Conjugacy Classes in Finite Groups, Commuting Graphs and Character Degrees

by

Eleanor Jane Cassell

A thesis submitted to
University of Birmingham
for the degree of
Doctor of Philosophy

School of Mathematics
University of Birmingham
February 2013

UNIVERSITY OF BIRMINGHAM

University of Birmingham Research Archive

e-theses repository

This unpublished thesis/dissertation is copyright of the author and/or third parties. The intellectual property rights of the author or third parties in respect of this work are as defined by The Copyright Designs and Patents Act 1988 or as modified by any successor legislation.

Any use made of information contained in this thesis/dissertation must be in accordance with that legislation and must be properly acknowledged. Further distribution or reproduction in any format is prohibited without the permission of the copyright holder.

Abstract

In the first half of this thesis we determine the connectivity of commuting graphs of conjugacy classes of semisimple and some unipotent elements in $GL(n, q)$. In the second half we prove that the degree of an irreducible character of a finite simple group divides the size of some conjugacy class of the group.

To Tom

Acknowledgements

I would like to thank my supervisor Chris Parker for supporting me throughout my PhD. I am also grateful to Luke Morgan for being a good friend. I thank my family for the love and support they have provided throughout the years. Finally, I acknowledge EPSRC for funding this work.

Contents

Chapter 1

Introduction

In this thesis we consider two problems relating to conjugacy classes in finite groups. In this short introduction we state our main theorems. Fuller introductions will be provided for each part.

In the first half we consider commuting graphs of conjugacy classes in $GL(n, q)$. Let $G = GL(n, q)$, $x \in G$ and let $\mathit{\Gamma}$ be the commuting graph for the conjugacy class of x. We use $cl_G(x)$ to denote the conjugacy class of x in G.

In Chapter 3, we assume x is a semisimple element in G, with characteristic polynomial $f_x = f_1^{z_1} \dots f_r^{z_r}$, where each f_i is irreducible over $GF(q)$, $\deg f_i = d_i$ and $f_i \neq f_j$ for $i \neq j$. Let Δ_x be the graph with vertex set $\{f_1, \dots, f_r\}$ and edge set

$$\{\{f_i, f_j\} \mid i \neq j, d_i a = d_j b \quad \text{for some} \quad 1 \leqslant a \leqslant z_i, 1 \leqslant b \leqslant z_j\}.$$

We say an edge $\{f_i, f_j\}$ is *exact* if and only if $d_i z_i = d_j z_j$ and $d_i a \neq d_j b$ for all $1 \leqslant a < z_i$, $1 \leqslant b < z_j$. Note Δ_x is a much smaller graph than $\mathit{\Gamma}$. The result is as follows.

Theorem 1.0.1 *Let $x \in G$ be semisimple with characteristic polynomial $f = f_1^{z_1} \dots f_r^{z_r}$, where f_i is irreducible for $1 \leqslant i \leqslant r$ and $f_i \neq f_j$ for $i \neq j$.*

(i) If $r = 1$ and $z_1 = 1$, then $\mathit{\Gamma}$ is disconnected.

(ii) If $r = 1$ and $z_1 \geqslant 2$, then Γ is connected.

(iii) If $r > 1$ then Γ is connected if and only if Δ_x is connected, with at least one non-exact edge.

In Chapter 4, we consider various unipotent elements of G. As we will see, this turns into a very complicated problem. If $SL(n, q)$ is contained in the stabilizer of a connected component in Γ we say Γ is *S-connected*. Let ε be the exponent of $PGL(2, q)$. We prove the following.

Theorem 1.0.2 *Suppose $x \in G$ is unipotent.*

(i) If x is of Jordan block type (n), then Γ is disconnected.

(ii) If x is of Jordan block type type $(m_1, \ldots, m_k)$, with $m_i \geqslant m_{i+1} + 2$ for $1 \leqslant i < k$, then Γ is disconnected.

(iii) If x is of Jordan block type $(m, m-1)$, then Γ is connected if and only if $m \leqslant \varepsilon$.

(iv) If x is of Jordan block type (m, m), then Γ is S-connected if and only if $(m, \varepsilon) = m$. Further, if $(m, q-1) = 1$ then Γ is connected.

In the second half of the thesis we consider a conjecture from [26] which states that if G is a finite group and χ is a primitive irreducible character of G, then there exists $g \in G$ such that $\chi(1)$ divides $|cl_G(g)|$. Our contribution is the following theorem.

Theorem 1.0.3 *In a finite simple group the degree of any irreducible character divides the size of some conjugacy class of the group.*

Chapter 2

Commuting Graphs

Definition 2.0.1 *Let G be a group and X a subset of the elements in G. The* commuting graph $\mathit{\Gamma}(G, X) = \mathit{\Gamma}$ *for X is the graph with vertex set $V(\mathit{\Gamma}) = X$ and edge set* $E(\mathit{\Gamma}) = \{x, y \mid x, y \in X, x \neq y, [x, y] = 1\}$.

Given a group G, there are various possibilities for the set X and a number of questions that can be asked about $\mathit{\Gamma}$. We mention some here.

In [6], G is taken to be a finite simple group and X to be the set of elements of odd prime order and the authors discuss the connectivity of $\mathit{\Gamma}$. In [37], G is a finite minimal nonsolvable group and $X = G \setminus \{1\}$, and it is shown that the diameter of $\mathit{\Gamma}$ is at least 3. In [25], G is taken to be either $Sym(n)$ or $Alt(n)$ and $X = G \setminus \{1\}$. It is shown that either $\mathit{\Gamma}$ is disconnected, or has diameter at most 5.

In [4], [3] and [5], X is taken to be a conjugacy class of involutions and G is the symmetric group, a finite Coxeter group or the special linear group respectively. Questions are answered about the connectivity, disc size and diameter of $\mathit{\Gamma}$.

A result which is particularly relevant for us is [8], where $G = Sym(n)$ and X is any conjugacy class. In order to state the result we need some definitions and notation.

Let $x \in Sym(n)$ have cycle type $e_1^{f_1} \dots e_m^{f_m}$. Define Δ to be a graph with vertex set

$V(\Delta) = \{1, \ldots, m\}$ and edge set

$$E(\Delta) = \{\{i, j\} \mid i \neq j, e_i h_i = e_j h_j \text{ for some } 1 \leqslant h_i \leqslant f_i, 1 \leqslant h_j \leqslant f_j\}.$$

An edge $\{i, j\} \in E(\Delta)$ is *exact* if $e_i h_i \neq e_j h_j$ for $1 \leqslant h_i < f_i, 1 \leqslant h_j < f_j$, and $e_i f_i = e_j f_j$. Further, for $1 \leqslant i \leqslant m$, let

$$b(i) = \frac{e_i}{lcm\{d \mid d \text{ divides } e_i, d \leqslant f_i\}},$$

and say an edge $\{i, j\} \in E(\Delta)$ is *special with source* i if $e_j f_j = e_i$ and $b(i) = e_i$. The following two theorems are proved.

Theorem 2.0.2 (Bundy) *Let $G = Sym(n)$, $x \in G$ have cycle type e^f and set $X = cl_G(x)$. Then $\Gamma(G, X)$ is connected if and only if $b(1) = 1$ or $e \leqslant 3$ and $f = 1$.*

Theorem 2.0.3 (Bundy) *Let $G = Sym(n)$, $x \in G$ have cycle type $e_1^{f_1} \ldots e_m^{f_m}$ for $m \geqslant 2$, and set $X = cl_G(x)$. Then $\Gamma(G, X)$ is connected if and only if*

(i) Δ is connected with at least one edge non-exact;

(ii) $gcd\{b(i) \mid 1 \leqslant i \leqslant m\} = 1$;

(iii) the vertex set of Δ is not of the form $E \cup Y$, with $E \cap Y = \emptyset$ and $E, Y \neq \emptyset$ such that

- *(a) for all $i, j \in E$ with $i \neq j$, $\{i, j\}$ is an exact edge,*
- *(b) there exists a vertex $y \in Y$ such that for all $i \in E$, $\{i, y\}$ is a special edge with source y,*
- *(c) no vertex of E is joined to a vertex of $Y \setminus \{y\}$,*
- *(d) $gcd\{b(i) \mid i \in Y\} = e_y$.*

We note that these theorems are similar to our result for semisimple conjugacy classes in $GL(n, q)$ in Chapter 3 and indeed our results were inspired by his work. Since conjugacy classes in $Sym(n)$ and semisimple conjugacy classes in $GL(n, q)$ are both determined by partitions, perhaps this is not surprising. Further, in [2], the diameter and disc structure of commuting graphs for conjugacy classes of $Sym(n)$ is considered.

A related problem is considered in [7]. There the authors let C and D be similarity classes of matrices in $M_n(q)$ and say C and D *commute* if there exist $X \in C$, $Y \in D$ such that X and Y commute. They reduce the problem to the nilpotent classes and provide a solution when the Jordan form corresponding to the similarity classes has two blocks. In Chapter 4 we use some similar techniques when we are considering conjugacy classes of unipotent elements. The difficulties that they encounter in the general case are similar to the difficulties that we uncover.

We now include some general results which will be useful in our study of commuting graphs. Let G be a finite group, $x \in G$, $\Gamma = \Gamma(G, cl_G(x))$ and let Γ_x be the connected component of Γ containing x.

Lemma 2.0.4 *Let $x \in G$ and suppose $g, h \in G$ with $x^g = x^h$. Then $g = kh$ for some $k \in C_G(x)$.*

Proof. Since $x^g = x^h$, we have $x^{gh^{-1}} = x$ and hence $gh^{-1} \in C_G(x)$. Then $g \in C_G(x)h$ and the result follows. $\square$

Lemma 2.0.5 *Let G be a group, $x \in G$ and set $H = C_G(x)$. Then $C_G(H) = Z(H)$.*

Proof. As $x \in H$, we have $C_G(H) \leqslant C_G(x) = H$. Therefore $C_G(H) = H \cap C_G(H) = Z(H)$. $\square$

We see G acts transitively on the vertices of Γ by conjugation, and so the connected components of Γ are conjugate.

Lemma 2.0.6 *Let $x, g \in G$. Then $\mathit{\Gamma}_{x^g} = (\mathit{\Gamma}_x)^g$.*

Proof. We have $x \in \mathit{\Gamma}_x$ and so $x^g \in (\mathit{\Gamma}_x)^g$. Therefore $\mathit{\Gamma}_{x^g} = (\mathit{\Gamma}_x)^g$. $\square$

Lemma 2.0.7 *Let $x \in G$. Then $C_G(x) \leqslant Stab_G(\mathit{\Gamma}_x)$.*

Proof. Let $g \in C_G(x)$. Then $\mathit{\Gamma}_x = \mathit{\Gamma}_{x^g} = (\mathit{\Gamma}_x)^g$ by Lemma 2.0.6, and so $g \in Stab_G(\mathit{\Gamma}_x)$. $\square$

Lemma 2.0.8 *Let $x, g \in G$. Then x and x^g are connected in $\mathit{\Gamma}$ if and only if $g \in Stab_G(\mathit{\Gamma}_x)$.*

Proof. Suppose $g \in Stab_G(\mathit{\Gamma}_x)$. Then $x^g \in \mathit{\Gamma}_x$ and so, since $x \in \mathit{\Gamma}_x$ and $\mathit{\Gamma}_x$ is connected, x and x^g are connected in $\mathit{\Gamma}$.

Now suppose x and x^g are connected in $\mathit{\Gamma}$. Then $\mathit{\Gamma}_x = \mathit{\Gamma}_{x^g} = (\mathit{\Gamma}_x)^g$ by Lemma 2.0.6, and hence $g \in Stab_G(\mathit{\Gamma}_x)$. $\square$

Lemma 2.0.9 *Let $x \in G$ and suppose $C_G(x)$ is abelian. Then $\mathit{\Gamma}_x$ has diameter* 1.

Proof. If $y \in C_G(x) \cap cl_G(x)$ we have $C_G(x) \subseteq C_G(y)$ as $C_G(x)$ is abelian. Also, since $C_G(y)$ is conjugate to $C_G(x)$, $C_G(y)$ is abelian and hence $x \in C_G(y)$ implies $C_G(y) \subseteq C_G(x)$. Thus $C_G(x) = C_G(y)$.

Now if $y \in \mathit{\Gamma}_x$, there is a sequence of elements $y_1, \ldots, y_r \in \mathit{\Gamma}_x$ such that $y_1 \in C_G(x)$, $y_i \in C_G(y_{i-1})$, for $1 < i \leqslant r$, and $y \in C_G(y_r)$. Then $C_G(x) = C_G(y_1) = \ldots = C_G(y_r) = C_G(y)$. Therefore we have $y \in C_G(x)$ for all $y \in \mathit{\Gamma}_x$, and so, as $C_G(x)$ is abelian, the result follows. $\square$

We finish this chapter with a result which gives some justification for our strategy of considering semisimple and unipotent elements separately.

Let $G = GL(n, q)$, where q is a power of the prime p. Recall an element in G is *semisimple* if it is a p'-element and *unipotent* if it is a p-element. Suppose $g \in G$. Then g can be written uniquely as $g = xy$ where x is semisimple, y is unipotent and $[x, y] = 1$. This is known as the *Jordan decomposition*, [9, p.11].

Lemma 2.0.10 *Let $g \in G$ have Jordan decomposition xy where x is semisimple and y is unipotent. Suppose $h \in G$ is such that $[g, g^h] = 1$. Then $[x, x^h] = [y, y^h] = 1$.*

Proof. Suppose $o(x) = m$ and $o(y) = p^a$. Then as $(m, p^a) = 1$, we have $\langle x^{p^a} \rangle = \langle x \rangle$ and $\langle y^m \rangle = \langle y \rangle$. Since $\langle g, g^h \rangle$ is an abelian group, $[g, g^h] = 1$ implies $[g^{p^a}, (g^h)^{p^a}] = [g^m, (g^h)^m] = 1$ and hence $[x^{p^a}, (x^h)^{p^a}] = [y^m, (y^h)^m] = 1$. Therefore $\langle x^{p^a}, (x^h)^{p^a} \rangle = \langle x, x^h \rangle$ and $\langle y^m, (y^h)^m \rangle = \langle y, y^h \rangle$ are abelian groups and so $[x, x^h] = [y, y^h] = 1$ as claimed. □

Theorem 2.0.11 *Suppose $g \in G$ has Jordan decomposition xy with x semisimple and y unipotent. If $\Gamma(G, cl_G(g))$ is connected, then $\Gamma(G, cl_G(x))$ and $\Gamma(G, cl_G(y))$ are connected.*

Proof. Let $z \in cl_G(x)$. Then $z = x^h$ for some $h \in G$. We have $g^h \in cl_G(g)$ and so, since $\Gamma(G, cl_G(g))$ is connected, there exists a path $g^{h_1}, g^{h_2}, \ldots, g^{h_r}$ in $\Gamma(G, cl_G(g))$, where $h_1 = 1$, $h_r = h$ and $g^{h_i} \in C_G(g^{h_{i-1}})$ for $2 \leqslant i \leqslant r$. We note $g^{h_i} = x^{h_i} y^{h_i}$ and $[g^{h_{i-1}}, g^{h_i}] = 1$ for $2 \leqslant i \leqslant r$. Therefore by Lemma 2.0.10 we have $[x^{h_{i-1}}, x^{h_i}] = 1$ for $2 \leqslant i \leqslant r$ and hence $x, x^{h_2}, \ldots, x^{h_r} = z$ is a path between x and z in $\Gamma(G, cl_G(x))$. Therefore $\Gamma(G, cl_G(x))$ is connected. The proof for $\Gamma(G, cl_G(y))$ is similar. □

Sadly the converse of this result is not true as the following example shows.

Example 2.0.12 *Let $G = GL(4, 2)$ and let $x, y \in G$ with*

$$x = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

We see x has order 3 so is semisimple and y has order 2 so is unipotent. The characteristic polynomial of x is $f_x(t) = (t^2 + t + 1)^2$ hence, by Theorem 1.0.1(ii), $\Gamma(G, cl_G(x))$ is *connected. The type of y is $(2,2)$ and so $\Gamma(G, cl_G(y))$ is connected by Theorem 1.0.2(iv). Now*

$$xy = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

and the centralizer of xy in G is abelian. Therefore Γ_{xy} has diameter 1 by 2.0.9, and hence every element of Γ_{xy} commutes with xy. Finally note

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

which does not commute with xy and therefore $\Gamma(G, cl_G(xy))$ is disconnected.

Chapter 3

Commuting Graphs of Semisimple Elements in $GL(n, q)$

In this chapter we determine the connectedness of commuting graphs for conjugacy classes of semisimple elements in $GL(n, q)$.

Let $\mathbb{F}$ be any field and V a finite dimensional vector space over $\mathbb{F}$.

Definition 3.0.1 *An element $X \in GL(n, \mathbb{F})$ is* semisimple *if there exists a field extension $\mathbb{E}$ of $\mathbb{F}$ over which X is diagonalizable.*

3.1 Preliminary Results

Lemma 3.1.1 *Suppose $X, Y \in GL(n, \mathbb{F})$ are conjugate. Then X and Y have the same characteristic polynomial.*

Proof. Suppose $Y = T^{-1}XT$ for some $T \in GL(n, \mathbb{F})$. Then the characteristic polynomial of Y is given by

$$\begin{aligned}
\det(Y - tI_n) &= \det(T^{-1}XT - tI_n) \\
&= \det(T^{-1}XT - T^{-1}(tI_n)T) \\
&= \det(T^{-1}(X - tI_n)T) \\
&= \det(T^{-1}) \det(X - tI_n) \det T \\
&= \det(X - tI_n).
\end{aligned}$$

So X and Y have the same characteristic polynomial. $\square$

Definition 3.1.2 *Let* $f(t) = \sum_{i=0}^{d} a_i t^i$ *be a monic polynomial in* $\mathbb{F}[t]$*. Then the* companion matrix *of* f *is*

$$C(f) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & & \ddots & & \\ \vdots & & & \ddots & \\ 0 & & & & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{d-1} \end{pmatrix}.$$

Note f *is the characteristic polynomial of* $C(f)$*.*

We write $\operatorname{diag}(\alpha_1, \dots, \alpha_n)$ for the matrix in $GL(n, \mathbb{F})$ with diagonal entries $\alpha_1, \dots, \alpha_n \in \mathbb{F}$, and write $\operatorname{diag}(A_1, \dots, A_r)$ for the block diagonal matrix with blocks $A_i \in GL(m_i, \mathbb{F})$, $1 \leqslant i \leqslant r$, where $\sum_{i=1}^{r} m_i = n$. We also use this notation to describe subgroups of $GL(n, \mathbb{F})$ consisting of block diagonal matrices e.g. $\operatorname{diag}(GL(m_1, \mathbb{F}), \dots, GL(m_r, \mathbb{F}))$, $\sum_{i=1}^{r} m_i = n$, is the subgroup of $GL(n, \mathbb{F})$ consisting of all matrices of the form $\operatorname{diag}(A_1, \dots, A_r)$ with $A_i \in GL(m_i, \mathbb{F})$, $1 \leqslant i \leqslant r$. So $\operatorname{diag}(GL(m_1, \mathbb{F}), \dots, GL(m_r, \mathbb{F}))$ is a subgroup of $GL(n, \mathbb{F})$ which preserves a decomposition of V into a direct sum

$V = V_1 \oplus \ldots \oplus V_r$ with $\dim V_i = m_i$ and an element $\mathrm{diag}(A_1, \ldots, A_r)$ maps $(v_1, \ldots, v_r)$ to $(v_1 A_1, \ldots, v_r A_r)$ where $v_i \in V_i$.

Suppose $X \in GL(n, \mathbb{F})$ is semisimple with characteristic polynomial

$$f_X(t) = f_1(t)^{z_1} \ldots f_r(t)^{z_r},$$

where the $f_i(t)$ are distinct irreducible polynomials in $\mathbb{F}[t]$ of degree d_i, for $i \in \{1, \ldots, r\}$. Then X is conjugate to a matrix

$$\mathrm{diag}(\underbrace{C(f_1), \ldots, C(f_1)}_{z_1 \text{ times}}, \ldots, \underbrace{C(f_r), \ldots, C(f_r)}_{z_r \text{ times}}),$$

where $C(f_i)$ occurs z_i times. See [21, p.262-270] for details. Note the minimal polynomial m_X of X is $f_1 \ldots f_r$. Together with Lemma 3.1.1 we have the following lemma.

Lemma 3.1.3 *Assume $X, Y \in GL(n, \mathbb{F})$ are semisimple. Then X and Y are conjugate if and only if they have the same characteristic polynomial.*

We finish this section with a collection of results which will be used in Section 3.3.

Lemma 3.1.4 *Let $f(t) = \sum_{i=0}^{d} a_i t^i$ be a monic irreducible polynomial over $GF(q)$ and suppose ε is a root of f. Then the set of roots of f is $\{\varepsilon, \varepsilon^q, \ldots, \varepsilon^{q^{d-1}}\}$ and $f(t) = \prod_{i=0}^{d-1}(t - \varepsilon^{q^i})$.*

Proof. Let α be any root of f so $f(\alpha) = 0$. Since $a^q = a$ for all $a \in GF(q)$, we have

$$f(t)^q = \left(\sum_{i=0}^{d} a_i t^i \right)^q = \sum_{i=0}^{d} a_i^q (t^i)^q = \sum_{i=0}^{d} a_i (t^q)^i,$$

as $a_i \in GF(q)$ for $0 \leqslant i \leqslant d - 1$. Then

$$f(\alpha^q) = \sum_{i=0}^{d} a_i (\alpha^q)^i = f(\alpha)^q = 0,$$

and thus α^q is also a root of f. Therefore $\varepsilon, \varepsilon^q, \ldots, \varepsilon^{q^{d-1}}$ are roots of f. Note $\varepsilon \in GF(q^d)$, and no proper subfield, so these roots are distinct.

Now let $g(t) = \prod_{i=0}^{d-1}(t - \varepsilon^{q^i})$. Then $g(t)$ is a polynomial of degree d which is a factor of $f(t)$. Therefore since both $f(t)$ and $g(t)$ are monic, $f(t) = g(t)$ as claimed. $\square$

Lemma 3.1.5 *Suppose $k, m \in \mathbb{N}$ with $k, m \leqslant n$ and $k + m > n$. Let*

$$H = \left\{ \left(\begin{array}{c|c} A & 0 \\ \hline 0 & I_{n-m} \end{array} \right) \middle| \; A \in GL(m,q) \right\},$$

and

$$K = \left\{ \left(\begin{array}{c|c} I_{n-k} & 0 \\ \hline 0 & B \end{array} \right) \middle| \; B \in GL(k,q) \right\}.$$

Then $\langle H, K \rangle = GL(n,q)$.

Proof. Let $E_{i,j}$ be the elementary matrix that is the same as the identity, but has a 1 in the i,jth position. For $1 \leqslant a \leqslant m$ and $b = m + j$ with $1 \leqslant j \leqslant n - m$, let $X = E_{m,b}$ and $Y = E_{a,m}$. Then $X \in K$, $Y \in H$ and $E_{a,b} = X^{-1}YXY^{-1}$. Likewise we can write any E_{ab} with $a = m + i$ for $1 \leqslant i \leqslant n - m$, $1 \leqslant b \leqslant m$, as a product of matrices from H and K. Therefore any elementary matrix in $GL(n,q)$ can be written as a product of matrices from H and K and so from [31, p.541], we have $SL(n,q) \subseteq \langle H, K \rangle$. Now note, for any $a \in GF(q)^*$,

$$\begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix} \in H,$$

and hence $GL(n,q) \subseteq \langle H, K \rangle$. $\square$

Definition 3.1.6 *A* Singer cycle *is an element of $GL(n,q)$ of order $q^n - 1$.*

Theorem 3.1.7 (Kantor) *Assume G is a subgroup of $GL(n,q)$ that contains a Singer cycle. Then $GL(n/s,q^s) \trianglelefteq G$ for some $s \in \mathbb{Z}$, and embeds naturally into $GL(n,q)$.*

Proof. See [29]. $\square$

Lemma 3.1.8 *Let Δ be a finite connected graph with $|V(\Delta)| \geqslant 2$, and fix an edge E in $E(\Delta)$. Then Δ contains a spanning tree with edge set containing E.*

Proof. Let Δ be a counterexample with $|E(\Delta)|$ minimal. Since Δ is not a tree, it contains a circuit. Let E' be an edge in the circuit such that $E' \neq E$. Then $\Delta \setminus E'$ is a connected graph with $E \in \Delta \setminus E'$. As Δ does not contain a spanning tree with edge set containing E, $\Delta \setminus E'$ is a counterexample with $|E(\Delta \setminus E')| < |E(\Delta)|$, contradicting the minimality of $|E(\Delta)|$. $\square$

Corollary 3.1.9 *Let Δ be a finite connected graph, with at least three vertices, and fix an edge E in $E(\Delta)$. Then there exists a vertex $v \in V(\Delta)$ such that $\Delta \setminus \{v\}$ is a connected graph with edge set containing E.*

Proof. By Lemma 3.1.8, Δ contains a spanning tree with edge set containing E. A finite tree has at least two vertices with valency 1, so as Δ has at least three vertices, there exists $v \in V(\Delta)$ which is not incident to E. Then $\Delta \setminus \{v\}$ is a connected graph with edge set containing E. $\square$

3.2 Centralizers

In this section we discuss the centralizers of semisimple elements in $GL(V)$ and $GL(n,\mathbb{F})$.

Lemma 3.2.1 *Let $X \in GL(V)$ be semisimple with minimal polynomial m_X. Assume that m_X is irreducible over $\mathbb{F}$. Then $\mathbb{F}\langle X \rangle \cong \mathbb{F}[t]/(m_X)$ is a field, where (m_X) is the ideal of $\mathbb{F}[t]$ generated by m_X.*

Proof. We can define an algebra homomorphism $\phi : \mathbb{F}[t] \to \mathbb{F}\langle X \rangle$ by setting $t\phi = X$ and extending linearly. Clearly ϕ is onto and has kernel (m_X). Then $\mathbb{F}[t]/(m_X) \cong \mathbb{F}\langle X \rangle$. Now, by hypothesis, m_X is irreducible over $\mathbb{F}$ so $\mathbb{F}[t]/(m_X)$ is a field [17, Th.29.4, Th.31.6], and hence $\mathbb{F}\langle X \rangle$ is a field. □

Keeping the conditions in Lemma 3.2.1, we let $\mathbb{E} = \mathbb{F}\langle X \rangle$ and $\deg m_X = d$. Note $\{1, X, \ldots, X^{d-1}\}$ is a basis for $\mathbb{E}$ over $\mathbb{F}$ and so $|\mathbb{E} : \mathbb{F}| = d$. We can make V into a vector space $\tilde{V}$ over $\mathbb{E}$ by defining $g \cdot v = vg$ for $g \in \mathbb{E}$, $v \in V$. Then we see $\dim \tilde{V} = n/d$. Note X acts as a scalar matrix on $\tilde{V}$.

Lemma 3.2.2 *Let $X \in GL(V)$ be semisimple with minimal polynomial m_X, and assume m_X is irreducible over $\mathbb{F}$. Then $C_{GL(V)}(X) \cong GL(\tilde{V})$.*

Proof. For any $h \in C_{GL(V)}(X)$, $g \in \mathbb{E}$, $v, w \in V$, we have

$$(g \cdot v + w)h = (vg + w)h = (vg)h + wh = (vh)g + wh = g \cdot (vh) + wh.$$

So h is a $\mathbb{E}$-linear map on $\tilde{V}$ and hence $h \in GL(\tilde{V})$. Thus we can define a map

$$\psi : C_{GL(V)}(X) \to GL(\tilde{V}),\ h\psi = h,$$

for all $h \in C_{GL(V)}(X)$.

Now suppose $h \in GL(\tilde{V})$. Then for $v \in V$,

$$v(Xh) = (vX)h = (X \cdot v)h = X \cdot (vh) = (vh)X = v(hX),$$

as h is an $\mathbb{E}$-linear map. Therefore $Xh = hX$ so $h \in C_{GL(V)}(X)$ and hence ψ is onto. So we have $C_{GL(V)}(X) \cong GL(\tilde{V})$. □

Corollary 3.2.3 *Let $X \in GL(n,q)$ be semisimple with characteristic polynomial $f_X = f^z$, where f is irreducible over $\mathbb{F}$ and $\deg f = d$. Then $C_{GL(n,q)}(X) \cong GL(z,q^d)$*

Proof. The minimal polynomial of X is $m_X = f$, so by Lemma 3.2.2, $C_{GL(V)}(X) \cong GL(\tilde{V})$, where $\tilde{V}$ is a vector space of dimension z over $GF(q)\langle X\rangle$. Now $GF(q)\langle X\rangle = GF(q^d)$ and so the result is clear. □

Corollary 3.2.4 *Suppose $X \in GL(n,q)$ is semisimple and has characteristic polynomial $f_X = f_1^{z_1}\dots f_r^{z_r}$, with f_i irreducible, $f_i \neq f_j$ for $i \neq j$, and $\deg f_i = d_i$ for $1 \leqslant i \leqslant r$. Then $C_{GL(n,q)}(X) \cong \mathrm{diag}(GL(z_1,q^{d_1}),\dots,GL(z_r,q^{d_r}))$.*

Proof. Let V be an n-dimensional vector space over $GF(q)$. Then $V|_X = W_1 \oplus \dots \oplus W_r$ where each W_i is a direct sum of isomorphic irreducible $\langle X\rangle$-modules and $X|_{W_i}$ has characteristic polynomial $f_i^{z_i}$. Let $T \in C_{GL(V)}(X)$. It is clear that T preserves the decomposition $V = W_1 \oplus \dots \oplus W_r$ and so $T|_{W_i} \in GL(W_i)$ for $1 \leqslant i \leqslant r$. Therefore $T|_{W_i} \in C_{GL(W_i)}(X|_{W_i})$, so $T \in \mathrm{diag}(C_{GL(W_1)}(X|_{W_1}),\dots,C_{GL(W_r)}(X|_{W_r}))$.

Now, for $1 \leqslant i \leqslant r$, $X|_{W_i}$ has characteristic polynomial $f_{X|_{W_i}} = f_i^{z_i}$ and by Corollary 3.2.3, $C_{GL(W_i)}(X|_{W_i}) \cong GL(z_i,q^{d_i})$. Therefore

$$\begin{aligned} C_{GL(n,q)}(X) &\cong C_{GL(V)}(X) \\ &\cong \mathrm{diag}(C_{GL(W_1)}(X|_{W_1}),\dots,C_{GL(W_r)}(X|_{W_r})) \\ &\cong \mathrm{diag}(GL(z_1,q^{d_1}),\dots,GL(z_r,q^{d_r})). \end{aligned}$$ □

Corollary 3.2.5 *Let $X = \mathrm{diag}(A_1,\dots,A_r) \in GL(n,\mathbb{F})$ be semisimple, where for $1 \leqslant i \leqslant r$, $A_i \in GL(d_iz_i,\mathbb{F})$ has characteristic polynomial $f_{A_i} = f_i^{z_i}$, with f_i irreducible. Then*

$$C_G(X) = \mathrm{diag}(C_{GL(d_1z_1,\mathbb{F})}(A_1),\dots,C_{GL(d_rz_r,\mathbb{F})}(A_r)).$$

Proof. This follows directly from Corollary 3.2.4. $\square$

Lemma 3.2.6 *Suppose $A, B \in GL(n,q)$ are semisimple, commute and have characteristic polynomials $f_A = f^z$ and $f_B = g_1^{h_1} \dots g_r^{h_r}$ respectively, where f and g_i are irreducible over $GF(q)$, for $1 \leqslant i \leqslant r$. Then for $1 \leqslant i \leqslant r$, $\deg f$ divides $h_i \deg g_i$.*

Proof. There exists $D \in GL(n,q)$ such that

$$B^D = \operatorname{diag}(\underbrace{C(g_1), \dots, C(g_1)}_{h_1 \text{ times}}, \dots, \underbrace{C(g_r), \dots, C(g_r)}_{h_r \text{ times}}).$$

Then A^D and B^D commute, and $f_{A^D} = f_A$, $f_{B^D} = f_B$, so it is no loss to assume $B = \operatorname{diag}(B_1, \dots, B_r)$ with $B_i = \operatorname{diag}(\underbrace{C(g_i), \dots, C(g_i)}_{h_i \text{ times}})$, for $1 \leqslant i \leqslant r$.

Now $A \in C_{GL(n,q)}(B)$ and so by Corollary 3.2.5, $A = \operatorname{diag}(A_1, \dots, A_r)$ where $A_i \in C_{GL(h_i \deg g_i, q)}(B_i)$. Now note for $1 \leqslant i \leqslant r$, $f_{A_i} = f^{w_i}$ for some $1 \leqslant w_i \leqslant z$, as f is irreducible. Then $w_i \deg f = h_i \deg g_i$ and hence $\deg f$ divides $h_i \deg g_i$ as claimed. $\square$

Lemma 3.2.7 *Assume $A, B \in GL(n,q)$ are semisimple, commute and have characteristic polynomials $f_A = f_1^{z_1} \dots f_r^{z_r}$, $f_B = g_1^{h_1} \dots g_s^{h_s}$ respectively. Then for each $i \in \{1, \dots, s\}$, there exists $k \in \{1, \dots, r\}$ such that $a \deg g_i = b \deg f_k$ for some $1 \leqslant a \leqslant h_i$, $1 \leqslant b \leqslant z_k$.*

Proof. As in Lemma 3.2.6 we may assume $B = \operatorname{diag}(B_1, \dots, B_s)$ with $B_i = \operatorname{diag}(\underbrace{C(g_i), \dots, C(g_i)}_{h_i \text{ times}})$, for $1 \leqslant i \leqslant s$. We have $A \in C_{GL(n,q)}(B)$ and so by Corollary 3.2.5, $A = \operatorname{diag}(A_1, \dots, A_s)$ where $A_i \in C_{GL(h_i \deg g_i, q)}(B_i)$. Now for $1 \leqslant i \leqslant s$, A_i and B_i commute, $f_{A_i} = f_1^{w_{i1}} \dots f_r^{w_{ir}}$ for some $0 \leqslant w_{ij} \leqslant z_j$, and $f_{B_i} = g_i^{h_i}$. Therefore by Lemma 3.2.6, $\deg g_i$ divides $w_{ij} \deg f_j$ for $1 \leqslant j \leqslant r$, so there exists $a_i \in \mathbb{Z}$ such that $a_i \deg g_i = w_{ij} \deg f_j$. Also $h_i \deg g_i = \sum_{j=1}^{r} w_{ij} \deg f_j$, so there exists $k \in \{1, \dots, r\}$ such that $w_{ik} \neq 0$. Hence $a_i \deg g_i = w_{ik} \deg f_k$, with $1 \leqslant a_i \leqslant h_i$ and $1 \leqslant w_{ik} \leqslant z_k$ as claimed. $\square$

3.3 Commuting Class Graphs

In this section we assume $\mathbb{F} = GF(q)$ and set $G = GL(n,q)$. We denote the class graph we are considering by Γ and let Γ_X be the connected component of Γ containing X.

First suppose $n = 1$. As $GL(1,q)$ is an abelian group, all conjugacy classes have size one and therefore the commuting class graph for each conjugacy class is trivially connected.

Next we consider $GL(2,2)$. The only conjugacy class of semisimple elements contains two elements of order 3. These commute and hence the class graph is connected.

From now on we assume $n \geqslant 2$ and $GL(n,q) \neq GL(2,2)$.

Lemma 3.3.1 *Suppose $X \in GL(n,q)$ is semisimple with characteristic polynomial $f_X = f$, where f is irreducible over $GF(q)$. Then the class graph of X is disconnected.*

Proof. By Corollary 3.2.3, $C_G(X) \cong GL(1,q^n)$, so is a cyclic group of order $q^n - 1$. Suppose $Y \in C_G(X) \cap cl_G(X)$. Then $C_G(X) \subseteq C_G(Y)$, as $C_G(X)$ is abelian, and hence $C_G(X) = C_G(Y)$. Suppose Γ is connected. Let $A \in GL(n,q)$. Then $X^A \in cl_G(X)$ and there exist $Y_1, \ldots, Y_k \in cl_G(X)$ such that $Y_1 \in C_G(X)$, $Y_i \in C_G(Y_{i-1})$ for $2 \leqslant i \leqslant k$, and $X^A \in C_G(Y_k)$. By above we have $C_G(X) = C_G(Y_1) = \cdots = C_G(Y_k) = C_G(X^A)$ and so $C_G(X)^A = C_G(X^A) = C_G(X)$. Therefore $C_G(X) \trianglelefteq GL(n,q)$.

Next we note $C_G(X)$ contains a Singer cycle, so $N_G(C_G(X))/C_G(X) = G/C_G(X)$ is a cyclic group of order n [23, p.187], and hence $|cl_G(X)| = n$. Suppose $n > 2$ or $q > 3$. Then $C_G(X) \trianglelefteq GL(n,q)$ implies either $C_G(X)$ is central or $SL(n,q) \subseteq C_G(X)$ [23, p.185]. We have $|C_G(X)| = q^n - 1 > q - 1 = |Z(GL(n,q))|$, so $C_G(X) \neq Z(GL(n,q))$. Therefore $SL(n,q) \subseteq C_G(X)$ and hence, as $Z(GL(n,q)) \subseteq C_G(X)$, $C_G(X) = GL(n,q)$, a contradiction. Now suppose $n = 2$, $q = 3$. Then $|C_G(X)| = 3^2 - 1$ and so $|cl_G(X)| = 6$, contradicting $|cl_G(X)| = n$. Therefore the class graph is disconnected. $\square$

Lemma 3.3.2 *Assume $X \in GL(n,q)$ is semisimple with characteristic polynomial $f_X = f^z$, where f is irreducible of degree d. Then $C_{M(n,q)}(C_{GL(n,q)}(X)) \cong GF(q^d)$ and hence $C_{M(n,q)}(C_{GL(n,q)}(X)) = GF(q)\langle X \rangle$.*

Proof. By Corollary 3.2.3, $C_{GL(n,q)}(X) \cong GL(z,q^d)$, and so acts irreducibly on V. Therefore by Schur's Lemma [27, p.4], $C_{M(n,q)}(C_{GL(n,q)}(X))$ is a division algebra and hence, as it is finite, a field [21, p.319]. It is sufficient to determine the multiplicative group of $C_{M(n,q)}(C_{GL(n,q)}(X))$. By Lemma 2.0.5,

$$C_{GL(n,q)}(C_{GL(n,q)}(X)) = Z(C_{GL(n,q)}(X)) \cong Z(GL(z,q^d)) \cong GF(q^d)^*.$$

Also, by Lemma 3.2.1, $GF(q)\langle X \rangle$ is a field isomorphic to $GF(q^d)$ and so since $GF(q)\langle X \rangle \leqslant C_{M(n,q)}(C_{GL(n,q)}(X))$ we have the result. $\square$

Lemma 3.3.3 *Assume $A \in GL(n,q)$ is semisimple with characteristic polynomial $f_A = f^2$, where f is irreducible of degree d. Then the class graph of A is connected.*

Proof. Let C be the companion matrix for f and let

$$X = \left(\begin{array}{c|c} C & 0 \\ \hline 0 & C \end{array}\right), \quad Y = \left(\begin{array}{c|c} C & 0 \\ \hline 0 & C^q \end{array}\right).$$

Note if ε is an eigenvalue of C, ε^q is an eigenvalue of C^q. Therefore the characteristic polynomial of C^q is the same as the characteristic polynomial of C by Lemma 3.1.4. Then X and Y commute and are in the same conjugacy class as A by Lemma 3.1.3.

