UNIVERSITY OF ALBERTA

Permutation Modules and Representation Theory

by

Peter Steven Campbell ©

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

in

Mathematics

Department of Mathematical Sciences

Edmonton, Alberta

Spring 2000

0-612-60107-2

UNIVERSITY OF ALBERTA

Library Release Form

Name of Author: Peter Steven Campbell.

Title of Thesis: Permutation Modules and Representation Theory.

Degree: Master of Science in Mathematics.

Year this Degree Granted: 2000.

Peter S. Campbell

5 Trinity Park

Duns

Berwickshire, TD11 3HN

Scotland

Date: 21st Dec. 1999

UNIVERSITY OF ALBERTA

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled **Permutation Modules and Representation Theory** submitted by Peter Steven Campbell in partial fulfillment of the requirements for the degree of Master of Science in Mathematics.

A. Weiss

Dr. A. Weiss (Chair)

Gerald Cliff

Dr. G.H. Cliff (Supervisor)

W.W. Armstrong

Dr. W.W. Armstrong

Date: Dec. 3, 1999

ABSTRACT

The sign character for Coxeter groups and the Steinberg character for finite groups with BN-pair can be expressed as alternating sums of permutation characters. We show that we can use the corresponding permutation modules to construct modules which afford these characters.

Further, we consider an analogue of the Steinberg character for $\mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$, $h \geq 2$, given by Hill. Using the same method as for the sign character and Steinberg character, we construct a module which affords this character. In addition, we show that this character can also be expressed as an alternating sum of permutation characters over certain subgroups of $\mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$ containing B, the subgroup of upper triangular matrices.

Contents

Chapter 1

Introduction

The aim of this thesis is to examine particular examples of characters which can be expressed as alternating sums of permutation characters and to show that we can construct modules which afford these characters using only permutation modules. Our main tool for constructing these modules will be self-adjoint idempotents, in particular the group sums $\widehat{H}$ for subgroups H of G.

Let F be an arbitrary field of characteristic 0 which is closed under complex conjugation, and let G be a finite group. The group ring FG can be regarded as a finite dimensional F-vector space with F-basis $\{g\}_{g\in G}$, thus we can consider the inner product for finite dimensional F-vector spaces as an inner product on FG

$$\left\langle \sum_{g\in G} a_g g, \sum_{x\in G} b_x x \right\rangle = \sum_{g\in G} a_g \overline{b_g},$$

where $\bar{\ }$ denotes complex conjugation. Further, this inner product is invariant with respect to multiplication by G and so for any FG-submodule M of FG, the vector space orthogonal complement $M^\perp$ is also an FG-module. Hence we get the orthogonal decomposition of FG,

$$FG = M \oplus M^\perp$$

and, using the orthogonal projection of FG onto M, we show that there is a unique idempotent $e \in FG$, called a self-adjoint idempotent, such that $M = FGe$ and $M^\perp = FG(1-e)$.

Now, given self-adjoint idempotents $e_1, \ldots, e_n \in FG$ we define other self-adjoint idempotents $e_1 \wedge \cdots \wedge e_n$ and $e_1 \vee \cdots \vee e_n$ in FG so that

$$FGe_1 \cap \cdots \cap FGe_n = FG(e_1 \wedge \cdots \wedge e_n)$$

and

$$FGe_1 + \cdots + FGe_n = FG(e_1 \vee \cdots \vee e_n).$$

We give some properties of these idempotents and show that they are essentially independent of the field F. Moreover, in the case where F is a subfield of $\mathbb{C}$ we see that they can be constructed using the idempotents $e_1, \ldots, e_n$ as

$$e_1 \wedge \cdots \wedge e_n = \lim_{k\to\infty} (e_1 \cdots e_n)^k$$

and

$$e_1 \vee \cdots \vee e_n = 1 - \lim_{k\to\infty} [(1-e_1)\cdots(1-e_n)]^k.$$

In Chapter 3 we examine the link between representation theory and self-adjoint idempotents. We show that given a self-adjoint idempotent $e \in FG$, the character χ of the corresponding FG-module FGe is

$$\chi(g) = \sum_{x\in G} e_{x^{-1}g^{-1}x}.$$

Consequently, if the self-adjoint idempotent can be expressed as an F-linear combination $e = a_1e_1 + \cdots + a_ne_n$ of other self-adjoint idempotents $e_1, \ldots, e_n \in FG$, then we have a corresponding decomposition for the character χ,

$$\chi = a_1\chi_1 + \cdots + a_n\chi_n$$

where χ_i is the character of FGe_i. In particular, we concentrate on the self-adjoint idempotents

$$\widehat{H} = \frac{1}{|H|}\sum_{h\in H} h$$

for subgroups H of G and the corresponding permutation modules $FG\widehat{H}$.

For Coxeter groups W, Solomon in [18] showed that the sign character ϵ of W could be expressed as an alternating sum of permutation characters

$$\epsilon = \sum_{J\subset S} (-1)^{|J|}(1_{W_J})^W.$$

Using self-adjoint idempotents we show that a module affording this character is given by the FW-module M in the following orthogonal decomposition

$$FW = M \oplus \sum_{\emptyset\neq J\subset S} FW\widehat{W_J}.$$

Similarly, for finite groups with BN-pair Curtis in [5] showed that the Steinberg character St was given by

$$\mathrm{St} = \sum_{J\subset S} (-1)^{|J|}(1_{W_J})^G.$$

Again we show that a module affording this character can be constructed as the FG-module M in the orthogonal decomposition

$$FG\widehat{B} = M \oplus \sum_{\emptyset \neq J \subset S} FG\widehat{P_J}.$$

Finally, we look at an analogue of the Steinberg character for $G = \mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$, $h \geq 2$, given by Hill in [11]. We construct certain subgroups K_J of G analogous to the subgroups P_J for $GL_n(\mathbb{Z}/p\mathbb{Z})$ and show that the FG-module M in the orthogonal decomposition

$$FG\widehat{B} = M \oplus \sum_{\emptyset \neq J \subset S} FG\widehat{K_J}$$

affords the character given by Hill. Further, we see that the self-adjoint idempotent $e \in FG$ such that $M = FGe$ is

$$e = \sum_{J \subset S} (-1)^{|J|} \widehat{K_J}$$

and so the character given by Hill can be expressed as the following alternating sum of permutation characters

$$\chi_M = \sum_{J \subset S} (-1)^{|J|} (1_{K_J})^G,$$

which is analogous to the expression for the Steinberg character given by Curtis in [5].

Chapter 2

Geometry of Finite Group Rings

In this chapter we develop certain techniques to investigate the submodule structure of a finite group ring FG, with emphasis on idempotents which generate the submodules as principal left ideals of FG. In particular, we give a distinguished idempotent for each submodule and use these to construct idempotents corresponding to the intersection and sum of a finite number of submodules of FG.

Further, we show that these self-adjoint idempotents are essentially independent of the field F and that they give a bijection between FG-submodules of FGe and S-submodules of S, where $S = eFGe$ and $e \in FG$ is a self-adjoint idempotent, which preserves irreducibility.

2.1 An Inner Product in Finite Group Rings

Let F be an arbitrary field of characteristic 0 which is closed under complex conjugation, and let G be a finite group. By the group ring FG of G over F we mean the set of all formal F-linear combinations of elements of G, i.e.

$$FG = \left\{ \sum_{g \in G} a_g g : a_g \in F \right\},$$

with addition given by

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and multiplication

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{x \in G} b_x x \right) = \sum_{g \in G} \sum_{x \in G} a_g b_x g x.$$

We will assume the basic definitions and results for rings; see [1] or [13] for particular emphasis on group rings and their connection to representation theory. However, we will prove the following result in full since it is used explicitly in a later proof.

2.1.1 Lemma $\mathrm{End}_{FG}(FG) \simeq (FG)^{\mathrm{op}}$.

Proof:

For each $r \in FG$, define the map $\phi_r : FG \to FG$ by $\phi_r(s) = sr$ for all $s \in FG$, i.e. ϕ_r is right multiplication on FG by r. Then for each $s, t \in FG$ we have that $\phi_r(s+t) = (s+t)r = sr + tr = \phi_r(s) + \phi_r(t)$ and $\phi_r(st) = str = s\phi_r(t)$, impying that ϕ_r is an FG-endomorphism. Further, if $\phi_r = \phi_s$ then $r = \phi_r(1) = \phi_s(1) = s$ and so the FG-endomorphisms ϕ_r are distinct.

On the other hand, suppose that we have an FG-endomorphism ψ. For each $r \in FG$ we see that $\psi(r) = r\psi(1)$ implying that $\psi = \phi_{\psi(1)}$. Hence every FG-endomorphism is of the form ϕ_r for some $r \in FG$.

Finally, for each $r, s, t \in FG$, $(\phi_r + \phi_s)(t) = \phi_r(t) + \phi_s(t) = tr + ts = t(r+s) = \phi_{r+s}(t)$ and $(\phi_r \circ \phi_s)(t) = \phi_r(ts) = tsr = \phi_{sr}(t)$, giving $\phi_r + \phi_s = \phi_{r+s}$ and $\phi_r \circ \phi_s = \phi_{sr}$.
□

Consider FG as an F-vector space of dimension $|G|$ with basis $\{g\}_{g \in G}$. We can give FG the corresponding vector space inner product

$$\left\langle \sum_{g \in G} a_g g, \sum_{x \in G} b_x x \right\rangle = \sum_{g \in G} a_g \overline{b_g},$$

where $\bar{\ }$ denotes complex conjugation. Moreover, we see that this inner product is invariant with respect to the action of G on FG:

2.1.2 Lemma Let $r, s \in FG$ and $g \in G$, then $\langle gr, gs \rangle = \langle r, s \rangle$ and $\langle rg, sg \rangle = \langle r, s \rangle$.

Proof:

Suppose that $r = \sum_{x \in G} a_x x$ and $s = \sum_{x \in G} b_x x$. Then

$$gr = \sum_{x \in G} a_x gx = \sum_{x \in G} a_{g^{-1}x} x$$

and

$$gs = \sum_{x \in G} b_x gx = \sum_{x \in G} b_{g^{-1}x} x,$$

thus

$$\langle gr, gs \rangle = \sum_{x \in G} a_{g^{-1}x} \overline{b_{g^{-1}x}} = \sum_{x \in G} a_x \overline{b_x} = \langle r, s \rangle .$$

Similarly for multiplication on the right. □

It is this inner product structure of FG that we will use to obtain information about the FG-submodules of FG; see [14] for basic definitions and results concerning inner products in real and complex vector spaces and [10] for F-vector spaces.

