

On the Representations of the Classical Groups

A thesis submitted to the University of Manchester for the
degree of Doctor of Philosophy in the Faculty of Technology

Robert Hasson

11 December 1989

ABSTRACT

This thesis deals with some aspects of both the ordinary and modular representations of the classical groups. The main theme of the thesis is a conjecture proposed by J.L. Alperin about the number of modular characters of a finite group. A new proof of this conjecture for a class of groups containing the classical groups is presented and as a consequence of the conjecture being proved true the following have been calculated

- the p -rank of the Cartan matrix of an arbitrary parabolic subgroup of the general linear group.
- the number of ordinary irreducible characters of an arbitrary parabolic subgroup of the general linear group up to dimension three.
- the number of ordinary irreducible characters of an arbitrary parabolic subgroup of the special linear group of dimension three.

CONTENTS

1. Background	1
1.1 The Classical Groups	1
1.2 The definition of a group with a BN-pair	2
1.3 Some Representation Theory	5
1.4 Representations of groups with BN-pairs	10
2. About the Alperin conjecture	13
2.1 The original formulation	13
2.2 Some equivalent forms	14
2.3 Special cases of the Alperin conjecture	19
3. The Alperin conjecture and the classical groups	25
3.1 A proof due to M. Cabanes	25
3.2 A new proof	27
4. The Alperin conjecture and the General Linear Group	30
4.1 Ordinary representations	30
4.2 The p -rank of the Cartan Matrix	37
5. The Alperin conjecture and the Special Linear Group	56
5.1 Case one: Three does not divide $q - 1$	56
5.2 Case two: Three divides $q - 1$	67

PREFACE

This thesis is my own original work and no part has been carried out in collaboration with anyone else. No portion of this work has been submitted in support of an application for another degree or qualification of this or any other university or other institution of learning.

This work was carried out under the guidance of my supervisor G.R. Robinson without whose encouragement and advice it would not have been possible. I would also like to thank C. Parker for many helpful conversations. My thanks also go to the Open University for allowing me to use their text processor to write up this thesis without which it would not look half as good. This work was done initially with the assistance of an Science and Engineering Research Council grant and finished with the aid of a U.M.I.S.T. Teaching Assistantship.

INTRODUCTION

This thesis arises from the investigation of three beautiful formulae obtained by R. Knörr and G.R. Robinson in reference [Kn-Ro] which they prove equivalent to a conjecture of J.L. Alperin for the classical groups. To be explicit the formulae are as follows :-

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} \ell(P_J)$$

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} k(P_J)$$

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} \ell_0(P_J)$$

with the following definitions

symbol	meaning
G	a group with a split BN-pair
I	an indexing set with $ I = \text{rank of } G$
P_J	a parabolic subgroup of G
p	a prime number
k	an algebraically closed field of characteristic p
F	an algebraically closed field of characteristic 0
$\ell(G)$	the number of simple kG -modules
$k(G)$	the number of simple FG -modules
$\ell_0(G)$	the p -rank of the Cartan matrix of kG
$f_0(G)$	the number of projective simple kG -modules

The first chapter contains background material and well-known results which are used in this thesis. This background information is gathered into four sections, one on the elementary definitions of the classical groups, another on groups with split BN-pairs (such as the classical groups), a third on the results and notation from representation theory that we have used and a final section on the representations of groups with split BN-pairs.

The second chapter consists of background information specific to the Alperin conjecture. A brief discussion of the origin of the conjecture is followed by an exposition of a reformulation of the conjecture due to G.R. Robinson and R. Knörr (see reference [Kn-Ro]). The last section of this chapter contains a natural simplification of the conjecture in the case of the classical groups in the natural characteristic. This simplification is well-known but I will give a new proof of this result.

In the third chapter the Alperin conjecture is proved true for the classical groups in the natural characteristic. Firstly a proof due to M. Cabanes is described which uses the original formulation of the conjecture. Then I present a new proof of my own devising which uses the first of the above reformulations of the Alperin conjecture.

The fourth chapter starts with an investigation into the second of the above formulae in the special case of the general linear group. The numbers in this equation are very hard to calculate and for a long time were considered intractable. We calculate $k(P_J)$ for P_J being any parabolic subgroup of the three dimensional general linear group over a field of characteristic p .

The second half of the fourth chapter is an investigation into the third of the above formulae in the case of the general linear group. A formula for the p -rank of the Cartan matrix of any parabolic subgroup of the general linear group is obtained. The next part of this section contains an exposition of some work of R.M. Bryant which gives a much tidier formula for the above in the special case of the parabolic subgroup being the whole of the general linear group. Finally, the last part of this section is an extension of this, in the spirit of the above, to obtain a neater formula for certain parabolic subgroups of the general linear group.

The fifth chapter contains another example of the usefulness of the Alperin conjecture in finding the number of ordinary irreducible characters of the parabolic subgroups of the classical groups. In this chapter the number of ordinary irreducible characters of any parabolic subgroup of the three dimensional special linear group are calculated. This chapter is also split into two sections in a way which mirrors a natural division of the problem.

1. BACKGROUND

This chapter is included to enable mathematicians that are not specialist group theorists to read this thesis. It contains some notation, definitions and elementary results that are standard¹ which the more experienced reader can omit. Theorems will be quite freely quoted without proof as there are so many books covering this material.

1.1 The Classical Groups

These groups are so named because they first appeared together in L.E. Dickson's 1901 book on group theory, and from which were derived most of the then known non-abelian finite simple groups (all in fact apart from the Mathieu groups and alternating groups). Today we still group them together because of the work of Chevalley who gave a unified description of all of these groups simultaneously. A more axiomatic unified description will be given later by means of BN-pairs which was first derived by Tits (see reference [Ti]). Firstly though we will give the original definitions of the groups involved, which are :-

The General Linear Groups These are defined to be the groups of all non-singular linear transformations of a vector space, V , of dimension n over a field with q elements. In a familiar way this group is usually identified with the group of all non-singular matrices of the appropriate dimension. Throughout this thesis I will denote the group of non-singular matrices of dimension n over a field with q elements as $GL_n(q)$.

The Special Linear Groups Contained within the General Linear Group is a group known as the Special Linear Group which consists of all of the elements of the general linear group which have determinant one, which I will denote by $SL_n(q)$.

The Orthogonal Groups This group consists of the non-singular transformations which preserve a non-singular orthogonal form (i.e. a non-singular symmetric bilinear form).

¹ the standard texts are given as references for further reading

The Symplectic Groups This group consists of the non-singular transformations which preserve a non-singular symplectic form (i.e. a non-singular alternating bilinear form). That is a non-singular bilinear form $(,)$ with the following property :-

$$(x, x) = 0 \quad \forall x \in V$$

The Unitary Groups This group consists of the non-singular transformations which preserve a non-singular unitary form. That is a non-singular bilinear form $(,)$ with the following property :-

$$(x, y) = \overline{(y, x)} \quad \forall x, y \in V$$

where $\bar{}$ is an automorphism of $GF(q)$ of order 2.

1.2 The definition of a group with a BN-pair

As mentioned above all of the classical groups obey an axiom system known as the axioms for a BN-pair . This gives a uniform description of the classical groups and it allows us to prove theorems about these similar groups without resorting to a case-by-case analysis . The axiom system is more general than the classical groups and many other interesting groups have BN-pairs (e.g. some sporadic simple groups).

The axioms have a geometric interpretation which serves as the motivation and intuition of workers in this field . However I will only appeal to the axioms algebraically and shall merely use the fact that the classical groups satisfy these axioms and so I will omit the geometry and instead refer the interested reader to chapter 8 of reference [Car1] and reference [Ti].

Definition

A group G is said to have a BN-pair if it has two subgroups B, N such that the following hold :-

1. $G = \langle B, N \rangle$
2. $H := B \cap N$ is a normal subgroup of N
3. $W := N/H$ is generated by $\{s_i \mid i \in I\}$ with $s_i^2 = 1$ (the cardinality of I is called the rank of the BN-pair).

4. If $n_i \in N$ maps to $s_i \in W$ under the natural homomorphism $\pi : N \rightarrow W$ then $n_i B n_i \neq B$.
5. $\forall n \in N$ and $\forall i \in I$ we have $n_i B n \subset B n_i n B \cup B n B$.

The BN-pair is said to be split and of characteristic p if :-

- $B = UH$ with U a normal p -subgroup of B , and H is an abelian group of order prime to p

The BN-pair is said to be of restricted type if :-

- The $\{n_i \mid i \in I\}$ can be chosen such that $n_i \in U_i U_i^- U_i$ where $U_i = U \cap s_i U^- s_i$ with $U^- = w_0 U w_0$ and $U_i^- = w_0 U_i w_0$ where w_0 is the unique longest word in the s_i (which always exists).

As mentioned before, all of the classical groups have a split BN-pair of restricted type. We shall now give a few more definitions which are useful in this field after a result that serves as motivation.

Theorem 1.1 (Bruhat decomposition): *If G is as above then $G = BNB$ and W is isomorphic to a set of double coset representatives of (B, B) in G .*

Definitions

- Define $N_J = \langle n_i \mid i \in J \rangle$ where $J \subseteq I$.
- Define $P_J = B N_J B$ where $J \subseteq I$. Then P_J is called a *parabolic subgroup* of G . Note that this is a subgroup by axiom 5 and that by the Bruhat decomposition $P_I = G$.
- If G has a split BN-pair then P_J has a decomposition analogous to that of B (called the Levi decomposition). We write $P_J = L_J U_J$ where $U_J = \langle U_i \rangle_{i \in I-J}$ is a normal p -subgroup and L_J is a subgroup of P_J such that $L_J \cap U_J = \{1\}$ and $P_J = U_J L_J$. A useful fact about this decomposition is that $U_J = O_p(P_J)$ (meaning that U_J is the largest normal p -subgroup of P_J). The group L_J has the property that it has a split BN-pair of rank $|J|$.

To illustrate this definition we give the following example

Example

The general linear group of linear transformations of a vector of dimension n over the field of q elements (i.e. $GL_n(q)$) has a BN-pair with the following definitions :-

$$B = \left\{ \left(\begin{array}{ccc} \alpha_{11} & \cdots & \alpha_{1n} \\ 0 & \ddots & \vdots \\ 0 & 0 & \alpha_{nn} \end{array} \right) : \alpha_{ij} \in GF(q), \prod_{i=1}^n \alpha_{ii} \neq 0 \right\}$$

N = the group of all matrices with one non-zero entry in each row and column

$$H = \left\{ \left(\begin{array}{ccc} \alpha_{11} & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \alpha_{nn} \end{array} \right) : \alpha_{ii} \neq 0, \alpha_{ii} \in GF(q) \right\}$$

W = the group of all $n \times n$ permutation matrices
 $\cong S_n$ (the Symmetric group on n -letters)

To illustrate what the subgroups P_J and L_J look like I will use the case $J = \{1, 4, 5, \dots, n\}$ as an example. The underlying set of P_J consists of all the matrices

$$\left(\begin{array}{cccccc} \alpha_{11} & \alpha_{12} & \alpha_{13} & \alpha_{14} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \alpha_{24} & \cdots & \alpha_{2n} \\ 0 & 0 & \alpha_{33} & \alpha_{34} & \cdots & \alpha_{3n} \\ 0 & 0 & 0 & \alpha_{44} & \cdots & \alpha_{4n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \alpha_{n4} & \cdots & \alpha_{nn} \end{array} \right)$$

with $\alpha_{ij} \in GF(q) \forall i, j \in \{1, 2, \dots, n\}$ and the determinant of the matrix non-zero. The underlying set of the corresponding L_J will consist of the matrices

$$\left(\begin{array}{cccccc} \alpha_{11} & \alpha_{12} & 0 & 0 & \cdots & 0 \\ \alpha_{21} & \alpha_{22} & 0 & 0 & \cdots & 0 \\ 0 & 0 & \alpha_{33} & 0 & \cdots & 0 \\ 0 & 0 & 0 & \alpha_{44} & \cdots & \alpha_{4n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \alpha_{n4} & \cdots & \alpha_{nn} \end{array} \right)$$

with $\alpha_{ij} \in GF(q) \forall i, j \in \{1, 2, \dots, n\}$ and the determinant of the matrix non-zero.

Notation

If G is a group with a split BN-pair then the above notation (B, N, H, I, P_J etc.) will be used without an explicit quotation, it being understood that they are as in the definition.

1.3 Some Representation Theory

Having said something about the groups we are going to study we would now like to outline some of the main results from the representation theory of finite groups that we shall be using. If you are already familiar with some representation theory then maybe you would like to skip to the end of this chapter where a selection of results specifically about the representations of groups with split BN-pairs are collected.

First of all we fix some notation that will hold throughout this thesis.

Notation

- G is always a *finite* group.
- H is always a subgroup of G .
- p is a fixed prime number.
- q is a fixed power of p .
- Q is always a p -subgroup of G
- R is a complete discrete valuation ring with field of fractions F and a unique maximal ideal with residue field k an algebraically closed field of characteristic p (i.e. (F, R, k) is a p -modular system) .

And we give the the fundamental definitions of representation theory :-

Definitions

- A kG -module M is a finite dimensional vector space over k together with a bilinear map $kG \times M \rightarrow M$ given by $(g, m) \mapsto g.m$ such that :-

$$g.(h.m) = (gh).m \quad \forall g, h \in G, m \in M$$

The group G is said to act on the vector space M and the linear map in this definition is called the G -action.

- A submodule N of a kG -module M is a subspace of M that is a kG -module with the restricted map $G \times N \rightarrow N$.
- A kG -module with no proper non-zero submodules is called *simple*

Clearly, if a module is simple then any module isomorphic to it is simple, and so the number of simple modules is not a useful quantity. So we will adopt the common convention that the phrase ‘number of simple modules’ will implicitly mean ‘number of non-isomorphic simple modules’.

Now we continue to give the basic definitions

Definitions

- A kG -module M is decomposable if there exists submodules M_1, M_2 of M such that :

$$M = M_1 \oplus M_2 \text{ (as vector spaces)}$$

This decomposition is said to be proper if $M_i \neq 0$ ($i = 1, 2$). We often write $M_1 \mid M$ as shorthand for the statement M_1 is a direct summand of M .

- A kG -module that does not have a proper decomposition is called *indecomposable*.

The notion of an FG -module is defined similarly. Representation theory is the study of these modules and we will now recall a few of the highlights of the theory.

Theorem 1.2 (R. Brauer): *The number of simple kG -modules is equal to the number of p -regular conjugacy classes of G .*

Corollary 1.3: *The number of simple kG -modules is finite.*

A similar theorem states that the number of non-isomorphic simple FG -modules is equal to the number of conjugacy classes G . We will denote the number of non-isomorphic simple kG -modules (resp. FG -modules) by $\ell(G)$ (resp. $k(G)$). We will now give a simple and useful lemma from group theory which enables us to calculate the number of conjugacy classes of a group in the examples contained in the later chapters.

Lemma 1.4: *Let π be any set of prime numbers and let π' be the set of all prime numbers that are not in π . Let G be any finite group. If an element $g \in G$ is of order m where all of the prime factors of m are in π then g is said to be a π -element. We can similarly define π' -elements.*

With these definitions the following formula holds

$$k(G) = \sum_{(g)} \#(\text{classes of } \pi\text{-elements of } C_G(g))$$

where (g) ranges over all the conjugacy classes of π' -elements of G .

Now we give a theorem which is very reminiscent of the fundamental theorem of arithmetic :-

Theorem 1.5 (Krull–Schmidt): *Let M_i ($i = 1, \dots, m$), N_j ($j = 1, \dots, n$) be indecomposable kG -modules and suppose that*

$$M_1 \oplus M_2 \oplus \dots \oplus M_m \cong N_1 \oplus N_2 \oplus \dots \oplus N_n$$

then $m = n$ and there exists a permutation π such that

$$M_i \cong N_{\pi(i)} \quad i = 1, \dots, n$$

Now we will focus on some results which make the study of the modular representations of G diverge from the theory of the ordinary representations of G . The definition of a vertex is the work of J.A. Green (see theorem 4 of reference [Gr2]).

