\gamma,\delta}\}$ for some $\gamma, \delta \in \Delta$ where $\mathcal{O}'_{\gamma,\delta} = \{(\gamma^g, \delta^{g^\varphi}) : g \in M\}$.

4. $\{((\beta, 2), (\alpha, 1)) : (\alpha, \beta) \in \mathcal{O}'_{\gamma,\delta}\}$ for some $\gamma, \delta \in \Delta$ where $\mathcal{O}'_{\gamma,\delta} = \{(\gamma^g, \delta^{g^\varphi}) : g \in M\}$.

Since $\Delta = \Phi^k$, we write the points $\alpha = (\alpha_1, ..., \alpha_k)$ and $\beta = (\beta_1, ..., \beta_k)$ where $\alpha_i, \beta_i \in \Phi$. By Corollary 8.1.4 (3), the 2-closure of the product action $M = M_{11}^k$ on $\Delta = \Phi^k$ is S_{12}^k. Let $y \in S_{12}$ be a fixed-point-free element of order 3 on Φ. Recall that $\varphi = (\tau_1, ..., \tau_k).\sigma$. Consider $h = ((y, 1, ..., 1), (y^{\tau_1}, 1, ..., 1)^\sigma) \in \mathrm{Diag}_\varphi(S_{12}^k \times S_{12}^k)$ acting on $\Delta \times \{1, 2\}$. We will show that h preserves N-orbits on ordered pairs, and hence h is a fixed-point-free element of order 3 in $N^{(2)}$ on Ω. By Lemma 2.4.1 (2), $G^{(2)} \geq N^{(2)}$, and hence $G^{(2)}$ also contains a fixed-point-free element of order 3 on Ω.

Since $M^{(2)} = S_{12}^k$, it is easy to see that h preserves N-orbits of the types 1 and 2. So we only need to check that h preserves N-orbits of type 3. (Note that the same argument will apply to the N-orbits of type 4.) Recall that $\varphi = (\tau_1, ..., \tau_k).\sigma$ for $\sigma \in S_k$, and for convenience, write τ_1 as τ. Suppose $1^\sigma = i$, then

$$h = ((y, 1, ..., 1), (1, ..., 1, y^\tau, 1, ..., 1)) \text{ where } y^\tau \text{ is at the } i^{\text{th}} \text{ component.}$$

Thus we only need to consider the action induced by the product action on the first component of Δ_1 and the i^{th} component of Δ_2. Then since we are only considering elements which act componentwise on Φ^k we may assume that $k = 1$, that is, $\Delta = \Phi$. Let $\gamma, \delta \in \Delta$ and

$$\Sigma = (\gamma, \delta)^{\{(g, g^\tau) \,|\, g \in M_{11}\}} = (\gamma, \delta)^{\text{Diag}_\tau(M_{11} \times M_{11})}.$$

Then Σ gives rise to an orbit of type 3. Let $(\alpha, \beta) \in \Sigma$, that is,

$$(\alpha, \beta) = (\gamma, \delta)^{(g_1, g_1^\tau)} \text{ for some } g_1 \in M_{11}.$$

Applying $h = (y, y^\tau)$ to (α, β), we have

$$(\alpha, \beta)^{(y, y^\tau)} = (\gamma^{g_1 y}, \delta^{\tau^{-1} g_1 y \tau}).$$

Then since $S_{12} \leq M_{11}^{(2)}$, (y, y) preserves the set

$$(\gamma, \delta^{\tau^{-1}})^{\{(g, g) \,|\, g \in M_{11}\}},$$

and so there exists some $g_2 \in M_{11}$, such that

$$(\alpha, \beta)^{(y, y^\tau)} = (\gamma^{g_2}, \delta^{\tau^{-1} g_2 \tau}) \in \Sigma.$$

Thus orbits of type 3 are fixed setwise by h, and hence h is a fixed-point-free element of order 3 in $G^{(2)}$. □

Finally, we look at the last family of examples described in Theorem 8.1.11.

Lemma 8.2.3 *Let $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$, where K is a transitive subgroup of S_k acting naturally on the k simple direct factors of M_{11}^k and k even. Suppose that K has an intransitive index 2 subgroup K' such that $K \setminus K'$ contains no elements of order 2 and let $L = (\mathrm{PSL}(2, 11)^{k/2} \times M_{11}^{k/2}) \rtimes K'$. Then the action of G on the set of right cosets of L in G is faithful, biquasiprimitive and elusive of degree $2 \cdot (12)^{k/2}$.*

Proof. Let Ω be the set of right cosets of L in G and let N be the unique minimal normal subgroup of G. Then $N = M_{11}^k$ and $LN = M_{11}^k \rtimes K'$. Let $G^+ = LN$. Then $|G : G^+| = 2$ and so N has two orbits Δ_1 and Δ_2 on Ω. Hence every normal subgroup of G has at most two orbits on Ω and so G is a biquasiprimitive permutation group of degree $2 \cdot (12)^{k/2}$.

By Corollary 8.1.4 (1), each element of prime order in $G^+ = M_{11} \wr K'$ fixes some point of Δ_1. Since $K \setminus K'$ contains no elements of order 2, $G \setminus G^+$ contains no elements of order 2 and hence contains no elements of prime order. Thus G is elusive on Ω. □

One example of (k, K, K') which satisfies the conditions of Lemma 8.2.3 is $k = 4$, $K = \langle(1234)\rangle$ and $K' = \langle(13)(24)\rangle$. The following lemma concerns the 2-closure of G when G is as in Lemma 8.2.3.

Lemma 8.2.4 *Suppose $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ is a biquasiprimitive elusive group given by Lemma 8.2.3. Then $G^{(2)}$ contains a fixed-point-free element of order* 3.