From Lemma 3.2.1, $GF(q)\langle X \rangle$ and $GF(q)\langle Y \rangle$ are fields isomorphic to $GF(q^d)$. Suppose $w \in GF(q)\langle X \rangle \cap GF(q)\langle Y \rangle$. Then $w = \sum_{i=0}^{d} a_i X^i = \sum_{i=0}^{d} b_i Y^i$, for some $a_i, b_i \in$

$GF(q)$, and so

$$\left(\begin{array}{c|c} \sum_{i=0}^{d} a_i C^i & 0 \\ \hline 0 & \sum_{i=0}^{d} a_i C^i \end{array}\right) = \left(\begin{array}{c|c} \sum_{i=0}^{d} b_i C^i & 0 \\ \hline 0 & \sum_{i=0}^{d} b_i (C^q)^i \end{array}\right).$$

We have $\sum_{i=0}^{d} a_i C^i = \sum_{i=0}^{d} b_i C^i$, which implies $a_i = b_i$ for $0 \leqslant i \leqslant d$, as $\{1, X, \ldots, X^{d-1}\}$ is a linearly independent set and hence so is $\{1, C, \ldots, C^{d-1}\}$. Then

$$\sum_{i=0}^{d} a_i C^i = \sum_{i=0}^{d} a_i C^{qi} = \left(\sum_{i=0}^{d} a_i C^i\right)^q,$$

as $a_i \in GF(q)$, which means $\sum_{i=0}^{d} a_i C^i \in GF(q)$ and hence $w \in GF(q)$. Therefore $GF(q)\langle X\rangle \cap GF(q)\langle Y\rangle \cong GF(q)$ and is the subalgebra of scalar matrices.

Let $H = \langle C_G(X), C_G(Y)\rangle$. Then

$$C_{M(n,q)}(H) = C_{M(n,q)}(C_G(X)) \cap C_{M(n,q)}(C_G(Y)) = GF(q)\langle X\rangle \cap GF(q)\langle Y\rangle,$$

by Lemma 3.3.2, and so $C_{M(n,q)}(H) \cong GF(q)$.

Since $C_G(X)$ contains a Singer cycle we have, by Theorem 3.1.7, $GL(n/s, q^s) \trianglelefteq H$ for some $s \in \mathbb{Z}$. First suppose $H = GL(n/s, q^s)$. Then

$$GF(q^s)^* \cong Z(H) \leqslant C_{GL(n,q)}(H) \cong GF(q)^*,$$

so $s = 1$ and hence $H = GL(n, q)$.

Now suppose $GL(n/s, q^s) \lhd H$ for some $s > 1$. The normalizer of $GL(n/s, q^s)$ in $GL(n, q)$ is $\mathit{\Gamma L}(n/s, q^s)$ and $\mathit{\Gamma L}(n/s, q^s)/GL(n/s, q^s)$ is cyclic. So $[H, H] \leqslant GL(n/s, q^s)$. As $GL(2, q^d) \cong C_G(X)$ we have $SL(2, q^d) \cong [C_G(X), C_G(X)]$. So $[C_G(X), C_G(X)]$ acts irreducibly on V and hence by Schur's Lemma, $C_{M(n,q)}(C_G(X)) = C_{M(n,q)}([C_G(X), C_G(X)])$.

Then

$$\begin{aligned}
GF(q^s) &\leqslant C_{M(n,q)}([H,H]) \\
&\leqslant C_{M(n,q)}(\langle [C_G(X), C_G(X)], [C_G(Y), C_G(Y)] \rangle) \\
&= C_{M(n,q)}([C_G(X), C_G(X)]) \cap C_{M(n,q)}([C_G(Y), C_G(Y)]) \\
&= C_{M(n,q)}(C_G(X)) \cap C_{M(n,q)}(C_G(Y)) \\
&= GF(q)\langle X \rangle \cap GF(q)\langle Y \rangle \\
&\cong GF(q),
\end{aligned}$$

a contradiction.

Therefore we have $H = GL(n,q)$, so $GL(n,q)$ stabilizes $\mathit{\Gamma}_X$ and hence the class graph is connected. □

Corollary 3.3.4 *Suppose A has characteristic polynomial $f_A = f^z$, where f is irreducible and $z \geqslant 2$. Then the class graph of A is connected.*

Proof. We proceed by induction on z. The initial case is Lemma 3.3.3, so now suppose $z > 2$. Let $X_z = \text{diag}(\underbrace{C, \ldots, C}_{z \text{ times}})$, where $C = C(f)$, so X_z is conjugate to A. Now note

$$X_z = \text{diag}(C, X_{z-1}) = \text{diag}(X_{z-1}, C).$$

So by induction, the stabilizer of $\mathit{\Gamma}_{X_z}$ contains $\text{diag}(C, GL(d(z-1), q))$ and $\text{diag}(GL(d(z-1), q), C)$, and so by Lemma 3.1.5 the stabilizer of $\mathit{\Gamma}_{X_z}$ is $GL(n,q)$. Therefore the class graph is connected. □

Let $X \in GL(n,q)$ be semisimple with characteristic polynomial $f_X = f_1^{z_1} \ldots f_r^{z_r}$, with each f_i irreducible over $GF(q)$, $\deg f_i = d_i$ and $f_i \neq f_j$ for $i \neq j$. Following [8] we let Δ_X

be the graph with vertex set $\{f_1, \ldots, f_r\}$ and edge set

$$\{\{f_i, f_j\} \mid i \neq j, d_i a = d_j b \quad \text{for some} \quad 1 \leqslant a \leqslant z_i, 1 \leqslant b \leqslant z_j\}.$$

We say an edge $\{f_i, f_j\}$ is *exact* if and only if $d_i z_i = d_j z_j$ and $d_i a \neq d_j b$ for all $1 \leqslant a < z_i$, $1 \leqslant b < z_j$.

We have the following theorem, whose proof will follow by a sequence of lemmas.

Theorem 3.3.5 *Suppose $T \in GL(n, q)$ is semisimple with characteristic polynomial $f_T = f_1^{z_1} \ldots f_r^{z_r}$ for $r \geqslant 2$, where f_i is irreducible over $GF(q)$ for $1 \leqslant i \leqslant r$ and $f_i \neq f_j$ for $i \neq j$. Then the class graph of T is connected if and only if Δ_T is connected with at least one edge non-exact.*

Example 3.3.6 *Let $X \in GL(36, q)$ be semisimple.*

(i) Suppose $f_X = f_1^4 f_2^3 f_3^2$ where $\deg f_1 = 3$, $\deg f_2 = 4$ and $\deg f_3 = 6$. Then $E(\Delta_X) = \{\{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}\}$, where $\{f_1, f_2\}$ and $\{f_2, f_3\}$ are exact edges and $\{f_1, f_3\}$ is non-exact. Therefore by Theorem 3.3.5, Γ is connected.

(ii) Suppose $f_X = f_1^3 f_2^2 f_3$ where $\deg f_1 = 4$, $\deg f_2 = 6$ and $\deg f_3 = 12$. Then $E(\Delta_X) = \{\{f_1, f_2\}, \{f_1, f_3\}, \{f_2, f_3\}\}$ where all edges are exact. By Theorem 3.3.5, Γ is disconnected.

(iii) Suppose $f_X = f_1^4 f_2^2 f_3^2 f_4^2$ where $\deg f_1 = 2$, $\deg f_2 = 3$, $\deg f_3 = 5$ and $\deg f_4 = 6$. Then $E(\Delta_X) = \{\{f_1, f_2\}, \{f_1, f_4\}, \{f_2, f_4\}\}$. So by Theorem 3.3.5, Γ is disconnected.

We now describe a technique for producing conjugates of certain matrices. Let f_1 be a monic irreducible polynomial over $GF(q)$ of degree d, and let $f = f_1^z$. Set $m = dz$ and fix a generator ε of $GF(q^m)^*$. Let $g_\varepsilon(t) = \prod_{i=0}^{m-1}(t - \varepsilon^{q^i})$. The coefficient of t^i for

$0 \leqslant i \leqslant m-1$ is a symmetric polynomial in $\{\varepsilon, \varepsilon^q, \ldots, \varepsilon^{q^{m-1}}\}$ and hence is fixed under the map $\alpha \to \alpha^q$. Therefore each coefficient of g_ε is in $GF(q)$, so $g_\varepsilon(t) \in GF(q)[t]$ and $C(g_\varepsilon) \in GL(n,q)$.

Note the roots of f_1 lie in $GF(q^d)$, and $GF(q^d)$ is a subfield of $GF(q^m)$, so we can find $k \in \mathbb{N}$ such that ε^k is a root of f_1. The eigenvalues of $C(g_\varepsilon)$ are $\varepsilon, \varepsilon^q, \ldots \varepsilon^{q^{m-1}}$, and so the eigenvalues of $C(g_\varepsilon)^k$ are $\varepsilon^k, \varepsilon^{kq}, \ldots \varepsilon^{kq^{m-1}}$. Since $\varepsilon^k \in GF(q^d)$, $\varepsilon^{kq^d} = \varepsilon^k$ and hence the eigenvalues of $C(g_\varepsilon)^k$ are $\varepsilon^k, \varepsilon^{kq}, \ldots \varepsilon^{kq^{d-1}}$, with each eigenvalue having multiplicity z. Therefore $C(g_\varepsilon)^k$ has characteristic polynomial $\left(\prod_{i=0}^{d-1}(t-\varepsilon^{kq^i})\right)^z = f_1^z$, by Lemma 3.1.4, and hence $C(g_\varepsilon)^k$ is conjugate to

$$\mathrm{diag}(\underbrace{C(f_1), \ldots, C(f_1)}_{z \text{ times}}),$$

by Lemma 3.1.3.

Lemma 3.3.7 *Assume $A \in GL(n,q)$ is semisimple and has characteristic polynomial $f_A = f_1^{z_1} f_2^{z_2}$, where f_1 and f_2 are irreducible and $f_1 \neq f_2$. Assume Δ_A is connected with a non-exact edge. Then the class graph of A is connected.*

Proof. Set $d_1 = \deg f_1$, $d_2 = \deg f_2$ and let $m = \mathrm{lcm}(d_1, d_2)$. The edge $\{f_1, f_2\}$ is non-exact so either $d_1 z_1 > m$ or $d_2 z_2 > m$. We may assume without loss of generality that $d_1 z_1 > m$. Let ε be a generator for $GF(q^m)^*$ and let $g_\varepsilon(t) = (t-\varepsilon)(t-\varepsilon^q)\ldots(t-\varepsilon^{q^{m-1}})$ with companion matrix $C(g_\varepsilon)$. Choose k_1, k_2 such that ε^{k_1} and ε^{k_2} are roots of f_1 and f_2 respectively.

First suppose $d_2 z_2 = m$. Let

$$X = \mathrm{diag}(C(g_\varepsilon)^{k_1}, \underbrace{C(f_1), \ldots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C(g_\varepsilon)^{k_2})$$

and

$$Y = \operatorname{diag}(C(g_\varepsilon)^{k_2}, \underbrace{C(f_1), \ldots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C(g_\varepsilon)^{k_1}).$$

Then X and Y commute and are in the conjugacy class of A by the discussion before the lemma. By Corollary 3.3.4, the stabilizer of Γ_X contains $\operatorname{diag}(GL(d_1z_1, q), \langle C(g_\varepsilon)\rangle)$ and the stabilizer of Γ_Y contains $\operatorname{diag}(\langle C(g_\varepsilon)\rangle, GL(d_1z_1, q))$. Therefore by Lemma 3.1.5 the stabilizer of the connected component containing X and Y is $GL(n, q)$. So the class graph is connected in this case.

Now suppose $d_2z_2 > m$. This time let

$$X = \operatorname{diag}(C(g_\varepsilon)^{k_1}, \underbrace{C(f_1), \ldots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C(g_\varepsilon)^{k_2}, \underbrace{C(f_2), \ldots, C(f_2)}_{z_2 - \frac{m}{d_2} \text{ times}}),$$

so the stabilizer of Γ_X contains $\operatorname{diag}(GL(d_1z_1, q), GL(d_2z_2, q))$, and let

$$Y = \operatorname{diag}(C(g_\varepsilon)^{k_2}, \underbrace{C(f_1), \ldots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C(g_\varepsilon)^{k_1}, \underbrace{C(f_2), \ldots, C(f_2)}_{z_2 - \frac{m}{d_2} \text{ times}}),$$

so the stabilizer of Γ_Y contains

$$\operatorname{diag}(\langle C(g_\varepsilon)\rangle, GL(d_1z_1, q), \langle C(f_2)\rangle, \ldots, \langle C(f_2)\rangle).$$

Again X and Y commute and are in the conjugacy class of A so $\Gamma_X = \Gamma_Y$. Therefore the stabilizer of Γ_X is $GL(n, q)$ by two applications of Lemma 3.1.5. $\square$

Lemma 3.3.8 *Assume $A \in GL(n, q)$ is semisimple with characteristic polynomial $f_A = f_1^{z_1} \ldots f_r^{z_r}$, where f_i is irreducible for $1 \leqslant i \leqslant r$, and $f_i \neq f_j$ for $i \neq j$. Assume Δ_A is connected with at least one non-exact edge. Then the class graph of A is connected.*

Proof. Set $d_i = \deg f_i$, for $1 \leqslant i \leqslant r$. We proceed by induction on r. The case $r = 2$ is

Lemma 3.3.7, so assume $r > 2$.

By Corollary 3.1.9, we can choose a vertex e in Δ_A such that the graph $\Delta_A \setminus \{e\}$ is connected with at least one non-exact edge. Without lose of generality suppose $e = f_r$. Then $\Delta_A \setminus \{f_r\}$ is connected with at least one non-exact edge and so the class in $GL(n - d_r z_r, q)$ corresponding to $f^* = f_1^{z_1} \dots f_{r-1}^{z_{r-1}}$ is connected by induction.

In Δ_A, f_r is connected to another vertex, say f_1. Let $m = \mathrm{lcm}(d_1, d_r)$ and let ε be a generator of $GF(q^m)^*$. Choose k_1, k_r such that ε^{k_1} and ε^{k_r} are roots of f_1 and f_r respectively. Set

$$C_i = (\underbrace{C(f_i), \dots, C(f_i)}_{z_i \text{ times}}),$$

for $2 \leqslant i \leqslant r-1$. There are three cases to consider.

First suppose the edge $\{f_1, f_r\}$ is exact. Then let

$$X = \mathrm{diag}(C(g_\varepsilon)^{k_1}, C_2, \dots, C_{r-1}, C(g_\varepsilon)^{k_r})$$

and

$$Y = \mathrm{diag}(C(g_\varepsilon)^{k_r}, C_2, \dots, C_{r-1}, C(g_\varepsilon)^{k_1}).$$

Then by induction $\mathit{\Gamma}_X$ is stabilized by $\mathrm{diag}(GL(n - d_r z_r, q), \langle C(g_\varepsilon) \rangle)$ and $\mathit{\Gamma}_Y$ is stabilized by $\mathrm{diag}(\langle C(g_\varepsilon) \rangle, GL(n - d_r z_r, q))$. Since X and Y commute we have $\mathit{\Gamma}_X = \mathit{\Gamma}_Y$ so $\mathit{\Gamma}_X$ is stabilized by $GL(n, q)$ by Lemma 3.1.5, and hence the class graph is connected.

Next suppose $\{f_1, f_r\}$ is non-exact and $d_r z_r = m$. We let

$$X = \mathrm{diag}(C(g_\varepsilon)^{k_1}, \underbrace{C(f_1), \dots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C_2, \dots, C_{r-1}, C(g_\varepsilon)^{k_r}),$$

and

$$Y = \mathrm{diag}(C(g_\varepsilon)^{k_r}, \underbrace{C(f_1), \dots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C_2, \dots, C_{r-1}, C(g_\varepsilon))^{k_1}).$$

Then Γ_X is stabilized by

$$\mathrm{diag}(GL(n - d_r z_r, q), \langle C(g_\varepsilon) \rangle),$$

and Γ_Y is stabilized by

$$\mathrm{diag}(\langle C(g_\varepsilon) \rangle, GL(n - d_r z_r, q)).$$

So again by Lemma 3.1.5 we see $GL(n, q)$ stabilizes $\Gamma_X = \Gamma_Y$ and so the class graph is connected.

Finally suppose $\{f_1, f_r\}$ is non-exact and $d_r z_r > m$. This time we let

$$X = \mathrm{diag}(C(g_\varepsilon)^{k_1}, \underbrace{C(f_1), \dots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C_2, \dots, C_{r-1}, C(g_\varepsilon)^{k_r}, \underbrace{C(f_r), \dots, C(f_r)}_{z_r - \frac{m}{d_r} \text{ times}}),$$

and

$$Y = \mathrm{diag}(C(g_\varepsilon)^{k_r}, \underbrace{C(f_1), \dots, C(f_1)}_{z_1 - \frac{m}{d_1} \text{ times}}, C_2, \dots, C_{r-1}, C(g_\varepsilon)^{k_1}, \underbrace{C(f_r), \dots, C(f_r)}_{z_r - \frac{m}{d_r} \text{ times}}).$$

Then by Lemma 3.3.4, the stabilizer of Γ_X contains $\mathrm{diag}(GL(n - d_r z_r, q), GL(d_r z_r, q))$ and the stabilizer of Γ_Y contains

$$\mathrm{diag}(\langle C(g_\varepsilon) \rangle, GL(n - d_r z_r, q), \langle C(f_r) \rangle, \dots, \langle C(f_r) \rangle).$$

So by Lemma 3.1.5, $\Gamma_X = \Gamma_Y$ is stabilized by $GL(n, q)$ and hence the class graph is connected. $\square$

We now consider when the class graph $\mathit{\Gamma}$ is disconnected.

Lemma 3.3.9 *Suppose $T \in GL(n,q)$ is semisimple with characteristic polynomial $f_T = f_1^{z_1} \dots f_r^{z_r}$, where f_i is irreducible for $1 \leqslant i \leqslant r$, and $f_i \neq f_j$ for $i \neq j$. Suppose also that Δ_T is connected, but all edges are exact. Then the class graph of T is disconnected.*

Proof. For $1 \leqslant i \leqslant r$, set $d_i = \deg f_i$. Since all the edges of Δ_T are exact, we have $d_1 z_1 = \dots = d_r z_r = m$. Let $X = \operatorname{diag}(A_1, \dots, A_r)$, where $A_i \in GL(m,q)$ has characteristic polynomial $f_i^{z_i}$. Then X is conjugate to T. Suppose $Y \in C_{GL(n,q)}(X) \cap cl_{GL(n,q)}(X)$. By Corollary 3.2.5, $Y = \operatorname{diag}(B_1, \dots, B_r)$, where $B_i \in GL(m,q)$ for $1 \leqslant i \leqslant r$. Since $Y \in cl_G(X)$, Y also has characteristic polynomial f_T and so for $1 \leqslant i \leqslant r$, $f_{B_i} = f_1^{w_{i1}} \dots f_r^{w_{ir}}$ with $0 \leqslant w_{ij} \leqslant z_j$.

Suppose there exists $i \in \{1, \dots, r\}$ such that $w_{ik}, w_{il} \neq 0$ for $1 \leqslant k, l \leqslant r$ with $k \neq l$. We may assume without loss of generality that $k \neq i$. Then as A_i and B_i commute, d_i divides $d_k w_{ik}$ by Lemma 3.2.6. Then $a d_i = d_k w_{ik}$ for some $a \in \mathbb{Z}$ and since $w_{ik} < z_k$, the vertices f_i, f_k in Δ_T are connected with a non-exact edge, a contradiction. Therefore for each $i \in \{1, \dots, r\}$, there exists $j \in \{1, \dots, r\}$ such that $f_{B_i} = f_j^{z_j}$.

Now suppose $Z \in \mathit{\Gamma}_X$. Then there exist $Y_1, \dots, Y_t \in \mathit{\Gamma}_X$ such that $Y_1 \in C_G(X)$, $Y_i \in C_G(Y_{i-1})$ for $2 \leqslant i \leqslant t$, and $Z \in C_G(Y_t)$. By using the above result on each of the pairs (X, Y_1),(Y_{i-1}, Y_i) for $2 \leqslant i \leqslant t$ and (Y_t, Z), we see Z has the form $\operatorname{diag}(B_1, \dots, B_r)$ with $B_i \in GL(m,q)$ and $f_{B_i} = f_j^{z_j}$ for some j.

Suppose $\mathit{\Gamma}$ is connected. Then $\langle cl_G(X) \rangle \subseteq \operatorname{diag}(GL(m,q), \dots, GL(m,q))$ and so $SL(n,q) \nleqslant \langle cl_G(X) \rangle$. Therefore as $\langle cl_G(X) \rangle \trianglelefteq GL(n,q)$, $\langle cl_G(X) \rangle$ is central [Huppert p.185], a contradiction. Thus the class graph is disconnected. $\square$

Lemma 3.3.10 *Suppose $T \in GL(n,q)$ is semisimple and Δ_T is disconnected. Then the class graph of T is disconnected.*

Proof. Let $f_T = f_1^{z_1} \dots f_r^{z_r}$ be the characteristic polynomial of T, where each f_i is irreducible over $GF(q)$ and $f_i \neq f_j$ for $i \neq j$. Since Δ_T is disconnected, we may choose δ_1 , δ_2 such that $\{f_i, f_j\}$ is not an edge of Δ_T for all $f_i \in \delta_1$, $f_j \in \delta_2$. Relabelling if necessary, suppose $\delta_1 = \{f_1, \dots, f_s\}$ and $\delta_2 = \{f_{s+1}, \dots, f_r\}$.

Let $X = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$, where A and B have characteristic polynomials $f_A = f_1^{z_1} \dots f_s^{z_s}$ and $f_B = f_{s+1}^{z_{s+1}} \dots f_r^{z_r}$ respectively. We have X and T are conjugate. Suppose $Y \in C_{GL(n,q)}(X) \cap cl_{GL(n,q)}(X)$. By Corollary 3.2.5, $Y = \left(\begin{array}{c|c} C & 0 \\ \hline 0 & D \end{array}\right)$, where $C \in GL(d_1 z_1 + \dots + d_s z_s, q)$. Now C has characteristic polynomial $f_C = f_1^{w_1} \dots f_r^{w_r}$ for $0 \leqslant w_i \leqslant z_i$ with $\sum_{i=1}^{s} z_i \deg f_i = \sum_{i=1}^{r} w_i \deg f_i$. Suppose $w_i \neq 0$ for some $s+1 \leqslant i \leqslant r$, then by Lemma 3.2.7, there exists $k \in \{1, \dots, s\}$ such that $a \deg f_i = b \deg f_k$ with $1 \leqslant a \leqslant w_i$, $1 \leqslant b \leqslant z_k$. Therefore there is an edge between f_i and f_j in Δ_T, a contradiction.

So we have $w_i = 0$ for $s+1 \leqslant i \leqslant r$ and hence $f_C = f_A$. Therefore the only elements in the connected component of the class graph containing X have the same shape as Y and $f_C = f_A$, $f_D = f_B$. Let $Z = \left(\begin{array}{c|c} B & 0 \\ \hline 0 & A \end{array}\right)$ and note Z is conjugate to X, but $f_B \neq f_A$. Therefore Z is not connected to X and hence Γ is disconnected. $\square$

We can now prove Theorem 3.3.5.

Proof (of Theorem 3.3.5). By Lemma 3.3.8, we have the class graph of T is connected if Δ_T is connected with at least one edge non-exact, and in Lemmas 3.3.9 and 3.3.10, we showed the class graph of T is disconnected otherwise. $\square$

Chapter 4

Commuting Graphs of Unipotent Elements of $GL(n, q)$

In this chapter we discuss the connectedness of commuting graphs for conjugacy classes of unipotent elements in $GL(n, q)$, where $q = p^a$ for some prime p and $a \in \mathbb{N}$. Recall an element $x \in GL(n, q)$ is unipotent if it has order a power of p. Equivalently x is unipotent if all of its eigenvalues are 1.

A Jordan block of size m is an $m \times m$ matrix of the form

$$B_m = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \ddots & 1 & 0 \\ 0 & 0 & \dots & \dots & 1 & 1 \end{pmatrix}.$$

A matrix $x = \mathrm{diag}(B_{m_1}, \dots, B_{m_r})$, where each B_{m_i} is a Jordan block of size m_i, is in Jordan normal form. Every unipotent element in $GL(n, q)$ is conjugate to a matrix in Jordan normal form, and we say $y \in GL(n, q)$ has type $(m_1, \dots, m_r)$ if it is conjugate to

$\mathrm{diag}(B_{m_1}, \ldots, B_{m_r})$. Note $\sum_{i=1}^{r} m_i = n$.

Throughout this chapter we denote the class graph we are considering by Γ and let Γ_x be the connected component of Γ containing x. In Sections 4.5 and 4.6 we will need the exponent ε of $PGL(2,q)$. We note here that if p is even, $\varepsilon = p(q^2-1)$ and if p is odd, $\varepsilon = p(q^2-1)/2$.

4.1 Preliminary Results

In this section we record some standard results and definitions that will be used later in the chapter. We start with some easy lemmas about matrices.

Lemma 4.1.1 *Suppose $M \in GL(2,q)$ is a non-scalar matrix. There exists a conjugate of M with non-zero top right entry.*

Proof. Let

$$M = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix},$$

and suppose all elements in the conjugacy class of M also have a zero for their top right entry. Conjugating M by

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

gives $b = 0$, and then conjugating by

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

gives $a = c$. Therefore M is a scalar matrix. □

Lemma 4.1.2 *Suppose $M \in GL(2,q)$ is a non-scalar matrix with projective order α.*

Then for any $k \in \mathbb{Z}$ with $k \not\equiv 0 \bmod \alpha$, there is a conjugate of M with non-zero top right entries in both itself and its kth power.

Proof. Let $N = M^k$. Since N is non-scalar, some conjugate N^L, with $L \in GL(2,q)$, must have non-zero top right entry by Lemma 4.1.1. Then $(M^L)^k = (M^k)^L = N^L$. So M^L is a conjugate of M with a non-zero entry in the top right of its kth power. Since any power of a lower triangular matrix is lower triangular, M^L also has a non-zero top right entry. □

Lemma 4.1.3 *Suppose $M \in GL(2,q)$ has non-zero top right entry, but zero top right entry in its mth power. Let α be the projective order of M and set $l = (\alpha, m)$. Then the top right entry of M^l is zero.*

Proof. As $(\alpha, m) = l$, there exist $s, r \in \mathbb{Z}$ such that $\alpha r + ms = l$. Then

$$M^l = M^{\alpha r + ms} = t(M^m)^s$$

for some scalar t. Therefore M^l is a scalar multiple of a power of a lower triangular matrix and so has top right entry zero. □

Lemma 4.1.4 *Let $M \in GL(2,q)$ have top right entry non-zero and suppose M^m has top right entry equal zero, where $m \in \mathbb{Z}$. Then $M^m \in Z(GL(2,q))$.*

Proof. Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } M^m = \begin{pmatrix} a_m & 0 \\ c_m & d_m \end{pmatrix}.$$

We note $M \in C_{GL(2,q)}(M^m)$ and so

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_m & 0 \\ c_m & d_m \end{pmatrix} = \begin{pmatrix} a_m & 0 \\ c_m & d_m \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Hence

$$\begin{pmatrix} aa_m + bc_m & bd_m \\ ca_m + dc_m & dd_m \end{pmatrix} = \begin{pmatrix} aa_m & ba_m \\ ac_m + cd_m & bc_m + dd_m \end{pmatrix}.$$

So since $b \neq 0$, we have $a_m = d_m$ and $c_m = 0$. $\square$

Lemma 4.1.5 *Let $a \in GF(q)^*$ and suppose $m \in \mathbb{Z}_{>0}$ is even. There exists $A \in GL(2,q)$ such that $A \notin Z(GL(2,q))$, $A^m \in Z(GL(2,q))$ and* $\det A = a$.

Proof. Let

$$A = \begin{pmatrix} 0 & 1 \\ -a & 0 \end{pmatrix}.$$

Then $A \in GL(2,q)$, $A \notin Z(GL(2,q))$ and $\det A = a$. Also

$$A^m = (A^2)^{\frac{m}{2}} = \begin{pmatrix} (-a)^{\frac{m}{2}} & 0 \\ 0 & (-a)^{\frac{m}{2}} \end{pmatrix} \in Z(GL(2,q)). \quad \square$$

Lemma 4.1.6 *Suppose $g_m \in GL(2m,q)$ with*

$$g_m = \begin{pmatrix} a_1 & 0 & \dots & 0 & b_1 & 0 & \dots & 0 \\ * & a_2 & \ddots & \vdots & * & b_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ * & \dots & * & a_m & * & \dots & * & b_m \\ c_1 & 0 & \dots & 0 & d_1 & 0 & \dots & 0 \\ * & c_2 & \ddots & \vdots & * & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ * & \dots & * & c_m & * & \dots & * & d_m \end{pmatrix}.$$

Then $\det g_m = \prod_{i=1}^{m}(a_i d_i - b_i c_i)$.

Proof. We proceed by induction. The result is clear for $m = 1$, so now consider $m = k$ for $k > 1$.

$$
\begin{aligned}
\det g_k =& a_k \det \begin{pmatrix}
a_1 & 0 & 0 & b_1 & 0 & \dots & 0 \\
* & \ddots & 0 & * & \ddots & \ddots & \vdots \\
* & * & a_{k-1} & * & * & b_{k-1} & 0 \\
c_1 & 0 & 0 & d_1 & 0 & \dots & 0 \\
* & \ddots & 0 & * & \ddots & \ddots & \vdots \\
* & * & c_{k-1} & \vdots & \ddots & \ddots & 0 \\
* & \dots & * & * & \dots & * & d_k
\end{pmatrix} \\
&+ (-1)^k c_k \det \begin{pmatrix}
a_1 & 0 & 0 & b_1 & 0 & \dots & 0 \\
* & \ddots & 0 & * & \ddots & \ddots & \vdots \\
* & * & a_{k-1} & \vdots & \ddots & \ddots & 0 \\
* & \dots & * & * & \dots & * & b_k \\
c_1 & 0 & 0 & d_1 & 0 & \dots & 0 \\
* & \ddots & 0 & * & \ddots & \ddots & \vdots \\
* & * & c_{k-1} & * & * & d_{k-1} & 0
\end{pmatrix} \\
=& (a_k d_k - b_k c_k) \det g_{k-1} \\
=& \prod_{i=1}^{k} (a_i d_i - b_i c_i),
\end{aligned}
$$

by induction. $\square$

Lemma 4.1.7 *Let α be a generator of $GF(q)^*$ and let m be even. Then* $\left\langle \alpha^m, \alpha^{\frac{m(m-1)}{2}} \right\rangle = \left\langle \alpha^{\frac{m}{2}} \right\rangle$.

Proof. Let $K = \left\langle \alpha^m, \alpha^{\frac{m(m-1)}{2}} \right\rangle$ and $L = \left\langle \alpha^{\frac{m}{2}} \right\rangle$. It is clear $K \leqslant L$. Also note, as m is even, $\frac{m-2}{2} \in GF(q)^*$, and

$$\alpha^{\frac{m(m-1)}{2}}(\alpha^m)^{-(\frac{m-2}{2})} = \alpha^{\frac{m}{2}}.$$

Therefore $L \leqslant K$. $\square$

Let V be an n-dimensional vector space over $GF(q)$ and set $G = GL(n, q)$. Our strategy in this chapter will be to consider whether there are any subspaces fixed by all elements in $\mathit{\Gamma}_x$. If not we will then show the stabilizer in $GL(n, q)$ of the connected component $\mathit{\Gamma}_x$ is irreducible. In Section 4.4 we show if $Stab_G(\mathit{\Gamma}_x)$ is irreducible, then $SL(n, q) \subseteq Stab_G(\mathit{\Gamma}_x)$. The leads to the following definition.

Definition 4.1.8 *A graph $\mathit{\Gamma}$ is* S-connected *if $SL(n, q) \subseteq Stab_G(\mathit{\Gamma}_x)$ for some $x \in V(\mathit{\Gamma})$.*

Once we have determined a graph is S-connected, we will consider whether it is connected.

We now introduce the subspaces of V we will be using.

Definition 4.1.9 *Let $x \in G$. For any $v \in V$, let $[v, x] = v(x-1)$ and $[V, x] = \{[v, x] \mid v \in V\}$. Set $[V, x; 1] = [V, x]$, and for $k > 1$, write $[V, x; k] = [[V, x; k-1], x]$.*

Lemma 4.1.10 *Let $x \in G$. For any $k \in \mathbb{Z}_{>0}$, $[V, x; k]$ is a $C_G(x)$-invariant subspace.*

Proof. Let $y \in C_G(x)$. Then for any $v \in V$,

$$\begin{aligned}
[v, x; k]y &= v(x-1)^k y \\
&= vy(x-1)^k \\
&= [vy, x; k] \\
&\in [V, x; k].
\end{aligned}$$

$\square$

Lemma 4.1.11 *Suppose $y \in C_G(x)$ and $[V, x] = [V, y]$. Then $[V, x; k] = [V, y; k]$ for any $k \in \mathbb{Z}_{>0}$.*

Proof. We proceed by induction on k. Suppose $[V, x; i] = [V, y; i]$ for all $1 \leqslant i < k$. Then

$$\begin{aligned} [V, x; k] &= [[V, x; k-1], x] \\ &= [[V, y; k-1], x] \\ &= [[V, x], y; k-1], \text{as } y \in C_G(x), \\ &= [[V, y], y; k-1] \\ &= [V, y; k]. \end{aligned}$$

□

Definition 4.1.12 *Let $x \in G$. Then $Soc(x) = \{v \in V \mid [v, x] = 0\}$, and for $k \in \mathbb{Z} > 0$, $Soc^k(x) = \{v \in V \mid [v, x; k] = 0\}$. When we want to emphasize the space rather than the element of G we use the notation $Soc(V)$ instead of $Soc(x)$.*

Lemma 4.1.13 *For $x \in G$ and $k \in \mathbb{Z} > 0$, $Soc^k(x)$ is a $C_G(x)$-invariant space.*

Proof. Let $y \in C_G(x)$, $v \in \mathrm{Soc}^k(x)$. Then

$$\begin{aligned} [vy, x; k] &= vy(x-1)^k \\ &= v(x-1)^k y \\ &= [v, x; k]y \\ &= 0. \end{aligned}$$

So $vy \in \mathrm{Soc}^k(x)$. □

Lemma 4.1.14 *Suppose $y \in C_G(x)$ and $Soc(x) = Soc(y)$. Then $Soc^k(x) = Soc^k(y)$ for all $k \in \mathbb{Z}_{>0}$.*

Proof. Suppose $v \in \mathrm{Soc}^k(x)$. Then $[v, x; k-1] \in \mathrm{Soc}(x) = \mathrm{Soc}(y)$, and so $[[v, x; k-1], y] = 0$. But $[[v, x; k-1], y] = [[v, y], x; k-1]$ so $[v, y] \in \mathrm{Soc}^{k-1}(x)$. Inductively, $\mathrm{Soc}^{k-1}(x) = \mathrm{Soc}^{k-1}(y)$, hence $[v, y] \in \mathrm{Soc}^{k-1}(y)$. Then $[v, y; k] = 0$, therefore $v \in \mathrm{Soc}^k(y)$ and so $\mathrm{Soc}^k(x) \subseteq \mathrm{Soc}^k(y)$. The opposite containment is similar. $\square$

Definition 4.1.15 *A* cyclic basis *for x is a basis $\mathcal{B}$ of V such that $[v, x] \in \mathcal{B}$ or $[v, x] = 0$ for all $v \in \mathcal{B}$. Let $\mathcal{B}$ be a cyclic basis for x, and $B = \{v \in \mathcal{B} \mid [u, x] \neq v \text{ for all } u \in \mathcal{B}\}$. Then B is a* cyclic basis generating set *for $\mathcal{B}$.*

Lemma 4.1.16 *Let $x \in G$ be unipotent. An element in the centralizer of x is completely determined by its action on a cyclic basis generating set for x.*

Proof. This is Lemma 3.6 in [7]. $\square$

Lemma 4.1.17 *Suppose $x \in G$ is unipotent of type (m, m). Then any two linearly independent vectors in $V \setminus [V, x]$ can be used to generate a cyclic basis of V for x.*

Proof. Let $v_1, u_1 \in V \setminus [V, x]$ be linearly independent and set $v_i = [v_1, x; i-1], u_i = [u_1, x; i-1]$ for $2 \leqslant i \leqslant m$. Let $\mathcal{B} = \{v_i, u_i \mid 1 \leqslant i \leqslant m\}$. As $v_1, u_1 \in V \setminus [V, x]$, we have $|\mathcal{B}| \leqslant 2m$. Suppose $\mathcal{B}$ is not linearly independent. For each i, $v_i, u_i \in [V, x; i-1] \setminus [V, x; i]$. Let i be minimal such that v_i, u_i are not linearly independent. Then there exist $\lambda, \mu \in GF(q)^*$ such that $\lambda v_i + \mu u_i \in [V, x; i]$. This implies

$$\lambda v_{i-1} + \mu u_{i-1} + [V, x; i-1] \in \mathrm{Soc}\left(V/[V, x; i]\right) = [V, x; i-1]/[V, x; i].$$

Then $\lambda v_{i-1} + \mu u_{i-1} \in [V, x; i-1]$, contradicting the minimality of i. $\square$

Definition 4.1.18 *An element $x \in GL(n, q)$ is* regular unipotent *if it is unipotent of type (n).*

We consider the class graph of a regular unipotent element in Section 4.2, but, as the following lemma suggests, regular unipotent elements are also useful in some of the other cases we consider.