Definitions

- If H is a subgroup of G and M is a kG -module then we can define the *restriction* of M to H (written M_H) to be the kH -module with underlying vector space M together with the H -action inherited from the G -action.
- If $H \leq G$ and N is a kH -module then we can define the *induced* module of N from H to G (written N^G) to be $kG \otimes_{kH} N$
- A kG -module M is said to be H -projective if there exist a kH -module N such that M is isomorphic to a direct summand of the module N induced from H to G . A kG -module will be called projective if it is $\langle 1_G \rangle$ -projective (this is not the usual definition, but is a consequence of a theorem of J.A. Green).
- The number of isomorphism types of projective simple kG -modules will be denoted by $f_0(G)$.

- If M is an indecomposable kG -module then the smallest H such that M is H -projective is called a vertex of M . J.A. Green proved that the vertices of M form a single conjugacy class of p -subgroups of G and so we will talk of *the* vertex of M (it being understood that we are only talking of it being unique up to G -conjugacy).

We now describe another invariant of a finite group which will be useful in later chapters. The following theorem will serve as motivation for the definition.

Theorem 1.6: *There exists a one-one correspondence between the projective indecomposable kG -modules and the simple kG -modules as follows :-*

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{isomorphism types of projective} \\ \text{indecomposable } kG\text{-modules} \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{l} \text{isomorphism types of} \\ \text{simple } kG\text{-modules} \end{array} \right\} \\ P & \longmapsto & Hd(P) \end{array}$$

where $Hd(P)$ (the head of P) is defined to be the largest quotient that is a direct sum of simple kG -modules.

Definitions

- If $\{P_1, P_2, \dots, P_m\}$ is a complete set of projective indecomposable kG -modules and $E_i = Hd(P_i)$ is the corresponding simple module then we can define the Cartan Invariant c_{ij} to be the multiplicity as a composition factor of E_j in P_i (see reference [La], page 12).
- The matrix $C = (c_{ij})$ is called the Cartan Matrix of kG .
- Since C is a matrix with integral entries we can consider the image of C in the ring of matrices over $GF(p)$. The rank of the resulting matrix is called the p -rank of C and will be denoted by $\ell_0(G)$.

To calculate this invariant we will never refer directly to the definition but we will use the following theorem :-

Theorem 1.7 (R. Brauer): *The p -rank of the Cartan matrix of G , $\ell_0(G)$, is equal to the number of conjugacy classes of p -regular elements such that p does not divide the order of the centralizer of the element in G .*

The following is a (very brief) description of a way of partitioning the simple modules of G into classes called blocks. There are many different ways of approaching this to give the same decomposition, we will describe

a way using module-theoretic terms which is due to J.L. Alperin and D.W. Burry (see reference [Al-Bu]).

However, there seems at the moment to be no best way of defining a block with all the approaches having their own individual merits. There are a number of texts in this field which might be consulted for other approaches (see references [Do] , [Cu-Re] , [Is] , [La]).

Definitions

- Regard the group algebra kG as a $k(G \times G)$ -module with action defined by :-

$$(g_1, g_2).a = g_1 a g_2^{-1} \quad \forall g_1, g_2 \in G, \forall a \in kG$$

and extended linearly. Express this as a direct sum of indecomposable $k(G \times G)$ -modules, say

$$kG \cong B_1 \oplus B_2 \oplus \cdots \oplus B_n$$

Then by the Krull-Schmidt theorem the B_i are unique up to isomorphism and these will be called the *blocks* of kG .

- The vertex of a block B_i is equal to $\{(d, d) \mid d \in D\} \leq G \times G$ for some p -subgroup D of G . This D is called the defect group of the block B_i . Since D is a p -group $|D| = p^d$ for some integer d , which is called the defect of B_i .

The decomposition of the module kG into indecomposable submodules is the same as the decomposition of the *ring* kG into indecomposable 2-sided ideals. Corresponding to this there is a decomposition of the identity element 1 of kG into central primitive idempotents say :

$$1 = e_1 + e_2 + \cdots + e_n$$

These central primitive idempotents are called the block idempotents and are in one-to-one correspondence with the blocks of kG .

The reason that the block idempotents have been mentioned is simply to define the idea that we mentioned earlier that the simple modules are partitioned into blocks. With this in mind we make the following definition:

Definition

- If B_i is a block and e_i is the corresponding block idempotent then the kG -module M is said to belong to the block B_i (written $M \in B_i$) if $e_i M \neq 0$.

If S is a simple kG -module then obviously it can only belong to one and only one block, so this does in fact partition the simple modules. The number of simple kG -modules in a block B will be written as $\ell(B)$. By lifting the idempotents the blocks of kG can be seen to partition the simple FG -modules and the number of simple FG -modules in the block B will be written as $k(B)$.

We now define one of the most useful tools in block theory; the Brauer correspondence.

Definitions

- If $H \leq G$ and b is a block of kH then we write $b^G = B$ if B is the unique block of kG with $b \mid B_{H \times H}$. This mapping of blocks is not always defined, but if there exists a p -subgroup Q such that $QC_G(Q) \leq H \leq G$ then it is defined. The map $b \mapsto b^G$ is called the Brauer correspondence.
- Let Q be a p -subgroup of the group G . Then we write $f_0^{(B)}(N_G(Q)/Q)$ to denote the number of Q -projective simple $kN_G(Q)$ -modules in the blocks of $kN_G(Q)$ that are the Brauer correspondents of the block B of kG . This notation arises from the fact that the Q -projective simple $kN_G(Q)$ -modules are in one-to-one correspondence with the projective simple $kN_G(Q)/Q$ -modules.

1.4 Representations of groups with BN-pairs

In this next section I collect together some results about the representation theory of groups with split BN-pairs. This is fairly well known and we shall refer the interested reader to references [Cu] (theorem 4.1) and [Ri] for the proofs of the results.

Definition

- Let G be a group with a split BN-pair of characteristic p of rank n . Let M be a kG -module. Then $0 \neq m \in M$ is called a *weight element* of weight $(\chi, \mu_1, \mu_2, \dots, \mu_n)$ where $\chi : B \rightarrow k^*$ is a homomorphism and $\mu_i \in k$ if

$$bm = \chi(b)m \quad \forall b \in B$$

and

$$\left(\sum_{u \in U_i} u \right) s_i m = \mu_i m \quad 1 \leq i \leq n$$

Theorem 1.8 (F. Richen, 1969): *If G is as in the above definition then*

1. *Every kG -module has a weight element.*
2. *If two simple kG -modules contain weight elements of the same weight then they are isomorphic.*
3. *There is a one-to-one correspondence between the simple kG -modules and the set of weights.*

This theorem goes together with the following one after we make the following definition.

Definition

- For a group with a split BN-pair we make the following definition :-

$$H_i = H \cap \langle U_i, U_i^- \rangle$$

Theorem 1.9 (F. Richen, 1969): *If G is as above with the extra condition of being of restricted type and $(\chi, \mu_1, \mu_2, \dots, \mu_n)$ is a weight then :-*

- *If the weight corresponds to a simple kG -module then*

$$\mu_i = 0 \quad \text{or} \quad -1$$

and moreover

$$(\chi|_{H_i} \neq 1) \Rightarrow \mu_i = 0$$

- *If $\mu_i = 0$ or -1 and $\mu_i = 0$ whenever $\chi|_{H_i} \neq 1$ then there is a simple kG -module corresponding to this weight.*

Corollary 1.10: *The number of simple kG -modules is*

$$\sum_{J \subseteq \{1, \dots, n\}} \frac{|H|}{|H_J|}$$

where $H_J = \langle H_i : i \in J \rangle$.

If G is one of the classical groups other than general linear group (e.g. $SL_n(q)$) then $H = \prod_i H_i$ (direct product) and $|H_i| = q - 1$ (where q is the cardinality of the field over which G is defined). So we can calculate the number of simple kG -modules to be q^n .

From the above we can calculate the number of simple $kGL_n(q)$ -modules and the number of simple $kSL_n(q)$ -modules. This gives us the following results (remembering that $SL_n(q), GL_n(q)$ have BN-pairs of rank $n - 1$).

$$\begin{aligned}\ell(SL_n(q)) &= q^{n-1} \\ \ell(GL_n(q)) &= (q - 1) \times q^{n-1}\end{aligned}$$

Theorem 1.11 (C.W. Curtis, 1970): *Let G be as above and let M be a simple kG -module. Then M contains a unique line stabilised by B . Let P_J be the full stabilizer of the line. Then P_J is a parabolic subgroup for some $J \subseteq \{1, \dots, n\}$ and M determines P_J and the homomorphism $\chi : P_J \rightarrow k^*$ (afforded by the line) uniquely.*

Conversely if two simple kG -modules determine the same parabolic subgroup and the same homomorphism χ then they must be isomorphic.

2. ABOUT THE ALPERIN CONJECTURE

This chapter concerns itself with a conjecture of J.L. Alperin about the representation theory of finite groups. The first section gives an outline of the conjecture and why it was thought to be true originally. The next section consists of an exposition of the work of G.R. Robinson and R. Knörr (see [Kn-Ro] and [Ro]) which gives some equivalent formulations of the conjecture. The last section gives outlines of some of the proofs of the conjecture for various classes of finite groups, these are due to several people and attributions are given locally.

2.1 The original formulation

The original formulation is (or course) due to J.L. Alperin and comes from an attempt to generalise some of the results in the representation theory of groups with split BN-pairs to the context of all finite groups. The concept that is most useful in the former is that of a weight (as defined in the previous chapter) and it would be useful to generalize this. Theorem 1.11 is the most useful in this respect as it gives a correspondence between the simple kG -modules and the set of pairs of parabolic subgroups and homomorphisms of them into k . So first we want to generalize the concept of parabolic subgroup to all finite groups, to which the following theorem provides a hint.

Theorem 2.1 (Borel – Tits): *If P is a parabolic subgroup of a group, G , with a split BN-pair then $P = N_G(O_p(P))$. Moreover, if Q is a subgroup of G satisfying $Q = O_p(N_G(Q))$ then Q is conjugate to a parabolic subgroup P_J of G (for some $J \subseteq I$).*

This theorem was originally formulated in the context of the overlying algebraic groups (see reference [Bo-Ti]), but can be proved by just using the properties of the finite groups (see R.W. Carter's book [Car1]). This theorem suggests that we use subgroups with this property as a substitute for the parabolic subgroups of a group with a split BN-pair. The homomorphisms

that arise in the theorem 1.11 are of a particular type and correspond to a special to a special type of module in this new context. This leads us to the following definition :-

Definition

- A weight for a finite group G is defined to be a pair (Q, b) where Q is a p -subgroup of G and b is a projective simple $k(\frac{N_G(Q)}{Q})$ -module (note that this implies that $Q = O_p(N_G(Q))$).

Having taken this into account the Alperin conjecture is not that there is a canonical correspondence

$$\left\{ \begin{array}{l} \text{isomorphism types of} \\ \text{simple } kG\text{-modules} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{conjugacy classes of} \\ \text{weights} \end{array} \right\}$$

as is the case for the General Linear Group but that there are the same number of objects on each side, so we arrive at a conjecture that looks like :-

$$\ell(G) = \sum_{(Q)} f_0 \left(\frac{N_G(Q)}{Q} \right) \quad (2.1)$$

where Q ranges over a set of representatives of the conjugacy classes of p -subgroups of G .

The conjecture is often put in a stronger form by linking it with the block structure of the group G . This stronger form looks like :-

$$\ell(B) = \sum_{(Q)} f_0^{(B)} \left(\frac{N_G(Q)}{Q} \right) \quad (2.2)$$

where Q ranges over a set of representatives of the conjugacy classes of p -subgroups of G .

2.2 Some equivalent forms

Before we describe some equivalent forms of the Alperin conjecture we first have to define a combinatorial object which can be attached to a finite group. This object is beginning to be called the Brown complex after K. Brown who used it to prove a generalisation of the Sylow theorems (see reference [Br]).

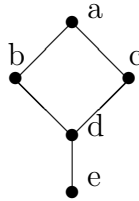
Definition

- Consider the poset of all p -subgroups, Q_i , of G ordered by set inclusion. Then form the chains of p -subgroups $Q_0 < Q_1 < \dots < Q_n$ (with $Q_0 = \langle 1_G \rangle$ by convention) ordered by subgroup inclusion to get the Brown complex, \mathcal{C} . The length of the above chain is defined to be n . Note that there is a natural G -action on this poset which is induced by the conjugation action of G on p -subgroups of G .

The reason it is called the Brown complex rather than the Brown poset is because it is usually thought of as a complex via the standard construction illustrated below by the following example.

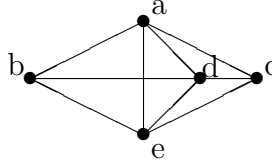
Example

Consider a poset defined by the following diagram (where a line joining two nodes is used to represent that the lower node is less than or equal to the higher node) :-



From this we are going to derive a simplicial complex, so the question to ask is what are the simplices. The 0-simplices (vertices) of the complex will correspond to the members of the poset, so in our case we will have five vertices which will be labelled a, b, c, d and e . The 1-simplices (edges) will correspond to the 1-chains in the poset (i.e. pairs of elements (x, y) with $x \leq y$ with $x \neq y$). So in our case there will be nine edges corresponding to $e \leq d, e \leq c, e \leq b, e \leq a, d \leq c, d \leq b, d \leq a, c \leq a$ and $b \leq a$. In general the n -simplices will correspond to the n -chains of the poset.

The other property that a simplicial complex has is some sort of face relation which in our case will be given by the subchains. As an example $e \leq d \leq b \leq a$ is a 3-chain which contains the following 2-chains as faces $d \leq b \leq a, e \leq b \leq a, e \leq d \leq a$ and $e \leq d \leq b$. Putting this all together we get the following diagram which consists of two tetrahedrons joined together in the common face ade .



In order to summarize the construction in the above example we restate that a typical $(n - 1)$ -simplex of the Brown complex corresponds to a chain of length n , which has the form :-

$$Q_0 < Q_1 < Q_2 < \dots < Q_n$$

and has the chains obtained by omitting one or more of the Q_i 's as its faces (not omitting Q_0 as doing this would not give a chain in the Brown complex). Before we prove a theorem of G. Robinson (which appears as the first theorem in reference [Ro]), we will define another simplicial complex which is very closely related to \mathcal{C} .

Definition

- Let \mathcal{N} be the subcomplex of \mathcal{C} which consists of all of the simplices

$$Q_0 < Q_1 < Q_2 < \dots < Q_n$$

with

$$Q_i \triangleleft Q_n \quad \forall i \in \{1, 2, \dots, n - 1\}$$

Two more definitions are needed before we can go ahead and prove the reformulation of the Alperin conjecture.

Definitions

- Let $C = Q_0 < Q_1 < \dots < Q_n$ be a simplex of \mathcal{C} . Note that the chain stabiliser of C (written G_C) can be written as

$$G_C = \bigcap_{i=0}^n N_G(Q_i)$$

because we insisted that all chains begin with $Q_0 = \{1\}$ and so we have avoided an intersection indexed by the empty set here.

- If \mathcal{C} is a simplicial complex on which the group G acts then the simplicial complex \mathcal{C}/G is defined to be the set obtained by taking one representative out of each orbit of \mathcal{C} under the action of G .

We prefix the proof of the theorem with a lemma which is proved as proposition 3.3 in reference [Kn-Ro].

Lemma 2.2:
$$\sum_{C \in \mathcal{C}/G} (-1)^{|C|} \ell(G_C) = \sum_{N \in \mathcal{N}/G} (-1)^{|N|} \ell(G_N)$$

The following theorem is a quotation from reference [Ro] where it constitutes the first theorem.