In particular, since we have an inner product on FG, we can define the orthogonal complement of an FG-submodule of FG.

2.1.3 Definition Let M be an FG-submodule of FG and define the *orthogonal complement* of M to be

$$M^{\perp} = \{r \in FG : \langle r, m\rangle = 0, \forall m \in M\}.$$

Further, since the inner product is G-invariant, $M^{\perp}$ is also an FG-module and, in a result analogous to the vector space case, we have the following orthogonal decomposition of FG:

2.1.4 Lemma $M^{\perp}$ is an FG-module, such that $FG = M \oplus M^{\perp}$.

Proof:

We know that the orthogonal complement of an F-vector space, is an F-vector space so we need only show that $M^{\perp}$ is closed under the action of G. Let $n \in M^{\perp}$, then for any $g \in G$ and any $m \in M$ we see that $\langle m, gn\rangle = \langle gg^{-1}m, gn\rangle = \langle g^{-1}m, n\rangle = 0$ since the inner product is G-invariant and since M is an FG-module. Hence $gn \in M^{\perp}$ and $M^{\perp}$ is an FG-module. Finally, the decomposition of FG follows from the same result for finite-dimensional F-vector spaces. □

2.1.5 Corollary Let M be an FG-submodule of M, then for any FG-submodule N of M, $M = N \oplus (N^{\perp} \cap M)$.

We would like to use this orthogonal decomposition to give a distinguished idempotent for the module M, i.e. to be able to pick an idempotent $e \in FG$ such that $M = FGe$ and $M^{\perp} = FG(1-e)$. To do this we define the adjoint of an element of FG and therefore the notion of self-adjoint ring elements.

2.1.6 Definition Let $r = \sum_{g \in G} a_g g \in FG$, then the *adjoint* of r is defined to be

$$r^{*} = \sum_{g \in G} \overline{a_{g^{-1}}} g.$$

We say that r is *self-adjoint* if $r = r^{*}$.

In particular, a ring element and its adjoint are related in the following way:

2.1.7 Lemma For each $r, s, t \in FG$, $\langle rs, t\rangle = \langle s, r^*t\rangle$ and $\langle sr, t\rangle = \langle s, tr^*\rangle$.

Proof:

Note that by Lemma 2.1.2, $\langle gr, s\rangle = \langle gr, gg^{-1}s\rangle = \langle r, g^{-1}s\rangle$. So, if $r = \sum_{g\in G} a_g g$ then

$$\begin{aligned}
\langle rs, t\rangle &= \left\langle \left(\sum_{g\in G} a_g g\right) s, t \right\rangle \\
&= \sum_{g\in G} a_g \langle gs, t\rangle \\
&= \sum_{g\in G} a_g \left\langle s, g^{-1}t\right\rangle \\
&= \left\langle s, \left(\sum_{g\in G} \overline{a_g} g^{-1}\right) t \right\rangle \\
&= \langle s, r^*t\rangle .
\end{aligned}$$

Similarly for multiplication by r on the right. □

Moreover, this shows us that the adjoint of a ring element is related to the adjoint of the corresponding linear map ϕ_r.

2.1.8 Corollary $(\phi_r)^* = \phi_{r^*}$.

Proof:

This follows from Lemma 2.1.7 and the definition of the adjoint of a linear map. □

The properties of the adjoint of a linear map then give us corresponding properties for the adjoint of a ring element.

2.1.9 Corollary Let $r, s \in FG$ and $\lambda, \mu \in F$, then

(i) $(\lambda r + \mu s)^* = \overline{\lambda} r^* + \overline{\mu} s^*$;

(ii) $(rs)^* = s^* r^*$.

Now consider an idempotent in $e \in FG$ which is also self-adjoint. Then

$$FG = FGe \oplus FG(1 - e),$$

the usual decomposition of FG given by the idempotent e, is in fact an orthogonal decompostion of FG as in Lemma 2.1.4.

2.1.10 Lemma Let $e \in FG$ be a self-adjoint idempotent, then $(FGe)^{\perp} = FG(1-e)$.

Proof:

Since e is self-adjoint, for each $re \in FGe$ and $s(1-e) \in FG(1-e)$, $\langle re, s(1-e)\rangle = \langle r, s(1-e)e\rangle = \langle r, 0\rangle = 0$. Hence $FG(1-e) \subset (FGe)^{\perp}$. However, we can express any $r \in FG$ as $r = re + r(1-e)$, and so $\langle re, r\rangle = \langle re, re\rangle + \langle re, r(1-e)\rangle = \langle re, re\rangle = 0$ if and only if $re = 0$, i.e. if $r \in FG(1-e)$. Thus $(FGe)^{\perp} = FG(1-e)$. □

We now show that every orthogonal decomposition of FG is of this form for some unique self-adjoint idempotent and so, for each FG-submodule M of FG, there is a unique self-adjoint idempotent $e \in FG$ such that $M = FGe$.

2.1.11 Definition Let M be an FG-submodule of FG and define the *orthogonal projection* of FG onto M to be

$$P_M : FG \to FG; r \mapsto m$$

where r is expressed uniquely as $r = m + n$ with $m \in M$ and $n \in M^{\perp}$.

The orthogonal projection P_M has the following properties:

2.1.12 Proposition Let M be an FG-submodule of FG. Then

(i) P_M is an FG-endomorphism;

(ii) $P_M^2 = P_M$;

(iii) $P_M^* = P_M$;

(iv) $I - P_M = P_{M^{\perp}}$.

Proof:

(i) Let $r \in FG$ be such that $r = m + n$ with $m \in M$, $n \in M^{\perp}$. Then, for any $s \in FG$, we see that since M and $M^{\perp}$ are FG-modules, $sm \in M$ and $sn \in M^{\perp}$ and $sr = sm + sn$. Thus $P_M(sr) = sm = sP_M(r)$, and P_M is an FG-endomorphism.

(ii) For all $m \in M$, $P_M(m) = m$ by definition. Thus, for all $r = m + n \in FG$ with $m \in M$ and $n \in M^{\perp}$,

$$P_M^2(r) = P_M(P_M(r)) = P_M(m) = m = P_M(r).$$

(iii) For every $r = m + n, r' = m' + n' \in FG$ with $m, m' \in M$ and $n, n' \in M^\perp$,

$$\begin{aligned} \langle P_M(r), r' \rangle &= \langle m, m' + n' \rangle \\ &= \langle m, m' \rangle + \langle m, n' \rangle \\ &= \langle m, m' \rangle \\ &= \langle m, m' \rangle + \langle n, m' \rangle \\ &= \langle m + n, m' \rangle \\ &= \langle r, P_M(r') \rangle . \end{aligned}$$

Hence, $P_M^* = P_M$ by the definition of the adjoint of a linear map.

(iv) Suppose that $r = m + n \in FG$ with $m \in M$ and $n \in M^\perp$, then since $M = (M^\perp)^\perp$, we see that $P_{M^\perp}(r) = n = r - m = (I - P_M)(r)$. □

Thus we can use the orthogonal projection P_M to give us the self-adjoint idempotent $e \in FG$ such that $M = FGe$.

2.1.13 Corollary Let M be an FG-submodule of FG, then there exists a unique self-adjoint idempotent $e \in FG$ such that $M = FGe$.

Proof:

By Proposition 2.1.12(i) P_M is an FG-endomorphism and so, by Lemma 2.1.1, there is a unique $e \in FG$ such that $P_M = \phi_e$. Further, $\phi_{e^2} = \phi_e^2 = \phi_e$ implies that e is an idempotent and $\phi_{e^*} = \phi_e^* = \phi_e$ implies that it is self-adjoint. Finally, $\phi_e(r) = re \in M$ for each $r \in FG$, so $FGe \subset M$, and $m = \phi_e(m) = me$ for each $m \in M$, thus $M = FGe$.

Suppose now that $f \in FG$ is another self-adjoint idempotent such that $M = FGf$. Then $e \in FGf$ implies that $ef = e$ and $f \in FGe$ implies $fe = f$. However, this gives $f = f^* = (fe)^* = e^* f^* = ef = e$. □

Now, since for each FG-submodule M of FG there is a unique self-adjoint idempotent $e \in FG$ such that $M = FGe$, this means that in particular, given FG-submodules $M_1, \ldots, M_n$ of FG, there must be unique self-adjoint idempotents for their intersection $M_1 \cap \cdots \cap M_n$ and their sum $M_1 + \cdots + M_n$.

2.1.14 Definition Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents and define the *meet*, $e_1 \wedge \cdots \wedge e_n$, and *join*, $e_1 \vee \cdots \vee e_n$, of $e_1, \ldots, e_n$ to be the unique self-adjoint idempotents in FG such that

$$FGe_1 \cap \cdots \cap FGe_n = FG(e_1 \wedge \cdots \wedge e_n)$$

and

$$FGe_1 + \cdots + FGe_n = FG(e_1 \vee \cdots \vee e_n).$$

Immediately from the definition we see that the meet has the following properties:

2.1.15 Lemma Let $e, f, x \in FG$ be self-adjoint idempotents, then

(i) $e \wedge e = e$;

(ii) $e \wedge f = f \wedge e$;

(iii) $(e \wedge f) \wedge x = e \wedge f \wedge x = e \wedge (f \wedge x)$;

(iv) If $ex = e$ or $fx = f$, then $e(e \wedge f) = e \wedge f = (e \wedge f)e$;

(v) If $xe = x$ and $xf = x$, then $x(e \wedge f) = x = (e \wedge f)x$.

Proof:

(i) $FG(e \wedge e) = FGe \cap FGe = FGe$;

(ii) $FG(e \wedge f) = FGe \cap FGf = FGf \cap FGe = FG(f \wedge e)$.

(iii) $FG((e \wedge f) \wedge x) = (FGe \cap FGf) \cap FGx = FGe \cap FGf \cap FGx = FG(e \wedge f \wedge x)$ and similarly $FG(e \wedge (f \wedge x)) = FGe \cap (FGf \cap FGx) = FGe \cap FGf \cap FGx = FG(e \wedge f \wedge x)$.

(iv) $FGe \subset FGx$ since $ex = e$. Hence, $FG(e \wedge f) = FGe \cap FGf \subset FGe \subset FGx$ and so $(e \wedge f)x = (e \wedge f)$. Moreover, $e = e^* = ((e \wedge f)x)^* = x^*(e \wedge f)^* = x(e \wedge f)$. Similarly for the case $fx = f$.