Proof. With the notation in Subsection 8.2.1, we may identify $\Omega = [G : L]$ with $\Delta \times \{1, 2\}$ where $\Delta \times \{i\} = \Delta_i$. Let $N = M_{11}^k$ and write $N = M_1 \times M_2$, where $M_i \cong M_{11}^{k/2}$ for $i = 1, 2$. Thus identify $L = (\mathrm{PSL}(2, 11)^{k/2} \times M_{11}^{k/2}) \rtimes K' = (\mathrm{PSL}(2, 11)^{k/2} \times M_2) \rtimes K'$ where $\mathrm{PSL}(2, 11)^{k/2} \leq M_1$. We observe that $N = M_1 \times M_2$ acts in a natural way on $\Omega = \Delta \times \{1, 2\}$, that is, $(\delta, i)^{(g_1, g_2)} = (\delta^{g_i}, i)$ for $i = 1, 2$, $\delta \in \Delta$ and $(g_1, g_2) \in M_1 \times M_2$. Moreover each M_i induces a faithful product action on $\Delta_i = \Delta \times \{i\}$, that is, $\Delta = \Phi^{k/2}$ where $\Phi = [M_{11} : \mathrm{PSL}(2, 11)]$ and $|\Delta_i| = 12^{k/2}$. Then for each i, $M_i \cong N^{\Delta_i}$ and so $M := N^{\Delta_1} \cong M_{11}^{k/2}$.

First we look at the orbits of N on the set $\Omega \times \Omega$ and see that they are of the following form.

1. $\{((\alpha, 1), (\beta, 1)) : (\alpha, \beta) \in \mathcal{O}, \}$ for each orbit $\mathcal{O}$ of M on $\Delta \times \Delta$.
2. $\{((\alpha, 2), (\beta, 2)) : (\alpha, \beta) \in \mathcal{O}, \}$ for each orbit $\mathcal{O}$ of M on $\Delta \times \Delta$.
3. $\{((\alpha, 1), (\beta, 2)) : (\alpha, \beta) \in \Delta \times \Delta\}$.
4. $\{((\beta, 2), (\alpha, 1)) : (\beta, \alpha) \in \Delta \times \Delta\}$.

By Corollary 8.1.4 (3), the 2-closure of the product action $M = M_{11}^{k/2}$ on $\Delta = \Phi^{k/2}$ is $S_{12}^{k/2}$. Let $h = (g_1, g_2) \in S_{12}^{k/2} \times S_{12}^{k/2}$. Then h acts on Ω by $(\delta, i)^h = (\delta^{g_i}, i)$. Moreover, h fixes each orbit of N on $\Omega \times \Omega$ and so $S_{12}^k \leq N^{(2)} \leq G^{(2)}$. Thus $G^{(2)}$ contains many fixed-point-free elements of prime order, in particular, a fixed-point-free element of order 3. □

8.3 Determining all biquasiprimitive elusive groups

Throughout this section, we keep using the notation fixed in Subsection 8.2.1. Our analysis in this section follows that given in Praeger's paper [46] and that of Giudici's thesis [15]. Let G be a biquasiprimitive elusive group, and let Δ_1, Δ_2 be the two orbits of G^+.

Lemma 8.3.1 *Let G be an elusive biquasiprimitive permutation group and let N be a minimal normal subgroup of G. Then $N \leq G^+$.*

Proof. Since N is a minimal normal subgroup of G, either $N \leq G^+$ or $N \cap G^+ = 1$. If $N \cap G^+ = 1$, then $G = G^+ \times N$ where $N = \langle g \rangle$ and g is an element of order 2 interchanging Δ_1 and Δ_2, which is not the case since G is elusive. Thus $N \leq G^+$. □

8.3.1 The case where G^+ acts faithfully on both orbits

In this subsection, we consider the case where G^+ acts faithfully on each orbit Δ_i for $i = 1, 2$.

Lemma 8.3.2 *Let G be an elusive biquasiprimitive group and suppose G^+ acts faithfully on both orbits Δ_i. Then G has a unique minimal normal subgroup N. Moreover, $N \cong T^k$ for some nonabelian simple group T.*

Proof. Let N and M be distinct minimal normal subgroups of G. By Lemma 8.3.1, we have $N, M \leq G^+$ and so $N^{\Delta_1}, M^{\Delta_1} \lhd (G^+)^{\Delta_1}$. Since $N \cap M = 1$ and G^+ is faithful on Δ_1, it follows that $N^{\Delta_1} \cong N$ and $M^{\Delta_1} \cong M$, and we have $N^{\Delta_1} \cap M^{\Delta_1} = 1$. Also the biquasiprimitivity of G implies that N^{Δ_1} and M^{Δ_1} are transitive. Thus by Theorem 2.3.1, N^{Δ_1} and M^{Δ_1} are regular. The same argument shows that N^{Δ_2} and M^{Δ_2} are regular. Then as both N and M are faithful on Δ_1 and Δ_2 it follows that N is semiregular, contradicting G being elusive. Thus G has a unique minimal normal subgroup. Suppose now that N is abelian. Then N^{Δ_1} and N^{Δ_2} are regular by Proposition 2.1.3, and so N is semiregular on Ω. This contradicts G being elusive and so $N \cong T^k$ for some nonabelian simple group T. □

Let $N \cong T^k$ be the minimal normal subgroup of G. We denote T_j to be the j^{th} simple direct factor of N and write $N = T_1 \times \cdots \times T_k$ where each $T_j \cong T$. Let $\alpha \in \Delta_1$ and let N_α be the stabilizer in N of α. We will first determine N and N_α. For each $j \in \{1, ..., k\}$, let $\pi_j : N \to T_j$ denote the projection onto the j^{th} simple direct factor of N, and let

$$N_j := N_\alpha \cap T_j.$$

Then $N_j \trianglelefteq N_\alpha$, and hence

$$N_j \cong \pi_j(N_j) \trianglelefteq \pi_j(N_\alpha), \quad \text{for each } j. \tag{$*$}$$

The next lemma proved in [15] by Giudici is true for all elusive groups.