Theorem 2.3: *The following are equivalent (in the sense that if one holds for all finite groups, G , then so does the other)*

1. *The Alperin conjecture is true i.e. equation 2.1 holds.*
2. *If \mathcal{N} is the simplicial complex defined above then the following holds*

$$f_0(G) = \sum_{C \in \mathcal{N}/G} (-1)^{|C|} \ell(G_C) \quad (2.3)$$

Proof

- 1) \Rightarrow 2) Suppose that the Alperin conjecture holds for all finite groups. We prove that the second formula is true by induction on $|G|_p$ (the p -part of the order of G).

Initial step ($|G|_p = 1$) : In this case the group G is a p' -group and so 2) is trivially true.

Induction step ($|G|_p = p^n$) : Let Q be a non-trivial p -subgroup of G .

We wish to calculate the contribution to the formula

$$\sum_{C \in \mathcal{N}/G} (-1)^{|C|} \ell(G_C)$$

coming from orbits of chains starting with conjugates of Q . In order to do this we note that we can pair off the G -orbits chains of length $n + 1$

$$Q_0 < Q < Q_1 < Q_2 < \dots < Q_n$$

of p -subgroups of G in the simplicial complex \mathcal{N} with the $N_G(Q)$ -orbits of chains

$$\bar{Q}_0 < \bar{Q}_1 < \bar{Q}_2 < \dots < \bar{Q}_n$$

of p -subgroups of $N_G(Q)/Q$ in \mathcal{D} , the complex corresponding to \mathcal{N} , of length n (where $\bar{}$ denotes images in $N_G(Q)/Q$). Hence the contribution to the above formula from chains beginning with conjugates of Q is

$$\sum_{D \in \mathcal{D}/N_G(Q)} (-1)^{|D|+1} \ell(\overline{N_G(Q)}_D)$$

where \mathcal{D} is the simplicial complex corresponding to \mathcal{N} in the group $N_G(Q)/Q$.

By the induction hypothesis applied to $N_G(Q)/Q$ (a group with smaller p -part since Q is non-trivial) we have that the above is equal to $-f_0(N_G(Q)/Q)$.

Hence when we sum over all the representatives of the conjugacy classes of non-trivial p -subgroups of G (and then add in the term coming from the chain consisting of Q_0 only) we get

$$\sum_{C \in \mathcal{N}/G} (-1)^{|C|} \ell(G_C) = \ell(G) - \sum_{(Q)} f_0(N_G(Q)/Q) \quad (2.4)$$

where Q ranges over a set of representatives of the conjugacy classes of the *non-identity* p -subgroups of G .

But we have, by assumption, that the Alperin conjecture holds for all finite groups G i.e.

$$\ell(G) = \sum_{(Q)} f_0(N_G(Q)/Q)$$

where Q ranges over a set of representatives of the conjugacy classes of *all* p -subgroups of G . So the result follows by combining the last two equations.

- 2) \Rightarrow 1) The proof in this direction is proved in a very similar way by induction on the p -part of the order of G . The initial step is as trivial as above and the induction step is proved by combining the assumption that 2) holds with equation 2.4. \square

Corollary 2.4: *The Alperin conjecture (i.e. equation 2.1) holds true for all finite groups if and only if the following formula holds true for all finite groups.*

$$f_0(G) = \sum_{C \in \mathcal{C}/G} (-1)^{|C|} \ell(G_C)$$

Proof

Simply combine the last theorem with the previous lemma. □

Also it is shown in reference [Kn-Ro] that the conjecture is equivalent to the following :-

$$f_0(G) = \sum_{C \in \mathcal{C}/G} (-1)^{|C|} k(G_C)$$

$$f_0(G) = \sum_{C \in \mathcal{C}/G} (-1)^{|C|} \ell_0(G_C)$$

This is done by proving that a certain module is virtually projective and then counting the number of virtual fixed points by two different methods.

2.3 Special cases of the Alperin conjecture

Symmetric group

The proof for this case was announced by J.L. Alperin in August 1984, and basically consists of forming a precise description of the groups Q which satisfy $Q = O_p(N_G(Q))$. Having done this then the classification of the characters of S_n of Osima can be use to count the objects on either side of the equation. It must be emphasized that this proof is just a counting argument and does not give a canonical correspondence as is the case for most of the other classes of groups for which the Alperin conjecture is known to be true.

General Linear Group in non-natural characteristic

The proof in this case is very similar to that of the symmetric group and was proved by P. Fong (see proposition 5' in reference [Fo]).

p-Solvable groups

The proof for this case actually predates the conjecture and is implicit in a paper of Okuyama (see the first theorem in reference [Ok]). The proof constructs a canonical correspondence between the simple kG -modules of vertex Q and the simple $kN_G(Q)$ -modules of vertex Q for every p -subgroup $Q \leq G$. The result needs a deep theorem of E.C. Dade on groups of the form $G = O_{p'}(G)N_G(P)$ where P is a p -group.

The classical groups in the natural characteristic

In this case, which I am going to study in the later chapters, there are some special reductions that can be made by linking the conjecture more closely with the structure of the group. This is done by using theorem 2.1 to identify the Brown complex with a simplicial complex known as the Tits building which we will now define.

Definition

- Consider the poset consisting of all of the parabolic subgroups of G ordered by reverse set inclusion. By the standard method outlined above we can construct a simplicial complex \mathcal{T} from this poset. This simplicial complex is often called the Tits building. Note that G has a natural action on \mathcal{T} which is induced by the conjugation action of G on its subgroups.

In order to simplify the wording in this section I will make a local definition and say that two posets are equivalent if all of the alternating sums that we are interested in are equal for these posets. To be more precise we make the following definition :

Definition

- If \mathcal{C}, \mathcal{D} are two simplicial complexes on which there is a G -action then they will be called equivalent if

$$\sum_{C \in \mathcal{C}/G} (-1)^{|C|} f(G_C) = \sum_{D \in \mathcal{D}/G} (-1)^{|D|} f(G_D)$$

where $f : \{\text{subgroups of } G\} \rightarrow A$ is any function that is constant on G -conjugacy classes of subgroups of G and A is any abelian group.

The proof that the Brown complex and the Tits building are $GL_n(q)$ -homotopy equivalent is a standard result (for example see [Bo]) but as we only need the special case of the complexes being equivalent in the above sense, we will prove this much simpler theorem. Before we can do this we need to prove a few combinatorial lemmas :-

Lemma 2.5: *Let I_n be the set $\{1, 2, \dots, n\}$.*

Let $N_{r,n}$ be the number of chains of subsets of I_n which are of length r .

Note that a typical chain contributing to $N_{r,s}$ is

$$\emptyset \subset J_1 \subset J_2 \subset \dots \subset J_{r-1} \subset I_n$$

Then the following reduction formula holds

$$N_{r,n} = r(N_{r,n-1} + N_{r-1,n-1})$$

Proof

Consider what happens when the element n is removed from the set I_n to yield the set I_{n-1} . The resulting chain may have two successive sets equal (in the case where they only differed by the element n) and so after removing a possible redundancy we will get either a chain of length r or $r - 1$.

Now consider a chain of length r of subsets of I_{n-1} , for example

$$\emptyset \subset J_1 \subset J_2 \subset \dots \subset J_{r-1} \subset I_{n-1}$$

How many ways can we add in the element n into this chain to yield an chain of subsets of I_n ? There are r ways of doing this since n could appear for the first time in any of the sets $J_1, J_2, \dots, J_{r-1}, I_n$.

Similarly if we start with a chain of length $r - 1$, e.g.

$$\emptyset \subset J_1 \subset J_2 \subset \dots \subset J_{r-2} \subset I_{n-1}$$

How many ways are there of getting a chain of length r ? Any of the r sets $\emptyset, J_1, \dots, J_{r-2}, I_{n-1}$ could be duplicated and n added to the second copy (and all subsequent sets) so this gives r choices in all.

The required formula now follows by combining the results of the last two paragraphs. □

Lemma 2.6: *Let I be the set $\{1, 2, \dots, n\}$.*

Let \mathcal{C} be the set of all chains of subsets of I which start with \emptyset and end with I e.g.

$$\emptyset \subset J_1 \subset J_2 \subset \dots \subset J_{r-1} \subset I$$

Then the following formula is true

$$\sum_{\mathcal{C} \in \mathcal{C}} (-1)^{|\mathcal{C}|} = (-1)^n$$

Proof

The above formula can be rewritten using the notation $N_{r,n}$ of the previous lemma to obtain the formula

$$\sum_{r=1}^n (-1)^r N_{r,n} = (-1)^n$$

by observing that $N_{r,n}$ is simply the number of chains of length r . The proof now proceeds by induction on n , the cardinality of I .

Initial step An easy calculation shows that for $n=1$ we have $\mathcal{C} = \{\emptyset \subset I\}$ and so both sides evaluate to -1 .

Induction step Suppose that the theorem is true for $n = k - 1$, that is the following holds

$$\sum_{r=1}^{k-1} (-1)^r N_{r,k-1} = (-1)^{k-1}$$

We wish to prove that the formula holds for $n = k$, so we expand the left hand side of the formula in this case :-

$$\begin{aligned} \text{L.H.S.} &= \sum_{r=1}^k (-1)^r N_{r,k} \\ &= \sum_{r=1}^k (-1)^r r [N_{r,k-1} + N_{r-1,k-1}] \\ &\quad \text{by the previous lemma} \\ &= \sum_{r=1}^k (-1)^r r N_{r,k-1} + \sum_{r=1}^k (-1)^r r N_{r-1,k-1} \\ &= \sum_{r=1}^k (-1)^r r N_{r,k-1} - \sum_{R=0}^{k-1} (-1)^R (R+1) N_{R,k-1} \\ &\quad \text{by substituting } R = r - 1 \\ &= -(-1)^0 \times 1 \times N_{0,k-1} + \sum_{r=1}^{k-1} (-1)^r [r - (r+1)] N_{r,k-1} \\ &\quad + (-1)^k \times k \times N_{k,k-1} \\ &= - \sum_{r=1}^{k-1} (-1)^r N_{r,k-1} \\ &\quad \text{since } N_{k,k-1}=0 \text{ and } N_{0,k-1} = 0 \\ &= -(-1)^{k-1} \\ &\quad \text{by induction hypothesis} \\ &= (-1)^k \\ &= \text{R.H.S. as required} \end{aligned}$$

□

Theorem 2.7: *If G is a group with a split BN-pair then the Brown complex of G is equivalent to the Tits building of G .*

Proof

Let \mathcal{U} be the subcomplex of the Brown complex \mathcal{C} consisting of all simplices

$$Q_0 < Q_1 < \dots < Q_n$$

that satisfy the condition

$$Q_i = O_p(N_G(Q_i)) \quad \forall i \in \{1, 2, \dots, n\} \quad (2.5)$$

It is proved in reference [Kn-Ro] (see proposition 3.3) that the Brown complex, \mathcal{C} is equivalent to the simplicial complex \mathcal{U} .

But since we are now in the setting of a group with a split BN-pair then we can apply the Borel-Tits theorem (ie. theorem 2.1) which says that the only subgroups of G that satisfy equation 2.5 are the unipotent radicals of parabolic subgroups and conversely that the unipotent radicals of parabolic subgroups of G satisfy equation 2.5. Pick a particular Borel subgroup B of G and choose as orbit representatives the unipotent radicals of parabolic subgroups which are contained in this B to get that a typical simplex \mathcal{U}/G is of the form

$$U_\emptyset \subset U_{J_1} \subset \dots \subset U_{J_n}$$

where $J_i \subseteq I$.

Now we consider the alternating sum :-

$$\sum_{C \in \mathcal{U}/G} (-1)^{|C|} f(G_C)$$

where $f : \{\text{subgroups of } G\} \rightarrow A$ is any function that is constant on G -conjugacy classes of subgroups of G and A is any abelian group.

The contribution to this sum from a typical simplex

$$U_\emptyset \subset U_{J_1} \subset \dots \subset U_{J_n}$$

is equal to $(-1)^n f(P_{J_n})$ (By using the fact that $P_X \subseteq P_Y$ if and only if $U_Y \subseteq U_X$). For convenience we will define $\text{Top}(C)$ to be the last group in the chain C (i.e. U_{J_n} in the above chain). So we have

$$\begin{aligned} \sum_{C \in \mathcal{U}/G} (-1)^{|C|} f(G_C) &= \sum_{J \subseteq I} \sum_{\substack{C \in \mathcal{U}/G \\ \text{Top}(C) = U_J}} (-1)^{|C|} f(G_C) \\ &= \sum_{J \subseteq I} f(P_J) \sum_{\substack{C \in \mathcal{U}/G \\ \text{Top}(C) = U_J}} (-1)^{|C|} \\ &\quad \text{by above argument} \\ &= \sum_{J \subseteq I} f(P_J) \sum_{(C)} (-1)^{|C|} \end{aligned}$$

where C ranges over the set consisting of all chains of subsets of $I - J$ which start with the empty set; a typical element of which has the form :-

$$\{\} \subset J_1 \subset J_2 \subset \dots \subset J_n \subset I - J$$

Here we are using the fact that there exists an order preserving bijection between the chains C in \mathcal{U}/G with $\text{Top}(C) = U_J$ and the subsets of $I - J$.

By using the previous lemma the above equation can be simplified to

$$\sum_{C \in \mathcal{U}/G} (-1)^{|C|} f(G_C) = \sum_{J \subseteq I} (-1)^{|I-J|} f(P_J)$$

So, by definition, the simplicial complex \mathcal{U} is equivalent to the simplicial complex obtained in the standard way from the poset

$$\{g^{-1}P_Jg \mid J \subseteq I \text{ and } g \in G\}$$

ordered by reverse inclusion which is precisely the Tits building \mathcal{T} . □

The Alperin conjecture for the classical groups can be recast into a nicer form by using theorem 2.7 (this was first done by G.R. Robinson and R. Knörr (see theorem 5.3 of reference [Kn-Ro])). The formulae obtained are the ones mentioned in the introduction , viz.

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} \ell(P_J)$$

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} k(P_J)$$

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} \ell_0(P_J)$$

These formulae are useful because they link the Alperin conjecture more closely with the structure of the classical groups. Similarly with the block form of the Alperin conjecture we can get different looking formulae e.g.

$$f_0^{(B)}(G) = \sum_{J \subseteq I} (-1)^{|I-J|} \ell_B(P_J)$$

If we count the contribution to both sides of the blocks of kG which are of defect zero we can obtain even better looking formulae, for example formulae like :-

$$\sum_{J \subseteq I} (-1)^{|I-J|} \ell_B(P_J) = 0$$

where B is a block of kG of positive defect.

3. THE ALPERIN CONJECTURE AND THE CLASSICAL GROUPS

This chapter begins with some work by M. Cabanes which proves that the Alperin conjecture is true for not only the classical groups but any group with a split BN-pair, which is from his thèse (see section III of reference [Ca1]). This theorem also appears as Proposition 8 in a more recent paper of M. Cabanes (see reference [Ca2]) where the notation is slightly different. This is followed by a new and quicker proof of my own devising that takes advantage of one of the reformulations of the Alperin conjecture.

3.1 A proof due to M. Cabanes

Before we begin the proof we must remark that for a group with a split BN-pair we have two definitions of a weight (defined both in chapter 1 and chapter 2). The proof that these two notions coincide is the main content of this section. However this causes notational difficulties and so we introduce the notion of an admissible pair as a substitute for the definition of a weight in chapter 1 (so henceforth when a weight is mentioned it will be as in the definition in chapter 2).

Definition

- Let $\chi : B \rightarrow k^*$ be a homomorphism.
Define $M(\chi) = \{i \in I \mid \chi(H_i) = 1\}$.
Then an admissible pair is a pair (S, χ) with $S \subseteq M(\chi)$.

As mentioned above, this definition is equivalent to the original definition of a weight and so we can index the simple kG -modules by admissible pairs. We also have the following lemma

Lemma 3.1: *Let G be a group with a split BN-pair of restricted type. If b is a projective simple kG -module then b is indexed by an admissible pair (\emptyset, χ) for some homomorphism $\chi : B \rightarrow k^*$ with $M(\chi) = I$.*

Conversely, the module indexed by (\emptyset, χ) where $M(\chi) = I$ is projective for any such χ .