(v) $FGx \subset FGe$ since $xe = x$, and $FGx \subset FGf$ since $xf = x$. Hence $FGx \subset FGe \cap FGf = FG(e \wedge f)$ and so $x(e \wedge f) = x$. Also, $x = x^* = (x(e \wedge f))^* = (e \wedge f)^* x^* = (e \wedge f)x$. □

Further, we can express the join $e_1 \vee \cdots \vee e_n$ in terms of the meet of some other self-adjoint idempotents. To do this we use the orthogonal complement to give the following correspondence between sums and intersections:

2.1.16 Lemma Let M, N be FG-submodules of FG, then $(M+N)^\perp = M^\perp \cap N^\perp$.

Proof:
Let $m \in M$ and $n \in N$, then for every $r \in M^\perp \cap N^\perp$ we see that $\langle r, m+n \rangle = \langle r, m \rangle + \langle r, n \rangle = 0$. Hence, $r \in (M+N)^\perp$ and $M^\perp \cap N^\perp \subset (M+N)^\perp$. Now, suppose that $r \in (M+N)^\perp$, then $\langle r, s \rangle = 0$ for every $s \in M+N$. In particular, since $M \subset M+N$ we see that $\langle r, m \rangle = 0$ for every $m \in M$ implying that $r \in M^\perp$, and since $N \subset M+N$, $\langle r, n \rangle = 0$ for every $n \in N$ implying that $r \in N^\perp$. Hence $r \in M^\perp \cap N^\perp$ and $(M+N)^\perp \subset M^\perp \cap N^\perp$. □

2.1.17 Corollary Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents, then

$$e_1 \vee \cdots \vee e_n = 1 - (1 - e_1) \wedge \cdots \wedge (1 - e_n).$$

Proof:

Note that

$$\begin{aligned} FG(e_1 \vee \cdots \vee e_n) &= FGe_1 + \cdots + FGe_n \\ &= [(FGe_1 + \cdots + FGe_n)^{\perp}]^{\perp} \\ &= [(FGe_1)^{\perp} \cap \cdots \cap (FGe_n)^{\perp}]^{\perp} \\ &= [FG(1 - e_1) \cap \cdots \cap FG(1 - e_n)]^{\perp} \\ &= [FG((1 - e_1) \wedge \cdots \wedge (1 - e_n))]^{\perp} \\ &= FG(1 - (1 - e_1) \wedge \cdots \wedge (1 - e_n)), \end{aligned}$$

and the result follows from uniqueness of the self-adjoint idempotents. □

Consequently, we get the corresponding properties for $e_1 \vee \cdots \vee e_n$:

2.1.18 Lemma Let $e, f, x \in FG$ be self-adjoint idempotents, then

(i) $e \vee e = e$;

(ii) $e \vee f = f \vee e$;

(iii) $(e \vee f) \vee x = e \vee f \vee x = e \vee (f \vee x)$;

(iv) If $xe = x$ or $xf = x$, then $x(e \vee f) = x = (e \vee f)x$;

(v) If $ex = e$ and $fx = f$ then $x(e \vee f) = e \vee f = (e \vee f)x$.

2.2 Changing the Field

Suppose now that we have some field K containing F. FG can be regarded as a subset of KG and therefore any FG-submodule M of FG is also a subset of KG. Hence, we can examine the the KG-submodule of KG generated by $M \subset KG$.

2.2.1 Definition Let M be an FG-submodule of FG and define KM to be the KG-submodule of KG

$$KM = Km_1 + \cdots + Km_n$$

for some basis $\{m_i\}_{i=1}^n$ for M over F.

An FG-submodule of FG is *absolutely irreducible* if, for all fields K containing F, KM is an irreducible KG-module.

We say that a KG-submodule N of KG is *realisable* over F if there is some FG-submodule M of FG such that $N = KM$.

We need to show two things about the definition. The first is that it is well-defined, i.e. KM does not depend on the basis for M.

2.2.2 Lemma Let M be an FG-module and suppose that $\{m_i\}_{i=1}^n$ and $\{m_i'\}_{i=1}^n$ are two bases for M over F. Then

$$Km_1 + \cdots + Km_n = Km_1' + \cdots + Km_n'.$$

Proof:

For each $1 \leq i \leq n$, we can write $m_i = \sum_{j=1}^n a_{i,j} m_j'$ for some $a_{i,j} \in F$. Then we see that for any $k \in K$ we have that

$$km_i = \sum_{j=1}^n ka_{i,j} m_j' \in Km_1' + \cdots + Km_n'.$$

Hence $Km_1 + \cdots + Km_n \subset Km_1' + \cdots + Km_n'$. Similarly for the reverse inclusion, and so $Km_1 + \cdots + Km_n = Km_1' + \cdots Km_n'$ as required. □

The second thing we need to show is that KM is indeed a KG-submodule of KG.

2.2.3 Lemma Let M be an FG-submodule of FG, then KM is a KG-submodule of KG.

Proof:

By definition, KM is a K-vector subspace of KG, so to show that KM is a KG-submodule of KG we need only show that it is closed under left multiplication by G. Let $\{m_i\}_{i=1}^n$ be a basis for M over F. Then, since M is an FG-module, we have that for each $g \in G$ and for each $1 \leq i \leq n$, $gm_i = \sum_{j=1}^n a_{i,j} m_j$ for some $a_{i,j} \in F$. Then, $a_{i,j} \in K$ and so $gm_i \in KM$, for each $1 \leq i \leq n$. Hence, since KM is the K-linear span of $\{m_i\}_{i=1}^n$, this implies that KM is closed under left multiplication by G. □

Now we restrict to the case where the field K is also closed under complex conjugation.

2.2.4 Lemma Let M be an FG-submodule of FG, then $\dim_F(M) = \dim_K(KM)$.

Proof:

Without loss of generality we may assume that the F-basis $\{m_i\}_{i=1}^n$ for M is orthogonal, i.e. $\langle m_i, m_j \rangle = 0$ if $i \neq j$. So if $k_1, \ldots k_n \in K$ are such that $k_1 m_1 + \cdots k_n m_n = 0$ then for each i we see that

$$0 = \langle k_1 m_1 + \cdots + k_n m_n, m_i \rangle = k_i \langle m_i, m_i \rangle$$

implying that $k_i = 0$. Hence, $\{m_i\}_{i=1}^n$ is a linearly independent set over K, and therefore is a K-basis for KM. □

As an immediate consequence we have the following result:

2.2.5 Corollary Let M be an FG-sumodule of FG and let $\{m_i\}_{i=1}^n$ be an F-basis for M. Then $\{m_i\}_{i=1}^n$ is a K-basis for KM.

2.2.6 Lemma Let M, N be FG-submodules of FG. Then

(i) $K(FG) = KG$;

(ii) $K(M^\perp) = (KM)^\perp$;

(iii) $K(M+N) = KM + KN$;

(iv) $K(M \cap N) = KM \cap KN$.

Proof:

(i) This follows immediately from the definition since $\{g\}_{g\in G}$ is both an F-basis for FG and a K-basis for KG.

(ii) Let $\{m_i\}_{i=1}^n$ be an orthogonal F-basis for M and extend it to an orthogonal basis $\{m_i\}_{i=1}^{|G|}$ for FG over F. Then $\{m_i\}_{i=n+1}^{|G|}$ is an orthogonal F-basis for $M^\perp$. Now $\langle m_i, m_j\rangle = 0$ for all $i \neq j$, so for each $n+1 \leq j \leq |G|$ and $k_1, \ldots, k_n \in K$,

$$\langle k_1 m_1 + \cdots + k_n m_n, m_j\rangle = k_1 \langle m_1, m_j\rangle + \cdots + k_n \langle m_n, m_j\rangle = 0.$$

So, $m_j \in (Km_1 + \cdots + Km_n)^\perp = (KM)^\perp$ and therefore $Km_{n+1} + \cdots + Km_{|G|} = K(M^\perp) \subset (KM)^\perp$.

On the other hand, since $\{m_i\}_{i=1}^{|G|}$ is an orthogonal K-basis for KG, so if $k_1 m_1 + \cdots + k_{|G|} m_{|G|} \in (KM)^\perp$ then for each $1 \leq i \leq n$,

$$\left\langle k_1 m_1 + \cdots k_{|G|} m_{|G|}, m_i\right\rangle = k_i \langle m_i, m_i\rangle = 0,$$

i.e. $k_i = 0$. Thus $(KM)^\perp \subset Km_{n+1} + \cdots Km_{|G|} = K(M^\perp)$.

(iii) Let $\{m_1, \ldots, m_n\}$ be an F-basis for $M \cap N$. Then we can extend it to F-bases $\{m_1, \ldots, m_n, m_{n+1}, \ldots, m_r\}$ and $\{m_1, \ldots, m_n, m'_{n+1}, \ldots, m'_s\}$ of M and N respectively. So, $\{m_1, \ldots, m_n, m_{n+1}, \ldots, m_r, m'_{n+1}, \ldots, m'_s\}$ is an F-basis for $M + N$ and is therefore a K-basis for $K(M+N)$. Hence we see that

$$
\begin{aligned}
KM + KN &= (Km_1 + \cdots + Km_n + Km_{n+1} + \cdots + Km_r) \\
&\quad + (Km_1 + \cdots + Km_n + Km'_{n+1} + \cdots + Km'_s) \\
&= Km_1 + \cdots + Km_n + Km_{n+1} \\
&\quad + \cdots + Km_r + Km'_{n+1} + \cdots + Km'_s \\
&= K(M + N).
\end{aligned}
$$

(iv) Keep the notation from the proof of part (iii). In particular, we see that since $\{m_1, \ldots, m_n, m_{n+1}, m_r, m'_{n+1}, \ldots, m'_s\}$ is a K-basis for $K(M+N)$ it is linearly independent over K. So, if $r \in KM \cap KN$ then $r = k_1m_1 + \cdots + k_nm_n + k_{n+1}m_{n+1} + \cdots + k_rm_r$ and $r = k'_1m_1 + \cdots + k'_nm_n + k'_{n+1}m'_{n+1} + \cdots + k'_sm_s$ for some $k_i, k'_i \in K$. Thus

$$
\begin{aligned}
& k_1m_1 + \cdots + k_nm_n + k_{n+1}m_{n+1} + \cdots + k_rm_r \\
= \; & k'_1m_1 + \cdots + k'_nm_n + k'_{n+1}m'_{n+1} + \cdots + k'_sm'_s
\end{aligned}
$$

implies $k_i = 0$ for $n+1 \leq i \leq r$ and $k'_j = 0$ for $n+1 \leq j \leq s$. Hence $KM \cap KN \subset Km_1 + \cdots Km_n = K(M \cap N)$. On the other hand, clearly $K(M \cap N) \subset KM$ and $K(M \cap N) \subset KN$ so $K(M \cap N) \subset KM \cap KN$. □

Now, if M is an FG-submodule of FG then there is a unique self-adjoint idempotent $e_F \in F$ such that $M = FGe_F$ and, since KM is a KG-submodule of KG, there is also a unique self-adjoint idempotent $e_K \in KG$ such that $KM = KGe_K$. However, for any self-adjoint idempotent $e \in FG$ then, considered as an element of KG, it is still a self-adjoint idempotent. Thus, we would like to be able to show that e_F and e_K are the same self-adjoint idempotent.