Lemma 8.3.3 [15, Lemma 4.5.1] *Let G be an elusive group on a set Ω and let N be a normal subgroup of G such that $N \cong T^k$ for some non-abelian simple group T. Let $\alpha \in \Omega$. Then for each $j \in \{1, ..., k\}$, the projection $\pi_j(N_\alpha)$ either equals T_j or is a proper subgroup of T_j which meets every $\mathrm{Aut}(T_j)$-conjugacy class of elements of T_j of prime order.*

Proof. Suppose that there exists $j \in \{1, \ldots, k\}$ such that $\pi_j(N_\alpha) \neq T_j$. For each $\mathrm{Aut}(T)$-conjugacy class C of elements of prime order in T, the set

$$\overline{C} = \{(t_1, \ldots, t_k) : t_i \in C\}$$

is an $\mathrm{Aut}(N)$-conjugacy class of elements of prime order in N. Then as G is elusive, $\overline{C} \cap N_\alpha \neq \varnothing$. Hence the projection $\pi_j(N_\alpha)$ is a proper subgroup of T_j which meets every $\mathrm{Aut}(T_j)$-conjugacy class of elements of T_j of prime order. □

Lemma 8.3.4 *Let G be a biquasiprimitive elusive group such that G^+ is faithful on both orbits, and let N be the unique minimal normal subgroup of G. With the notation preceding Lemma 8.3.3, there exists at least one $i \in \{1, ..., k\}$ such that $\pi_i(N_\alpha)$ is a proper subgroup of T_i which meets every $\mathrm{Aut}(T_i)$-conjugacy class of T_i. In addition,*

1. *$T = A_6, M_{11}, \mathrm{P}\Omega^+(8, 2)$ or $\mathrm{P}\Omega^+(8, 3)$, and $\pi_i(N_\alpha) \cong A_5, \mathrm{PSL}(2, 11)$, $\mathrm{P}\Omega(7, 2)$ or $\mathrm{P}\Omega(7, 3)$, respectively. In particular, $\pi_i(N_\alpha)$ is a nonabelian simple group.*
2. *$N_i \cong \pi_i(N_\alpha)$.*

Proof. (1) Since G^+ is faithful on Δ_1, $N \leq G^+$ (by Lemma 8.3.1) is faithful on Δ_1, and hence N_α does not contain any of the simple direct factors of N. Now let $t \in T$ have prime order, then $(t, 1, ..., 1) \in N$ has prime order. Let C be the G-conjugacy class of the prime order element $(t, 1, ..., 1)$. Since G is elusive and $C \subset N$, we have $C \cap N_\alpha \neq \varnothing$. Thus, there exists $i \in \{1, ..., k\}$ such that $N_i \neq 1$, and hence $\pi_i(N_i) \neq 1$. Since T is simple and N_α does not contain any of the simple direct factors of N, together with $(*)$, we have $\pi_i(N_\alpha)$ is a proper subgroup of T. By Lemma 8.3.3, $\pi_i(N_\alpha)$ meets every $\mathrm{Aut}(T)$-conjugacy class of elements of prime order in T. By Theorem 8.1.7, we have $T = A_6, M_{11}, \mathrm{P}\Omega^+(8, 2)$ or $\mathrm{P}\Omega^+(8, 3)$, and $\pi_i(N_\alpha) \cong A_5, \mathrm{PSL}(2, 11), \mathrm{P}\Omega(7, 2)$ or $\mathrm{P}\Omega(7, 3)$, respectively.

(2) Note that $\pi_i(N_\alpha)$ is simple. Hence $(*)$ and the fact that $\pi_i(N_i) \neq 1$ imply that $N_i \cong \pi_i(N_\alpha)$. □

Lemma 8.3.5 *Suppose G is an elusive biquasiprimitive group and G^+ acts faithfully on its two orbits. Let N be the unique minimal normal subgroup of G and suppose that $N \cong T^k$ for some nonabelian simple group T. Then for each $\alpha \in \Omega$, we have*

$N_\alpha \cong R^k$, where (T, R) is one of (A_6, A_5), $(M_{11}, \mathrm{PSL}(2, 11))$, $(\mathrm{P}\Omega^+(8, 2), \mathrm{P}\Omega(7, 2))$ or $(\mathrm{P}\Omega^+(8, 3), \mathrm{P}\Omega(7, 3))$.

Proof. By Lemma 8.3.4, we have that $N = T_1 \times \cdots \times T_k$ where each $T_i \cong T \in \{A_6, M_{11}, \mathrm{P}\Omega^+(8, 2), \mathrm{P}\Omega^+(8, 3)\}$. Without loss of generality, we may suppose $\alpha \in \Delta_1$. Since N is transitive on Δ_1, we have $G^+ = NG_\alpha$. Also since N is a minimal normal subgroup of G, G acts transitively by conjugation on the set of k simple direct factors of N. Note that G^+ is an index 2 subgroup of G, hence G^+ either acts transitively or has two equal length orbits on the set of k simple direct factors of N.

First we suppose that G^+ is transitive on the set of k simple direct factors of N. Since $G^+ = NG_\alpha$, G_α is also transitive on the set of k simple direct factors of N. So for each $i, j \in \{1, ..., k\}$, we have $\pi_i(N_\alpha) \cong \pi_j(N_\alpha)$. By Lemma 8.3.4, $\pi_j(N_\alpha) \neq T_j$ for each j. Moreover, by Lemma 8.3.4 (2), we have $N_j = N_\alpha \cap T_j \cong \pi_j(N_\alpha)$ for each j. Hence $N_\alpha = N_1 \times \cdots \times N_k \cong R^k$ where (T, R) is one of (A_6, A_5), $(M_{11}, \mathrm{PSL}(2, 11))$, $(\mathrm{P}\Omega^+(8, 2), \mathrm{P}\Omega(7, 2))$ or $(\mathrm{P}\Omega^+(8, 3), \mathrm{P}\Omega(7, 3))$. The result holds in this case.