Proof

See reference [St] or corollary 4 on page 22 of reference [Ca2]. □

Theorem 3.2 (M.Cabanes): *The Alperin conjecture holds for groups with split BN-pairs of restricted type, i.e.*

$$\ell(G) = \sum_{(Q)} f_0 \left(\frac{N_G(Q)}{Q} \right)$$

where Q ranges over a set of representatives of the conjugacy classes of p -subgroups of G .

Proof

We actually prove is a stronger statement than that given in the theorem; we construct a bijection between the following sets :

$$\{\text{iso. types of simple } kG\text{-modules}\} \longleftrightarrow \{\text{conj. classes of weights}\}$$

We can index the simple kG -modules by admissible pairs and so to prove the theorem all we have to do is index the weights by admissible pairs. To do this we set up the following correspondence :-

$$(S, \chi) \mapsto \text{the conjugacy class of } (Q, b)$$

where $Q = U_J$ and $J = M(\chi) - S$

and b is the kL_J -module corresponding to (\emptyset, χ)
 (we can use this since L_J has a split BN-pair of rank $|J|$)

Now we are done if we can show that the above correspondence is a bijection. This will (as usual) be done in two halves :-

1) The correspondence is surjective : Let (Q, b) be a weight of kG , then since $N_G(Q)/Q$ has a projective simple kG -module we have $Q = O_p(N_G(Q))$ (see reference [Cu-Re], page 625). So by the Borel-Tits theorem (theorem 2.1), Q is conjugate to some U_J for some $J \subseteq I$.

By the above lemma, b must correspond (as an kL_J -module) to an admissible pair (\emptyset, χ) where $\chi : B \rightarrow k^*$ is a homomorphism. Finally, it is easy to check that the admissible pair $(M(\chi) - J, \chi)$ corresponds to (Q, b) under the above correspondence.

2) **The correspondence is injective** : Suppose that (S, χ) and (S', χ') both map to (Q, b) under the above correspondence. By the above argument $Q = U_J$ for some $J \subseteq I$ and b corresponds to (\emptyset, ψ) where $\psi : B \rightarrow k^*$ is a homomorphism. Then we have that b is indexed by (\emptyset, χ) and (\emptyset, ψ) so $\chi = \psi$ since this correspondence is bijective (similarly $\chi' = \psi$). So we have that :-

$$\begin{aligned} S &= M(\chi) - J \\ &= M(\chi') - J \\ &= S' \end{aligned}$$

and hence $(S, \chi) = (S', \chi')$ as required □

3.2 A new proof

The above proof is good since it proves that there is a canonical correspondence between the simple kG -modules and the conjugacy classes of weights. However, if we are just interested in whether the conjecture holds or not then a simpler proof is available. Before we exhibit the simpler proof of the same conjecture we will first prove a little lemma that is needed to prove the result.

Lemma 3.3: *If G is a group with a split BN-pair of restricted type then $f_0(G) = |H/H_I|$*

Proof

By lemma 3.1 we have the following one-to-one correspondence :-

$$\{\text{projective simple } kG\text{-modules}\} \leftrightarrow \{\text{admissible pairs } (\emptyset, \chi) \text{ s.t. } M(\chi) = I\}$$

But if $M(\chi) = I$ then by definition we have that

$$\chi|_{H_i} = 1 \quad \forall i \in I$$

This simply says that $\chi|_{H_I} = 1$ and so we can regard χ as a character of the group H/H_I . This gives the result since H/H_I is an abelian p' -group. □

Having proved this simple lemma we can now go on to state and prove the main content of this section by using the lemma together with the binomial theorem.

Theorem 3.4: *The Alperin conjecture holds for the Classical groups, i.e.*

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} \ell(P_J)$$

Proof

We begin by simplifying the right hand side of the equation

$$\begin{aligned} \text{R.H.S.} &= \sum_{J \subseteq I} (-1)^{|I-J|} \ell(P_J) \\ &= \sum_{J \subseteq I} (-1)^{|I-J|} \ell(P_J/U_J) \\ &\quad \text{since } U_J \text{ is a normal } p\text{-subgroup of } P_J \\ &= \sum_{J \subseteq I} (-1)^{|I-J|} \left(\sum_{K \subseteq J} \left| \frac{H}{H_K} \right| \right) \\ &\quad \text{by corollary 1.10 since } P_J/U_J \text{ has} \\ &\quad \text{a BN-pair of rank } |J|. \\ &= \left| \frac{H}{H_I} \right| \sum_{J \subseteq I} (-1)^{|I-J|} \left(\sum_{K \subseteq J} \left| \frac{H_I}{H_K} \right| \right) \\ &\quad \text{taking out the common factor} \end{aligned}$$

Note that in the above equations we have used the fact that the group corresponding to H_K in P_J is equal to H_K if $K \subseteq J$. This is because the definition of H_K can be stated to only involve the roots (i.e. $\{s_i \mid i \in I\}$) which are contained in P_K (and hence contained in any parabolic subgroup that contains P_K). Recall that

$$H_J = \langle H_j \rangle_{j \in J}$$

where $H_j = H \cap \langle U_j^-, U_j \rangle$. This can be simplified because G is assumed to be one of the Classical groups using the following fact (see chapter 6 of reference [Car1]).

$$\langle U_j^-, U_j \rangle \cong SL_2(q)$$

This isomorphism is a canonical isomorphism which maps the diagonal subgroup of $\langle U_j^-, U_j \rangle$ onto the diagonal subgroup of $SL_2(q)$. Hence H_j is isomorphic to the multiplicative group of the field with q elements, and so we have $|H_j| = q - 1$. Also for the groups that are considering the following holds (see reference [Car1] or pages 493–494 of reference [Go])

$$H_J = \prod_{j \in J} H_j \text{ (direct product)}$$

so we can calculate that

$$|H_J| = (q-1)^{|J|}$$

to simplify the right hand side further :-

$$\begin{aligned}
\text{R.H.S.} &= \left| \frac{H}{H_I} \right| \sum_{J \subseteq I} (-1)^{|I-J|} \left(\sum_{K \subseteq J} (q-1)^{|I-K|} \right) \\
&= \left| \frac{H}{H_I} \right| \sum_{J \subseteq I} (-1)^{|I-J|} \left[(q-1)^{|I-J|} \cdot \sum_{k=0}^{|J|} \binom{|J|}{k} (q-1)^{|J|-k} \right] \\
&= \left| \frac{H}{H_I} \right| \sum_{J \subseteq I} (-1)^{|I-J|} (q-1)^{|I-J|} [(q-1) + 1]^{|J|} \\
&= \left| \frac{H}{H_I} \right| \sum_{j=0}^{|I|} (-1)^{|I|-j} \binom{|I|}{j} (q-1)^{|I|-j} q^j \\
&= \left| \frac{H}{H_I} \right| [q - (q-1)]^{|I|} \\
&= \left| \frac{H}{H_I} \right| \\
&= f_0(G) \quad \text{by the previous lemma} \\
&= \text{L.H.S. as required.}
\end{aligned}$$

□

4. THE ALPERIN CONJECTURE AND THE GENERAL LINEAR GROUP

This chapter deals with some applications of the Alperin conjecture in the more specialised setting of the General Linear Group which is the most important of the classical groups and has the most well understood theory. For example see theorem 14 on page 433 of reference [Gr1] where the value of any complex character on any conjugacy class is obtained.

4.1 Ordinary representations

In this section we will try to calculate the number of isomorphism types of simple FG -modules (i.e. the number of ordinary irreducible characters) of the parabolic subgroups of the general linear group.

This problem is very hard even for the Borel subgroup of the general linear group (which we take to be the group of upper triangular matrices) and we cannot solve the general case. However the Alperin conjecture is very useful in this context and to illustrate the usefulness of the Alperin conjecture we will give an example. Having said this, the special case in which we consider the whole group can be done by classical methods, so we will not explore this case any further and just state the result.

The number of conjugacy classes of the general linear group is equal to the number of rational canonical forms of non-singular $n \times n$ matrices over $GF(q)$, which can be described in terms of the number of partitions of n . This enables us to give a generating function for this number as follows (using $p_n(q)$ to denote $k(Gl_n(q))$).

$$1 + \sum_{n=1}^{\infty} p_n(q)x^n = \prod_{i=1}^{\infty} \frac{(1-x^i)}{(1-qx^i)} \quad (4.1)$$

For details of how this is derived see the preamble leading up to equation 14 of reference [Fe-Fi] and to see an equivalent formula which is easier to calculate with see equation 1 of reference [Be-Fe-Ho].

Before we go ahead and give an example of the calculations involved we will just collect together the results that were obtained and display them as the following table where the entry corresponding to $n = n_0$ and $J = J_0$ is the number of conjugacy classes of the parabolic subgroup P_{J_0} of $GL_{n_0}(q)$.

	$J = \emptyset$	$J = \{1\}$	$J = \{2\}$	$J = \{1, 2\}$
$n = 1$	$q - 1$			
$n = 2$	$q^2 - q$	$q^2 - 1$		
$n = 3$	$q^3 - 2q + 1$	$q^3 - 2q + 1$	$q^3 - 2q + 1$	$q^3 - q$

The only non-trivial calculations in the above table are in the row labeled $n = 3$ and so we will omit the rest. The calculations for the three dimensional general linear group are as follows :-

Lemma 4.1: *The number of isomorphism types of simple $FG L_n(q)$ -modules is equal to $q^3 - q$, or written symbolically*

$$k(GL_n(q)) = q^3 - q$$

Proof

This is an easy calculation using formula 4.1 to find $p_3(q)$. □

Now we focus our attention on the Borel subgroup, B , of $GL_3(q)$ which we take to be group of all non-singular upper triangular matrices, viz.

$$B = \left\{ \left(\begin{array}{ccc} \alpha_{11} & \cdots & \alpha_{1n} \\ 0 & \ddots & \vdots \\ 0 & 0 & \alpha_{nn} \end{array} \right) \mid \alpha_{ij} \in GF(q) \text{ and } \prod_{i=1}^n \alpha_{ii} \neq 0 \right\}$$

Before we can calculate the number of ordinary irreducible characters of the Borel subgroup of $GL_3(q)$ a few lemmas are needed to break up the calculation into portions of manageable sizes.

Lemma 4.2: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$$

with α, β and γ all distinct elements of $GF(q)$. Then there is only one class of p -elements in $C_B(g)$.

Proof

This is true since

$$C_B(g) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \alpha, \beta, \gamma \neq 0 \right\}$$

and the only p -element in this set is the identity element. \square

Lemma 4.3: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$$

with α and β distinct elements of $GF(q)$. Then there are two classes of p -elements in $C_B(g)$.

Proof

By direct calculation we have

$$C_B(g) = \left\{ \begin{pmatrix} \alpha & \delta & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \alpha, \beta, \gamma \neq 0 \right\}$$

and so g centralizes the p -elements

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

which form q conjugacy classes in $C_U(g)$ but only two conjugacy classes in $C_B(g)$, namely the classes containing :-

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

\square

Lemma 4.4: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

with α and β distinct elements of $GF(q)$. Then there are two classes of p -elements in $C_B(g)$.

Proof

The proof of this result is entirely similar to the proof of the previous lemma. \square

Lemma 4.5: *Suppose that*

$$g = \begin{pmatrix} \beta & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

with α and β distinct elements of $GF(q)$. Then there are two classes of p -elements in $C_B(g)$.

Proof

The proof of this result is entirely similar to the proof of the previous lemma. \square

Lemma 4.6: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

with $\alpha \in GF(q)$ then there are five classes of p -elements in $C_B(g)$.

Proof

This type of element is in the center of B and so the centralizer is the whole of B . So what we need to calculate is the number of B -conjugacy classes of U (since U is a Sylow p -subgroup of B). So we need to calculate the number of H -orbits of U -conjugacy classes of U (since $B = HU$). So the first thing that we need to calculate is the number of U -conjugacy classes of U (i.e. $k(U)$). The classes of U can be summarised by the following table :-

type of element of U	order of centralizer in U	number of classes of this type
$\begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	q^3	q
$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}$ α, γ not both zero	q^2	$q^2 - 1$

Hence the number of classes of U can be calculated from the class equation of U to be $q^2 + q - 1$. Having calculated this we return to calculating the number of H -orbits of these classes for which we use a theorem of Glauberman (see reference [Gl]) that has the consequence that the number of U -classes fixed by $h \in H$ is equal to the number of classes of the centralizer in U of h (since $|H|$ and $|U|$ are coprime). So we can calculate the following :-

type of member of H	number of classes of this type	number of U -classes fixed by element
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ α, β, γ distinct	$(q-1)(q-2)(q-3)$	1
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$ α, β distinct	$(q-1)(q-2)$	q
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ α, β distinct	$(q-1)(q-2)$	q
$\begin{pmatrix} \beta & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ α, β distinct	$(q-1)(q-2)$	q
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$	$q-1$	$q^2 + q - 1$

So by Burnside's formula we have :-

$$\begin{aligned}
 \text{number of } H\text{-orbits of } U\text{-conjugacy classes of } U &= \frac{1}{(q-1)^3} [1 \times (q-1)(q-2)(q-3) \\
 &+ q \times (q-1)(q-2) \\
 &+ q \times (q-1)(q-2) \\
 &+ q \times (q-1)(q-2) \\
 &+ (q^2 + q - 1) \times (q-1)] \\
 &= 5
 \end{aligned}$$

□

We may now proceed to prove the following theorem :-

Theorem 4.7: *If B is the Borel subgroup of $GL_3(q)$ then*

$$k(B) = (q-1)(q^2 + q - 1)$$

Proof

We use the fact that the p -regular elements of B are in one-to-one correspondence with the elements of H (since $B = UH$ with U a normal p -subgroup and H an abelian p' -group). The way that we calculate this is to count the number of classes of p -elements in the centraliser of each p -regular element and then use the formula

$$k(B) = \sum_{(g)} \#(\text{classes of } p\text{-elements of } C_B(g))$$

where (g) runs through a set of representatives for the conjugacy classes of p -regular elements of B . The results of the last three lemmas can be summarised in the following table :-

type of p -regular element	number of classes of this type	number of classes of p -elements in centraliser
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ α, β, γ distinct	$(q-1)(q-2)(q-3)$	1
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$ α, β distinct	$(q-1)(q-2)$	2
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ α, β distinct	$(q-1)(q-2)$	2
$\begin{pmatrix} \beta & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ α, β distinct	$(q-1)(q-2)$	2
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$	$q-1$	5

So now we can calculate the number of conjugacy classes of B as follows

$$\begin{aligned}
\# \text{ of classes of } B &= 1 \times (q-1)(q-2)(q-3) \\
&\quad + 2 \times (q-1)(q-2) \\
&\quad + 2 \times (q-1)(q-2) \\
&\quad + 2 \times (q-1)(q-2) \\
&\quad + 5 \times (q-1) \\
&= (q-1)(q^2 + q - 1) \\
&\quad \text{as required}
\end{aligned}$$

□

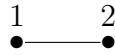
Having calculated the number of ordinary irreducible characters of the Borel subgroup we can now obtain the number of ordinary irreducible characters of a maximal parabolic subgroup.

Theorem 4.8: *The number of ordinary irreducible characters of both of the maximal parabolic subgroups of $GL_3(q)$ is equal to $(q-1)(q^2 + q - 1)$. This can be written as*

$$k(P) = (q-1)(q^2 + q - 1)$$

Proof

Firstly we show that the two maximal parabolic subgroups of $GL_3(q)$ are isomorphic. To do this we note that the general linear group is a Chevalley group and so has a Dynkin diagram associated with it. The diagram for $GL_3(q)$ is as follows



By Theorem 12.5.1 on page 211 of reference [Car1] the graph automorphism which interchanges nodes one and two of the above graph induces an automorphism of the Chevalley group $GL_3(q)$. This automorphism of $GL_3(q)$ is clearly seen to map the subgroup $P_{\{1\}}$ to the subgroup $P_{\{2\}}$.