Lemma 4.1.19 *A regular unipotent element fixes precisely one subspace of* V *of each dimension* $1, \ldots, n$.

Proof. Let $x \in G$ be regular unipotent and $\mathcal{B}$ be a cyclic basis for x. Then with respect to $\mathcal{B}$, x is in Jordan normal form and it is clear $[V, x; i]$ is the unique subspace of V of dimension $n - i$ fixed by x, for $0 \leqslant i < n$. $\square$

We now consider centralizers of general unipotent elements in G.

Definition 4.1.20 *A matrix over* $GF(q)$ *is* triangularly striped *if it has the form*

(i)

$$\begin{pmatrix} a_1 & 0 & \ldots & 0 \\ a_2 & a_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_r & \ldots & a_2 & a_1 \end{pmatrix},$$

(ii)

$$\begin{pmatrix} 0 & \ldots & \ldots & 0 \\ \vdots & & & \vdots \\ 0 & \ldots & \ldots & 0 \\ a_1 & 0 & \ldots & 0 \\ a_2 & a_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_r & \ldots & a_2 & a_1 \end{pmatrix}, \textit{ or}$$

(iii)

$$\begin{pmatrix} a_1 & 0 & \dots & \dots & \dots & \dots & 0 \\ a_2 & a_1 & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ a_r & \dots & a_2 & a_1 & 0 & \dots & 0 \end{pmatrix},$$

with $a_i \in GF(q)$ for $1 \leqslant i \leqslant r$.

Lemma 4.1.21 *Suppose $x \in GL(n,q)$ is unipotent of type $(m_1, m_2, \dots, m_t)$, written in Jordan normal form. Then*

$$C_G(x) = \left\{ \begin{pmatrix} C_{11} & \dots & C_{1t} \\ \vdots & & \vdots \\ C_{t1} & \dots & C_{tt} \end{pmatrix} \in G \;\middle|\; C_{ij} \text{ is a triangularly striped } m_i \times m_j \text{ matrix} \right\}.$$

Proof. This is [38, p.28]. □

Example 4.1.22 *Let*

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \in GL(5,q).$$

Then

$$C_G(x) = \left\{ \begin{pmatrix} a_1 & 0 & 0 & 0 & 0 \\ a_2 & a_1 & 0 & b_1 & 0 \\ a_3 & a_2 & a_1 & b_2 & b_1 \\ c_1 & 0 & 0 & d_1 & 0 \\ c_2 & c_1 & 0 & d_2 & d_1 \end{pmatrix} \middle| \; a_1, d_1 \in GF(q)^*, a_2, a_3, b_1, b_2, c_1, c_2, d_2 \in GF(q) \right\}.$$

We have the following corollaries to Lemma 4.1.21.

Corollary 4.1.23 *Let $x \in G$ be regular unipotent. Then $|C_G(x)| = (q-1)q^{n-1}$.*

Proof. Choose a basis of V so x is written in Jordan normal form. Then

$$C_G(x) = \left\{ \begin{pmatrix} a_1 & 0 & \dots & 0 \\ a_2 & a_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_n & \dots & a_2 & a_1 \end{pmatrix} \middle| \; a_1 \in GF(q)^*, a_i \in GF(q) \text{ for } 2 \leqslant i \leqslant n \right\},$$

by Lemma 4.1.21, and the result is clear. □

Corollary 4.1.24 *Suppose $x \in GL(2m, q)$ is unipotent of type (m, m). Then every element in $C_G(x)$ has determinant an mth power.*

Proof. Choose a basis of V so x is written in Jordan normal form and let $g \in C_G(x)$.

Then $t = 2$ so by Lemma 4.1.21,

$$g = \begin{pmatrix} C_{1,1} & C_{1,2} \\ C_{2,1} & C_{2,2} \end{pmatrix} = \begin{pmatrix} a & & & b & & \\ * & \ddots & & * & \ddots & \\ * & * & a & * & * & b \\ c & & & d & & \\ * & \ddots & & * & \ddots & \\ * & * & c & * & * & d \end{pmatrix},$$

for some $a, b, c, d \in GF(q)$. Therefore by Lemma 4.1.6, $\det g = (ad - bc)^m$. $\square$

Definition 4.1.25 *Let V be an n-dimensional vector space over $GF(q)$, with $n \geqslant 2$. A* transvection *is an element of $GL(V)$ such that $\dim[V, t] = 1$, $\dim C_V(t) = n - 1$ and $[V, t] \subseteq C_V(t)$. An $n-1$-dimensional subspace of V is a* hyperplane *and a 1-dimensional subspace of V is a* point*. For a hyperplane $H \subset V$ and a point $P \subseteq H$, let $R(H, P) = \langle t \in GL(V) \mid H = C_V(t), P = [V, t]\rangle$. We say $R(H, P)$ is a* subgroup of root type *and elements of $R(H, P)$ are root elements.*

We note for any $g \in G$, $R(H, P)^g = R(H^g, Pg)$, so the conjugate of a root subgroup is a root subgroup.

The following two results of McLaughlin [34, 35], about groups generated by subgroups of root type, will be used in Section 4.4.

Theorem 4.1.26 *Suppose $\mathbb{F} \neq GF(2)$, V is a vector space over $\mathbb{F}$ with $\dim V \geqslant 2$, and G is a subgroup of $SL(V)$ which is generated by subgroups of root type. Also suppose the identity subgroup 1 is the only normal unipotent subgroup of G. Then for some $s \geqslant 1$, $V = V_0 \oplus V_1 \oplus \ldots \oplus V_s$ and $G = G_1 \times \ldots \times G_s$, where*

(i) The V_i are stable for the G_j;

(ii) $G_i|_{V_j} = 1$ *if* $i \neq j$*;*

(iii) $G_i|_{V_i} = SL(V_i)$ *or* $Sp(V_i)$*.*

Theorem 4.1.27 *Suppose* $\mathbb{F} = GF(2)$*,* V *is a vector space over* $\mathbb{F}$ *of dimension* $n \geqslant 2$*, and* G *is an irreducible subgroup of* $SL(V)$ *which is generated by transvections. Then either* $G = SL(V)$ *or* $n \geqslant 4$ *and* G *is a subgroup of* $Sp(V)$*.*

We conclude this section with a few results about vector spaces with forms which will also be used in Section 4.4. Let $[V,T] = \{[v,t] \mid v \in V, t \in T\}$ and $Isom(V)$ be the group of isometries of V.

Lemma 4.1.28 *Let* V *be a finite dimensional vector space over* $\mathbb{F}$ *which supports a nondegenerate symmetric or symplectic form, and let* U *be a subspace of* V*. Then*

$$\dim U^{\perp} = \dim V - \dim U.$$

Proof. See [1, 19.2]. □

Lemma 4.1.29 *Let* V *be a finite dimensional vector space over the field* $\mathbb{F}$*. Suppose* $(\ ,\ )$ *is a nondegenerate symmetric or symplectic form on* V *and* $T \leqslant Isom(V)$*. Then* $[V,T]^{\perp} = C_V(T)$*.*

Proof. Let $v, w \in V$ and $t \in T$. Then

$$\begin{aligned}([v,t],w) &= (v(t-1),w)\\ &= (vt,w)-(v,w)\\ &= (v,wt^{-1})-(v,w)\\ &= (v,w(t^{-1}-1))\\ &= (v,[w,t^{-1}]).\end{aligned}$$

So if $w \in C_V(T)$ then $[w, t^{-1}] = 0$ for all $t \in T$ and so $([v, t], w) = 0$ for all $v \in V$, $t \in T$. Therefore $w \in [V, T]^{\perp}$. Conversely, if $w \in [V, T]^{\perp}$, then $([v, t], w) = 0$ for all $v \in V$, $t \in T$ and so $(v, [w, t^{-1}]) = 0$ for all $v \in V$, $t \in T$. Then since the form is nondegenerate, $[w, t^{-1}] = 0$ for all $t \in T$ and hence $w \in C_V(T)$. □

Lemma 4.1.30 *Suppose V is a vector space over $\mathbb{F}$ and $T \leqslant Sp(V)$ with $\dim[V, T] = 1$. Then $|T| \leqslant |\mathbb{F}|$.*

Proof. Let $0 \neq w \in [V, T]$. Then as $\dim[V, T] = 1$, for any $v \in V$, $t \in T$, there exists $\lambda \in \mathbb{F}$ such that $[v, t] = \lambda w$. So there are at most $|\mathbb{F}|$ elements in $[V, T]$.

Now, by Lemma 4.1.29, $[V, T]^{\perp} = C_V(T)$, and by Lemma 4.1.28,

$$\dim[V, T]^{\perp} = \dim V - \dim[V, T].$$

So $\dim C_V(T) = \dim V - 1$ and we can choose $u \in V \setminus C_V(T)$. Suppose there exist $t_1, t_2 \in T$ such that $[u, t_1] = [u, t_2]$. Then $ut_1 = ut_2$ and hence $u \in C_V(t_1 t_2^{-1})$. Clearly $C_V(T) \subseteq C_V(t_1 t_2^{-1})$ and so since $u \notin C_V(T)$ and $\dim C_V(T) = \dim V - 1$, we have $V = C_V(t_1 t_2^{-1})$. As $t_1 t_2^{-1} \in Aut(V)$, we have $t_1 = t_2$ and hence $[u, t_1] = [u, t_2]$ if and only if $t_1 = t_2$. Then $|\{[u, t] \mid u \in V\}| \leqslant |\mathbb{F}|$ implies $|T| \leqslant |\mathbb{F}|$. □

4.2 Regular Unipotent Classes

In this section we consider the commuting graph of a regular unipotent element in $G = GL(n, q)$.

Lemma 4.2.1 *Let $x \in G$ be regular unipotent. Then $C_G(x)$ is abelian.*

Proof. Let $\{v_n, v_{n-1}, \ldots, v_1\}$ be a cyclic basis for x. Then for $1 \leqslant i < n$, $v_{n-i} = [v_n, x; i] = v_n(x-1)^i$. Let $y \in C_G(x)$. By Lemma 4.1.16, the action of every element in $C_G(x)$ is completely given by its action on v_n, so for some $\lambda_i \in GF(q)$ we have

$$\begin{aligned} v_n y &= \sum_{i=1}^{n} \lambda_i v_i \\ &= \sum_{i=1}^{n} \lambda_i v_n (x-1)^{n-i} \\ &= v_n \sum_{i=1}^{n} \lambda_i (x-1)^{n-i}. \end{aligned}$$

Let $z = y - \sum_{i=1}^{n} \lambda_i (x-1)^{n-i}$. Then $v_n z = 0$ and for $1 \leqslant i < n$,

$$v_{n-i} z = v_n (x-1)^i z = v_n z (x-1)^i = 0,$$

as $z \in C_G(x)$. Therefore $z = 0$ and hence $y = \sum_{i=1}^{n} \lambda_i (x-1)^{n-i}$. So every element of $C_G(x)$ can be written as a polynomial in $x - 1$ and hence $C_G(x)$ is abelian. □

Corollary 4.2.2 *The connected component $\mathit{\Gamma}_x$ has diameter* 1.

Proof. This follows from Lemma 2.0.9 as $C_G(x)$ is abelian by Lemma 4.2.1. □

Since, from Lemma 2.0.9 we see the elements in $\mathit{\Gamma}_x$ are precisely the regular unipotent elements in $C_G(x)$, we can count them and hence determine how many components $\mathit{\Gamma}$ has.

Lemma 4.2.3 *Let $x \in GL(n,q)$ be a regular unipotent element in Jordan normal form. Then*

$$C_G(x) \cap cl_G(x) = \left\{ \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ \lambda_1 & 1 & \ddots & & \vdots \\ \lambda_2 & \lambda_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \lambda_{n-1} & \dots & \lambda_2 & \lambda_1 & 1 \end{pmatrix} \middle| \; \lambda_i \in GF(q) \text{ for } 1 \leqslant i \leqslant n-1, \lambda_1 \neq 0 \right\}.$$

Proof. Since all unipotent elements have characteristic polynomial $f(t) = (t-1)^n$, the unipotent elements in $C_G(x)$ are those with 1's on the leading diagonal.

Recall, a regular unipotent element fixes a unique 1-space. Let $\{v_n, \dots, v_1\}$ be a cyclic basis for x and let

$$y = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ \lambda_1 & 1 & \ddots & & \vdots \\ \lambda_2 & \lambda_1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \lambda_{n-1} & \dots & \lambda_2 & \lambda_1 & 1 \end{pmatrix},$$

with $\lambda_i \in GF(q)$, $1 \leqslant i \leqslant n-1$. If $\lambda_1 = 0$ then both $\langle v_1 \rangle$ and $\langle v_2 \rangle$ are fixed by y, and if $\lambda_1 \neq 0$, the only space fixed by y is $\langle v_1 \rangle$. Therefore y is regular unipotent if and only if $\lambda_1 \neq 0$. □

Corollary 4.2.4 *The number of elements in Γ_x is $q^{n-2}(q-1)$.*

Proof. We have seen above that the elements in Γ_x are precisely the conjugates of x in $C_G(x)$, and from Lemma 4.2.3 we see $|C_G(x) \cap cl_G(x)| = q^{n-2}(q-1)$. □

Theorem 4.2.5 *Let $x \in GL(n,q)$ be regular unipotent. Then the commuting class graph of x consists of $q^{\frac{(n-2)(n-3)}{2}}(q+1)\prod_{i=3}^{n}(q^i-1)$ components, each of which is a complete graph with $q^{n-2}(q-1)$ vertices.*

Proof. We have $|C_G(x)| = q^{n-1}(q-1)$ by Corollary 4.1.23, so the number of conjugates of x in G is $q^{\frac{(n-1)(n-2)}{2}}\prod_{i=2}^{n}(q^i-1)$. Each component contains $q^{n-2}(q-1)$ vertices, by Corollary 4.2.4, and is a complete graph by Corollary 4.2.2. So the number of components is $q^{\frac{(n-2)(n-3)}{2}}(q+1)\prod_{i=3}^{n}(q^i-1)$ as claimed. □

4.3 Classes where the Jordan block sizes differ by 2 or more

In this section we let x be unipotent of type $x = (m_1, m_2, \ldots, m_k)$ with $m_j \geqslant m_{j+1} + 2$, for $1 \leqslant j < k$. Let

$$B = \{v_{i,j} \mid 1 \leqslant j \leqslant k, 1 \leqslant i \leqslant m_j\}$$

be a cyclic basis for V with respect to x, where

$$[v_{i,j}, x] = \begin{cases} v_{i-1,j} & \text{if } i > 1 \\ 0 & \text{if } i = 1. \end{cases}$$

So we can think as the basis as an array, where commutating any basis element with x moves it down one row.

$$\begin{array}{cccc}
v_{m_1,1} & & & \\
v_{m_1-1,1} & & & \\
\vdots & & & \\
v_{m_2,1} & v_{m_2,2} & & \\
\vdots & \vdots & & \\
v_{m_k,1} & v_{m_k,2} & \cdots & v_{m_k,k} \\
\vdots & \vdots & \ldots & \vdots \\
v_{1,1} & v_{1,2} & \cdots & v_{1,k}
\end{array}$$

For $1 \leqslant a \leqslant m_1$, let $W_a = \langle v_{i,j} \mid i + j \leqslant a + 1 \rangle$.

The next result requires our hypothesis on the structure of Jordan blocks of x.

Lemma 4.3.1 *Let $y \in C_G(x) \cap cl_G(x)$. For $1 \leqslant a \leqslant m_1$, W_a is a y-invariant subspace of V and further, for $2 \leqslant a \leqslant m_1$, we have $[W_a, y] \subseteq W_{a-1}$.*

Proof. First note, as $m_1 > m_2$, $W_1 = \langle v_{1,1} \rangle = [V, x; m_1 - 1]$, and so is y-invariant and, furthermore, $[W_1, y] = 0$.

We now proceed by induction. Assume W_{a-1} is y-invariant. It suffices to show $[W_a, y] \subseteq W_{a-1}$ for $2 \leqslant a \leqslant m_1$, or equivalently, since

$$B \cap W_a \setminus W_{a-1} = \{v_{i,j} \in B \mid i + j = a + 1\} = \{v_{a+1-j,j} \in B \mid m_j > a - j\},$$

$[v_{a+1-j,j}, y] \in W_{a-1}$ for all $v_{a+1-j,j} \in B$, with $m_j > a - j$.

Suppose $v_{a+1-j,j} \in B$ with $m_j + j > a$. Let

$$U_{a,j} = \begin{cases} \mathrm{Soc}^{a-j+1}(x) \cap [V, x; m_j - (a-j) - 1], & \text{if } m_j - a > 0 \\ \mathrm{Soc}^{a-j+1}(x), & \text{if } m_j - a \leqslant 0. \end{cases}$$

Since $a + 1 - j$ is the smallest $h \in \mathbb{Z}$ such that $v_{a+1-j,j} \in \mathrm{Soc}^h(x)$, we see $v_{a+1-l,l} \notin \mathrm{Soc}^{a-j+1}(x)$ for $l < j$, as $a+1-l > a+1-j$. Similarly, for any $v_{a+1-l,l} \in B \cap W_a \setminus W_{a-1}$, $m_l - (a-l) - 1$ is the largest $h \in \mathbb{Z}$ such that $v_{a+1-l,l} \in [V, x; h]$. Now, for $l > j$, since $m_i \geqslant m_{i+1} + 2$ for $1 \leqslant i < k$, we have $m_j \geqslant m_l + 2(l - j)$. Then

$$\begin{aligned} m_l - (a-l) - 1 &\leqslant m_j - 2(l-j) - (a-l) - 1 \\ &= m_j - (a-j) - 1 + j - l \\ &< m_j - (a-j) - 1, \end{aligned}$$

and hence $v_{a+1-l,l} \notin [V, x; m_j - (a-l) - 1]$. Therefore $v_{a+1-j,j}$ is the only member of $B \cap W_a \setminus W_{a-1}$ which is also in $U_{a,j}$.

So $(U_{a,j} + W_{a-1})/W_{a-1}$ is a y-invariant 1-space generated by $v_{a+1-j,j} + W_{a-1}$ and hence, since y is unipotent, $[v_{a+1-j,j}, y] \in W_{a-1}$ as required. □

Corollary 4.3.2 *With x and y as in Lemma 4.3.1, $W_1 = [V, x; m_1 - 1] = [V, y; m_1 - 1]$ and so is $\langle x, y \rangle$ invariant.*

Proof. By repeated applications of Lemma 4.3.1, $[V, y; m_1 - 1] = [W_{m_1}, y; m_1 - 1] \subseteq W_1 = [V, x; m_1 - 1]$. Therefore, since $\dim[V, y; m_1 - 1] = \dim[V, x; m_1 - 1] = 1$, we have $[V, y; m_1 - 1] = [V, x; m_1 - 1]$, as required. Hence W_1 is $\langle x, y \rangle$ invariant. $\square$

Theorem 4.3.3 *Suppose x is unipotent of type $x = (m_1, m_2, \ldots, m_k)$ with $m_i \geqslant m_{i+1}+2$, for $1 \leqslant i < k$. Then the commuting graph for the conjugacy class in G of x is disconnected.*

Proof. Let Γ_x be the connected component of the commuting graph containing x. From Corollary 4.3.2 it is clear for any $y \in \Gamma_x$, we have $[V, y; m_1 - 1] = [V, x; m_1 - 1]$. Therefore since we can find $z \in cl_G(x)$ such that $[V, z; m_1 - 1] \neq [V, x; m_1 - 1]$, the commuting graph is disconnected. $\square$

4.4 Components of Commuting Graphs Stabilized by Irreducible Subgroups

Let $x \in GL(n, q)$ be unipotent and $H = \langle C_G(y) \mid y \in V(\Gamma_x) \rangle$, where Γ_x is the connected component containing x. In this section we show that if H acts irreducibly on V, then $SL(V) \leqslant H$. This result will be used in the following sections.

Lemma 4.4.1 *There is a subgroup of root type in $C_G(x)$.*

Proof. Let $\mathcal{B}$ be a cyclic basis for x, so x is in Jordan normal form with respect to $\mathcal{B}$. For any $\lambda \in GF(q)$, let

$$t_\lambda = \begin{pmatrix} 1 & 0 & \dots & \dots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & & \ddots & \ddots & 0 \\ \lambda & 0 & \dots & 0 & 1 \end{pmatrix},$$

and let $R = \langle t_\lambda | \lambda \in GF(q) \rangle$. Then $R = R(K, P)$, where $K = \langle (1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, \dots, 1, 0) \rangle$ and $P = \langle (1, 0, \dots, 0) \rangle$. By Lemma 4.1.21, $R \leqslant C_G(x)$. □

For $X \subseteq GL(V)$ let $\mathcal{R}(X)$ be the set of subgroups of root type in X and set

$$H_0 = \langle \mathcal{R}(H) \rangle .$$

Suppose H is irreducible. Recall for any group G, $O_p(G)$ is the largest normal p-subgroup of G.

Lemma 4.4.2 *We have $H_0 \trianglelefteq H$ and $O_p(H_0) = 1$.*

Proof. The conjugate of a root subgroup is a root subgroup, so for $h \in H$ and $R \in \mathcal{R}(H)$, R^h is a root subgroup of H and hence is in $\mathcal{R}(H)$. Since $\mathcal{R}(H)$ generates H_0 we have $H_0 \trianglelefteq H$.

Since $O_p(H_0)$ is a characteristic subgroup of H_0 and $H_0 \trianglelefteq H$, we have $O_p(H_0) \trianglelefteq H$ and hence $O_p(H_0) \leqslant O_p(H)$. Suppose $O_p(H) \neq 1$. For $v \in C_V(O_p(H))$, $h \in H$ and $g \in O_p(H)$, we have $vhg = vhgh^{-1}h = vh$, and so $C_V(O_p(H))$ is a H-invariant subspace of V. Therefore $C_V(O_p(H)) = 0$ or V as H is irreducible. Since $O_p(H)$ is a p-group we cannot have $C_V(O_p(H)) = 0$, and since $O_p(H)$ is a group of automorphisms of V we also cannot have $C_V(O_p(H)) = V$. Therefore $O_p(H) = 1$ and hence $O_p(H_0) = 1$ as required. □

We can now use Clifford's Theorem [27, Thm 6.5, p.80] to write

$$V|_{H_0} = W_1 \oplus \cdots \oplus W_s,$$

where the W_i are irreducible conjugate H_0-modules, i.e. $W_i = W_1 h$ for some $h \in H$.

Lemma 4.4.3 *Let t be a root element in H. Then there is a unique $i \in \{1, \ldots, s\}$ such that $[W_i, t] \neq 0$.*

Proof. As t is a root element, $\dim C_V(t) = \dim V - 1$. So since $V = W_1 \oplus \cdots \oplus W_s$, t cannot centralize all of the W_i's else $V \subseteq C_V(t)$. Now suppose $W_i, W_j \not\subseteq C_V(t)$, for some $i, j \in \{1, \ldots, s\}$, $i \neq j$, and let $U = W_i \oplus W_j$. Since t is in a root subgroup of H, $t \in H_0$, then as W_i, W_j are H_0-invariant, we have $[W_i, t] \neq [W_j, t]$. Now $[U, t] = [W_i, t] + [W_j, t]$, and hence $\dim[U, t] = \dim[W_i, t] + \dim[W_j, t] = 2$, a contradiction. □

Lemma 4.4.4 *For some $i \in \{1, \ldots, s\}$, W_i is x-invariant.*

Proof. There is a root element $t \in C_G(x)$, by Lemma 4.4.1. This t is in a subgroup of root type and so $t \in H_0$. We may suppose, without loss of generality, W_1 is not centralized by t. We claim W_1 is x-invariant. Suppose not. Note $W_1 x$ is an irreducible H_0-module and so we have $W_1 x \cong W_i$ for some $i \in \{2, \ldots, s\}$. Then, by Lemma 4.4.3, t centralizes W_i and hence $W_1 x$. So

$$\begin{aligned}
0 &= [W_1 x, t] \\
&= [W_1 x, t] x^{-1} \\
&= W_1 x (t-1) x^{-1} \\
&= W_1 (t-1) x x^{-1} \text{ as } t \in C_G(x) \\
&= [W_1, t],
\end{aligned}$$

a contradiction. $\square$

Relabeling if necessary, assume from now on that W_1 is x-invariant and $t \in C_G(x) \cap H_0$ is a root element which doesn't centralize W_1. We set $U = W_2 \oplus \ldots \oplus W_s$. Note U is centralized by t and, since $x \in H$, Ux is a H_0-module. Suppose U is not x-invariant, so $Ux + U > U$. Now, $V/U \cong W_1$ is irreducible as a H_0-module, and therefore $Ux + U = V$. Then

$$\begin{aligned}[V, t] &= [Ux + U, t] \\ &= [Ux, t] + [U, t] \\ &= [Ux, t] \text{ as } [U, t] = 0.\end{aligned}$$

So, since $[V, t] = [W_1, t] \neq 0$, and W_1 is an irreducible H_0-module, $W_1 \subseteq Ux$. Then, as W_1 is x-invariant $W_1 = W_1 x^{-1} \subseteq U$, a contradiction.

Lemma 4.4.5 *We have $s = 1$ and so H_0 is irreducible.*

Proof. Suppose $s > 1$. Let $\mathcal{B}_1$ be a cyclic basis of W_1 for x, let $\mathcal{B}_2$ be a cyclic basis of U for x and let $\mathcal{B} = \{\mathcal{B}_1, \mathcal{B}_2\}$. Then with respect to $\mathcal{B}$, x is written in Jordan normal form. Since W_1 and U are H_0-invariant, with respect to $\mathcal{B}$, any $h \in H_0$ can be written

$$h = \begin{pmatrix} H_1 & 0 \\ 0 & H_2 \end{pmatrix},$$

where $H_1 \in GL(W_1)$, $H_2 \in GL(U)$. Let Ω be the set of matrices in $Mat_{\dim W_1 \times \dim U}(q)$

with non-zero bottom left entry and zeros everywhere else and let

$$T = \left\{ \begin{pmatrix} I_1 & 0 \\ C & I_2 \end{pmatrix} \;\middle|\; C \in \Omega \right\},$$

where I_1 and I_2 are appropriately sized identity matrices. Then T is a root subgroup in $C_G(x)$, by Lemma 4.1.21, but is not contained in H_0, a contradiction. Therefore $s = 1$ and hence H_0 is irreducible. $\square$

Now, by Lemma 4.4.5, H_0 is an irreducible subgroup generated by subgroups of root type such that $O_p(H_0) = 1$, so we can apply Theorems 4.1.26, 4.1.27 by McLaughlin to see H_0 is either $SL(V)$, $Sp(V)$ or, if $q = 2$, a subgroup of $Sp(V)$.

Suppose $H_0 = Sp(V)$ or is a subgroup of $Sp(V)$. Assume x has type $(m_1, \ldots, m_k)$, with $k > 1$, and choose a basis of V so x is written in Jordan normal form. For any $\lambda \in GF(q)$ let

$$s_\lambda = \begin{pmatrix} I_{m_1} & 0 & \ldots & 0 \\ B_\lambda & I_{m_2} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \ldots & \ldots & I_{m_k} \end{pmatrix},$$

and

$$t_\lambda = \begin{pmatrix} I_{m_1} & 0 & \ldots & 0 \\ 0 & I_{m_2} & \ldots & 0 \\ \vdots & & \ddots & \vdots \\ C_\lambda & \ldots & \ldots & I_{m_k} \end{pmatrix},$$

where B_λ and C_λ have the entry λ in their bottom left corners and zero everywhere else. Then for all $\lambda \in GF(q)$, s_λ and t_λ are transvections contained in $C_G(x)$ and hence H_0. Let $T = \langle s_\lambda, t_\lambda \mid \lambda \in GF(q) \rangle$, so $|T| \geqslant q^2$. We have $[V, s_\lambda] = [V, t_\mu]$ for all $\lambda, \mu \in GF(q)$ and hence $\dim[V,T] = 1$. Then, by Lemma 4.1.30, we see $T \nleqslant Sp(V)$ and hence $H_0 \nleqslant SP(V)$. Thus $H_0 = SL(V)$.

We have shown the following.

Theorem 4.4.6 *Let $x \in GL(n,q)$ be unipotent and $H = \langle C_G(y) \mid y \in V(\Gamma_x)\rangle$. If H is irreducible, then $SL(V) \leqslant H$.*

Proof. Let $H_0 = \langle \mathcal{R}(H)\rangle$. Then by Lemma 4.4.2 we have $H_0 \trianglelefteq H$ and $O_p(H_0) = 1$, and by Lemma 4.4.5, H_0 is irreducible on V. Therefore we can apply Theorems 4.1.26 and 4.1.27 to see H_0 is either $SL(V)$, $Sp(V)$ or a subgroup of $Sp(V)$. Then by Lemma 4.1.30 and the discussion afterwards, we have $H_0 = SL(V)$. Therefore $SL(V) \leqslant H$ as claimed.□

4.5 Classes of Type $(m, m-1)$

Suppose $x \in G$ is unipotent of type $(m, m-1)$. Let

$$\mathcal{B}_x = \{v_{i,1}, v_{j,2} \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant m-1\}$$

be a cyclic basis for x where, for $k \in \{1,2\}$,

$$[v_{i,k}, x] = \begin{cases} v_{i-1,k} & \text{if } i > 1 \\ 0 & \text{if } i = 1. \end{cases}$$

Again we can think of the basis as an array as follows.

$$\begin{array}{cc} v_{m,1} & \\ v_{m-1,1} & v_{m-1,2} \\ v_{m-2,1} & v_{m-2,2} \\ \vdots & \\ v_{1,1} & v_{1,2} \end{array}$$

where commutating a basis vector with x moves it down a row.

For $1 \leqslant k \leqslant m-1$,

$$\mathrm{Soc}^k(x) = \langle v_{i,1}, v_{i,2} \mid 1 \leqslant i \leqslant k \rangle ,$$

and

$$[V, x; k] = \langle v_{i,1}, v_{j,2} \mid 1 \leqslant i \leqslant m-k, 1 \leqslant j \leqslant m-k-1 \rangle .$$

Lemma 4.5.1 *There exists a regular unipotent element in $C_G(x)$.*

Proof. Let

$$y_m = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{$J(m)$}} & \begin{matrix} 0 & \dots & 0 \end{matrix} \\ \cline{3-3} & & \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} \\ \hline \begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & J(m-1) \end{array} \right),$$

where $J(i)$ is a Jordan block of size i. By Lemma 4.1.21, $y_m \in C_G(x)$. We show y_m is a regular unipotent element.

We have

$$y_2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

so the characteristic polynomial of y_2 is $f_{y_2}(t) = (1-t)^3$. Now, proceeding by induction and taking determinants along row 1 and then row $m+1$ in $y_m - I_{2m-1}t$ we see

$$f_{y_m}(t) = (1-t)^2 \det(y_{m-1} - I_{2m-3}t) = (1-t)^{2m+1},$$

where I_k is the k by k identity matrix. Therefore all of the eigenvalues of y_m are 1 and hence y_m is unipotent.

Next we observe that the only 1-space of V fixed by y_m is $\langle(1,0,\ldots,0)\rangle$. So y_m is a unipotent element which fixes a single 1-space and therefore y_m is regular unipotent. $\square$

Corollary 4.5.2 *There is exactly one $C_G(x)$-invariant subspace of dimension d for $d \in \{1,\ldots,n\}$.*

Proof. First note that if d is even, $d = 2k$ for some $k \in \{1,\ldots,m-1\}$ and $\dim \mathrm{Soc}^k(x) = d$. If d is odd, $d = 2k-1$ for some $k \in \{1,\ldots,m-1\}$ and $\dim[V,x;m-k] = d$. Therefore, since the spaces $\mathrm{Soc}^k(x)$ and $[V,x;k]$ are $C_G(x)$-invariant for $k \in \{1,\ldots,m\}$ by Lemmas 4.1.10 and 4.1.13, there is at least one $C_G(x)$-invariant subspace of V of each dimension. By Lemma 4.5.1 there is a regular unipotent element $z \in C_G(x)$ and, by Lemma 4.1.19, z leaves invariant exactly one subspace of each dimension. The result follows. $\square$

First we consider the case $m = 2$. Choose a basis of V such that x is given in Jordan normal form, and let

$$y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Then $y, z \in C_G(x)$ by Lemma 4.1.21, and $y, z \in cl_G(x)$. Then only proper non-trivial subspace of V are $[V,x]$ and $\mathrm{Soc}(x)$ by Corollary 4.5.2. We have $[V,x] = \langle(1,0,0)\rangle$ and $\mathrm{Soc}(x) = \langle(1,0,0),(0,0,1)\rangle$. Now note $[V,y] = \langle(0,0,1)\rangle \neq [V,x]$ and $\mathrm{Soc}(z) = \langle(1,0,0),(0,1,0)\rangle \neq \mathrm{Soc}(x)$. Let $H = \langle C_G(y) \mid y \in \Gamma_x\rangle$. We have $x, y, z \in H$ and so H acts irreducibly on V.

We now assume $m > 2$. Let $y \in C_G(x) \cap cl_G(x)$. Then the action of y on V is completely given by its action on $v_{m,1}$ and $v_{m-1,2}$ by Lemma 4.1.16, so let

$$[v_{m,1}, y] = \sum_{i=1}^{m-1} \lambda_i v_{m-i,1} + \sum_{i=1}^{m-1} \mu_i v_{m-i,2},$$

and

$$[v_{m-1,2}, y] = \sum_{i=1}^{m-1} \tau_i v_{m-i,1} + \sum_{i=1}^{m-2} \sigma_i v_{m-1-i,2}.$$

Now we note that $[V, y]$ is a $C_G(x)$-invariant subspace by Lemma 4.1.10, and $V/[V, y]$ is a 2-space. Therefore as x is unipotent, $[V, x; 2] \subseteq [V, y]$. Since $V/[V, x; 2]$ is a 4-space, we can look at the 2-space $[V, y]/[V, x; 2]$. We have

$$[v_{m,1}, y] + [V, x; 2], [v_{m-1,1}, y] + [V, x; 2], [v_{m-1,2}, y] + [V, x; 2] \in [V, y]/[V, x; 2],$$

and therefore these vectors must be linearly dependent. That is,

$$\lambda_1 v_{m-1,1} + \mu_1 v_{m-1,2} + \mu_2 v_{m-2,2} + [V, x; 2],$$

$$\mu_1 v_{m-2,2} + [V, x; 2]$$

and

$$\tau_1 v_{m-1,1} + \sigma_1 v_{m-2,2} + [V, x; 2]$$

are linearly dependent and so we see that either

$$\tau_1 = 0 \text{ or } \mu_1 = 0. \tag{4.5.3}$$

We first consider the case $\tau_1 = 0$.

Lemma 4.5.4 *If $\tau_1 = 0$, then we have $Soc^k(x) = Soc^k(y)$ for all $k \in \{1, \ldots, m\}$.*

Proof. Suppose $u \in \mathrm{Soc}(x)$. Then $u = \alpha v_{1,1} + \beta v_{1,2}$, for some $\alpha, \beta \in GF(q)$. Then

$$[u, y] = \alpha[v_{1,1}, y] + \beta[v_{1,2}, y] = \beta\tau_1 v_{1,1} = 0,$$

so $u \in \mathrm{Soc}(y)$. The lemma now follows from Lemma 4.1.14. $\square$

Next we consider the case $\tau_1 \neq 0$. Then $\mu_1 = 0$.