2.2.7 Lemma Let $e \in FG$ be a self-adjoint idempotent, then $K(FGe) = KGe$.

Proof:

Let $\{m_i\}_{i=1}^n$ be an F-basis for FGe. Since $e \in FGe$, $e = \sum_{i=1}^n a_im_i$ for some $a_i \in F$. Then, $a_i \in K$ implies that $e = \sum_{i=1}^n a_im_i \in Km_1 + \cdots + Km_n = K(FGe)$, and therefore $KGe \subset K(FGe)$. Conversely, for each $1 \leq i \leq n$, $m_i \in FGe$ implies that $m_ie = e$. Thus for any $r \in K(FGe)$, $r = k_1m_1 + \cdots + k_nm_n$ for some $k_1, \ldots, k_n \in K$, and

$$re = k_1m_1e + \cdots k_nm_ne = k_1m_1 + \cdots k_nm_n = r.$$

Hence, $K(FGe) \subset KGe$ and so $K(FGe) = KGe$. □

2.2.8 Corollary Let M be an FG-submodule of FG, then $e \in FG$ is the unique self-adjoint idempotent such that $M = FGe$ if and only if it is the unique self-adjoint idempotent in KG such that $KM = KGe$.

Proof:

Suppose that $e \in FG$ is the self-adjoint idempotent such that $M = FGe$, then we see that $KM = K(FGe) = KGe$ and $e \in KG$ is the unique self-adjoint idempotent such that $KM = KGe$.

Conversely, suppose that $e \in KG$ is the unique self-adjoint idempotent such that $KM = KGe$. Then, since $M = FGf$ for some unique self-adjoint idempotent $f \in FG$, $KGe = KM = K(FGf) = KGf$ implies that $e = f$ and so $e \in FG$ is the unique self-adjoint idempotent such that $M = FGe$. □

Immediately from this we are able to give a necessary and sufficient condition for a KG-submodule N of KG to be realisable over F.

2.2.9 Corollary Let N be a KG-submodule of KG with corresponding self-adjoint idempotent $e \in KG$. Then N is realisable over F if and only if $e \in FG$.

Proof:

Suppose that $N = KM$ for some FG-submodule M of FG, then by Corollary 2.2.8, if $e \in FG$ is the self-adjoint idempotent such that $M = FGe$, then it is also the self-adjoint idempotent such that $N = KGe$. On the other hand, if $M = KGe$ with $e \in FG$, we see that FGe is an FG-submodule of FG such that $K(FGe) = KGe = M$. □

Further, for any self-adjoint idempotents $e_1, \ldots, e_n \in FG$ we know that there are self-adjoint idempotents $e_1 \wedge_F \cdots \wedge_F e_n$ and $e_1 \vee_F \cdots \vee_F e_n$ in FG such that

$$FGe_1 \cap \cdots \cap FGe_n = FG(e_1 \wedge_F \cdots \wedge_F e_n)$$

and

$$FGe_1 + \cdots + FGe_n = FG(e_1 \vee_F \cdots \vee_F e_n).$$

However, since $e_1, \ldots, e_n$ are also self-adjoint idempotents in KG, there are self-adjoint idempotents $e_1 \wedge_K \cdots \wedge_K e_n$ and $e_1 \vee_K \cdots \vee_K e_n$ in KG such that

$$KGe_1 \cap \cdots \cap KGe_n = KG(e_1 \wedge_K \cdots \wedge_K e_n)$$

and

$$KGe_1 + \cdots + KGe_n = KG(e_1 \vee_K \cdots \wedge_K e_n).$$

Again, we would like to show that these self-adjoint idempotents are independent of the field, i.e. $e_1 \wedge_F \cdots \wedge_F e_n = e_1 \wedge_K \cdots \wedge_K e_n$ and $e_1 \vee_F \cdots \vee_F e_n = e_1 \vee_K \cdots \vee_K e_n$.

2.2.10 Lemma Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents, then

$$e_1 \wedge_F \cdots \wedge_F e_n = e_1 \wedge_K \cdots \wedge_K e_n.$$

Proof:

The result follows from the uniqueness of the self-adjoint idempotents in the following

$$\begin{aligned} KG(e_1 \wedge_F \cdots \wedge_F e_n) &= K(FG(e_1 \wedge_F \cdots \wedge_F e_n)) \\ &= K(FGe_1 \cap \cdots \cap FGe_n) \\ &= K(FGe_1) \cap \cdots \cap K(FGe_n) \\ &= KGe_1 \cap \cdots \cap KGe_n \\ &= KG(e_1 \wedge_K \cdots \wedge_K e_n). \end{aligned}$$

□

2.2.11 Corollary Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents, then

$$e_1 \vee_F \cdots \vee_F e_n = e_1 \vee_K \cdots \vee_K e_n.$$

Proof:

Using Corollary 2.1.17 we see that

$$\begin{aligned} e_1 \vee_F \cdots \vee_F e_n &= 1 - (1 - e_1) \wedge_F \cdots \wedge_F (1 - e_n) \\ &= 1 - (1 - e_1) \wedge_K \cdots \wedge_K (1 - e_n) \\ &= e_1 \vee_K \cdots \vee_K e_n. \end{aligned}$$

□

2.3 Subrings $eFGe$ of FG

Let $e \in FG$ be a self-adjoint idempotent and define S to be the subring $S = eFGe$ of FG with identity element $e \in S$. In particular, we see that S can also be regarded as an F-vector subspace of FG and so has the inner product of FG restricted to S. Further, note that for any $s \in S$, $s = ere$ for some $r \in FG$ and so $s^* = er^*e \in S$. Thus, we can define the adjoint of an element of S in the same way as in Definition 2.1.6.

Moreover, as in the case of FG, we can define the orthogonal complement of an S-submodule of S.

2.3.1 Definition Let N be an S-submodule of S and define the *orthogonal complement* of N to be

$$N^\perp = \{s \in S : \langle s, n \rangle = 0, \forall n \in N\}.$$

Again, we find that the orthogonal complement of an S-submodule of S is also an S-module and we get an orthogonal decomposition of S:

2.3.2 Lemma Let N be an S-submodule of S, then $N^\perp$ is an S-module such that $S = N \oplus N^\perp$.

Proof:
$N^\perp$ is an F-vector space so to show that it is an S-module it suffices to show that it is closed under left multiplication by S. For each $n' \in N^\perp$ and for every $n \in N$, $s \in S$, we see that $\langle sn', n\rangle = \langle n', s^*n\rangle = 0$, since $s^*n \in N$. Hence $sn' \in N^\perp$ and $N^\perp$ is an S-module. Finally, the decomposition of S follows from the same decomposition for F-vector spaces. □

In particular, when $f \in S$ is a self-adjoint idempotent we see that we have the usual decomposition of S,

$$S = Sf \oplus S(e - f).$$

2.3.3 Lemma Let $f \in S$ be a self-adjoint idempotent, then $(Sf)^\perp = S(e - f)$.

Proof:
The proof is exactly the same as in Lemma 2.1.10. □

Now, to prove that every S-submodule N of S is of the form $N = Sf$ for some unique self-adjoint idempotent $f \in S$ we could once again define the orthogonal projection of S onto N. However, it is simpler to use the corresponding result for FG-submodules of FG.

2.3.4 Theorem For each S-submodule N of S, there is a unique self-adjoint idempotent $f \in S$ such that $N = Sf$.

Proof:
Let N be an S-submodule of S. Define $M = FGN$, then, since $N \subset FGe$, M is clearly an FG-submodule of FGe. Consequently, $M = FGf$ for a unique self-adjoint idempotent $f \in FG$ such that $fe = f$. In addition, $f = f^* = (fe)^* = e^*f^* = ef$ and so $f \in eFGe = S$. Hence, we see that

$$Sf = (eFGe)f = e(FGf) = eM = eFGN = (eFGe)N = SN = N.$$

□

As a consequence of this, the self-adjoint idempotents give a bijection between FG-submodules of FGe and S-submodules of S.

2.3.5 Corollary There is a bijective correspondence between FG-submodules of FGe and S-submodules of S given by

$$FGf \leftrightarrow Sf.$$

Proof:

Given an FG-submodule M of FGe, $M = FGf$ for some self-adjoint idempotent $f \in FG$ with $fe = f$. Then $ef = f$ also, so $f \in S$ and Sf is an S-submodule of S. Conversely, given an S-submodule N of S, by Theorem 2.3.4 $N = Sf$ for some self-adjoint idempotent $f \in S$. Then $fe = f$ and FGf is an FG-submodule of FGe. The fact that this is a bijection is due to the uniquness of the self-adjoint idempotents. □

In particular, this bijection sends irreducible modules to irreducible modules.

2.3.6 Corollary FGf is an irreducible FG-submodule of FGe if and only if Sf is an irreducible S-submodule of S.

Proof:

Suppose that $0 \subsetneq FGx \subsetneq FGf$. Then, since $xf = x$ with $x \neq 0$ and $x \neq f$, we have that $0 \subsetneq Sx \subsetneq Sf$. Similarly for the reverse direction. □

Note that the bijection also preserves intersections and sums of modules.