Now we can use the Alperin conjecture (as reformulated in reference [Kn-Ro]). The particular form that we use is :-

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} k(P_J) \tag{4.2}$$

In the above formula there are two unknowns, $k(P_{\{1\}})$ and $k(P_{\{2\}})$, but these are equal because by the above argument $P_{\{1\}} \cong P_{\{2\}}$.

By using lemma 3.3, it is an easy calculation to show that $f_0(G) = q - 1$ and substituting this into equation 4.2 gives

$$(q-1) = (q^3 - q) - 2 \times k(P) + (q-1)(q^2 + q - 1)$$

from which the result follows.

□

4.2 The p -rank of the Cartan Matrix

The problem that I am going to solve in this section is that of finding the p -rank of the Cartan matrix of any parabolic subgroup of the general linear group. As well as being an interesting invariant of a finite group we show that this is equal to the number of polynomials of a certain type, which we will now define.

Definitions

- The set of all monic polynomials of degree n over the field with q elements without repeated factors and with non-zero constant term will be denoted by $S_{n,q}$.
- Let $J \subseteq I$ and consider the parabolic subgroup of the general linear group denoted by P_J . It is well known that the Levi complement (denoted L_J) of P_J has a split BN-pair and is in fact just a direct product of general linear groups of various degrees, say

$$L_J \cong GL_{n_1}(q) \times GL_{n_2}(q) \times \dots \times GL_{n_N}(q)$$

So we can associate a composition of n^1 to the parabolic subgroup P_J , namely (n_1, n_2, \dots, n_N) .

Note that

$$n = \sum_{i=1}^N n_i$$

by counting the rows of the matrices involved in the above equation (see the example on page 4).

- If $\lambda = (n_1, n_2, \dots, n_N)$ then λ is said to be a partition of n (written $\lambda \vdash n$) if all of the following hold :-

1. $n_i > 0 \forall i \in \{1, 2, \dots, N\}$
2. $n_1 \geq n_2 \geq \dots \geq n_N$
3. $\sum_{i=1}^N n_i = n$

¹ a composition of n being a sequence of positive integers that add up to n

An alternative notation for partitions will also be used, viz.

$$\lambda_i = (1^{m_1}, 2^{m_2}, 3^{m_3}, \dots)$$

This notation is simply to say that m_i is the multiplicity of i in the partition λ . By convention, if i does not appear in the partition λ then m_i is zero.

- Let s be any polynomial of degree n over a field with q elements. Let λ be a composition of n , then s is said to be of type λ if there exist polynomials s_1, s_2, \dots, s_m such that

$$s = s_1 s_2 \dots s_m$$

where $\lambda = (\deg s_1, \deg s_2, \dots, \deg s_m)$.

- We define $S_{n,q}(\lambda)$ to be the following set

$$S_{n,q}(\lambda) = \{(s_1, s_2, \dots, s_m) \mid s_1 \dots s_m \in S_{n,q} \text{ and } s_1 \dots s_m \text{ is of type } \lambda\}$$

Proposition 4.9: *Let P_J be a parabolic subgroup of $GL_n(q)$ containing the upper triangular matrices and let $g \in P_J$.*

Then p does not divide the order of $C_{P_J}(g)$ if and only if the characteristic polynomial of g has no repeated factors.

Proof

Let $g = su = us$ where s is a semi-simple (i.e. p -regular) element in P_J and u is a unipotent element (i.e. a p -element) in P_J . Then g and s have the same characteristic polynomial $q(x)$.

Now we suppose that the polynomial $q(x)$ has no repeated factors. Consider this polynomial $q(x)$ as a polynomial over its splitting field $GF(q^{n!})$ and express it as a product of linear factors. So the semi-simple element s of $GL_n(q^{n!})$ with characteristic polynomial $q(x)$ is conjugate to a diagonal matrix with distinct elements on the diagonal, call this matrix D . So we have that there exists a matrix $m \in GL_n(q^{n!})$ such that

$$D = m s m^{-1}$$

Let v be any matrix of $GL_n(q^{n!})$ that commutes with s then we have

$$sv = vs$$

So we can proceed as follows

$$\begin{aligned}
Dmvm^{-1} &= (msm^{-1})mvm^{-1} \\
&= msvm^{-1} \\
&= mvsm^{-1} \\
&= mvm^{-1}(msm^{-1}) \\
&= mvm^{-1}D
\end{aligned}$$

So mvm^{-1} commutes with D , but any element of $GL_n(q^{n!})$ that commutes with D must be a diagonal matrix. So v is conjugate to a diagonal matrix and thus must be p -regular since there are no diagonal matrices that are of order divisible by p . Hence no p -element of $GL_n(q)$ commutes with s since any p -element of $GL_n(q)$ is also a p -element of $GL_n(q^{n!})$ (under the natural embedding $GL_n(q) \hookrightarrow GL_n(q^{n!})$). So no p -element of P_J commutes with s and we must have $g = s$. This implies that p does not divide the order of the centralizer in P_J of g , as required.

To prove the other implication, we prove the contrapositive statement : $q(x)$ has repeated factors implies that p divides $|C_{P_J}(g)|$. So suppose that $q(x)$ has repeated factors. If $u \neq 1$ then we have that p divides the order of g and so p divides $|C_{P_J}(g)|$ and we are done. So the case remaining is when $u = 1$ and hence $g = s$ is a semi-simple element.

But P_J has a normal p -subgroup U_J and hence every P_J -class of p -regular elements of P_J has a representative in $L_J \cong P_J/U_J$. So g is conjugate within P_J to an element of L_J . From now on we will assume that we have picked our conjugacy class representatives such that $g \in L_J$ (we can do this since the condition that p does not divide $|C_{P_J}(g)|$ only depends on the P_J -conjugacy class of g). Since we have that

$$L_J \cong GL_{n_1}(q) \times GL_{n_2}(q) \times \dots \times GL_{n_N}(q)$$

we have that, within L_J , g is conjugate to a matrix of the form

$$\begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & B_m \end{pmatrix}$$

where B_i for each $i \in \{1, 2, \dots, m\}$ is a companion matrix of some irreducible factor of $q(x)$. Since we are only interested in a property which only depends on the conjugacy class of g we may assume that g has the above form.

But $q(x)$ has repeated factors and hence $B_i = B_j$ for some $i \neq j$. And so the above matrix can easily be seen to commute with the matrix which

has the same block structure as above and has identity matrices along the diagonal and an identity matrix the size of B_i in the $(i, j)^{th}$ position and null matrices elsewhere i.e. the matrix

$$\begin{pmatrix} \ddots & 0 & \cdots & \cdots & 0 \\ 0 & I_i & \cdots & I_i & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & I_j & 0 \\ 0 & \cdots & \cdots & 0 & \ddots \end{pmatrix}$$

where I_k denotes an identity matrix the same size as B_k . This element is clearly a p -element (being a member of the Sylow p -subgroup of $GL_n(q)$). Hence we have $C_U(g) \neq 1$ and so p divides $|C_{P_J}(g)|$ as required. \square

Having proved this proposition, we can now prove the equality mentioned above.

Theorem 4.10: *Let P_J be a parabolic subgroup of the general linear group and let λ be the composition of n that corresponds to P_J under the correspondence defined above. Then the p -rank of the Cartan matrix of P_J is equal to the number of polynomials of degree n over a field with q elements without repeated factors and of type λ , i.e.*

$$\ell_0(P_J) = |S_{n,q}(\lambda)|$$

Proof

By theorem 1.7 what we need to do is to count the number of P_J -conjugacy classes of P_J such that p does not divide the order of the centralizer in P_J of an element of that class. So suppose that g is an element of P_J with p not dividing $|C_{P_J}(g)|$. Let $q(x)$ be the characteristic polynomial of g . As in the proof of the preceding proposition we have that g is conjugate within P_J to an element of L_J . Hence we have :-

$$g \sim \begin{pmatrix} B_{n_1} & 0 & \cdots & 0 \\ 0 & B_{n_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & B_{n_N} \end{pmatrix}$$

where B_{n_i} is a matrix in $GL_{n_i}(q)$. So if we define $q_i(x)$ to be the characteristic polynomial of B_{n_i} we have

$$q(x) = q_1(x)q_2(x) \dots q_N(x)$$

This says explicitly that $q(x)$ is of type $\lambda = (n_1, n_2, \dots, n_N)$. Conversely, if $q(x)$ is of type λ and has non-zero constant term then we can reverse the above argument to get a corresponding semi-simple matrix in L_J .

By the above proposition we have that $q(x)$ has no repeated factors and by combining the last two statements we are done. \square

The most important case of the above theorem is when $J = I$ (i.e. $P_J = GL_n(q)$) and so this is stated separately as a corollary.

Corollary 4.11: *The p -rank of the Cartan matrix of the general linear group, $GL_n(q)$, is equal to the number of monic polynomials of degree n over a field with q elements without repeated factors with non-zero constant term, i.e.*

$$\ell_0(G) = |S_{n,q}|$$

Proof

This follows immediately from the above theorem since the whole group is always a parabolic subgroup of itself. \square

In order to illustrate the method of calculating the answer to the question of finding the value of $\ell_0(P_J)$ using the above theorem we will show a few worked examples.

Example

The first example that we shall consider is the easiest case of the above which is calculating the p -rank of the Cartan matrix of a Borel subgroup of the general linear group (i.e. the case where $J = \emptyset$).

In this case the p -regular elements are all of the diagonal matrices with non-zero entries on the diagonal. Therefore we have $(q - 1)^n$ p -regular elements and we want all of the elements on the diagonal to be distinct to count (as in the proof of the last theorem). So we have $q - 1$ choices for the first element, $q - 2$ choices for the second element, \dots and $q - n$ choices for the last element. So this gives

$$\ell_0(P_\emptyset) = (q - 1)(q - 2) \dots (q - n)$$

Note that this formula will be true even if $n \geq q$.

Example

The second most easy case is that when J consists of just a singleton, say $J = \{1\}$. In this case we have two cases to consider, one when the characteristic polynomial of our representative of a conjugacy class of p -regular elements factorises into a product of linear factors and another where it factorises as an irreducible quadratic and some linear factors.

In the first case we have basically the same as the above with the exception that the first two entries on the diagonal can be taken in any order (since the matrix with the submatrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ in the top left hand corner is now in the group of matrices that we are allowed to conjugate by). This allows us to calculate the contribution from the first case to be

$$\frac{1}{2}(q-1)(q-2)\dots(q-n)$$

In the second case we have to consider, we have one irreducible quadratic factor and $n-2$ linear factors. So we need to know the number of monic irreducible quadratics over a field with q elements, which by an easy calculation we can derive :-

$$I_2(q) = \frac{1}{2}q(q-1)$$

So with an argument similar to that in the last example we can calculate the contribution from this case to be

$$\frac{1}{2}q(q-1) \times (q-1)(q-2)\dots(q-n+2)$$

By adding the previous two equations we have the result :-

$$\ell_0(P_{\{1\}}) = \frac{1}{2}(q-1)(q-2)\dots(q-n+2)[(q-n+1)(q-n) + q(q-1)]$$

After these two examples the situation in the general case should be clear, but before we do a more complicated example a few definitions are necessary in order to simplify the notation.

Definitions

- We will use $I_n(q)$ to denote the number of irreducible monic polynomials of degree n over a field with q elements with non-zero constant term. This can be calculated explicitly by using the formulae that follow

$$I_1(q) = q - 1$$

since $x - \alpha$ is an irreducible polynomial with non-zero constant term for any $\alpha \neq 0$. For a polynomial that is non-linear the condition that an irreducible polynomial has a non-zero constant term is vacuous and hence the number of them can be computed using the standard formula

$$I_n(q) = \frac{1}{n} \sum_{d|n} \mu(n/d)q^d$$

where the sum ranges over all of the divisors of n and μ is the Möbius function i.e.

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^k & \text{if } n = p_1 p_2 \dots p_k \text{ for distinct primes } p_i \end{cases}$$

For details of how this formula is derived see reference [Li-Ni], theorem 3.25 on page 84.

Example

We will now consider the special case of calculating the p -rank of the Cartan matrix of the whole of the general linear group (i.e. the case where $J = I$).

As proved above, this is equivalent to counting the number of polynomials of degree n over a field with q elements without repeated factors (i.e. calculating the cardinality of $S_{n,q}$). So consider an element $s(x) \in S_{n,q}$ and express this as a product of irreducible polynomials as follows

$$s(x) = s_1(x)s_2(x) \dots s_m(x)$$

and we order the factors so that $\deg s_1 \geq \deg s_2 \geq \dots \geq \deg s_m$. So we can associate a partition of n with the above decomposition by setting $\lambda = (\deg s_1, \deg s_2, \dots, \deg s_m)$. Rewrite λ in another notation to get $\lambda = (1^{m_1}, 2^{m_2}, \dots, i^{m_i}, \dots)$ i.e. let m_i be the number of polynomials of degree i that occur in the above decomposition of $s(x)$.

Now we consider the contribution to $\ell_0(G)$ from all polynomials that correspond to a partition λ in the way described above. Consider the contribution from the part of the polynomial $s(x)$ which consists of the factors of degree j . There are m_j of these and so we get $I_j(q)$ choices for the first factor and $I_j(q) - 1$ choices for the second factor, \dots and $I_j(q) - m_j + 1$ choices for the m_j^{th} factor. But these factors can occur in any order so we have

counted each $s(x)$ a total of $m_j!$ times, when this is taken into account we have a contribution from the factors of degree j of

$$\frac{1}{m_j!} I_j(q) [I_j(q) - 1] \dots [I_j(q) - m_j + 1]$$

this is simply the binomial coefficient

$$\binom{I_j(q)}{m_j}$$

Once this is done for any j the contribution from polynomials that correspond to λ can be calculated as the product of all of the possibilities for each size of factor, so we get the contribution from polynomials corresponding to λ to be

$$\prod_{j=1}^{\infty} \binom{I_j(q)}{m_j}$$

All that now remains to be done to calculate $\ell_0(G)$ is to sum over all of the possible partitions of n to get

$$\ell_0(G) = \sum_{\lambda \vdash n} \prod_{j=1}^{\infty} \binom{I_j(q)}{m_j}$$

A simpler formula for $\ell_0(G)$ can be derived by another method which relies on the characterisation of $\ell_0(G)$ as the cardinality of $S_{n,q}(\lambda)$. An exposition of the derivation of the simpler formula, which is due to R.M. Bryant, is given at the end of this chapter.

We now proceed to find a formula similar to the above for the p -rank of the Cartan matrix a parabolic subgroup of the general linear group.

Theorem 4.12: *Let P_J be an arbitrary parabolic subgroup of the general linear group, $GL_n(q)$. Let (n_1, n_2, \dots, n_N) be the composition of n that is associated to P_J . Then we have :-*

$$\ell_0(P_J) = \sum_{\lambda_1 \vdash n_1} \dots \sum_{\lambda_N \vdash n_N} \left[\prod_{i=1}^N p_i(q) \right]$$

where

$$p_i(q) = \prod_{j=1}^{\infty} \binom{I_j(q) - \sum_{k=1}^{i-1} m_j^{(k)}}{m_j^{(i)}}$$

where

$$\lambda_i = (1^{m_1^{(i)}}, 2^{m_2^{(i)}}, \dots)$$

Proof

By the previous corollary what we need to do is calculate the number of polynomials in the set $S_{n,q}(\lambda)$ where $\lambda = (n_1, n_2, \dots, n_N)$.

The number of polynomials in $S_{n_i,q}$ can be calculated, as in the above example, to be as follows

$$|S_{n_i,q}| = \sum_{\lambda_i \vdash n_i} \prod_{j=1}^{\infty} \binom{i_j(q)}{m_j^{(i)}}$$

The p -rank of the Cartan matrix of P_J is not just the product of these since if a particular polynomial contributes to any one of the above sums for any i then it must not occur in any of the others. Hence we must take into account the number of irreducible polynomials of degree j that occur in the components of λ that are before i , this is exactly the sum

$$\sum_{k=1}^{i-1} m_j^{(k)}$$

So taking this into account we get the contribution to $\ell_0(P_J)$ from the component n_i to be

$$\sum_{\lambda_i \vdash n_i} \prod_{j=1}^{\infty} \binom{I_j(q) - \sum_{k=1}^{i-1} m_j^{(k)}}{m_j^{(i)}}$$

The result is now obtained by taking the product of all of these terms as i ranges between 1 and N . □

The formula given in the last theorem is a bit cumbersome to work with, but is the best I have obtained. A better formula can be obtained in the case of the whole general linear group, and I will give an exposition of this. The following argument is due to R.M. Bryant.