Lemma 4.5.5 *If $\tau_1 \neq 0$ and $\mu_1 = 0$, then for all $k \in \{1, \ldots, m\}$, we have $[V, x; k] = [V, y; k]$.*

Proof. Note

$$[v_{m,1}, y] = \sum_{i=1}^{m-1} \lambda_i v_{m-i,1} + \sum_{i=2}^{m-1} \mu_i v_{m-i,2} \in [V, x],$$

and

$$[v_{m-1,2}, y] = \sum_{i=1}^{m-1} \tau_i v_{m-i,1} + \sum_{i=1}^{m-2} \sigma_i v_{m-1-i,2} \in [V, x].$$

Therefore $[V, y] \subseteq [V, x]$, and hence $[V, y] = [V, x]$. The result now follows from Lemma 4.1.11. $\square$

Continuing the assumption $\tau_1 \neq 0$, $\mu_1 = 0$, for $0 \leqslant k \leqslant m-2$ we restrict the map defined by the commutator of y to

$$\psi_k : [V, x; k]/[V, x; k+1] \to [V, x; k+1]/[V, x; k+2].$$

So

$$(v_{m-k,1} + [V, x; k+1])\psi_k = \lambda_1 v_{m-k-1,1} + \mu_2 v_{m-k-2,2} + [V, x; k+2],$$

$$(v_{m-k-1,2} + [V, x; k+1])\psi_k = \tau_1 v_{m-k-1,1} + \sigma_1 v_{m-k-2,2} + [V, x; k+2].$$

For each k, the map ψ_k is given by the matrix

$$A = \begin{pmatrix} \lambda_1 & \mu_2 \\ \tau_1 & \sigma_1 \end{pmatrix}.$$

Lemma 4.5.6 *The matrix A is in $GL(2,q)$.*

Proof. First note $[v_{1,1}, y] = 0$ and

$$[\tau_1 v_{2,1} - \lambda_1 v_{1,2}, y] = \tau_1 [v_{2,1}, y] - \lambda_1 [v_{1,2}, y] = \tau_1 \lambda_1 v_{1,1} - \lambda_1 \tau_1 v_{1,1} = 0.$$

Therefore $\langle v_{1,1}, \tau_1 v_{2,1} - \lambda_1 v_{1,2} \rangle \subseteq \mathrm{Soc}(y)$ and, as $\tau_1 \neq 0$, we have $\dim \langle v_{1,1}, \tau_1 v_{2,1} - \lambda_1 v_{1,2} \rangle = 2$. Now suppose A is not invertible, so we have $\lambda_1 \sigma_1 - \tau_1 \mu_2 = 0$. Let

$$u = \tau_1 v_{3,1} - \lambda_1 v_{2,2} + \tau_2 v_{2,1} - \lambda_2 v_{1,2}.$$

Then

$$\begin{aligned}
[u, y] &= \tau_1 [v_{3,1}, y] - \lambda_1 [v_{2,2}, y] + \tau_2 [v_{2,1}, y] - \lambda_2 [v_{1,2}, y] \\
&= \tau_1 (\lambda_1 v_{2,1} + \lambda_2 v_{1,1} + \mu_2 v_{1,2}) - \lambda_1 (\tau_1 v_{2,1} + \tau_2 v_{1,1} + \sigma_1 v_{1,2}) + \tau_2 \lambda_1 v_{1,1} - \lambda_2 \tau_1 v_{1,1} \\
&= (\tau_1 \mu_2 - \lambda_1 \sigma_1) v_{1,2} \\
&= 0.
\end{aligned}$$

Therefore $u \in \mathrm{Soc}(y)$. As $\tau_1 \neq 0$, $u \notin \langle v_{1,1}, \tau_1 v_{2,1} - \lambda_1 v_{1,2} \rangle$ and hence $\dim \mathrm{Soc}(y) > 2$, a contradiction. $\square$

Let ε be the exponent of $PGL(2, q)$, and write

$$A^k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}.$$

Lemma 4.5.7 *Fix $k \in \{1, \ldots, m\}$ and suppose ε divides k. Then $Soc^k(y) = Soc^k(x)$.*

Proof. First note $[V, x; m-k] = [V, y; m-k]$, by Lemma 4.5.5, and so $[V, x; m-k] \subseteq \mathrm{Soc}^k(y)$. Now $\mathcal{B}_x \cap \mathrm{Soc}^k(x) \setminus [V, x; m-k] = \{v_{k,2}\}$, and $[v_{k,2}, y; k] = c_k v_{1,1}$. By Lemma 4.5.6, $A \in GL(2, q)$, and so as ε divides k, A^k is scalar and hence $c_k = 0$. Therefore $v_{k,2} \in \mathrm{Soc}^k(y)$ and hence $\mathrm{Soc}^k(x) \subseteq \mathrm{Soc}^k(y)$. So we have $\mathrm{Soc}^k(y) = \mathrm{Soc}^k(x)$ as required.□

Theorem 4.5.8 *Suppose $m > \varepsilon$. Then $Soc^\varepsilon(x) = Soc^\varepsilon(y)$, for all $y \in C_G(x) \cap cl_G(x)$.*

Proof. By 4.5.3, either $\tau_1 = 0$ or $\tau_1 \neq 0$ and $\mu_1 = 0$. If $\tau_1 = 0$, then Lemma 4.5.4 gives the result, and if $\tau_1 \neq 0$ and $\mu_1 = 0$, Lemma 4.5.7 does. □

We now consider what happens when $m \leqslant \varepsilon$.

Lemma 4.5.9 *Fix $k \in \{1, \ldots, m-1\}$ and assume ε does not divide k. Then there exists $y \in C_G(x) \cap cl_G(x)$ such that $[V, x; k] \neq [V, y; k]$.*

Proof. By Lemma 4.1.2, we can find $A \in GL(2, q)$ with non-zero entries in the top right of both A and A^k. Write

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } A^i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix},$$

so $b, b_k \neq 0$. We define an element $y \in C_G(x)$ by $[v_{m,1}, y] = av_{m-1,1} + bv_{m-1,2}$ and $[v_{m-1,2}, y] = cv_{m-2,1} + dv_{m-2,2}$. First note $[v_{m,1}, y; i] = a_i v_{m-i,1} + b_i v_{m-i,2}$ and $[v_{m-1,2}, y; i] = c_i v_{m-i-1,1} + d_i v_{m-i-1,2}$. So $[v_{m,1}, y; m] = [v_{m-1,2}, y; m] = 0$ and hence the largest Jordan block of y has size at most m. Now observe $\{v_{1,1}, v_{1,2}\} \in \mathrm{Soc}(y)$ so $\dim \mathrm{Soc}(y) \geqslant 2$. Suppose $u \in \mathrm{Soc}(y)$, where $u = \sum_{i=1}^{m} \alpha_i v_{i,1} + \sum_{i=1}^{m-1} \beta_i v_{i,2}$. Then

$$\begin{aligned}
0 &= [u, y] \\
&= \sum_{i=1}^{m} \alpha_i [v_{i,1}, y] + \sum_{i=1}^{m-1} \beta_i [v_{i,2}, y] \\
&= \sum_{i=2}^{m} \alpha_i (a v_{i-1,1} + b v_{i-1,2}) + \sum_{i=2}^{m-1} \beta_i (c v_{i-1,1} + d v_{i-1,2}) \\
&= \alpha_m (a v_{m-1,1} + b v_{m-1,2}) + \sum_{i=1}^{m-1} ((\alpha_i a + \beta_i c) v_{i-1,1} + (\alpha_i b + \beta_i d) v_{i-1,2}).
\end{aligned}$$

Then $\alpha_m b = 0$ and for $2 \leqslant i \leqslant m-1$, $\alpha_i a + \beta_i c = \alpha_i b + \beta_i d = 0$. So as $b \neq 0$, $\alpha_m = 0$ and

$$0 = \alpha_i a + \beta_i c = \alpha_i ab + \beta_i bc = -\beta_i ad + \beta_i bc = \beta_i(-ad + bc).$$

Then A invertible implies $\beta_i = 0$ and hence $\alpha_i = 0$, for $2 \leqslant i \leqslant m-1$. Therefore $u = \alpha_1 v_{1,1} + \beta_1 v_{1,2} \in \langle v_{1,1}, v_{1,2} \rangle$ so $\dim \mathrm{Soc}(y) = 2$. Thus y has two Jordan blocks so we see y has type $(m, m-1)$ and hence is conjugate to x.

Now, $[v_{m,1}, y; k] = a_k v_{m-k,1} + b_k v_{m-k,2} \in [V, y; k]$, but since $b_k \neq 0$, $[v_{m,1}, y; k] \notin [V, x; k]$. Therefore $[V, x; k] \neq [V, y; k]$ as required. □

Lemma 4.5.10 *Fix $k \in \{1, \ldots, m-1\}$ such that ε does not divide k. Then there exists $y \in C_G(x) \cap cl_G(x)$ such that $Soc^k(x) \neq Soc^k(y)$.*

Proof. By Lemma 4.1.2, there exists $M \in GL(2, q)$ with non-zero entries in the top right of both itself and its kth power. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be the transpose of M and write

$$A^i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix},$$

for $i \in \mathbb{Z}_{>0}$. We use A to define an element $y \in C_G(x)$. Let $[v_{m,1}, y] = av_{m-1,1} + bv_{m-2,2}$ and $[v_{m-1,2}, y] = cv_{m-1,1} + dv_{m-2,2}$. Now, $[v_{m,1}, y; i] = a_i v_{m-i,1} + b_i v_{m-1-i,2}$ and $[v_{m-1,2}, y; i] = c_i v_{m-i,1} + d_i v_{m-1-i,2}$, so $[v_{m,1}, y; m] = [v_{m-1,2}, y; m] = 0$. Therefore the largest Jordan block of y has size at most m.

Note $\langle v_{1,1}, cv_{2,1} - av_{1,2} \rangle \subseteq \mathrm{Soc}(y)$, so since $c \neq 0$, $\dim \mathrm{Soc}(y) \geqslant 2$. Now suppose $u \in \mathrm{Soc}(y)$, where $u = \sum_{i=1}^{m} \alpha_i v_{i,1} + \sum_{i=1}^{m-1} \beta_i v_{i,2}$. Then

$$\begin{aligned}
0 &= [u, y] \\
&= \sum_{i=1}^{m} \alpha_i [v_{i,1}, y] + \sum_{i=1}^{m-1} \beta_i [v_{i,2}, y] \\
&= \alpha_2 a v_{1,1} + \beta_1 c v_{1,1} + \sum_{i=3}^{m} \alpha_i (av_{i-1,1} + bv_{i-2,2}) + \sum_{i=2}^{m-1} \beta_i (cv_{i,1} + dv_{i-1,2}) \\
&= (\alpha_2 a + \beta_1 c) v_{1,1} + \sum_{i=3}^{m} \alpha_i (av_{i-1,1} + bv_{i-2,2}) + \sum_{i=3}^{m} \beta_{i-1} (cv_{i-1,1} + dv_{i-2,2}) \\
&= (\alpha_2 a + \beta_1 c) v_{1,1} + \sum_{i=3}^{m} ((\alpha_i a + \beta_{i-1} c) v_{i-1,1} + (\alpha_i b + \beta_{i-1} d) v_{i-2,2}),
\end{aligned}$$

so $\alpha_2 a + \beta_1 c = 0$ and for $3 \leqslant i \leqslant m$, $\alpha_i a + \beta_{i-1} c = \alpha_i b + \beta_{i-1} d = 0$. Now $c \neq 0$, so for $3 \leqslant i \leqslant m$,

$$0 = \alpha_i b + \beta_{i-1} d = \alpha_i bc + \beta_{i-1} cd = \alpha_i bc - \alpha_i ad = \alpha_i (bc - ad).$$

We have A invertible, so $\alpha_i = 0$ and hence $\beta_{i-1} = 0$. Then

$$u = \alpha_1 v_{1,1} + \alpha_2 v_{2,1} + \beta_1 v_{1,2} = \alpha_1 v_{1,1} + \alpha_2 c^{-1} (cv_{2,1} - av_{1,2}),$$

as $\alpha_2 a + \beta_1 c = 0$. So $u \in \langle v_{1,1}, cv_{2,1} - av_{1,2}\rangle$ and hence $\mathrm{Soc}(y) = \langle v_{1,1}, cv_{2,1} - av_{1,2}\rangle$. Therefore y has two Jordan blocks, so is of type $(m, m-1)$ and hence is conjugate to x. Further, $[v_{k,2}, y; k] = c_k v_{1,1}$ and $c_k \neq 0$, so $v_{k,2} \notin \mathrm{Soc}^k(y)$. But $v_{k,2} \in \mathrm{Soc}^k(x)$, and so $\mathrm{Soc}^k(x) \neq \mathrm{Soc}^k(y)$ as required. $\square$

Theorem 4.5.11 *Suppose $m \leqslant \varepsilon$ and set $H = \langle C_G(y) \mid y \in \Gamma_x\rangle$. Then H is an irreducible subgroup of G.*

Proof. For any $k \in \{1, \ldots, m-1\}$ we can find $y_k \in C_G(x) \cap cl_G(x)$ such that $[V, x; k] \neq [V, y_k; k]$ by Lemma 4.5.9 and $z_k \in C_G(x) \cap cl_G(x)$ such that $\mathrm{Soc}^k(x) \neq \mathrm{Soc}^k(z_k)$ by Lemma 4.5.10. Now $C_G(y_k), C_G(z_k) \subseteq H$, for each $k \in \{1, \ldots, m-1\}$, and so H does not stabilize $[V, x; k]$ or $\mathrm{Soc}^k(x)$ for any $1 \leqslant k \leqslant m-1$. These are all of the $C_G(x)$-invariant subspaces of V by Corollary 4.5.2, and hence H is irreducible. $\square$

We now have the main result of this section.

Theorem 4.5.12 *Let $x \in GL(n, q)$ be unipotent of type $(m, m-1)$ and let ε be the exponent of $PGL(2, q)$. The class graph of x is connected if and only if $m \leqslant \varepsilon$.*

Proof. By Theorem 4.5.8, if there exists $k \in \{1, \ldots, m-1\}$ such that ε divides k, we have $\mathrm{Soc}^k(x) = \mathrm{Soc}^k(y)$ for all $y \in C_G(x) \cap cl_G(x)$. Therefore for any $y \in \Gamma_x$, $\mathrm{Soc}^k(x) = \mathrm{Soc}^k(y)$, as x is arbitrary. Then, since there exists $z \in cl_G(x)$ with $\mathrm{Soc}^k(x) \neq \mathrm{Soc}^k(z)$, the class graph is disconnected.

Now suppose ε does not divide k for any $k \in \{1, \ldots, m-1\}$. Then $H = \langle C_G(y) \mid y \in \Gamma_x\rangle$ is irreducible by Theorem 4.5.11. So by Theorem 4.4.6, $SL(n, q) \subseteq H$. Let $g \in cl_G(x)$ be in Jordan normal form, so there exists $h \in GL(n, q)$ such that $x = h^{-1}gh$. For any $a \in GF(q)^*$, $r = \mathrm{diag}(a, \ldots, a, a^{-1}, \ldots, a^{-1}) \in C_G(g)$ by Lemma 4.1.21, and so $h^{-1}rh \in C_G(x)$. Note $\det h^{-1}rh = \det r = a$, so for any element $a \in GF(q)^*$, H contains an element with determinant a. Therefore $H = GL(n, q)$, thus $GL(n, q)$ stabilizes Γ_x and so the class graph is connected. $\square$

4.6 Classes of Type (m, m)

Throughout this section let $x \in GL(2m, q)$ be unipotent of type (m, m). We proceed just as in the last section.

Lemma 4.6.1 *There exists a regular unipotent element in $C_G(x)$.*

Proof. Let

$$y_m = \left(\begin{array}{c|cc} & \begin{matrix} 0 & \dots & 0 \end{matrix} & 0 \\ \cline{2-3} J(m) & I_{m-1} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \hline I_m & J(m) & \end{array}\right),$$

where $J(m)$ is a Jordan block of size m and I_m is the $m \times m$ identity. We have $y_m \in C_G(x)$ by Lemma 4.1.21 and now show y_m is unipotent by induction on m.

First note

$$y_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix},$$

and so the characteristic polynomial of y_2 is

$$f_{y_2}(t) = \det \begin{pmatrix} 1-t & 0 & 0 & 0 \\ 1 & 1-t & 1 & 0 \\ 1 & 0 & 1-t & 0 \\ 0 & 1 & 1 & 1-t \end{pmatrix} = (1-t)^4.$$

Now consider f_{y_m}, the characteristic polynomial of y_m. Taking determinants along row 1 and then row $m+1$ in $y_m - I_{2m}t$ we have

$$f_{y_m}(t) = (1-t)^2 \det(y_{m-1} - I_{2m-2}t) = (1-t)^{2m+2},$$

by induction. Therefore y_m is unipotent. Next we note the only 1-space of V fixed by y_m is $\langle(1,0,\ldots,0)\rangle$. Therefore y_m is regular unipotent as claimed. $\square$

Lemma 4.6.2 *The only $C_G(x)$-invariant spaces of V are $Soc^k(x) = [V,x;m-k]$ for $1 \leqslant k \leqslant m-1$.*

Proof. Let

$$K = \left\{ \left(\begin{array}{cccccc} a & & & b & & \\ 0 & \ddots & & 0 & \ddots & \\ 0 & 0 & a & 0 & 0 & b \\ c & & & d & & \\ 0 & \ddots & & 0 & \ddots & \\ 0 & 0 & c & 0 & 0 & d \end{array} \right) \middle| \; a,b,c,d \in GF(q), ad-bc \neq 0 \right\}.$$

By Lemma 4.1.21 $K \leqslant C_G(x)$ and it is easy to see K acts on $[V,x;i-1]/[V,x;i]$ as $GL(2,q)$, for $1 \leqslant i \leqslant m$. Therefore $[V,x;i-1]/[V,x;i]$ has no non-trivial $C_G(x)$-invariant subspaces for $1 \leqslant i \leqslant m$.

Suppose the lemma is false. Let U be a minimal dimensional $C_G(x)$-invariant subspace of V such that U is not a commutator of x. Consider $[U,x]$. This is a $C_G(x)$-invariant subspace of V, as U is, and we have $\dim[U,x] < \dim U$ as x is unipotent. So by minimality of U, $[U,x] = [V,x;j]$ for some j. Now $[U,x] = [V,x;j]$ implies $U \subseteq [V,x;j-1]$ and since U is not a commutator, this containment is proper. Therefore $[V,x;j] \subset U \subset$

$[V, x; j-1]$ and hence $U/[V, x; j]$ is a non-trivial $C_G(x)$-invariant subspace of the 2-space $[V, x; j-1]/[V, x; j]$, a contradiction. $\square$

If $m = 1$, x is the identity so the class graph is trivially connected. Suppose $m = 2$ so x is unipotent of type $(2, 2)$. Let

$$\mathcal{B}_x = \{v_{2,1}, v_{1,1}, v_{2,2}, v_{1,2} \mid [v_{2,1}, x] = v_{1,1}, [v_{2,2}, x] = v_{1,2}\}$$

be a cyclic basis for x, so with respect to $\mathcal{B}_x$, x is written in Jordan normal form. Let

$$y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

and note $y \in C_G(x) \cap cl_G(x)$. We have $\mathrm{Soc}(x) = \langle v_{1,1}, v_{1,2}\rangle$ and $\mathrm{Soc}(y) = \langle v_{1,1}, v_{2,1}\rangle$ so $\mathrm{Soc}(x) \neq \mathrm{Soc}(y)$. Therefore $H = \langle C_G(z) \mid z \in \mathit{\Gamma}_x\rangle \geqslant \langle C_G(x), C_G(y)\rangle$ acts irreducibly on V by Lemma 4.6.2 and hence by Theorem 4.4.6, $SL(4, q) \subseteq H \subseteq Stab_G(\mathit{\Gamma}_x)$.

Now let $r_a = \mathrm{diag}(a, 1, 1, 1)$ for $a \in GF(q)^*$, and note

$$r_a^{-1} x r_a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \in C_G(x) \cap cl_G(x),$$

and $\det r = a$. So for any $a \in GF(q)^*$, r_a stabilizes $\mathit{\Gamma}_x$ and so there are elements in $Stab_G(\mathit{\Gamma}_x)$ with determinant a. Therefore $GL(4, q)$ stabilizes $\mathit{\Gamma}_x$ and the class graph is connected.

From now on assume $m \geqslant 3$. Let $y \in C_G(x) \cap cl_G(x)$. We know $[V, x]$ is y-invariant by Lemma 4.1.10 and so we can consider the action of y on $V/[V, x]$. First suppose y acts as the identity on $V/[V, x]$. Then for any $v \in V$ we have $v + [V, x] = (v + [V, x])y = vy + [V, x]$ giving $[v, y] \in [V, x]$. Therefore $[V, y] \subseteq [V, x]$ and hence, as $\dim[V, y] = \dim[V, x]$, we have $[V, y] = [V, x]$. It follows from Lemma 4.1.11 that $[V, x; k] = [V, y; k]$ for any $k \in \mathbb{Z}_{>0}$.

Now suppose y does not act as the identity on $V/[V, x]$. Then, since $\dim V/[V, x] = 2$, we can choose linearly independent vectors $v_{m,1}, v_{m,2}$ in $V \setminus [V, x]$ such that y acts on $V/[V, x]$ as

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

with respect to the basis $\{v_{m,1} + [V, x], v_{m,2} + [V, x]\}$. By Lemma 4.1.17, $\{v_{m,1}, v_{m,2}\}$ generates a cyclic basis $\mathcal{B}_x$ of V with respect to x. As usual we think of this basis as an array

$$\begin{array}{cc} v_{m,1} & v_{m,2} \\ v_{m-1,1} & v_{m-1,2} \\ \vdots & \vdots \\ v_{1,1} & v_{1,2}, \end{array}$$

where commutating any basis element with x moves it down one row.

Note $\dim V/[V, y] = 2$ and, since x and y commute, $[V, y]$ is x-invariant. Therefore $[V, x; 2] \subseteq [V, y]$ as x is unipotent. From the dimensions of the spaces we see $\dim[V, y]/[V, x; 2] = 2$, and so

$$[v_{m,1}, y] + [V, x; 2],$$

$$[v_{m,2}, y] + [V, x; 2]$$

and

$$[v_{m-1,1}, y] + [V, x; 2]$$

are linearly dependent. Now

$$[v_{m,1}, y] + [V, x; 2] = v_{m,2} + av_{m-1,1} + bv_{m-1,2} + [V, x; 2],$$

$$[v_{m,2}, y] + [V, x; 2] = ev_{m-1,1} + dv_{m-1,2} + [V, x; 2]$$

and

$$[v_{m-1,1}, y] + [V, x; 2] = v_{m-1,2} + [V, x; 2],$$

for some $a, b, d, e \in \mathbb{Z}$. It follows that $e = 0$.

Let $V_m = V$, $V_0 = \langle v_{1,2} \rangle$ and for $1 \leqslant k \leqslant m-1$ let $V_k = \langle v_{i,1}, v_{i+1,2}, v_{1,2} \mid 1 \leqslant i \leqslant k \rangle$. Then $[v_{m,1}, y] \in av_{m-1,1} + v_{m,2} + V_{m-2}$ and $[v_{m,2}, y] \in cv_{m-2,1} + dv_{m-1,2} + V_{m-3}$, with $a, c, d \in GF(q)$, and we see $[V_k, y] \subseteq V_{k-1}$ for all $k \in \{1, \dots, m\}$.

For $1 < k < m$ we restrict the map defined by the commutator of y to

$$\phi_k : V_k/V_{k-1} \to V_{k-1}/V_{k-2},$$

where

$$(v_{k,1} + V_{k-1})\phi_k = av_{k-1,1} + v_{k,2} + V_{k-2}$$

and

$$(v_{k+1,2} + V_{k-1})\phi_k = cv_{k-1,1} + dv_{k,2} + V_{k-2}.$$

Then for each k the map ϕ_k is given by the matrix

$$A = \begin{pmatrix} a & 1 \\ c & d \end{pmatrix}.$$

Write

$$A^k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix},$$

for $k \in \mathbb{Z}$, where $a_k, b_k.c_k, d_k \in GF(q)$, and note $[v_{m,1}, y; k] \in a_k v_{m-k,1} + b_k v_{m-k+1,2} + V_{m-k-1}$ and $[v_{m,2}, y; k] \in c_k v_{m-k-1,1} + d_k v_{m-k+1,2} + V_{m-k-2}$.

Lemma 4.6.3 *The matrix A is invertible and $b_m = 0$.*

Proof. First note $\langle v_{2,2} - dv_{1,1}, v_{1,2} \rangle \subseteq \mathrm{Soc}(y)$. Suppose A is not invertible, so $ad - c = 0$. As $v_{2,1}, v_{3,2} \in V_2$, we have $[v_{2,1}, y] = av_{1,1} + v_{2,2} + ev_{1,2}$ and $[v_{3,2}, y] = cv_{1,1} + dv_{2,2} + fv_{1,2}$, for some $e, f \in GF(q)$. Let $u = v_{3,2} - dv_{2,1} + ev_{2,2} - fv_{1,1}$. Then

$$\begin{aligned} [u, y] &= [v_{3,2}, y] - d[v_{2,1}, y] + e[v_{2,2}, y] - f[v_{1,1}, y] \\ &= cv_{1,1} + dv_{2,2} + fv_{1,2} - d(av_{1,1} + v_{2,2} + ev_{1,2}) + dev_{1,2} - fv_{1,2} \\ &= (c - ad)v_{1,1} \\ &= 0. \end{aligned}$$

So $u \in \mathrm{Soc}(y)$, and hence $\dim \mathrm{Soc}(y) \geqslant 3$, a contradiction. Therefore A is invertible. Clearly $[v_{i,1}, y; m] = 0$ for $1 \leqslant i \leqslant m - 1$, and $[v_{i,2}, y; m] = 0$ for $1 \leqslant i \leqslant m$, however $[v_{m,1}, y; m] = b_m v_{1,2}$. Therefore $b_m = 0$. $\square$

Let ε be the exponent of $PGL(2, q)$ and Γ_x be the connected component of the commuting graph containing x.

Lemma 4.6.4 *Let $(m, \varepsilon) = k$. Then $[V, x; k] = [V, y; k]$ for all $y \in C_G(x) \cap cl_G(x)$.*

Proof. Let $y \in C_G(x) \cap cl_G(x)$. We have already shown if y acts as the identity on $V/[V,x]$ then $[V,x;i] = [V,y;i]$ for all $i \in \mathbb{Z} > 0$. Now suppose y acts as a regular unipotent element on $V/[V,x]$ and let A be the matrix described above. We have A invertible and $b_m = 0$, by Lemma 4.6.3. Let α be the projective order of A, $l = (m, \alpha)$ and apply Lemma 4.1.3 to see $b_l = 0$. Since l divides k, A^k is a power of a lower triangular matrix and so $b_k = 0$.

We have $[v_{i,1}, y; k] \in [V,x;k]$ for $1 \leqslant i \leqslant m-1$, and $[v_{i,2}, y; k] \in [V,x;k]$ for $1 \leqslant i \leqslant m$, and $[v_{m,1}, y; k] \in b_k v_{m-k+1,2} + [V,x;k] = [V,x;k]$ as $b_k = 0$. So $[V,y;k] \subseteq [V,x;k]$ and hence $[V,x;k] = [V,y;k]$. $\square$

Theorem 4.6.5 *Let $x \in GL(2m,q)$ have type (m,m) and suppose $(m,\varepsilon) < m$. Then the commuting graph of x is disconnected.*

Proof. Suppose $y \in \mathit{\Gamma}_x$. Then there is a sequence $y_1, \ldots, y_r$ of conjugates of x such that $y_1 \in C_G(x)$, $y_i \in C_G(y_{i-1})$ for $1 < i \leqslant r$ and $y \in C_G(y_r)$. We now apply Lemma 4.6.4 to each of the pairs (x, y_1), (y_1, y_2), $\ldots$, (y_r, y), to see

$$[V,x;k] = [V,y_1;k] = \ldots = [V,y_r;k] = [V,y;k].$$

Therefore $[V,x;k] = [V,y;k]$ for all $y \in \mathit{\Gamma}_x$. Since there are conjugates of x with different k-th commutators, the graph is disconnected. $\square$

We now consider what happens when $(m,\varepsilon) = m$. Suppose $A \in GL(2,q)$ with top right entry non-zero, and $A^m \in Z(GL(2,q)$. Write

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and for $1 < i \leqslant m$,

$$A^i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}.$$

Note $b \neq 0$, $b_m = c_m = 0$ and $a_m = d_m$. We use A to define $y \in C_G(x) \cap cl_G(x)$.

By Lemma 4.1.16, we only need to specify the action of y on $\{v_{m,1}, v_{m,2}\}$, a cyclic basis generating set for $\mathcal{B}_x$. So let $[v_{m,1}, y] = av_{m-1,1} + bv_{m,2}$ and $[v_{m,2}, y] = cv_{m-2,1} + dv_{m-1,2}$. We have $y \in C_G(x)$ by construction, but we need to check it is conjugate to x.

First note $[v_{m,1}, y; i] = a_i v_{m-i,1} + b_i v_{m-i+1,2}$ and $[v_{m,2}, y; i] = c_i v_{m-i-1,1} + d_i v_{m-i,2}$, for $1 \leqslant i \leqslant m$ so $[v_{m,1}, y; m] = b_m v_{1,2} = 0$ as $b_m = 0$, and $[v_{m,2}, y; m] = 0$. Therefore the largest Jordan block of y has size at most m. We have $\langle v_{1,2}, bv_{2,2} - dv_{1,1} \rangle \subseteq \mathrm{Soc}(y)$, so $\dim \mathrm{Soc}(y) \geqslant 2$. Now suppose $u \in \mathrm{Soc}(y)$, where $u = \sum_{i=1}^{m} (\alpha_i v_{i,1} + \beta_i v_{i,2})$. Then

$$\begin{aligned}
0 &= [u, y] \\
&= \sum_{i=1}^{m} (\alpha_i [v_{i,1}, y] + \beta_i [v_{i,2}, y]) \\
&= \alpha_1 b v_{1,2} + \beta_2 d v_{1,2} + \sum_{i=2}^{m} \alpha_i (a v_{i-1,1} + b v_{i,2}) + \sum_{i=2}^{m-1} \beta_{i+1} (c v_{i-1,1} + d v_{i,2}) \\
&= (\alpha_1 b + \beta_2 d) v_{1,2} + \alpha_m (a v_{m-1,1} + b v_{m,2}) + \sum_{i=2}^{m-1} ((\alpha_i a + \beta_{i+1} c) v_{i-1,1} + (\alpha_i b + \beta_{i+1} d) v_{i,2}),
\end{aligned}$$

so $\alpha_1 b + \beta_2 d = 0$, $\alpha_m a = \alpha_m b = 0$, and for $2 \leqslant i \leqslant m-1$, $\alpha_i a + \beta_{i+1} c = \alpha_i b + \beta_{i+1} d = 0$. Then as $b \neq 0$, $\alpha_m = 0$ and

$$0 = \alpha_i a + \beta_{i+1} c = \alpha_i ab + \beta_{i+1} bc = -\beta_{i+1} ad + \beta_{i+1} bc = \beta_{i+1}(-ad + bc).$$

So since A is invertible, $\beta_{i+1} = 0$ and hence $\alpha_i = 0$. Then

$$u = \alpha_1 v_{1,1} + \beta_1 v_{1,2} + \beta_2 v_{2,2} = \beta_1 v_{1,2} + \beta_2 b^{-1}(bv_{2,2} - dv_{1,1}) \in \langle v_{1,2}, bv_{2,2} - dv_{1,1} \rangle .$$

Therefore $\mathrm{Soc}(y) = \langle v_{1,2}, bv_{2,2} - dv_{1,1} \rangle$ and so $\dim \mathrm{Soc}(y) = 2$. Thus y has two Jordan blocks so is of type (m, m) and hence is conjugate to x.

Lemma 4.6.6 *Fix $1 \leqslant k \leqslant m - 1$. There exists an element $y \in C_G(x) \cap cl_G(x)$ such that $[V, y; k] \neq [V, x; k]$.*

Proof. Since m divides the exponent of $PGL(2, q)$, there exists $M \in GL(2, q)$ such that $M^m \in Z(GL(2, q))$ but $M^k \notin Z(GL(2, q))$. Then by Lemma 4.1.2, there is a conjugate A of M with non-zero entries in the top right corner of both itself and its k-th power. We use A to define y as above. We have shown $y \in C_G(x) \cap cl_G(x)$. Now $[v_{m,1}, y; k] = a_k v_{m-k,1} + b_k v_{m-k+1,2}$ with $b_k \neq 0$. Therefore $[v_{m,1}, y; k] \notin [V, x; k]$ and hence $[V, y; k] \not\subseteq [V, x; k]$. □

Theorem 4.6.7 *Let $x \in GL(n, q)$ be unipotent of type (m, m) and suppose $(m, \varepsilon) = m$. Let $H = \langle C_G(y) \mid y \in \mathit{\Gamma}_x \rangle$. Then H is an irreducible subgroup of $GL(n, q)$. Furthermore, $SL(n, q) \subseteq H$.*

Proof. For any $k \in \{1, \ldots, m - 1\}$, we can find $y_k \in C_G(x) \cap cl_G(x)$ such that $[V, x; k] \neq [V, y_k; k]$ by Lemma 4.6.6. Each $y_k \in H$ and so H cannot stabilize $[V, x; k]$ for any $k \in \{1, \ldots, m - 1\}$. Therefore, since these are all of the $C_G(x)$-invariant subspaces by Lemma 4.6.2, we have H irreducible. We now apply Theorem 4.4.6 to see $SL(n, q) \subseteq H$.□

Recall a class graph $\mathit{\Gamma}$ is S-connected if $SL(n, q) \subseteq Stab_G(\mathit{\Gamma}_x)$ for all $x \in V(\mathit{\Gamma})$.

Theorem 4.6.8 *Let $x \in GL(n, q)$ be unipotent of type (m, m). The class graph of x is S-connected if and only if $(m, \varepsilon) = m$. In particular, if $\mathit{\Gamma}$ is connected, then $m \leqslant \varepsilon$.*

Proof. This follows directly from Theorems 4.6.5 and 4.6.7 and the definition of S-connected.□

We now consider how many components there are in a graph which is S-connected and hence determine when the class graph is connected. Recall the number of components in Γ is given by $|G : Stab_G(\Gamma_x)|$ for any $x \in V(\Gamma)$. If Γ is S-connected, $SL(n,q) \subseteq Stab_G(\Gamma_x)$ and so to work out $|G : Stab_G(\Gamma_x)|$ we need to determine what values the determinants of elements in $Stab_G(\Gamma_x)$ take.

Let $g \in \mathrm{Stab}_G(\Gamma_x)$. Then $x^g \in \Gamma_x$ and so there exist $y_1, \ldots, y_r \in \Gamma_x$ with $y_1 = x$, $y_r = x^g$, such that $y_{i+1} \in C_G(y_i)$ for $1 \leqslant i < r$. For each pair (y_i, y_{i+1}), $1 \leqslant i < r$, we can work out a change of basis matrix B_i from $\mathcal{B}_{y_i}$ to $\mathcal{B}_{y_{i+1}}$, where $\mathcal{B}_z$ is a cyclic basis for z. Then $x^g = x^{B_1 \ldots B_{r_1}}$ and therefore, by Lemma 2.0.4, $g = kB_1 \ldots B_{r-1}$ for some $k \in C_G(x)$. Then $\det g = \det k \det B_1 \ldots \det B_{r-1}$.

Let $x \in GL(n,q)$ be unipotent of type (m,m) and let $v_{m,1}, v_{m,2}$ generate a cyclic basis $\mathcal{B}_x$ for x. First suppose $y \in C_G(x) \cap cl_G(x)$ acts as the identity on $V/[V,x]$. Then the action of y is completely given by

$$[v_{m,1}, y] = \sum_{i=1}^{m-1} (\lambda_i v_{m-i,1} + \mu_i v_{m-i,2}),$$

and

$$[v_{m,2}, y] = \sum_{i=1}^{m-1} (\tau_i v_{m-i,1} + \sigma_i v_{m-i,2}),$$

where

$$M = \begin{pmatrix} \lambda_1 & \mu_1 \\ \tau_1 & \sigma_1 \end{pmatrix},$$

is invertible.

The matrix of y with respect to the basis $\mathcal{B}_x$ is

$$\begin{pmatrix}
1 & 0 & \dots & \dots & 0 & 0 & \dots & \dots & \dots & 0 \\
\lambda_1 & 1 & \ddots & & \vdots & \mu_1 & \ddots & & & \vdots \\
\vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & & \vdots \\
\vdots & & \ddots & \ddots & 0 & \vdots & & \ddots & \ddots & \vdots \\
\lambda_{m-1} & \dots & \dots & \lambda_1 & 1 & \mu_{m-1} & \dots & \dots & \mu_1 & 0 \\
0 & \dots & \dots & \dots & 0 & 1 & 0 & \dots & \dots & 0 \\
\tau_1 & \ddots & & & \vdots & \sigma_1 & 1 & \ddots & & \vdots \\
\vdots & \ddots & \ddots & & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & \vdots & \vdots & & \ddots & \ddots & 0 \\
\tau_{m-1} & \dots & \dots & \tau_1 & 0 & \sigma_{m-1} & \dots & \dots & \sigma_1 & 1
\end{pmatrix}.$$

Now let $u_{m,1} = v_{m,1}, u_{m,2} = v_{m,2}$ and use these to generate a cyclic basis $\mathcal{B}_y$ for y. For convenience we let $\lambda_1 = a$, $\mu_1 = b$, $\tau_1 = c$ and $\sigma_1 = d$. So

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and write

$$M^i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix},$$

for $i \in \mathbb{Z}_{>0}$.

The change of basis matrix from $\mathcal{B}_x$ to $\mathcal{B}_y$ is given by

$$B = \begin{pmatrix} a_{m-1} & 0 & \dots & \dots & 0 & b_{m-1} & \dots & \dots & \dots & 0 \\ * & \ddots & \ddots & & \vdots & * & \ddots & & & \vdots \\ \vdots & \ddots & a_2 & \ddots & \vdots & \vdots & \ddots & b_2 & & \vdots \\ \vdots & & \ddots & a & 0 & \vdots & & \ddots & b & \vdots \\ * & \dots & \dots & * & 1 & * & \dots & \dots & * & 0 \\ c_{m-1} & \dots & \dots & \dots & 0 & d_{m-1} & 0 & \dots & \dots & 0 \\ * & \ddots & & & \vdots & * & \ddots & \ddots & & \vdots \\ \vdots & \ddots & c_2 & & \vdots & \vdots & \ddots & d_2 & \ddots & \vdots \\ \vdots & & \ddots & c & \vdots & \vdots & & \ddots & d & 0 \\ * & \dots & \dots & * & 0 & * & \dots & \dots & * & 1 \end{pmatrix}.$$

Using Lemma 4.1.6 we see

$$\begin{aligned} \det B &= (a_1 d_1 - b_1 c_1)(a_2 d_2 - b_2 c_2) \dots (a_{m-1} d_{m-1} - b_{m-1} c_{m-1}) \\ &= \det M \det M^2 \dots \det M^{m-1} \\ &= (\det M)^{\frac{m(m-1)}{2}}. \end{aligned}$$

We have shown the following.

Lemma 4.6.9 *Suppose* $y \in C_G(x) \cap cl_G(x)$ *acts as the identity on* $V/[V, x]$. *Then* $\det B_y = \alpha^{\frac{m(m-1)}{2}}$, *for some* $\alpha \in GF(q)^*$.

We also have the following converse.

Lemma 4.6.10 *Given* $\alpha \in GF(q)^*$, *there exists* $y \in C_G(x) \cap cl_G(x)$ *such that* $\det B_y = \alpha^{\frac{m(m-1)}{2}}$.