Secondly we suppose that G^+, and hence G_α, have two orbits, say, $\mathcal{O}_1 = \{T_1, ..., T_{k/2}\}$ and $\mathcal{O}_2 = \{T_{(k/2)+1}, ..., T_k\}$ on the set of k simple direct factors of N. Thus, $\pi_i(N_\alpha) \cong \pi_j(N_\alpha)$ if $i, j \in \{1, ..., k/2\}$ or $i, j \in \{(k/2) + 1, ..., k\}$. By Lemma 8.3.4, there exists i such that $\pi_i(N_\alpha) \neq T_i$ and $N_i = N_\alpha \cap T_i \cong \pi_i(N_\alpha)$. Moreover $\pi_i(N_\alpha)$ is determined by T. Without loss of generality, we may assume $T_i \in \mathcal{O}_1$. Then as G_α is transitive on $\mathcal{O}_1$, it follows that $N_1 \times \cdots \times N_{k/2} \leq N_\alpha$ and $N_1 \times \cdots \times N_{k/2} \cong R^{k/2}$ where (T, R) is one of (A_6, A_5), $(M_{11}, \mathrm{PSL}(2, 11))$, $(\mathrm{P}\Omega^+(8, 2), \mathrm{P}\Omega(7, 2))$ or $(\mathrm{P}\Omega^+(8, 3), \mathrm{P}\Omega(7, 3))$. Moreover, by Lemma 8.3.3, for each $j \in \{(k/2) + 1, ..., k\}$, either $\pi_j(N_\alpha) \cong R$ or $\pi_j(N_\alpha) = T_j$. Let $t \in T$ have prime order, and let C be the G-conjugacy class of the prime order element $(t, 1, ..., 1, t)$. Note that $C \cap N_\alpha \neq \varnothing$. Since G preserves the partition $\{\mathcal{O}_1, \mathcal{O}_2\}$ of $\{T_1, ..., T_k\}$, every element of C has precisely one nontrivial coordinate in $\mathcal{O}_1$ and precisely one nontrivial coordinate in $\mathcal{O}_2$. Thus, as $N_1 \times \cdots \times N_{k/2} \leq N_\alpha$ and for each $i \in \{1, ..., k/2\}$ we have $\pi_i(N_\alpha) \cong N_i$, it follows that there exists $j \in \{1 + (k/2), ..., k\}$ such that $N_j \neq 1$. By $(*)$, $1 \neq \pi_j(N_j) \trianglelefteq \pi_j(N_\alpha)$. However, T and R are simple. Hence $N_j \cong T$ or R. But N_α does not contain any of the simple direct factors of N (as N is faithful on Δ_1), so $\pi_j(N_\alpha) \cong R$ and $N_j \cong R$. Since G_α is transitive on $\mathcal{O}_2$, it follows that $N_\alpha \cong R^k$. Thus the assertion holds in this case too. □

Finally, we determine all biquasiprimitive elusive groups G where G^+ acts faithfully on both orbits.

Proposition 8.3.6 *Suppose that G is an elusive biquasiprimitive group, and G^+ acts* *faithfully on both orbits. Let N be a minimal normal subgroup of G. Then $N \cong T^k$ where $T = M_{11}$ or A_6. Moreover, if $T = A_6$, then $G = M_{10}$ acting on 12 points.*

Proof. By Lemma 8.3.4, $N \cong T^k$ where $T = A_6, M_{11}, \mathrm{P}\Omega^+(8,2)$ or $\mathrm{P}\Omega^+(8,3)$. Moreover, by Lemma 8.3.2, N is the unique minimal normal subgroup of G and so $C_G(N) = 1$. Thus $G \leq \mathrm{Aut}(N) = \mathrm{Aut}(T) \wr S_k$. Let $\alpha \in \Omega$. Then by Lemma 8.3.5, $N_\alpha \cong R^k$ where $R = A_5, \mathrm{PSL}(2,11)$, $\mathrm{P}\Omega(7,2)$ or $\mathrm{P}\Omega(7,3)$, respectively.

With the notation in Subsection 8.2.1, since G^+ acts faithfully on both orbits Δ_1 and Δ_2, $G^+ = \mathrm{Diag}_\varphi(H \times H)$ where $H = (G^+)^{\Delta_1}$ and $\varphi \in \mathrm{Aut}(H)$. Identifing $\Omega = \Delta \times \{1,2\}$, the action of G is given by (8.1) (see Subsection 8.2.1). Let $M = N^{\Delta_1} \lhd H$. Then $M \cong T^k$. Since $C_G(N) = 1$, φ induces a nontrivial automorphism of M, and so we also write $N = \mathrm{Diag}_\varphi(M \times M)$ where $\varphi \in \mathrm{Aut}(M)$. Note that, when $T = A_6$, there are two conjugacy classes of subgroups isomorphic to A_5; when $T = M_{11}$, there is one conjugacy class of subgroups isomorphic to $\mathrm{PSL}(2,11)$; when $T = \mathrm{P}\Omega^+(8,2)$, there are three conjugacy classes of subgroups isomorphic to $\mathrm{P}\Omega(7,2)$; while when $T = \mathrm{P}\Omega^+(8,3)$, there are six conjugacy classes of subgroups isomorphic to $\mathrm{P}\Omega(7,3)$. However, in all cases there is a unique class of subgroups isomorphic to R under $\mathrm{Aut}(T)$. Hence the stabilizer of a point in N^{Δ_1} is conjugate under $\mathrm{Aut}(N)$ to R^k. By Lemma 2.1.8 we may assume $N^{\Delta_1} = M = T^k$, with point stabilizer $M_\alpha = R^k$, acting on $\Delta_1 = \Phi^k$ with $|\Phi| = |T : R|$ as a natural product action.