Lemma 4.13: *Let $g_n(q)$ denote the number of monic polynomials of degree n over a field with q elements with no repeated factors. Then:*

$$g_n(q) = \begin{cases} q^n & \text{if } n = 0, 1 \\ q^n - q^{n-1} & \text{if } n \geq 2 \end{cases}$$

Proof

Let $f_r(q)$ denote the number of monic irreducible polynomials of degree r over a field with q elements. Let r to be an fixed integer and consider the polynomial

$$(1 + x^r)^{f_r(q)} = \sum_{k=0}^{f_r(q)} \binom{f_r(q)}{k} x^{rk}$$

and note that the coefficient of x^{rk} is the number of possible products of k *distinct* monic irreducible polynomials of degree r .

Now consider the formal power series

$$C(x) = \prod_{r=1}^{\infty} (1 + x^r)^{f_r(q)}$$

and note that from the above remark the coefficient of x^n is the number of monic polynomials of degree n *with no repeated factors* i.e.

$$C(x) = \sum_{n=0}^{\infty} g_n(q) x^n \tag{4.3}$$

Now that we have two interpretations of the formal power series $C(x)$ we proceed to manipulate $C(x)$ to get a simpler expression in a purely formal manner. So we get

$$\log C(x) = \sum_{r=1}^{\infty} f_r(q) \log(1 + x^r)$$

which we can differentiate formally to yield

$$\frac{C'(x)}{C(x)} = \sum_{r=1}^{\infty} \frac{x^{r-1} r f_r(q)}{1 + x^r}$$

and proceed as follows

$$\begin{aligned} \frac{x C'(x)}{C(x)} &= \sum_{r=1}^{\infty} \frac{x^r r f_r(q)}{1 + x^r} \\ &= \sum_{r=1}^{\infty} r f_r(q) x^r (1 - x^r + x^{2r} - \dots) \\ &= \sum_{r=1}^{\infty} r f_r(q) (x^r - x^{2r} + x^{3r} - \dots) \\ &= \sum_{n=1}^{\infty} \left[\sum_{r|n} r f_r(q) (-1)^{(n/r-1)} \right] x^n \end{aligned}$$

We now use a standard result from the theory of finite fields, namely

$$\sum_{r|n} r f_r(q) = q^n$$

which is derived in reference [Li-Ni] as corollary 3.21 on page 82.

If n is odd the coefficient of x^n in $C(x)$ is just $\sum_{r|n} r f_r(q)$ which by the above formula is just q^n .

If n is even the coefficient of x^n may be written as

$$\sum_{r|n} r f_r(q) - 2 \left[\sum_{\{r|n:n/r \text{ is even}\}} r f_r(q) \right]$$

But since n/r is even if and only if $r \mid (n/2)$ we get that the coefficient of x^n in $C(x)$ is equal to

$$\sum_{r|n} r f_r(q) - 2 \left[\sum_{r|(n/2)} r f_r(q) \right] = q^n - 2q^{(n/2)}$$

So we obtain

$$\begin{aligned} \frac{x C'(x)}{C(x)} &= \sum_{n=1}^{\infty} q^n x^n - 2 \sum_{n=1}^{\infty} q^n x^{2n} \\ &= 1 + \sum_{n=0}^{\infty} q^n x^n - 2 \sum_{n=0}^{\infty} q^n x^{2n} \\ &= 1 + \frac{1}{1 - qx} - \frac{2}{1 - qx^2} \end{aligned}$$

Continuing to simplify this expression we get

$$\begin{aligned} \frac{C'(x)}{C(x)} &= \frac{1}{x} + \frac{1}{x(1 - qx)} - \frac{2}{x(1 - qx^2)} \\ &= \frac{1}{x} + \frac{1}{x} + \frac{q}{1 - qx} - \frac{2}{x} - \frac{2qx}{1 - qx^2} \\ &= \frac{q}{1 - qx} - \frac{2qx}{1 - qx^2} \\ &= \frac{d}{dx} \left[\log \left(\frac{1 - qx^2}{1 - qx} \right) \right] \end{aligned}$$

So we have arrived at the equation

$$\frac{d}{dx} [\log C(x)] = \frac{d}{dx} \left[\log \left(\frac{1 - qx^2}{1 - qx} \right) \right]$$

which we can solve to get

$$C(x) = A \left(\frac{1 - qx^2}{1 - qx} \right)$$

for some constant A , which we can determine since we know that $C(0) = 1$ (and hence $A = 1$). So we have

$$\begin{aligned} C(x) &= \frac{1 - qx^2}{1 - qx} \\ &= (1 - qx^2)(1 + qx + q^2x^2 + q^3x^3 + \dots) \\ &= 1 + qx + (q^2 - q)x^2 + (q^3 - q^2)x^3 + \dots + (q^n - q^{n-1})x^n + \dots \end{aligned}$$

But by equation 4.3 the coefficient of x^n in the above equation is equal to $g_n(q)$ and so the result follows. \square

The way that the above lemma is related to our problem is given by the following lemma.

Lemma 4.14: *Let $g_n(q)$ be as given in the previous lemma and let $h_n(q) = \ell_0(GL_n(q))$ (i.e. $h_n(q)$ is the p -rank of the Cartan matrix of the general linear group of $n \times n$ matrices over a field of q elements). Then*

$$h_n(q) + h_{n-1}(q) = g_n(q)$$

Proof

By corollary 4.11, $h_n(q)$ can be interpreted as the number of monic polynomials of degree n over a field of q elements with no repeated factors and non-zero constant term.

Now consider the number $g_n(q) - h_n(q)$, this represents the number of monic polynomials of degree n over a field of q elements with no repeated factors and zero constant term. Such polynomials can be factorised into the form $xp(x)$ where $p(x)$ is a monic polynomial of degree $n - 1$ with no repeated factors. The polynomial $p(x)$ does not have the linear polynomial x as a factor since this would imply that $xp(x)$ had repeated factors. So $p(x)$ has non-zero constant term and hence contributes to $h_{n-1}(q)$, moreover any polynomial that contributes to $h_{n-1}(q)$ would give such a $p(x)$. So we have $h_{n-1}(q)$ choices for $p(x)$ and the result follows \square

Theorem 4.15: *The p -rank of the Cartan matrix of the general linear group of $n \times n$ matrices over a field of q elements is equal to*

$$h_n(q) = (q - 1) \left[\frac{q^n + (-1)^{n-1}}{q + 1} \right]$$

Proof

We prove this result by induction on n .

Initial step: $n=1$ Since $GL_1(q)$ is isomorphic to the multiplicative group of the field $GF(q)$ it is cyclic of order $q - 1$ and contains only p' -elements. So by theorem 1.7 the p -rank of the Cartan matrix of $GL_1(q)$ is equal to $q - 1$.

The above formula gives

$$\begin{aligned} h_n(q) &= (q - 1) \left[\frac{q^1 + (-1)^0}{q + 1} \right] \\ &= (q - 1) \end{aligned}$$

Induction step Suppose that the formula is true for $n = k - 1$ i.e.

$$h_{k-1}(q) = (q - 1) \left[\frac{q^{k-1} + (-1)^k}{q + 1} \right]$$

we need to show that the formula holds for $n = k$.

By the previous lemma we have

$$h_k(q) = g_k(q) - h_{k-1}(q)$$

Now we simply substitute the value of $g_k(q)$ (obtained in the previous lemma (note that the last case applies since $k \geq 2$)) and the value of $h_{k-1}(q)$ (given by the induction hypothesis) and simplify :

$$\begin{aligned} h_k(q) &= g_k(q) - h_{k-1}(q) \\ &= [q^k - q^{k-1}] - (q - 1) \left[\frac{q^{k-1} + (-1)^k}{q + 1} \right] \\ &= (q - 1) \left[q^{k-1} - \frac{q^{k-1} + (-1)^k}{q + 1} \right] \end{aligned}$$

$$\begin{aligned}
&= (q-1) \left[\frac{(q^k + q^{k-1}) - (q^{k-1} + (-1)^k)}{q+1} \right] \\
&= (q-1) \left[\frac{q^k + (-1)^{k-1}}{q+1} \right] \\
&\text{as required.}
\end{aligned}$$

□

The following lemma is due to G.R. Robinson

Lemma 4.16: *The number of polynomials of the form $s_1(x)s_2(x)\dots s_N(x)$ where s_i is a monic polynomial of degree n_i , and where the product has no repeated factor is the coefficient of $x_1^{n_1}x_2^{n_2}\dots x_N^{n_N}$ in*

$$\prod_{r=1}^{\infty} (1 + x_1^r + \dots + x_N^r)^{f_r(q)}$$

Proof

To simplify the notation in this proof we will use multinomial coefficients as defined by

$$\binom{n}{r_1, r_2, \dots, r_k} = \frac{n!}{r_1! r_2! \dots r_k!}$$

Now let r to be an fixed integer and consider the polynomial

$$(1 + x_1^r + \dots + x_N^r)^{f_r(q)} = \sum_{k_i} \binom{f_r(q)}{k_1, k_2, \dots, k_N, k_{N+1}} x_1^{rk_1} x_2^{rk_2} \dots x_N^{rk_N} 1^{rk_{N+1}}$$

and note that the coefficient of $x_1^{rk_1} \dots x_N^{rk_N}$ is the number of ways of choosing k_1 *distinct* monic irreducible polynomials of degree r and then another k_2 *distinct* monic irreducible polynomials of degree r from the remaining set and another $k_3 \dots$

Now consider the formal power series

$$\prod_{r=1}^{\infty} (1 + x_1^r + \dots + x_N^r)^{f_r(q)}$$

The coefficient of $x_1^{n_1} x_2^{n_2} \dots x_N^{n_N}$ in the above expression is just the result of summing the above multinomial coefficient over all partitions of n_1, n_2, \dots, n_N respectively. To be precise the coefficient of $x_1^{n_1} x_2^{n_2} \dots x_N^{n_N}$ in the above expression is

$$\sum_{\lambda_1 \vdash n_1} \sum_{\lambda_2 \vdash n_2} \dots \sum_{\lambda_N \vdash n_N} \prod_{r=1}^n \binom{f_r(q)}{m_1^{(r)}, m_2^{(r)}, \dots, m_N^{(r)}}$$

where $\lambda_i = (1^{m_1^{(i)}}, 2^{m_2^{(i)}}, \dots)$.

The last formula is easily seen to be equal to the formula given in theorem 4.12, as required. \square

By using this lemma it is possible to determine an explicit formula for the p -rank of the Cartan matrix for certain parabolic subgroups of $GL_n(q)$. The case that I will describe is that of finding $\ell_0(P_J)$ where the composition of n that is associated with P_J is $(n-1, 1)$.

Lemma 4.17: *Let $g_{n,m}(q)$ denote the number of monic polynomials of degree n over a field with q elements with no repeated factors and of type (n, m) i.e. we define $g_{n,m}(q)$ as follows :-*

$$g_{n,m}(q) = |S_{n+m,q}((n, m))|$$

Then the following formula is true

$$g_{n,1}(q) = \begin{cases} q & \text{if } n = 0 \\ q(q-1) \left[\frac{q^n + (-1)^{n-1}}{q+1} \right] & \text{if } n \geq 1 \end{cases}$$

Proof

Consider the following power series in two algebraically independent indeterminates

$$C(x, y) = \prod_{r=1}^{\infty} (1 + x^r + y^r)^{f_r(q)}$$

then by the above lemma the number that we are interested in, $g_{n,1}(q)$, is the coefficient of $x^n y$ in this power series. To determine this coefficient we note that it is the coefficient of x^n in the formal partial derivative of $C(x, y)$ with respect to y . So we first calculate this partial derivative as follows

$$\begin{aligned} \log C(x, y) &= \sum_{r=1}^{\infty} f_r(q) \log(1 + x^r + y^r) \\ \Rightarrow \frac{\partial}{\partial y} \log C(x, y) &= \sum_{r=1}^{\infty} \frac{f_r(q) r y^{r-1}}{1 + x^r + y^r} \\ \Rightarrow \frac{\partial}{\partial y} C(x, y) &= C(x, y) \times \left[\sum_{r=1}^{\infty} \frac{f_r(q) r y^{r-1}}{1 + x^r + y^r} \right] \end{aligned}$$

Now we note that the constant term is obtained by putting $y = 0$ in the above formula, so we get

$$\begin{aligned}
\left. \frac{\partial}{\partial y} C(x, y) \right|_{y=0} &= \left[\prod_{r=1}^{\infty} (1+x^r)^{f_r(q)} \right] \times \left[\sum_{r=1}^{\infty} \frac{f_r(q) r 0^{r-1}}{1+x^r} \right] \\
&= \left[\prod_{r=1}^{\infty} (1+x^r)^{f_r(q)} \right] \times \left[\frac{f_1(q) \times 1 \times 1}{1+x^1} \right] \\
&\quad \text{since only the first term} \\
&\quad \text{in the right hand sum is non-zero} \\
&= \left[\prod_{r=1}^{\infty} (1+x^r)^{f_r(q)} \right] \times \left[\frac{q}{1+x} \right] \\
&\quad \text{since } f_1(q) = q \\
&= \frac{1-qx^2}{1-qx} \frac{q}{1+x} \\
&\quad \text{by the argument in the proof of lemma 4.13} \\
&= q \left[1+qx + (q^2-q)x^2 + (q^3-q^2)x^3 + \dots \right] \\
&\quad \times \left[1-x+x^2-x^3+x^4-\dots \right] \\
&= q \left[1+(q-1)x + (q^2-q-q+1)x^2 + \right. \\
&\quad \left. ((q^3-q^2) - (q^2-q) + q-1)x^3 + \dots \right] \\
&= q \left[1+(q-1)x + (q-1)(q-1)x^2 + \right. \\
&\quad \left. (q-1)(q^2+q-1)x^3 + \dots \right]
\end{aligned}$$

So we have if $n \geq 2$ the coefficient of x^n in the above power series has the following form

$$q(q-1) \left[q^{n-1} - q^{n-2} + q^{n-3} - \dots + (-1)^{n-1} \right]$$

which can be simplified by noting that the term in the square brackets is a geometric progression and so we get that the coefficient of x^n is

$$q(q-1) \left[\frac{q^n + (-1)^{n-1}}{q+1} \right]$$

The result now follows from the remarks made at the beginning of this proof. \square

The above lemma is linked to the problem of finding the p -rank of the Cartan matrix of certain parabolic subgroups via the following lemma.

Lemma 4.18: *Let P_J be a parabolic subgroup of the general linear group, $GL_n(q)$, and suppose that the composition of n that is associated with P_J is $(n-1, 1)$. Define $h_{n-1,1}(q)$ by*

$$h_{n-1,1}(q) = \ell_0(P_J)$$

Then the following reduction formula holds

$$h_{n-1,1}(q) = g_{n-1,1}(q) - h_{n-2,1}(q) - h_{n-1}(q)$$

where $h_{n-1}(q)$ is given by the formula in theorem 4.15.

Proof

By theorem 4.10, $h_{n-1,1}(q)$ can be interpreted as the number of monic polynomials of degree n over a field of q elements with no repeated factors and non-zero constant term and of type $(n-1, 1)$.

