UNIVERSITY OF SOUTHAMPTON

Explicit Brauer Induction and the Glauberman Correspondence

Adam Martin Case

Submitted for the degree of

Doctor of Philosophy

Faculty of Mathematical Studies

March 2002

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF MATHEMATICAL STUDIES

Doctor of Philosophy

EXPLICIT BRAUER INDUCTION AND THE GLAUBERMAN CORRESPONDENCE

by Adam Martin Case

Let S and G be finite groups of coprime order such that S acts on G. If S is solvable, Glauberman [11] proves the existence of a bijection between the $S-$fixed irreducible representations of G and the irreducible representations of G^S.

In the case of G solvable, Isaacs [13] uses a totally different method to prove the existence of a bijection between the same two sets of representations.

Assuming the existence of the Glauberman correspondence, Boltje [5] uses the method of Explicit Brauer Induction (EBI) to give an explicit version of this correspondence for the case in which S is a $p-$group.

After presenting the above results, we outline a strategy for investigating these correspondences using Explicit Brauer Induction, and we use these ideas to give a new proof for the theorems of Glauberman and Boltje. We move on to suggest some ideas of how this work may extend to Isaacs' correspondence. We also mention a link to Shintani's correspondence [25]. In the final chapter, we look at cryptography, and mention a potential application of some of our techniques (Adams Operations) in this field.

Contents

Acknowledgements

I would like to thank my supervisor, Professor Victor Snaith, for his constant ideas, support and encouragement. I would also like to thank the other members of staff of this faculty (both academic and clerical), in particular Dr. Ian Leary, and my advisor, Dr. David Singerman.

I would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council for their financial support.

I am grateful for the support of my fellow students, and to all my friends and family. In particular, I must thank Adrian for the crosswords and lunchtime frivolity, and Ian for the puzzles, without both of whom I probably would have finished some time sooner!

Chapter 1

Introduction

Let S and G be finite groups of coprime order such that S acts on G. If S is solvable, Glauberman [11] proves the existence of a bijection between the $S-$fixed irreducible representations of G and the irreducible representations of G^S.

In the case of G solvable, Isaacs [13] uses a totally different method to prove the existence of a bijection between the same two sets of representations.

Assuming the existence of the Glauberman correspondence, Boltje [5] uses the method of Explicit Brauer Induction (EBI) to give an explicit version of this correspondence for the case in which S is a p-group.

Here, we give a brief introduction to representation theory (together with induced representations and the representation ring), followed by an overview of Explicit Brauer Induction. We then move on to give a description of the Glauberman correspondence, and of Boltje's explicit characterisation.

Chapter 4 outlines a cohomological strategy for dealing with these correspondences, we use these ideas to give a new proof for the theorems of Glauberman and Boltje in Chapter 5, and move on to suggest some ideas

about how the work may extend to Isaacs' correspondence. We also mention a link to Shintani's correspondence. In the final chapter, we look at cryptography, and mention a potential application of some of our techniques (Adams Operations) in this field.

Chapter 2

Representation Theory

We give a brief introduction to representation theory, and the theory of Explicit Brauer Induction.

2.1 Basic Results and Definitions

This section presents the basic results (omitting proofs, etc) on group representation theory needed to work with the Explicit Brauer Induction formula. We only introduce necessary concepts (for example, all representations are taken over the complex numbers, rather than an arbitrary vector space over a field).

Definition 2.1.1 *Let G be a finite group. A (complex) representation of G is a group homomorphism $\rho : G \to GL(V)$ where V is an n-dimensional vector space over $\mathbb{C}$. Two representations ρ, ρ' are equivalent if there exists $T \in GL(V)$ such that $\rho(g) = T^{-1}\rho'(g)T$ for all $g \in G$. The dimension of such a representation,* $\dim(\rho) = n$.

Note that we can choose an isomorphism (by choice of basis) between V and $\mathbb{C}^n$ so $\rho : G \to GL(\mathbb{C}^n) = GL_n(\mathbb{C})$ where $GL_n(\mathbb{C})$ is the group of invertible $n \times n$ matrices over $\mathbb{C}$. We can define an action of G on V as follows: if $g \in G$ and $\mathbf{v} \in V$ then the action induced from a representation ρ is $g \circ \mathbf{v} = \rho(g)(\mathbf{v})$.

Definition 2.1.2 *If $\rho : G \to GL(V)$ is a representation and W is an m-dimensional $\mathbb{C}$-subspace of V which is preserved by the G-action, then the induced homomorphism $\rho' : G \to GL(W)$ is a subrepresentation of G of dimension m. We say W is a subrepresentation of V.*

Definition 2.1.3 *If ρ_1 and ρ_2 are two representations of G with dimensions n_1 and n_2 respectively, $\rho_i : G \to GL_{n_i}(\mathbb{C})$ $(i = 1, 2)$ then we define the direct sum:*

$$\begin{aligned} \rho_1 \oplus \rho_2 \quad &: \quad G \to GL_{n_1+n_2}(\mathbb{C}) \\ (\rho_1 \oplus \rho_2)(g) \quad &= \quad \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix} \end{aligned} \tag{2.1}$$

This is clearly an $(n_1 + n_2)$-dimensional representation of G. The tensor product, $\rho_1 \otimes \rho_2$ is induced from the vector operations in the same way: it has dimension $n_1 \cdot n_2$ and is given by the Kronecker product of ρ_1 and ρ_2.

Theorem 2.1.4 *(Maschke's Theorem) Let $\rho : G \to GL(V)$ be a representation of G and W_1 a subrepresentation. Then there exists a subrepesentation W_2 such that $V = W_1 \oplus W_2$.*

Definition 2.1.5 *If a representation $\rho : G \to GL(V)$ has no subrepresentations except ρ and the zero homomorphism, we say ρ is irreducible. Maschke's theorem tells us that given $V = W_1 \oplus W_2$ for subrepresentations W_1 and W_2, ρ is irreducible if $W_1 = 0$ or V. We write $\rho = \rho_1 \oplus \rho_2$ where ρ_1 and ρ_2 correspond to the subrepresentations for W_1 and W_2 respectively.*

Note that a one-dimensional representation

$$\lambda : G \to GL_1(\mathbb{C}) = \mathbb{C}^* = \mathbb{C} - \{0\} \tag{2.2}$$

is clearly irreducible.

Given a representation ρ, we can apply these results to obtain a decomposition of ρ into a direct sum of its irreducible constituents

$$\rho = \bigoplus_{i=1}^{s} n_i \lambda_i \tag{2.3}$$

where $n_i, s \in \mathbb{N}$ and λ_i are irreducible representations. We now give some further results concerning group characters and irreducible representations, before moving on to look at induced representations.

Definition 2.1.6 *Given a representation ρ, the character of ρ is defined to be the complex-valued function, χ_ρ, given by:*

$$\chi_\rho(g) = Trace(\rho(g)) = \sum_{i=1}^{n} (\rho(g))_{ii} \tag{2.4}$$

Definition 2.1.7 *The Schur Inner Product of two representations ρ, ρ' with characters χ_ρ and $\chi_{\rho'}$ is defined by:*

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_{\rho'}(g)} \tag{2.5}$$

Lemma 2.1.8 *The following results hold for representations ρ and ρ' :*

1. *If ρ, ρ' are equivalent, then $\chi_\rho(g) = \chi_{\rho'}(g)$ for all $g \in G$.*
2. *$\chi_\rho(1) = n$, the dimension of ρ.*
3. *$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$ (complex conjugation)*
4. *$\chi_\rho + \chi_{\rho'}$ is the character of $\rho \oplus \rho'$*
5. *$(\chi_\rho) \cdot (\chi_{\rho'})$ is the character of $\rho \otimes \rho'$*
6. *$\chi_\rho = \chi_{\rho'}$ if and only if $\rho = \rho'$*

Theorem 2.1.9 *The following results hold for representations ρ and ρ' and irreducible representation λ :*

1. *$\langle \chi_\rho, \chi_\lambda \rangle$ is equal to the multiplicity of λ in ρ (the number of times λ appears in the decomposition of ρ as a direct sum of irreducibles, as in 2.1.5).*
2. *$\langle \chi_\rho, \chi_\rho \rangle = 1$ if and only if ρ is irreducible*
3. *$\langle \chi_\rho, \chi_{\rho'} \rangle = \langle \chi_{\rho'}, \chi_\rho \rangle$*

Corollary 2.1.10 *If $\rho_1, ..., \rho_t$ are the distinct irreducible representations of G then:*

$$|G| = \sum_{i=1}^{t} \dim(\rho_i)^2 \tag{2.6}$$

2.2 The representation ring, $R(G)$

Definition 2.2.1 *The complex representation ring of G, denoted by $R(G)$, is defined to be the free abelian group on the complex irreducible representations of G.*

The ring structure on $R(G)$ is defined using the tensor product as follows: in the free abelian group of irreducible representations $\{R_i\}$, we identify a formal sum

$$x = \sum_i \alpha_i R_i \tag{2.7}$$

with a formal difference of representations

$$x = S_+ - S_- \tag{2.8}$$

$$S_+ = \bigoplus_{\alpha_i > 0} \alpha_i R_i \qquad\qquad S_- = \bigoplus_{\alpha_i < 0} (-\alpha_i) R_i \tag{2.9}$$

Similarly, if $y = T_+ - T_- \in R(G)$ we may define the product:

$$xy = [(S_+ \otimes T_+) \oplus (S_- \otimes T_-)] - [(S_+ \otimes T_-) \oplus (S_- \otimes T_+)] \tag{2.10}$$

This is well-defined and makes $R(G)$ into a commutative ring.

2.3 Representations as $\mathbb{C}G$-modules

Lemma 2.3.1 *Representations of a finite group G over $\mathbb{C}$ are equivalent to $\mathbb{C}G$-modules.*

Proof Given a representation $\rho : G \to GL(V)$, where V is an n-dimensional vector space over $\mathbb{C}$, we can define an n-dimensional $\mathbb{C}G$-module by letting G act on V by $g.v = \rho(g).v$. The product extends to elements of $\mathbb{C}G$ in the obvious way:

$$\left(\sum_{g\in G} c_g g\right) v = \sum_{g\in G} c_g \left(\rho(g)v\right) \tag{2.11}$$

Conversely, given a $\mathbb{C}G$-module M, for each $g \in G$ we define $\rho(g) : M \to M$ by $\rho(g)(m) = g \cdot m$. Then $\rho(g) \in GL(V)$ and ρ is a homomorphism because of the multiplication rules imposed by the $\mathbb{C}G$-module structure. ■

Lemma 2.3.2 *If M_1, M_2 are both $\mathbb{C}G$-modules, then $M_1 \cong M_2$ as $\mathbb{C}G$-modules if and only if the corresponding representations ρ_1 and ρ_2 are equivalent.*

Proof Assume $M_1 \cong M_2$ as $\mathbb{C}G$-modules, and let $\pi : M_1 \to M_2$ be the isomorphism. Let M_1 have basis $\{m_1, ..., m_n\}$ and M_2 have basis $\{s_1, ..., s_n\}$. For any $g \in G$ we have:

$$\begin{aligned} g \cdot \pi(m_i) &= \pi(g \cdot s_i) \\ \rho_2(g)\pi(m_i) &= \pi(\rho_1(g)s_i) \end{aligned} \tag{2.12}$$

π is invertible so $\pi^{-1}\rho_2(g)\pi = \rho_1(g)$, and the result follows by taking the matrix T of π in the basis given, so $T^{-1}\rho_2(g)T = \rho_1(g)$ with $T \in GL_n(\mathbb{C})$ as required. The converse is obtained by applying the same argument in reverse. ■

We see from these results that we can consider all representations of G as $\mathbb{C}G$-modules. We can show that the *irreducible* representations of G correspond to the *simple* $\mathbb{C}G$-modules (modules with no proper submodules)

and study representations in this new way (the approach followed in Leary [17]). We have introduced this in order to give the definition of induced representations.

2.4 Induced Representations

Definition 2.4.1 *Suppose H is a subgroup of G. A representation ρ of H is equivalent to a left $\mathbb{C}H$-module M from the results above. $\mathbb{C}G$ is both a left $\mathbb{C}G$-module and a right $\mathbb{C}H$-module, so the tensor product*

$$\mathbb{C}G \otimes_{\mathbb{C}H} M \tag{2.13}$$

is another (left) $\mathbb{C}G$-module, and is therefore equivalent to a representation of G. We call this the representation of G induced from ρ, and denote by $Ind_H^G(\rho)$.

Definition 2.4.2 *If H is a subgroup of G and $\rho : G \to GL(V)$ is a representation, then $\rho\,|_H : H \to GL(V)$ is a representation of H. We call this the restriction of ρ to H, denoted by $Res_H^G(\rho)$.*

There are several useful results (including Frobenius reciprocity) which can be obtained by combining the *Ind* and *Res* maps, which are stated and proved in Snaith [28] and Leary [17] which we will not repeat here.

2.5 Explicit Brauer Induction

We present a summary of results from Snaith [28] and Boltje [5] to introduce the method of Explicit Brauer Induction.

Definition 2.5.1 *For a finite group G, let $R_+(G)$ denote the free abelian group on G-conjugacy classes of one-dimensional representations $\lambda : H \to \mathbb{C}^*$, where $H \leq G$. We denote this element by (H, λ) and its conjugacy class by $(H, \lambda)^G \in R_+(G)$, where the action of G is given by $g \circ (H, \lambda) \stackrel{def}{=} (gHg^{-1}, g^{-1} * \lambda)$, with $g^{-1} * \lambda(h) \stackrel{def}{=} \lambda(g^{-1}hg)$, for all $g \in G, h \in H$.*

More specifically, for any finite group G, we define $\widehat{G}$ to be the multiplicative group of one dimensional representations of G, $Hom(G, \mathbb{C}^*)$. Let $\widehat{R}(G)$ be the $\mathbb{Z}$ -span of $\widehat{G}$, and $M(G) = \{(H, \lambda) \mid H \leq G, \lambda \in \widehat{H}\}$.

We see $M(G)$ is a $\mathbb{Z}$-basis for $\bigoplus_{H \leq G} \widehat{R}(H)$ on which G acts by conjugation, and this basis is invariant with respect to this action, as gHg^{-1} is another subgroup of G, and $g^{-1} * \lambda$ maps an element $ghg^{-1} \in gHg^{-1}$ to $\lambda(h)$. We write $(H, \lambda)^G$ for the G-orbit of $(H, \lambda) \in M(G)$.

We can now define $R_+(G)$ as the free abelian group on the elements $(H, \lambda)^G \in G \backslash M(G)$ as in definition 2.5.1. Snaith [28] demonstrates how a product can be defined on $R_+(G)$ to give it a ring structure, and we give several properties of $R_+(G)$ from Snaith [28]:

Definition 2.5.2 *For $J \leq G$, we can define an induction map:*

$$Ind_J^G : R_+(J) \to R_+(G), \text{ given by } Ind_J^G((H, \lambda)^J) = (H, \lambda)^G \qquad (2.14)$$

We also define the following map:

$$b_G : R_+(G) \to R(G), \qquad (H,\lambda)^G \to Ind_H^G(\lambda) \tag{2.15}$$

Using the ring structure on $R_+(G)$ mentioned above, we can show that b_G is a ring homomorphism on $R_+(G)$. The Brauer Induction Theorem (2.1.20 of [28]) gives that it is surjective.

Definition 2.5.3 *For $J \leq K \leq G$, define a restriction map:*

$$Res_J^K : R_+(K) \to R_+(J) \tag{2.16}$$

by the double-coset formula:

$$(H,\lambda)^K \to \sum_{z \in J\backslash K/H} (J \cap zHz^{-1}, Res^{zHz^{-1}}_{J\cap zHz^{-1}}(z^{-1} * \lambda))^J \tag{2.17}$$

We can show that the maps $\{b_G\}$ commute with these restriction maps (see for example [5].

The next theorem effectively gives an inverse map $a_G : R(G) \to R_+(G)$ such that $b_G a_G = 1$, this is the canonical form for Brauer Induction. We also give properties of the map a_G which we will use in order to calculate this map explicitly for given groups. The version of this theorem we state is taken from Boltje [5], however it was first discovered in Snaith [31] (see also [30]), improved upon in [4] and [3] and developed and applied in [6],[27],[32], and [28].

Theorem 2.5.4 *If G is a finite group, there is a unique family of maps $a_G : R(G) \to R_+(G)$ such that for $H \leq G$, the following diagram commutes:*

$$\begin{array}{ccc} R(G) & \xrightarrow{\quad a_G \quad} & R_+(G) \\ \Big\downarrow{\scriptstyle Res^G_H} & & \Big\downarrow{\scriptstyle Res^G_H} \\ R(H) & \xrightarrow{\quad a_H \quad} & R_+(H) \end{array} \tag{2.18}$$

Moreover, if $(H, \lambda) \in M(G)$ and $\rho \in R(G)$, and the coefficient of $a_G(\rho)$ at the basis element $(H, \lambda)^G$ of $R_+(G)$ is denoted by $\alpha_{(H,\lambda)}(\rho) \in \mathbb{Z}$, so:

$$a_G(\rho) = \sum_{(H,\lambda) \in G \backslash M(G)} \alpha_{(H,\lambda)}(\rho)(H, \lambda)^G \in R_+(G) \tag{2.19}$$

then:

1. $b_G a_G = 1_{R(G)}$
2. *For all $\lambda \in \widehat{G}$ we have $a_G(\lambda) = (G, \lambda)^G$*
3. *If ρ is a representation of G and $(H, \lambda) \in M(G)$ then $\left\langle \lambda, Res^G_H(\rho) \right\rangle = 0$ implies $\alpha_{(H,\lambda)}(\rho) = 0$*
4. *If $\rho \in R(G)$ and $(H, \lambda) \in M(G)$ then $\alpha_{(H,\lambda)}(\rho) \neq 0$ implies $Z(G) \leq H$ (where $Z(G)$ denotes the centre of G)*
5. *For any automorphism $\sigma : G \to G$ and any $\rho \in R(G)$ we have $a_G(\sigma \circ \rho) = \sigma^{-1} \circ a_G(\rho)$ where:*

$$\sigma \circ \rho(g) \stackrel{def}{=} \rho(\sigma(g)), \text{ and } \rho \circ (H, \lambda)^G \stackrel{def}{=} (\rho(H), \rho^{-1} \circ \lambda)^G \tag{2.20}$$

6. *For any $\rho \in R(G)$ we have*

$$\sum_{(H,\lambda)^G \in G \backslash M(G)} \alpha_{(H,\lambda)}(\rho) = \rho(1) \tag{2.21}$$

We also give one further result from Snaith [28]:

Corollary 2.5.5 *If* $\rho \in R(G)$ *and* $(H, \lambda) \in M_G$ *is an element which is maximal among those satisfying* $\langle \lambda, Res^G_H(\rho) \rangle \neq 0$ *then:*

$$\alpha_{(H,\lambda)^G}(\rho) = \langle \lambda, Res^G_H(\rho) \rangle \cdot ([N_G(H, \lambda) : H])^{-1} \tag{2.22}$$

(we use the term 'maximal' in the sense that $(H', \lambda') \leq (H, \lambda)$ *if and only if* $H' \leq H$ *and* $Res^H_{H'}(\lambda) = \lambda'$*) where* $N_G(H, \lambda)$ *is the set* $\{g \in G \mid \lambda(ghg^{-1}) = \lambda(h)$ *for all* $h \in H\}$.

Chapter 3

Glauberman's Correspondence

Let G and S be finite groups of coprime order, and assume S is a solvable group acting on G. After some preliminary results concerning the existence of extensions, we give a characterisation of the Glauberman correspondence (first described in [11]), a bijective correspondence between $Irr(G)^S$ and $Irr(G^S)$ for special cases of S. We then show how Boltje [5] used the methods of Explicit Brauer Induction along with Glauberman's proofs to create an explicit form of this correspondence for the case in which the most explicit characterisation exists, when S is a p–group, and we briefly give some examples to illustrate this (later we will present a new proof of Glauberman's results for the special cases mentioned above, and show how this extends to all solvable groups S).