First we suppose that $T = A_6$, then $|\Phi| = 6$. There are two conjugacy classes of elements of order 3 in A_6, one with cycle structure 3^2, another with cycle structure 3.1^3. They are interchanged by an outer automorphism of S_6. Let $y \in A_6$ with cycle structure 3^2, let $z \in A_6$ with cycle structure 3.1^3. For each $j \in \{1,...,k\}$, consider an element $h_j \in N$ of order 3 where $h_j^{\Delta_1} = (1,...,1,y_j,1,...,1)$ such that $y_j \in T_j$ has cycle structure 3^2 and T_j is the j^{th} direct factor of M. Then

$$h_j = ((1,...,1,y_j,1,...,1),(1,...,1,y_j,1,...,1)^\varphi).$$

Since $h_j^{\Delta_1}$ is fixed-point-free on Δ_1 and G is elusive, we have $(1,...,1,y_j,1,...,1)^\varphi$ must have a fixed point on Δ_2. This means $\varphi = (\tau_1,...,\tau_k).\sigma$ where each $\tau_i \in \mathrm{Aut}(A_6)$ interchanges the two conjugacy classes of elements of order 3 in T, and $\sigma \in S_k$. Now if $k \geq 2$, consider the following element of order 3,

$$h = ((y,z,1,...,1),(y,z,1,...,1)^\varphi).$$

It is easy to see that h is fixed-point-free on Ω. Hence $k = 1$, and G is almost simple. By [16, Page 83], $G = M_{10}$ acting on 12 points.

Next suppose that $T = \mathrm{P\Omega}^+(8,2)$ or $\mathrm{P\Omega}^+(8,3)$, then by Lemma 8.3.4, $R = \mathrm{P\Omega}(7,2)$ or $\mathrm{P\Omega}(7,3)$. There are three conjugacy classes of elements of order 5 in T. Using the permutation characters and character tables in [6, pp.85-87, pp.136-140], we see that precisely two of the conjugacy classes do not meet R. Thus, given $\varphi \in \mathrm{Aut}(T^k)$, say, $\varphi = (\tau_1, ..., \tau_k).\sigma$, for $\tau_i \in \mathrm{Aut}(T)$ and $\sigma \in S_k$, we can find two elements y_1, y_2 of order 5, such that $y_1^{\tau_1} = y_2$, and the conjugacy classes of y_1 and y_2 do not meet R. Thus

$$h = ((y_1, 1, ..., 1), (y_1, 1, ..., 1)^{\varphi})$$

is a fixed-point-free element of order 5 in N, which is a contradiction. Thus T cannot be $\mathrm{P\Omega}^+(8,2)$ or $\mathrm{P\Omega}^+(8,3)$.

The proof is now complete. □

This leaves us the final case where $T = M_{11}$ and the unique minimal normal subgroup $N \cong T^k$ for $k \geq 1$.

Lemma 8.3.7 *Suppose that G is an elusive biquasiprimitive group on Ω, and G^+ acts faithfully on both orbits. Let N be a minimal normal subgroup of G with $N \cong M_{11}^k$. Then G is given by Lemma 8.2.1, that is, G satisfies:*

(1) $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ where $K \leq S_k$ acts transitively by permuting the k simple direct factors of M_{11}^k.

(2) $G^+ = M_{11}^k \rtimes K'$ where $|K : K'| = 2$ and $K \setminus K'$ contains no elements of order 2.

(3) For $\alpha \in \Omega$, $G_\alpha \cong \mathrm{PSL}(2,11)^k \rtimes K'$, and $|\Omega| = 2 \cdot 12^k$.

Proof. By Lemma 8.3.2, N is the unique minimal normal subgroup of G. Hence $C_G(N) = 1$, and so $G \leq \mathrm{Aut}(N) = M_{11}^k \rtimes S_k$ where the top group S_k acts by permuting the k simple direct factors of N. That is, there exists a subgroup $K \leq S_k$ such that $G = M_{11}^k \rtimes K$. Since N is a minimal normal subgroup, K is transitive on the set of k simple direct factors. Thus condition (1) holds.

By Lemma 8.3.1, $N \leq G^+$, and so $G^+ = M_{11}^k \rtimes K'$ where $|K : K'| = 2$. Since G is elusive, $G \setminus G^+$ contains no elements of order 2. Hence $K \setminus K'$ contains no elements of order 2. Thus condition (2) holds.

The biquasiprimitivity implies that N and G^+ have the same two orbits. By Lemma 8.3.5, we have $N_\alpha \cong \mathrm{PSL}(2,11)^k$. Thus N induces a product action on each orbit and $|\Omega| = 2 \cdot 12^k$. Now conditions (1) and (2) imply that $G_\alpha = \mathrm{PSL}(2,11)^k \rtimes K' \leq G^+$, so condition (3) holds and the proof is complete. □

8.3.2 The case where G^+ is not faithful on its orbits.

Lemma 8.3.8 *Let G be a biquasiprimitive elusive group acting on a set Ω such that G^+ does not act faithfully on at least one of its orbits. Then G has a unique minimal normal subgroup N. Moreover $N \cong M_{11}^k$ with k even and for $\alpha \in \Omega$, we have $N_\alpha \cong \mathrm{PSL}(2,11)^{k/2} \times M_{11}^{k/2}$ and $|\Omega| = 2 \cdot 12^{k/2}$.*