Proof. Let $M \in GL(2,q)$ be such that $\det M = \alpha$. We use M to determine an element $y \in C_G(x)$ as follows. Write

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and let $[v_{m,1}, y] = av_{m-1,1} + bv_{m-1,2}$, $[v_{m,2}, y] = cv_{m-1,1} + dv_{m-1,2}$. It is clear $[v_{m,1}, y; m] = [v_{m,2}, y; m] = 0$ and $\mathrm{Soc}(y) = \langle v_{1,1}, v_{1,2}\rangle$, and therefore y is conjugate to x. Now by Lemma 4.6.9, $\det B_y = (\det M)^{\frac{m(m-1)}{2}} = \alpha^{\frac{m(m-1)}{2}}$. □

Now suppose $y \in C_G(x) \cap cl_G(x)$ acts as a regular unipotent element on $V/[V,x]$. As earlier in this section we choose linearly independent vectors $v_{m,1}, v_{m,2} \in V \setminus [V,x]$ such that y acts on $V/[V,x]$ as

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

with respect to the basis $\{v_{m,1} + [V,x], v_{m,2} + [V,x]\}$. Let $\mathcal{B}_x$ be the cyclic basis for x generated by $v_{m,1}, v_{m,2}$. Then we know the action of y on V is completely determined by

$$[v_{m,1}, y] = av_{m-1,1} + v_{m,2} + \sum_{i=2}^{m-1} (\lambda_i v_{m-i,1} + \mu_i v_{m-i+1,2}) + \mu_m v_{1,2},$$

and

$$[v_{m,2}, y] = cv_{m-2,1} + dv_{m-1,2} + \sum_{i=3}^{m-1} (\tau_i v_{m-i,1} + \sigma_i v_{m-i+1,2}) + \sigma_m v_{1,2},$$

where

$$A = \begin{pmatrix} a & 1 \\ c & d \end{pmatrix},$$

is invertible with the top right entry in its m-th power zero, and $\lambda_i, \mu_i, \tau_i, \sigma_i \in GF(q)$ for $2 \leqslant i \leqslant m$.

The matrix of y with respect to the basis $\mathcal{B}_x$ is

$$
\begin{pmatrix}
1 & 0 & \dots & \dots & 0 & 1 & \dots & \dots & \dots & 0 \\
a & 1 & \ddots & & \vdots & \mu_2 & \ddots & & & \vdots \\
\lambda_2 & \ddots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & & \vdots \\
\vdots & \ddots & \ddots & \ddots & 0 & \vdots & & \ddots & \ddots & \vdots \\
\lambda_{m-1} & \dots & \lambda_2 & a & 1 & \mu_m & \dots & \dots & \mu_2 & 1 \\
0 & \dots & \dots & \dots & 0 & 1 & 0 & \dots & \dots & 0 \\
0 & \ddots & & & \vdots & d & 1 & \ddots & & \vdots \\
c & \ddots & \ddots & & \vdots & \sigma_3 & \ddots & \ddots & \ddots & \vdots \\
\vdots & & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \ddots & 0 \\
\tau_{m-1} & \dots & c & 0 & 0 & \sigma_m & \dots & \sigma_3 & d & 1
\end{pmatrix}.
$$

Now let $u_{m,1} = v_{m,1}, u_{m,2} = v_{m-1,2}$ and use these to generate a cyclic basis $\mathcal{B}_y$ for y. Again write

$$
A^i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix},
$$

for $i \in \mathbb{Z}_{>0}$.

The change of basis matrix from $\mathcal{B}_x$ to $\mathcal{B}_y$ is given by

$$
B = \begin{pmatrix}
a_{m-1} & 0 & \dots & \dots & 0 & * & b_{m-1} & \dots & \dots & 0 \\
* & \ddots & \ddots & & \vdots & \vdots & \ddots & \ddots & & \vdots \\
\vdots & \ddots & a_2 & \ddots & \vdots & \vdots & & \ddots & b_2 & \vdots \\
* & \dots & * & a & 0 & * & \dots & \dots & * & b \\
0 & \dots & \dots & 0 & 1 & 0 & \dots & \dots & 0 & 0 \\
0 & \dots & \dots & \dots & 0 & b_{m-1} & 0 & \dots & \dots & 0 \\
a_{m-2} & \ddots & & & \vdots & * & \ddots & \ddots & & \vdots \\
* & \ddots & \ddots & & \vdots & \vdots & \ddots & b_2 & \ddots & \vdots \\
* & * & a & \ddots & \vdots & * & \dots & * & 1 & 0 \\
0 & \dots & 0 & 1 & 0 & 0 & \dots & \dots & \dots & 0
\end{pmatrix}.
$$

So using Lemma 4.1.6 we see

$$
\det B = -b_{m-1} \det \begin{pmatrix}
a_{m-1} & & & b_{m-1} & & \\
* & \ddots & & * & \ddots & \\
* & * & a_2 & * & * & b_2 \\
a_{m-2} & & & b_{m-2} & & \\
* & \ddots & & * & \ddots & \\
* & * & a & * & * & 1
\end{pmatrix}
$$

$$
= -b_{m-1}(a_2 - ab_2)(a_3 b_2 - a_2 b_3) \dots (a_{m-1} b_{m-2} - a_{m-2} b_{m-1}).
$$

Now we note

$$
\begin{aligned}
A^i &= A^{i-1}A \\
&= \begin{pmatrix} a_{i-1} & b_{i-1} \\ c_{i-1} & d_{i-1} \end{pmatrix} \begin{pmatrix} a & 1 \\ c & d \end{pmatrix} \\
&= \begin{pmatrix} aa_{i-1} + cb_{i-1} & ba_{i-1} + db_{i-1} \\ ac_{i-1} + cd_{i-1} & bc_{i-1} + dd_{i-1} \end{pmatrix}.
\end{aligned}
$$

So $a_i = aa_{i-1} + cb_{i-1}$ and $b_i = ba_{i-1} + db_{i-1}$. Then for $i > 2$,

$$
\begin{aligned}
a_i b_{i-1} - a_{i-1} b_i &= (aa_{i-1} + cb_{i-1})(ba_{i-2} + db_{i-2}) - (aa_{i-2} + cb_{i-2})(ba_{i-1} + db_{i-1}) \\
&= (ad - c)(a_{i-1} b_{i-2} - a_{i-2} b_{i-1}).
\end{aligned}
$$

Also $a_2 - ab_2 = (a^2 + c) - a(a + d) = -(ad - c)$. So $a_i b_{i-1} - a_{i-1} b_i = -(ad - c)^{i-1}$ and

$$
\det B = (-1)^{m-1} b_{m-1} (ad - c)^{\frac{(m-1)(m-2)}{2}} = (-1)^{m-1} b_{m-1} (\det A)^{\frac{(m-1)(m-2)}{2}}.
$$

Now $AA^{m-1} = A^m = a_m I$ by Lemma 4.1.4. So

$$
A^{m-1} = a_m A^{-1} = \frac{a_m}{\det A} \begin{pmatrix} d & -1 \\ -c & a \end{pmatrix},
$$

and hence $b_{m-1} = -a_m / \det A$. Thus

$$
\det B = (-1)^m a_m (\det A)^{\frac{m(m-3)}{2}}.
$$

Also note $a_m^2 = \det(A^m) = (\det A)^m$.

Suppose m is odd. Then $m-3$ is even and so

$$\begin{aligned}
\det B &= (-1)^m a_m((\det A)^m)^{\frac{m-3}{2}} \\
&= (-1)^m a_m(a_m^2)^{\frac{m-3}{2}} \\
&= (-1)^m a_m^{m-2} \\
&= \frac{(-1)^m a_m^m}{a_m^2} \\
&= \left(\frac{-a_m}{\det A}\right)^m .
\end{aligned}$$

Now suppose m is even. Then $a_m = \pm(\det A)^{\frac{m}{2}}$. So

$$\begin{aligned}
\det B &= \pm(-1)^m(\det A)^{\frac{m(m-2)}{2}} \\
&= \pm((\det A)^{\frac{m-2}{2}})^m.
\end{aligned}$$

We have shown the following

Lemma 4.6.11 *Suppose $y \in C_G(x) \cap cl_G(x)$ acts as a regular unipotent element on $V/[V,x]$. If m is odd, $\det B_y = \alpha^m$ for some $\alpha \in GF(q)^*$, and if m is even, $\det B_y = \pm\alpha^{\frac{m(m-2)}{2}}$ for some $\alpha \in GF(q)^*$.*

We consider the cases for m even and m odd separately.

Lemma 4.6.12 *Suppose m is odd and divides ε. The number of components in the class graph is $(m, q-1)$.*

Proof. Suppose $g \in C_G(x)$. Then $\det g$ is an mth power by Lemma 4.1.24 and further it is clear for any $\alpha \in GF(q)^*$, there exists $g \in C_G(x)$ such that $\det g = \alpha^m$. Also by Lemmas 4.6.9 and 4.6.11 we see for any $y, z \in V(\Gamma_x)$ such that $[y,z]=1$, a change of basis matrix from $\mathcal{B}_y$ to $\mathcal{B}_z$ has determinant an mth power in $GF(q)^*$. Therefore the determinant map

$$\det : Stab_G(\Gamma_x) \to GF(q)^*, \ g \to \det g,$$

has image set $\{\alpha^m \mid \alpha \in GF(q)^*\}$, and hence $|G : Stab_G(\Gamma_x)| = (m, q-1)$. $\square$

Lemma 4.6.13 *Suppose m is even and divides ε. The number of components in the class graph is at most $(\frac{m}{2}, q-1)$.*

Proof. If $g \in C_G(x)$ then $\det g$ is an mth power by Lemma 4.1.24 and for any $\alpha \in GF(q)^*$, there exists $g \in C_G(x)$ such that $\det g = \alpha^m$. By Lemmas 4.6.9 and 4.6.10, if y acts as the identity on $V/[V,x]$ we have $\det B_y = \alpha^{\frac{m(m-1)}{2}}$ and if $\alpha \in GF(q)^*$ there exists $y \in C_G(x) \cap cl_G(x)$ such that $\det B_y = \alpha^{\frac{m(m-1)}{2}}$.

Therefore by Lemma 4.1.7 the determinant map

$$\det : Stab_G(\Gamma_x) \to GF(q)^*, \ g \to \det g,$$

is onto $\{\alpha^{\frac{m}{2}} \mid \alpha \in GF(q)^*\}$. Thus $|G : Stab_G(\Gamma_x)| \leqslant (\frac{m}{2}, q-1)$. $\square$

Example 4.6.14 *First note the exponent of $PGL(2,5)$ is 60 and the exponent of $PGL(2,7)$ is 168.*

(1) Let $x \in GL(6,5)$ be of type $(3,3)$. Then $(m,\varepsilon) = (3,120) = 3$ so the class graph is S-connected. Further $(m,q-1) = (3,4) = 1$ and so the class graph is connected.

(2) Let $x \in GL(6,7)$ be of type $(3,3)$. Then $(m,\varepsilon) = (3,168) = 3$ so the class graph is S-connected. However, $(m,q-1) = (3,6) = 3$ and so the graph has three components.

(3) Let $x \in GL(12,5)$ be of type $(6,6)$. Then $(m,\varepsilon) = (6,120) = 6$ so the class graph is S-connected. Now note $(m,q-1) = (6,4) = 2$, but $(m/2,q-1) = (3,4) = 1$, so in this case the graph is connected.

(4) Let $x \in GL(12,7)$ *be of type* $(6,6)$*. Then* $(m,\varepsilon) = (6,168) = 6$ *so the class graph is S-connected. Now,* $(m/2, q-1) = (3,6) = 3$*. So the graph has at most three components.*

Chapter 5

Conjugacy Classes and Character Degrees

The aim of the second half of this thesis is to prove the following theorem.

Theorem 5.0.1 *In a finite simple group the degree of any irreducible character divides the size of some conjugacy class of the group.*

This problem is considered in [26] where the authors say they have verified this for all groups in the Atlas, [12]. It would be nice if Theorem 5.0.1 could be extended to all finite groups, however the extraspecial groups provide a counterexample. If we have $E = p^{1+2n}$ then the set of character degrees of E is $\{1, p^n\}$ and the set of conjugacy class degrees is $\{1, p\}$.

A character of a finite group G is *imprimitive* if it is induced from a proper subgroup of G, otherwise it is *primitive*. In the extraspecial group $E = p^{1+2n}$, those characters of degree p^n are imprimitive. This leads to the following conjecture in [26].

Conjecture 5.0.2 *Let G be a finite group and let χ be a primitive irreducible character of G. Then there exists $g \in G$ such that $\chi(1)$ divides $|cl_G(g)|$.*

In [26] this is considered for solvable groups and the following is proved.

Lemma 5.0.3 *Let G be a finite solvable group and let χ be a primitive irreducible character of G. Then there exists $g \in G$ such that $(\chi(1))_p$ divides $|cl_G(g)|^3$ for any prime divisor p of $|G|$, where $(\chi(1))_p$ is the p-part of $\chi(1)$.*

This has been improved in [20] to the following.

Lemma 5.0.4 *Let G be a finite solvable group, let χ be a primitive irreducible character of G and p a prime divisor of $|G|$. Then the number of $g \in G$ such that $(\chi(1))_p$ divides $|cl_G(g)|^3$ is at least $\frac{2|G|}{1+\log_p |G|_p}$. Also if $\chi(1)_p > 1$ there exists a p'-element $g \in G$ such that $p^3\chi(1)_p$ divides $|cl_G(g)|^3$.*

Similar problems have been also been considered. In [15] Dolfi showed if G is a solvable group and distinct primes p and q divide the degree of an irreducible character then they also divide the size of a conjugacy class of G. In [11] it was shown that the same result holds without the condition that G is solvable.

In Chapter 6 we prove the result for both the symmetric groups and the alternating groups and also for their double covers. Chapter 7 considers some combinatorial results which will be used in Chapter 9. In Chapter 8 we introduce algebraic groups and go on to discuss the finite groups of Lie type. Towards the end we concentrate on the conjugacy classes of two particular types of element - regular unipotent and regular semisimple. Finally in Chapter 9 we briefly discuss characters in the finite groups of Lie type and go on to prove the result for groups of adjoint type. We then prove the theorem for the simple groups of Lie type. Note the result for the sporadic groups has been checked from the Atlas [12]. Our main theorem then follows from the classification of finite simple groups.

Chapter 6

The Symmetric Group

6.1 Conjugacy Classes

The symmetric group S_n is the set of permutations of the set $\Omega = \{1, 2, \ldots, n\}$. We start with some basic properties of elements in S_n.

Any element of S_n can be written as a product of disjoint cycles, uniquely up to the order of the cycles.

Definition 6.1.1 *Let $\pi = (x_1, x_2, \ldots, x_{r_1})(y_1, y_2, \ldots, y_{r_2}) \ldots (z_1, z_2, \ldots, z_{r_k})$, be an element of S_n written as a product of disjoint cycles. The* cycle shape *of π is $(r_1, r_2, \ldots, r_k)$.*

Lemma 6.1.2 *Suppose $\pi = (x_1, x_2, \ldots, x_r) \in S_n$ and τ is any element of S_n. Then $\tau^{-1}\pi\tau = (x_1\tau, x_2\tau, \ldots, x_r\tau)$.*

Proof. For $i < r$, $(x_i\tau)\tau^{-1}\pi\tau = x_i\pi\tau = x_{i+1}\tau$. For $i = r$, $(x_r\tau)\tau^{-1}\pi\tau = x_r\pi\tau = x_1\tau$. $\square$

Lemma 6.1.3 *Conjugate elements of S_n have the same cycle shape.*

Proof. Let $\pi = (x_1, x_2, \ldots, x_{r_1})(y_1, y_2, \ldots, y_{r_2}) \ldots (z_1, z_2, \ldots, z_{r_k}) \in S_n$ and let $\tau \in S_n$.

Then

$$\begin{aligned}\tau^{-1}\pi\tau &= \tau^{-1}(x_1, x_2, \ldots, x_{r_1})(y_1, y_2, \ldots, y_{r_2}) \ldots (z_1, z_2, \ldots, z_{r_k})\tau \\ &= \tau^{-1}(x_1, x_2, \ldots, x_{r_1})\tau\tau^{-1}(y_1, y_2, \ldots, y_{r_2})\tau \ldots \tau^{-1}(z_1, z_2, \ldots, z_{r_k})\tau \\ &= (x_1\tau, x_2\tau, \ldots, x_{r_1}\tau)(y_1\tau, y_2\tau, \ldots, y_{r_2}\tau) \ldots (z_1\tau, z_2\tau, \ldots, z_{r_k}\tau)\end{aligned}$$

by Lemma 6.1.2. □

Lemma 6.1.4 *Let $\pi, \sigma \in S_n$. Then π and σ are conjugate in S_n if and only if they have the same cycle shape.*

Proof. Suppose π and σ have the same cycle shape. Let
$\pi = (x_1, x_2, \ldots, x_{r_1})(y_1, y_2, \ldots, y_{r_2}) \ldots (z_1, z_2, \ldots, z_{r_k})$ and
$\sigma = (a_1, a_2, \ldots, a_{r_1})(b_1, b_2, \ldots, b_{r_2}) \ldots (c_1, c_2, \ldots, c_{r_k})$, and let

$$\tau = \begin{pmatrix} x_1 & x_2 & \ldots & x_{r_1} & y_1 & y_2 & \ldots & y_{r_2} & \ldots & z_1 & z_2 & \ldots & z_{r_k} \\ a_1 & a_2 & \ldots & a_{r_1} & b_1 & b_2 & \ldots & b_{r_2} & \ldots & c_1 & c_2 & \ldots & c_{r_k} \end{pmatrix}.$$

Then $\sigma = \tau^{-1}\pi\tau$. The converse is Lemma 6.1.3. □

Definition 6.1.5 *A* partition *of n is a set of positive integers $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ such that $\sum_{i=1}^{k} \lambda_i = n$. Write $\lambda \vdash n$ to show λ is a partition of n. We will assume $\lambda_i \geqslant \lambda_{i+1}$ for all $1 \leqslant i \leqslant k$, unless otherwise stated. We say $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \vdash n$ is a* strict partition *if $\lambda_i > \lambda_{i+1}$ for all $1 \leqslant i \leqslant k$.*

From Lemma 6.1.4 we see that each conjugacy class of S_n corresponds uniquely to a partition of n.

Lemma 6.1.6 *The size of the conjugacy class in S_n corresponding to the partition $\lambda \vdash n$*

is

$$|cl_{S_n}(\lambda)| = \frac{n!}{1^{m_1}m_1!2^{m_2}m_2!\dots n^{m_n}m_n!},$$

where m_i is the number of cycles in λ of length i.

Proof. See [36, p.3]. $\square$

6.2 Representations and Character Degrees

In this section we follow the development in [36].

Definition 6.2.1 *Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ be a partition of n. A* Young diagram *for λ consists of n nodes placed in k left-justified rows with $|\lambda_i|$ nodes in row i. Label the nodes (i, j) where i is the row number and j is the column number. We also use λ for the name of the diagram.*

Example 6.2.2 *For $\lambda = (6, 4, 3, 1)$ the Young diagram for λ is*

$$\begin{array}{llllll}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & & \\
\bullet & \bullet & \bullet & & & \\
\bullet & & & & &
\end{array}$$

Definition 6.2.3 *Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_k)$ be a partition of n. A* Young tableau *for λ is a Young diagram for λ with the nodes replaced by the integers $1, \dots, n$ in some order.*

Let t^λ denote a Young tableau for λ, and label the entries $t(i, j)$ for $1 \leqslant i \leqslant |\lambda_i|$, $1 \leqslant j \leqslant k$.

Definition 6.2.4 *Two Young tableaux for λ are* equivalent *if they contain the same numbers in each row. A* Young tabloid *for λ is an equivalence class for this equivalence relation. We write $\{t^\lambda\}$.*

For a Young tableau t, let

$$R_t = \{\pi \in S_n \mid \pi \text{ stabilizes each row in } t\}$$

and

$$C_t = \{\pi \in S_n \mid \pi \text{ stabilizes each column in } t\}.$$

Define $R_t^+ = \sum_{\pi\in R_t} \pi$ and $C_t^- = \sum_{\pi\in C_t}(sgn\pi)\pi$, and note R_t^+ and C_t^- are in the group ring of S_n.

Definition 6.2.5 *Let t be a Young tableau. The* polytabloid *of t is $e_t = C_t^- R_t^+ t = C_t^-\{t\}$.*

Definition 6.2.6 *The* Specht module *corresponding to the partition λ is the module generated by the polytabloids e_t, where t runs over the tableaux for λ.*

It can be shown that the Specht modules form a complete set of irreducible modules for S_n, see [36, Th. 2.4.6, p.66]. Therefore we have a 1-1 correspondence between the partitions of n and the irreducible modules, and hence characters, of S_n.

We now state a useful result which enables the character degree corresponding to the partition λ to be calculated from the Young diagram for λ.

Definition 6.2.7 *The* hook length *of a node in the Young diagram is the sum of the number of nodes directly to the right of the node and the number of nodes directly beneath the node, plus 1 for the node itself. Let $h(i,j)$ be the hook number of the node (i,j).*

Definition 6.2.8 *The* hook length diagram*, $H(\lambda)$, for a partition λ consists of the Young diagram for λ with each node replaced by the hook length at that node.*

Example 6.2.9 *The hook length diagram for $\lambda = (6,4,3,1)$ is*

$$\begin{array}{cccccc} 9 & 7 & 6 & 4 & 2 & 1 \\ 6 & 4 & 3 & 1 & & \\ 4 & 2 & 1 & & & \\ 1 & & & & & \end{array}$$

Theorem 6.2.10 *The degree of the character χ, corresponding to the partition λ is given by*

$$\chi(1) = \frac{n!}{\prod_{(i,j)\in\lambda} h(i,j)}.$$

Proof. See [36, Th. 3.10.2, p.124]. □

Example 6.2.11 *Let $\lambda = (6,4,3,1) \vdash 14$. The degree of the character corresponding to λ is*

$$\chi(1) = \frac{14!}{9\times 7\times 6\times 4\times 2\times 1\times 6\times 4\times 3\times 1\times 4\times 2\times 1\times 1} = 50050.$$

Our result for the symmetric group is as follows.

Theorem 6.2.12 *The degree of an irreducible character of S_n divides the size of some conjugacy class of S_n.*

Proof. Let λ be a partition of n corresponding to the irreducible character χ of S_n. The set of hook lengths on the diagonal of $H(\lambda)$ is $\{h(1,1), h(2,2), \ldots, h(r,r)\}$. Each node in $H(\lambda)$ is counted by exactly one hook in the above set and therefore $\sum_{i=1}^{r} h(i,i) = n$. Also $h(i,i) > h(i+1,i+1)$ for $1 \leqslant i \leqslant r$. So $\mu = (h(1,1), h(2,2), \ldots, h(r,r))$ is a strict partition of n with

$$|cl_{S_n}(\mu)| = \frac{n!}{\prod_{i=1}^{r} h(i,i)},$$

from Lemma 6.1.6. By Theorem 6.2.10,

$$\chi(1) = \frac{n!}{\prod_{(i,j)\in\lambda} h(i,j)} = \frac{n!}{\prod_{i=1}^{r} h(i,i) \prod_{(i,j)\in\lambda, i\neq j} h(i,j)},$$

which clearly divides $|cl_{S_n}(\mu)|$. So $\chi(1)$ divides the size of the conjugacy class corresponding to the partition μ. □

We finish this section by considering a related question. Given a non-trivial conjugacy class K in S_n can we find a non-linear irreducible character whose degree divides $|K|$? It turns out that we cannot, as the following example shows.

Example 6.2.13 *Let $G = S_{19}$. Let $K_1 = cl_G((12))$ and $K_2 = cl_G((123))$. Then $|K_1| = 171$ and $|K_2| = 1938$ and there do not exist any non-linear irreducible characters of G whose degrees divide the order of these classes.*

6.3 The Alternating Group

Any element in S_n can be written as a product of transpositions. This product is not unique, but either always contains an even number of transpositions, or always contains an odd number of transpositions. We say an element of S_n is even if it can be written as a product of an even number of transpositions. The alternating group A_n consists of all the even permutations in S_n. The conjugacy classes and irreducible character degrees in A_n can be calculated from those in S_n.

Lemma 6.3.1 *Let $\pi \in A_n$. The conjugacy class of π in S_n splits into two conjugacy classes of equal size in A_n if and only if π does not commute with an odd element of S_n. Otherwise it remains the same.*

Proof. First suppose π commutes with an odd element of S_n, say τ. Let σ be any conjugate of π in S_n. Then for some $\delta \in S_n$ we have $\sigma = \delta^{-1}\pi\delta = (\tau\delta)^{-1}\pi\tau\delta$. Now, since τ is an odd element, one of δ and $\tau\delta$ must be even and so $\sigma \in cl_{A_n}(\pi)$.

Now suppose π does not commute with any odd elements of S_n. Then $C_{A_n}(\pi) = C_{S_n}(\pi)$ and so $|cl_{A_n}(\pi)| = \frac{|A_n|}{|C_{A_n}(\pi)|} = \frac{|S_n|}{2|C_{S_n}(\pi)|} = \frac{1}{2}|cl_{S_n}(\pi)|$. Let $\gamma \in cl_{S_n}(\pi) \setminus cl_{A_n}(\pi)$. Then γ cannot commute with any odd element, so by the same argument, $|cl_{A_n}(\gamma)| = \frac{1}{2}|cl_{S_n}(\pi)|$. Then $cl_{S_n}(\pi) = cl_{A_n}(\pi) \cup cl_{A_n}(\gamma)$, where $|cl_{A_n}(\pi)| = |cl_{A_n}(\gamma)|$. $\square$

Lemma 6.3.2 *Let χ be an irreducible character of S_n. If χ is non-zero somewhere outside of A_n, χ restricted to A_n is irreducible. If χ is zero everywhere outside of A_n, it restricts to the sum of two distinct irreducible characters of the same degree in A_n. All the irreducible characters of A_n come from restrictions of irreducible characters of S_n in one of these ways.*

Proof. See [28, 20.13, p.219]. $\square$

Definition 6.3.3 *Let λ be a partition of n. The conjugate partition λ' is the partition obtained by reflecting along the diagonal in the Young diagram for λ. The Young diagram for λ is symmetric if $\lambda = \lambda'$.*

Example 6.3.4 *Let $\lambda = (6, 4, 3, 1)$. Then $\lambda' = (4, 3, 3, 2, 1, 1)$ and so λ is not symmetric. Let $\mu = (5, 4, 2, 2, 1)$. Then $\mu = \mu'$ and so μ is symmetric.*

Now we come to the result for the alternating groups.

Theorem 6.3.5 *The degree of an irreducible character of A_n divides the size of some conjugacy class of A_n.*

Proof. Let λ be a partition of n corresponding to the irreducible character χ of S_n. Again we consider the strict partition $\mu = (\mu_1, \mu_2, \ldots, \mu_r)$ given by the set of hook lengths on the diagonal of $H(\lambda)$. Let π be an element of S_n of shape μ and write $\pi = \pi_1\pi_2 \dots \pi_r$ as a product of disjoint cycles. There are several cases to deal with.

First suppose π is an even element of S_n which commutes with an odd element. By Lemma 6.3.1, the conjugacy class of π in S_n does not split in A_n. Therefore $\chi(1)$ divides $|cl_{A_n}(\pi)|$ by Theorem 6.2.12, and so the degree of the irreducible characters of A_n corresponding to χ divides $|cl_{A_n}(\pi)|$ by Lemma 6.3.2.

Now suppose π is an even element of S_n which does not commute with an odd element. By Lemma 6.3.1 this means the conjugacy class of π in S_n splits into two classes of equal size in A_n. Also, $h(i,i)$ must be odd for $1 \leqslant i \leqslant r$.

If the Young diagram of λ is symmetric, χ restricts to A_n as a sum of two irreducible characters, each of degree $\frac{1}{2}\chi(1)$ by [14]. These character degrees clearly divide $|cl_{A_n}(\pi)|$.

If the Young diagram is not symmetric we must have $h(x,y) = 2$ for some $(x,y) \in \lambda$, $x \neq y$. Then

$$|cl_{A_n}(\pi)| = \frac{n!}{2\prod_{i=1}^{r} h(i,i)},$$

and

$$\chi(1) = \frac{n!}{\prod_{(i,j)\in\lambda} h(i,j)} = \frac{n!}{2\prod_{i=1}^{r} h(i,i) \prod_{(i,j)\in\lambda, i\neq j, (i,j)\neq(x,y)} h(i,j)}.$$

So again we have $\chi(1)$ divides $|cl_{A_n}(\pi)|$ and hence by Lemma 6.3.2 so does the corresponding irreducible character degrees in A_n.

Next we consider what happens when π is an odd element of S_n. In this case, when π is written as a product of disjoint cycles, π must have a cycle of even length. Let π_m be the smallest such cycle. Suppose $m = r$, and let $\pi^* = \pi_1 \dots \pi_{r-1}\pi_m^2$. This corresponds to the partition $\mu^* = (\mu_1, \dots, \mu_{r-1}, \frac{1}{2}\mu_m, \frac{1}{2}\mu_m)$. We have $\mu^* \vdash n$ and $\pi^* \in A_n$. There are two cycles of the same length in π^* so its conjugacy class in S_n does not split in A_n. The size of the conjugacy class of π^* is

$$|cl_{A_n}(\pi^*)| = |cl_{S_n}(\pi^*)| = \frac{n!}{2\dfrac{h(m,m)}{2}\dfrac{h(m,m)}{2}\displaystyle\prod_{i=1}^{r-1} h(i,i)} = \frac{n!}{\dfrac{h(m,m)}{2}\displaystyle\prod_{i=1}^{r} h(i,i)}.$$

It is clear that $\frac{1}{2}h(m,m)$ occurs somewhere on the hook of (m,m), say at (a,b). Then

$$\chi(1) = \frac{n!}{\displaystyle\prod_{(i,j)\in\lambda} h(i,j)} = \frac{n!}{\dfrac{h(m,m)}{2}\displaystyle\prod_{i=1}^{r} h(i,i) \prod_{(i,j)\in\lambda, i\neq j, (i,j)\neq(a,b)} h(i,j)}.$$

Therefore $\chi(1)$ divides $|cl_{A_n}(\pi^*)|$, and by Lemma 6.3.2, so will its irreducible constituents in A_n.

Finally, suppose π is an odd element of S_n and π_m is the smallest cycle of even length, but $m \neq r$. The hook diagram of λ has the form

$$\begin{array}{ccccccccc}
\ddots & & & & & & & & \\
& l & k+d+1 & \beta_b+d+1 & \cdots & \beta_1+d+1 & d & \cdots & 1 \\
& k+c+1 & k & \beta_b & \cdots & \beta_1 & & & \\
& \alpha_a+c+1 & \alpha_a & \ddots & & & & & \\
& \vdots & \vdots & & & & & & \\
& \alpha_1+c+1 & \alpha_1 & & & & & & \\
& c & & & & & & & \\
& \vdots & & & & & & & \\
& 1 & & & & & & &
\end{array}$$

where k and all entries on the diagonal below k are odd, and $l = h(m,m)$ is even. From the diagram we see $l = k+c+d+2 = (k+c+1)+(k+d+1)-k$. So since l is even and k is odd, we have $k+c+1 \neq k+d+1$. Without loss of generality assume $k+d+1 > k+c+1$. Then $d > c$ and hence $d \geqslant c+1$. So we have a hook number of $c+1$ on the hook through (m,m). Note $(k+d+1)+(c+1) = l$ and so $k+d+1$ and

$c+1$ have the same parity. Let $\mu^* = (\mu_1, \ldots, \mu_{m-1}, k+d+1, c+1, \mu_{m+1}, \ldots, \mu_r)$.

If $k+d+1$ is even, then $k+d+1, c+1 \neq \mu_i$ for $1 \leqslant i \leqslant r$ and μ^* commutes with an odd element of S_n. Therefore the conjugacy class corresponding to μ^* in S_n does not split in A_n. We may rearrange μ^* into a strict partition so this is like the first case we considered.

If $k+d+1$ is odd, $\mu_{m-1} > k+d+1 > \mu_{m+1}$, but we may have $c+1 = \mu_i$ for some $m+1 \leqslant i \leqslant r$. If $c+1 \neq \mu_i$ for $m+1 \leqslant i \leqslant r$, μ^* can be rearranged to a strict partition, so the conjugacy class of μ^* in S_n splits in A_n. If $c+1 = \mu_i$ for some i, μ^* commutes with an odd permutation, so the conjugacy class does not split in A_n. Either way we have

$$|cl_{A_n}(\mu^*)| = \frac{n!}{2(k+d+1)(c+1)\displaystyle\prod_{1 \leqslant i \leqslant r, i \neq m} h(i,i)}.$$

The hook diagram has an even number on its diagonal so it cannot be symmetric. Therefore we must have a hook number equal 2 and so this is like the second case we considered. This completes the investigation of all cases. $\square$

6.4 $\tilde{S}_n$

In this section we assume $n \geqslant 4$ and consider the double covers of the symmetric group.

Definition 6.4.1 *We define $\tilde{S}_n$ to be the group generated by $z, t_1, \ldots, t_{n-1}$, with the following relations.*

(i) $z^2 = 1$.

(ii) $zt_i = t_i z$, *for* $1 \leqslant i \leqslant n-1$.

(iii) $t_i^2 = z$, *for* $1 \leqslant i \leqslant n-1$.

(iv) $(t_i t_{i+1})^3 = z$, *for* $1 \leqslant i \leqslant n-2$.

(v) $t_i t_j = z t_j t_i$, *for* $|i-j| > 1$, $1 \leqslant i, j \leqslant n-1$.

Lemma 6.4.2 *The group $\tilde{S}_n$ satisfies the following.*

(i) $|\tilde{S}_n| = 2|S_n| = 2n!$.

(ii) $Z = \{1, z\} \subseteq Z(\tilde{S}_n)$ *and* $\tilde{S}_n/Z \cong S_n$.

Proof. See [22, Th. 2.8, p19]. $\square$

Let $\theta : \tilde{S}_n \to S_n$, $t_i\theta = (i, i+1)$ for $1 \leqslant i < n$. Suppose C is a conjugacy class in S_n. Then $\theta^{-1}(C)$ is either a conjugacy class in $\tilde{S}_n$ or a union of two conjugacy classes in $\tilde{S}_n$, [22, Th. 3.6, p.28]. We can calculate the sizes of conjugacy classes in $\tilde{S}_n$ from those in S_n.

Lemma 6.4.3 *Let $\lambda \in S_n$ be written as a product of disjoint cycles and let $\tilde{\lambda}$ be a preimage of λ in $\tilde{S}_n$. Let m_i be the number of cycles in λ of length i, for $1 \leqslant i \leqslant n$. If λ is an even permutation,*

$$|cl_{\tilde{S}_n}(\tilde{\lambda})| = \begin{cases} |cl_{S_n}(\lambda)| & \text{if } m_{2i} = 0, \text{ for } 1 \leqslant i \leqslant \frac{1}{2}n, \\ 2|cl_{S_n}(\lambda)| & \text{otherwise.} \end{cases}$$

If λ is an odd permutation,

$$|cl_{\tilde{S}_n}(\tilde{\lambda})| = \begin{cases} |cl_{S_n}(\lambda)| & \text{if } m_i = 0 \text{ or } 1, \text{ for } 1 \leqslant i \leqslant n, \\ 2|cl_{S_n}(\lambda)| & \text{otherwise.} \end{cases}$$

Proof. See [22, Th. 3.8, p29]. $\square$

There are two types of irreducible representations in $\tilde{S}_n$, positive and negative. The positive representations are the same as those for S_n and so have been dealt with in the previous chapter. The negative representations come from projective representations of

S_n. It is the characters of these we are interested in here. For each strict partition λ of n we have an irreducible character θ_λ of $\tilde{S}_n$. If λ is an odd partition, there is another irreducible character θ_λ^a, but $\theta_\lambda^a(1) = \theta_\lambda(1)$, [22, p.77], so we don't need to consider these characters. These are all the irreducible characters of $\tilde{S}_n$ from the negative representations, [22, Th. 8.6, p.115].

Let $\lambda = \{\lambda_1, \ldots, \lambda_k\}$ be a strict partition of n. We form the shifted diagram $S(\lambda)$ of λ by placing λ_1 nodes in the first row and λ_i nodes in the ith row, starting from the ith column.

Example 6.4.4 *Let* $\lambda = (6, 4, 3, 1)$*. Then* $S(\lambda)$ *is*

$$\begin{array}{cccccc}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
 & \bullet & \bullet & \bullet & \bullet & \\
 & & \bullet & \bullet & \bullet & \\
 & & & \bullet & &
\end{array}$$

We then form the shift symmetric diagram, $Y(\lambda)$ of λ, by placing λ_1 nodes in the 0th column and λ_i nodes in the $(i-1)$th column beneath the i nodes already there. This is a Young diagram for S_{2n}.

Example 6.4.5 *Let* $\lambda = (6, 4, 3, 1)$*. Then* $Y(\lambda)$ *is*

$$\begin{array}{ccccccc}
\circ & \bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\circ & \circ & \bullet & \bullet & \bullet & \bullet & \\
\circ & \circ & \circ & \bullet & \bullet & \bullet & \\
\circ & \circ & \circ & \circ & \bullet & & \\
\circ & \circ & \circ & & & & \\
\circ & & & & & &
\end{array}$$

We can now form the hook diagram of $Y(\lambda)$ as in the case for S_n. Finally we delete the nodes in the hook diagram of $Y(\lambda)$ which are not in $S(\lambda)$. This leaves $H(\lambda)$.

Example 6.4.6 *Let $\lambda = (6,4,3,1)$. The hook diagram of $Y(\lambda)$ is*

$$\begin{array}{ccccccc}
12 & 10 & 9 & 7 & 6 & 4 & 1 \\
10 & 8 & 7 & 5 & 4 & 2 & \\
9 & 7 & 6 & 4 & 3 & 1 & \\
7 & 5 & 4 & 2 & 1 & & \\
4 & 2 & 1 & & & & \\
1 & & & & & &
\end{array}$$

and $H(\lambda)$ is

$$\begin{array}{cccccc}
10 & 9 & 7 & 6 & 4 & 1 \\
 & 7 & 5 & 4 & 2 & \\
 & & 4 & 3 & 1 & \\
 & & & 1 & &
\end{array}$$

Recall $\lambda = \{\lambda_1, \ldots, \lambda_k\}$. We can divide $S(\lambda)$ into nodes of three types. The nodes in column k are type 2. The nodes to the right of column k are type 1 and the nodes to the left of column k are type 3.