3.1 Extensions of representations

For an irreducible representation ρ of G, the existence of a unique (canonical) extension to the semi-direct product $S \ltimes G$ (for an appropriate S acting on G) is well-known. We will give a version of the proof from Glauberman [11].

Definition 3.1.1 *Let $S \ltimes G$ be the semi-direct product with respect to the action of S on G, the cartesian product of S and G with multiplication defined as*

$$(s_1, g_1)(s_2, g_2) = (s_1 s_2, g_1 s_1(g_2)) \text{ for all } s_1, s_2 \in S \text{ and } g_1, g_2 \in G \tag{3.1}$$

Consider the $\mathbb{Z}[S]-$module given by $R_+(G)$. If $s \in S$, $s\,(H, \phi)^G$ is the $G-$conjugacy class of $s\,(\phi) : s(H) \to \mathbb{C}^*$ given by $s\,(\phi)\,(s\,(h)) = \phi\,(h)$, for $h \in H$.

If we have a commutative diagram with G acting by conjugation as above:

$$\begin{array}{ccc} H & \xrightarrow{g\_g^{-1}} & gHg^{-1} \\ & {\scriptstyle\phi}\searrow \quad \swarrow{\scriptstyle\psi} & \\ & \mathbb{C}^* & \end{array} \tag{3.2}$$

then:

$$\begin{array}{ccc} s(H) & \xrightarrow{s(g)\_s(g)^{-1}} & s(gHg^{-1}) \\ & {\scriptstyle s(\phi)}\searrow \quad \swarrow{\scriptstyle s(\psi)} & \\ & \mathbb{C}^* & \end{array} \tag{3.3}$$

commutes because:

$$s(\phi)(s(h)) = \phi(h) = \psi(ghg^{-1}) = s(\psi)(s(g)s(h)s(g)^{-1}) \tag{3.4}$$

This shows that S acts on $R_+(G)$.

Theorem 3.1.2 *(Glauberman) Let S act on G with $(|G|, |S|) = 1$. If $\rho \in Irr(G)$ such that for all $s \in S$, ρ is equivalent to ρ_s given by:*

$$\rho_s(g) = \rho(s(g)) \tag{3.5}$$

then there exists a unique representation $\tilde{\rho} \in R(S \ltimes G)$ such that $\tilde{\rho}(g) = \rho(g)$ for all $g \in G$ and $det(\tilde{\rho}(s)) = 1$ for all $s \in S$.

Proof

For $s \in S$, there exists a matrix $M_s \in GL_r(\mathbb{C})$ (where r is the degree of ρ) such that:

$$\rho_s(g) = \rho(s(g)) = M_s^{-1}\rho(g)M_s \tag{3.6}$$

for all $g \in G$. Take $s, t \in S$ and $g \in G$. Then:

$$M_{st}^{-1}\rho(g)M_{st} = \rho(st(g)) = \rho(s(t(g))) = M_s^{-1}\rho(t(g))M_s = M_s^{-1}M_t^{-1}\rho(g)M_tM_s \tag{3.7}$$

thus $M_tM_sM_{st}^{-1}$ centralizes $\rho(g)$ for all $g \in G$. As $\rho \in Irr(G)$, $M_tM_sM_{st}^{-1}$ is a scalar multiple of the identity, by Schur's Lemma.

Take $c_{s,t} \in \mathbf{C}$ such that:

$$M_tM_s = c_{s,t}M_{st} \tag{3.8}$$

Now let $d(s) = det(M_s)$ for all $s \in S$. From 3.8 we see:

$$d(t)d(s) = c_{s,t}^r d(st) \tag{3.9}$$

and:

$$\begin{aligned} c_{s,t}c_{u,st} &= M_tM_sM_{st}^{-1}M_{st}M_uM_{ust}^{-1} \\ &= M_tM_sM_uM_{ust}^{-1} \\ &= M_tM_sM_uM_{us}^{-1}M_{us}M_{ust}^{-1} \\ &= M_tc_{u,s}M_{us}M_{ust}^{-1} \\ &= c_{us,t}c_{u,s} \end{aligned} \tag{3.10}$$

Hence we see:

$$c_{s,t}c_{u,st} = c_{us,t}c_{u,s} \tag{3.11}$$

Let $e(t) = \prod_{s\in S} c_{s,t}$ for all $t \in S$. Multiplying each side of 3.11 over all $u \in S$ gives, where $|S| = n$:

$$c_{s,t}^n e(st) = e(t)e(s) \tag{3.12}$$

n and r are coprime, so there exists integers i, j such that $in + jr = 1$. Let $f(s) = d(s)^j e(s)^i$ for $s \in S$. Equations 3.11 and 3.12 give:

$$\begin{aligned} c_{s,t} &= (c_{s,t})^{in+jr} = (c_{s,t})^{in}(c_{s,t})^{jr} \\ &= (c_{s,t}^n)^i(c_{s,t}^r)^j = (e(t)e(s)e(st)^{-1})^i(d(t)d(s)d(s,t)^{-1})^j \\ &= d(s)^j e(s)^i d(t)^j e(t)^i d(st)^{-j} e(st)^{-i} \\ &= f(s)f(t)f(st)^{-1} \end{aligned} \tag{3.13}$$

Define $M'_s = f(s)^{-1}M_s$ for $s \in S$. From 3.8 and 3.13, $M'_{st} = M'_tM'_s$ for all $s, t \in S$. For each $s \in S$, let $d'(s) = det(M'_s)$ and $M''_s = d'(s)^{-j}M'_s$.

For $g \in G$ and $s, t \in S$ we see:

$$M_s''^{-1}\rho(g)M''_s = M_s{}^{-1}\rho(g)M_s = \rho(s(g)) \tag{3.14}$$

and

$$M''_s M''_t = M''_{ts} \tag{3.15}$$

so that

$$det(M''_s) = (d'(s)^{-j})^r d'(s) = d'(s)^{in} = d'(s^n)^i = d'(1)^i = 1 \tag{3.16}$$

We define $\tilde{\rho}$ by $\tilde{\rho}(s,g) = M''_s \rho(g)$ for all $s \in S$ and $g \in G$.

We show $\tilde{\rho}$ is unique: let $\tilde{\tau}$ be another representation such that $\tilde{\tau}(g) = \tilde{\rho}(g) = \rho(g)$ for all $g \in G$ and $det(\tilde{\tau}(s)) = 1$ for all $s \in S$. For $s \in S$ and each $g \in G$ we see:

$$\rho(s(g)) = \tilde{\rho}(s)^{-1}\rho(g)\tilde{\rho}(s) = \tilde{\tau}(s)^{-1}\rho(g)\tilde{\tau}(s) \tag{3.17}$$

So $\tilde{\rho}(s)\tilde{\tau}(s)^{-1}$ centralizes $\rho(g)$ for every $g \in G$. ρ is irreducible hence there exists $h(s) \in \mathbb{C}$ such that $\tilde{\tau}(s) = h(s)\tilde{\rho}(s)$. By comparing determinants, we see $h(s)^r = 1$. $\tilde{\rho}(1) = \tilde{\tau}(s)^n = h(s)^n \tilde{\rho}(s)^n = h(s)^n \rho(1)$ hence $h(s)^n = 1$. We see $h(s) = h(s)^{in+jr} = 1^{i+j} = 1$.

Take $s \in S$ and $g \in G$ then $\tilde{\tau}(s,g) = \tilde{\tau}(s)\rho(g) = \tilde{\rho}(s)\rho(g) = \tilde{\rho}(s,g)$. ■

Definition 3.1.3 *Let m be an integer, and ρ an irreducible character of G. Denote by $\mathbb{Q}_m$ the field obtained by adjoining the complex m-th roots of unity to $\mathbb{Q}$, and let $\mathbb{Q}(\rho)$ be the field obtained by adjoining the values of ρ to $\mathbb{Q}$.*

Theorem 3.1.4 *Let $\rho \in Irr(G)^S$:*

a. There exists a unique $\tilde{\rho} \in Irr(S \ltimes G)$ such that $Res_G^{S \ltimes G}(\tilde{\rho}) = \rho$ and $det(\tilde{\rho}(s)) = 1$ for all $s \in S$.

b. If $\tilde{\rho}$ satisfies (a) then $\mathbb{Q}(\tilde{\rho}) = \mathbb{Q}(\rho)$ and $\tilde{\rho}(s) \in \mathbb{Q}$ for all $s \in S$.

c. Assume $\tilde{\rho}$ satisfies (a). If $\tilde{\phi} \in Irr(S \ltimes G)$ and ρ is a constituent of $Res_G^{S \ltimes G}(\tilde{\phi})$, then there exists a unique $\beta \in Irr(S \ltimes G/G)$ such that $\beta \otimes \rho$ is an irreducible character of $S \ltimes G$ and ρ is a constituent of $Res_G^{S \ltimes G}(\beta \otimes \rho)$.

Proof

a. The degree of ρ divides $|G|$ and is coprime to $|S| = n$. Take $\tilde{\rho}$ as in Theorem 3.1.2.

b. $Res_G^{S \ltimes G}(\tilde{\rho}) = \rho$, so $\mathbb{Q}(\rho) \subseteq \mathbb{Q}(\tilde{\rho})$. Conversely for every automorphism σ of $\mathbb{Q}_{|G|n}$ that fixes elements of $\mathbb{Q}(\rho)$, $\sigma(\tilde{\rho})$ is an irreducible character of $S \ltimes G$ such that $Res_G^{S \ltimes G}(\sigma(\tilde{\rho})) = \sigma(\rho) = \rho$, so we see $det(\sigma(\tilde{\rho}))(s) = \sigma(1) = 1$ for all $s \in S$. Hence $\sigma(\tilde{\rho}) = \tilde{\rho}$ and $\mathbb{Q}(\tilde{\rho}) \subseteq \mathbb{Q}(\rho)$.

Take $s \in S$ then $\tilde{\rho}(s) \in \mathbb{Q}(\tilde{\rho}) \cap \mathbb{Q}_n = \mathbb{Q}(\rho) \cap \mathbb{Q}_n \subseteq \mathbb{Q}_{|G|} \cap \mathbb{Q}_n = \mathbb{Q}$.

c. $S \ltimes G$ fixes ρ by the hypothesis, and by Frobenius Reciprocity, $\tilde{\phi}$ is a constituent of $Ind_G^{S \ltimes G}(\rho)$, and the result follows immediately from Theorem 2 of [10]. ■

Definition 3.1.5 *For $\rho \in Irr(G)^S$, the unique extension described above, $\tilde{\rho} \in Irr(S \ltimes G)$ is called the canonical extension of ρ.*

We give one further property of the canonical extension.

Lemma 3.1.6 *Let S be cyclic and $\rho \in Irr(G)^S$. If $s \in S$ is a generator, and a an integer prime to $|S| = n$, then:*

$$\tilde{\rho}(s,t) = \tilde{\rho}(s^a,t) \tag{3.18}$$

for all $t \in G^S$.

Proof Choose integers α and β such that $\alpha|G| + \beta|S| = 1$, and let $b = a + \beta|S|(1-a)$, so we see $b \equiv 1 \pmod{|G|}$, $b \equiv a \pmod{n}$ and b is prime to the order of $S \ltimes G$.

Consider the action of the element σ of $Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$ which sends ξ_n (a primitive $n-$th root of unity) to $(\xi_n)^b$ and fixes all roots of unity prime to n.

Thus σ fixes every element of $\mathbb{Q}_{|G|}$ and as $\mathbb{Q}(\tilde{\rho}) \subseteq \mathbb{Q}_{|G|}$, $\sigma(\tilde{\rho}) = \tilde{\rho}$.

For $g \in G$, $\sigma(\tilde{\rho}(s,g)) = \tilde{\rho}(s,g)$, and for $t \in G^S$ we see:

$$\tilde{\rho}(s,t) = \sigma(\tilde{\rho}(s,t)) = \tilde{\rho}((s,t)^b) = \tilde{\rho}(s^b,t^b) = \tilde{\rho}(s^b,t) = \tilde{\rho}(s^a,t) \tag{3.19}$$

■

3.2 Characterisation of Glauberman's Correspondence

With G and S as above, the necessary facts about Glauberman's correspondence can be summarised in the following results from Glauberman [11]:

Lemma 3.2.1 *Let S be cyclic, and ρ an irreducible representation of G such that $s \circ \rho = \rho$ for all $s \in S$ (ie $\rho \in Irr(G)^S$). Then (using the notation above) there exists a unique sign $\epsilon = \pm 1$ and a unique $\lambda \in Irr(G^S)$ such that*

$$\tilde{\rho}(s,t) = \epsilon\lambda(t), \tag{3.20}$$

for all s which generate S, and all $t \in G^S$. Moreover, for every $\lambda \in Irr(G^S)$, there exists a unique $\rho \in Irr(G)^S$ which corresponds to λ as in Equation 3.20.

Lemma 3.2.2 *Let S be a p-group, and $\rho \in Irr(G)^S$. If*

$$Res^G_{G^S}(\rho) = n_1\lambda_1 + ... + n_t\lambda_t, \tag{3.21}$$

where λ_j are distinct irreducible representations of G^S, there exists a unique i such that $p \nmid n_i$. Moreover, $n_i \equiv \pm 1 \pmod{p}$.

Theorem 3.2.3 *If S is solvable, then there is a unique bijection*

$$\pi^{S,G} : Irr(G)^S \to Irr(G^S), \tag{3.22}$$

called the Glauberman correspondence, satisfying the following conditions:

1. *If $T \trianglelefteq S$, then $\pi^{T,G}\left(Irr\,(G)^S\right) = Irr(G^T)^S$ and $\pi^{S,G} = \pi^{S/T,G^T} \circ \pi^{T,G}$.*
2. *If S is a p-group and $\rho \in Irr(G)^S$, then $\pi^{S,G}(\rho)$ is the unique irreducible constituent λ_i of $Res^G_{G^S}(\rho)$ with $p \nmid n_i$ (using the notation from Lemma 3.2.2).*

3.3 Boltje's Explicit Characterisation

This section contains a summary of the work done by Boltje [5] to obtain an explicit formula for the Glauberman correspondence, when S is a p-group. We give Boltje's results here, later we will return to this correspondence and use our results from Section 4 to give our own proof of Boltje's main result. Boltje's treatment assumes the existence of the Glauberman correspondence, but our treatment does not: we give a new proof using Explicit Brauer Induction.

For $\rho \in Irr(G)$ we define $Tr_S(\rho)$ to be the S-orbit sum of ρ, ie

$$Tr_S(\rho)(g) = \sum_{s \in \frac{S}{Stab_S(\rho)}} s \circ \rho(g) = \sum_{s \in \frac{S}{Stab_S(\rho)}} \rho(s(g)) \tag{3.23}$$

We note that $Tr_S(\rho) \in R(G)^S$. If ρ runs through a set of orbit representatives of the S-orbits $S\backslash Irr(G)$ of $Irr(G)$, then the elements $Tr_S(\rho)$ form a $\mathbb{Z}$-basis of $R(G)^S$, and we write $R(G)^S_{<S}$ for the $\mathbb{Z}$-span of the elements $Tr_S(\rho)$ with $\rho \in Irr(G)$ with $Stab_S(\rho) < S$. Then we have:

$$R(G)^S = \mathbb{Z}.Irr(G)^S + R(G)^S_{<S} \tag{3.24}$$

Boltje [5] goes on to derive some consequences of Lemma 3.2.1. We give his proofs in detail because they illustrate how the existence of the Glauberman map is fundamental to Boltje's work:

Proposition 3.3.1 *Let S be a p-group.*

1. *For $\rho \in Irr(G)^S$ with $Stab_S(\rho) < S$ we have:*

$$Res^G_{G^S}(Tr_S(\rho)) \equiv 0 \pmod{pR(G^S)} \tag{3.25}$$

2. *For $\lambda \in Irr(G^S)$ we have $Ind^G_{G^S}(\lambda) \in R(G)^S$, and there is a unique $\rho \in Irr(G)^S$ such that $p \nmid \langle \rho, Ind^G_{G^S}(\lambda) \rangle_G$.*

   Moreover, $\langle \rho, Ind^G_{G^S}(\rho) \rangle_G \equiv \pm 1 \pmod{p}$.

3. *For $\lambda \in R(G^S)$ we have*

$$Res^G_{G^S}(Ind^G_{G^S}(\lambda)) \equiv \lambda \pmod{pR(G^S)} \tag{3.26}$$

4. *For $\rho \in R(G)^S$ we have*

$$Ind^G_{G^S}(Res^G_{G^S}(\rho)) \equiv \rho \pmod{pR(G)^S + R(G)^S_{<S}} \tag{3.27}$$

Proof

1. Let $T = Stab_S(\rho)$. We see:

$$\begin{aligned} Res^G_{G^S}(Tr_S(\rho)) &= \sum_{s \in S/T} Res^G_{G^S}(s \circ \rho) \\ &= \sum_{s \in S/T} s \circ Res^G_{G^S}(\rho) \\ &= |S/T| \cdot Res^G_{G^S}(\rho) \end{aligned} \tag{3.28}$$

   and $|S/T| \equiv 0 \pmod{p}$, since S is a p–group.

2. For $s \in S$, we see

$$s \circ Ind^G_{G^S}(\lambda) = Ind^G_{G^S}(s \circ \lambda) = Ind^G_{G^S}(\lambda) \tag{3.29}$$

   hence $Ind^G_{G^S}(\lambda) \in R(G)^S$. Now, as the Glauberman map $\pi^{G,S} : Irr(G)^S \to Irr(G^S)$ is bijective, Lemma 3.2.1 gives that λ is the irreducible constituent of $Res^G_{G^S}(\rho)$ for a unique $\rho \in Irr(G)^S$ such that p does not divide its multiplicity, ie

$$p \nmid \left\langle \lambda, Res^G_{G^S}(\rho) \right\rangle_{G^S} = \left\langle Ind^G_{G^S}(\lambda), \rho \right\rangle_G \tag{3.30}$$

   The final part also follows from Lemma 3.2.2.

3. It is sufficient to prove for $\lambda \in Irr(G^S)$. If $\lambda = \pi^{G,S}(\rho)$ for some $\rho \in Irr(G)^S$, then by part 2:

$$Ind^G_{G^S}(\lambda) \equiv \pm\rho \pmod{pR(G)^S + R(G)^S_{<S}} \tag{3.31}$$

   Hence $Res^G_{G^S}(Ind^G_{G^S}(\lambda)) \equiv \lambda \pmod{pR(G)^S}$ by part 1.

4. It is sufficient to prove for $Tr_S(\rho)$ for $\rho \in Irr(G)$, as these elements form a $\mathbb{Z}$-basis for $R(G)^S$. If $Stab_S(\rho) < S$, then:

$$Ind_{G^S}^G(Res_{G^S}^G(Tr_S(\rho))) \in pR(G) \subseteq pR(G)^S + R(G)_{<S}^S, \qquad (3.32)$$

by part 1, and we also have $Tr_S(\rho) \in pR(G)^S + R(G)_{<S}^S$.

If $Stab_S(\rho) = S$ and $\lambda \in Irr(G^S)$ is the Glauberman correspondent of $\rho = Tr_S(\rho)$, then $Res_{G^S}^G(\rho) \equiv \pm\lambda \pmod{pR(G^S)}$ and $Ind_{G^S}^G(\pm\lambda) \equiv \rho \pmod{pR(G)^S + R(G)_{<S}^S}$ from part 2.

Putting these two parts together gives the result for $Tr_S(\rho)$ and hence for ρ.

■

We now have enough background material to deduce the canonical map. Firstly we give some useful results concerning coprime action:

Theorem 3.3.2 *(Schur-Zassenhaus) Let $N \trianglelefteq G$ and G be finite, with either G or G/N solvable. Assume $|N| = n$ and $|G : N| = m$ are coprime. Then G contains subgroups of order m and any two such are conjugate in G.*

Proof See for example [22] ■

Lemma 3.3.3 *(Glauberman [11]) Let S act on G with $(|S|, |G|) = 1$. Assume one of G or S is solvable. Let S and G both act on a set Ω such that:*

a. $s(g(\alpha)) = s(g)(s(\alpha))$ for all $\alpha \in \Omega$, $g \in G$, $s \in S$ and

b. G is transitive on Ω,

then S fixes a point of Ω.