Now consider the number $g_{n-1,1}(q) - h_{n-1,1}(q)$, this represents the number of monic polynomials of degree n over a field of q elements with no repeated factors and zero constant term. Such polynomials can be factorised into the form $xp(x)$ where $p(x)$ is a monic polynomial of degree $n-1$ with no repeated factors. This polynomial, $p(x)$, can either be of type $(n-2, 1)$ or of type $(n-1)$. The polynomial $p(x)$ does not have the linear polynomial x as a factor since this would imply that $xp(x)$ had repeated factors. So $p(x)$ has non-zero constant term and hence contributes to either $h_{n-2,1}(q)$ or $h_{n-1}(q)$. Moreover any polynomial that contributes to either $h_{n-2,1}(q)$ or $h_{n-1}(q)$ would give such a $p(x)$. So we have $h_{n-2,1}(q) + h_{n-1}(q)$ choices for $p(x)$ and the result follows. \square

The previous two lemmas can be combined to give the following theorem

Theorem 4.19: *Let P_J be a parabolic subgroup of the general linear group, $GL_n(q)$, and suppose that the composition of n that is associated with P_J is $(n-1, 1)$. Define $h_{n-1,1}(q)$ by*

$$h_{n-1,1}(q) = \ell_0(P_J)$$

Then $h_{n-1,1}(q)$ can be calculated by the following formula

$$h_{n,1}(q) = (-1)^{n-1} \frac{(q-1)^2}{(q+1)^2} \left[(-q)^{n+1} + (n+1)q + n \right] + (-1)^n (q-1)$$

Proof

We prove this result by induction on n .

Initial step: $n=1$ The p -rank of the Cartan matrix of a parabolic subgroup, P_J , of $GL_2(q)$ which is associated with the composition $(1, 1)$ can easily be calculated by theorem 4.12 to be the following

$$\ell_0(P_J) = (q - 1)(q - 2)$$

While the above formula gives

$$\begin{aligned} h_{1,1}(q) &= \frac{(q-1)^2}{(q+1)^2} [q^2 + 2q + 1] - (q-1) \\ &= (q-1)[(q-1) - 1] \\ &= (q-1)(q-2) \end{aligned}$$

Induction step Suppose that the formula is true for $n = k - 1$ i.e.

$$h_{k-1,1}(q) = \frac{(q-1)^2}{(q+1)^2} [q^k + k(-1)^k q + (k-1)(-1)^k] + (-1)^{k-1}(q-1)$$

we need to show that the formula holds for $n = k$.

By the previous lemma we have

$$h_{k,1}(q) = g_{k,1}(q) - h_{k-1}(q) - h_{k-1,1}(q)$$

Now we simply substitute the value of $g_{k,1}(q)$ (obtained in the previous lemma (note that the last case applies since $k \geq 2$)), the value of $h_{k-1}(q)$ (derived in theorem 4.15) and the value of $h_{k-1,1}(q)$ (given by the induction hypothesis) and simplify :

$$\begin{aligned} h_{k,1}(q) &= q(q-1) \left[\frac{q^k + (-1)^{k-1}}{q+1} \right] \\ &\quad - (q-1) \left[\frac{q^k + (-1)^{k-1}}{q+1} \right] \\ &\quad - \left\{ \frac{(q-1)^2}{(q+1)^2} [q^k + k(-1)^k q + (k-1)(-1)^k] \right. \\ &\quad \left. + (-1)^{k-1}(q-1) \right\} \end{aligned}$$

$$\begin{aligned}
&= (q-1)^2 \left[\frac{q^k + (-1)^{k-1}}{q+1} \right] \\
&\quad - \frac{(q-1)^2}{(q+1)^2} \left[q^k + k(-1)^k q + (k-1)(-1)^k \right] \\
&\quad + (-1)^k (q-1) \\
&= \frac{(q-1)^2}{(q+1)^2} \left[q^{k+1} + q(-1)^{k-1} + q^k + (-1)^{k-1} \right. \\
&\quad \quad \left. - q^k - k(-1)^k q - (k-1)(-1)^k \right] \\
&\quad + (-1)^k (q-1) \\
&= \frac{(q-1)^2}{(q+1)^2} \left[q^{k+1} + (k+1)(-1)^{k-1} q + k(-1)^{k-1} \right] \\
&\quad + (-1)^k (q-1) \\
&\text{as required}
\end{aligned}$$

□

5. THE ALPERIN CONJECTURE AND THE SPECIAL LINEAR GROUP

This chapter is concerned with finding the number of ordinary characters of any parabolic subgroup of the three dimensional special linear group. This splits naturally into two cases depending on how many solutions there are to the equation $x^3 = 1$.

5.1 Case one: Three does not divide $q - 1$

As in the example of the three dimensional general linear group given in chapter four we first try to calculate the number of ordinary irreducible characters of the Borel subgroup and we begin by proving some simple lemmas

Lemma 5.1: *Consider a p -regular element of the type*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

with $\alpha \in GF(q)$. To be an element of $SL_3(q)$ we must have $\alpha^3 = 1$ which means α must be 1 since we are studying the case where 3 does not divide q . So without loss of generality we may assume that

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

With this g we have that there are five classes of p -elements in $C_B(g)$.

Proof

Obviously $C_B(g) = B$, so what we need to calculate is the number of B -conjugacy classes of U (since U is a Sylow p -subgroup of B). So we need to calculate the number of H -orbits of U -conjugacy classes of U (since $B = HU$). So we need to calculate the number of conjugacy classes of U .

But since the subgroup U of $SL_3(q)$ is isomorphic to the subgroup U of $GL_3(q)$ we can use the calculation of lemma 4.6 to obtain

$$k(U) = q^2 + q - 1$$

Now we need to calculate the number of H -orbits of these classes for which we use a theorem of Glauberman (see reference [Gl]) that has the consequence that the number of U -classes fixed by $h \in H$ is equal to the number of classes of the centralizer in U of h (since $|H|$ and $|U|$ are coprime). So we can calculate the following :-

type of element of H	number of classes of this type	number of U -classes fixed by element
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	$q^2 + q - 1$
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}$ α, α^{-2} distinct	$3(q - 2)$	q
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ α, β, γ distinct $\alpha\beta\gamma = 1$	$(q - 1)^2 - 3(q - 2) - 1$ $= q^2 - 5q + 6$	1

So by Burnside's formula we have :-

$$\begin{aligned} \text{number of } H\text{-orbits of } U\text{-conjugacy classes of } U &= \frac{1}{(q-1)^2} \left[1 \times (q^2 + q - 1) \right. \\ &\quad \left. + 3(q - 2) \times q \right. \\ &\quad \left. + (q^2 - 5q + 6) \times 1 \right] \\ &= 5 \end{aligned}$$

□

Lemma 5.2: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}$$

with α any element of $GF(q)$. Then there are $q - 2$ elements of B of this type and for each such g there are two classes of p -elements in $C_B(g)$.

Proof

The number of matrices of this type arise from the fact that α can be any element of $GF(q)$ except zero (since then the matrix would be singular) or one (since then the matrix would be of the type considered in the previous lemma). To prove the second part of the lemma we simply calculate the centraliser explicitly to get :-

$$C_B(g) = \left\{ \begin{pmatrix} \alpha & \delta & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \alpha, \beta, \gamma \neq 0 \right\}$$

and so g centralizes the p -elements

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

where a is any element of $GF(q)$ which form two conjugacy classes in $C_B(g)$, namely the classes generated by :-

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

□

As before there are three distinct types of conjugacy classes of B with isomorphic centralisers, namely

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}, \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^{-2} & 0 \\ 0 & 0 & \alpha \end{pmatrix} \text{ and } \begin{pmatrix} \alpha^{-2} & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

We will treat these as if they were of the same type and multiply our answers by three in the final calculation.

Lemma 5.3: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$$

with α, β and γ all distinct elements of $GF(q)$ (note that for this to be a conjugacy class of $SL_3(q)$ we must have $\alpha\beta\gamma = 1$).

Then there are $q^2 - 5q + 6$ distinct such g and for each g there is only one class of p -elements in $C_B(g)$.

Proof

To calculate the number of such matrices with distinct elements down the diagonal we simply take the number of matrices with equal elements from $|H|$. Using the results of the above two lemmas we get

$$\begin{aligned} \text{number of such } g &= (q - 1)^2 - 3(q - 2) - 1 \\ &= q^2 - 5q + 6 \end{aligned}$$

The remaining part of the lemma is true since

$$C_B(g) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \alpha, \beta, \gamma \neq 0 \right\}$$

and the only p -element in this set is the identity element. □

We can now proceed to calculate the number of conjugacy classes of the Borel subgroup of $SL_3(q)$.

Theorem 5.4: *The number of ordinary characters of the Borel subgroup of the three dimensional special linear group, $SL_3(q)$ is*

$$k(B) = q^2 + q - 1$$

Proof

We collect together the results of the results of the previous three lemmas and summarise them in the following table :-

type of p -regular element	number of classes of this type	number of classes of p -elements in centraliser
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ α, β, γ distinct	$(q - 2)(q - 3)$	1
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}$ α, α^{-2} distinct	$3(q - 2)$	2
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	5

The set consisting of the matrices in the above table is clearly a set of representatives of the conjugacy classes of p -regular elements of the Borel subgroup of $SL_3(q)$. So we have enough information to use lemma 1.4 with $\pi = \{p\}$, i.e.

$$k(B) = \sum_{(g)} \#(\text{classes of } p\text{-elements of } C_B(g))$$

where (g) runs through a set of representatives for the conjugacy classes of p -regular elements of B . By substituting the above values into the R.H.S. we can calculate the following

$$\begin{aligned} \# \text{ of classes of } B &= 1 \times (q-2)(q-3) + 2 \times 3(q-2) + 5 \times 1 \\ &= (q^2 + q - 1) \\ &\text{as required} \end{aligned}$$

□

The next parabolic subgroup we shall consider is the whole of $SL_3(q)$ which we will denote by G . The calculation of $k(G)$ is large and we will split it up by prefixing the theorem with several lemmas.

Lemma 5.5: *Suppose that*

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

then there are q^2 p -regular classes in the centraliser of this element.

Proof

Since by lemma 1.4, the number of p -regular classes is equal to the number of non-isomorphic simple kG -modules, this result has already been stated as corollary 1.10.

□

Lemma 5.6: *Suppose that*

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

then there is one p -regular class in the centraliser of this element.

Proof

An easy calculation shows that

$$C_G(g) = \left\{ \left(\begin{array}{ccc} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{array} \right) \mid a, b \in GF(q) \right\}$$

From this it is easy to see that the only p -regular element is the identity matrix. \square

Lemma 5.7: *Suppose that*

$$g = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array} \right)$$

then there are $q - 1$ p -regular classes in the centraliser of this element.

Proof

In this case we have

$$C_G(g) = \left\{ \left(\begin{array}{ccc} a & b & c \\ 0 & a & 0 \\ 0 & d & e \end{array} \right) \mid a, b, c, d, e \in GF(q) \right\}$$

The determinant of this matrix is a^2e and so for this matrix to be in the special linear group we must have $e = 1/a^2$.

This centraliser contains the following normal p -subgroup :-

$$H = \left\{ \left(\begin{array}{ccc} 1 & b & c \\ 0 & 1 & 0 \\ 0 & d & 1 \end{array} \right) \mid b, c, d \in GF(q) \right\}$$

So we can choose a set of conjugacy class representatives of p' -elements from the quotient group $C_G(g)/H$. The quotient group is as follows

$$C_G(g)/H = \left\{ \left(\begin{array}{ccc} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & e \end{array} \right) \mid a, e \in GF(q) \right\}$$

The p -regular classes in this quotient group result from different choices of a which can be any non-zero element of $GF(q)$. So there are $q - 1$ choices for a , from which the result follows. \square

Theorem 5.8: *If G denotes $SL_3(q)$ then there are $q^2 + q$ conjugacy classes in G , i.e.*

$$k(G) = q^2 + q$$

Proof

The method that we are going to employ to calculate $k(G)$ is to use lemma 1.4 with π equal to the set of all primes not equal to p , i.e. we will use :-

$$k(G) = \sum_{(g)} \# (\text{classes of } p\text{-regular elements of } C_G(g))$$

where (g) ranges over all the conjugacy classes of p -elements of G .

So we must firstly calculate a set of representatives of the conjugacy classes of p -elements of G . We may assume that all of our representatives are members of a single Sylow p -subgroup of G (since these are conjugate by Sylow's Theorem). So we may assume that we pick our representatives from U , say, and so a typical candidate for a conjugacy class representative is :-

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}$$

with α, β and γ elements of $GF(q)$. The matrices that will result from our calculation are precisely the matrices that appeared in the previous three lemmas, namely :-

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

We now separate the calculation into four cases depending on whether α and γ are zero or non-zero. We will show that in all four cases the resulting matrix is conjugate to one of the above three matrices.

Case 1 $\alpha = \gamma = 0$

In this case we have the matrix

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

with β an element of $GF(q)$.

If $\beta = 0$ then we have the identity matrix which obviously belongs to a conjugacy class of its own. If on the other hand $\beta \neq 0$ then we can conjugate by the matrix

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

to get the matrix

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

and then conjugate by the matrix

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

to get the matrix

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

which is one of our representatives.

Case 2 $\alpha = 0$ and $\gamma \neq 0$

In this case our matrix has the form

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

with β any element of $GF(q)$ and γ any non-zero element of $GF(q)$. So we can conjugate by the matrix

$$\begin{pmatrix} 1 & -\beta/\gamma & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

to yield the matrix

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

which we can conjugate by the matrix

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

to yield the matrix

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

which we can conjugate by

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

to yield the matrix

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

which is one of our candidate conjugacy class representatives.

Case 3 $\alpha \neq 0$ and $\gamma = 0$

In this case our typical matrix has the form

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

where β is any element of $GF(q)$ and α is any non-zero element of $GF(q)$. We can conjugate this by the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \beta/\alpha \\ 0 & 0 & 1 \end{pmatrix}$$

to obtain the matrix

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

which can be conjugated by

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

to yield the matrix

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

which is one of our set of candidate conjugacy class representatives.

Case 4 $\alpha \neq 0$ and $\gamma \neq 0$

In this case our typical matrix has the form

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}$$

with β any element of $GF(q)$ and α, γ any non-zero elements of $GF(q)$.

We can conjugate this matrix by the matrix

$$\begin{pmatrix} 1 & -\beta/\gamma & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

to obtain the matrix

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

Now consider conjugating this by the matrix

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a\alpha & 0 \\ 0 & 0 & a\alpha\gamma \end{pmatrix}$$

to yield the matrix

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

which is the third of the matrices in our set of candidate conjugacy class representatives. For the conjugating matrix to be in $SL_3(q)$ we must have

$$a^3 = \frac{1}{\alpha^2\gamma}$$

which we can solve for a since we are in the case where 3 does not divide $q - 1$.

Now that we know that we have a complete set of representatives of the conjugacy classes of p -elements of $SL_3(q)$ we can summarise the previous three lemmas to obtain a table, knowing that the table is complete.

type of p -element	number of classes of p -regular elements in centraliser
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	q^2
$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	1
$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$q - 1$

So by using lemma 1.4 with π equal to the set of all primes except p , we have

$$\begin{aligned} k(G) &= q^2 + 1 + (q - 1) \\ &= q^2 + q \\ &\text{as required} \end{aligned}$$

□

Now we can go on to calculate the number of ordinary characters of the remaining parabolic subgroups of $SL_3(q)$.

Theorem 5.9: *The number of ordinary characters of both of the maximal parabolic subgroups of $SL_3(q)$ is equal to $q^2 + q - 1$. This can be written as*

$$k(P) = q^2 + q - 1$$

Proof

By arguing as in theorem 4.8 we have that the two maximal parabolic subgroups of $SL_3(q)$ containing the upper triangular matrices are isomorphic. Now we can use the Alperin conjecture (as reformulated in reference [Kn-Ro]) in the form :-

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} k(P_J)$$

We substitute in the values of $k(G)$ and $k(B)$ obtained in the above theorems. We also substitute in the value $f_0(G) = 1$ (an easy calculation using lemma 3.3) to obtain :-

$$1 = q^2 + q - 2 \times k(P) + q^2 + q - 1$$

from which the result follows. □

5.2 Case two: Three divides $q - 1$

This case proceeds in exactly the same manner as the previous case and so we start with some lemmas needed to calculate the number of ordinary irreducible characters of the Borel subgroup of the special linear group.