2.3.7 Lemma Let $f_1, \dots, f_n \in S$ be self-adjoint idempotents, then $f_1 \wedge \cdots \wedge f_n$ is the unique self-adjoint idempotent such that

$$Sf_1 \cap \cdots \cap Sf_n = S(f_1 \wedge \cdots \wedge f_n)$$

and $f_1 \vee \cdots \vee f_n$ is the unique self-adjoint idempotent such that

$$Sf_1 + \cdots + Sf_n = S(f_1 \vee \cdots \vee f_n).$$

Proof:

Let $r \in Sf_1 \cap \cdots \cap Sf_n$, then $rf_i = r$ for each i. Hence, by Lemma 2.1.15(iv), $r(f_1 \wedge \cdots \wedge f_n) = f$ and so $r \in S(f_1 \wedge \cdots \wedge f_n)$. Conversely, suppose that $r \in S(f_1 \wedge \cdots \wedge f_n)$, then $r(f_1 \wedge \cdots \wedge f_n) = r$. So, since for each i $f_i f_i = f_i$, by Lemma 2.1.15(iii) $(f_1 \wedge \cdots \wedge f_n) f_i = f_1 \wedge \cdots \wedge f_n$. Thus $rf_i = r$ and $r \in Sf_i$ for each i, so $r \in Sf_1 \cap \cdots \cap Sf_n$. Hence $Sf_1 \cap \cdots \cap Sf_n = S(f_1 \wedge \cdots \wedge f_n)$.

Similarly for $Sf_1 + \cdots + Sf_n = S(f_1 \vee \cdots \vee f_n)$. □

2.4 Constructing the Meet and Join

By Section 2.1 we know that for self-adjoint idempotents $e_1, \ldots, e_n \in FG$, the self-adjoint idempotents $e_1 \wedge \cdots \wedge e_n \in FG$ and $e_1 \vee \cdots \vee e_n \in FG$ from Definition 2.1.14 exist and are unique. However, we would like to be able to construct them using only $e_1, \ldots, e_n$.

In the particular case where the idempotents commute we have the following results:

2.4.1 Lemma Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents such that $e_ie_j = e_je_i$ for each $1 \leq i, j \leq n$. Then

$$e_1 \wedge \cdots \wedge e_n = e_1 \cdots e_n.$$

Proof:

Note that $e_1 \cdots e_n \in FG$ is a self-adjoint idempotent since $(e_1 \cdots e_n)^2 = e_1^2 \cdots e_n^2 = e_1 \cdots e_n$ and $(e_1 \cdots e_n)^* = e_n^* \cdots e_1^* = e_n \cdots e_1 = e_1 \cdots e_n$. Further, for each $1 \leq i \leq n$, we see that $(e_1 \cdots e_n)e_i = e_1 \cdots e_i^2 \cdots e_n = e_1 \cdots e_n$ so $FG(e_1 \cdots e_n) \subset FGe_i$, and therefore $FG(e_1 \cdots e_n) \subset FGe_1 \cap \cdots \cap FGe_n$. Further, for each $r \in FGe_1 \cap \cdots \cap FGe_n$, $r \in FGe_i$ implies $re_i = r$ for each i. Thus $r(e_1 \cdots e_n) = r$ and $r \in FG(e_1 \cdots e_n)$, i.e. $FGe_1 \cap \cdots \cap FGe_n \subset FG(e_1 \cdots e_n)$. Hence $FGe_1 \cap \cdots \cap FGe_n = FG(e_1 \cdots e_n)$ and so, by definition, $e_1 \wedge \cdots \wedge e_n = e_1 \cdots e_n$. □

2.4.2 Corollary Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents such that $e_ie_j = e_je_i$ for each $1 \leq i, j \leq n$. Then

$$e_1 \vee \cdots \vee e_n = 1 - (1 - e_1) \cdots (1 - e_n).$$

Proof:

Note that for each $1 \leq i, j \leq n$, $(1-e_i)(1-e_j) = 1-e_i-e_j+e_ie_j = 1-e_j-e_i+e_je_i = (1-e_j)(1-e_i)$. Thus the result follows from Lemma 2.4.1 and Corollary 2.1.17. □

We now construct $e_1 \wedge \cdots \wedge e_n$ and $e_1 \vee \cdots \vee e_n$ in general for self-adjoint idempotents $e_1, \ldots, e_n \in FG$ where F is a subfield of $\mathbb{C}$. Since $F \subset \mathbb{C}$, by Lemma 2.2.10 and Corollary 2.2.11, we saw that if we consider $e_1, \ldots, e_n$ as self-adjoint idempotents in $\mathbb{C}G$, then

$$e_1 \wedge_F \cdots \wedge_F e_n = e_1 \wedge_{\mathbb{C}} \cdots \wedge_{\mathbb{C}} e_n$$

and

$$e_1 \vee_F \cdots \vee_F e_n = e_1 \vee_{\mathbb{C}} \cdots \vee_{\mathbb{C}} e_n.$$

Thus it suffices to consider the case of self-adjoint idempotents $e_1, \ldots, e_n \in \mathbb{C}G$.

To construct $e_1 \wedge \cdots \wedge e_n$ and $e_n \vee \cdots \vee e_n$ we will use the corresponding orthogonal projections. In particular, we would like to look at limits of certain sequences of compositions of the orthogonal projections, and so we must define a norm on $\mathrm{End}_{\mathbb{C}G}(\mathbb{C}G)$. First note that the inner product on $\mathbb{C}G$ gives rise to the induced norm

$$||r|| = \langle r, r\rangle^{\frac{1}{2}}$$

for each $r \in \mathbb{C}G$. Thus we can define a norm on $\mathrm{End}_{\mathbb{C}G}(\mathbb{C}G)$ by

$$||\psi||_E = \sup\{||\psi(r)|| : r \in \mathbb{C}G, ||r|| \leq 1\}$$

for each $\psi \in \mathrm{End}_{\mathbb{C}G}(\mathbb{C}G)$.

2.4.3 Lemma Let $\psi, \phi \in \mathrm{End}_{\mathbb{C}G}(\mathbb{C}G)$, then $||\psi \circ \phi||_E \leq ||\psi||_E \, ||\phi||_E$.

2.4.4 Lemma Let M be a $\mathbb{C}G$-submodule of $\mathbb{C}G$, then $||P_M||_E = 1$.

Proof:

Let $r \in \mathbb{C}G$, $r = m + n$ with $m \in M$, $n \in N^{\perp}$. Then $\langle r, r\rangle = \langle m+n, m+n\rangle = \langle m, m\rangle + \langle m, n\rangle + \langle n, m\rangle + \langle n, n\rangle = \langle m, m\rangle + \langle n, n\rangle$, i.e. $||r||^2 = ||m||^2 + ||n||^2$. Hence $||P_M(r)|| = ||m|| = (||r||^2 - ||n||^2)^{\frac{1}{2}} \leq ||r||$. □

We can now prove the following result which describes the orthogonal projection onto the intersection of $\mathbb{C}G$-submodules $M_1, \ldots, M_n$ of $\mathbb{C}G$ in terms of the orthogonal projections P_{M_i}.

2.4.5 Theorem Let $M_1, \ldots, M_n$ be $\mathbb{C}G$-submodules of $\mathbb{C}G$ with corresponding orthogonal projections $P_{M_1}, \ldots, P_{M_n}$. Then $\lim_{k\to\infty}(P_{M_n} \circ \cdots \circ P_{M_1})^k = P_N$ where $N = M_1 \cap \cdots \cap M_n$.

Proof:

Let $T = (P_{M_n} \circ \cdots \circ P_{M_1}) - P_N$ and note that $T^k = (P_{M_n} \circ \cdots \circ P_{M_1})^k - P_N$. In addition, we see that

$$T = (P_{M_n} \circ \cdots \circ P_{M_1}) - P_N = (P_{M_n} \circ \cdots \circ P_{M_1}) \circ (I - P_N) = (P_{M_n} \circ \cdots \circ P_{M_1}) \circ P_{N^{\perp}},$$

thus $||T||_E \leq ||P_{M_n}||_E \cdots ||P_{M_1}||_E \, ||P_{N^{\perp}}||_E = 1$. Hence, for each k, $||T^k||_E \leq ||T||_E^k = 1$ and for $l > k$

$$||T^l||_E = ||T^{l-k} \circ T^k||_E \leq ||T||_E^{l-k} \, ||T^k|| = ||T^k||_E .$$

Suppose that $r \in \mathbb{C}G$ with $r \notin N^{\perp}$, then by the proof of Lemma 2.4.4,

$$||T(r)|| \leq ||P_{N^{\perp}}(r)|| < ||r|| .$$

Similarly, if $r \in M_{i-1} \cap \cdots \cap M_1 \cap N^{\perp}$, but $r \notin M_i$, then

$$||T(r)|| \leq \left|\left|P_{M_i} \circ P_{M_{i-1}} \circ \cdots \circ P_{M_1} P_{N^{\perp}}(r)\right|\right| = ||P_{M_i}(r)|| < ||r|| .$$

Hence, we see that $||T(r)|| < ||r||$ for all $r \notin M_n \cap \cdots \cap M_1 \cap N^{\perp} = N \cap N^{\perp} = 0$. Thus if T has eigenvalue λ with eigenvector x, then

$$|\lambda| \, ||x|| = ||\lambda x|| = ||T(x)|| < ||x||$$

and $|\lambda| < 1$. So, if T has eigenvalues $\lambda_1, \ldots, \lambda_m$ then, for each k, T^k has eigenvalues $\lambda_1^k, \ldots, \lambda_m^k$ and, since $|\lambda_i| < 1$ for each i, $\lambda_i^k \to 0$ as $k \to \infty$, i.e. the eigenvalues of T^k tend to 0 as $k \to \infty$.

Now, since $\left|\left|T^k\right|\right|_E \leq 1$ for each k, $\{T^k\}_{k=1}^{\infty}$ is a bounded sequence in $\mathrm{End}_{\mathbb{C}G}(\mathbb{C}G)$ and so has a convergent subsequence $\{T^{k_j}\}_{j=1}^{\infty}$, say $T^{k_j} \to S$ as $j \to \infty$. However, by the above, all the eigenvalues of S are 0 and this implies that $S^m = 0$ for some m. Thus

$$\lim_{j\to\infty} T^{mk_j} = \lim_{j\to\infty} (T^{k_j})^m = \left(\lim_{j\to\infty} T^{k_j}\right)^m = S^m = 0,$$

i.e. $\{T^k\}$ has a subsequence converging to 0. Without loss of generality we may therefore assume that $S = 0$. So, for each $\epsilon > 0$, we may pick k_j such that $\left|\left|T^{k_j}\right|\right|_E < \epsilon$. Thus, for every $k > k_j$ we see that

$$\left|\left|T^k\right|\right|_E \leq \left|\left|T^{k_j}\right|\right|_E < \epsilon,$$

i.e. $T^k \to 0$ as $k \to \infty$. Hence the result. □

As a consequence of this we are able to construct $e_1 \wedge \cdots \wedge e_n$ from the self-adjoint idempotents $e_1, \ldots, e_n$.