Proof (Proof taken from [13], Lemma 13.8)

Define an action of $S \ltimes G$ on Ω by:

$$(s, g)(\alpha) = s(g(\alpha)) \text{ for } \alpha \in \Omega \tag{3.33}$$

This is an action by condition (a) above. For $\alpha \in \Omega$, let

$$\begin{aligned} H &= \{\text{stabiliser of } \alpha \text{ in } S \ltimes G\} \\ &= \{(s, g) \in S \ltimes G | (s, g)(\alpha) = s(g(\alpha)) = \alpha\} \end{aligned} \tag{3.34}$$

G is transitive on Ω, hence $|\Omega| = |G : G \cap H| = |S \ltimes G : H|$ and hence $|H : G \cap H| = |S|$.

Now, application of Theorem 3.3.2 gives that there exists a subgroup T of order $|G \cap H|$, a complement for $G \cap H$ in H. Then $|T| = |S|$ and T is a complement for G in $S \ltimes G$.

The conjugacy part of Theorem 3.3.2 gives that $S = x^{-1}Tx$ for $x \in S \ltimes G$, hence $S \subseteq x^{-1}Hx$ and S fixes $x(\alpha) \in \Omega$, completing the proof. ■

Corollary 3.3.4 *In the situation of Lemma 3.3.3, the set of $S-$fixed points of Ω is an orbit under the action of G^S.*

Proof (this proof taken from [13], 13.9)

If $\alpha \in \Omega$ is fixed by S and $t \in G^S$ then $s(t(\alpha)) = s(t)(s(\alpha)) = t(\alpha)$ so $t(\alpha)$ is $S-$fixed also.

If $\alpha, \beta \in \Omega$ are both $S-$fixed, then let $X = \{g \in G | g(\alpha) = \beta)\}$. Because the action of G on Ω is transitive, X is a left coset of the set $G_\beta = \{\text{stabiliser of } \beta \text{ in } G\} = \{g \in G | g(\beta) = \beta\}$ and is $S-$fixed.

Let G_β act on X by left multiplication. G_β is $S-$fixed and transitive on X. For $x \in X, g \in G_\beta, s \in S$ we have $s(g(x)) = s(gx) = s(g)s(x) = s(g)(s(x))$

so Lemma 3.3.3 applies to the action of S on G_β and of S and G_β on X. So S fixes some element $x \in X$. Hence $x \in G^S$ and $x(\alpha) = \beta$. ■

Definition 3.3.5 *Using the notation from Section 2.5, we define the map* $bol^{S,G}$ *as the following composition:*

$$bol^{S,G} : R(G)^S \xrightarrow{a_G} R_+(G)^S \xrightarrow{bol_+^{S,G}} R_+(G^S) \xrightarrow{b_{GS}} R(G^S) \tag{3.35}$$

We still have to determine the map $bol_+^{S,G} : R_+(G)^S \to R_+(G^S)$. If $\rho \in R(G)$ is S-fixed (ie $\rho(s \circ g) = \rho(g)$ for all $s \in S$, $g \in G$), then from part 5 of Theorem 2.5.4 we have

$$s \circ a_G(\rho) = a_G(s^{-1} \circ \rho) = a_G(\rho) \tag{3.36}$$

so each S-fixed point of $R(G)$ is mapped under a_G to an S-fixed point of $R_+(G)$ (recall that the action of S on $R_+(G)$ is given by $s \circ (H, \lambda)^G = (s \circ H, s^{-1} \circ \lambda)$, where $s \circ \lambda(g) = \lambda(s \circ g)$, and we see that the basis elements $(H, \lambda)^G$ of $R_+(G)$ corresponding to $G\backslash M(G)$ are permuted by this S–action).

The G-orbit of $(H, \lambda) \in M(G)$ is $\{(gHg^{-1}, g^{-1} * \lambda) \mid g \in G\}$. If

$$\begin{aligned} T &= Stab_S((H, \lambda)^G) \\ &= \{s \in S, (s \circ H, s^{-1} \circ \lambda) = (gHg^{-1}, g^{-1} * \lambda) \ \ for\ some\ g \in G\} \end{aligned} \tag{3.37}$$

then the S-orbit sums

$$\sum_{s \in S/T} s \circ (H, \lambda)^G, \qquad (H, \lambda) \in S \ltimes G\backslash M(G) \tag{3.38}$$

form a $\mathbb{Z}$-basis of $R_+(G)^S$. By considering the action of T and G on (H, λ), the G–action is transitive so we can apply Lemma 3.3.3, hence there exists a T-fixed point (H', λ') in the G-orbit of (H, λ).

ie $t(H',\lambda') = (H',\lambda')$ for all $t \in T$, and $(H,\lambda)^G = (H',\lambda')^G$ with $T = Stab_S((H,\lambda)^G) = Stab_S((H',\lambda')^G)$. We can now define the map:

$$bol_+^{S,G}\left(\sum_{s\in S/T} s\circ(H,\lambda)^G\right) = \begin{cases} (G^S\cap H', Res^{H'}_{G^S\cap H'}(\lambda'))^{G^S}, & if\ T=S \\ 0, & if\ T<S \end{cases} \tag{3.39}$$

If $T = S$, we can write H'^S instead of $G^S \cap H'$. By Corollary 3.3.4, the definition of $bol_+^{S,G}$ does not depend on the choice of the $S-$stable representative (H',λ') we choose from within $(H,\lambda)^G$.

The following results of Boltje [5] show that the map $bol^{S,G}$ can indeed be taken as a definition for the Glauberman correspondence for the case when S is a $p-$group.

Proposition 3.3.6 *Let S be a p-group. For $\rho \in \widehat{G}$ we have:*

$$bol^{S,G}(Tr_S(\rho)) = \begin{cases} Res^G_{G^S}(\rho) = \pi^{S,G}(\rho), & if\ Stab_S(\rho) = S \\ 0, & if\ Stab_S(\rho) < S \end{cases} \tag{3.40}$$

Proof

$$Tr_S(\rho) = \sum_{s\in \frac{S}{Stab_S(\rho)}} s\circ\rho \in R(G)^S \tag{3.41}$$

applying the map a_G to this gives (from part 2 of Theorem 2.5.4):

$$\sum_{s\in \frac{S}{Stab_S(\rho)}} s\circ(G,\rho)^G \tag{3.42}$$

If $Stab_S(\rho) < S$, applying $bol_+^{S,G}$ gives 0 (direct from definition of $bol_+^{S,G}$ given in 3.39). If $Stab_S(\rho) = S$, we get:

$$(G^S\cap G, Res^G_{G^S}(\rho))^{G^S} = (G^S, Res^G_{G^S}(\rho))^{G^S} \in R(G^S) \tag{3.43}$$

Finally, we apply the map b_{G^S} to see $bol^{S,G}(Tr_S(\rho)) = Ind^{G^S}_{G^S} Res^G_{G^S}(\rho) = Res^G_{G^S}(\rho)$ as required. ■

Theorem 3.3.7 *Let S be a p-group.*

1. *For $\rho \in R(G)^S$ we have*

$$bol^{S,G}(\rho) \equiv Res^G_{G^S}(\rho) \pmod{pR(G^S)} \tag{3.44}$$

2. *For $\rho \in R(G)^S_{<S}$ we have*

$$bol^{S,G}(\rho) \equiv 0 \pmod{pR(G^S)} \tag{3.45}$$

Proof Boltje gives full details in [5], we will give a new proof later in Chapter 5. ■

This theorem together with Theorem 2.5.4 shows that the map $bol^{S,G}$ can indeed be used as a definition for the Glauberman correspondence in the case where S is a p-group. However, the Glauberman map is defined for any G and solvable S of coprime order, as we will also see in Chapter 5.

3.4 Examples of the explicit correspondence

We give two examples considered by Boltje.

3.4.1 Example: Quaternion group of order 8

Definition 3.4.1 *Let $G =< a, b \mid a^4 = b^4 = 1, a^2 = b^2, aba^{-1} = b^{-1} >$ be the quaternion group of order 8 and $S =< s \mid s^3 = 1 >$ act on G by $s \circ a = b$, $s \circ b = ab$.*

There are four proper subgroups of G. Let $H_1 =< a >$, $H_2 =< b >$, $H_3 =< ab >$, the three subgroups of order four and $Z = Z(G) =< a^2 >$, the centre of G. Keown [16] gives a detailed exposition for finding the character table of this group (there are five conjugacy classes and hence five irreducible representations: the trivial representation and three further one-dimensional alternating representations, and one irreducible representation ρ of degree 2 with character 2 on the conjugacy class $\{1\}$, -2 on $\{a^2\}$ and 0 on the other conjugacy classes).

We see $G^S = Z$ and $Irr(G)^S = \{1, \rho\}$. If $\lambda_i \in \widehat{H}_i$ and $\tau \in \widehat{Z}$ are irreducible representations of the subgroups then we can calculate the Explicit Brauer Induction formula of G on $\rho \in Irr(G)^S$, (one way is to build a table of $Res^G_H(\rho)$ for all subgroups $H \leq G$ and apply the various parts of Theorem 2.5.4 as outlined in Snaith [28]) which is given by:

$$a_G(\rho) = \sum_{i=1}^{3} (H_i, \lambda_i)^G - (Z, \tau)^G \tag{3.46}$$

Now, observing that $Stab_S(\rho) = S$, so $Tr_S(\rho) = \rho$ and we can apply the map $bol^{S,G}$ to ρ to obtain:

$$\rho \overset{a_G}{\to} \sum_{i=1}^{3} (H_i, \rho_i)^G - (Z, \tau)^G \overset{bol^{S,G}_{+}}{\to} -(Z, Res^G_{G^S}(\tau))^{G^S = Z} \overset{b_{G^S}}{\to} -Ind^Z_Z(\tau) = -\tau \tag{3.47}$$

We also see $Res^G_{G^S}(\rho) = Res^G_Z(\rho) = 2\tau$. We have $p = 3$ and indeed, $p \nmid \langle \tau, Res^G_{G^S}(\rho) \rangle$ as expected. Applying part 2 of Theorem 3.2.3, we see that $\pi^{G,S}(\rho) = 2\tau \equiv -\tau \pmod{p}$ so we do indeed have the correct correspondent.

3.4.2 Example: Extraspecial p-group of order p^{2n+1}

Let G be the extraspecial group of order p^{2n+1} and exponent p for p an odd prime.

Let S be a finite group acting on G such that $(|S|, |G|) = 1$ and such that $G^S = Z$, the centre of G. Dornhoff [8] demonstrates that G has $p-1$ irreducible representations of degree greater than 1 (they all have degree p^n) and that these are all fixed by S. Let $\rho \in Irr(G)$ be one such representation, and we find $Res^G_{GS}(\rho) = p^n\lambda$, where λ is a one-dimensional representation of Z. Applying part 2 of Theorem 3.2.3, we see that $\pi^{G,S}(\rho) = \lambda$. We state a result from Boltje [5]:

Proposition 3.4.2 *With the notation above, the Explicit Brauer Induction formula for ρ is given by:*

$$a_G(\rho) = \sum_{d=0}^{n} \sum_{\substack{Z \leq H \text{ abelian} \\ |H/Z| = p^{n-d}}} (-1)^d p^{d(d-1)} (H, \widetilde{\lambda})^G \tag{3.48}$$

where $\widetilde{\lambda}$ is a one-dimensional representation of H, an arbitrary extension of $\lambda \in Irr(Z)$.

Proof Covered in detail by Boltje [5], using the property that G/Z is a symplectic vector space over Z when it is identified with the field of p elements. ■

The action of S on a representation $\widetilde{\lambda}$ as above gives another extension of λ, which is therefore a $G-$conjugate to $\widetilde{\lambda}$ (using the results of Clifford

theory) hence an element $(H, \widetilde{\lambda})^G$ is fixed by S if and only if H is fixed by S. Hence, applying $bol_+^{S,G}$ to the equation above gives:

$$\sum_{d=0}^{n} \sum_{\substack{Z \leq H \text{ abelian} \\ H \ S-invariant \\ |H/Z|=p^{n-d}}} (-1)^d p^{d(d-1)} (G^S \cap H, Res^H_{G^S \cap H}(\widetilde{\lambda}))^{G^S} \tag{3.49}$$

However, $G^S = Z$ and $Z \leq H$ for each summand so this reduces to:

$$\sum_{d=0}^{n} \sum_{\substack{Z \leq H \text{ abelian} \\ H \ S-invariant \\ |H/Z|=p^{n-d}}} (-1)^d p^{d(d-1)} (Z, Res^H_Z(\widetilde{\lambda}))^Z \tag{3.50}$$

Finally, observing that $Res^H_Z(\widetilde{\lambda}) = \lambda$, we apply b_G to obtain the map $bol^{S,G}$:

$$bol^{S,G}(\rho) = \sum_{d=0}^{n} \sum_{\substack{Z \leq H \text{ abelian} \\ H \ S-invariant \\ |H/Z|=p^{n-d}}} (-1)^d p^{d(d-1)} \cdot \lambda \tag{3.51}$$

We can reduce this by making further assumptions about the action of S, for example if we assume that Z is the only S-stable abelian subgroup containing Z, then $bol^{S,G}(\rho) = (-1)^n p^{n(n-1)} \lambda$. If all abelian subgroups of G containing Z are S-invariant, we can show $bol^{S,G}(\rho) = p^n \lambda$.

Chapter 4

Cohomological Ideas

Throughout this chapter, we let S be a group of order n acting on a finite group G of order prime to n.

Consider the $\mathbb{Z}[S]-$module given by $R_+(G)$ where the action of $s \in S$ given by $s \circ (H, \phi)^G$ is the $G-$conjugacy class of $s(\phi) : s(H) \longrightarrow \mathbf{C}^*$ given by $s(\phi)(s(h)) = \phi(h)$, for $h \in H$.

Recall that ([29] Definition 1.1.2 p.3), if

$$N_S = \sum_{s \in S} s \in \mathbb{Z}[S] \tag{4.1}$$

is the norm element and for a $\mathbb{Z}[S]-$module M,

$$M^S = \{m \in M \mid s(m) = m \ for \ all \ s \in S\} \tag{4.2}$$

is the $S-$fixed points, the $0-$th Tate cohomology group is defined by:

$$\hat{H}^0(S; M) = M^S/(N_S M) \tag{4.3}$$

For any $\mathbb{Z}[S]-$permutation module of the form $M = \bigoplus_i Ind_{S_i}^S(\mathbb{Z})$ we set

$$M_0 = \bigoplus_{i,\ S_i=S} Ind_{S_i}^S(\mathbb{Z}) \tag{4.4}$$

and we have $\mathbb{Z}[S]-$maps:

$$M_0 \xrightarrow{j} M \xrightarrow{\pi} M_0 \tag{4.5}$$

with j the inclusion map and $\pi j = 1$. Also,

$$\hat{H}^0(S;M) \cong \bigoplus_i \mathbb{Z}/|S_i| \underset{j_*}{\overset{\pi_*}{\rightleftarrows}} \hat{H}^0(S,M_0) \cong \bigoplus_{i,\ S_i=S} \mathbb{Z}/|S| \tag{4.6}$$

Specifically, we will apply this to:

$$R_+(G) \cong \bigoplus_{\substack{(H,\phi)^G, \\ J=Stab_S(H,\phi)^G}} Ind_J^S(\mathbb{Z}) \tag{4.7}$$

Hence (the sums are taken over the same elements as above)

$$\begin{aligned} \hat{H}^0(S;R_+(G)) &\cong \hat{H}^0(S;\bigoplus Ind_J^S(\mathbb{Z})) \\ &\cong \bigoplus \hat{H}^0(S;Ind_J^S(\mathbb{Z})) \\ &\cong \bigoplus \mathbb{Z}/|J| \end{aligned} \tag{4.8}$$

From this we see:

$$\hat{H}^0(S;R_+(G)_0) \cong \bigoplus_{\substack{(J,\phi)\in R_+(G), \\ S=Stab_S(J,\phi)^G}} \mathbb{Z}/|S| \tag{4.9}$$

Similarly,

$$\hat{H}^0(S; R_+(G^S)) \cong \bigoplus_{(J,\phi)\in R_+(G^S)} \mathbb{Z}/|S|. \tag{4.10}$$

4.1 Non-Abelian Cohomology

Lemma 4.1.1 *If G is solvable, and $J \subseteq G$ is an $S-$invariant subgroup, then $H^1(S; J) = \{*\}$, the set with one element.*

Proof J is solvable and by induction on $|J|$, we can find a normal subgroup $A \trianglelefteq J$ such that A is abelian, non-trivial and $S-$invariant. The following sequence in non-abelian cohomology is then exact (see [27] Chapter 2):

$$\ldots \longrightarrow H^1(S; A) \longrightarrow H^1(S; J) \longrightarrow H^1(S; J/A) \tag{4.11}$$

The groups S and A have coprime order, hence we see $H^1(S; A)$ is trivial (a well-known fact from abelian cohomology), and the result follows by induction on $|J|$. ■

Lemma 4.1.2 *Let p be a prime not dividing $|G|$ and let S be a p-group acting on G. Then $H^1(S; G) = \{*\}$, the set with one element.*

Proof Let $f : S \longrightarrow G$ be a $1-$cocycle so that $f(s_1.s_2) = f(s_1)s_1(f(s_2))$ for all $s_1, s_2 \in S$. We must find $g \in G$ such that $f(s) = gs(g^{-1})$ for all $s \in S$ ([27] p.37).

Consider the injective homomorphism

$$\Phi : S \longrightarrow S \ltimes G \tag{4.12}$$

given by $\Phi(s) = (s, f(s))$. By Sylow's Theorem, $Im(\Phi)$ is conjugate to $S = \{(s,1) \in S \ltimes G \mid s \in S\}$ in $S \ltimes G$. Therefore there exist $s_0 \in S, g \in G$ such that

$$\begin{aligned}(s_0^{-1}, s_0^{-1}(g^{-1}))(s, f(s))(s_0, g) &= (s_0^{-1}, s_0^{-1}(g^{-1}))(ss_0, f(s)s(g)) \\ &= (s_0^{-1}ss_0, s_0^{-1}(g^{-1})s_0^{-1}(f(s)s(g))) \\ &= (s_0^{-1}ss_0, 1)\end{aligned} \tag{4.13}$$

for all $s \in S$. This implies that $1 = g^{-1}f(s)s(g)$ for all $s \in S$, as required. ■

Lemma 4.1.3 *Let S be a solvable group acting on G, with $(|S|, |G|) = 1$. Then $H^1(S; G) = \{*\}$.*

Proof Let T be a proper abelian normal subgroup of S. Then by Lemma 4.1.2, $H^1(T; G) = \{*\}$. We see from page 73 of [24], that the following sequence in non-abelian cohomology is exact:

$$H^1(S/T; G^T) \longrightarrow H^1(S; G) \longrightarrow H^1(T; G)^{S/T} \tag{4.14}$$

and the map $H^1(S/T; G^T) \longrightarrow H^1(S; G)$ is injective. By induction, $H^1(S/T; G)$ is trivial, hence $H^1(S; G) = \{*\}$ as required. ■

4.1.4 The Feit-Thompson Theorem [9] states that every group of odd order is solvable, so that the condition $(|S|, |G|) = 1$ implies that at least one of S or G must be solvable and by applying Lemmas 4.1.1 and 4.1.3, we see $H^1(S; G) = \{*\}$. We now continue working towards Glauberman's result with results using a solvable S.