Example 6.4.7 *For $\lambda = (6,4,3,1)$ we have*

type 3			*type 2*	*type 1*	
•	•	•	•	•	•
	•	•	•	•	
		•	•	•	
			•		

Lemma 6.4.8 *Let $\lambda = (\lambda_1, \ldots, \lambda_k)$ be a strict partition of n. There are exactly $\frac{1}{2}(n-r)$ even numbers in $H(\lambda)$, where r is the number of even parts in λ.*

Proof. Consider the entries in $H(\lambda)$ in row i. The type 2 node of row i has hook length λ_i. The type 3 nodes have hook lengths $\lambda_i + \lambda_{i+1}, \ldots, \lambda_i + \lambda_k$. The type 1 nodes have hook lengths $\lambda_i - 1, \lambda_i - 2, \ldots, 2, 1$ with $\lambda_i - \lambda_{i+1}, \ldots, \lambda_i - \lambda_k$ removed, see [22, p190].

Clearly for $i < j \leqslant k$ either $\lambda_i + \lambda_j$ and $\lambda_i - \lambda_j$ are both even or they are both odd. Let x be the number of even hook lengths at type 3 nodes in row i.

If λ_i is an even number we have $\frac{1}{2}(\lambda_i - 2) - x$ even hook lengths of type 1. So the total number of even numbers in row i is

$$\frac{\lambda_i - 2}{2} - x + 1 + x = \frac{\lambda_i}{2}.$$

If λ_i is an odd number we have $\frac{1}{2}(\lambda_i - 1) - x$ even hook lengths of type 1. So the total number of even numbers in row i is

$$\frac{\lambda_i - 1}{2} - x + 0 + x = \frac{\lambda_i - 1}{2}.$$

Therefore the total number of even hook lengths in $H(\lambda)$ is

$$\sum_{\lambda_i odd} \frac{\lambda_i - 1}{2} + \sum_{\lambda_i even} \frac{\lambda_i}{2} = \frac{n-r}{2}. \qquad \square$$

Recall θ_λ is the character corresponding to the strict partition λ. We have the following Theorem from [22, Th. 10.7, p191].

Theorem 6.4.9 *Let λ be a strict partition of n with length k. Then*

$$\theta_\lambda(1) = \frac{2^{\frac{1}{2}(n-k-\varepsilon(\lambda))} n!}{h(\lambda)},$$

where

$$\varepsilon(\lambda) = \begin{cases} 0 & \text{if } \lambda \text{ is an even partition} \\ 1 & \text{if } \lambda \text{ is an odd partition} \end{cases}$$

and $h(\lambda)$ is the product of the hook numbers in $H(\lambda)$.

Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ be a strict partition of n. Reordering λ if necessary, write $\lambda = (\lambda_1, \ldots, \lambda_r, \lambda_{r+1}, \ldots, \lambda_{r+s})$, where $\lambda_1, \ldots, \lambda_r$ are cycles of odd length and $\lambda_{r+1}, \ldots, \lambda_{r+s}$ are cycles of even length, with $\lambda_1 > \lambda_2 > \ldots > \lambda_r$ and $\lambda_{r+1} > \lambda_{r+2} > \ldots > \lambda_{r+s}$.

We use λ to define another partition, μ, of n. For $r \geqslant s$, let

$$\mu = (\lambda_1 + \lambda_{r+1}, \ldots, \lambda_s + \lambda_{r+s}, \lambda_{s+1}, \ldots, \lambda_r),$$

for $r < s$ and $s - r$ even, let

$$\mu = (\lambda_1 + \lambda_{r+1}, \ldots, \lambda_r + \lambda_{2r}, \lambda_{2r+1} + \lambda_{2r+2}, \ldots, \lambda_{r+s-1} + \lambda_{r+s}),$$

and for $r < s$ with $s - r$ odd, let

$$\mu = (\lambda_1 + \lambda_{r+1}, \ldots, \lambda_r + \lambda_{2r}, \lambda_{2r+1} + \lambda_{2r+2}, \ldots, \lambda_{r+s-2} + \lambda_{r+s-1}, \lambda_{r+s}).$$

Then μ can be rearranged to a strict partition of n. Let $\mu = (\mu_1, \mu_2, \ldots, \mu_l)$.

Example 6.4.10 *If $\lambda = (6, 4, 3, 1)$, then $\mu = (9, 5)$. If $\lambda = (10, 9, 6, 5, 4, 2)$, then $\mu = (19, 11, 6)$.*

Theorem 6.4.11 *Let λ and μ be as above and let $\tilde{\mu}$ be a preimage of μ in $\tilde{S}_n$. Then $\theta_\lambda(1)$ divides $|cl_{\tilde{S}_n}(\tilde{\mu})|$.*

Proof. By Lemma 6.4.3, $|cl_{\tilde{S}_n}(\tilde{\mu})| = |cl_{S_n}(\mu)|$ or $2|cl_{S_n}(\mu)|$, so it is sufficient to show $\theta_\lambda(1)$ divides $|cl_{S_n}(\mu)|$. That is

$$\frac{2^{\frac{1}{2}(n-k-\varepsilon(\lambda))} n!}{h(\lambda)} \text{ divides } \frac{n!}{\mu_1 \ldots \mu_l}.$$

This is equivalent to

$$2^{\frac{1}{2}(n-k-\varepsilon(\lambda))} \text{ divides } \frac{h(\lambda)}{\mu_1 \dots \mu_l}.$$

We know $\mu_1, \dots, \mu_{l-1}$ appear as type 3 hook numbers in $H(\lambda)$. Also, μ_l is a hook number in $H(\lambda)$ of type 3 or type 2. So if we can show there are at least $\frac{1}{2}(n-k-\varepsilon(\lambda))$ even numbers left in $H(\lambda)$ after $\mu_1, \dots, \mu_l$ have been removed, we are done.

Let $K(\lambda)$ be the set of hook numbers in $H(\lambda)$ without $\mu_1, \mu_2, \dots, \mu_l$. There are several cases to consider.

First suppose $0 \leqslant s \leqslant r$. Then $k \geqslant r$ and

$$\mu = (\lambda_1 + \lambda_{r+1}, \dots, \lambda_s + \lambda_{r+s}, \lambda_{s+1}, \dots, \lambda_r) = (\mu_1, \dots, \mu_l).$$

For all $1 \leqslant i \leqslant l$, μ_i is an odd number, so the number of even numbers in $K(\lambda)$ is $\frac{1}{2}(n-r)$ by Lemma 6.4.8. Therefore we have

$$\frac{n-k-\varepsilon(\lambda)}{2} \leqslant \frac{n-r}{2}$$

as required.

Next suppose $0 \leqslant r < s$ and $s-r$ is even. Then $k \geqslant s$ and

$$\mu = (\lambda_1 + \lambda_{r+1}, \dots, \lambda_r + \lambda_{2r}, \lambda_{2r+1} + \lambda_{2r+2}, \dots, \lambda_{r+s-1} + \lambda_{r+s}) = (\mu_1, \dots, \mu_l).$$

We have $\frac{1}{2}(s-r)$ even numbers in μ and so we have

$$\frac{n-r}{2} - \frac{s-r}{2} = \frac{n-s}{2}$$

even numbers in $K(\lambda)$, by Lemma 6.4.8. Then

$$\frac{n-k-\varepsilon(\lambda)}{2} \leqslant \frac{n-s-\varepsilon(\lambda)}{2} \leqslant \frac{n-s}{2}.$$

Finally we suppose $0 \leqslant r < s$ and $s-r$ is odd. Then $k \geqslant s$ and

$$\mu = (\lambda_1 + \lambda_{r+1}, \ldots, \lambda_r + \lambda_{2r}, \lambda_{2r+1} + \lambda_{2r+2}, \ldots, \lambda_{r+s-2} + \lambda_{r+s-1}, \lambda_{r+s}) = (\mu_1, \ldots, \mu_l).$$

We have $\frac{1}{2}(s-r-1)+1$ even numbers in μ and so we have

$$\frac{n-r}{2} - \left(\frac{s-r-1}{2} + 1\right) = \frac{n-s-1}{2}$$

even numbers in $K(\lambda)$.

If s is even, then λ is an even permutation so $\varepsilon(\lambda) = 0$. Also, $r > 0$ since $s-r$ is odd, so $k > s$ and hence $k \geqslant s+1$. Then

$$\frac{n-k-\varepsilon(\lambda)}{2} = \frac{n-k}{2} \leqslant \frac{n-s-1}{2}.$$

If s is odd, then λ is an odd permutation so $\varepsilon(\lambda) = 1$. Then

$$\frac{n-k-\varepsilon(\lambda)}{2} = \frac{n-k-1}{2} \leqslant \frac{n-s-1}{2}. \qquad \square$$

6.5 $\tilde{A}_n$

Again throughout this section we assume $n \geqslant 4$.

Definition 6.5.1 *In Lemma 6.4.2 we stated that there is a projection of $\tilde{S}_n$ onto S_n. We define $\tilde{A}_n$ to be the inverse image of A_n under this projection.*

We can calculate the sizes of the conjugacy classes in $\tilde{A}_n$ from those in A_n, and the degrees of the irreducible negative representations from those in $\tilde{S}_n$.

Lemma 6.5.2 *Let $\lambda \in A_n$, written as a product of disjoint cycles, and let $\tilde{\lambda}$ be a preimage of λ in $\tilde{A}_n$. Let m_i be the number of cycles in λ of length i, for $1 \leqslant i \leqslant n$.*

$$|cl_{\tilde{A}_n}(\tilde{\lambda})| = \begin{cases} |cl_{A_n}(\lambda)| & \text{if } m_{2i} = 0, \text{ for } 1 \leqslant i \leqslant \frac{1}{2}n, \text{ or if } m_i = 0 \text{ or } 1, \text{ for } 1 \leqslant i \leqslant n, \\ 2|cl_{A_n}(\lambda)| & \text{otherwise.} \end{cases}$$

Proof. See [22, Th. 3.9, p30]. □

Lemma 6.5.3 *Let λ be a strict partition of n and let θ_λ be the corresponding character in $\tilde{S}_n$. If λ is an even partition, the restriction of θ_λ to $\tilde{A}_n$ is the sum of two distinct irreducible characters, each of degree $\frac{1}{2}\theta_\lambda(1)$. If λ is an odd partition, the restriction of θ_λ to $\tilde{A}_n$ is irreducible. This gives us all the characters of the irreducible negative representation of $\tilde{A}_n$.*

Proof. See [22, Th. 8.6, p114]. □

Theorem 6.5.4 *The degree of an irreducible character of $\tilde{A}_n$ divides the size of some conjugacy class of $\tilde{A}_n$.*

Proof. Let λ be a strict partition of n and let θ_λ be the corresponding character in $\tilde{S}_n$. Let $\tilde{\theta}_\lambda$ be an irreducible constituent of the restriction of θ_λ to $\tilde{A}_n$. Write $\lambda = (\lambda_1, \ldots, \lambda_r, \lambda_{r+1}, \ldots, \lambda_{r+s})$, where $\lambda_1, \ldots, \lambda_r$ are cycles of odd length and $\lambda_{r+1}, \ldots, \lambda_{r+s}$ are cycles of even length, with $\lambda_1 > \lambda_2 > \ldots > \lambda_r$ and $\lambda_{r+1} > \lambda_{r+2} > \ldots > \lambda_{r+s}$. Let μ be as in the case for $\tilde{S}_n$.

1. Suppose $0 \leqslant s \leqslant r$. Then μ is an even partition with only odd length cycles. Therefore we have $|cl_{\tilde{A}_n}(\tilde{\mu})| = |cl_{A_n}(\mu)| = \frac{1}{2}|cl_{S_n}(\mu)| = \frac{1}{2}|cl_{\tilde{S}_n}(\tilde{\mu})|$. If s is even, then

λ is an even partition and so $\tilde{\theta}_\lambda(1) = \frac{1}{2}\theta_\lambda(1)$. We know from Theorem 6.4.11, $\theta_\lambda(1)$ divides $|cl_{\tilde{S}_n}(\tilde{\mu})|$, so clearly $\tilde{\theta}_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu})|$. If s is odd, then λ is an odd partition and so $\tilde{\theta}_\lambda(1) = \theta_\lambda(1)$. So we need to show

$$\frac{2^{\frac{1}{2}(n-k-\varepsilon(\lambda))}n!}{h(\lambda)} \text{ divides } \frac{n!}{2\mu_1 \dots \mu_l}.$$

Therefore if we can show there are at least $\frac{1}{2}(n-k-\varepsilon(\lambda))+1$ even numbers in $K(\lambda)$, we are done. Now, s is odd so $s \geqslant 1$ and thus $k \geqslant r+1$. Also, λ is odd so $\varepsilon(\lambda) = 1$. Therefore we have

$$\frac{n-k-\varepsilon(\lambda)}{2} + 1 = \frac{n-k+1}{2} \leqslant \frac{n-r}{2}.$$

So by Lemma 6.4.8 this case is complete.

2. Suppose $0 \leqslant r < s$ and μ is an even partition. We can rearrange μ to be a strict partition and it has at least one even length cycle. Therefore $|cl_{\tilde{A}_n}(\tilde{\mu})| = |cl_{A_n}(\mu)| = |cl_{S_n}(\mu)|$. We know, from Theorem 6.4.11, $\theta_\lambda(1)$ divides $|cl_{S_n}(\mu)|$. So $\theta_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu})|$, and therefore $\tilde{\theta}_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu})|$ as required.

3. Suppose $0 \leqslant r < s$, $s-r$ is even, λ is even and μ is odd. Let $\mu^* = (\mu_1, \dots, \mu_{l-1}, \lambda_{r+s-1}, \lambda_{r+s})$. Then μ^* can be rearranged to a strict partition of n, $\tilde{\mu^*} \in \tilde{A}_n$, and $|cl_{\tilde{A}_n}(\tilde{\mu^*})| = |cl_{A_n}(\mu^*)| = |cl_{S_n}(\mu^*)| = \frac{n!}{\mu_1 \dots \mu_{l-1}\lambda_{r+s-1}\lambda_{r+s}}$. Let $K^*(\lambda)$ be the set of hook numbers in $H(\lambda)$ with $\mu_1, \dots, \mu_{l-1}, \lambda_{r+s-1}, \lambda_{r+s}$ removed. We have $\frac{1}{2}(n-r)$ even numbers in $H(\lambda)$, $\frac{1}{2}(s-r)+1$ even numbers in μ^*, and so $\frac{1}{2}(n-s-2)$ even numbers in $K^*(\lambda)$. Since λ is even,

$$\tilde{\theta}_\lambda(1) = \frac{1}{2}\theta_\lambda(1) = \frac{2^{\frac{1}{2}(n-k)}n!}{2h(\lambda)}.$$

We have

$$\frac{n-k}{2} - 1 = \frac{n-k-2}{2} \leqslant \frac{n-s-2}{2},$$

so $\tilde{\theta}_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu^*})|$.

4. Suppose $0 < r < s$, $s-r$ is even, λ is odd and μ is odd. Let $\mu^* = (\mu_1, \ldots, \mu_{l-1}, \lambda_{r+s-1}, \lambda_{r+s})$. Then, following the previous case we have $\frac{1}{2}(n-s-2)$ even numbers in $K^*(\lambda)$. As λ is odd,

$$\tilde{\theta}_\lambda(1) = \theta_\lambda(1) = \frac{2^{\frac{1}{2}(n-k-1)} n!}{h(\lambda)}.$$

We have $k > s$, so $k \geqslant s+1$. Therefore

$$\frac{n-k-1}{2} \leqslant \frac{n-s-2}{2},$$

so $\tilde{\theta}_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu^*})|$.

5. Suppose $0 < r < s$, $s-r$ is odd, λ is even and μ is odd.

Let $\mu^* = (\mu_1, \ldots, \mu_{l-2}, \lambda_{r+s-2}, \lambda_{r+s-1}, \lambda_{r+s})$. Then μ^* can be rearranged to a strict partition of n, $\tilde{\mu^*} \in \tilde{A}_n$, and $|cl_{\tilde{A}_n}(\tilde{\mu^*})| = |cl_{A_n}(\mu^*)| = |cl_{S_n}(\mu^*)| = \frac{n!}{\mu_1 \cdots \mu_{l-2} \lambda_{r+s-2} \lambda_{r+s-1} \lambda_{r+s}}$. Let $K^*(\lambda)$ be the set of hook numbers in $H(\lambda)$ with $\mu_1, \ldots, \mu_{l-2}, \lambda_{r+s-2}, \lambda_{r+s-1}, \lambda_{r+s}$ removed. We have $\frac{1}{2}(n-r)$ even numbers in $H(\lambda)$, $\frac{1}{2}(s-r+1)+1$ even numbers in μ^*, and so $\frac{1}{2}(n-s-3)$ even numbers in $K^*(\lambda)$. Since λ is even,

$$\tilde{\theta}_\lambda(1) = \frac{1}{2}\theta_\lambda(1) = \frac{2^{\frac{1}{2}(n-k)} n!}{2h(\lambda)}.$$

We have $k > s$, so $k \geqslant s+1$. Therefore

$$\frac{n-k}{2} - 1 = \frac{n-k-2}{2} \leqslant \frac{n-s-3}{2},$$

and so $\tilde{\theta}_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu^*})|$.

6. Suppose $0 < r < s$, $s-r$ is odd, λ is odd and μ is odd.

   Let $\mu^* = (\mu_1, \ldots, \mu_{l-2}, \lambda_{r+s-2}, \lambda_{r+s-1}, \lambda_{r+s})$. Then, as in the previous case we have $\frac{1}{2}(n-s-3)$ even numbers in $K^*(\lambda)$. Note λ is odd so

$$\tilde{\theta}_\lambda(1) = \theta_\lambda(1) = \frac{2^{\frac{1}{2}(n-k-1)} n!}{h(\lambda)}.$$

   We have s odd so must have r even and hence, since $r > 0$, $k \geqslant s+2$. Therefore

$$\frac{n-k-1}{2} \leqslant \frac{n-s-3}{2},$$

   and so $\tilde{\theta}_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu^*})|$.

7. Finally suppose $r = 0$, λ is an odd permutation and μ is an odd permutation. Then $\tilde{\theta}_\lambda(1) = \theta_\lambda(1)$. Let $\mu^* = (\mu_1, \ldots, \mu_{l-1}, \frac{1}{2}\mu_l, \frac{1}{2}\mu_l)$. Then $\tilde{\mu^*} \in \tilde{A}_n$ and $|cl_{\tilde{A}_n}(\tilde{\mu^*})| = 2|cl_{A_n}(\mu^*)| = 2|cl_{S_n}(\mu^*)| = \frac{2n!}{\mu_1 \ldots \mu_l (\frac{1}{2}\mu_l)}$. We show $\tilde{\theta}_\lambda(1)$ divides $|cl_{\tilde{A}_n}(\tilde{\mu^*})|$.

$$\tilde{\theta}_\lambda(1) = \frac{2^{\frac{1}{2}(n-k-1)} n!}{h(\lambda)},$$

   so we need $2^{\frac{1}{2}(n-k-1)-1} \mu_1 \ldots \mu_l (\frac{1}{2}\mu_l)$ divides $h(\lambda)$. Clearly $\frac{1}{2}\mu_l$ is the hook number of a node in row k of $H(\lambda)$, so $\mu_1 \ldots \mu_l(\frac{1}{2}\mu_l)$ divides $h(\lambda)$. Let $K^*(\lambda)$ be the set of hook numbers in $H(\lambda)$ with $\mu_1, \ldots, \mu_l, \frac{1}{2}\mu_l$ removed. There are $\frac{1}{2}n$ even numbers in $H(\lambda)$ so there are at least $\frac{1}{2}n - \frac{1}{2}(s+1) = \frac{1}{2}(n-s-2)$ even numbers in $K^*(\lambda)$.

Then,

$$\frac{n-k-1}{2} - 1 = \frac{n-s-3}{2} < \frac{n-s-1}{2},$$

as required. □

Chapter 7

Combinatorial Results

In this short technical chapter we consider some results which we will use in the following chapters.

Lemma 7.0.1 *Let $m \in \mathbb{Z}$, $m > 2$ and let $L_m = \binom{m-1}{2} + \binom{m-2}{2} + \ldots + \binom{2}{2}$. Then*

$$L_m = \sum_{i=1}^{m-1} (m-i)(i-1).$$

Proof. We proceed by induction on m. Suppose $m = 3$. Then $L_m = \binom{2}{2} = 1 = \sum_{i=1}^{2}(3-i)(i-1)$. Now, by induction, we have

$$\begin{aligned}
L_{m+1} &= L_m + \binom{m}{2} \\
&= \sum_{i=1}^{m-1}(m-i)(i-1) + \frac{m(m-1)}{2} \\
&= \sum_{i=1}^{m-1}(m-i)(i-1) + \sum_{i=1}^{m-1} i \\
&= \sum_{i=1}^{m-1}(m-i)(i-1) + \sum_{i=1}^{m}(i-1) \\
&= \sum_{i=1}^{m}(m+1-i)(i-1)
\end{aligned}$$

as required. $\square$

Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_m)$ be a sequence of length m. For such an α, define

$$N_\alpha = \sum_{i=1}^{m-1} (m-i)(\alpha_i + i - 1) - L_m,$$

where L_m is as in Lemma 7.0.1.

Lemma 7.0.2 *Let l be a positive integer and $\alpha = (\alpha_1, \dots, \alpha_m)$ be a partition of $l+1$ with $\alpha_1 \leqslant \alpha_2 \leqslant \dots \leqslant \alpha_m$ and $m < l+1$. Then there exists a partition $\beta = (\beta_1, \dots, \beta_{m+1})$ of $l+1$, with $\beta_1 \leqslant \dots \leqslant \beta_{m+1}$, such that $N_\alpha < N_\beta$.*

Proof. Let j be minimal such that $\alpha_j \neq 1$. Let $\beta = (1, \dots, 1, \alpha_j - 1, \alpha_{j+1}, \dots, \alpha_m)$, where $\beta_{j+1} = \alpha_j - 1$. Note $\beta_i = \alpha_{i-1}$ for $i \neq j+1$. Then by Lemma 7.0.1

$$\begin{aligned}
N_\beta - N_\alpha &= \sum_{i=1}^{m} (m+1-i)(\beta_i + i - 1) - \sum_{i=1}^{m} (m+1-i)(i-1) - \sum_{i=1}^{m-1} (m-i)(\alpha_i + i - 1) \\
&\quad + \sum_{i=1}^{m-1} (m-i)(i-1) \\
&= \sum_{i=1}^{m} (m+1-i)\beta_i - \sum_{i=1}^{m-1} (m-i)\alpha_i \\
&= \sum_{i=1}^{m} (m+1-i)\beta_i - \sum_{i=2}^{m} (m+1-i)\alpha_{i-1} \\
&= m\beta_1 + \sum_{i=2}^{m} (m+1-i)(\beta_i - \alpha_{i-1}) \\
&= m + (m+1-(j+1))(\beta_{j+1} - \alpha_j) \\
&= j \\
&> 0.
\end{aligned}$$

$\square$

Definition 7.0.3 *Let $l \in \mathbb{Z}$, $l \geqslant 2$. An l-sequence of length m is a sequence $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_m)$ satisfying* *(i)* $\alpha_i \in \mathbb{Z}_{\geqslant 0}$ *for all* $1 \leqslant i \leqslant m$*;*

(ii) $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_m$*;*

(iii) $\alpha_2 \neq 0$*;*

(iv) $\alpha_i \neq \alpha_{i+2}$*;*

(v) $\sum_{i=1}^{m} \alpha_i = l + \left[\left(\frac{m-1}{2}\right)^2\right]$, *where* $[z]$ *is the largest integer less than or equal to* z*.*

Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ be a sequence of length m. For such an α, define $A_\alpha = \sum_{i=1}^{m-1}(m-i)\alpha_i - M_m$, where $M_m = \binom{m-2}{2} + \binom{m-4}{2} + \ldots + \binom{x}{2}$, with $x = 2$ if m is even and $x = 3$ if m is odd.

Lemma 7.0.4 *Let* $m \geqslant 5$ *be odd and suppose* $\alpha = (0, 1, 1, \ldots, \frac{m-3}{2}, \frac{m-3}{2}, \frac{m-1}{2}, l)$*, with* $l \geqslant \frac{m-1}{2}$*. Then* α *is an* l*-sequence and* $A_\alpha = \left(\frac{m-1}{2}\right)^2$*.*

Proof. It is clear α satisfies Definition 7.0.3(i)-(iv). We have

$$\begin{aligned} \sum_{i=1}^{m} \alpha_i &= 2\sum_{i=1}^{\frac{m-3}{2}} i + \frac{m-1}{2} + l \\ &= \left(\frac{m-3}{2}\right)\left(\frac{m-1}{2}\right) + \frac{m-1}{2} + l \\ &= \left(\frac{m-1}{2}\right)^2 + l. \end{aligned}$$

Therefore α satisfies Definition 7.0.3(v) and so is an l-sequence.

We prove the second claim by induction on $k = \frac{m-1}{2}$. For $k = 2$, $\alpha = (0, 1, 1, 2, l)$ and $A_\alpha = \sum_{i=1}^{4}(5-i)\alpha_i - \binom{3}{2} = 4$ as required. Now let $\beta = (0, 1, 1, \ldots, \frac{m-5}{2}, \frac{m-5}{2}, \frac{m-3}{2}, l)$.

Inductively we have $A_\beta = (\frac{m-3}{2})^2$. Then

$$\begin{aligned} A_\alpha &= A_\beta + \sum_{i=1}^{m-3} 2\alpha_i + 2\alpha_{m-2} + \alpha_{m-1} - \binom{m-2}{2} \\ &= \left(\frac{m-3}{2}\right)^2 + 4\sum_{i=1}^{\frac{m-3}{2}} i + \frac{m-1}{2} - \frac{(m-2)(m-3)}{2} \\ &= \left(\frac{m-1}{2}\right)^2. \end{aligned}$$

□

Lemma 7.0.5 *Let $m \geqslant 4$ be even and suppose $\alpha = (0, 1, 1, \ldots, \frac{m-2}{2}, \frac{m-2}{2}, l)$, with $l > \frac{m-2}{2}$. Then α is an l-sequence and $A_\alpha = \left(\frac{m-2}{2}\right)\left(\frac{m}{2}\right)$.*

Proof. Clearly α satisfies Definition 7.0.3(i)-(iv). We have

$$\begin{aligned} \sum_{i=1}^{m} \alpha_i &= 2\sum_{i=1}^{\frac{m-2}{2}} i + l \\ &= \left(\frac{m-2}{2}\right)\left(\frac{m}{2}\right) + l \\ &= \left[\left(\frac{m-1}{2}\right)^2\right] + l. \end{aligned}$$

Therefore α satisfies 7.0.3(v), so is an l-sequence.

The second claim is proved by induction on $k = \frac{m-2}{2}$. For $k = 1$, $\alpha = (0, 1, 1, l)$ and $A_\alpha = \sum_{i=1}^{3}(4-i)\alpha_i - \binom{2}{2} = 2$. Now let $\beta = (0, 1, 1, \ldots, \frac{m-4}{2}, \frac{m-4}{2}, l)$. Inductively we have

$A_\beta = \binom{\frac{m-4}{2}}{}\binom{\frac{m-2}{2}}{}$. Then

$$
\begin{aligned}
A_\alpha &= A_\beta + \sum_{i=1}^{m-3} 2\alpha_i + 2\alpha_{m-2} + \alpha_{m-1} - \binom{m-2}{2} \\
&= \left(\frac{m-4}{2}\right)\left(\frac{m-2}{2}\right) + 4\sum_{i=1}^{\frac{m-4}{2}} i + 3\frac{(m-2)}{2} - \frac{(m-2)(m-3)}{2} \\
&= \left(\frac{m-4}{2}\right)\left(\frac{m-2}{2}\right) + 2\left(\frac{m-4}{2}\right)\left(\frac{m-2}{2}\right) + 3\frac{(m-2)}{2} - \frac{(m-2)(m-3)}{2} \\
&= \left(\frac{m-2}{2}\right)\left(\frac{m}{2}\right).
\end{aligned}
$$

This proves the claim. $\square$

Lemma 7.0.6 *Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ be an l-sequence and let*

$$\beta = (\alpha_1, \ldots, \alpha_{j-1}, \alpha_j + 1, \alpha_{j+1}, \ldots, \alpha_{k-1}, \alpha_k - 1, \alpha_{k+1}, \ldots, \alpha_m) = (\beta_1, \beta_2, \ldots, \beta_m).$$

Then $A_\beta = A_\alpha + k - j$.

Proof. We compute

$$
\begin{aligned}
A_\beta &= \sum_{i=1}^{m-1}(m-i)\beta_i - M_m \\
&= \sum_{i=1}^{j-1}(m-i)\alpha_i + (m-j)(\alpha_j+1) + \sum_{i=j+1}^{k-1}(m-i)\alpha_i \\
&\quad + (m-k)(\alpha_k - 1) + \sum_{i=k+1}^{m-1}(m-i)\alpha_i - M_m \\
&= \sum_{i=1}^{m-1}(m-i)\alpha_i - M_m + k - j \\
&= A_\alpha + k - j
\end{aligned}
$$

as claimed. $\square$

Let m be odd and $l \geqslant \frac{m-1}{2}$. Set

$$\sigma = \left(0, 1, 1, \ldots, \frac{m-3}{2}, \frac{m-3}{2}, \frac{m-1}{2}, l\right) = (\sigma_1, \ldots, \sigma_m).$$

Note σ is an l-sequence by Lemma 7.0.4. Let $\beta = (\beta_1, \ldots, \beta_m)$ be an l-sequence of length m. By Definition 7.0.3(v), $\sum_{i=1}^m \beta_i = \sum_{i=1}^m \sigma_i$, and by Definition 7.0.3(ii),(iii),(iv), we see $\beta_m \leqslant \sigma_m$ and $\beta_i \geqslant \sigma_i$ for $1 \leqslant i < m$. Therefore any l-sequence β of length m can be obtained from σ by subtracting a positive integer from σ_m and distributing it among the other σ_i's to obtain the given β_i's.

Lemma 7.0.7 *With σ and β as above, we have $A_\sigma \leqslant A_\beta$.*

Proof. This follows by Lemma 7.0.6. □

Lemma 7.0.8 *Let β be an l-sequence of length m, with m odd. Then either $m < 2l+1$ and $A_\beta \leqslant (l-1)^2$, or $m = 2l+1$ and $A_\beta = l^2$.*

Proof. Let $\beta = (\beta_1, \ldots, \beta_m)$. First suppose $m < 2l+1$. In order for β to be an l-sequence, we must have $\beta_m \geqslant \frac{m+1}{2}$. Each time we subtract 1 from σ_m and add it to another σ_i, we increase A_σ by at most $(m-1)$ by Lemma 7.0.6. Therefore, by Lemma 7.0.4,

$$\begin{aligned} A_\beta &\leqslant \left(\frac{m-1}{2}\right)^2 + (m-1)\left(l - \frac{m+1}{2}\right) \\ &= 1 + 3 + \ldots + (m-2) + (m-1)\left(l - \frac{m+1}{2}\right) \\ &\leqslant 1 + 3 + \ldots + (m-2) + m + \ldots + (2(l-1)-1) \\ &= (l-1)^2. \end{aligned}$$

Now suppose $m = 2l + 1$. By Definition 7.0.3, we must have

$$\sum_{i=1}^{2l+1} \beta_i = l + \left(\frac{(2l+1)-1}{2}\right)^2 = l(l+1).$$

Therefore the only l-sequence of length $2l+1$ is $\beta = (0, 1, 1, \ldots, l, l)$. Then, by Lemma 7.0.4,

$$A_\beta = \left(\frac{(2l+1)-1}{2}\right)^2 = l^2.$$

Finally suppose we have $m > 2l + 1$. Then

$$\begin{aligned}
\sum_{i=1}^{m} \beta_i &\geqslant 2\sum_{i=1}^{\frac{m-1}{2}} i \\
&= \left(\frac{m-1}{2}\right)\left(\frac{m+1}{2}\right) \\
&= \left(\frac{m-1}{2}\right)^2 + \frac{m-1}{2} \\
&> \left(\frac{m-1}{2}\right)^2 + \frac{(2l+1)-1}{2} \\
&= \left(\frac{m-1}{2}\right)^2 + l,
\end{aligned}$$

so β does not satisfy Definition 7.0.3. □

Now let m be even and $l \geqslant \frac{m}{2}$. Set

$$\sigma = \left(0, 1, 1, \ldots, \frac{m-2}{2}, \frac{m-2}{2}, l\right) = (\sigma_1, \ldots, \sigma_m).$$

By Lemma 7.0.5, σ is an l-sequence. We can obtain any l-sequence β of length m as in th case when m is odd.

Lemma 7.0.9 *For any l-sequence of length m, we have $A_\sigma \leqslant A_\beta$.*

Proof. This follows by Lemma 7.0.6. □

Lemma 7.0.10 *Let β be an l-sequence of length m, with m even. Then either $m < 2l$ and $A_\beta \leqslant l(l-2)$ or $m = 2l$ and $A_\beta = l(l-1)$.*

Proof. Let $\beta = (\beta_1, \ldots, \beta_m)$ be an l-sequence. First suppose $m < 2l$. In order to satisfy the conditions in Definition 7.0.3, we must have $\beta_m \geqslant \frac{m}{2}$. Each time we subtract 1 from σ_m and add it to another σ_i, we increase A_σ by at most $(m-1)$ by Lemma 7.0.6. If $\beta \neq \sigma$, $\beta_{m-1} \geqslant \sigma_{m-1} + 1$. Therefore, by Lemma 7.0.5,

$$\begin{aligned}
A_\beta &\leqslant A_\sigma + 1 + (m-1)\left(l - \frac{m}{2} - 1\right) \\
&= 2 + 4 + \ldots + (m-2) + 1 + (m-1)\left(l - \frac{m}{2} - 1\right) \\
&\leqslant 2 + 4 + \ldots + (m-2) + m + \ldots + (2(l-1) - 2) + 1 \\
&= (l-2)(l-1) + 1 \\
&\leqslant l(l-2).
\end{aligned}$$

Now suppose $m = 2l$. Then by Definition 7.0.3,

$$\sum_{i=1}^{2l} \beta_i = l + \left\lceil \left(\frac{2l-1}{2}\right)^2 \right\rceil = l + \left\lceil l^2 - l + \frac{1}{4} \right\rceil = l^2.$$

So we must have $\beta = (0, 1, 1, \ldots, l-1, l-1, l)$. Then by Lemma 7.0.5 we have

$$A_\beta = \binom{2l-2}{2}\binom{2l}{2} = l(l-1).$$

Finally suppose $m > 2l$. Then

$$\begin{aligned}
\sum_{i=1}^{m} \beta_i &\geqslant 2\sum_{i=1}^{\frac{m-2}{2}} i + \frac{m}{2} \\
&= \left(\frac{m-2}{2}\right)\left(\frac{m}{2}\right) + \left(\frac{m}{2}\right) \\
&> \left[\left(\frac{m-1}{2}\right)^2\right] + l,
\end{aligned}$$

so β does not satisfy Definition 7.0.3. $\square$

Chapter 8

Algebraic Groups and Finite Groups of Lie Type

8.1 Root Systems

Let V be a finite-dimensional vector space over $\mathbb{R}$, with an inner product $(\cdot,\cdot)$. Let $\langle\alpha,\beta\rangle = \frac{2(\beta,\alpha)}{(\alpha,\alpha)}$, and define

$$r_\alpha(\beta) = \beta - \langle\alpha,\beta\rangle\,\alpha.$$

Then r_α is a *reflection* in the hyperplane perpendicular to α.

Definition 8.1.1 *A* root system *is a finite subset* Σ *of* V *such that, for all* $\alpha,\beta\in\Sigma$, $r_\alpha(\Sigma)\subseteq\Sigma$, $\langle\alpha,\beta\rangle\in\mathbb{Z}$, *and* $c\alpha\in\Sigma$ *implies* $c=\pm1$. *The elements of* Σ *are called* roots.

Lemma 8.1.2 *Let* Σ *be a root system. If* $\alpha,\beta\in\Sigma$, *with* $\alpha\neq\pm\beta$, *then*

$$\langle\alpha,\beta\rangle\,\langle\beta,\alpha\rangle\in\{0,1,2,3\}.$$

Proof. We have $\langle\alpha,\beta\rangle\,\langle\beta,\alpha\rangle = \frac{4(\alpha,\beta)(\beta,\alpha)}{(\alpha,\alpha)(\beta,\beta)} = 4\cos^2\theta$, where θ is the angle between α and β. So since $\langle\alpha,\beta\rangle\in\mathbb{Z}$, we must have $\langle\alpha,\beta\rangle\,\langle\beta,\alpha\rangle\in\{0,1,2,3,4\}$. Suppose $\langle\alpha,\beta\rangle\,\langle\beta,\alpha\rangle = 4$.

Then $\cos\theta = \pm 1$, which implies $\theta = 0$ or π, so $\alpha = \pm\beta$, a contradiction. Therefore we have $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle \in \{0, 1, 2, 3\}$. $\square$

Corollary 8.1.3 *Suppose* $(\alpha, \beta) < 0$. *Then either* $\langle \alpha, \beta \rangle = -1$ *or* $\langle \beta, \alpha \rangle = -1$.

Proof. Clearly $(\alpha, \beta) < 0$ implies both $\langle \alpha, \beta \rangle < 0$ and $\langle \beta, \alpha \rangle < 0$. So the result follows from Lemma 8.1.2. $\square$

Definition 8.1.4 *A* fundamental system *of a root system* Σ *is a linearly independent subset* Π, *such that every element of* Σ *is either a non-negative or non-positive linear combination of elements of* Π.

For a fixed $\Pi \subseteq \Sigma$, let Σ^+ be the subset of Σ consisting of those elements which can be written as a non-negative linear combination of Π, and let Σ^- be the subset of Σ consisting of those elements which can be written as a non-positive linear combination of Π. Note $\Sigma = \Sigma^+ \cup \Sigma^-$.

Lemma 8.1.5 *Suppose* $\alpha, \beta \in \Pi$ *with* $\alpha \neq \beta$. *Then* $(\alpha, \beta) \leqslant 0$ *and hence* $\langle \alpha, \beta \rangle \leqslant 0$.