2.4.6 Corollary Let $e_1, \ldots, e_n \in \mathbb{C}G$ be self-adjoint idempotents, then

$$e_1 \wedge_{\mathbb{C}} \cdots \wedge_{\mathbb{C}} e_n = \lim_{k\to\infty} (e_1 \cdots e_n)^k.$$

Proof:

From Corollary 2.1.13 and Theorem 2.4.5,

$$\begin{aligned} e_1 \wedge_{\mathbb{C}} \cdots \wedge_{\mathbb{C}} e_n &= P_{\mathbb{C}Ge_1 \cap \cdots \cap \mathbb{C}Ge_n}(1) \\ &= \lim_{k\to\infty} (P_{\mathbb{C}Ge_n} \circ \cdots \circ P_{\mathbb{C}Ge_1})^k(1) \\ &= \lim_{k\to\infty} (e_1 \cdots e_n)^k. \end{aligned}$$

□

2.4.7 Corollary Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents, then

$$e_1 \wedge_F \cdots \wedge_F e_n = \lim_{k\to\infty} (e_1 \cdots e_n)^k \in FG.$$

Proof:
This follows from Lemma 2.2.10. □

2.4.8 Corollary Let $e_1, \ldots, e_n \in FG$ be self-adjoint idempotents, then

$$e_1 \vee_F \cdots \vee_F e_n = \lim_{k\to\infty} 1 - [(1-e_1)\cdots(1-e_n)]^k.$$

Proof:
Use Corollary 2.1.17. □

Note that in general we do not necessarily have $(e_1 \wedge \cdots \wedge e_n) = (e_1 \cdots e_n)^k$ for any k, as the following example shows:

2.4.9 Example Let $G = S_3$, the symmetric group on 3 letters. Define

$$e = \frac{1}{2}(1 + (1 \quad 2)) \text{ and } f = \frac{1}{2}(1 - (1 \quad 3)),$$

then e and f are clearly self-adjoint idempotents in FG. Further, if we let

$$x = \frac{1}{3}(1 + (1 \quad 2) - (1 \quad 3) - (1 \quad 3 \quad 2))$$

then we see that x is also an idempotent in FG, which is not self-adjoint, but is such that $ef = \frac{3}{4}x$. Consequently,

$$\lim_{k\to\infty} (ef)^k = \lim_{k\to\infty} \left(\frac{3}{4}x\right)^k = \lim_{k\to\infty} \left(\frac{3}{4}\right)^k x^k = \lim_{k\to\infty} \left(\frac{3}{4}\right)^k x = 0,$$

and so $e \wedge f = 0$. However $(ef)^k = \left(\frac{3}{4}\right)^k x \neq 0$ for each k.

Chapter 3

Permutation Modules

We now examine the connection between self-adjoint idempotents and representation theory. In particular, we look at permutation modules and their corresponding self-adjoint idempotents.

3.1 Representations and Characters

Before proceeding any further we introduce some basic concepts from representation theory. We will only use a few basic results, but for more detailed results concerning representations see [9], [16] or [12] for characters.

3.1.1 Definition Let G be a group, then an *F-representation* of G is a homomorphism

$$\rho : G \to GL(V)$$

where V is a finite dimensional vector space over F. The *trivial representation* of G is the homomorphism $\rho_1 : G \to GL(F)$ given by $\rho_1(g) = \mathrm{Id}_F$ for each $g \in G$.

3.1.2 Remark F-representations of G and FG-modules are related in the following way. Suppose that we have an F-representation $\rho : G \to GL(V)$, then we can make V into an FG-module by defining the action of G on V by $g \cdot v = \rho(g)v$ for each $g \in G$, $v \in V$. Conversely, given an FG-module M, we have an F-representation of G, $\rho : G \to GL(M)$ where $\rho(g)$ is left multiplication on M by g.

3.1.3 Definition Let $\rho : G \to GL(V)$ be an F-representation of G, then the *F-character* χ of ρ is the map

$$\chi : G \to F; \quad \chi(g) = \mathrm{tr}[\rho(g)].$$

The *trivial character* 1_G of G is the character of the trivial representation ρ_1.

Let M be an FG-module, then χ_M, the *character afforded by* M, is the character of the corresponding representation. Further, χ_M is *irreducible* if M is an irreducible FG-module.

3.1.4 Remark In the particular case where the representation $\rho : G \to \mathrm{GL}(F)$ is 1-dimensional, we have that $\rho(g) \in F$ is a 1 by 1 matrix for each $g \in G$. Thus, since the trace of $\rho(g)$ is $\rho(g)$, $\chi(g) = \rho(g)$ for each $g \in G$, i.e. for 1-dimensional representations there is no difference between the representation and its character.

3.1.5 Lemma Let M and N be FG-modules. Then

(i) $\chi_M(1) = \dim_F(M)$;

(ii) $\chi_M(g^{-1}) = \overline{\chi_M(g)}$;

(iii) $\chi_{M\oplus N} = \chi_M + \chi_N$;

(iv) $\chi_M = \chi_N$ if and only if $M \simeq N$.

3.1.6 Corollary Let ζ be an F-character, then ζ can be expressed uniquely as

$$\zeta = \sum_{i=1}^{r} a_i\chi_i$$

for some irreducible F-characters χ_i and positive integers a_i.

3.1.7 Definition Let χ, ζ be F-characters of G and define

$$(\chi, \zeta) = \frac{1}{|G|}\sum_{g\in G} \chi(g)\overline{\zeta(g)}.$$

Then we see that this gives an inner product on the F-space spanned by the F-characters of G.

3.1.8 Lemma Let $\chi, \chi', \zeta, \zeta'$ be F-characters and $\lambda, \mu \in F$. Then

(i) $(\lambda\chi + \mu\chi', \zeta) = \lambda(\chi, \zeta) + \mu(\chi', \zeta)$;

(ii) $(\chi, \lambda\zeta + \mu\zeta') = \overline{\lambda}(\chi, \zeta) + \overline{\mu}(\chi, \zeta')$;

(iii) $(\chi, \zeta) = \overline{(\zeta, \chi)}$;

(iv) $(\chi, \chi) > 0$.

Moreover, Corollary 3.1.6 shows that it is spanned by the irreducible F-characters of G and below we see that the irreducible F-characters in fact form an orthonormal F-basis.

3.1.9 Lemma Let χ, ζ be irreducible F-characters of G. Then

$$(\chi, \zeta) = \begin{cases} 1 & \text{if } \chi = \zeta, \\ 0 & \text{if } \chi \neq \zeta. \end{cases}$$

3.1.10 Corollary Let ζ be an F-character of G, then

$$\zeta = \sum_{\chi} (\zeta, \chi)\chi$$

where the sum is over the irreducible F-characters χ of G.

3.1.11 Definition Let $\rho : G \to GL(V)$ be an F-representation of G and H be a subgroup of G, then the *restriction* of ρ to H is

$$\mathrm{Res}_H^G \rho = \rho\,|_H\colon H \to GL(V).$$

If χ is the character of ρ, then the character of the restriction $\mathrm{Res}_H^G \rho$ is denoted χ_H.

3.1.12 Definition Let H be a subgroup of G and M be an FH-module, then the *induced* FG-module is defined to be

$$\mathrm{Ind}_H^G M = FG \otimes_{FH} M.$$

If χ is the character of M, then the character of the induced module is denoted χ^G.

The following result is immediate from the definition of induced modules and it gives a necessary and sufficient condition for an FG-submodule of FG to have been induced from an FH-submodule of FH.

3.1.13 Lemma Let H be a subgroup of G and $e \in FH$ a self-adjoint idempotent. Then

$$\mathrm{Ind}_H^G FHe = FGe.$$

Further, if M is an FG-submodule of FG such that $M = FGe$ for a self-adjoint idempotent $e \in FH$, then

$$M = \mathrm{Ind}_H^G FHe.$$

3.2 Characters and Idempotents

We know that for each character of G there is an FG-submodule of FG which affords this character and, further, corresponding to this module there is a unique self-adjoint idempotent. We would like to be able to explicitly construct this idempotent knowing only the character. Unfortunately this is not possible except for certain special cases.

3.2.1 Lemma Let χ be an absolutely irreducible F-character of G, then

$$e_\chi = \frac{1}{|G|}\sum_{g\in G}\chi(1)\chi(g^{-1})g \in FG$$

is the self-adjoint idempotent such that the FG-module FGe_χ affords the character $\chi(1)\chi$.

Proof:
See [12] Theorem 2.12. □

In particular, in the case where we have a linear character of G, i.e. a character afforded by a 1-dimensional representation of G, we get the following result:

3.2.2 Corollary Let $\lambda : G \to \mathrm{GL}(F)$ be a 1-dimensional representation of G. Then

$$u = \frac{1}{|G|}\sum_{g\in G}\lambda(g^{-1})g \in FG$$

is the self-adjoint idempotent such that FGu affords the character λ.

Proof:
For each $x \in G$ we have that

$$xu = \frac{1}{|G|}\sum_{g\in G}\lambda(g^{-1})xg = \frac{1}{|G|}\sum_{g\in G}\lambda(g^{-1}x)g = \frac{1}{|G|}\sum_{g\in G}\lambda(g^{-1})\lambda(x)g = \lambda(x)u.$$

Thus $FGu = Fu$ affords the character λ. Further,

$$u^2 = \frac{1}{|G|}\sum_{x\in G}\lambda(x^{-1})xu = \frac{1}{|G|}\sum_{x\in G}\lambda(x^{-1})\lambda(x)u = \frac{1}{|G|}\sum_{x\in G}u = u$$

and so $u \in FG$ is an idempotent. Finally, u is self-adjoint since $\lambda(g^{-1}) = \overline{\lambda(g)}$ for all $g \in G$. □

We can then extend this to induced characters λ^G using Lemma 3.1.13.

3.2.3 Corollary Let H be a subgroup of G and $\lambda : H \to \mathrm{GL}(F)$ be a 1-dimensional representation of H. Then

$$u = \frac{1}{|H|} \sum_{h \in H} \lambda(h^{-1})h \in FG$$

is the self-adjoint idempotent such that FGu affords the character λ^G.