4.2 Isomorphism in Tate $\hat{H}^0$

Theorem 4.2.1 *Let S be a $p-$group acting on G of coprime order, and adopting the notation above, the restriction and induction homomorphisms induce inverse modulo p isomorphisms*

$$\hat{H}^0(S; R_+(G)_0) \underset{\pi_*}{\overset{j_*}{\rightleftarrows}} \hat{H}^0(S; R_+(G)) \underset{Ind_{G^S}^G}{\overset{Res_{G^S}^G}{\rightleftarrows}} \hat{H}^0(S; R_+(G^S)) \tag{4.15}$$

Corollary 4.2.2 *With S and G as above, the restriction homomorphism induces a modulo p isomorphism*

$$Res_{G^S}^G : \hat{H}^0(S; R(G)_0) \xrightarrow{\cong} \hat{H}^0(S; R(G^S)) \tag{4.16}$$

Proof

$$\begin{array}{ccc} \hat{H}^0(S; R_+(G)) & \xrightarrow{Res_{G^S}^G} & \hat{H}^0(S; R_+(G^S)) \\ \downarrow b_G \quad \uparrow a_G & & \downarrow b_{G^S} \quad \uparrow a_{G^S} \\ \hat{H}^0(S; R(G)) & \xrightarrow{Res_{G^S}^G} & \hat{H}^0(S; R(G^S)) \end{array} \tag{4.17}$$

By naturality each of the homomorphisms a_G, b_G, a_{G^S} and b_{G^S} is a $\mathbb{Z}[S]$-module homomorphism. By Theorem 2.5.4 and functoriality of b_G all these homomorphisms commute with the restriction homomorphisms. Since $b_G a_G = 1$ and $b_{G^S} a_{G^S} = 1$, the restriction homomorphism on $\hat{H}^0(S; R(G)_0)$ is a natural summand of the restriction homomorphism on $\hat{H}^0(S; R_+(G)_0)$, and is therefore an isomorphism. ■

Theorem 4.2.1 will be proved in 4.2.6 below after a series of preliminary results.

Lemma 4.2.3 *Assuming the situation given in 4.1.3, if S fixes $(H,\psi)^G \in R_+(G)$ then there exists $J \subseteq G$ and $\phi : J \longrightarrow \mathbf{C}^*$ such that $(J,\phi)^G = (H,\psi)^G$ and $s(J,\phi) = (J,\phi)$ all $s \in S$.*

Proof The proof is by direct application of the fixed point Lemma 3.3.3. G and S both act on (H,ψ); the conjugation $G-$action is transitive and we can easily see that condition (a) is met, hence there is an $S-$fixed point (J,ϕ) as required. ■

We note that G does not act on the double-cosets in the next lemma, so we cannot apply Glauberman's Lemma 3.3.3. Instead, we use the non-abelian cohomology results from above.

Proposition 4.2.4 *Assuming the situation given in 4.1.3, suppose that $J \subseteq G$ is a subgroup such that $s(J) = J$ for all $s \in S$. Then*

$$(G^S \backslash G / J)^S = G^S \cdot 1 \cdot J \tag{4.18}$$

the identity double coset.

Proof Assume S is cyclic of order m, generated by an element s. If S fixes a double coset $G^S \cdot z \cdot J$ then there exists $\alpha \in G^S$, $\beta \in J$ such that $s(z) = \alpha z \beta$. Therefore we see that

$$\begin{aligned} s^2(z) &= s(\alpha z \beta) = \alpha \alpha z \beta s(\beta) = \alpha^2 z \beta s(\beta), \\ s^3(z) &= s(\alpha^2 z \beta s(\beta)) = \alpha^3 z \beta s(\beta) s^2(\beta), \\ &\vdots \quad \vdots \quad \vdots \\ z = s^m(z) &= \alpha^m z \beta s(\beta) s^2(\beta) \dots s^{m-1}(\beta) \end{aligned} \tag{4.19}$$

and so $z^{-1}\alpha^{-m}z \in J$. Since $|S| = m$ is prime to the order of α, we find that $z^{-1}\alpha z = z^{-1}s(z)\beta^{-1} \in J$ and so $z^{-1}s(z) \in J$. This holds for all elements of S which means we may define a 1-cocycle, $f : S \longrightarrow J$, by $f(s) = z^{-1}s(z)$ for all $s \in S$. By Lemma 4.1.3, there exists $j \in J$ such that $j^{-1}s(j) = f(s) = z^{-1}s(z)$ for all $s \in S$ and so $zj^{-1} \in G^S$. Hence $\alpha z \beta = \alpha(zj^{-1})(j\beta)$ and this implies that $G^S \cdot z \cdot J = G^S \cdot 1 \cdot J$ as required.

Assume S is non-cyclic, and take $S' \lhd S$ such that S/S' is cyclic. Let

$$X_{S'} = \{G^S \cdot z \cdot J | z \in G^{S'}\} \tag{4.20}$$

we see S/S' acts on $X_{S'}$. We will proceed by induction on $|S|$. Choose S'' such that S''/S' is cyclic. By considering the action of S''/S' on $X_{S'}$, from the argument above if $\alpha \in G^S$, $\beta \in J$ such that $\alpha z \beta \in X_{S'}$ is fixed by S''/S', there exists $j \in J$ such that $zj^{-1} \in G^{S''}$, then $\alpha z \beta = \alpha(zj^{-1})(j\beta)$ and we see $(X_{S'})^{S''/S'} = X_{S''}$. The result then follows by induction. ■

Lemma 4.2.5 *Assuming the situation given in 4.1.3, if* $J', J \subseteq G^S$ *and* $(J,\phi)^G = (J',\phi')^G \in R_+(G)$ *then*

$$(J,\phi)^{G^S} = (J',\phi')^{G^S} \in R_+(G^S). \tag{4.21}$$

Proof By definition, there exists $g \in G$ such that $gJg^{-1} = J'$ and $\phi(j) = \phi'(gjg^{-1})$ for all $j \in J$. Now consider the function, $f : S \longrightarrow G$, given by $f(s) = g^{-1}s(g)$. Define the normaliser of (J,ϕ) in G, $N_G(J,\phi)$, to be the subgroup given by

$$N_G(J,\phi) = \{z \in N_G J \mid \phi(zjz^{-1}) = \phi(j) \ for\ all\ j \in J\}. \tag{4.22}$$

For $j \in J$ we have

$$\begin{aligned} \phi(f(s)jf(s)^{-1}) &= \phi(g^{-1}s(g)j(s(g))^{-1}g) \\ &= \phi(g^{-1}s(gjg^{-1})g) \\ &= \phi'(s(gjg^{-1})) \\ &= \phi'(gjg^{-1}) \\ &= \phi(j) \end{aligned} \tag{4.23}$$

so that f is a 1-cocycle with values in $N_G(J,\phi)$. By Lemma 4.1.3, there exists $g_1 \in N_G(J,\phi)$ such that $g^{-1}s(g) = f(s) = g_1^{-1}s(g_1)$ for all $s \in S$. Hence $g_1 g^{-1} = s(g_1 g^{-1})$ and therefore $g_1 g^{-1} \in G^S$. Hence, for all $j \in J$,

$$\phi(j) = \phi(g_1^{-1}jg_1) = \phi'(gg_1^{-1}jg_1g^{-1}). \tag{4.24}$$

which implies that $(J,\phi)^{G^S} = (J',\phi')^{G^S} \in R_+(G^S)$, as required. ■

4.2.6 *Proof of Theorem 4.2.1*

We have only to show that $Ind_{G^S}^G$ induces a modulo p inverse to $Res_{G^S}^G$ on Tate cohomology in dimension zero.

Given $(H,\psi)^G \in R_+(G)^S$, Lemma 4.2.3 gives that we can find an element (J,ϕ) such that $(H,\psi)^G = (J,\phi)^G$ and $Stab_S(J,\phi) = S$. Proposition 4.2.4 gives that $(G^S\backslash G/J)^S$ is the identity double coset. The following composition

$$\hat{H}^0(S;R_+(G)_0) \xrightarrow{j_*} \hat{H}^0(S;R_+(G)) \xrightarrow{Res_{G^S}^G} \hat{H}^0(S;R_+(G^S)) \xrightarrow{Ind_{G^S}^G} \hat{H}^0(S;R_+(G)) \tag{4.25}$$

on $(H,\psi)^G$ gives

$$\begin{aligned} Ind_{G^S}^G(Res_{G^S}^G(H,\psi)^G) &= Ind_{G^S}^G(Res_{G^S}^G(J,\phi)^G) \\ &= Ind_{G^S}^G\left(\sum_{z\in G^S\backslash G/J}(G^S\cap zJz^{-1},(z^{-1})^*(\phi))^{G^S}\right) \\ &= \sum_{z\in G^S\backslash G/J}(G^S\cap zJz^{-1},(z^{-1})^*(\phi))^G \end{aligned} \tag{4.26}$$

The action of S permutes the terms in this sum, so we can separate the fixed and non-fixed terms, and apply Proposition 4.2.4 to see that there is exactly one fixed double coset:

$$Ind_{G^S}^G(Res_{G^S}^G(J,\phi)^G) = (J,\phi)^G + \sum_{s\in S} s\left(\sum_z (G^S\cap zJz^{-1},(z^{-1})^*(\phi))^G\right) \tag{4.27}$$

where the final sum is taken over appropriate non-fixed double cosets. We see that all the terms in this sum are fixed by the action of S, and because S is a $p-$group, all the $S-$orbits have orbit size a multiple of p. Hence:

$$Ind_{G^S}^{G}(Res_{G^S}^{G}(J,\phi)^G) \equiv (J,\phi)^G \pmod{p} \tag{4.28}$$

Similarly, if $(J,\phi)^{G^S} \in R_+(G^S)$ then

$$\begin{aligned} Res_{G^S}^{G}(Ind_{G^S}^{G}(J,\phi)^{G^S}) &= Res_{G^S}^{G}(J,\phi)^G \\ &= \sum_{z \in G^S \backslash G/J} (G^S \cap zJz^{-1}, (z^{-1})^*(\phi))^{G^S} \end{aligned} \tag{4.29}$$

Applying Proposition 4.2.4, there is exactly one $S-$fixed double-coset; the remaining non-fixed terms appear with order a multiple of p. Combining this with the discussion at the beginning of the chapter, we see $Ind_{G^S}^{G}$ induces a surjection on $\hat{H}^0$. By Lemma 4.2.5, we see that $Ind_{G^S}^{G}$ is one-to-one, which completes the proof.

Corollary 4.2.7 *Let S be a cyclic group acting on G with $(|S|,|G|) = 1$. Then $|Irr(G)^S| = |Irr(G^S)|$.*

Proof Let S be a $p-$group, let $\lambda_1, \ldots, \lambda_t$ denote the irreducible representations of the fixed group G^S and let $\rho_1, \ldots, \rho_{t'}$ denote the S-fixed irreducible representations of G. t counts the irreducible elements of $R(G)$ with stabiliser S, which is the rank of $\hat{H}^0(S; R(G)_0)$. t' is the number of irreducible elements of $R(G^S)$ which is the rank of $\hat{H}^0(S; R(G^S))$. By Corollary 4.2.2, these numbers are equal. If S is cyclic, let $S = S_1 \times S_2$ where $(|S_1|, |S_2|) = 1$. Then we see:

$$|Irr(G)^S| = |(Irr(G)^{S_1})^{S_2}| = |Irr(G^{S_1})^{S_2}| = |Irr(G^{S_1 \times S_2})| \tag{4.30}$$

hence the result follows by induction on $|S|$. ■

Chapter 5

New proofs of Glauberman and Boltje

5.1 Glauberman's Correspondence

Let S be cyclic, let $\lambda_1, \ldots, \lambda_t$ denote the irreducible representations of the fixed group G^S and let $\rho_1, \ldots, \rho_{t'}$ denote the S-fixed irreducible representations of G. By Corollary 4.2.7, $t = t'$.

Let $\tilde{\rho}_i$ be an extension of ρ_i to the semi-direct product, $S \ltimes G$. We shall assume that $\tilde{\rho}_i$ is the *canonical extension* of ρ_i, as given in Section 3.1.

Let $C_G(g)$ denote the centraliser of g in G so that the order of the $G-$conjugacy class of g is equal to $|G|/|C_G(g)|$. The following lemma is from Glauberman ([11], Lemma 2), and we will use this at various stages to switch between Schur inner product calculations over $S \ltimes G$, $S \ltimes G^S$, G and G^S.

Lemma 5.1.1 *Let $T =< s >$ be a cyclic subgroup of S of order n, not dividing $|G|$.*

a. For any $g \in G$ the $T \ltimes G$-conjugacy class of (s, g) contains an element of the form (s, g') with $g' \in G^T$.

b. Let $z, z' \in G^T$. Then (s, z) and (s, z') are conjugate in $T \ltimes G$ iff z and z' are conjugate in G^T.

c. If H is a group and $z \in H$, let $Cl_H(z)$ denote the H-conjugacy class of z. Suppose that $z \in G^T$. Then

$$|Cl_{T \ltimes G}(s, z)| = \frac{|G|}{|G^T|} |Cl_{G^T}(z)| \tag{5.1}$$

Proof

a. Let Ω be the conjugacy class of (s, g) in $T \ltimes G$. T acts on Ω by conjugating elements by $(s, 1)$ and G acts on Ω by conjugation by $(1, z)$ for $z \in G$. It is easy to show that these actions satisfy $s(g(\alpha)) = s(g)(s(\alpha))$ for all $\alpha \in \Omega$, and by application of Lemma 3.3.3 there exists a fixed point (s, g') of Ω with $g' \in G^T$, as required.

b. If $z, z' \in G^T$ are conjugate in G^T then $(s, z), (s, z')$ are clearly $T \times G^T$−conjugate and so are $T \ltimes G$−conjugate.

Conversely, suppose that (s, z) and (s, z') are $T \ltimes G$-conjugate. Since $(s^i, g)(s, z)(s^i, g)^{-1} = (1, g)(s, z)(1, g)^{-1}$, for all $g \in G$ and $1 \leq i \leq n - 1$, we may assume there exists $g \in G$ such that

$$(s, z') = (1, g)(s, z)(1, g)^{-1} = (s, gz)(1, g^{-1}) = (s, gzs(g^{-1})) \tag{5.2}$$

Let k, l be integers such that $k|G| + ln = 1$, hence $k|G| \equiv 1 \pmod{n}$. Since $z \in G^T$, $(s,z)^m = (s^m, z^m)$ for any integer m and we have $(s,z)^{k|G|} = (s,z')^{k|G|} = (s,1)$. Hence

$$\begin{aligned}
(s,1) &= (s,z')^{k|G|} \\
&= ((1,g)(s,z)(1,g)^{-1})^{k|G|} \\
&= (1,g)(s,z)^{k|G|}(1,g)^{-1} \qquad (5.3) \\
&= (1,g)(s,1)(1,g^{-1}) \\
&= (s, gs(g^{-1}))
\end{aligned}$$

which implies that $1 = gs(g^{-1})$ or, equivalently, $g \in G^T$. Therefore $z' = gzs(g^{-1}) = gzg^{-1}$, as required.

c. Setting $z = z'$ in the argument of part (b) shows that $C_{T \ltimes G}(s,z) = T \times C_{G<s>}(z)$ and therefore

$$|Cl_{T \ltimes G}(s,z)| = \frac{n|G|}{|C_{T \ltimes G}(s,z)|} = \frac{n|G|}{n|C_{G^T}(z)|} = \frac{|G|}{|G^T|}|Cl_{G^T}(z)|, \qquad (5.4)$$

as required. ■

We will now work towards a proof of Glauberman's characterisation, Lemmas 3.2.1 and 3.2.2. For simplicity, we first present the working for the situation with S a cyclic group order p^2 before moving on to the general cyclic case, although the method for both cases is the same.

5.1.1 Cyclic groups order p^2

We start, to get the idea, with the case of a cyclic group $S = C_{p^2}$ for a prime p. Let s be a generator of S. The irreducible representations of S are given by powers of the representation y given by $y : s \to e^{2\pi i/p^2}$.

We first consider the Galois orbits of elements of the set $\{y^j | 0 \leq j \leq p^2 - 1\}$ under the action of elements of the Galois group $Gal(\mathbb{Q}(\xi_{p^2})/\mathbb{Q})$ (where ξ_{p^2} is a primitive root of unity). We see there are three orbits, namely:

$$\begin{aligned} y^0 &\to 1 \\ y^1 &\to \sum_{\substack{(k,p^2)=1 \\ 1\leq k\leq p^2-1}} y^k = Ind_1^{C_{p^2}}(1) - Ind_{C_p}^{C_{p^2}}(1) \\ y^p &\to \sum_{\substack{(k,p)=1 \\ 1\leq k\leq p-1}} y^{kp} = Ind_{C_p}^{C_{p^2}}(1) - 1 \end{aligned}$$

Recalling the properties of the canonical extension (Lemma 3.1.6), we see $\tilde{\rho}_j(s^a, g) = \tilde{\rho}_j(s^b, g)$ for any a, b such that s^a and s^b are in the same Galois orbit, and $g \in G^S$. This implies that:

$$\begin{aligned} Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_i) &= a_{i1}(1 \otimes U_{i1}) + a_{i2}((Ind_1^{C_{p^2}}(1) - Ind_{C_p}^{C_{p^2}}(1)) \otimes U_{i2}) \\ &\quad + a_{i3}((Ind_{C_p}^{C_{p^2}}(1) - 1) \otimes U_{i3}) \in R(S) \otimes R(G^S) \\ &= \alpha_{i1}(1 \otimes (U_{i1} - U_{i3})) + \alpha_{i2}(Ind_1^{C_{p^2}}(1) \otimes U_{i2}) + \alpha_{i3}(Ind_{C_p}^{C_{p^2}}(1) \otimes (U_{i2} - U_{i3})) \\ &= \alpha_{i1}(1 \otimes A_i) + \alpha_{i2}(Ind_1^{C_{p^2}}(1) \otimes B_i) + \alpha_{i3}(Ind_{C_p}^{C_{p^2}}(1) \otimes C_i) \end{aligned} \tag{5.5}$$

with U_{ij}, A_i, B_i, C_i virtual representations of G^S and $a_{ij}, \alpha_{ij} \in \mathbb{Z}$ for $1 \leq j \leq 3$.