Lemma 5.10: *Consider a p -regular element of the type*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

with $\alpha \in GF(q)$. To be an element of $SL_3(q)$ we must have $\alpha^3 = 1$ which means α can be any of the three cube roots of unity. So there are three matrices of the above form and for each g of this form there are seven classes of p -elements in $C_B(g)$.

Proof

This element is in the center of B and so the centralizer is the whole of B . So what we need to calculate is the number of B -conjugacy classes of U (since U is a Sylow p -subgroup of B). So we need to calculate the number of H -orbits of U -conjugacy classes of U (since $B = HU$). So we need to calculate the number of conjugacy classes of U . But since the subgroup U of $SL_3(q)$ is isomorphic to the subgroup U of $GL_3(q)$ we can use the calculation of lemma 4.6 to obtain :-

$$k(U) = q^2 + q - 1$$

Now we need to calculate the number of H -orbits of these classes for which we use a theorem of Glauberman (see reference [Gl]) that has the consequence that the number of U -classes fixed by $h \in H$ is equal to the number of classes of the centralizer in U of h (since $|H|$ and $|U|$ are coprime). So we can calculate the following :-

type of member of H	number of classes of this type	number of U -classes fixed by element
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$	3	$q^2 + q - 1$
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}$ α, α^{-2} distinct	$3(q - 4)$	q
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ α, β, γ distinct	$(q - 1)^2 - 3(q - 4) - 3$ $= q^2 - 5q + 10$	1

The entry in the middle of the above table arises from the fact that there are $q - 4$ choices for α (any element of $GF(q)$ except zero or the three cube roots of unity) and the α^{-2} could appear in any of the three columns of the matrix.

By using the values in the above table and Burnside's formula we have :-

$$\begin{aligned} \text{number of } H\text{-orbits of } U\text{-conjugacy classes of } U &= \frac{1}{(q-1)^2} \left[3 \times (q^2 + q - 1) \right. \\ &\quad \left. + 3(q - 4) \times q \right. \\ &\quad \left. + (q^2 - 5q + 10) \times 1 \right] \\ &= 7 \end{aligned}$$

□

Lemma 5.11: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}$$

with α any element of $GF(q)$. Then there are $q - 4$ classes of B of this type and for each such g there are two classes of p -elements in $C_B(g)$.

Proof

The number of matrices of this type arise from the fact that α can be any element of $GF(q)$ except zero (since then the matrix would be singular) or any of the cube roots of unity (since then the matrix would be of the type considered in the previous lemma). To prove the second part of the lemma we simply calculate the centraliser explicitly to get :-

$$C_B(g) = \left\{ \begin{pmatrix} \alpha & \delta & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \alpha, \beta, \gamma \neq 0 \right\}$$

and so g centralizes the p -elements

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

where a is any element of $GF(q)$ which form two conjugacy classes in $C_B(g)$, namely the classes containing the elements :-

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

□

As before there are three distinct types of conjugacy classes of B with isomorphic centralisers, namely

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}, \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^{-2} & 0 \\ 0 & 0 & \alpha \end{pmatrix} \text{ and } \begin{pmatrix} \alpha^{-2} & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$$

We will treat these as if they were of the same type and multiply our answers by three in the final calculation.

Lemma 5.12: *Suppose that*

$$g = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$$

with α, β and γ all distinct elements of $GF(q)$ (note that for this to be a class of B we must have $\alpha\beta\gamma = 1$).

Then there are $q^2 - 5q + 10$ distinct such g and for each g there is only one class of p -elements in $C_B(g)$.

Proof

To calculate the number of such matrices with distinct elements down the diagonal we simply take the number of matrices with equal elements from $|H|$. Using the results of the above two lemmas we get

$$\begin{aligned} \text{number of such } g &= (q-1)^2 - 3(q-4) - 3 \\ &= q^2 - 5q + 10 \end{aligned}$$

The remaining part of the lemma is true since

$$C_B(g) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} : \alpha, \beta, \gamma \neq 0 \right\}$$

and the only p -element in this set is the identity element. □

We can now proceed to calculate the number of conjugacy classes of the Borel subgroup of $SL_3(q)$.

Theorem 5.13: *The number of ordinary characters of the Borel subgroup of the three dimensional special linear group, $SL_3(q)$ is*

$$k(B) = q^2 + q + 7$$

Proof

The results of the previous three lemmas can be summarized as follows :-

type of p -regular element	number of classes of this type	number of classes of p -elements in centraliser
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ α, β, γ distinct	$q^2 - 5q + 10$	1
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha^{-2} \end{pmatrix}$ α, α^{-2} distinct	$3(q - 4)$	2
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$	3	7

The types of matrix in the above table are clearly a set of representatives of the conjugacy classes of p -regular elements of $SL_3(q)$. So we have enough information to use lemma 1.4 with $\pi = \{p\}$, which can be written as

$$k(B) = \sum_{(g)} \#(\text{classes of } p\text{-elements of } C_B(g))$$

where (g) runs through a set of representatives for the conjugacy classes of p -regular elements of B . By substituting in values we get

$$\begin{aligned} \# \text{ of classes of } B &= 1 \times (q^2 - 5q + 10) + 2 \times 3(q - 4) + 7 \times 3 \\ &= q^2 + q + 7 \\ &\text{as required} \end{aligned}$$

□

The next parabolic subgroup we shall consider is the whole of $SL_3(q)$ which we will denote by G . The calculation of $k(G)$ is large and we will split it up by prefixing the theorem with several lemmas.

Lemma 5.14: *Suppose that*

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

then there are q^2 p -regular classes in the centraliser of this element.

Proof

Since by lemma 1.4, the number of p -regular classes is equal to the number of non-isomorphic simple kG -modules, this result has already been stated as corollary 1.10. \square

Lemma 5.15: *Suppose that*

$$g = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix}$$

then there are three p -regular classes in the centraliser of this element.

Proof

An easy calculation shows that

$$C_G(g) = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & \lambda b \\ 0 & 0 & a \end{pmatrix} \mid a, b \in GF(q) \right\}$$

So the p -regular elements in $C_G(g)$ are the diagonal matrices with a cube root of unity down the diagonal as required. \square

Lemma 5.16: *Suppose that*

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

then there are $q - 1$ p -regular classes in the centraliser of this element.

Proof

In this case we have

$$C_G(g) = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & 0 \\ 0 & d & e \end{pmatrix} \mid a, b, c, d, e \in GF(q) \right\}$$

The determinant of this matrix is a^2e and so for this matrix to be in the special linear group we must have $e = 1/a^2$.

This centraliser contains the following normal p -subgroup :-

$$H = \left\{ \begin{pmatrix} 1 & b & c \\ 0 & 1 & 0 \\ 0 & d & 1 \end{pmatrix} \mid b, c, d \in GF(q) \right\}$$

So we can choose a set of conjugacy class representatives of p' -elements from the quotient group $C_G(g)/H$. The quotient group is as follows

$$C_G(g)/H = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & e \end{pmatrix} \mid a, e \in GF(q) \right\}$$

The p -regular classes in this quotient group result from different choices of a which can be any non-zero element of $GF(q)$. So there are $q - 1$ choices for a , from which the result follows. \square

Theorem 5.17: *If G denotes $SL_3(q)$ then there are $q^2 + q + 8$ conjugacy classes in G , i.e.*

$$k(G) = q^2 + q + 8$$

Proof

The proof of this theorem proceeds in exactly the same manner as theorem 5.8. All of the conjugations in that theorem are still valid (i.e. the conjugating matrices are in the special linear group) except for matrix used in the final conjugation of case 4. This was the case of conjugating the element

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

where α and γ are non-zero, to get the matrix

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

This conjugation can no longer be achieved in the special linear group (e.g. the matrix in theorem 5.8 is singular if $3 \mid q - 1$). All is not lost however, we can add an extra degree of freedom to our conjugating matrix to make the determinant one; so we can try conjugating by the matrix

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a\alpha & 0 \\ 0 & 0 & a\alpha\gamma/\lambda \end{pmatrix}$$

to yield the matrix

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

The condition for the conjugating matrix to be in the special linear group in this case is

$$a^3 = \frac{\lambda}{\alpha^2\gamma}$$

For any α, γ there is a choice of λ, a which satisfies this equation (e.g. take $a = 1$ and $\lambda = \alpha^2\gamma$). The problem now is to decide just how few values of λ we need to be able to compute an a for every choice of $\alpha^2\gamma$. We proceed as follows: let $GF(q)^\#$ denote the multiplicative group of the field $GF(q)$. By a standard theorem $GF(q)^\#$ is cyclic (see reference [Li-Ni] page 46, theorem 2.8) so let ζ be a generator. Now we define a subgroup of $GF(q)^\#$ as follows

$$H = \langle \zeta^3 \rangle \quad (\text{the subgroup generated by } \zeta^3)$$

Clearly, this is a proper subgroup of $GF(q)^\#$ since $3 \mid (q-1)$ and we have a coset decomposition

$$GF(q)^\# = H \cup \zeta H \cup \zeta^2 H$$

Note that since every element of H is expressible as x^3 for some x we have that the equation $a^3 = x$ is solvable for every $x \in H$. So we need to pick λ such that

$$\frac{\lambda}{\alpha^2\gamma} \in H$$

and by the above coset decomposition we can do this with $\lambda = 1, \zeta$ or ζ^2 . So we can conjugate any p-element of the above form to one of the following matrices :-

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \zeta \\ 0 & 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \zeta^2 \\ 0 & 0 & 1 \end{pmatrix}$$

We now show that the above matrices are not conjugate in $SL_3(q)$ we consider the effect of conjugating one of the above matrices by a matrix to obtain a matrix of the same form. So we consider the product :-

$$\begin{aligned} & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \lambda' \\ 0 & 0 & 1 \end{pmatrix} \\ \Rightarrow & \begin{pmatrix} a+d & b+e & c+f \\ d+\lambda g & e+\lambda h & f+\lambda i \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & a+b & \lambda'b+c \\ d & d+e & \lambda'e+f \\ g & g+h & \lambda'h+i \end{pmatrix} \end{aligned}$$

This gives nine equations that have to be satisfied, and when this is done we get the following matrix

$$\begin{pmatrix} a & b & c \\ 0 & a & \lambda'b \\ 0 & 0 & a\lambda'/\lambda \end{pmatrix}$$

For this matrix to be in the special linear group we need the following equation to be satisfied

$$\frac{a^3\lambda'}{\lambda} = 1$$

But $a^3 \in H$ since H is the subgroup of $GF(q)^\#$ which contains all the cubes. So for the above matrix to be in the special linear group we need

$$\frac{\lambda'}{\lambda} \in H$$

with $\lambda, \lambda' \in \{1, \zeta, \zeta^2\}$. This forces $\lambda'/\lambda = 1$ since we have the above coset decomposition of $GF(q)^\#$. This gives $\lambda = \lambda'$ and hence the above three matrices are non-conjugate.

By combining the above with the results of the previous three lemmas we get :-

type of p -element	number of p -elements of this type	number of classes of p -regular elements in centraliser
$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	q^2
$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \lambda \\ 0 & 0 & 1 \end{pmatrix}$	3	3
$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	1	$q - 1$

So by using lemma 1.4 with π equal to the set of all primes except p , we have

$$\begin{aligned} k(G) &= q^2 + 3 \times 3 + (q - 1) \\ &= q^2 + q + 8 \\ &\text{as required} \end{aligned}$$

□

Now we can go on to calculate the number of ordinary characters of the remaining parabolic subgroups of $SL_3(q)$.

Theorem 5.18: *The number of ordinary characters of both of the maximal parabolic subgroups of $SL_3(q)$ is equal to $q^2 + q + 7$. This can be written as*

$$k(P) = q^2 + q + 7$$

Proof

By arguing as in theorem 4.8 we have that the two maximal parabolic subgroups of $SL_3(q)$ containing the upper triangular matrices are isomorphic. Now we can use the Alperin conjecture (as reformulated in reference [Kn-Ro]) in the form :-

$$f_0(G) = \sum_{J \subseteq I} (-1)^{|I-J|} k(P_J)$$

We substitute in the values of $k(G)$ and $k(B)$ obtained in the above theorems. We also substitute in the value $f_0(G) = 1$ (an easy calculation using lemma 3.3) to obtain :-

$$1 = q^2 + q + 8 - 2 \times k(P) + q^2 + q + 7$$

from which the result follows. □

BIBLIOGRAPHY

- [Al-Bu] J.L. Alperin, D.W. Burry
Block theory with modules
J. Alg. 65 (1980), 225–233
- [Be-Fe-Ho] D. Benson, W. Feit, R. Howe
Finite linear groups, the Commodore 64, Euler and Sylvester
American Mathematical Monthly (November 1986), 717–719
- [Bo-Ti] A. Borel, J. Tits
Eléments unipotents et sous-groupes paraboliques des groupes réductifs I
Invent. Math. 12 (1971)
- [Bo] S. Bouc
Modules de Möbius
C.R.Acad.Sci. ,Paris sér. 1, 299 (1984), 49–52
- [Br] K. Brown
Euler characteristics of groups : the p -fractional part
Invent. Math. 29 (1975), 1–5
- [Ca1] M. Cabanes
Représentations modulaires et sous-groupes de Levi
Thèse de 3ème cycle, Université Paris VII
- [Ca2] M. Cabanes
Brauer Morphism between Modular Hecke Algebras
J. Alg. 115 (1988), 1–31
- [Car1] R.W. Carter
Finite groups of Lie type
Wiley-Interscience, London, 1972
- [Car2] R.W. Carter
Simple groups of Lie type
Wiley-Interscience, London, 1985

- [Cu] C.W. Curtis
Irreducible representations of finite groups of Lie type
J. für Math. 219 Heft 3/4, 180–199
- [Cu-Re] C.W.Curtis, I.Reiner
Representation theory of finite groups and associative algebras
Interscience, New York, 2nd ed., 1966
- [Do] L. Dornhoff
Group Representation Theory (Part B)
Decker, New York, 1972
- [Fe-Fi] W. Feit, N.J. Fine
Pairs of commuting matrices over a finite field
Duke Math J. 27 (1960), 91–94
- [Fo] P. Fong
Alperin's conjecture for S_m and $GL_m(q)$
preprint
- [Gl] G. Glauberman
Correspondence of characters for relatively prime operator groups
Can. J. Math. 20 (1968), 1465–1488
- [Go] D. Gorenstein
Finite Groups
Harper and Row, New York, 1968
- [Gr1] J.A. Green
The characters of the general linear groups
Trans. A.M.S. 80 (1955), 402–447
- [Gr2] J.A. Green
On the indecomposable representations of a finite group
Math. Z. 70 (1959), 430–445
- [Gr3] J.A. Green
Some remarks on defect groups
Math. Z. 107 (1968) 133–150
- [Is] I.M. Isaacs
Character theory of finite groups
Academic Press, New York, 1976

- [Kn-Ro] R. Knörr and G.R.Robinson
Some remarks on Alperin's conjecture
J. London Math. Soc. (2) 39 (1989), 48–60
- [La] P.Landrock
Finite group algebras and their modules
Cambridge University Press (London Math. Soc. Lecture Note
Series #84), London, 1983
- [Li-Ni] R.Lidl and H.Neiderreiter
Introduction to finite fields and their applications
Cambridge University Press, London, 1986
- [Ok] T. Okuyama
Module correspondences in finite groups
Hokkaido Math. J. 10 (1981), 299–318
- [Ri] F. Richen
Representations of groups with split BN-pairs
Trans. Amer. Math. Soc. 140 (1969) 435–460
- [Ro] G.R.Robinson
A Remark on a Conjecture of Alperin
preprint
- [Sr] Bhama Srinivasan
The characters of the finite symplectic group $SP(4, q)$
Trans. Amer. Math. Soc. 131 (1968) 488–525
- [St] R. Steinberg
Representations of algebraic groups
Nagoya Math. J. 22 (1963), 33–56
- [Ti] J. Tits
BN-pairs of spherical type
Springer-Verlag (Lecture Notes In Mathematics #386), Berlin,
1974