On the other hand, for each self-adjoint idempotent $e \in FG$ we can easily construct the F-character afforded by the FG-module FGe.

3.2.4 Proposition Let $e \in FG$ be a self-adjoint idempotent and χ the character afforded by the FG-module FGe. Then, for each $g \in G$

$$\chi(g) = \sum_{x \in G} e_{x^{-1}g^{-1}x}.$$

Proof:

Consider the linear map $S : FG \to FG$ given by $r \mapsto gre$. Then for each $h \in G$,

$$S(h) = ghe = gh \sum_{x \in G} e_x x = \sum_{x \in G} e_x ghx = \sum_{x \in G} e_{(gh)^{-1}x}.$$

Hence, the trace of S with respect to the basis $\{g\}_{g \in G}$ is

$$\mathrm{tr}[S] = \sum_{x \in G} e_{(gx)^{-1}x} = \sum_{x \in G} e_{x^{-1}g^{-1}x}.$$

Now suppose that $\{m_1, \ldots, m_n\}$ is an orthogonal basis for FGe. Since FGe is an FG-module, $gm_i = \sum_{j=1}^{n} a_{i,j} m_j$ for some $a_{i,j} \in F$, and then

$$\chi(g) = \sum_{i=1}^{n} a_{i,i}.$$

Further, using the Gram-Schmidt othogonalisation process we can extended this basis to an orthogonal basis for FG, $\{m_1, \ldots, m_n, m_{n+1}, \ldots, m_{|G|}\}$. In particular, we have that $\{m_{n+1}, \ldots, m_{|G|}\}$ is an orthogonal basis for $(FGe)^{\perp} = FG(1-e)$. Thus, for $1 \le i \le n$, $m_i \in FGe$ and so $m_i e = e$, and for $n+1 \le i \le |G|$, $m_i \in FG(1-e)$ and so $m_i e = 0$. Therefore, for each m_i

$$S(m_i) = gm_i e = \begin{cases} \sum_{j=1}^{n} a_{i,j} m_j & \text{if } 1 \le i \le n, \\ 0 & \text{if } n+1 \le i \le |G|. \end{cases}$$

Hence, with respect to the basis $\{m_1, \ldots, m_n, m_{n+1}, \ldots, m_{|G|}\}$ of FG, we also have that

$$\mathrm{tr}[S] = \sum_{i=1}^{n} a_{i,i} = \chi(g).$$

Hence the result follows. □

Consequently, we can find the dimension of the FG-module FGe immediately.

3.2.5 Corollary Let $e \in FG$ be a self-adjoint idempotent. Then

$$\dim_F(FGe) = |G|e_1.$$

Proof:

From Lemma 3.1.5(i), if χ is the character afforded by FGe, then we have that $\chi(1) = \dim_F(FGe)$. Then, by Proposition 3.2.4, this gives

$$\dim_F(FGe) = \chi(1) = \sum_{x \in G} e_{x^{-1}1x} = \sum_{x \in G} e_1 = |G|e_1.$$

□

Further, if we have a decomposition of the self-adjoint idempotent $e \in FG$ into a linear combination of self-adjoint idempotents then we can express the character χ_{FGe} as a corresponding linear combination of characters.

3.2.6 Corollary Let $e \in FG$ be a self-adjoint idempotent which can be expressed as $e = a_1e_1 + \cdots + a_ne_n$ for some self-adjoint idempotents $e_1, \ldots, e_n \in FG$ and $a_1, \ldots, a_n \in F$. Then

$$\chi_{FGe} = a_1\chi_{FGe_1} + \cdots + a_n\chi_{FGe_n}.$$

Proof:

For each $g \in G$ we see that

$$\begin{aligned}
\chi_{FGe}(g) &= \sum_{x \in G} e_{x^{-1}g^{-1}x} \\
&= \sum_{x \in G} (a_1(e_1)_{x^{-1}g^{-1}x} + \cdots + a_n(e_n)_{x^{-1}g^{-1}x}) \\
&= a_1 \sum_{x \in G} (e_1)_{x^{-1}g^{-1}x} + \cdots + a_n \sum_{x \in G} (e_n)_{x^{-1}g^{-1}x} \\
&= a_1\chi_{FGe_1}(g) + \cdots + a_n\chi_{FGe_n}(g).
\end{aligned}$$

□

3.3 Group Sums and Permutation Modules

We now concentrate on a particular case of self-adjoint idempotents.

3.3.1 Definition Let S be a subset of G, and define

$$\widehat{S} = \frac{1}{|S|}\sum_{s\in S} s.$$

Then, when we have a subgroup of G, by Corollary 3.2.3 we get the following result:

3.3.2 Lemma Let H be a subgroup of G, then $\widehat{H} \in FG$ is the self-adjoint idempotent such that $FG\widehat{H}$ affords the character $(1_H)^G$ of G.

3.3.3 Definition Let H be a subgroup of G, then we call the self-adjoint idempotent $\widehat{H} \in FG$ the *group sum* of H, the FG-module $FG\widehat{H}$ the *permutation module* of G on H and the corresponding character $(1_H)^G$ the *permuation character* of G on H.

3.3.4 Lemma Let H and K be subgroups of G, then $\widehat{H}\widehat{K} = \widehat{HK}$.

Proof:

For each $x \in K$ we see that

$$x\widehat{K} = x\left(\frac{1}{|K|}\sum_{k\in K} k\right) = \frac{1}{|K|}\sum_{k\in K} xk = \frac{1}{|K|}\sum_{k\in K} k = \widehat{K}$$

and so if $H \leq K$ then we have that $HK = K$ and

$$\widehat{H}\widehat{K} = \frac{1}{|H|}\sum_{h\in H} h\widehat{K} = \frac{1}{|H|}\sum_{h\in H} \widehat{K} = \widehat{K} = \widehat{HK}.$$

Suppose now that $H \not\leq K$ and let $\mathcal{T}$ be a left transversal for $H \cap K$ in H. Then we see that $HK = \cup_{t\in\mathcal{T}} tK$, but if $t, s \in \mathcal{T}$ are such that $tK = sK$ then $t = sk$ for some $k \in K$. Thus $k = s^{-1}t \in H$ implies that $k \in H \cap K$ and so $t = s$. Hence $HK = \bigsqcup_{t\in\mathcal{T}} tK$ and

$$\begin{aligned}\widehat{H}\widehat{K} &= \frac{1}{|H|}\sum_{h\in H} h\widehat{K} \\ &= \frac{1}{|H|}\sum_{t\in\mathcal{T}}\sum_{x\in H\cap K} tx\widehat{K}\end{aligned}$$

$$
\begin{aligned}
&= \frac{|H\cap K|}{|H|}\sum_{t\in\mathcal{T}} t\widehat{H\cap K}\widehat{K} \\
&= \frac{|H\cap K|}{|H|}\sum_{t\in\mathcal{T}} t\widehat{K} \\
&= \frac{|H\cap K|}{|H||K|}\sum_{t\in\mathcal{T}}\sum_{k\in K} tk \\
&= \frac{1}{|HK|}\sum_{x\in HK} x \\
&= \widehat{HK},
\end{aligned}
$$

since $|HK| = |H||K|/|H\cap K|$. □

Note that if we do not assume that H and K are groups then this is not in general true.

We now prove some basic results about permutation modules which we will need later.

3.3.5 Lemma $FG\widehat{H}$ has F-basis $\{t\widehat{H}\}_{t\in\mathcal{T}}$ where $\mathcal{T}$ is a left transversal for H in G.

Proof:

Clearly, $FG\widehat{H}$ is spanned by $\{g\widehat{H}\}_{g\in G}$. Let $\mathcal{T}$ be a left transversal for H in G, then for any $t\in\mathcal{T}$ and $g\in tH$ we see that $g = th$ and so $g\widehat{H} = th\widehat{H} = t\widehat{H}$. Hence, $\{t\widehat{H}\}_{t\in\mathcal{T}}$ spans $FG\widehat{H}$ and, further, the coefficient of g in $t\widehat{H}$ is 0 if $g\notin tH$ and non-zero if $g\in tH$. So $\{t\widehat{H}\}_{t\in\mathcal{T}}$ must be linearly independent, since the left cosets of H in G are disjoint, and therefore is a basis for $FG\widehat{H}$. □

3.3.6 Lemma Let H, K be subgroups of G. Then

(i) $FG\widehat{H}\subset FG\widehat{K}$ if and only if $K\le H$;

(ii) $FG\widehat{H}\cap FG\widehat{K} = FG\widehat{\langle H, K\rangle}$;

(iii) $FG\widehat{H} + FG\widehat{K}\subset FG\widehat{H\cap K}$.

Proof:

(i) Suppose that $K\le H$, then by Lemma 3.3.4, $\widehat{H}\widehat{K} = \widehat{HK} = \widehat{H}$ implying that $FG\widehat{H}\subset FG\widehat{K}$. Conversely, if $FG\widehat{H}\subset FG\widehat{K}$, then $\widehat{H} = \widehat{H}\widehat{K} = \widehat{HK}$ so $HK = H$, i.e. $K\le H$.

(ii) Since $H \leq \langle H, K\rangle$ and $K \leq \langle H, K\rangle$, by part (i) we see that $FG\widehat{\langle H, K\rangle} \subset FG\widehat{H}$ and $FG\widehat{\langle H, K\rangle} \subset FG\widehat{K}$, so $FG\widehat{\langle H, K\rangle} \subset FG\widehat{H} \cap FG\widehat{K}$. Now, for any $r \in FG\widehat{H} \cap FG\widehat{K}$ we see that $r\widehat{H} = r$ and $r\widehat{K} = r$. Thus, for any $h \in H$, $rh = r\widehat{H}h = r\widehat{H} = r$ and, similarly, for each $k \in K$, $rk = r\widehat{K}k = r\widehat{K} = r$. So, since each $x \in \langle H, K\rangle$ can be expressed as $x = h_1 k_1 \cdots h_n k_n$ for some $h_i \in H$ and $k_i \in K$, we see that $rx = rh_1 k_1 \cdots h_n k_n = r$. In particular this means that

$$r\widehat{\langle H, K\rangle} = \frac{1}{|\langle H, K\rangle|} \sum_{x \in \langle H, K\rangle} rx = \frac{1}{|\langle H, K\rangle|} \sum_{x \in \langle H, K\rangle} r = r$$

and so $r \in FG\widehat{\langle H, K\rangle}$. Hence $FG\widehat{H} \cap FG\widehat{K} \subset FG\widehat{\langle H, K\rangle}$ and therefore $FG\widehat{H} \cap FG\widehat{K} = FG\widehat{\langle H, K\rangle}$.