Considering the values of induced characters, we see that α_{i2} and α_{i3} vanish on the character of this representation on elements $(s^a, g) \in S \times G^S$ with a coprime to p, so for such a choice of a we see:

$$\begin{aligned}\frac{1}{|G^S|}\sum_{g\in G^S} Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_i)(s^a,g)\overline{Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_j)(s^a,g)} &= \frac{1}{|G^S|}\sum_{g\in G^S}\alpha_{i1}A_i(g)\alpha_{j1}\overline{A_j(g)} \\ &= \alpha_{i1}\alpha_{j1}\left\langle A_i(g), A_j(g)\right\rangle_{G^S}\end{aligned} \tag{5.6}$$

We now evaluate this sum differently, to show it is equal to δ_{ij}, by writing the elements of $S \ltimes G$ in a similar way to the Galois orbits above.

$$\begin{aligned}\delta_{i,j} &= \langle\tilde{\rho}_i, \tilde{\rho}_j\rangle_{S\ltimes G} \\ &= \frac{1}{p^2|G|}\sum_{(s^a,g),a=0,\ldots,p^2-1,g\in G}\tilde{\rho}_i(s^a,g)\overline{\tilde{\rho}_j(s^a,g)} \\ &= \frac{1}{p^2|G|}\sum_{g\in G}\rho_i(g)\overline{\rho_j(g)} + \frac{1}{p^2|G|}\sum_{(s^a,g),a=1,\ldots,p^2-1,g\in G}\tilde{\rho}_i(s^a,g)\overline{\tilde{\rho}_j(s^a,g)} \\ &= \frac{\delta_{i,j}}{p^2} + \frac{1}{p^2|G|}\sum_{(s^a,g),a=1,\ldots,p^2-1,g\in G}\tilde{\rho}_i(s^a,g)\overline{\tilde{\rho}_j(s^a,g)} \\ &= \frac{\delta_{i,j}}{p^2} + \frac{1}{p^2|G|}\sum_{\substack{(a,p^2)=1\\ a=1,\ldots,p^2-1},g\in G}\tilde{\rho}_i(s^a,g)\overline{\tilde{\rho}_j(s^a,g)} + \frac{1}{p^2|G|}\sum_{\substack{(a,p)=1\\ a=1,\ldots,p-1},g\in G}\tilde{\rho}_i(s^{ap},g)\overline{\tilde{\rho}_j(s^{ap},g)}\end{aligned} \tag{5.7}$$

From the properties of the canonical extension, each $\tilde{\rho}_i(s^a, g)$ is independent of the choice of a over which the sum is taken. In particular, if we choose a such that $(a, p^2) = 1$, $1 \leq a \leq p^2 - 1$, then by applying lemma 5.1.1 we see:

$$\begin{aligned}
&\frac{1}{|G|}\sum_{g\in G}\tilde{\rho}_i(s^a,g)\overline{\tilde{\rho}_j(s^a,g)} \\
&= \frac{1}{|G|}\sum_{g\in G^S}\frac{|G|}{|G^S|}Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_i)(s^a,g)\overline{Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_j)(s^a,g)} \\
&= \frac{1}{|G^S|}\sum_{g\in G^S}Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_i)(s^a,g)\overline{Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_j)(s^a,g)}
\end{aligned} \tag{5.8}$$

Also, if we choose a such that $(a,p)=1$, $1\leq a\leq p-1$ then we see $< s^{ap} > \cong C_p$, hence (considering the properties of the canonical extension):

$$\begin{aligned}
&\frac{1}{|G|}\sum_{g\in G}\tilde{\rho}_i(s^{ap},g)\overline{\tilde{\rho}_j(s^{ap},g)} \\
&= \frac{1}{|G^{C_p}|}\sum_{g\in G^{C_p}}Res^{S\ltimes G}_{C_p\times G^{C_p}}(\tilde{\rho}_i)(s^{ap},g)\overline{Res^{S\ltimes G}_{S\times G^S}(\tilde{\rho}_j)(s^{ap},g)} \\
&= \frac{1}{|G^{C_p}|}\sum_{g\in G^{C_p}}Res^{C_p\ltimes G}_{C_p\times G^{C_p}}(\tilde{\rho}_i)(s^{ap},g)\overline{Res^{C_p\ltimes G}_{C_p\times G^{C_p}}(\tilde{\rho}_j)(s^{ap},g)} \\
&= \delta_{ij}
\end{aligned} \tag{5.9}$$

Let T_{ij} be the common value of Equation 5.8 for appropriate choice of a, and putting back into 5.7, we see:

$$\delta_{ij} = \frac{\delta_{ij}}{p^2} + \frac{\phi(p^2)}{p^2}T_{ij} + \frac{\phi(p)}{p^2}\delta_{ij}, \tag{5.10}$$

where ϕ is the Euler phi-function. Hence we see $T_{ij}=\delta_{ij}$ as required. Choosing a coprime to p and substituting in Equation 5.6 gives:

$$\delta_{ij} = \alpha_{i1}\alpha_{j1}\left\langle A_i(g), A_j(g)\right\rangle_{G^S} \tag{5.11}$$

Since the α_{ik} are integers, we must have $\langle A_i, A_j\rangle_{G^S} = \delta_{ij}$ and $\alpha_{i1}^2 = \alpha_{j1}^2 = 1$. By Corollary 4.2.7, the distinct irreducible representations,

$\{A_1, \ldots A_t\}$, of G^S must be precisely $\{\lambda_1, \ldots \lambda_t\}$ which implies that there exists a permutation, σ, and a sign $\epsilon_i \in \{\pm 1\}$ such that

$$A_i = \epsilon_i \lambda_{\sigma(i)} \tag{5.12}$$

for $1 \leq i \leq p-1$. Therefore

$$Res^G_{G^S}(\rho_i) = \epsilon_i \lambda_{\sigma(i)} + p^2 \alpha_{i2} B_i + p\alpha_{i3} C_i \equiv \epsilon_i \lambda_{\sigma(i)} \pmod{p} \tag{5.13}$$

which is the required Glauberman correspondence.

5.1.2 General cyclic groups

We now repeat the ideas covered above, but more generally, to give the Glauberman correspondence for all cyclic groups. Let $S =< s >$ be cyclic of order n where $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ for distinct primes p_i. The irreducible representations of S are given by powers of the representation y given by $y : s \to e^{2\pi i/n}$.

We first consider the Galois orbits of elements of the set $\{y^j | 0 \leq j \leq n\}$ under the action of elements of the Galois group $Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$ (where ξ_n is a primitive $n-$th root of unity). There are $(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1)$ such orbits.

For $\beta | n$, the Galois orbit of y^β, G_β is given by

$$G_\beta = \sum_{\substack{(k, \frac{n}{\beta})=1 \\ 1 \leq k \leq \frac{n}{\beta}-1}} y^{\beta k} \tag{5.14}$$

For $\beta | n$, we can use the Artin induction formula (see [28], Theorem 2.1.3) to rewrite each G_β as a sum of induced representations:

$$G_\beta = Ind_{C_\beta}^{C_n}(1) - \sum_{C_\gamma > C_\beta} \mu_\gamma Ind_{C_\gamma}^{C_n}(1) \tag{5.15}$$

where for each γ, μ_γ is an integer (these can calculated using Möbius coefficients but this is not necessary here) with $\mu_\beta = 1$, and the C_γ are cyclic groups. We recall a property of the canonical extension, Lemma 3.1.6: if $s \in S$, $g \in G^S$ and a an integer coprime to the order of s then the character value, $\tilde{\rho}_i(s^a, g)$, is independent of a. Using this and by summing G_β over all $\beta | n$ and gathering together terms, we see:

$$Res_{S \times G^S}^{S \ltimes G}(\tilde{\rho}_i) = \sum_{\beta | n} \alpha_{i\beta}(Ind_{C_\beta}^{C_n}(1) \otimes A_{i\beta}) \tag{5.16}$$

for integers $\alpha_{i\beta}$ and virtual representations $A_{i\beta} \in R(G^S)$ (yet to be determined).

Choose a such that $(a, n) = 1$, and we see all the terms in the sum of Equation 5.16 vanish on s^a except the term $\beta = n$, so:

$$Res_{S \times G^S}^{S \ltimes G}(\tilde{\rho}_i)(s^a, g) = \alpha_{in} A_{in}(g) \tag{5.17}$$

Hence:

$$\begin{aligned} \frac{1}{|G^S|} \sum_{g \in G^S} Res_{S \times G^S}^{S \ltimes G}(\tilde{\rho}_i)(s^a, g) \overline{Res_{S \times G^S}^{S \ltimes G}(\tilde{\rho}_j)(s^a, g)} &= \frac{1}{|G^S|} \sum_{g \in G^S} \alpha_{in} A_{in}(g) \alpha_{jn} \overline{A_{jn}(g)} \\ &= \alpha_{in} \alpha_{jn} \langle A_{in}(g), A_{jn}(g) \rangle_{G^S} \end{aligned} \tag{5.18}$$

We now evaluate the left-hand side of this equation in another way:

Proposition 5.1.2 *If $S =< s >$ is a cyclic group order n and a an integer satisfying $1 \leq a \leq n-1$ and $(a, n) = 1$, and let T_{ij} be defined:*

$$T_{ij} = \frac{1}{|G^S|} \sum_{g \in G^S} Res^{S \ltimes G}_{S \times G^S}(\tilde{\rho}_i)(s^a, g)\overline{Res^{S \ltimes G}_{S \times G^S}(\tilde{\rho}_j)(s^a, g)} \tag{5.19}$$

Then $T_{ij} = \delta_{ij}$.

Proof For $\beta | n$, let k_β be an integer satisfying $1 \leq k_\beta \leq \frac{n}{\beta} - 1, (k_\beta, \frac{n}{\beta}) = 1$. Let $S_\beta =< s^{\beta k_\beta} >$, (note S_β is independent of the choice of k_β) and by application of Lemma 5.1.1 we see:

$$\begin{aligned}
\delta_{ij} &= \langle \tilde{\rho}_i, \tilde{\rho}_j \rangle_{S \ltimes G} \\
&= \frac{1}{n|G|} \sum_{\beta | n} \phi\left(\frac{n}{\beta}\right) \sum_{g \in G} \tilde{\rho}_i(s^{\beta k_\beta}, g)\overline{\tilde{\rho}_i(s^{\beta k_\beta}, g)} \\
&= \frac{1}{n|G|} \sum_{\beta | n} \phi\left(\frac{n}{\beta}\right) \frac{|G|}{|G^{S_\beta}|} \sum_{g \in G^{S_\beta}} Res^{S \ltimes G}_{S_\beta \times G^{S_\beta}}(\tilde{\rho}_i)(s^{\beta k_\beta}, g)\overline{Res^{S \ltimes G}_{S_\beta \times G^{S_\beta}}(\tilde{\rho}_j)(s^{\beta k_\beta}, g)} \\
&= \frac{1}{n} \sum_{\beta | n} \phi\left(\frac{n}{\beta}\right) \frac{1}{|G^{S_\beta}|} \sum_{g \in G^{S_\beta}} Res^{S_\beta \ltimes G}_{S_\beta \times G^{S_\beta}}(\tilde{\rho}_i)(s^{\beta k_\beta}, g)\overline{Res^{S_\beta \ltimes G}_{S_\beta \times G^{S_\beta}}(\tilde{\rho}_j)(s^{\beta k_\beta}, g)}
\end{aligned} \tag{5.20}$$

By induction on $|S|$, we can assume the result true for all cases above except the case $\beta = 1$, hence we see:

$$\delta_{ij} = \frac{\phi(n)}{n} T_{ij} + \frac{\delta_{ij}}{n} \sum_{\substack{\beta | n \\ \beta \neq 1}} \phi\left(\frac{n}{\beta}\right) \tag{5.21}$$

We recall $\sum_{\beta | n} \phi(\beta) = \sum_{\beta | n} \phi\left(\frac{n}{\beta}\right) = n$, hence:

$$\begin{aligned}
n\delta_{ij} &= \phi(n) T_{ij} + \delta_{ij} \sum_{\substack{\beta | n \\ \beta \neq 1}} \phi\left(\frac{n}{\beta}\right) \\
&= \phi(n) T_{ij} + n\delta_{ij} - \phi(n)\delta_{ij}
\end{aligned} \tag{5.22}$$

Hence $T_{ij} = \delta_{ij}$ as required. ■

Proposition 5.1.2 and Equation 5.18 give:

$$\delta_{ij} = \alpha_{in}\alpha_{jn} \langle A_{in}(g), A_{jn}(g) \rangle_{G^S} \tag{5.23}$$

Since α_{in} and α_{jn} are integers, we must have $\langle A_{in}, A_{jn} \rangle_{G^S} = \delta_{ij}$ and $\alpha_{in}^2 = 1$. By the discussion at the start of the chapter, the distinct irreducible representations $\{A_{1n}, \ldots A_{tn}\}$, of G^S must be precisely $\{\lambda_1, \ldots \lambda_t\}$ which implies that there exists a permutation, σ, and a sign $\epsilon_i \in \{\pm 1\}$ such that for

$$A_{in} = \epsilon_i \lambda_{\sigma(i)} \tag{5.24}$$

for $1 \leq i \leq t$. If we choose a coprime to n and put into Equation 5.16, we see for $t \in G^S$:

$$Res^{S \times G}_{S \times G^S}(\tilde{\rho}_i)(s^a, t) = \tilde{\rho}_i(s^a, t) = A_{in}(t) = \epsilon_i \lambda_{\sigma(i)} \tag{5.25}$$

This proves the following lemma (this is exactly Glauberman's Lemma 3.2.1 above):

Lemma 5.1.3 *Let S be a cyclic group and $\rho \in Irr(G)^S$. Then there exists a unique sign $\epsilon = \pm 1$ and a unique $\lambda \in Irr(G^S)$ such that*

$$\tilde{\rho}(s, t) = \epsilon \lambda(t), \tag{5.26}$$

for all s which generate S, and all $t \in G^S$. Moreover, for every $\lambda \in Irr(G^S)$, there exists a unique $\rho \in Irr(G)^S$ which corresponds to λ as in 5.26.

From the above equations, we also see:

$$Res^G_{G^S}(\rho_i) = \epsilon_i \lambda_{\sigma(i)} + \sum_{\substack{\beta | n \\ \beta \neq n}} \binom{n}{\beta} \alpha_{i\beta} A_{i\beta} \tag{5.27}$$

If S is a $p-$group we note that all terms except the first term disappear modulo p, hence we immediately get the following:

Lemma 5.1.4 *Let S be a cyclic p-group, and $\rho \in Irr(G)^S$. If*

$$Res^G_{G^S}(\rho) = n_1\lambda_1 + ... + n_t\lambda_t, \tag{5.28}$$

where λ_j are distinct irreducible representations, there exists a unique i such that $p \nmid n_i$. Moreover, $n_i \equiv \pm 1 \pmod{p}$.

In the next section, we will strengthen this result by dropping the condition that S is cyclic (we consider the lemma above applied to the final term of a composition series for S). This will achieve Glauberman's Lemma 3.2.2.

Definition 5.1.5 *For a cyclic group S, let*

$$\pi^{S,G} : Irr(G)^S \to Irr(G^S) \tag{5.29}$$

be the bijective correspondence described in Lemma 5.1.3 above: if $\rho \in Irr(G)^S$ then $\pi^{S,G}(\rho) = \lambda$, and for $\lambda \in Irr(G^S)$, then $(\pi^{S,G})^{-1}(\lambda) = \rho$.

This gives a characterisation for the correspondence for cyclic groups. We will follow Glauberman's method and demonstrate how to give the correspondence for all solvable groups S.

An alternative proof of Glauberman's Theorem was given in Alperin [1], using Brauer's work in block theory. When G is a $p-$group, it is possible to

describe the characters and $p-$blocks of the semi-direct product $S \ltimes G$ in a canonical way, in particular those with defect group S. These can then be related to the characters of $S \times G^S$ and modulo p congruences established to give the correspondence.

Finally, we note the following alternative proof. If the result of 5.1.3 is established for the case of cyclic $p-$groups (slightly simpler than the working for general cyclics given above), we can use the following lemma:

Lemma 5.1.6 *Let T be a cyclic $p-$group (for a prime p), acting on a group G of coprime order. Assume that for all $\rho \in Irr(G)^T$, there exists a unique $\epsilon \in \pm 1$ and $\lambda \in Irr(G^T)$ such that for all $g \in G^T$ and t a generator of T,*

$$\tilde{\rho}(t, g) = \epsilon\lambda(g) \tag{5.30}$$

where $\tilde{\rho}$ is the canonical extension of ρ. Then this also holds true for all cyclic groups S.

Proof Let S_1, S_2 be as above with $(|S_1|, |S_2|) = 1$ then we would like to show that for $S = S_1 \times S_2$ and $\rho \in Irr(G)^S$, there exists a unique $\epsilon = \pm 1$ and $\lambda \in Irr(G^S)$ as above.

Let $\tilde{\rho} \in Irr(S \ltimes G)$ be the canonical extension of ρ. Hence for $i = 1, 2$ we have, by uniqueness, $Res^{S\ltimes G}_{S_i \ltimes G}(\tilde{\rho}) \in Irr(S_i \ltimes G)$ is equal to the canonical extension of ρ to $S_i \ltimes G$. Also if $s_1 \in S_1$ then

$$s_1 \circ (Res^{S\ltimes G}_{S_2\ltimes G}(\tilde{\rho})) = Res^{S\ltimes G}_{S_2\ltimes G}(\tilde{\rho}) \tag{5.31}$$

so that $Res^{S\ltimes G}_{S_2\ltimes G}(\tilde{\rho}) \in Irr(S_2 \ltimes G)^{S_1}$ and there exists a unique $\lambda_1 \in Irr(S_2 \ltimes G^{S_1})$ and $\epsilon_1 = \pm 1$ such that

$$\lambda_1(s_2, g_1) = \epsilon_1\tilde{\rho}(s_1, s_2, g_1) \tag{5.32}$$

for all $< s_1 >= S_1, s_2 \in S_2, g_1 \in G^{S_1}$.

Also $Res^{S \ltimes G}_{S_1 \ltimes G}(\tilde{\rho}) \in Irr(S_1 \ltimes G)$ yields, from the S_1-correspondence for ρ, a unique $\lambda_2 \in Irr(G^{S_1})$ such that

$$\lambda_2(g_1) = \epsilon_2 Res^{S \ltimes G}_{S_1 \ltimes G}(\tilde{\rho})(s_1, g_1) = \tilde{\rho}(s_1, 1, g_1) \tag{5.33}$$

for all $< s_1 >= S_1, g_1 \in G^{S_1}$ and for $\epsilon_2 = \pm 1$.

The character values of $Res^{S_2 \ltimes G^{S_1}}_{G^{S_1}}(\lambda_1)$ satisfy

$$Res^{S_2 \ltimes G^{S_1}}_{G^{S_1}}(\lambda_1)(g_1) = \lambda_1(1, g_1) = \epsilon_1 \tilde{\rho}(s_1, 1, g_1) = \epsilon_1 \epsilon_2 \lambda_2(g_1) \tag{5.34}$$

for all $g_1 \in G^{S_1}$. Since λ_2 is irreducible we must have $\epsilon_1 = \epsilon_2$ and λ_1 is the canonical extension of $\lambda_2 \in Irr(G^{S_1})^{S_2}$. Hence there exists $\lambda \in Irr((G^{S_1})^{S_2}) = Irr(G^S)$ such that

$$\lambda(g) = \epsilon \lambda_1(s_2, g) = \epsilon \tilde{\rho}(s_1, s_2, g) \tag{5.35}$$

for all $< s_1 >= S_1, < s_2 >= S_2, g \in G^S$. Corollary 4.2.7 gives that this is unique. ■

5.2 Extension to solvable groups

We now use our results from the previous section and follow Glauberman's approach to demonstrate how the correspondence extends to a solvable group S. We start by recalling Lemma 4 of [11]:

Lemma 5.2.1 *Let S be a cyclic group acting on G, with coprime order. Suppose S is a normal subgroup of S' which also acts on G. Let $T = G^S$. Suppose $\lambda \in Irr(T)$ and $x \in S'$ and let $\rho = \pi^{S,G}(\lambda)$. Then $x(\lambda) \in Irr(T)$ and $x(\rho) = \pi^{S,G}(x(\lambda))$.*

Proof x normalises S so x fixes $G^S = T$, hence $x(\lambda) \in Irr(T)$. Let $\tilde{\rho}$ be the canonical extension of ρ to $S \ltimes G$. $S \ltimes G \lhd S' \ltimes G$ so $x(\rho) \in Irr(S \ltimes G)$. Let s generate S and take $\epsilon = \pm 1$ such that $\tilde{\rho}(s,t) = \epsilon\lambda(t)$ for all $t \in T$. Let $s' = xsx^{-1}$ and we see s' also generates S, so for all $t \in T$, $\tilde{\rho}(s',t) = \tilde{\rho}(s,t)$. Now $Res_G^{S \ltimes G}(x(\tilde{\rho})) = x(\rho) \in Irr(G)$. Also, $det(x(\tilde{\rho}))(s,1) = det(x(\tilde{\rho}))(xsx^{-1},1) = 1$ so $x(\tilde{\rho})$ is the canonical extension of $x(\rho)$ to $S \ltimes G$. For all $t \in T$,

$$x(\tilde{\rho})(s,t) = \tilde{\rho}(xsx^{-1}, x^{-1}t) = \epsilon\lambda(x^{-1}t) = \epsilon x(\lambda)(t) \tag{5.36}$$

Hence $x(\rho) = Res_G^{S \ltimes G}(x(\tilde{\rho})) = \pi^{S,G}(x(\lambda))$ as required. ■

Definition 5.2.2 *Let S be solvable, and C be a composition series for S of the form:*

$$S = S_0 > S_1 > \ldots > S_n = 1 \tag{5.37}$$

Let $T_i = G^{S_i}$ so $T = T_0 = G^S$. We note that T normalises S_i, so S_{i-1} fixes T_i and we can consider S_{i-1}/S_i as acting on T_i, with fixed point subgroup S_{i-1}. We follow Glauberman and define two character sequences:

1. For $\lambda \in Irr(G^S) = Irr(T)$ define λ_i for $i = 0, \ldots, n$ by $\lambda_0 = \lambda$ and for $i > 0$,

$$\lambda_i = \pi^{S_{i-1}/S_i, T_i}(\lambda_{i-1}) \tag{5.38}$$

We see $\lambda_i \in Irr(T_i)^{S_{i-1}/S_i}$, so λ_i is an irreducible character of T_i. Let $\pi_C(\lambda) = \lambda_n$, so $\pi_C(\lambda) \in Irr(G)^S$.