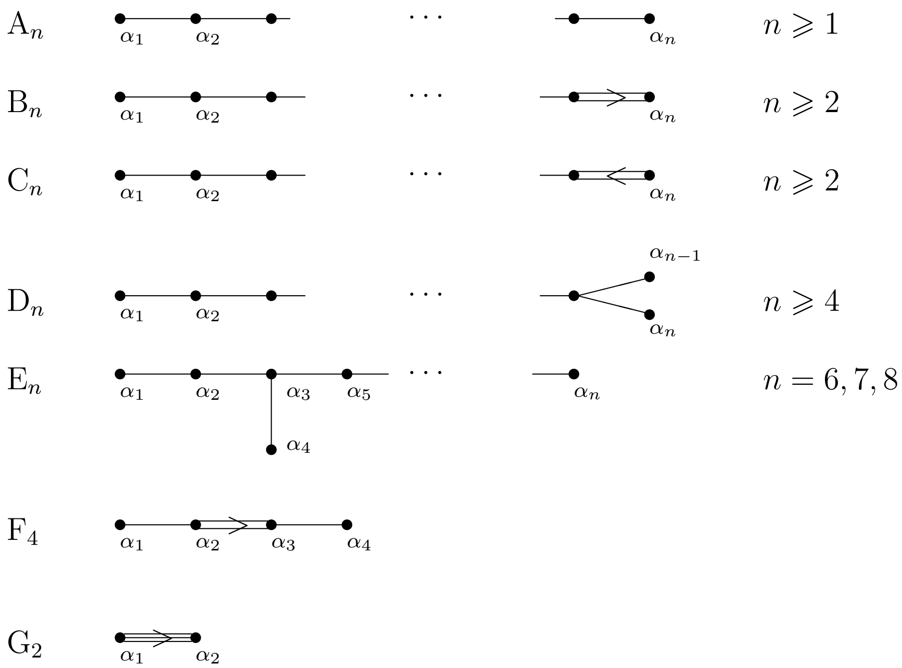
Proof. See [33, p.270]. $\square$

The root system Σ is *irreducible* if there do not exist non-empty disjoint subsets Σ_1, Σ_2 in Σ such that $\Sigma = \Sigma_1 \cup \Sigma_2$ and $(\alpha, \beta) = 0$ for all $\alpha \in \Sigma_1$, $\beta \in \Sigma_2$.

Definition 8.1.6 *A* Dynkin diagram *is a graph with vertex set* Π *and* $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle$ *edges connecting the vertices* $\alpha, \beta \in \Pi$. *If* α *and* β *are joined by at least one edge then, by Corollary 8.1.3, at least one of* $\langle \alpha, \beta \rangle = -1$ *or* $\langle \beta, \alpha \rangle = -1$ *holds. If* $\langle \alpha, \beta \rangle \neq -1$ *the edges between* α *and* β *are labelled with an arrow.*

A complete set of connected Dynkin diagrams is given in Table 8.1.

Table 8.1: Dynkin Diagrams



Theorem 8.1.7 *The irreducible root systems correspond to the connected Dynkin diagrams.*

Proof. [33, Th. 9.6]. $\square$

Lemma 8.1.8 *Suppose* Π *is a fundamental system of the root system* Σ*, with a connected Dynkin diagram. Let* $\alpha \in \Pi$ *and* $\delta = \sum_{\tau\in\Pi} \tau$*. Then there exist positive roots* $\beta_1 = \alpha, \dots, \beta_l = \delta$ *such that* $\beta_i = \beta_{i-1} + \rho$*, where* $\rho \in \Pi$*. In particular,* δ *is a root.*

Proof. We use induction on $|\Pi|$. The case $|\Pi| = 1$ is clear so assume $|\Pi| > 1$. Let Δ be a subset of Π such that $\alpha \in \Delta$, $|\Delta| = |\Pi| - 1$ and Δ has a connected diagram. Inductively there exist positive roots $\beta_1 = \alpha, \dots, \beta_{l-1} = \sum_{\tau\in\Delta} \tau$, spanned by Δ. Now let $\omega \in \Pi \setminus \Delta$. Since Δ is connected and the Dynkin diagram corresponding to Π is a tree, ω is joined to a unique node $\lambda \in \Delta$. Then $\langle \lambda, \omega\rangle \neq 0$ and $\langle \mu, \omega\rangle = 0$ for all $\mu \in \Delta \setminus \{\lambda\}$, so we have

$$(\beta_{l-1}, \omega) = \sum_{\tau\in\Delta} (\tau, \omega) = (\lambda, \omega) < 0.$$

Therefore, by Corollary 8.1.3, either $\langle \beta_{l-1}, \omega\rangle = -1$ or $\langle \omega, \beta_{l-1}\rangle = -1$. If $\langle \beta_{l-1}, \omega\rangle = -1$, then

$$r_\omega(\beta_{l-1}) = \beta_{l-1} - \langle \beta_{l-1}, \omega\rangle\, \omega = \delta,$$

and if $\langle \omega, \beta_{l-1}\rangle = -1$, then

$$r_{\beta_{l-1}}(\omega) = \omega - \langle \omega, \beta_{l-1}\rangle\, \beta_{l-1} = \delta.$$

So δ is a positive root and the lemma holds. $\square$

Let $\Pi = \{\alpha_1, \dots, \alpha_l\}$ be a set of simple roots for the root system Σ. Let $\beta \in \Sigma$. Then we can write $\beta = \sum_{i=1}^{l} m_i\alpha_i$, with $m_i \in \mathbb{Z}$ and either all m_i non-negative, or all m_i

non-positive. We define the *height* of β by $ht(\beta) = \sum_{i=1}^{l} m_i$. The *highest root* is the root with the greatest height, and is unique.

Example 8.1.9 *Let* $\Pi = \{\alpha_1, \ldots, \alpha_7\}$ *be the set of fundamental roots in* E_7. *Let* α^* *be the highest root. Then by [19, p.12],* $\alpha^* = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4 + 3\alpha_5 + 2\alpha_6 + \alpha_7$.

Lemma 8.1.10 *In* E_7, $\alpha^* - \alpha_1$ *is a root.*

Proof. The only node in the Dynkin diagram of type E_7 which α_1 is joined to is α_2, so by Corollary 8.1.3, either $\langle \alpha_1, \alpha_2 \rangle = -1$ or $\langle \alpha_2, \alpha_1 \rangle = -1$, and $\langle \alpha_j, \alpha_1 \rangle = 0$ for $j > 2$. First suppose $\langle \alpha_1, \alpha_2 \rangle = -1$. Then

$$\begin{aligned} r_{\alpha^*}(\alpha_1) &= \alpha_1 - \langle \alpha_1, \alpha^* \rangle \alpha^* \\ &= \alpha_1 - (3\langle \alpha_1, \alpha_2 \rangle + 2\langle \alpha_1, \alpha_1 \rangle)\alpha^* \\ &= \alpha_1 - (-3+4)\alpha^* \\ &= \alpha_1 - \alpha^*. \end{aligned}$$

So $\alpha_1 - \alpha^*$ is a root and hence so is $\alpha^* - \alpha_1$. Now suppose $\langle \alpha_2, \alpha_1 \rangle = -1$. Then

$$\begin{aligned} r_{\alpha_1}(\alpha^*) &= \alpha^* - \langle \alpha^*, \alpha_1 \rangle \alpha_1 \\ &= \alpha^* - (3\langle \alpha_2, \alpha_1 \rangle + 2\langle \alpha_1, \alpha_1 \rangle)\alpha_1 \\ &= \alpha^* - (-3+4)\alpha_1 \\ &= \alpha^* - \alpha_1. \end{aligned}$$

So again $\alpha^* - \alpha_1$ is a root. $\square$

Example 8.1.11 *Let* $\Pi = \{\alpha_1, \ldots, \alpha_8\}$ *be the set of fundamental roots in* E_8. *The highest root is given by* $\alpha^* = 2\alpha_1 + 4\alpha_2 + 6\alpha_3 + 3\alpha_4 + 5\alpha_5 + 4\alpha_6 + 3\alpha_7 + 2\alpha_8$, *see [19, p.12].*

Lemma 8.1.12 *In E_8, $\alpha^* - \alpha_8$ is a root.*

Proof. The proof is similar to that of Lemma 8.1.10, using α_8 in place of α_1. $\square$

8.2 Algebraic Groups

Let K be an algebraically closed field and let $A = K[x_1, \ldots, x_n]$ be the ring of polynomials in n independent commuting variables over K. For any $S \subseteq A$, we define an *algebraic set* to be the set of common zeros of S. That is, algebraic sets have the form

$$\mathcal{V}(S) = \{x \in K^n \mid f(x) = 0 \text{ for all } f \in S\}.$$

The sets $\mathcal{V}(S)$ for $S \subseteq A$ form the *closed* sets of the *Zariski topology* on K^n.

Let $X \subseteq K^n$ be an algebraic set. The *vanishing ideal* of X is

$$\mathcal{I}(X) = \{f \in A \mid f(x) = 0 \text{ for all } x \in X\}.$$

Let $K[X] = A/\mathcal{I}(X)$. This is the *coordinate ring* of X. Since K is algebraically closed, $\mathcal{I}(X)$ is a radical ideal. If X is irreducible, $\mathcal{I}(X)$ is a prime ideal and hence $K[X]$ is an integral domain, see [18] for details.

Definition 8.2.1 *An* affine variety *is a pair $(X, K[X])$ as defined above. Generally we just say X is an affine variety.*

Definition 8.2.2 *Let $K(X)$ be the quotient field of $K[X]$. The dimension of X is the transcendence degree of $K(X)$ over K.*

Definition 8.2.3 *Let K be an algebraically closed field. A* linear algebraic group *G over K is a group which is also an affine variety over K. Let G and H be linear algebraic groups. A map $\phi : G \to H$ is an* algebraic group homomorphism *if ϕ is both a group homomorphism and a morphism of affine varieties.*

Lemma 8.2.4 *A group G is a linear algebraic group over K if and only if it is isomorphic to a closed subgroup of $GL_n(K)$, for some n.*

Proof. See [18, Cor. 2.4.4, p.135]. $\square$

Definition 8.2.5 *A topological space X is* connected *if it cannot be written as the union of two disjoint non-empty open subsets.*

Let G be a linear algebraic group. We denote the closed connected component containing the identity by G°, and note it has finite index in G, see [18, Prop. 1.3.13, p.31]. The dimension of G is defined to be the dimension of G° as an affine variety.

Definition 8.2.6 *Let G be a connected linear algebraic group. The* radical *$R(G)$ of G is the largest closed connected solvable normal subgroup of G. The* unipotent radical *$R_u(G)$ is the largest closed connected unipotent normal subgroup of G. We say G is* semisimple *if and only if $R(G) = 1$ and* reductive *if and only if $R_u(G) = 1$.*

We have $R_u(G) \subseteq R(G)$, so a semisimple group is reductive.

Definition 8.2.7 *A connected linear algebraic group G is* simple *if any proper normal subgroup of G is finite and contained in $Z(G)$.*

Definition 8.2.8 *Let G be a linear algebraic group. A* Borel *subgroup of G is a maximal closed connected solvable subgroup of G.*

If G is a linear algebraic group, every element of G lies in some Borel subgroup of G, and any two Borel subgroups of G are conjugate, see [18, Thm. 3.4.3, p.198].

Definition 8.2.9 *Let G_m be the multiplicative group of K. A* torus *is isomorphic to a direct product of finitely many copies of G_m. A torus is* maximal *in G if it is not properly contained in any other torus in G. Suppose T is a torus in G with $T \cong \underbrace{G_m \times \ldots \times G_m}_{k \text{ times}}$. Then the* dimension *of T is k.*

If G is a linear algebraic group, any two maximal tori in G are conjugate and every torus is contained in some Borel subgroup of G.

Definition 8.2.10 *Let G be an algebraic group with maximal torus T. The* rank *of G is the dimension of T. Let S be a maximal torus in G', the derived subgroup of G. The* semisimple rank *of G is the dimension of S.*

Let G be a linear algebraic group and let B be a Borel subgroup of G. Since B is solvable and connected, we can write $B = R_u(B)T$, where $R_u(B)$ is the unipotent radical of B and T is any maximal torus of B, see [19]. We say $b \in B$ is *unipotent* if $b \in R_u(B)$, and *semisimple* if $b \in T$.

Definition 8.2.11 *Let G be a linear algebraic group and $x \in G$. As above, x must lie in some Borel subgroup B of G. Then x is* unipotent *in G if it is unipotent in B and x is* semisimple *in G if it is semisimple in B. Also, x is* regular *if $\dim C_G(x) =$ rank G.*

Let T be a maximal torus of the connected reductive group G. The *character group* X of T is the set of algebraic group homomorphisms from T to G_m, with multiplication $(\chi_1 + \chi_2)(t) = \chi_1(t)\chi_2(t)$ for all $\chi_1, \chi_2 \in X$, $t \in T$. We define the *cocharacter group* Y to be the set of algebraic group homomorphisms from G_m to T, with multiplication $(\gamma_1 + \gamma_2)(\lambda) = \gamma_1(\lambda)\gamma_2(\lambda)$ for all $\gamma_1, \gamma_2 \in Y$, $\lambda \in G_m$. Write $X = Hom(T, G_m)$ and $Y = Hom(G_m, T)$ to denote these entities.

Lemma 8.2.12 *$Hom(G_m, G_m) \cong \mathbb{Z}$.*

Proof. Clearly $f(x) = x^j \in Hom(G_m, G_m)$ for all $j \in \mathbb{Z}$. Conversely, suppose $f \in Hom(G_m, G_m)$. Then since $Hom(G_m, G_m) \subseteq K[x, x^{-1}]$, $f(x) = \sum_{i \in \mathbb{Z}} a_i x^i$ with all but a finite number of $a_i's$ zero. Let j be the smallest i such that $a_j \neq 0$. Then $g(x) = f(x)x^{-j} \in Hom(G_m, G_m)$ has non-zero constant term and no negative powers. Suppose g has degree r. Define $h(x) = g(x^2) - g(x)^2$. As h has degree at most $2r$, either h has $2r$

roots in K or $h = 0$. Since g is a homomorphism, we have $h(\lambda) = 0$ for all $\lambda \in G_m$, and hence $h = 0$. Let $g(x) = b_r x^r + \ldots + b_1 x + b_0$, where $b_0 \neq 0$. Then

$$h(x) = b_r x^{2r} + \ldots + b_1 x^2 + b_0 - (b_r x^r + \ldots + b_1 x + b_0)^2 = 0.$$

So by equating coefficients we have $b_0 = 1$ and $b_i = 0$ for all $i \neq 1$. Therefore $g = 1$ and hence $f(x)x^{-j} = 1$, that is $f(x) = x^j$. □

Let $\chi \in X$ be a character, and $\gamma \in Y$ be a cocharacter. Then the composition $\chi \circ \gamma$ is a homomorphism from G_m to G_m, so there exists $n \in \mathbb{Z}$ such that $(\chi \circ \gamma)(\lambda) = \lambda^n$ for all $\lambda \in K$, by Lemma 8.2.12. Define $\langle \chi, \gamma \rangle = n$. We can then define a map $\psi : X \times Y \to \mathbb{Z}$ by $\psi((\chi, \gamma)) = \langle \chi, \gamma \rangle$, for $\chi \in X$, $\gamma \in Y$.

Lemma 8.2.13 *We have $X \cong Hom(Y, \mathbb{Z})$ and $Y \cong Hom(X, \mathbb{Z})$.*

Proof. For $\chi \in X$, define $\psi_\chi : Y \to \mathbb{Z}$ by $\psi_\chi(\gamma) = \langle \chi, \gamma \rangle$ for $\gamma \in Y$. Similarly for $\gamma \in Y$ define $\psi_\gamma : X \to \mathbb{Z}$ by $\psi_\gamma(\chi) = \langle \chi, \gamma \rangle$ for $\chi \in X$. By [33, p.23, Prop. 3.6], the maps $\chi \to \psi_\chi$ and $\gamma \to \psi_\gamma$ are isomorphisms from X to $Hom(Y, \mathbb{Z})$ and Y to $Hom(X, \mathbb{Z})$ respectively. □

Again, fix a maximal torus T of G. Let G_a be the additive group of the field K. Any subgroup of G which is isomorphic to G_a is called a *one-parameter subgroup*. A *root subgroup* is a one-parameter subgroup of G which is normalized by T. Let H be a root subgroup of G. Then T acts on H by conjugation, giving a homomorphism $\phi : T \to Aut\ G_a$. So, since $Aut\ G_a$ is isomorphic to G_m, we have $\phi \in X$. Any such homomorphism ϕ is called a root, and we let Φ denote the set of roots. We have Φ is a finite set and, up to isomorphism, is independent of the choice of T. We say Φ is the *root system* of G. By [9, p.77], Φ is a root system in the sense of Section 8.1.

Theorem 8.2.14 *Let X_α be the root subgroup corresponding to the root $\alpha \in \Phi$. Then $G = \langle T, X_\alpha \mid \alpha \in \Phi \rangle$.*

Proof. See [9, p.19]. $\square$

Let G be a connected reductive group with maximal torus T and character and cocharacter groups X and Y respectively. Let Φ be the root system of G with respect to T, with fundamental system Δ. For any $\beta \in \Phi$, there exists $\beta^\vee \in Y$ such that, for all $\alpha \in \Phi$, $\langle \alpha, \beta \rangle = \langle \alpha, \beta^\vee \rangle$, where $\langle \alpha, \beta \rangle$ is as in Section 8.1 and $\langle \alpha, \beta^\vee \rangle$ is as above, [9, p.19]. Let $\Phi^\vee = \{\beta^\vee \mid \beta \in \Phi\}$. This is the set of *coroots* of G and is a finite subset of Y. Clearly, $|\Phi| = |\Phi^\vee|$.

Definition 8.2.15 *Define $(X, \Phi, Y, \Phi^\vee)$ to be the* root datum *for G.*

Let G be a connected semisimple group. Given root datum $(X, \Phi, Y, \Phi^\vee)$, we have $\mathbb{Z}\Phi \leqslant X$ and $\mathbb{Z}\Phi^\vee \leqslant Y$, with both subgroups having finite index [9, p.23]. Let $\Omega = Hom(\mathbb{Z}\Phi^\vee, \mathbb{Z})$. By restriction we have an injection $Hom(Y, \mathbb{Z}) \to \Omega$, so since $X \cong Hom(Y, \mathbb{Z})$, by Lemma 8.2.13, we may identify X with a subgroup of Ω. By [9, p.23], $|\Omega : X| = |Y : \mathbb{Z}\Phi^\vee|$, and so $|X : \mathbb{Z}\Phi||Y : \mathbb{Z}\Phi^\vee| = |\Omega : \mathbb{Z}\Phi|$.

Let G be a connected reductive group with root system Φ. Let Δ be the set of fundamental roots of Φ. If Δ has a connected Dynkin diagram, G is a simple group. However, there is normally more than one linear algebraic group with a particular Dynkin diagram. From a given Dynkin diagram, Φ and $\Phi^\vee$ can be determined up to isomorphism and hence so can Ω. Given G corresponding to a certain Dynkin diagram, there is a subgroup X such that $\mathbb{Z}\Phi \subseteq X \subseteq \Omega$ which determines G up to isomorphism.

Definition 8.2.16 *With G and X as above, G is called adjoint if $X = \mathbb{Z}\Phi$ and simply connected if $X = \Omega$.*

Definition 8.2.17 *Let G and H be linear algebraic groups. An* isogeny *is a surjective homomorphism $\psi : G \to H$ such that ker ψ is finite.*

Let G_{ad} and G_{sc} be the adjoint and simply connected groups corresponding to a given Dynkin diagram. There is an isogeny $G_{sc} \to G_{ad}$, with kernel $Hom(\Omega/\mathbb{Z}\Phi, G_m)$. The centre of G_{sc} is isomorphic to this kernel. Note $Z(G_{ad}) = 1$.

Definition 8.2.18 *Let G be a simple linear algebraic group and assume $\Delta = \{\alpha_1, \ldots, \alpha_l\}$ is a set of fundamental roots. Let $h = \sum_{i=1}^{l} m_i\alpha_i$ be the highest root. A prime p is* bad *for G if p divides m_i for some $1 \leqslant i \leqslant l$. A prime is* good *for G if it is not bad.*

The bad primes for the simple algebraic groups are as follows, [33, p.117].

Group Type	Bad Primes
A_l	none
B_l	2
C_l	2
D_l	2
G_2	2,3
F_4	2,3
E_6	2,3
E_7	2,3
E_8	2,3,5

8.3 Finite Groups of Lie Type

In this section we discuss how the finite groups of Lie type can be obtained from the linear algebraic groups.

Definition 8.3.1 *[9, p.31] Let K be an algebraically closed field of characteristic p and q some positive power of p. Define $F_q : GL_n(K) \to GL_n(K)$ by $F_q((a_{ij})) = (a_{ij}^q)$. Now let G be a linear algebraic group over K and F a homomorphism of G. Suppose there exists an injective map $i : G \to GL_n(K)$ such that $i \circ F = F_q \circ i$. Then F is a* standard

Frobenius map. *A* Frobenius map *on G is a homomorphism $F : G \to G$ such that there is some integer $m > 0$ with F^m a standard Frobenius map. Following [19], we say F is a Frobenius map of* level $q^{\frac{1}{m}}$.

Definition 8.3.2 *Let G be a linear algebraic group and F be a Frobenius map on G. The fixed point set of F on G is*

$$G^F = \{g \in G \mid F(g) = g\}.$$

Lemma 8.3.3 *If G is a linear algebraic group and F is a Frobenius map on G, then G^F is a finite group.*

Proof. See [18, Prop. 4.1.4, p.228]. □

Definition 8.3.4 *Let G be a connected reductive group and F be a Frobenius map on G. Then G^F is called a* finite group of Lie type.

Proposition 8.3.5 *Let F be a Frobenius map on G, of level q_0 and let H be a closed subgroup of G. Then the restriction of F to H is a Frobenius map on H of level q_0.*

Proof. See [19, Prop. 2.1.10, p.34]. □

The following is the Lang-Steinberg Theorem.

Theorem 8.3.6 (Lang-Steinberg) *Let G be a connected linear algebraic group over K, with Frobenius map F. Then the map $L : G \to G$, $L(g) = g^{-1}F(g)$, is surjective.*

Proof. See [9, p.32]. □

Definition 8.3.7 *Let G be a connected linear algebraic group over K, with Frobenius map F. A subgroup H of G is F-*stable *if $F(H) = H$.*

The following result is a standard application of the Lang-Steinberg Theorem.

Lemma 8.3.8 *Let G be a connected reductive group with Frobenius map F. Then G contains an F-stable Borel subgroup, and an F-stable maximal torus.*

Proof. Let B be a Borel subgroup in G. Then $F(B)$ is also a Borel subgroup and so, as all Borel subgroups of G are conjugate in G, there exists $g \in G$ such that $F(B) = g^{-1}Bg$. Now by the Lang-Steinberg Theorem, $g = x^{-1}F(x)$ for some $x \in G$. Then

$$F(xBx^{-1}) = F(x)F(B)F(x)^{-1} = xgF(B)g^{-1}x^{-1} = xBx^{-1}.$$

So xBx^{-1} is an F-stable Borel subgroup in G. The proof is the same for maximal tori.□

Definition 8.3.9 *Let G be a connected reductive group with Frobenius map F. Let B be an F-stable Borel subgroup and T an F-stable maximal torus of G. Then we say B^F is a* Borel subgroup *and T^F is a* maximal torus *of G^F.*

Definition 8.3.10 *Let G be a connected reductive group with Frobenius map F. A* maximally split torus *of G is an F-stable maximal torus T which is contained in an F-stable Borel subgroup. Then T^F is a* maximally split torus *of G^F.*

Lemma 8.3.11 *Let G be a simple linear algebraic group with Frobenius map F. Let H be the preimage of $(G/Z(G))^F$ in G under the natural homomorphism. Then $\psi : H \to Z(G)$, $\psi(h) = h^{-1}F(h)$, is a surjective homomorphism with kernel G^F.*

Proof. Let $g, h \in H$. Then

$$\psi(gh) = (gh)^{-1}F(gh) = h^{-1}g^{-1}F(g)F(h) = h^{-1}\psi(g)F(h) = \psi(g)h^{-1}F(h) = \psi(g)\psi(h),$$

since $\psi(g) \in Z(G)$. So ψ is a homomorphism. Now let T be an F-stable maximal torus of G. Note T is connected and $Z(G) \leqslant T$, see [19, Th. 1.9.5, p.14], so for any $z \in Z(G)$

there is a $t \in T$ such that $z = t^{-1}F(t)$, by the Lang-Steinberg Theorem. For any $g \in G$, $g \in H$ if and only if $g^{-1}F(g) \in Z(G)$. Therefore $t \in H$ and hence ψ is surjective. Finally, $k \in \ker\psi$ if and only if $k^{-1}F(k) = 1$. So, since $G^F \leqslant H$, we have $\ker\psi = G^F$. □

8.4 Dual Groups

Let G be a connected reductive group with root datum $(X, \Phi, Y, \Phi^\vee)$. Then $(Y, \Phi^\vee, X, \Phi)$ is also the root datum for a connected reductive group G^*, [9, Prop 4.2.1, p.112]. We call G^* the *dual group* of G and note it is unique up to isomorphism.

Suppose F is a Frobenius map on G. We can define an action of F on X and Y as follows. Let T be a maximally split torus of G with respect to F. For $\chi \in X$, $t \in T$, let $(F(\chi))(t) = \chi(F(t))$, and for $\gamma \in Y$, $\lambda \in G_m$, let $(F(\gamma))(\lambda) = F(\gamma(\lambda))$. We have the following definition from [9, Prop. 4.3.1, p.114].

Definition 8.4.1 *Suppose G and G^* are connected reductive groups with Frobenius maps F and F^* respectively, and let $T \leqslant G$ and $T^* \leqslant G^*$ be maximally split tori. Let the corresponding root datum for G be $(X, \Phi, Y, \Phi^\vee)$ and for G^* be $(X^*, \Phi^*, Y^*, \Phi^{*\vee})$. Then (G, F) and (G^*, F^*) are in duality if there exists an isomorphism $\delta : X \to Y^*$ such that*

(i) $\delta(\Phi) = \Phi^{*\vee}$;

(ii) $\langle \chi, \alpha^\vee \rangle = \langle \alpha^*, \delta(\chi) \rangle$ *for all* $\chi \in X$, $\alpha \in \Phi$, *where* $\delta(\alpha) = (\alpha^*)^\vee$;

(iii) $\delta(F(\chi)) = F^*(\delta(\chi))$ *for all* $\chi \in X$.

Parts (i) and (ii) of this definition show G and G^* are dual groups.

Definition 8.4.2 *Suppose (G, F) and (G^*, F^*) are in duality. Then G^F and ${G^*}^{F^*}$ are* dual groups.

Lemma 8.4.3 *Suppose G^F and ${G^*}^{F^*}$ are dual groups. Then $|G^F| = |{G^*}^{F^*}|$.*

Proof. See [9, Prop. 4.4.4, p.118]. □

Let G be a simple algebraic group with Frobenius map F. Generally, if G^F is of adjoint type, the dual group G^{*F^*} is the corresponding simply connected group with the same root system. The only exceptions are $G^F = (B_l)_{ad}(q)$, where $G^{*F^*} = (C_l)_{sc}(q)$, and $G^F = (C_l)_{ad}(q)$, where $G^{*F^*} = (B_l)_{sc}(q)$, [9, p.120].

8.5 Centralizers

For this section let G be a connected reductive group and fix a maximal torus T of G. Let X be the character group of T and Φ the corresponding root system, with fundamental system Δ. Recall every semisimple element in G is conjugate to an element of T.

Theorem 8.5.1 *Let s be a semisimple element of T. Then $s \in C_G(s)^\circ$ and $C_G(s)^\circ$ is reductive with root system $\Phi_1 = \{\alpha \in \Phi : \alpha(s) = 1\}$, where $C_G(s)^\circ$ is the connected component of $C_G(s)$.*

Proof. See [9, section 3.5]. □

Lemma 8.5.2 *Suppose $\alpha \in \Delta$ with $\alpha(x) \neq 1$, for $x \in T$. Then for any $\beta \in \Phi$, if $\alpha + \beta \in \Phi$, $(\alpha + \beta)(x) \neq 1$.*

Proof. From the definition of multiplication in X, we have $(\alpha + \beta)(x) = \alpha(x)\beta(x) \neq 1$. □

Let $s \in T$ be a non-central semisimple element of G and let $C_G(s)^\circ$ have root system Φ_1. If $\Delta \subseteq \Phi_1$, we have $\Phi \subseteq \Phi_1$ and hence $\Phi = \Phi_1$. This implies $C_G(s)^\circ = G$, a contradiction. Therefore there exists $\alpha \in \Delta$ such that $\alpha \notin \Phi_1$. So by Lemma 8.1.8 there are at least $|\Delta|$ roots in Φ^+ which are not in Φ_1^+. This gives us the following lemma.

Lemma 8.5.3 *With the above conditions, we have $|\Phi_1^+| \leqslant |\Phi^+| - |\Delta|$.*

Corollary 8.5.4 *If the root system of G is not of type A_l, we have $|\Phi_1^+| \leqslant |\Phi^+| - |\Delta| - 1$. Further, if the root system of G is of type E_7 or E_8, $|\Phi_1^+| \leqslant |\Phi^+| - |\Delta| - 2$.*

Proof. The highest root α^* is a positive root including α in its sum. Therefore, by Lemma 8.5.2, $\alpha^*(s) \neq 1$ and so $\alpha^* \notin \Phi_1$. For groups of type other than A_l, the root α^* is not one of the β_i, $1 \leqslant i \leqslant l$, in Lemma 8.1.8, so we are done. For groups of type E_7 and E_8 we also have the roots given by Lemmas 8.1.10 and 8.1.12. $\square$

We have the following lemma from [9, p.27].

Lemma 8.5.5 *Let x be an element of an algebraic group G. Then $C_G(x)$ is a closed subgroup of G.*

Lemma 8.5.6 *Let F be a Frobenius map on G and let x be an element in G^F. Then $C_G(x)$ is F-stable.*

Proof. Let $g \in C_G(x)$. Then

$$F(g)^{-1}xF(g) = F(g^{-1})F(x)F(g) = F(g^{-1}xg) = F(x) = x,$$

and so $F(g) \in C_G(x)$. $\square$

Corollary 8.5.7 *Let F be a Frobenius map on G and let s be a semisimple element in G^F. Then F is a Frobenius map on $C_G(s)$.*

Proof. This follows from Lemmas 8.3.5, 8.5.5 and 8.5.6. $\square$

Lemma 8.5.8 *Let F be a Frobenius map on G, let $g \in G^F$ and $x \in G$. Then $g^x \in G^F$ if and only if $xF(x^{-1}) \in C_G(g)$.*

Proof. Suppose $g^x \in G^F$. Then $F(g^x) = g^x$ and hence $F(g)^{F(x)} = g^x$. Therefore, since $g \in G^F$, $g^{F(x)} = g^x$ and so $xF(x^{-1}) \in C_G(g)$. Conversely, if $xF(x^{-1}) \in C_G(g)$, $g^x = g^{F(x)} = F(g)^{F(x)} = F(g^x)$ as required. $\square$

Lemma 8.5.9 *Let G be a connected reductive group with root system Φ and let F be a Frobenius map on G. Then a Sylow p-subgroup of G^F has order $q^{|\Phi^+|}$.*

Proof. See [9, p.74]. $\square$

Corollary 8.5.10 *Let G be a connected reductive group with Frobenius map F, and let $s \in G^F$ be semisimple. Assume $C_G(s)$ is connected with root system Φ_1. Then $|C_{G^F}(s)|_p \leqslant q^{(|\Phi^+|-|\Delta|)}$. Further, if G is not of type A_l, $|C_{G^F}(s)|_p \leqslant q^{(|\Phi^+|-|\Delta|-1)}$ and if G is of type E_7 or E_8, $|C_{G^F}(s)|_p \leqslant q^{(|\Phi^+|-|\Delta|-2)}$.*

Proof. By Corollary 8.5.7, F is a Frobenius map on $C_G(s)$. Therefore $C_G(s)$ is a connected reductive group with Frobenius map F, so by Lemma 8.5.9 $|C_{G^F}(s)|_p = q^{|\Phi_1^+|}$. Hence by Lemma 8.5.3 we have $|C_{G^F}(s)|_p \leqslant q^{(|\Phi^+|-|\Delta|)}$ as required. The remainder follows from Corollary 8.5.4. $\square$

8.6 Regular Unipotent Conjugacy Classes

In this section, we assume G is a connected reductive group with a connected centre and F is a Frobenius map on G.

Lemma 8.6.1 *There exist regular unipotent elements in G^F. The number of them is $\frac{|G^F|}{|Z(G)^F|q^l}$, where l is the semisimple rank of G.*

Proof. See [9, Prop. 5.1.7, p.130, Prop. 5.1.9, p.131]. $\square$

Lemma 8.6.2 *Let u be a regular unipotent element in G. Then $C_G(u)$ is abelian.*

Proof. See [16, Cor. 1.16, p.220]. $\square$

Definition 8.6.3 *Let H be an F-invariant subgroup of G. Define an equivalence relation on H by $x \sim y$ if and only if there exists $g \in H$ such that $y = gxF(g^{-1})$. Let $H^1(F, H)$ denote the equivalence classes of this relation.*

Lemma 8.6.4 *Let H be a closed F-invariant subgroup of G. There is a bijection from $H^1(F, H)$ to $H^1(F, H/H^\circ)$.*

Proof. See [19, Thm. 2.1.4, p.32]. $\square$

Corollary 8.6.5 *Let u be a regular unipotent element in G^F. Then there is a bijection from $H^1(F, C_G(u))$ to $H^1(F, C_G(u)/C_G(u)^\circ)$.*

Proof. We see $C_G(u)$ is closed and F-stable by Lemmas 8.5.5 and 8.5.6, so this follows by Lemma 8.6.4. $\square$

Lemma 8.6.6 *Let u be an element in G^F. Suppose $u^x, u^y \in G^F$ for $x, y \in G$. Then u^x and u^y are conjugate in G^F if and only if $xF(x^{-1}) \sim yF(y^{-1})$ in $C_G(u)$.*

Proof. Suppose there exists $g \in G^F$ such that $u^x = (u^y)^g$. Then $u = u^{ygx^{-1}}$ and so $ygx^{-1} \in C_G(u)$. Let $h \in C_G(u)$ be such that $ygx^{-1} = h$. Then $g = y^{-1}hx$ and since $g \in G^F$, $F(y^{-1}hx) = y^{-1}hx$. This means $yF(y^{-1}) = hxF(x^{-1})F(h^{-1})$, and so $xF(x^{-1}) \sim yF(y^{-1})$.

Conversely, suppose $xF(x^{-1}) \sim yF(y^{-1})$. Then since $xF(x^{-1}), yF(y^{-1}) \in C_G(u)$ by Lemma 8.5.8, there exists $h \in C_G(u)$ such that $yF(y^{-1}) = hxF(x^{-1})F(h^{-1})$. Then $y^{-1}hx = F(y^{-1}hx)$ and so $y^{-1}hx \in G^F$. Now, $(u^y)^{y^{-1}hx} = u^{hx} = u^x$ and so u^x and u^y are conjugate in G^F. $\square$

Lemma 8.6.7 *Let u be a regular unipotent element in G^F. There is a bijection between the set of regular unipotent conjugacy classes in G^F and $H^1(F, C_G(u)/C_G(u)^\circ)$.*

Proof. By the Lang-Steinberg Theorem, every element of $C_G(u)$ can be written as $xF(x^{-1})$, for some $x \in G$. From Lemmas 8.5.8 and 8.6.6, we have u^x is conjugate to u^y in G^F if and only if $xF(x^{-1}) \sim yF(y^{-1})$ where $\sim$ is an the equivalence relation with equivalence classes $H^1(F, C_G(u))$. The result now follows from Corollary 8.6.5. $\square$

Corollary 8.6.8 *The number of conjugacy classes of regular unipotent elements in G^F is $|H^1(F, C_G(u)/C_G(u)^\circ)|$.*

Proof. This follows directly from Lemma 8.6.7. $\square$

Now let $g_1, \ldots, g_s$ be representatives of the distinct classes of $H^1(F, C_G(u))$. By the Lang-Steinberg Theorem, there exist $h_i \in G$ such that $g_i = h_i F(h_i^{-1})$ for $1 \leqslant i \leqslant s$. For each i, let $w_i = u^{h_i}$. Then $\{w_1, \ldots, w_s\}$ is a set of conjugacy class representatives for the regular unipotent conjugacy classes of G^F. Let $F_i = F c_{g_i^{-1}}$, where c_g is conjugation by g.