Proof. Denote the two orbits of G^+ on Ω by Δ_1 and Δ_2. For $i = 1, 2$, let K_i be the kernel of the action of G^+ on Δ_i. Then K_1 acts faithfully on Δ_2 and K_2 acts faithfully on Δ_1, and at least one of K_1, K_2 is nontrivial. Moreover, each $g \in G \setminus G^+$ interchanges K_1 and K_2, and so $K_1 \times K_2 \lhd G$. In particular, $K_1 \cong K_2 \neq 1$. By the biquasiprimitivity of G it follows that K_1 is transitive on Δ_2 and K_2 is transitive on Δ_1. Now $K_1 \lhd G^+$ and so contains a minimal normal subgroup M_1 of G^+. Then for any $g \in G \setminus G^+$, $M_1^g \leq K_2$ and $M_1^g \lhd G^+$. Moreover $g^2 \in G^+$ and hence normalizes M_1, so $(M_1^g)^g = M_1$. Hence $N := M_1 \times M_1^g$ is a minimal normal subgroup of G and by the biquasiprimitivity of G it follows that M_1 is transitive on Δ_2 and M_1^g is transitive on Δ_1. Suppose M_1 contains an element h of prime order which is fixed-point-free on Δ_2. Then h^g is fixed-point-free on Δ_1, and hence $(h, h^g) \in N$ is fixed-point-free on Ω. As G is elusive, it follows that M_1 is elusive on Δ_2. Hence by [16, Proposition 2.1], $M_1 \cong M_{11}^{k/2}$ for some even integer k and for $\alpha \in \Delta_2$, $(M_1)_\alpha \cong \mathrm{PSL}(2,11)^{k/2}$. Hence $|\Delta_2| = 12^{k/2}$. It follows that $N \cong M_{11}^k$, $|\Omega| = 2 \cdot 12^{k/2}$ and for all $\alpha \in \Omega$, $N_\alpha \cong \mathrm{PSL}(2,11)^{k/2} \times M_{11}^{k/2}$.

Moreover, for $\alpha \in \Delta_2$, we have that $(M_1)_\alpha$ is self normalizing in M_1. Thus by Theorem 2.3.1, $C_{\mathrm{Sym}(\Delta_2)}(M_1) = 1$ and so $\mathrm{soc}((G^+)^{\Delta_2}) = M_1$. Let $H = (G^+)^{\Delta_2}$. Then by [46, Lemma 3.2], $\mathrm{soc}(G) \leq \mathrm{soc}(H) \times \mathrm{soc}(H)$. Hence G has a unique minimal normal subgroup $N = M_1 \times M_1^g$ as asserted. $\square$

Finally we determine all biquasiprimitive elusive groups G where G^+ does not act faithfully on at least one of its orbits.

Lemma 8.3.9 *Suppose G is a biquasiprimitive elusive group on Ω and G^+ does not act faithfully on at least one of its orbits. Then G is as given by Lemma 8.2.3, that is, G satisfies the following conditions.*

(1) $G = M_{11}^k \rtimes K \leq M_{11} \wr S_k$ *where* $K \leq S_k$ *is transitive.*

(2) $G^+ = M_{11}^k \rtimes K'$ *where* $|K : K'| = 2$, *and* K' *is intransitive. Moreover there are no elements of order* 2 *in* $K \setminus K'$.

(3) For any $\alpha \in \Omega$, *we have* $G_\alpha \cong (\mathrm{PSL}(2,11)^{k/2} \times M_{11}^{k/2}) \rtimes K'$ *and* $|\Omega| = 2 \cdot 12^{k/2}$.

Proof. By Lemma 8.3.8, $\mathrm{soc}(G) = M_{11}^k$ is the unique minimal normal subgroup of G, and hence we have condition (1) satisfied. Now G^+ is an index 2 subgroup of G, so we have $G^+ = M_{11}^k \rtimes K'$ and $|K : K'| = 2$. By the proof of Lemma 8.3.8, G^+ has at least two minimal normal subgroups, and so K' is intransitive. Also, since G is elusive, $G \setminus G^+$ contains no elements of order 2, and so $K \setminus K'$ contains no elements of order 2. Finally, by Lemma 8.3.8, $|\Omega| = 2 \cdot 12^{k/2}$ and hence $G_\alpha \cong (\mathrm{PSL}(2, 11)^{k/2} \times M_{11}^{k/2}) \rtimes K'$. □

Now we are ready to prove Theorem 8.1.11.

Proof of Theorem 8.1.11: First note that by Example 8.1.2 (2), Lemma 8.2.1 and Lemma 8.2.3, each group G in (1)-(3) is biquasiprimitive and elusive. Now let G be a biquasiprimitive elusive permutation group on Ω. Suppose first that G^+ is faithful on its orbits. Then by Proposition 8.3.6 and Lemma 8.3.7, either $G = M_{10}$ acting on 12 points or G is of the type given in Lemma 8.2.1. In the first case, Example 8.1.2 (2) shows that $M_{10}^{(2)}$ contains $A_6 \times A_6$, and hence contains a fixed-point-free element of order 3. In the latter case, by Lemma 8.2.2, $G^{(2)}$ contains a fixed-point-free element of order 3. Next we suppose that G^+ is not faithful on at least one of its orbits. By Lemma 8.3.9, G is as in Lemma 8.2.3. Then by Lemma 8.2.4, $G^{(2)}$ contains a fixed-point-free element of order 3. The proof is complete. □

8.4 Proofs of Theorems 8.1.8 and 8.1.10

Finally we prove Theorems 8.1.8 and 8.1.10, finishing this chapter.

Proof of Theorem 8.1.8: We may assume that Γ is connected. First suppose that there exists a non-trivial normal subgroup N of G such that N has at least 3 orbits on the vertex set $V\Gamma$ of the graph Γ. By Theorem 2.5.5, N is semiregular on $V\Gamma$ and so contains fixed-point-free elements of prime order. Next suppose that every non-trivial normal subgroup is transitive on $V\Gamma$. Then G is quasiprimitive on $V\Gamma$. So by Theorem 8.1.5, either G contains a fixed-point-free element of prime order or $|V\Gamma| = 12^k$ and $G = M_{11} \wr K$ for some transitive subgroup $K \leq S_k$. In the latter case, by Corollary 8.1.4, the 2-closure of M_{11}^k on Ω is S_{12}^k. By Lemma 2.4.1 (2), $S_{12} \wr K \leq G^{(2)} \leq \mathrm{Aut}\Gamma^{(2)} = \mathrm{Aut}(\Gamma)$. Thus Γ has a fixed-point-free automorphism of order 3.