2. For $\rho \in Irr(G)^S$ define ρ_i for $i = n, n-1, \ldots, 0$ by $\rho_n = \rho$, and for $i < n$, ρ_i is an irreducible character of T_i which is fixed by S_i given by:

$$\rho_i = \left(\pi^{S_i/S_{i+1},T_{i+1}}\right)^{-1}(\rho_{i+1}) \tag{5.39}$$

We see $\rho_i \in Irr((T_{i+1})^{S_i/S_{i+1}}) = Irr((G^{S_{i+1}})^{S_i/S_{i+1}}) = Irr(G^{S_i}) = Irr(T_i)$. *Define* $(\pi_C)^{-1}(\rho) = \rho_0$, *hence* $(\pi_C)^{-1}(\rho) \in Irr(T)$.

Lemma 5.2.3 $\pi_C(\lambda)$ *and* $(\pi_C)^{-1}(\rho)$ *are well-defined. For every* $\lambda \in Irr(T)$, $\pi_C(\lambda)$ *is* S*–fixed and* $\lambda = (\pi_C)^{-1}(\pi_C(\lambda))$

Proof $(\pi_C)^{-1}(\rho)$ is well-defined if ρ_i is fixed by S_i/S_{i+1} for $i = n, \ldots, 0$. S fixes ρ_n, so suppose $i < n$ and S fixes ρ_{i+1}. We can regard S_i/S_{i+1} as a normal subgroup of S/S_{i+1} so by Lemma 5.2.1, S fixes ρ_i. Similarly, S fixes $\pi_C(\lambda)$ for every $\lambda \in Irr(T)$. Let $\chi = \pi_C(\lambda)$; by induction $\chi_i = \lambda_i$ for $i = n, \ldots, 0$. Hence $(\pi_C)^{-1}(\pi_C(\lambda)) = \lambda$. Likewise, $\pi_C((\pi_C)^{-1}(\rho)) = \rho$. ■

We now use these definitions to strengthen Lemma 5.1.4:

Lemma 5.2.4 *Let* S *be a* p*-group, and* $\rho \in Irr(G)^S$. *If*

$$Res^G_{G^S}(\rho) = n_1\lambda_1 + \ldots + n_t\lambda_t, \tag{5.40}$$

where λ_j *are distinct irreducible representations, there exists a unique* i *such that* $p \nmid n_i$. *Moreover,* $n_i \equiv \pm 1 \pmod{p}$.

Proof We use induction on $|S|$. Assume $|S| > 1$. By induction, $Res^{T_{n-1}}_T(\lambda_{n-1}) \equiv \epsilon'\lambda \pmod{p}$ for some $\epsilon' = \pm 1$. Since $|S_{n-1}| = p$, by Lemma 5.1.4, there exists $\epsilon'' = \pm 1$ such that $Res^G_{T_{n-1}}(\rho) \equiv \epsilon''\lambda_{n-1} \pmod{p}$. Since $T \leq T_{n-1}$, $Res^G_T(\rho) \equiv \epsilon'' Res^{T_{n-1}}_T(\lambda_{n-1}) \pmod{p}$, and since

$$Res^G_T(\rho) - \epsilon'' Res^{T_{n-1}}_T(\lambda_{n-1}) - \epsilon''(Res^{T_{n-1}}_T(\lambda_{n-1}) - \epsilon'\lambda) = Res^G_T(\rho) + \epsilon'\epsilon''\lambda \tag{5.41}$$

we see $Res^G_T(\rho) \equiv \epsilon'\epsilon''\lambda \pmod{p}$ and the result follows. ■

The following theorem completes the characterisation of Glauberman's correspondence for solvable groups. We firstly show that for cyclic groups S, $\pi_C(\lambda)$ agrees with the characterisation given in Lemma 5.1.3, then we move on to show that when we take S to be solvable, the value of $\pi_C(\lambda)$ is independent of the choice of composition series. This is Glauberman's Theorem 4 [11].

Theorem 5.2.5 *Let S be a solvable group acting on G with coprime order. Assuming the notation above, let C be a composition series for S and let $\lambda \in Irr(G^S)$ with $\rho = \pi_C(\lambda)$. Then:*

a. If S is cyclic then $\rho = \pi^{S,G}(\lambda)$.

b. If D is any other composition series for S, then $\pi_D(\lambda) = \rho$.

Proof

a. We use induction on $|S|$. Assume $|S| > 1$. By Lemma 5.2.3, S fixes ρ. Let $\lambda_0 = (\pi^{S,G})^{-1}(\rho)$ and let $\tilde{\rho}$ be the canonical extension of ρ to $S \ltimes G$. Take $\epsilon_0 = \pm 1$ such that $\epsilon_0 \lambda_0(t) = \tilde{\rho}(s,t)$ for all $t \in T$ and all $s \in S$ satisfying $< s >= S$. We have two cases to consider:

1. $|S| = p^n$ for some prime p. By Lemma 5.1.4, $Res^G_{G^S}(\rho) \equiv \epsilon_0 \lambda_0 \pmod{p}$ so $p \nmid \langle Res^G_{G^S}(\rho), \lambda_0 \rangle$ and hence by part (a), $\lambda = \lambda_0$. We see $\rho = \pi^{S,G}(\lambda_0) = \pi^{S,G}(\lambda)$.

2. Suppose $|S|$ is not a prime power. Let $p = |S/S_1|$, then $S = A \times B$ for a group A with order prime to p such that $A \leq S_1$ and a $p-$group B. Let $\lambda_1 = \pi^{S/S_1,T_1}(\lambda_0)$ and let C^* be the series obtained by removing S_1 from C. Then $\rho = \pi_{C^*}(\lambda_1)$. By induction, $\rho = \pi^{S_1,G}(\lambda_1)$ so ρ doesn't depend on C^*. Since $1 \leq A \leq S_1$, we can assume that A is one of the terms in C^*. Let $\lambda' = \pi^{S/A,G^A}(\lambda)$ and similarly, we can show that $\rho = \pi^{A,G}(\lambda')$.

Let a and b be generators for A and B respectively. Consider A acting on $B \ltimes G$ (these groups have coprime order) and note $(B \ltimes G)^A = B \ltimes G^A$. Let $\tilde{\rho}$ be the canonical extension of ρ to $S \ltimes G$, and by the properties of the canonical extension, we see that $Res^{S \ltimes G}_{B \ltimes G}(\tilde{\rho})$ is the canonical extension of ρ to $B \ltimes G$ and hence irreducible.

By Lemma 5.1.3 there exists $\epsilon' = \pm 1$ such that:

$$\tilde{\rho}(a, x) = \epsilon' X(x) \tag{5.42}$$

for all $x \in B \ltimes G^A$, and by applying part (c) of Theorem 3.1.4, we see:

$$\epsilon' X(x) = \epsilon' \theta'(a) \tilde{\rho}'(x) \tag{5.43}$$

where $\theta' \in Irr(A)$ and $\tilde{\rho}' \in Irr(B \ltimes G^A)$. Consider this formula for $x \in G^A$. As $\rho = \pi^{A,G}(\lambda')$, we see $Res^{B \ltimes G^A}_{G^A}(\tilde{\rho}') = \lambda'$. Now,

$$\lambda' = \pi^{S/A, G^A}(\lambda) = \pi^{B, G^A}(\lambda) \tag{5.44}$$

so there exists $\epsilon = \pm 1$ and $\theta \in Irr(B \ltimes G^A/G^A)$ such that:

$$\tilde{\rho}'(b, t) = \epsilon \theta(b) \lambda(t) \tag{5.45}$$

Putting 5.43 and 5.45 together, we see:

$$\tilde{\rho}(ab, t) = \epsilon \epsilon' \theta(b) \theta'(a) \lambda(t) \tag{5.46}$$

Since $< ab >= S$, we have $\rho = \pi^{S,G}(\lambda)$ as required.

b. Let D have the form $S = B_0 \geq B_1 \geq \ldots \geq B_m = 1$. We use induction on m. If $m \leq 1$ then clearly $\pi_D(\lambda) = \rho$. Suppose $m > 2$. If $S_1 = B_1$ then

$$\pi^{S/S_1, G^{S_1}}(\lambda) = \pi^{S/B_1, G^{S_1}}(\lambda) \tag{5.47}$$

so $\pi_D(\lambda) = \pi_C(\lambda)$ by induction.

Assume now that $S_1 \neq B_1$. Let $J = S_1 \cap B_1$. Then $J \lhd S$. By induction, $\pi_C(\lambda)$ and $\pi_D(\lambda)$ are unchanged if we let $S_2 = B_2 = J$. Consider S/J acting on G^J and J acting on G. By induction, we have $\pi_D(\lambda) = \pi_C(\lambda)$.

Finally, we consider the case $m = 2$, we must have $S = S_1 \times B_1$; S_1 and B_1 both have prime order and either $|S_1| = |B_1|$ or S is cyclic. In the first case, the result follows from application of Lemmas 5.2.4, 5.2.3 and 5.1.3. In the second case, part (a) gives that $\pi_C(\lambda) = \pi^{S,G}(\lambda) = \pi_C(\lambda)$. ■

5.3 The Glauberman correspondence à la Shintani

The Shintani correspondence [25] (see also [7]) is a similar correspondence between irreducible representations but in the case when $S = G(F_{q^p}/F_q)$ for a prime q, the Galois group of the finite field extension, F_{q^p}/F_q and $G = GL_n(F_{q^p})$ with the entry-by-entry Galois action. The most important fact to notice about this correspondence is that $p = |S|$ *may* divide the order of G.

Given an irreducible representation, ρ, of $GL_n(F_{q^p})$ whose character is fixed by the action of $G(F_{q^p}/F_q)$ we may choose an irreducible representation, $\tilde{\rho}$, of the semi-direct product $G(F_{q^p}/F_q) \ltimes GL_n(F_{q^p})$. All choices of $\tilde{\rho}$ are obtained by tensoring any such $\tilde{\rho}$ with one-dimensional representations of $G(F_{q^p}/F_q)$. If $s = Frob_q \in S$ is the generator given by the Frobenius automorphism of F_{q^p}, $z \mapsto z^q$, then the *Shintani norm* of $g \in GL_n(F_{q^p})$ is denoted by $N(g)$ and is a conjugacy class in $GL_n(F_q) = G^S$, which is defined in the following manner. The p-th power of $(Frob_q, g) \in G(F_{q^p}/F_q) \ltimes GL_n(F_{q^p})$ has the form $(1, N_g)$ where $N_g = gFrob_q(g)Frob_q^2(g)\ldots Frob_q^{p-1}(g) \in GL_n(F_{q^p})$ whose conjugacy class is fixed by $G(F_{q^p}/F_q)$. In fact, the conjugacy class of N_g intersects $GL_n(F_q)$ in the conjugacy class of the Shintani norm, $N(g)$.

If $Sh(\rho)$ is the irreducible representation of $GL_n(F_q)$ corresponding to ρ then the character functions are related by the equation

$$\tilde{\rho}(Frob_q, g) = \epsilon Sh(\rho)(N(g)) \tag{5.48}$$

for all $g \in GL_n(F_q)$, where $\epsilon \in \{\pm 1\}$. Note that, if $g \in G^S$ then $N(g)$ is the conjugacy class of g^p.

The following result recasts the Glauberman correspondence, $\rho_i \longleftrightarrow \lambda_{\sigma(i)}$ in a form analogous to that of the Shintani correspondence. First we introduce the Adams operation:

Definition 5.3.1 *Let ρ be a complex representation of G, with character value χ_ρ, and $p \geq 0$ be an integer. The Adams operation, ψ^p is defined by the character formula:*

$$\chi_{\psi^p(\rho)}(g) = \chi_\rho(g^p) \tag{5.49}$$

for all $g \in G$.

Chapter 4 of [28] gives further properties of Adams operations. In particular, we note the following property:

Lemma 5.3.2 *If p is coprime to the order of G, $\psi^p : R(G) \longrightarrow R(G)$ is an isomorphism which permutes the irreducible representations of G.*

Proof The isomorphism assertion follows from the fact that, if $tp \equiv 1$ (modulo $|G|$), then $\psi^t \cdot \psi^p = \psi^{tp} = 1$. To see that representations (rather than virtual representations) are permuted, realise each d-dimensional representation by a homomorphism, ρ, into $GL_d(K)$ where K is a cyclotomic field containing primitive $|G|$-th roots of unity. If $\sigma \in G(K/\mathbb{Q})$ is a Galois

automorphism which raises to the p-th power all primitive $|G|-$th roots of unity then $\sigma(\rho)$ is a representation whose character satisfies

$$trace(\sigma(\rho)(g)) = trace(\rho(g^p)) = \psi^p(\rho)(g) \tag{5.50}$$

Finally, if $\phi_1, \ldots, \phi_t$ are the irreducible representations of G the Schur inner product satisfies

$$\begin{aligned} \langle \psi^p(\phi_i), \psi^p(\phi_j) \rangle_G &= \tfrac{1}{|G|} \textstyle\sum_{g \in G} \psi^p(\phi_i)(g)\overline{\psi^p(\phi_j)(g)} \\ &= \tfrac{1}{|G|} \textstyle\sum_{g \in G} \phi_i(g^p)\overline{\phi_j(g^p)} \\ &= \tfrac{1}{|G|} \textstyle\sum_{h \in G} \phi_i(h)\overline{\phi_j(h)} \\ &= \langle \phi_i, \phi_j \rangle_G \end{aligned} \tag{5.51}$$

so that $\{\psi^p(\phi_i) \mid 1 \leq i \leq t\}$ constitutes a full set of irreducible representations of G, as claimed. ■

Proposition 5.3.3 *Let S be a cyclic group acting on a group G of coprime order. Then, in the notation of 5.1, there is a bijection*

$$\rho_i \longleftrightarrow Sh(\rho_i) \tag{5.52}$$

between the S-fixed irreducible representations of G and the irreducible representations of G^S which is characterised by the relation

$$\tilde{\rho}_i(s, g) = \epsilon_i Sh(\rho_i)(g^p) \tag{5.53}$$

for all $g \in G^S$. Here $\epsilon_i \in \{\pm 1\}$.

Proof Define Sh to be the correspondence given by composing the Glauberman correspondence with

$$(\psi^p)^{-1} : \{\lambda_1, \ldots, \lambda_t\} \longrightarrow \{\lambda_1, \ldots, \lambda_t\}, \tag{5.54}$$

where the λ_i's are the irreducible representations of G^S. Hence, if $\psi^p(\lambda_i) = \lambda_{\tau(i)}$ for some permutation, τ, the Glauberman correspondence canonically extends ρ_i to $\tilde{\rho}_i$ on $S \ltimes G$, sending ρ_i to $\lambda_{\sigma(i)}$ where, for all $g \in G^S$ and s a generator of S,

$$\tilde{\rho}_i(s, g) = \epsilon_i \lambda_{\sigma(i)}(g). \tag{5.55}$$

If $\psi^p(\lambda_j) = \lambda_{\sigma(i)}$ then $\lambda_{\sigma(i)}(g) = \lambda_j(g^p)$ for all $g \in G^S$ and $\tau(j) = \sigma(i)$. Hence, for all $g \in G^S$ and s a generator of S,

$$\tilde{\rho}_i(s, g) = \epsilon_i \lambda_{\tau^{-1}(\sigma(i))}(g) = \epsilon_i Sh(\rho_i)(g^p), \tag{5.56}$$

as required. ■

5.4 Boltje's Explicit Map

We recall the map $bol^{S,G}$ from 3.3.5 is defined as the following composition:

$$bol^{S,G} : R(G)^S \xrightarrow{a_G} R_+(G)^S \xrightarrow{bol_+^{S,G}} R_+(G^S) \xrightarrow{b_{G^S}} R(G^S) \tag{5.57}$$

Let S be a p-group, and $\rho \in Irr(G)^S$. From the results of Chapter 4 (specifically lemma 5.2.4), we have established Glauberman's characterisation for $p-$groups, that $Res^G_{G^S}(\rho) \equiv \epsilon\lambda \pmod p$ for a unique irreducible

representation $\lambda \in Irr(G^S)$. Applying the EBI homomorphism a_G to this, we see:

$$\begin{aligned} Res^G_{G^S}(a_G(\rho)) &= a_{G^S}(Res^G_{G^S}(\rho)) \\ &\equiv a_{G^S}(\epsilon\lambda) \pmod{p} \end{aligned} \tag{5.58}$$

Also, we can apply Frobenius reciprocity (for some $H_i \leq G$ and $\phi_i \in Irr(H_i)$),

$$\begin{aligned} Res^G_{G^S}(a_G(\rho)) &= Res^G_{G^S}(\sum_i n_i(H_i, \phi_i)^G) \\ &= \sum_i n_i \sum_{z \in G^S \backslash G / H_i} (G^S \cap zH_iz^{-1}, (z^{-1})^*(\phi_i))^{G^S} \end{aligned} \tag{5.59}$$

By Theorem 2.5.4, we can split $a_G(\rho)$:

$$a_G(\rho) = \sum_i (H_i, \phi_i)^G = \sum_j (J_j, \phi_j)^G + \sum_{s \in S} \sum_k s(K_k, \psi_k) \tag{5.60}$$

where the $(J_j, \phi_j)^G$ terms are S-fixed, and the (K_k, ψ_k) terms are not. Further from Lemma 4.2.3, we can assume that $s(J_j) = J_j$ and $s(\phi_j) = \phi_j$ for all j. We have:

$$\begin{aligned} Res^G_{G^S}(a_G(\rho)) = &\sum_j \sum_{z \in G^S \backslash G / J_j} (G^S \cap zJ_jz^{-1}, (z^{-1})^*(\phi_j))^{G^S} \\ &+ \sum_{k, s \in S} \sum_{z \in G^S \backslash G / K_k} s(G^S \cap zK_kz^{-1}, (z^{-1})^*(\psi_k))^{G^S} \end{aligned} \tag{5.61}$$

From Proposition 4.2.4, the first sum gives a single term for each j, as there is only one double coset to sum over ($z = 1$). The terms in the second sum all restrict to subgroups and representations of G^S, so the action of s

leaves the element unchanged in its G^S orbit, and each term will therefore appear a multiple of p times. Hence:

$$Res^G_{G^S}(a_G(\rho)) \equiv \sum_j (G^S \cap J_j, Res^{J_j}_{G^S \cap J_j}(\phi_j))^{G^S} \pmod{p} \tag{5.62}$$

Combining this with Equation 5.58, we see we have obtained the EBI formula for the Glauberman correspondent modulo p, and to filter out the appropriate terms, we have removed the $(H_i, \phi_i)^G$ from $a_G(\rho)$ which are not S-fixed. This immediately gives us a proof that Boltje's map $bol^{S,G}$ (given in 3.3.5), is equivalent to Glauberman's correspondence modulo p, when S is a p-group, this is Theorem 3.3.7 above.

Chapter 6

Isaacs' Correspondence

If we drop the Glauberman assumption that S is solvable, we see from the Feit-Thompson theorem that the order of S is even, hence the order of G is odd, and therefore G must be solvable.