Lemma 8.6.9 *For $1 \leqslant i \leqslant s$, the action of F on $C_G(w_i)$ is equivalent to the action of F_i on $C_G(u)$.*

Proof. Let $x \in C_G(u)$. Then $F(x^{h_i}) = F(x)^{F(h_i)} = (F(x)^{g_i^{-1}})^{h_i} = (F_i(x))^{h_i}$, since $g_i = h_i F(h_i^{-1})$. $\square$

Corollary 8.6.10 *For $1 \leqslant i \leqslant s$, $|C_{G^F}(w_i)| = |C_{G^{F_i}}(u)|$.*

Lemma 8.6.11 *We have $C_{G^{F_i}}(u) = C_{G^F}(u)$ for $1 \leqslant i \leqslant s$.*

Proof. $x \in C_{G^{F_i}}(u)$ if and only if $x \in C_G(u)$ and $F_i(x) = x$. So by Lemma 8.6.2, this is if and only if $x \in C_{G^F}(u)$. $\square$

Corollary 8.6.12 *The centralizers of all regular unipotent elements in G^F have the same size.*

Proof. For $1 \leqslant i \leqslant s$, $|C_{G^F}(w_i)| = |C_{G^{F_i}}(u)| = |C_{G^F}(u)|$, by Corollary 8.6.10 and Lemma 8.6.11. $\square$

Lemma 8.6.13 *Let x be a regular unipotent element in G^F. Then there is a unique maximal connected unipotent subgroup U of G containing x. Furthermore we have the following results.*

(i) $C_G(x) = Z(G)C_U(x)$*. So if* G *is of adjoint type,* $C_G(x) = C_U(x)$*.*

(ii) $C_U(x)$ *is connected if and only if* p *is a good prime for* G*.*

(iii) If G *is simple and* p *is bad for* G*, the order of* $C_U(x)/C_U(x)^\circ$ *is* p *unless* G *is of type* E_7 *or* E_8 *and* $p = 2$*. In these cases* $C_U(x)/C_U(x)^\circ$ *has order* 4*.*

(iv) If G *is simple and adjoint, the number of* G^F *conjugacy classes of regular unipotent elements is* $|C_U(x)/C_U(x)^\circ|$*.*

Proof. See [16, p.220]. □

Theorem 8.6.14 *Let* G *be a simple algebraic group of adjoint type. If* p *is a good prime for* G*, there is only one conjugacy class of regular unipotent elements in* G^F *and its order is* $\frac{|G^F|}{q^l}$*. If* p *is a bad prime for* G*, every regular unipotent conjugacy class in* G^F *has size* $\frac{|G^F|}{pq^l}$ *unless* G *is of type* E_7 *or* E_8 *and* $p = 2$*, in which case it has size* $\frac{|G^F|}{4q^l}$*.*

Proof. Since G is of adjoint type, $Z(G) = 1$. The result is clear for good primes from Lemmas 8.6.1 and 8.6.13. Now suppose p is a bad prime for G. From Lemma 8.6.13 there are p conjugacy classes of regular unipotent elements in G^F, except if G is of type E_7 or E_8 and $p = 2$, when there are four such classes. So, since by Corollary 8.6.12, the centralizers of regular unipotent elements in G^F all have the same order, we have the result. □

8.7 Regular Semisimple Elements

Let G be a connected semisimple group with Frobenius map F.

Definition 8.7.1 *Let* $x \in G^F$ *be semisimple. Then* x *is* regular *if and only if* $|C_{G^F}(x)|_p = 1$*.*

Lemma 8.7.2 *There exist regular semisimple elements in* G^F_{sc}*.*

Proof. This follows from [32, Th. 3.3]. $\square$

Lemma 8.7.3 *Suppose $x \in G_{sc}^F$ is regular semisimple. Let $Z = Z(G_{sc}^F)$ and $K = G_{sc}^F/Z$. Then xZ is regular semisimple in K.*

Proof. Let $X = \langle x, Z\rangle$, so $C_K(xZ) = C_K(X/Z)$. Suppose xZ is not regular semisimple. Then p divides $|C_K(X/Z)|$ and so there exists $cZ \in C_K(X/Z)$ which has order p. We have $(|Z|, p) = 1$, so $|\langle c, Z\rangle| = p|Z|$, and hence we may assume c has order p. Let $C = \langle c\rangle$. Then $(|C|, |X|) = 1$ and so the action of C on X is coprime. Hence, by [30, 8.2.7, p.187], $[X, C] = [X, C, C] \leqslant [Z, C] = 1$. Therefore C centralizes X and in particular $c \in C_{G_{sc}^F}(x)$ which implies p divides $|C_{G_{sc}^F}(x)|$, a contradiction. $\square$

Corollary 8.7.4 *There exist regular semisimple elements in G_{ad}^F.*

Proof. We have $K \cong (G_{ad}^F)'$ and so by Lemma 8.7.3, there is a regular unipotent element $z \in (G_{ad}^F)'$. Now note $G_{ad}^F/(G_{ad}^F)'$ is a p'-group, so $|C_{G_{ad}^F}(z)|_p = |C_{(G_{ad}^F)'}(z)|_p = 1$. Therefore z is a regular unipotent element in G_{ad}^F. $\square$

Chapter 9

Character degrees of Finite groups of Lie Type

9.1 Characters

The aim of this section is to provide the character theoretic background needed to prove our theorem. The theory is known as Deligne-Lusztig theory and is developed in [9].

Definition 9.1.1 *Let $\chi_1, \ldots, \chi_k$ be all the irreducible characters of a finite group G. A* generalized character *of G is any function $\chi = \sum_{i=1}^{k} n_i \chi_i$, with $n_i \in \mathbb{Z}$ for $1 \leqslant i \leqslant k$.*

From now on, let G be a connected reductive group with a Frobenius map F. For any maximal torus T^F in G^F, let $\widehat{T}^F = Hom(T^F, \mathbb{C}^*)$ be the set of complex characters of T^F. In [9], Carter defines an equivalence relation on the pairs (T, θ), where T is a maximal F-stable torus of G and $\theta \in \widehat{T}^F$. This is known as geometric conjugacy, see [9, p.107] for details.

Lemma 9.1.2 *Let G^* be a connected reductive group with Frobenius map F^* and assume (G, F) and (G^*, F^*) are in duality. Then there is a bijection between the geometric conjugacy classes in G and the F^*-stable semisimple conjugacy classes in G^*.*

Proof. See [9, Thm. 4.4.6, p.119]. □

In [13], Deligne and Lusztig defined a generalized character $R_{T,\theta}$ for each F-stable maximal torus T and each $\theta \in \widehat{T}^F$. The theory is very complicated, and includes cohomology groups, so we shall just state a couple of facts about these characters, without including the details.

Lemma 9.1.3 *Let χ be an irreducible character of G^F. Then χ is a constituent of $R_{T,\theta}$ for some F-stable maximal torus T and $\theta \in \widehat{T}^F$.*

Proof. See [9, Cor. 7.5.7, p.236]. □

Lemma 9.1.4 *Suppose T and T' are F-stable maximal tori of G and let $\theta \in \widehat{T}^F$ and $\theta' \in \widehat{T'}^F$. If (T, θ) and (T', θ') are not in the same geometric conjugacy class, then $R_{T,\theta}$ and $R_{T',\theta'}$ have no common irreducible constituents.*

Proof. See [9, Th. 7.3.8, p.220]. □

Now suppose for some irreducible character χ of G, we have $(R_{T,\theta}, \chi) \neq 0$ and $(R_{T',\theta'}, \chi) \neq 0$, where T, T', θ and θ' are as before. Then by Lemma 9.1.4, (T, θ) and (T', θ') must be in the same geometric conjugacy class. Thus, by Lemma 9.1.3, each irreducible character of G^F determines some geometric conjugacy class.

Definition 9.1.5 *Let χ_i and χ_j be irreducible characters of G^F. We say χ_i and χ_j are* geometrically conjugate *if they determine the same geometric conjugacy class.*

We now need to assume our connected reductive group G has a connected centre.

Definition 9.1.6 *Let χ be an irreducible character of G^F. If its average value on the regular unipotent elements of G^F is nonzero then we say that χ is* semisimple.

Every geometric conjugacy class, κ, of irreducible characters of G^F contains exactly one semisimple character. This character is defined by

$$\chi_\kappa = \pm \sum_{(T,\theta)\in\kappa, mod G^F} \frac{R_{T,\theta}}{(R_{T,\theta}, R_{T,\theta})},$$

where the sum is taken over one representative of each G^F-orbit on κ and the sign is chosen to make $\chi_\kappa(1)$ positive, [9, p.288].

An important result for us is the following.

Lemma 9.1.7 *The degree of any semisimple character is coprime to p.*

Proof. See [9, Th. 8.4.8, p.288]. □

The geometric conjugacy class containing the principal character is the one corresponding to $(T, 1)$, where T is any F-stable maximal torus of G.

Definition 9.1.8 *Let χ be an irreducible character of G^F. If χ is a constituent of $R_{T,1}$ for any F-stable maximal torus of G then it is called* unipotent.

Lists of the degrees of the unipotent characters of G^F, for G simple, are given in [9, Ch. 13].

There is the following Jordan decomposition for characters, see [9, 12.9, p.391]. This will be very useful to us.

Lemma 9.1.9 *Let χ be an irreducible character of G^F. Then there exists a pair (χ_s, χ_u) such that $\chi(1) = \chi_s(1)\chi_u(1)$, where χ_s is a semisimple character of G^F and χ_u is a unipotent character of $C_{G^{*F^*}}(s^*)$, where s^* is a semisimple element in the conjugacy class of ${G^*}^{F^*}$ determined by χ_s as in Lemma 9.1.2.*

At last our first concrete result.

Lemma 9.1.10 *Let G be a simple connected reductive group of adjoint type and let F be a Frobenius map on G. Let χ be an irreducible character of G^F which is not unipotent. Then $\chi(1)$ divides $|cl_{G^F}(u)|$, where u is any regular unipotent element in G^F.*

Proof. First, let p be a good prime for G. Then $|cl_{G^F}(u)| = \frac{|G^F|}{q^l}$, by Theorem 8.6.14. We know $\chi(1)$ divides $|G^F|$, so we only need to consider the p-part of $\chi(1)$. Let (χ_s, χ_u) be the Jordan decomposition of χ. By Lemma 9.1.7, $(\chi_s(1))_p = 1$ and since χ is not unipotent, χ_s is not the principal character. Then s^* is a non-central element of G^{*F^*}. Now, χ_u is a character of $C_{G^*F^*}(s^*)$, so $\chi_u(1)$ divides $|C_{G^*F^*}(s^*)|$. Therefore by Corollary 8.5.10, $(\chi_u(1))_p \leqslant q^{|\Phi^+|-l}$, and so since $|G^F|_p = q^{|\Phi^+|}$, $\chi(1)$ divides $\frac{|G^F|}{q^l}$ as required.

Now we consider the situation for bad primes. Let p be a bad prime for G, but assume we do not have $p = 2$ and G of type E_7 or E_8. Then we have $|cl_{G^F}(u)| = \frac{|G^F|}{pq^l}$ by Theorem 8.6.14. Clearly $\frac{|G^F|}{q^{l+1}}$ divides $\frac{|G^F|}{pq^l}$. So, since we have $|C_{G^*F^*}(s^*)|_p \leqslant q^{|\Phi^+|-l-1}$ by Corollary 8.5.10, the result follows as above.

Finally we consider the case $p = 2$ and G of type E_7 or E_8. By Theorem 8.6.14, $|cl_{G^F}(u)| = \frac{|G^F|}{4q^l}$ and so the result follows from Corollary 8.5.10 as before. □

9.2 The Steinberg Character

Definition 9.2.1 *A group $\mathcal{G}$, with subgroups $\mathcal{B}$ and $\mathcal{N}$, is said to have a BN-*pair *if the following are satisfied.*

(i) $\mathcal{G} = \langle \mathcal{B}, \mathcal{N} \rangle$.

(ii) $\mathcal{H} = \mathcal{B} \cap \mathcal{N} \trianglelefteq \mathcal{N}$.

(iii) $\mathcal{W} = \mathcal{N}/\mathcal{H}$ *is generated by a set* $S = \{s_i \mid i \in I, s_i^2 = 1\}$.

(iv) For $i \in I$, $n_i \mathcal{B} n_i \neq \mathcal{B}$, *where* $n_i \in \mathcal{N}$ *is any preimage of* s_i.

(v) $n_i \mathcal{B} n \subseteq \mathcal{B} n_i n \mathcal{B} \cup \mathcal{B} n_i \mathcal{B}$ *for* $n \in \mathcal{N}$ *and* n_i *as before.*

Definition 9.2.2 *Let $\mathcal{G}$ be a group with a BN-pair, $\mathcal{B}, \mathcal{N}$. Then $\mathcal{G}$ has a split BN-pair if there exists a unipotent subgroup $\mathcal{U} \trianglelefteq \mathcal{B}$ such that:*

(i) $\mathcal{B} = \mathcal{U}\mathcal{H}$ *and* $\mathcal{U} \cap \mathcal{H} = \{1\}$;

(ii) $\bigcap_{n \in \mathcal{N}} n\mathcal{B}n^{-1} = \mathcal{H}$.

Example 9.2.3 *Set $\mathcal{G} = GL(n, K)$. Let $\mathcal{B}$ be the subgroup of lower triangular matrices, $\mathcal{N}$ be the subgroup of monomial matrices and $\mathcal{U}$ be the subgroup of lower unitriangular matrices. Then $\mathcal{B}, \mathcal{N}$ is a split BN-pair for $\mathcal{G}$. Note $\mathcal{H}$ is the subgroup of diagonal matrices.*

Let $\mathcal{G}$ be a group with a BN-pair, $\mathcal{B}, \mathcal{N}$. For any $J \subseteq I$ let $\mathcal{W}_J = \langle s_i : i \in J \rangle$, and $\mathcal{N}_J$ be such that $\mathcal{N}_J/\mathcal{H} = \mathcal{W}_J$. Define $\mathcal{P}_J = \mathcal{B}\mathcal{N}_J\mathcal{B}$. This is a subgroup by [9, Prop 2.1.4, p.43].

Definition 9.2.4 *We say $\mathcal{P}_J$ is a* standard parabolic subgroup *of $\mathcal{G}$.*

Definition 9.2.5 *Let $\mathcal{G}$ be a finite group with a BN-pair. The* Steinberg character *of $\mathcal{G}$ is given by*

$$St = \sum_{J \subseteq I} (-1)^{|J|} (1_{\mathcal{P}_J})^{\mathcal{G}},$$

where $(1_{\mathcal{P}_J})^{\mathcal{G}}$ is the principal character of $\mathcal{P}_J$ induced up to $\mathcal{G}$.

Lemma 9.2.6 *The Steinberg character is irreducible.*

Proof. See [9, Cor. 6.2.4, p.190]. □

Theorem 9.2.7 *Let G be a connected reductive group with Frobenius map F. Then*

(i) G has a split BN-pair;

(ii) G^F has a split BN-pair.

Proof. Let B be an F-stable Borel subgroup in G and let T be an F-stable maximal torus of G contained in B. Let $N = N_G(T)$ and $U = R_u(B)$, the unipotent radical of B. Note N and U are also F-stable and $B \cap N = T$. Then B, N is a split BN-pair for G and B^F, N^F is a split BN-pair for G^F. See [9, p.22,23,34] for details. $\square$

From now on suppose G is a finite group of Lie type and P_J is a standard parabolic subgroup of G. Then P_J is a semidirect product $P_J = L_J U_J$ where $L_J \cap U_J = 1$ and U_J is the largest normal unipotent subgroup of P_J. This is known as the *Levi decomposition* of P_J and L_J is called a *standard Levi subgroup.* Furthermore, L_J is a finite group of Lie type. See [10, p.119] for details.

The following lemma gives us a way to calculate the values of the Steinberg character on G.

Lemma 9.2.8 *Let St_G and St_{L_J} be the Steinberg characters of G and L_J respectively. Then $St_G \downarrow_{P_J} = St_{L_J} \uparrow^{P_J}$.*

Proof. See [9, p.191]. $\square$

Lemma 9.2.9 *Let G be a finite group of Lie type. Then $St_G(1) = |R_U(B)|$.*

Proof. From Lemma 9.2.8 we have $St_G(1) = St_{L_J} \uparrow^{P_J} (1)$. Let $J = \emptyset$. Then $P_J = L_J U_J = T R_U(B) = B$. So

$$St_G(1) = St_T \uparrow^B (1) = \frac{1}{|T|} \sum_{x \in B} St_T(1) = \frac{|B|}{|T|} St_T(1) = |R_U(B)|,$$

since T is abelian. $\square$

Theorem 9.2.10 *Let G be a connected reductive group with a Frobenius map F. Let g be a regular semisimple element in G^F. Then $St(1)$ divides $|cl_{G^F}(g)|$.*

Proof. From Lemma 9.2.9, $St(1) = |G^F|_p$. So since $|C_{G^F}(g)|_p = 1$, the result clearly follows. $\square$

9.3 Unipotent Characters

The aim of this section is to prove the following result.

Theorem 9.3.1 *Let G be a simple algebraic group of adjoint type, with Frobenius map F, and let χ be any irreducible unipotent character of G^F, other than the Steinberg character. Then $\chi(1)$ divides $|cl_{G^F}(u)|$ for any regular unipotent element $u \in G^F$.*

To prove this lemma, we need to consider the different types of root system separately. We rely heavily on the results in [9, 13.8].

Suppose G is of type A_l. Then the unipotent characters are parameterized by partitions of $l+1$. Let $\alpha = (\alpha_1, \ldots, \alpha_m) \vdash l+1$, with $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_m$, and let $\lambda_i = \alpha_i + i - 1$, for $1 \leqslant i \leqslant m$. Let χ_α be the character corresponding to α. Then from [9, p.465]

$$\chi_\alpha(1) = \frac{\displaystyle\prod_{k=1}^{l+1}(q^k-1)\prod_{i,j,j<i}(q^{\lambda_i}-q^{\lambda_j})}{\displaystyle q^{L_m}\prod_i\prod_{k=1}^{\lambda_i}(q^k-1)},$$

where

$$L_m = \binom{m-1}{2} + \binom{m-2}{2} + \ldots + \binom{2}{2}.$$

Lemma 9.3.2 *Let χ_α be the irreducible unipotent character of G^F corresponding to $\alpha \vdash l+1$. Then $(\chi_\alpha(1))_p = q^{\sum_{i=1}^{m-1}(m-i)\alpha_i}$.*

Proof. We have

$$
\begin{aligned}
(\chi_\alpha(1))_p &= \frac{\displaystyle\prod_{i,j,j<i} q^{\lambda_j}}{q^{L_m}} \\
&= q^{\sum_{i=1}^{m-1}(m-i)\lambda_i - L_m} \\
&= q^{\sum_{i=1}^{m-1}(m-i)\alpha_i}
\end{aligned}
$$

from Lemma 7.0.1. □

Lemma 9.3.3 *Theorem 9.3.1 holds for G of type A_l.*

Proof. From Lemma 7.0.2 we know the unipotent character with the largest p-part is given by the partition $(1, 1, \ldots, 1) \vdash l + 1$. This corresponds to the Steinberg character. By the same lemma, the character with the next largest p-part corresponds to $\alpha = (1, \ldots, 1, 2) \vdash l + 1$. By Lemma 9.3.2, for this α we have

$$(\chi_\alpha(1))_p = q^{\sum_{i=1}^{l-1}(l-i)} = q^{\frac{l(l-1)}{2}}.$$

There are no bad primes for A_l, so for all p and regular unipotent $u \in G^F$, $|cl_{G^F}(u)| = \frac{|G^F|}{q^l}$, by Theorem 8.6.14, and hence $|cl_{G^F}(u)|_p = q^{\frac{l(l-1)}{2}}$. So the result follows. □

Now suppose G is of type ${}^2A_l(q^2)$. The irreducible unipotent characters of G^F are parameterized by partitions of $l + 1$ as for A_l. Let χ_α be the character corresponding to α. Then from [9, p.465],

$$\chi_\alpha(1) = \frac{\displaystyle\prod_{k=1}^{l+1}(q^k + (-1)^{k+1}) \prod_{i,j,j<i} (q^{\lambda_i} - (-1)^{\lambda_i+\lambda_j} q^{\lambda_j})}{\displaystyle q^{L_m} \prod_i \prod_{k=1}^{\lambda_i} (q^k - (-1)^k)},$$

where L_m is as above.

Lemma 9.3.4 *Theorem 9.3.1 holds for G of type ${}^2A_l$.*

Proof. Both the p-parts of the unipotent character degrees and the regular unipotent conjugacy class sizes are the same as in the A_l case. Therefore the proof is the same as that of Lemma 9.3.3. $\square$

Now suppose G is of type B_l or C_l. Let $\lambda = (\lambda_1, \ldots, \lambda_a)$ with $0 \leqslant \lambda_1 < \ldots < \lambda_a$, and $\mu = (\mu_1, \ldots, \mu_b)$ with $0 \leqslant \mu_1 < \ldots < \mu_b$. We consider pairs (λ, μ) such that $a - b$ is odd and positive and λ_1 and μ_1 are not both 0. The rank of (λ, μ) is given by $\sum_{i=1}^{a} \lambda_i + \sum_{j=1}^{b} \mu_i - \left(\frac{a+b-1}{2}\right)^2$. Suppose G^F is of rank l, then the unipotent characters of G^F correspond to the pairs of sequences with rank l. Let $\theta_{(\lambda,\mu)}$ be the character corresponding to the pair (λ, μ).

First assume p is a good prime for G. Then from [9, p.467],

$$(\theta_{(\lambda,\mu)}(1))_p = \frac{\displaystyle\prod_{i,i',i'<i} q^{\lambda_{i'}} \prod_{j,j',j'<j} q^{\mu_{j'}} \prod_{i,j} q^{min\{\lambda_i,\mu_j\}}}{q^{M_m}}.$$

where $M_m = \binom{a+b-2}{2} + \binom{a+b-4}{2} + \ldots + \binom{3}{2}$.

Since we are only interested in the p-part of the character degrees, we may combine the pair (λ, μ) to form an l-sequence $\alpha = (\alpha_1, \ldots, \alpha_m)$, where $m = a + b$, as in Definition 7.0.3.

Lemma 9.3.5 *Let α be an l-sequence corresponding to the pair (λ, μ). Then*

$$(\theta_{(\lambda,\mu)}(1))_p = q^{A_\alpha},$$

where $A_a = \sum_{i=1}^{m-1} (m - i)\alpha_i - M_m$.

Proof. We have

$$\sum_{i,i',i'<i} \lambda_{i'} + \sum_{j,j',j'<j} \mu_{j'} + \sum_{i,j} min\{\lambda_i, \mu_j\} = \sum_{i,j,j<i} \alpha_j = \sum_{i=1}^{m-1} (m-i)\alpha_i,$$

and so the result follows. $\square$

From Lemma 7.0.8, we see that if $m = 2l+1$ we have the unique pair (λ, μ) with $\lambda = (0, 1, 2, \ldots, l)$ and $\mu = (1, 2, \ldots, l)$. It follows from Lemma 7.0.8 and Lemma 9.3.5 that $(\theta_{(\lambda,\mu)}(1))_p = q^{l^2}$ and so this is the Steinberg character. By the same lemmas, if $m < 2l+1$ we have $(\theta_{(\lambda,\mu)})_p \leqslant q^{(l-1)^2}$.

Now, since p is a good prime for G, we have from Theorem 8.6.14, $|cl_{G^F}(u)| = \frac{|G^F|}{q^l}$ so $|cl_{G^F}(u)|_p = q^{l(l-1)}$, where u is any regular unipotent element in G^F. Therefore for $a + b < 2l + 1$, $\theta_{(\lambda,\mu)}(1)$ divides $|cl_{G^F}(u)|$ as required.

The only bad prime for $G = B_l$ is $p = 2$. In this case we have

$$(\theta_{(\lambda,\mu)}(1))_p = \frac{\prod_{i,i',i'<i} q^{\lambda_{i'}} \prod_{j,j',j'<j} q^{\mu_{j'}} \prod_{i,j} q^{min\{\lambda_i,\mu_j\}}}{2^{\binom{\frac{a+b-1}{2}}{}} q^{M_m}}.$$

where $M_m = \binom{a+b-2}{2} + \binom{a+b-4}{2} + \ldots + \binom{3}{2}$.

By Theorem 8.6.14, for any regular unipotent element $u \in G^F$, we have $|cl_{G^F}(u)| = \frac{|G^F|}{2q^l}$ and hence $|cl_{G^F}(u)|_2 = \frac{q^{l(l-1)}}{2}$. Then for any unipotent character $\theta_{(\lambda,\mu)}$, except the Steinberg character, we have

$$\begin{aligned}
(\theta_{(\lambda,\mu)}(1))_2 &\leqslant q^{(l-1)^2} \\
&\leqslant q^{l(l-1)-1} \\
&\leqslant \frac{q^{l(l-1)}}{2} \\
&= |cl_{G^F}(u)|_2.
\end{aligned}$$

Therefore we have proved the following.

Lemma 9.3.6 *Theorem 9.3.1 holds for G of type B_l or C_l.*

Now suppose G is of type D_l. Let $\lambda = (\lambda_1, \ldots, \lambda_a)$ with $0 \leqslant \lambda_1 < \ldots < \lambda_a$ and $\mu = (\mu_1, \ldots, \mu_b)$ with $0 \leqslant \mu_1 < \ldots < \mu_b$. We consider pairs (λ, μ) such that $a-b$ is divisible by 4 and λ_1 and μ_1 are not both 0. The rank of (λ, μ) is $\sum_{i=1}^{a} \lambda_i + \sum_{j=1}^{b} \mu_i - \left[\left(\frac{a+b-1}{2}\right)^2\right]$. Suppose G^F is of rank l, then the unipotent characters of G^F correspond to the pairs of sequences with rank l, where (μ, λ) corresponds to the same character as (λ, μ), and if $\lambda = \mu$, there are two characters of the same degree. Let $\theta_{(\lambda,\mu)}$ be a character corresponding to the pair (λ, μ).

Let p be a good prime for G. Then we have, from [9, p.471],

$$(\theta_{(\lambda,\mu)}(1))_p = \frac{\prod\limits_{i,i',i'<i} q^{\lambda_{i'}} \prod\limits_{j,j',j'<j} q^{\mu_{j'}} \prod\limits_{i,j} q^{min\{\lambda_i,\mu_j\}}}{q^{M_m}}.$$

where $M_m = \binom{a+b-2}{2} + \binom{a+b-4}{2} + \ldots + \binom{3}{2}$.

Again we may combine the pair (λ, μ) to form an l-sequence $\alpha = (\alpha_1, \ldots, \alpha_m)$, where $m = a + b$, as in Definition 7.0.3. Lemma 9.3.5 also holds here and so we have $(\theta_{(\lambda,\mu)}(1))_p = q^{A_\alpha}$.

From Lemma 7.0.10, if $m = 2l$ we have $\lambda = (0, 1, \ldots, l-1)$ and $\mu = (1, \ldots, l-1, l)$ and so $(\theta_{(\lambda,\mu)}(1))_p = q^{l^2}$, hence this is the Steinberg character. Also from Lemma 7.0.10, if $m < 2l$ we have $(\theta_{(\lambda,\mu)}(1))_p \leqslant q^{l(l-2)}$. So, since by Theorem 8.6.14 we have $|cl_{G^F}(u)|_p = q^{l(l-2)}$ for any regular unipotent $u \in G^F$, the result follows.

Now suppose $p = 2$. Then from [9, p.471],

$$(\theta_{(\lambda,\mu)}(1))_p = \frac{\prod\limits_{i,i',i'<i} q^{\lambda_{i'}} \prod\limits_{j,j',j'<j} q^{\mu_{j'}} \prod\limits_{i,j} q^{min\{\lambda_i,\mu_j\}}}{2^c q^{M_m}}.$$

where

$$c = \begin{cases} \left[\frac{a+b-1}{2}\right] & \text{if} \lambda \neq \mu \\ a = b & \text{if} \lambda = \mu \end{cases},$$

and M_m is as before.

Let u be any regular unipotent element in G^F. Then by Theorem 8.6.14 $|cl_{G^F}(u)|_p = \frac{q^{l(l-2)}}{2} \geqslant q^{l(l-2)-1}$. Then for any unipotent character, except the Steinberg character, by Lemma 7.0.10 we have

$$(\theta_{(\lambda,\mu)})_2 \leqslant q^{(l-2)(l-1)+1} \leqslant q^{l(l-2)-1} \leqslant |cl_{G^F}(u)|_p.$$

Therefore we have proved the following lemma.

Lemma 9.3.7 *If G has type D_l then Theorem 9.3.1 holds.*

We can now complete the proof of Theorem 9.3.1.

Proof (Theorem 9.3.1). Lemmas 9.3.3, 9.3.4. 9.3.6 and 9.3.7 show the result for G of types A_l, ${}^2A_l$, B_l, C_l and D_l. For G of type ${}^2D_l$ the proof is similar to that of D_l except we have $a - b \equiv 2 \bmod 4$. Finally, if G^F is one of $G_2(q)$, ${}^3D_4(q^3)$, $F_4(q)$, $E_6(q)$, ${}^2E_6(q^2)$, $E_7(q)$, $E_8(q)$, ${}^2B_2(q)$, ${}^2G_2(q)$ or ${}^2F_4(q)$, we can check the unipotent character degrees directly from [9, Ch. 13] to see the theorem holds, including for bad primes. □

9.4 The Simple Groups

Let G be a simple algebraic group with Frobenius map F. Then

$$K = (G^F_{ad})' \cong G^F_{sc}/Z(G^F_{sc})$$

is a finite simple group, except in a few small cases. In this section we prove the following.

Theorem 9.4.1 *Let K be as above. Then for any irreducible character χ of K there exists $x \in K$ such that $\chi(1)$ divides $|cl_K(x)|$.*

In fact we prove the following corollary.

Corollary 9.4.2 *There exist two conjugacy classes in K such that the degree of any irreducible character of K divides the order one of them.*

Lemma 9.4.3 *Let x be any regular unipotent element in G_{ad}^F. Then*
$(|Z(G^{*F^*})|, |C_{G_{ad}^F}(x)|) = 1$.

Proof. By Lemma 8.6.1 $|C_{G_{ad}^F}(x)| = q^l$. The order of $|Z(G^{*F^*})| = |Z(G_{sc}^F)|$ is p-prime by [19, p.19]. □

Lemma 9.4.4 *Let $u \in G_{ad}^F$ be unipotent. Then $u \in K$.*

Proof. A unipotent element in G^F has order a power of p, see [16]. Therefore, since $|G_{ad}^F : K| = |Z(G_{sc}^F)|$ has p-prime order we have the result. □

Lemma 9.4.5 *Let x be a regular unipotent element in G^F. Then $C_K(x) = C_{G^F}(x)$.*

Proof. By Lemma 8.6.13, $C_G(x) = C_U(x)$ where U is a maximal connected unipotent subgroup of G containing x. Therefore all the elements in G which centralize x are unipotent and so the same must be true in G^F. Hence $C_{G^F}(x) \leqslant K$, and we have $C_K(x) = C_{G^F}(x)$. □

Lemma 9.4.6 *Let x be a regular unipotent element in G^F. Then $|cl_K(x)| = \frac{|cl_{G^F}(x)|}{|Z(G^{*F^*})|}$*

Proof. We have $|cl_K(x)| = \frac{|K|}{|C_K(x)|} = \frac{|G^F|}{|Z(G^{*F^*})||C_{G^F}(x)|} = \frac{|cl_{G^F}(x)|}{|Z(G^{*F^*})|}$. □

Lemma 9.4.7 *Let χ be an irreducible unipotent character of G^F which is not the Steinberg character, and let x be a regular unipotent element of K. Then $\chi(1)$ divides $|cl_K(x)|$.*

Proof. If χ is a unipotent character of G^F, then it is also a unipotent character of G^{*F^*}. So $\chi(1)$ divides $\frac{|G^{*F^*}|}{|Z(G^{*F^*})|}$ by [24, Th. 6.5, p.68]. We also have $\chi(1)$ divides $\frac{|G^F|}{|C_{G^F}(x)|}$ by Theorem 9.3.1. Therefore, since $(|Z(G^{*F^*})|, |C_{G^F}(x)|) = 1$, we have $\chi(1)$ divides $\frac{|G^F|}{|Z(G^{*F^*})||C_{G^F}(x)|} = |cl_K(x)|$ by Lemma 9.4.6. $\square$

The following lemma is from [9, p.288].

Lemma 9.4.8 *Let χ_s be a semisimple character of G^F. Let s^* be a semisimple element in the conjugacy class of the dual group determined by χ_s, as in Lemma 9.1.2. Then $\chi(1) = |G^{*F^*} : C_{G^{*F^*}}(s^*)|_{p'}$.*

Lemma 9.4.9 *Let χ be an irreducible character of G^F which is not unipotent and let x be a regular unipotent element of K. Then $\chi(1)$ divides $|cl_K(x)|$.*

Proof. By Lemma 9.1.9, we have $\chi(1) = \chi_s(1)\chi_u(1)$, where χ_s is a semisimple character of G^F and χ_u a unipotent character of $C_{G^{*F^*}}(s^*)$ for s^* a semisimple element of G^{*F^*} in the conjugacy class determined by χ_s. Then $\chi_u(1)$ divides $\frac{|C_{G^{*F^*}}(s^*)|}{|Z(C_{G^{*F^*}}(s^*))|}$ by [24, Th. 6.5, p.68], and $\chi_s(1)$ divides $\frac{|G^{*F^*}|}{|C_{G^{*F^*}}(s^*)|}$ by Lemma 9.4.8. So $\chi_s(1)\chi_u(1)$ divides $\frac{|G^{*F^*}|}{|Z(C_{G^{*F^*}}(s^*))|}$ and hence $\frac{|G^{*F^*}|}{|Z(G^{*F^*})|}$. By Lemma 9.1.10, $\chi_s(1)\chi_u(1)$ divides $|cl_{G^F}(x)|$ and so, since $(|Z(G^{*F^*})|, |C_{G^F}(x)|) = 1$, $\chi_s(1)\chi_u(1)$ divides $\frac{|G^F|}{|Z(G^{*F^*})||C_{G^F}(x)|} = |cl_K(x)|$. $\square$

Lemma 9.4.10 *Let χ be the Steinberg character of G^F_{ad}. The there exists $x \in K$ such that $\chi(1)$ divides $|cl_K(x)|$.*

Proof. By Lemma 8.7.3 there exists a regular semisimple element x in K. Then $|cl_K(x)|_p = \frac{|K|_p}{|C_K(x)|_p} = |K|_p = |G|_p$ since $|Z(G^F_{sc})|$ is p-prime. Therefore the result follows by Theorem 9.2.10. $\square$

Proof (Theorem 9.4.1). Since K is a normal subgroup of G^F_{ad}, the degree of any irreducible character of K must divide the degree of some irreducible character of G^F_{ad}. By Lemmas

9.4.7, 9.4.9 and 9.4.10 we have shown the degree of any irreducible character of G_{ad}^F divides the size of some conjugacy class of K. Therefore the result follows. $\square$

List of References

[1] M. Aschbacher. *Finite Group Theory*. Cambridge, 2000.

[2] C. Bates, D. Bundy, S. Hart, and P. Rowley. A note on commuting graphs for symmetric groups. *Electronic Journal of Combinatorics*, 16, 2009.

[3] C. Bates, D. Bundy, S. Perkins, and P. Rowley. Commuting involution graphs for finite coxeter groups. *Journal of Group Theory*, 6:461–476, 2003.

[4] C. Bates, D. Bundy, S. Perkins, and P. Rowley. Commuting involution graphs for symmetric groups. *Journal of Algebra*, 266:133–153, 2003.

[5] C. Bates, D. Bundy, S. Perkins, and P. Rowley. Commuting involution graphs in special linear groups. *Communications in Algebra*, 32:4179–4196, 2004.

[6] B. Baumeister and A. Stein. Commuting graphs of odd prime order elements in simple groups. *arXiv*, 2009.

[7] John R. Britnell and Mark Wildon. On types and classes of commuting matrices over finite fields. *J. London Math. Soc.*, 83:470–492, 2011.

[8] D. Bundy. The connectivity of commuting graphs. *Journal of Combinatorial Theory, Series A*, 113:995–1007, 2006.

[9] R. W. Carter. *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*. Wiley Classics Library, 1985.

[10] R. W. Carter. *Simple Groups of Lie Type*. Wiley Classics Library, 1989.

[11] Casolo and Dolfi. Products of primes in conjugacy class sizes and irreducible character degrees. *Israel Journal of Mathematics*, 174:403–418, 2009.

[12] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of Finite Groups*. Oxford University Press, 1984.

[13] Deligne and Lusztig. Representations of reductive groups over finite fields. *Ann. of Math*, 103:103–161, 1976.

[14] Djoković and Malzan. Imprimitive irreducible complex characters of the symmetric group. *Math. Z.*, 138:219–224, 1974.

[15] S. Dolfi. Prime factors of conjugacy class lengths and irreducible character degrees in finite soluble groups. *Journal of Algebra*, 174:749–752, 1995.

[16] Borel et al. Seminar on algebraic groups and related finite groups. 1968.

[17] John B. Fraleigh. *A First Course in Abstact Algebra*. Addison-Wesley, 1974.

[18] Meinholf Geck. *An Introduction to Algebraic Geometry and Algebraic Groups*. Oxford, 2003.

[19] Gorenstein, Lyons, and Solomon. *The Classification of the Finite Simple Groups, Number 3*. AMS, 1994.

[20] Guralnick and Maróti. Average dimension of fixed point spaces with applications. 2010.

[21] I. N. Herstein. *Topics in Algebra*. Xerox, 1964.

[22] P. N. Hoffman and J. F. Humphreys. *Projective Representations of the Symmetric Groups*. Oxford, 1992.

[23] B. Huppert. *Endliche Gruppen I*. Springer, 1967.

[24] Bertram Huppert. *Character Theory of Finite Groups*. W de G, 1998.

[25] A. Iranmanesh and A. Jafarzadeh. On the commuting graph associated with the symmetric and alternating groups. *J. Algebra Appl.*, 7:129–146, 2008.

[26] Isaacs, Keller, Meierfrankenfeld, and Moreto. Fixed point spaces, primitive character degrees and conjugacy class sizes. *Proceedings of the AMS*, 134:3123–3130, 2006.

[27] I. Martin Isaacs. *Character Theory of Finite Groups*. AMS Chelsea, 1976.

[28] Gordon James and Martin Liebeck. *Representations and Characters of Groups*. Cambridge, 2006.

[29] William M. Kantor. Linear groups containing a singer cycle. *Journal of Algebra*, 62:232–234, 1980.

[30] Kurzweil and Stellmacher. *The Theory of Finite Groups*. Springer, 2004.

[31] Serge Lang. *Algebra*. Springer, 2002.

[32] G. I. Lehrer. Rational tori, semisimple orbits and the topology of hyperplane complements. *Comment. Math. Helvetici*, 67:226–251, 1992.

[33] Gunter Malle and Donna Testerman. *Linear Algebraic Groups and Finite Groups of Lie Type*. Cambridge, 2011.

[34] J McLaughlin. Some groups generated by transvections. *Archiv Der Mathematik*, 18:364–368, 1967.

[35] J McLauglin. Some subgroups of $SL_n(F_2)$. *Illinois J. Math*, 13:108–115, 1969.

[36] Bruce E. Sagan. *The Symmetric Group*. Springer, 2001.

[37] Yoav Segev. The commuting graph of minimal nonsolvable groups. *Geometric Dedicata*, 88:55–66, 2001.

[38] D. A. Suprunenko and R. I. Tyshkevich. *Commutative Matrices*. Academic Press, 1968.