We are left to deal with the case where every nontrivial normal subgroup of G has at most 2 orbits on $V\Gamma$ and there exists one nontrivial normal subgroup with precisely 2 orbits, that is, G is biquasiprimitive on $V\Gamma$. Either G contains a fixed-point-free element of prime order, or G is an elusive biquasiprimitive group. In the latter case, by Theorem 8.1.11, $G^{(2)}$ is not elusive. Hence by Lemma 2.4.1 (2), $G^{(2)} \leq \mathrm{Aut}(\Gamma)^{(2)} = \mathrm{Aut}(\Gamma)$, and Γ

has a fixed-point-free automorphism of prime order. □

Proof of Theorem 8.1.10: Consider the orbital (undirected) graph Γ of G relative to Σ (note that Σ is self-paired) with vertex set Ω and edge set $(\omega, \alpha)^G$ for $\alpha \in \Sigma$. By assumption, $G \leq \mathrm{Aut}(\Gamma)$ is vertex-transitive and locally-quasiprimitive. Now by the proof of Theorem 8.1.8, we have $G^{(2)}$ contains a fixed-point-free element of prime order. The proof is complete. □

Chapter 9

Concluding Remarks

We conclude with a few words about future research on the two main problems of this thesis.

9.1 Further questions on closures of affine permutation groups

Our results about 3-closures of affine permutation groups raise three further questions that are more specific versions of Question 1.2.1.

First, we consider the case $k = 2$. If $H \in C_i$ and H is not transitive on $V(d,p) \setminus \{0\}$, then does $H^{(1)} \cap \mathrm{GL}(d,p)$ also lie in C_i? We actually prove that this is true for $i = 1, 2, 4, 5, 7$ and some cases of $H \in C_8$ in Chapter 6. But what about the other cases?

Second, if $H \in C_9$ is not 2-transitive on $V \setminus \{0\}$, then by Theorem 6.0.6, $K = H^{(2)} \cap \Gamma\mathrm{L}(d,q) \in C_9$. Can we conclude in this case that $H/(H \cap Z)$ and $K/(K \cap Z)$ have the same socles?

Lastly, Theorem 6.0.6 only tells us H and $H^{(2)} \cap \Gamma\mathrm{L}(d,q)$ lie in the same Aschbacher class. However, this does not guarantee that H and $H^{(2)} \cap \Gamma\mathrm{L}(d,q)$ are close in size. Can we find a way to clarify how close (or not) they may be?

9.2 Future work on the Polycirculant Conjecture

We have proved in Chapter 8 that every vertex-transitive locally-quasiprimitive graph has a semiregular automorphism. Next it is natural to consider graphs that are arc-transitive but not locally-quasiprimitive. For example, we can consider arc-transitive graphs of valency $2p$ for p a prime. We are currently working on this case. Since there are a lot of results about arc-transitive graphs in the literature, we may be able to consider wider classes of arc-transitive graphs. Hopefully, we might find a good way to handle arc-transitive graphs for the Polycirculant Conjecture.

Another direction is to consider the vertex-transitive graphs of small valencies. We may first look at the case of prime valency. Since Marušič and Scapellato [35] proved the Polycirculant Conjecture for vertex-transitive graphs of valency three, the next one we should look at is vertex-transitive graphs of valency five. Since arc-transitive graphs of valency five are locally-quasiprimitive, we only need to consider ones which are not arc-transitive. Our goal is to use both combinatorics and group theoretic methods to find a feasible strategy for general vertex-transitive graphs that are not arc-transitive.

Bibliography

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* 76 (1984), 469-514.

[2] M. Aschbacher, *Finite group theory*, Cambridge University Press, Cambridge, 1986.

[3] M. Aschbacher and L. L. Scott, Maximal subgroups of finite groups, *J. Algebra* 92 (1985), 44-80.

[4] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, New York, 1974.

[5] M. Bhattacharjee, D. Macpherson, R. G. Moller and P. M. Neumann, *Notes on Infinite Permutation Groups*, Lecture Notes in Mathematics, Vol. 1698, Springer-Verlag, 1998.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985.

[7] P. J. Cameron, M. Giudici, G. A. Jones, W. M. Kantor, M. H. Klin, D. Marušič, and L. A. Nowitz, 'Transitive permutation groups without semiregular subgroups', *J. London Math. Soc.* **66** (2002), 325–333.

[8] P. J. Cameron and W. M. Kantor, 2-transitive and antiflag transitive collineation groups of finite projective spaces, *J. Algebra* 60 (1979), no.2, 384-422.

[9] P. J. Cameron (ed.), 'Problems from the Fifteenth British Combinatorial Conference', *Discrete Math.* **167/168** (1997), 605–61.

[10] P. J. Cameron, *Permutation groups*, in *London Mathematical Society Student Texts* 45 (Cambridge University Press, Cambridge, 1999).

[11] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leibzig: Teubner 1901 (New York: Dover Publ. 1958).

[12] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag, New York-Heidelberg-Berlin, 1996.

[13] L. Dornhoff, *Group Representation Theory*, Marcel Dekker, Inc., New York, 1971.

[14] B. Fein, W. M. Kantor, and M. Schacher, 'Relative Brauer groups. II', *J. Reine Angew. Math.* **328** (1981), 39–57.

[15] M. Giudici, 'Fixed point free elements of prime order in permutation groups', PhD thesis, University of London, 2002.

[16] M. Giudici, 'Quasiprimitive permutation groups with no fixed point free elements of prime order', *J. London Math. Soc.* **67** (2003), 73–84.

[17] M. Giudici and J. Xu, All vertex-transitive locally-quasiprimitive graphs have a semiregular automorphism, *submitted.*

[18] D. Gorenstein, *Finite Groups*, Harper, Evanston and London, 1968.

[19] W. H. Greub, *Multilinear Algebra*, Springer-Verlag, New York-Heidelberg-Berlin, 1967.