Starting with the assumption of a solvable G (in which case S may or may not be solvable), Isaacs [14] showed how to construct a bijection between $Irr(G^S)$ and $Irr(G)^S$ by a group-theoretic method entirely different to Glauberman's correspondence. We start by giving the characterisation of Isaacs' correspondence and we briefly give the results relating to the 'overlapping' case, in which both G and S are solvable. We give some properties of this correspondence, relating to its behaviour with respect to induction and restriction. Finally, we consider how it may be possible to use the results from the earlier chapters, in particular the arguments from Chapter 4 to prove results about the Isaacs situation from the Glauberman case.

6.1 Definition and Properties

The main step to Isaacs' correspondence is the following theorem, first proved in [14]:

Theorem 6.1.1 *Assume S acts on G with $(|S|, |G|) = 1$, and G solvable of odd order. Let H be a group such that $G^S \subseteq H \subseteq G$, and suppose there exists S-invariant normal subgroups K and L of G such that:*

a. $L \subseteq K$ and the quotient K/L is abelian

b. $G = G^S \ltimes K$

c. $H = G^S \ltimes L$

Then for each $\rho \in Irr(G)^S$, there exists a unique $\lambda \in Irr(H)^S$ such that $\langle res^G_H(\rho), \lambda \rangle$ is odd. The map $\rho \leftrightarrow \lambda$ is a bijection between $Irr(G)^S$ and $Irr(H)^S$.

Proof This is effectively Corollary 10.7 of [14], the proof of this is the main aim of Isaacs' paper. ■

To construct Isaacs' correspondence we construct a chain of subgroups:

$$G = C_0 > C_1 > ... > C_k = G^S \tag{6.1}$$

To define the maps, let H be an S-invariant subgroup of G with $G^S \subseteq H \subseteq G$. Let $H^* = G^S \ltimes [H, S]'$ (where $[A, B]$ is the commutator subgroup of A and B, and $[A, B]'$ refers to $[[A, B], [A, B]]$). Since $[H, S] \lhd S \ltimes H$, it follows that $[H, S]' \lhd S \ltimes H$ and hence H^* is S-invariant. If $H > G^S$ then $[H, S] > 1$ and $[H, S] > [H, S]'$ (by the solvability of H). Furthermore, since $[H^*, S] \subseteq [H, S]'$, it follows that $H^* < H$. Now, let $C_0 = G$ and $C_{i+1} = (C_i)^*$ for $1 < i \leq k$, and we have the desired chain of subgroups.

Let $K = [G, S]$ and $L = [G, S]'$. We check the conditions of Theorem 6.1.1: For the first part, the argument above gives that K and L are normal S-invariant subgroups of G and K/L is abelian. The second part follows from Glauberman's Lemma 3.3.3, and the third part comes from the definition of G^* above.

We can therefore apply Theorem 6.1.1 to each C_i to obtain a series of maps $Irr(C_i)^S \to Irr(C_{i+1})^S$ for each i. Isaacs' correspondence is the composition of these maps, we will refer to this map as $is^{S,G}$.

Example 6.1.2 *Wolf [33] gives an example to show that the composition of maps is necessary in the definition of Isaacs' correspondence:*

Let $G = B \ltimes E$ where $|E| = 23^5$ and $|B| = 11^5$ (diagonal subgroups of $GL_5(23)$ and $GL_5(11)$ respectively). Let S be the cyclic group of order 5 acting on G by permuting the subgroup generators transitively. We can then choose $\rho \in Irr(G)^S$ such that there is a unique $\lambda' \in Irr(G^S)$ with $\langle Res^G_{G^S}(\rho), \lambda' \rangle$ odd. However, $is^{S,G}(\rho) \neq \lambda'$. To find the Isaacs Correspondent, we have to go through a series with $G^S = C_2$ above.

Let both S and G be solvable groups. We see that the conditions for both the Glauberman and Isaacs correspondence are met, and quote the following theorem from Wolf [33]:

Theorem 6.1.3 *Assume S and G are solvable groups such that S acts on G, with $(|S|, |G|) = 1$. Then the Glauberman correspondence and Isaacs' correspondence for S and G coincide.*

As a consequence of this theorem, we can define $\pi^{S,G}$ to be the correspondence between $Irr(G)^S$ and $Irr(G^S)$ regardless of the solvability of S and G.

We give a property of $\pi^{S,G}$ from Isaacs [15], some special cases of which are also mentioned in Wolf [34].

Theorem 6.1.4 *Suppose H is an S-invariant subgroup of G. Let $\rho \in Irr(G)^S$ and $\theta \in Irr(H)^S$. Then:*

$$\begin{array}{ccc} \rho \in Irr(G)^S & \xrightarrow{\pi^{S,G}} & Irr(G^S) \\ Ind \uparrow \; \downarrow Res & & Ind \uparrow \; \downarrow Res \\ \theta \in Irr(H)^S & \xrightarrow{\pi^{S,H}} & Irr(H^S) \end{array} \tag{6.2}$$

1. *If $Ind_H^G(\theta) = \rho$ then $Ind_{H^S}^{G^S}(\pi^{S,H}(\theta)) = \pi^{S,G}(\rho)$ and*

2. *If $Res_H^G(\rho) = \theta$ then $Res_{H^S}^{G^S}(\pi^{S,G}(\rho) = \pi^{S,H}(\theta)$.*

6.2 Isaacs' Correspondence via Glauberman

We would like to be able to use the ideas of Chapter 5 to derive Isaacs' correspondence from that of Glauberman, and we propose a strategy for approaching this work, based on the following result from Snaith [28]:

Definition 6.2.1 *A complex representation ρ of G is called a monomial representation if $\rho = Ind_H^G(\phi)$ for some $\phi : H \to \mathbb{C}^*$. An $M-$group is a group all of whose irreducible complex representations are monomial. In particular, it is possible to show that an $M-$group is solvable.*

Proposition 6.2.2 *([28], Proposition 2.1.17) Let S be any finite group. Then there exist $M-$groups, $S_\alpha \leq S$, such that*

$$1 = \sum_\alpha n_\alpha Ind_{S_\alpha}^S(1) \in R(S) \tag{6.3}$$

for suitable integers, $\{n_\alpha\}$.

We want to construct a map similar to Isaacs' correspondence by finding such a relation and applying the Glauberman correspondence to the solvable components S_α. We give some preliminary notation first.

Given a correspondence (a bijective map of sets) $\alpha : Irr(G^S) \to Irr(G)^S$, we can obtain a homomorphism $\phi : R(G^S) \to R(G)^S$ by writing $x \in R(G^S)$ as:

$$x = \sum_{V \in Irr(G^S)} n_V V \tag{6.4}$$

and defining

$$\phi(x) = \sum_{V \in Irr(G^S)} n_V \alpha(V) \in R(G)^S \tag{6.5}$$

Conversely, given such a ϕ we may obtain a map:

$$\tilde{\phi} : R(G^S) \longrightarrow \bigoplus_{V \in Irr(G)^S} \mathbb{Z} < V > \tag{6.6}$$

by observing that $R(G)^S$ is the free abelian group on a basis of elements of the form given by $L(V)$ for $V \in Irr(G)$ where:

$$L(V) = \sum_{s \in \frac{S}{Stab_S(V)}} s(V) \tag{6.7}$$

So we have

$$\bigoplus_{V \in Irr(G)^S} \mathbb{Z} < V > \cong \frac{R(G)^S}{< L(V) | V \in Irr(G), Stab_S(V) \lneq S >} \tag{6.8}$$

Given ϕ, we may form

$$\tilde{\phi} : R(G^S) \xrightarrow{\phi} R(G)^S \xrightarrow{\sigma} \bigoplus_{V \in Irr(G)^S} \mathbb{Z} < V > \tag{6.9}$$

and then we obtain a correspondence if we can show that the matrix of $\sigma\phi$ with respect to the two $\mathbb{Z}-$bases, $Irr(G^S)$ and $Irr(G)^S$, is diagonal: then we may define $\lambda(V) = W$ when $\sigma(\phi(V)) = mW$ for each $V \in Irr(G^S)$, for some non-zero integer m and some $W \in Irr(G)^S$. Usually $m \in \{\pm 1\}$.

Example 6.2.3 *When S is a $p-$group and given ϕ, we can get the correspondence back from the homomorphism by the following composition:*

$$R(G^S) \xrightarrow{\phi} R(G)^S \xrightarrow{\sigma} \bigoplus_{V \in Irr(G)^S} \mathbb{Z} < V > \xrightarrow{\sigma_p} \bigoplus_{V \in Irr(G)^S} \mathbb{Z}/p < V > \tag{6.10}$$

Now, let S be solvable and assume that we have a Glauberman homomorphism:

$$\widetilde{gl}^{S,G} : R(G^S) \longrightarrow R(G)^S \tag{6.11}$$

such that the composition

$$R(G^S) \xrightarrow{\widetilde{gl}^{S,G}} R(G)^S \xrightarrow{\sigma} \bigoplus_{V \in Irr(G)^S} \mathbb{Z} < V > \tag{6.12}$$

gives a Glauberman correspondence

$$gl^{S,G} : Irr(G^S) \longrightarrow Irr(G)^S \tag{6.13}$$

satisfying

$$\sigma\left(\widetilde{gl}^{S,G}(V)\right) = \epsilon^{S,G}(V) gl^{S,G}(V) \tag{6.14}$$

with $\epsilon^{S,G}(V) \in \{\pm 1\}$ for each $V \in Irr(G^S)$. Note that we are using the map gl to be the inverse of the correspondence π as previously defined for ease of notation.

We will now propose a correspondence for general groups S and G of coprime order, and demonstrate that the definition works when S is a $p-$group.

Definition 6.2.4 *If V is an irreducible representation of G fixed by S we have a canonical extension, $\tilde{V} \in Irr(S \ltimes G)$, in order to define an extension, we call this $e^{S,G}(V)$.*

If V is an irreducible representation of G and $H = Stab_S(V)$ we have a canonical extension $e^{H,G}(V) \in Irr(H \ltimes G)$ and we extend:

$$e^{S,G}(V) = Ind_{H \ltimes G}^{S \ltimes G}(e^{H,G}(V)) \in R(S \ltimes G) \tag{6.15}$$

This defines a homomorphism:

$$e^{S,G} : R(G)^S \longrightarrow R(S \ltimes G) \tag{6.16}$$

extending the canonical extension on $S-$fixed irreducibles.

Definition 6.2.5 *Define a homomorphism*

$$d^{S,G} : R(S \ltimes G) \longrightarrow \bigoplus_{V \in Irr(G)^S} \mathbb{Z} < V > \tag{6.17}$$

by setting:

$$d^{S,G}(W) = \begin{cases} 0 & \text{if } Res_G^{S \ltimes G}(W) \text{ is reducible,} \\ Res_G^{S \ltimes G}(W) & \text{if this is irreducible} \end{cases} \tag{6.18}$$

and extending linearly.

Now consider a relation of the form given in Proposition 6.2.2:

$$1 = \sum_{\alpha} n_\alpha Ind_{S_\alpha}^{S}(1) \in R(S) \tag{6.19}$$

and the inflation of this to $S \ltimes G$:

$$1 = \sum_{\alpha} n_\alpha Ind_{S_\alpha \ltimes G}^{S \ltimes G}(1) \in R(S \ltimes G) \tag{6.20}$$

where the $S_\alpha \leqslant S$ may be allowed to equal S.

For $W_\alpha \in Irr(G^{S_\alpha})$, let

$$\widetilde{gl}^{S_\alpha, G}(W_\alpha) = \epsilon^{S_\alpha, G}(W_\alpha) gl^{S_\alpha, G}(W_\alpha) \tag{6.21}$$

and extend linearly.

Consider the composition:

$$\begin{array}{ccc} R(G^S) & \xrightarrow{Ind_{G^S}^{G^{S_\alpha}}} & R(G^{S_\alpha}) \\ & \widetilde{gl}^{S_\alpha,G} \searrow & \\ R(G)^{S_\alpha} & \xrightarrow{e^{S_\alpha,G}} & R(S_\alpha \ltimes G) \\ & Ind_{S_\alpha \ltimes G}^{S \ltimes G} \searrow & \\ R(S \ltimes G) & \xrightarrow{d^{S,G}} & \bigoplus_{V \in Irr(G)^S} \mathbb{Z} < V > \end{array} \tag{6.22}$$

Proposition 6.2.6 *If S is a $p-$group, then the above composition of maps is congruent to the Glauberman correspondence $gl^{S,G}$ modulo p.*

Proof We shall evaluate this composition (mod p) on $V \in Irr(G^S)$.

We have shown already in Theorem 4.2.1 (via the modulo p isomorphism) that:

$$\widetilde{gl}^{S_\alpha,G} \equiv Ind_{G^{S_\alpha}}^{G} \pmod{p} \tag{6.23}$$

and that $Res_{G^{S_\alpha}}^{G}$ (mod p) gives the inverse isomorphism (mod p), up to a sign. That is,

$$\begin{aligned} Ind_{G^{S_\alpha}}^{G} &\equiv \epsilon^{S_\alpha,G}(V)\widetilde{gl}^{S_\alpha,G}(V) \pmod{p} \\ &\equiv \epsilon^{S_\alpha,G}(V) gl^{S_\alpha,G}(V) \pmod{p} \end{aligned} \tag{6.24}$$

This means that

$$\begin{aligned}
\widetilde{gl}^{\prime S_\alpha, G}(Ind_{G^S}^{G^{S_\alpha}}(V)) &= \widetilde{gl}^{\prime S_\alpha, G}\left(\sum_{\substack{\beta, \\ W_\beta \in Irr(G^{S_\alpha})}} m_\beta W_\beta\right) \\
&\equiv Ind_{G^S}^{G} Ind_{G^S}^{G^{S_\alpha}}(V) \pmod{p} \qquad (6.25)
\end{aligned}$$

$$\begin{aligned}
\widetilde{gl}^{\prime S_\alpha, G}(Ind_{G}^{G^{S_\alpha}}(V)) &\equiv Ind_{G^S}^{G}(V) \\
&\equiv \epsilon^{S,G}(V) gl^{S,G}(V) \pmod{p} \qquad (6.26)
\end{aligned}$$

Now, $W = e^{S,G}(gl^{S,G}(V))$ is an irreducible representation of $S \ltimes G$ which restricts to the canonical extension $e^{S_\alpha, G}(gl^{S,G}(V))$ on $S_\alpha \ltimes G$. Hence (by Frobenius reciprocity):

$$\begin{aligned}
Ind_{S_\alpha \ltimes G}^{S \ltimes G}(e^{S_\alpha, G}(\widetilde{gl}^{\prime S_\alpha, G}(Ind_{G^S}^{G^{S_\alpha}}(V)))) &\equiv Ind_{S_\alpha \ltimes G}^{S \ltimes G}(Res_{S_\alpha \ltimes G}^{S \ltimes G}(W)) \pmod{p} \\
&\equiv W \cdot Ind_{S_\alpha \ltimes G}^{S \ltimes G}(1) \pmod{p} \qquad (6.27)
\end{aligned}$$

We can substitute the relation from Equation 6.20:

$$\begin{aligned}
\sum_\alpha n_\alpha Ind_{S_\alpha \ltimes G}^{S \ltimes G}(e^{S_\alpha, G}(\widetilde{gl}^{\prime S_\alpha, G}(Ind_{G^S}^{G^{S_\alpha}}(V)))) &\equiv \sum_\alpha W \cdot n_\alpha Ind_{S_\alpha \ltimes G}^{S \ltimes G}(1) \pmod{p} \\
&\equiv W \pmod{p} \\
&\equiv e^{S,G}(gl^{S,G}(V)) \pmod{p} \qquad (6.28)
\end{aligned}$$

If we finally apply $d^{S,G}$ to the above chain of maps, we see the result is congruent to $gl^{S,G}(V) \pmod{p}$ as required. ■

Unfortunately we have been unable to obtain any further results about the composition for a general S, but it seems likely that a composition of this form is a possible candidate for Isaacs' correspondence for non-solvable S.

Chapter 7

Cryptographic Applications

In 5.3, we saw a connection between the Glauberman correspondence and Adams operations on representations. In the context of cryptography, we make some further remarks about Adams operations.

The first section gives a brief overview of the three main asymmetric cryptographic systems. We move on to describe how we can recast the Discrete Logarithm Problem (DLP) within complex representations of a finite group using Adams operations. We consider pairings to demonstrate the isomorphism between abelian groups and their irreducible representations.

We can then define the Representation Discrete Logarithm Problem (RDLP) on a group G, extending the definition to include non-abelian groups.

Finally, we consider an example of RDLP on the representations of GL_2F_q, the group of invertible 2x2 matrices over a finite field. We look in detail at these representations and how to apply Adams operations. We consider a specific example for GL_2F_3, and finally give a brief outline of how this approach may lead indirectly to an attack on ECDLP.

7.1 Existing Cryptographic Ideas

7.1.1 The Integer Factorization Problem

The Integer Factorization Problem (IFP) forms the basis of the RSA encryption system. The IFP is stated as follows: given an integer n that is known to be the product of two primes $n = pq$, find p and q. Further details of the RSA algorithm can be found in Chapter 19 of [23].

7.1.2 The Discrete Logarithm Problem

Let G be a finite abelian group. The Discrete Logarithm Problem (DLP) is the problem of finding the smallest integer $x \geq 0$ (if it exists) which satisfies $h = g^x$, given the two elements g and h in G.

In practice, the difficulty of solving the DLP is exploited by cryptographic algorithms such as the Diffie-Hellman key exchange (D-H), and the Digital Signature Algorithm (DSA) among others. Full details of all the commonly used algorithms can be found in Chapter 1 of Blake, Seroussi & Smart [2]. To give the idea, we describe the D-H algorithm here:

Diffie-Hellman key exchange

Using the standard cryptographic language, we assume that Alice wishes to send a message to Bob without an eavesdropper, Eve, being able to interpret the message. Here, they just wish to agree on a randomly chosen element of the group G (which in practice is then used as a key for a high-speed cryptographic algorithm). An element $g \in G$ is chosen, and is publicly communicated along with the group G.

Alice and Bob follow this process:

1. Alice generates a random integer $1 \leq x_A \leq n-1$, where n is the order of g. She calculates g^{x_A} and sends this to Bob.

2. Bob generates a random integer $1 \leq x_B \leq n-1$. He calculates g^{x_B} and sends to Alice.

3. Alice can now compute the key $k \in G$, using $k = g^{x_A x_B} = (g^{x_B})^{x_A}$.

4. Bob can also compute $k \in G$, using $k = g^{x_A x_B} = (g^{x_A})^{x_B}$.

The only information available to Eve is G, g, g^{x_A}, g^{x_B}. It is easy to see that if Eve can solve the DLP in G, then she can recover k and compromise the system. It is widely believed that the converse is also true (polynomial-time algorithms exist to reduce D-H to DLP and vice-versa).

7.1.3 Elliptic Curve Discrete Logarithm Problem

The Elliptic Curve Discrete Logarithm Problem (ECDLP) is formed from taking the DLP over the additive group of points on an elliptic curve (further details of the definitions of elliptic curves can be found in [26] and [2]).

Let F_q be the finite field of order q, where $q = p^r$ for some prime p. Let $E(F_q)$ be an elliptic curve defined over F_q. The ECDLP is the following: given a point $P \in E(F_q)$ of order n and a point $Q \in E(F_q)$, determine the integer m, $1 \leq m \leq n-1$ satisfying $Q = mP$ (if it exists). We note that Elliptic Curve groups are generally written using additive notation.

Pohlig and Hellman gave an algorithm (detailed in Chapter 5 of [2]), based on the Chinese Remainder Theorem to solve ECDLP by determining m modulo s, where s ranges over each of the prime divisors of n, so in

practice, n is taken to be prime to provide the strongest possible security level.

7.1.4 Best Known Attacks

The measure of the security of the above cryptosystems is given in terms of the best known attacks. Details of the full list of best known attacks together with their running times is given in [19]. The current best known general-purpose attacks, those not relying on specially chosen situations (for example the super-singular elliptic curves, which are assumed to be avoided) are: for IFP, the Number Field Sieve algorithm [18]; for DLP, a variant of this algorithm [12]; for ECDLP, the Pollard rho-method ([21] and Chapter 5 of [2]). The running time of this method takes the order of $\sqrt{\pi n}/2$ steps (a 'step' is considered to be an elliptic curve addition) which is significantly slower than the best methods for IFP and DLP, as the Number Field Sieve algorithm is sub-exponential in both cases, for comparable sized systems (see [19] for a full discussion of this). For this reason, ECDLP is believed to be much harder than IFP and DLP.

7.2 Representation Theory and Pairings

Definition 7.2.1 *Let G be an abelian group. A pairing $<,>$ is a non-singular bilinear form:*

$$<,>: G \times G \to \mathbb{Q}/\mathbb{Z} \tag{7.1}$$

We see such a pairing gives rise to an isomorphism between G and $Irr(G)$, the set of complex irreducible representations of G (these are all one-dimensional as G is abelian):

For each $g \in G$, define $\phi_g : G \to \mathbb{C}^*$ by $\phi_g(h) = \langle g, h \rangle$, then the correspondence is given by:

$$\begin{aligned} G &\longleftrightarrow Irr(G) = Hom(G, \mathbb{Q}/\mathbb{Z}) \\ g &\longleftrightarrow \phi_g : G \to \mathbb{C}^* \end{aligned} \tag{7.2}$$

Example 7.2.2 *Let E be an elliptic curve defined over F_q. Let $n \geq 2$ be an integer coprime to the characteristic p of F_q, and $E[n]$ be the $n-$torsion points of the curve. Let μ_n be the group of $n-th$ roots of unity. The Weil pairing e_n is a pairing:*

$$e_n : E[n] \times E[n] \to \mu_n \tag{7.3}$$

The explicit definition of the Weil pairing is given in Chapter 3 of [2] (including an algorithm to compute this function for given points). This gives a bijection:

$$\begin{aligned} E[n] &\longleftrightarrow Irr(E[n]) \\ Q &\longleftrightarrow \phi_Q \end{aligned} \tag{7.4}$$

where $\phi_Q(P) = e_n(P, Q)$ for all $n-$torsion points $P \in E(F_q)$.

We recall the definition of the Adam operations (from 5.3.1)

Definition 7.2.3 *Let ρ be a complex representation of G, with character value χ_ρ, and $m \geq 0$ be an integer. The Adams operation, ψ^m is defined by the character formula:*

$$\chi_{\psi^m(\rho)}(g) = \chi_\rho(g^m) \tag{7.5}$$

for all $g \in G$.

Section 5.3 along with Chapter 4 of [28] gives further properties and applications of Adams operations. In particular, we note the following properties for $\rho \in Irr(G)$:

1. $dim(\rho) = dim(\psi^m(\rho))$

2. If m is coprime to $|G|$ then $\psi^m(\rho) \in Irr(\rho)$ (lemma 5.3.2)

Returning to example 7.2.2, we see that if Q and P are two points as above, with $Q = mP$, then this gives $\phi_Q = \psi^m(\phi_P)$ in the corresponding representations.

7.3 The Representation Discrete Logarithm Problem (RDLP)

For the abelian group $E(F_q)$, the Weil-pairing above shows that if two points P, Q on the elliptic curve are related as in ECDLP, ie $Q = mP$ for some integer m, then $\phi_Q = \psi^m(\phi_P)$, and conversely.

Let G be any finite group (not necessarily abelian). We can define RDLP on $Irr(G)$ as follows: let ρ_1 and ρ_2 be elements of $Irr(G)$. What is the smallest integer m (if it exists) such that $\rho_1 = \psi^m(\rho_2)$?

For abelian elliptic curve groups, Section 7.2 demonstrates that RDLP corresponds to ECDLP. We would like to know more about the difficulty of RDLP in the case of non-abelian G.

7.4 Representations of GL_2F_q

We give a summary of the results from Chapter 2 of Snaith [28] in which the representations of GL_2F_q (the group of invertible 2×2-matrices with elements in the finite field F_q) are calculated.

7.4.1 The Weil Representations

Let F_{q^2} denote the field of order q^2, so the Galois group $G(F_{q^2}/F_q)$ is cyclic of order two, generated by the Frobenius automorphism, F:

$$\begin{aligned} F : F_{q^2} &\to F_{q^2} \\ z &\to z^q \end{aligned} \tag{7.6}$$

Let $\Theta : F_{q^2}^* \to \mathbb{C}^*$ be a non-trivial character satisfying $\Theta \neq F^*(\Theta)$ (where $F^*(\Theta)(z) = \Theta(F(z))$ for all $z \in F_{q^2}^*$).

We note that the elements of GL_2F_q can be divided into four types of conjugacy class:

Type	Minimal polynomial	Conjugacy class representative	Number in class
I	$(t-\alpha)(t-\beta)$ $\alpha \neq \beta \in F_q^*$	$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$	$q(q+1)$
II	$(t-\alpha)^2$ $\alpha \in F_q^*$	$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$	q^2-1
III	$(t-\alpha)$ $\alpha \in F_q^*$	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$	1
IV	$t^2-(x+F(x))t+xF(x)$ $F(x) \neq x \in F_{q^2}^*$	$\begin{pmatrix} 0 & -xF(x) \\ 1 & x+F(x) \end{pmatrix}$	q^2-q

Theorem 7.4.1 *For each choice of Θ, we can define a unique irreducible representation $r(\Theta) : Gl_2F_q \to GL_{q-1}(\mathbb{C})$, called the Weil-representation associated to Θ. The character values of this representation on the elements of GL_2F_q is summarised in the following table:*

Type	Conjugacy class representative	Character value
I	$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$	0
II	$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$	$-\Theta(\alpha)$
III	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$	$(q-1)\Theta(\alpha)$
IV	$\begin{pmatrix} 0 & -xF(x) \\ 1 & x+F(x) \end{pmatrix}$	$-\{\Theta(x)+\Theta(F(x))\}$

Proof Contained in Section 3.1 of [28]. ■

7.4.2 A full list of irreducible representations

We can now give a complete list of the irreducible representations of GL_2F_q:

Definition 7.4.2 *The Borel subgroup, $B \leq GL_2F_q$ is defined:*

$$B = \left\{ X \in GL_2F_q | X = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \right\} \tag{7.7}$$

Suppose we are given characters of the form:

$$\rho, \rho_1, \rho_2 : F_q^* \to \mathbb{C}^* \tag{7.8}$$

then we have a one-dimensional representation, $L(\rho)$, given by composing ρ with the determinant map:

$$L(\rho) = \rho \cdot det : GL_2F_q \xrightarrow{det} F_q^* \xrightarrow{\rho} \mathbb{C}^* \tag{7.9}$$

If ρ_1 and ρ_2 are distinct, define:

$$Inf_T^B(\rho_1 \otimes \rho_2) : B \to \mathbb{C}^* \tag{7.10}$$

by inflating $\rho_1 \otimes \rho_2$ from the diagonal torus T to the Borel subgroup B. That is,

$$Inf_T^B(\rho_1 \otimes \rho_2) \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = \rho_1(\alpha)\rho_2(\delta) \tag{7.11}$$

Define a $(q+1)-$dimensional representation $R(\rho_1, \rho_2)$, by:

$$R(\rho_1, \rho_2) = Ind_B^{Gl_2F_q}(Inf_T^B(\rho_1 \otimes \rho_2)) \tag{7.12}$$

When $\rho = \rho_1 = \rho_2$, we have:

$$Inf_T^B(\rho \otimes \rho) = Res_B^{Gl_2F_q}(L(\rho)) : B \to \mathbb{C}^* \tag{7.13}$$

so there is a canonical surjection:

$$Ind_B^{Gl_2F_q}(Inf_T^B(\rho \otimes \rho)) \to Ind_{Gl_2F_q}^{Gl_2F_q}(L(\rho)) = L(\rho) \tag{7.14}$$

Therefore, we may define a $q-$dimensional representation, $S(\rho)$, by means of the following short exact sequence of representations:

$$0 \to S(\rho) \to Ind_B^{GL_2F_q}(Inf_T^B(\rho \otimes \rho)) \to L(\rho) \to 0 \tag{7.15}$$

Theorem 7.4.3 *A complete list of the representations of GL_2F_q is given by:*

1. *$L(\rho)$ of 7.9 for $\rho : F_q^* \longrightarrow \mathbb{C}^*$,*

2. *$S(\rho)$ of 7.15 for $\rho : F_q^* \longrightarrow \mathbb{C}^*$,*

3. *$R(\rho_1, \rho_2) = R(\rho_2, \rho_1)$ of 7.12 for any two distinct $\rho_1, \rho_2 : F_q^* \longrightarrow \mathbb{C}^*$,*

4. *$r(\Theta) = r(F^*(\Theta))$ of 7.4.1 for any character $\Theta : F_{q^2}^* \longrightarrow \mathbb{C}^*$ which is distinct from its Frobenius conjugate, $F^*(\Theta)$.*

Proof Theorem 3.2.4 of [28] has full details. We note that the number of each type of representation is $q-1, q-1, (q-1)(q-2)/2$ and $(q^2-q)/2$ respectively. These representations have degree $1, q^2, (q+1)^2, (q-1)^2$ respectively. Calculating Schur inner products of each type of representation with itself and with the others demonstrates that they are all distinct and irreducible, and summing the number of each type multiplied by the square of the dimension gives the size of the group, hence all the irreducibles are included. ■

We can calculate the character values of these representations, and summarise in the following table (taken from Theorem 3.2.5 of [28]), where $N = N_{F_{q^2}/F_q}$ denotes the norm:

Type	$L(\rho)$	$R(\rho_1, \rho_2)$	$S(\rho)$	$r(\Theta)$
I	$\rho(\alpha\beta)$	$\rho_1(\alpha)\rho_2(\beta) + \rho_2(\alpha)\rho_1(\beta)$	$\rho(\alpha\beta)$	0
II	$\rho(\alpha)^2$	$\rho_1(\alpha)\rho_2(\alpha)$	0	$-\Theta(\alpha)$
III	$\rho(\alpha)^2$	$(q+1)\rho_1(\alpha)\rho_2(\alpha)$	$q\rho(\alpha)^2$	$(q-1)\Theta(\alpha)$
IV	$\rho(N(x))$	0	$-\rho(N(x))$	$-\{\Theta(x) + \Theta(F(x))\}$

7.4.3 Application of Adams Operations

We want to investigate RDLP for GL_2F_q. Firstly, we consider the behaviour of the representations listed above on applying the Adams operation ψ^m, where m is a positive integer coprime to $q(q-1)(q^2-1)$, the order of GL_2F_q.

From the remarks following 5.3.1 we note that if ϕ is an irreducible resentation of GL_2F_q, $\psi^m(\phi)$ is irreducible of the same dimension. This immediately gives us that ψ^m preserves the representation type in Theorem 7.4.3.

We can calculate the m-th powers of the types of conjugacy class GL_2F_q and summarise in the following table:

Type	X = Conjugacy class representative	Representative of X^m
I	$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$	$\begin{pmatrix} \alpha^m & 0 \\ 0 & \beta^m \end{pmatrix}$
II	$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$	$\begin{pmatrix} \alpha^m & 1 \\ 0 & \alpha^m \end{pmatrix}$
III	$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$	$\begin{pmatrix} \alpha^m & 0 \\ 0 & \alpha^m \end{pmatrix}$
IV	$\begin{pmatrix} 0 & -xF(x) \\ 1 & x+F(x) \end{pmatrix}$	$\begin{pmatrix} 0 & -x^mF(x^m) \\ 1 & x^m+F(x^m) \end{pmatrix}$

In all cases, we note that the conjugacy class representative for X^m lies in the same type of class as that for X (note in type–IV that we have

$x \neq F(x)$, hence $x^m \neq F(x^m)$ as m is prime to the order of the group). We can immediately see from the two tables above how the application of ψ^m permutes the irreducible representations of GL_2F_q within their types, and use this to calculate the new character values.

7.4.4 This observation gives the motivation for an algorithm to tackle ECDLP for Weil-representations. Given two distinct representations $\Theta_i : F_{q^2}^* \to \mathbb{C}^*$ as above, for $i = 1, 2$, if $\psi^m(\Theta_1) = \Theta_2$ for some integer m coprime to the order of GL_2F_q, we know the corresponding Weil-representations $r(\Theta_1)$ and $r(\Theta_2)$ are such that $\psi^m(r(\Theta_1)) = r(\Theta_2)$. If we choose $x \in F_{q^2}^*$ such that $F(x) \neq x$, then the type−IV matrix R given by:

$$R = \begin{pmatrix} 0 & -x^m F(x^m) \\ 1 & x^m + F(x^m) \end{pmatrix} \tag{7.16}$$

satisfies the character formula:

$$\chi_{r(\Theta_1)}(R) = -(\Theta_1(x) + \Theta_1(F(x))) = \alpha \tag{7.17}$$

and

$$\begin{aligned} \chi_{r(\Theta_2)}(R) &= -(\Theta_2(x) + \Theta_2(F(x))) \\ &= -(\Theta_1(x)^m + \Theta_1(F(x))^m) = \beta \end{aligned} \tag{7.18}$$

α and β are complex numbers lying on the unit circle, hence by calculating the angles between them (provided this is not a rational multiple of π) we are able to recover the integer m.

Combining this with the Weil-pairing, or a similar computable function allowing a mapping between Elliptic Curve points and representations, we

may be able to use this method as part of an algorithm to tackle ECDLP. If we can use points on a curve in place of matrices, we can calculate equivalents of α and β above *without* having to know the choice of x.

There are several problems. In order to compute the Weil-pairing for example, we need to determine the smallest integer k such that $E[n] \subseteq E(F_{q^k})$ (where n is the order of P, the curve point corresponding to Θ_1). Algorithms to determine this value k are only known for the class of supersingular curves, which are the target of the MOV attack (this attack and the class of curves is described in detail in Menezes, Okamoto and Vanstone [20]).

We finish with an example of the Weil-representations for the group GL_2F_3.

7.4.4 Example: $G = GL_2F_3$

We calculate first the Weil-representations of G, which has order 48. The conjugacy classes are as follows:

Type	Number of Classes	Size	Conjugacy Class Representatives
I	1	12	$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
II	2	8	$B_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B_2 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$
III	2	1	$C_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $C_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
IV	3	6	$D_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $D_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $D_3 = \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}$

There are three Weil-representations. Let j be a root of $x^2 + 1$, an irreducible quadratic polynomial over F_3, and consider $F_9 = F_3[j]$. The Weil-representations are given by $r(\theta_m)$ for $1 \leq m \leq 3$ where $\theta_m : (1-j) \to e^{\pi i m/2}$.

The character values on eight conjugacy classes are calculated as follows:

Type	A	B_1	B_2	C_1	C_2	D_1	D_2	D_3
$r(\theta_1)$	0	-1	1	2	-2	0	$\sqrt{2}i$	$-\sqrt{2}i$
$r(\theta_2)$	0	-1	-1	2	2	2	0	0
$r(\theta_3)$	0	-1	1	2	-2	0	$-\sqrt{2}i$	$\sqrt{2}i$

Consider the image of $\begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}$ under $r(\theta_1)$ and $r(\theta_3)$. We note

$$\chi_{r(\theta_1)} \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix} = -\sqrt{2} \tag{7.19}$$

and

$$\chi_{r(\theta_3)} \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix} = \sqrt{2} \tag{7.20}$$

Unfortunately, for this example, we see the angle between these points is π, which hits the indeterminate situation: we are not able to recover the power $r(\theta_3) = \psi^5(r(\theta_1))$ in this particular case, and in fact with any other pairs of Weil-representations for GL_2F_3. However, with a large group order, a random choice from the available type$-$IV representations should eliminate the ambiguity.

Bibliography

[1] J. L. Alperin. The main problem of block theory. In W. R. Scott and F. Gross, editors, *Proc. Conf. on Finite Groups*, pages 341–365, Park City, Utah, 1976. Academic Press.

[2] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography.* Cambridge University Press, 2000.

[3] R. Boltje. *Canonical and explicit Brauer induction in the character ring of a finite group and a generalisation for Mackey functors.* PhD thesis, Augsburg University, 1989.

[4] R. Boltje. A canonical Brauer induction formula. *Astérisque*, 181:31–59, 1990.

[5] R. Boltje. Glauberman's Correspondence via Canonical Induction Formulae. *Akad. gemein. Wiss. Erfurt, Sitzungsber. Math.-Nat.*, 7:19–35, 1996.

[6] R. Boltje, V.P. Snaith, and P. Symonds. Algebraicisation of Explicit Brauer Induction. *J. Alg*, 148:504–527, 1992.

[7] F. Digne and J. Michel. Fonctions-L des variétés de Deligne-Lusztig et descente de Shintani. *Mem. Math. Soc. France*, 20, 1985.

[8] Larry Dornhoff. *Group Representation Theory (Parts 1 & 2).* Marcel Dekker Inc., 1971.

[9] W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific Journal of Mathematics 13*, pages 775–1029, 1963.

[10] P. X. Gallagher. Group characters and normal Hall subgroups. *Nagoya Math. J.*, 21:223–230, 1962.

[11] George Glauberman. Correspondence of Characters for Relatively Prime Operator Groups. *Canadian Journal of Mathematics 20*, pages 1465–1488, 1968.

[12] D. Gordon. Discrete logarithms in $GF(p)$ using the number field sieve. *SIAM Journal on Discrete Mathematics*, 6:124–138, 1993.

[13] I. M. Isaacs. *Character Theory of Finite Groups.* Academic Press Inc., 1976.

[14] I.M. Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math*, 95:594–635, 1973.

[15] I.M. Isaacs and Gabriel Navarro. Character correspondences and irreducible induction and restriction. *Amer. J. Math*, 140:131–140, 1991.

[16] R. Keown. *An Introduction to Group Representation Theory.* Academic Press Inc., 1975.

[17] I. J. Leary. Topics in modular representation theory. Unpublished course notes from Southampton University.

[18] A.K. Lenstra, H.W. Lenstra Jr., M.S. Manasse, and J.M. Pollard. The number field sieve. In *The Development of the Number Field Sieve*,

volume 1554 of *Lecture Notes in Mathematics*, pages 11–42. Springer-Verlag, 1993.

[19] A.K. Lenstra and E.R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14(4):255–293, 2001.

[20] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Trans. Info. Theory*, 39(5):1639–1646, 1993.

[21] J. Pollard. Monte carlo methods for index computation mod p. *Mathematics of Computation*, 32:918–924, 1978.

[22] Derek J. S. Robinson. *A Course in the Theory of Groups.* Graduate Texts in Mathematics #80. Springer-Verlag, second edition, 1995.

[23] B. Schneier. *Applied Cryptography.* John Wiley & Sons, Inc., 1996.

[24] Jean-Pierre Serre. *Cohomologie Galoisienne.* Lecture Notes in Mathematics #5. Springer-Verlag, 1997.

[25] T. Shintani. Two remarks on irreducible characters of finite general linear groups. *J. Math. Soc. Japan*, 28:495–531, 1976.

[26] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1985.

[27] Victor P. Snaith. *Topological Methods in Galois Representation Theory.* Canadian Mathematical Society, Wiley-Interscience, 1989.

[28] Victor P. Snaith. *Explicit Brauer Induction.* Cambridge University Press, 1994.

[29] Victor P. Snaith. *Galois Module Structure.* Fields Institute Monographs, American Mathematical Society, 1994.

[30] V.P. Snaith. Applications of Explicit Brauer Induction. *A. Math. Soc. Proc. Symp. Pure*, 47:495–531, 1987.

[31] V.P. Snaith. Explicit Brauer Induction. *Inventiones Math.*, 94:455–478, 1988.

[32] V.P. Snaith. A local construction of the local root numbers. In de Gruyter, editor, *Proceedings of the 1987 Laval Number Theory Conference*, pages 823–840, 1989.

[33] T. R. Wolf. Character correspondences in solvable groups. *Illinois J. Math.*, 22(2):327–340, 1978.

[34] T. R. Wolf. Character correspondences induced by subgroups of operator groups. *J. Alg.*, 57:502–521, 1979.