[20] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, New York-Heidelberg-Berlin, 1967.

[21] M. Iranmanesh and C. E. Praeger, On Non-Cayley vertex-transitive graphs of order a product of three primes, *J. Combin. Theory (B)* 81, (2001) 1-19.

[22] D. Jordan, 'Eine symmetrieeigenschaft von graphen,graphentheorie und ihre anwendungen (Stadt Wehlen, 1988), 17–20', *Dresdner Reihe Forsch.* **9** (1988).

[23] J. D. Key and J. Siemons, On the k-closure of finite linear groups, *Bollettino U.M.I.* (7) 1-B (1987), 31-55.

[24] O. H. King, On subgroups of the special linear group containing the special unitary group, *Geom. Dedicata* 19 (1985), no.3, 297-310.

[25] O. H. King, On subgroups of the special linear group containing the special orthogonal group, *J.Algebra* 96 (1985), no.1, 178-193.

[26] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Notes Series 129, Cambridge University Press, Cambridge, 1990.

[27] L. G. Kovacs, Maximal subgroups in composite finite groups, *J. Algebra* 99 (1986), no. 1, 114–131.

[28] L. G. Kovacs, Primitive subgroups of wreath products in product action, *Proc. London Math. Soc.* (3) 58 (1989), 306-322.

[29] S. Lang, *Algebra*, Addison-Wesley, 1965.

[30] C. H. Li, C. E. Praeger, A. Venkatesh, and S. Zhou, 'Finite locally-quasiprimitive graphs', *Discrete Math.* **246** (2002), 197-218.

[31] M. W. Liebeck and C. E. Praeger, Relation algebras and finite permutation groups, *J. London Math. Soc.* (2) 45 (1992), 433-445.

[32] M. W. Liebeck, C. E. Praeger and J. Saxl, On the 2-closures of finite permutation groups, *J. London Math. Soc.* (2) 37 (1988), 241-252.

[33] M. W. Liebeck, C. E. Praeger and J. Saxl, On the O'Nan-Scott Theorem for finite primitive permutation groups, *J. Austral. Math. Soc.* (A) 44 (1988), 389-396.

[34] D. Marušič, 'On vertex symmetric digraphs', *Discrete Math.* **36** (1981), 69–81.

[35] D. Marušič and R. Scapellato, 'Permutation groups, vertex-transitive digraphs and semiregular automorphisms', *European Journal of Combinatorics* **19** (1998), 707–712.

[36] B. D. McKay and C. E. Praeger, Vertex-transitive graphs which are not Cayley graphs I, *J. Austral. Math. Soc. (A)* 56 (1994), 53-63.

[37] B. D. McKay and C. E. Praeger, Vertex-transitive graphs which are not Cayley graphs II, *J. Graph Theory* 22 (1996), 321-334.

[38] A. A. Miller and C. E. Praeger, Non-Cayley vertex-transitive graphs of order twice the product of two odd primes. *J. Algebraic Combin.* 3 (1994), 77-111.

[39] P. M. Neumann, Finite permutation groups, edge-coloured graphs, and matrices, in *Topics in group theory and computation*, (ed. M.P.J.Curran) Academic Press, London, (1977),pp. 82-116.

[40] C. E. Praeger, Imprimitive symmetric graphs, *Ars Combin.* 19 A (1985) 149-163.

[41] C. E. Praeger, The inclusion problem for finite primitive permutaion groups, *Proc. London Math. Soc. (3)* 60 (1990), 68-88.

[42] C. E. Praeger, Closures of finite permutation groups and relation algebras, in *Groups, Combinatorics & Geometry (Durham, 1990)*, London Math. Soc. Lecture Note Series 165, Cambridge Univ. Press, Cambridge, 1992, pp.368-379.

[43] C. E. Praeger, An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs, *J. London Math. Soc. (2)* 47, (1993), 227-239.

[44] C. E. Praeger, Finite transitive permutation groups and finite vertex transitive graphs, in: G. Hahn, G. Sabidussi (Eds.) Graph Symmetry, NATO Advanced Science Institute Series C, Mathematical and Physical Sciences, Vol. 497, Kluwer Academic Publishing, Dordrecht, 1997, pp. 277-318.

[45] C. E. Praeger, Finite quasiprimitive graphs, in: R.A. Bailey (Eds.), London Mathematical Society, Lecture Note Series, Vol. 241, Cambridge University Press, Cambridge, 1997, pp. 65-85.

[46] C. E. Praeger, 'Finite transitive permutation groups and bipartite vertex-transitive graphs', *Illinois Journal of Mathematics* **47** (2003), 461-475.

[47] C. E. Praeger and J. Saxl, Closures of finite primitive permutation groups, *Bull. London Math. Soc.* 24 (1992). 251-258.

[48] L. L. Scott, 'Representations in characteristic p', in *The Santa Cruz Conference on Finite Groups, Proceedings of Symposia in Pure Mathematics* **37** (1980), 319-331.

[49] E. Snapper and R. J. Troyer, *Metric Affine Geometry*, Academic Press, New York and London, 1971.

[50] M. Suzuki, *Group Theory I*, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

[51] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics, Vol. 9, Heldermann-Verlag, Berlin, 1992.

[52] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York and London, 1964. Also publised in *Wielandt, Helmut, Mathematische Werke/Mathematical works. Vol. 1. Group theory.* Walter de Gruyter & Co., Berlin, 1994, pp.119-198.

[53] H. Wielandt, *Permutation Groups Through Invariant Relations and Invariant Functions*, Lecture Notes, Ohio State University, Columbus, 1969. Also publised in *Wielandt, Helmut, Mathematische Werke/Mathematical works. Vol. 1. Group theory.* Walter de Gruyter & Co., Berlin, 1994, pp.237-296.

[54] J. Xu, C. H. Li, C. E. Praeger and M. Giudici, On closures of affine permutation groups, *submitted*.

[55] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. für Math. und Phys. 3 (1892), 265-284.