(iii) $H \cap K \leq H$ and $H \cap K \leq K$ implies that $FG\widehat{H} \subset FG\widehat{H \cap K}$ and $FG\widehat{K} \subset FG\widehat{H \cap K}$ by (i). Thus $FG\widehat{H} + FG\widehat{K} \subset FG\widehat{H \cap K}$. □

3.4 Infinite Products of Group Sums

By Lemma 3.3.6(ii), for subgroups $H_1, \ldots, H_n$ of G we have that

$$FG\widehat{H_1} \cap \cdots \cap FG\widehat{H_n} = FG\widehat{\langle H_1, \ldots, H_n\rangle},$$

and so,

$$\widehat{H_1} \wedge \cdots \wedge \widehat{H_n} = \widehat{\langle H_1, \ldots, H_n\rangle}.$$

In this section we will demonstrate how we can use Corollary 2.4.7 to prove this result, i.e. we will show that

$$\lim_{k \to \infty} (\widehat{H_1} \cdots \widehat{H_n})^k = \widehat{\langle H_1, \ldots, H_n\rangle}.$$

In fact, we will prove a stronger result about arbitrary products of group sums.

Let $\{H_k\}_{k=1}^{\infty}$ be a sequence of subgroups of G such that for each $k \geq 1$ there is some $l > k$ with $H_l = H_k$. Further, denote by H the subgroup of G generated by $\{H_k\}_{k=1}^{\infty}$.

Suppose that

$$\widehat{H_1} \cdots \widehat{H_k} = \sum_{g \in G} a_g(k) g,$$

and

$$\widehat{H_k} \cdots \widehat{H_l} = \sum_{g \in G} b_g(k, l) g,$$

for each $l > k$. Then, we see that

$$\begin{aligned}\widehat{H_1}\cdots\widehat{H_k}\widehat{H_{k+1}}\cdots\widehat{H_l} &= \left(\sum_{g\in G} a_g(k)g\right)\left(\sum_{x\in G} b_x(k+1,l)g\right) \\ &= \sum_{g\in G}\sum_{x\in G} a_g(k)b_x(k+1,l)gx \\ &= \sum_{g\in G}\left(\sum_{x\in G} a_{gx^{-1}}(k)b_x(k+1,l)\right)g\end{aligned}$$

and so

$$a_g(l) = \sum_{x\in G} a_{gx^{-1}}(k)b_x(k+1,l).$$

As a special case of this we see

$$a_g(k+1) = \frac{1}{|H_{k+1}|}\sum_{x\in H_{k+1}} a_{gx^{-1}}(k).$$

Hence, since $\sum_{g\in G} a_g(1) = \frac{1}{|H_1|}\sum_{x\in H_1} 1 = 1$ we see that for each k,

$$\sum_{g\in G} a_g(k+1) = \frac{1}{|H_{k+1}|}\sum_{g\in G}\sum_{x\in H_{k+1}} a_{gx^{-1}}(k) = \frac{1}{|H_{k+1}|}\sum_{g\in G}\sum_{x\in H_{k+1}} a_g(k) = \sum_{g\in G} a_g(k) = 1.$$

Similarly, for each $l > k$ we also have $\sum_{g\in G} b_g(k,l) = 1$.

3.4.1 Lemma For each k, $a_g(k) = 0$ if $g \notin H_1\cdots H_k$ and $a_g(k) > 0$ if $g \in H_1\cdots H_k$.

Proof:

Clearly, $a_g(1) = 0$ if $g \notin H_1$ and $a_g(1) > 0$ if $g \in H_1$. Now suppose that $a_g(k) = 0$ if $g \notin H_1\cdots H_k$ and $a_g(k) > 0$ if $g \in H_1\cdots H_k$. In particular this means that $a_g(k) \geq 0$ for all $g \in G$. Note that if $g \notin H_1\cdots H_kH_{k+1}$, then $gx^{-1} \notin H_1\cdots H_k$ for all $x \in H_{k+1}$, since $gx^{-1} \in H_1\cdots H_k$ with $x \in H_{k+1}$ implies $g = gx^{-1}x \in H_1\cdots H_kH_{k+1}$. Thus

$$a_g(k+1) = \sum_{x\in H_{k+1}} \frac{a_{gx^{-1}}(k)}{|H_{k+1}|} = 0.$$

On the other hand, if $g \in H_1\cdots H_kH_{k+1}$ then $g = g'x$ for some $g' \in H_1\cdots H_k$ and $x \in H_k$, and so $gx^{-1} = g' \in H_1\cdots H_k$. This then gives

$$a_g(k+1) = \sum_{x\in H_{k+1}} \frac{a_{gx^{-1}}(k)}{|H_{k+1}|} > 0,$$

and the result follows by induction. □

3.4.2 Corollary For each $l > k$, $b_g(k,l) = 0$ if $g \notin H_k \cdots H_l$ and $b_g(k,l) > 0$ if $g \in H_k \cdots H_l$.

3.4.3 Lemma There exists some n such that $H_1 \cdots H_n = H$.

Proof:

Since G is finite, the increasing chain of subsets

$$H_1 \subset H_1 H_2 \subset \cdots \subset H_1 \cdots H_k \subset \cdots \subset G$$

must stabilise, i.e. there exists some n such that for each $m > n$,

$$H_1 \cdots H_n H_{n+1} \cdots H_m = H_1 \cdots H_n.$$

In particular this means that for all $m > n$, $H_1 \cdots H_n H_m = H_1 \cdots H_n$ and, since for each $k \leq n$ there must be some $m > n$ with $H_k = H_m$, $(H_1 \cdots H_n)(H_1 \cdots H_n) = H_1 \cdots H_n$. Hence $(H_1 \cdots H_n) = \langle H_1, \ldots, H_n \rangle = H$. □

3.4.4 Corollary For any k, there exists some n such that $H_k \cdots H_{k+n} = H$.

By Lemma 3.4.1 and the definition of H, $a_g(k) = 0$ for all $g \notin H$ and all k, so we would like to examine $\lim_{k\to\infty} a_h(k)$ for each $h \in H$. Clearly, for all $h \in H$ and for each k, $\min_{g\in G}\{a_g(k)\} \leq a_h(k) \leq \max_{g\in G}\{a_g(k)\}$. Thus

$$\lim_{k\to\infty} \min_{g\in G}\{a_g(k)\} \leq \lim_{k\to\infty} a_h(k) \leq \lim_{k\to\infty} \max_{g\in G}\{a_g(k)\}.$$

Further, by Lemma 3.4.3 we know that for some n and for all $k \geq n$, $a_h(k) > 0$ so we can instead consider $\min^+_{g\in G}\{a_g(k)\}$, the minimum over the non-zero $a_g(k)$. Thus, if we can show that $\lim_{k\to\infty} \min^+_{g\in G}\{a_g(k)\} = \lim_{k\to\infty} \max_{g\in G}\{a_g(k)\}$ we can then find $\lim_{k\to\infty} a_h(k)$ for all $h \in H$. To do this we first prove the following properties of the max and $\min^+$ of the $a_g(k)$:

3.4.5 Lemma For each k,

(i) $\max_{g\in G}\{a_g(k+1)\} \leq \max_{g\in G}\{a_g(k)\}$;

(ii) $\min^+_{g\in G}\{a_g(k+1)\} \geq \frac{1}{|H_{k+1}|} \min^+_{g\in G}\{a_g(k)\}$ if $H_1 \cdots H_k \neq H_1 \cdots H_k H_{k+1}$;

(iii) $\min^+_{g\in G}\{a_g(k+1)\} \geq \min^+_{g\in G}\{a_g(k)\}$ if $H_1 \cdots H_k = H_1 \cdots H_k H_{k+1}$;

where $\min^+$ denotes the minimum over the non-zero terms.

Proof:

We see that for each $g \in G$,

$$a_g(k+1) = \sum_{x \in H_{k+1}} \frac{a_{gx^{-1}}(k)}{|H_{k+1}|} \leq \sum_{x \in H_{k+1}} \frac{\max_{g \in G}\{a_g(k)\}}{|H_{k+1}|} = \max_{g \in G}\{a_g(k)\}$$

so $\max_{g \in G}\{a_g(k+1)\} \leq \max_{g \in G}\{a_g(k)\}$. Further, if $a_g(k+1) > 0$ then $g \in H_1 \cdots H_{k+1}$ and so, by the argument in Lemma 3.4.1, there is some $x \in H_k$ with $gx^{-1} \in H_1 \cdots H_k$, i.e. $a_{gx^{-1}}(k) > 0$ for some $x \in H_k$. Thus, if $a_g(k+1) > 0$,

$$a_g(k+1) = \sum_{x \in H_{k+1}} \frac{a_{gx^{-1}}(k)}{|H_{k+1}|} \geq \frac{\min^+_{g \in G}\{a_g(k)\}}{|H_{k+1}|}$$

and so $\min_{g \in G}{}^+\{a_g(k+1)\} \geq \frac{1}{|H_{k+1}|}\min_{g \in G}{}^+\{a_g(k)\}$.

Suppose now that $H_1 \cdots H_k = H_1 \cdots H_k H_{k+1}$. For each $g \in H_1 \cdots H_k H_{k+1}$ and $x \in H_{k+1}$ we see that $g \in H_1 \cdots H_k$ and $x^{-1} \in H_{k+1}$ implying that $gx^{-1} \in H_1 \cdots H_k H_{k+1} = H_1 \cdots H_k$. Hence, if $a_g(k+1) > 0$ and then for each $x \in H_{k+1}$, $a_{gx^{-1}}(k) > 0$ and so

$$a_g(k+1) = \sum_{x \in H_{k+1}} \frac{a_{gx^{-1}}(k)}{|H_{k+1}|} \geq \sum_{x \in H_{k+1}} \frac{\min_{g \in G}{}^+\{a_g(k)\}}{|H_{k+1}|} = \min_{g \in G}{}^+\{a_g(k)\}.$$

Consequently, $\min_{g \in G}{}^+\{a_g(k+1)\} \geq \min_{g \in G}{}^+\{a_g(k)\}$. □

Similarly, we have the following results for the max and min$^+$ of the $b_g(k,l)$:

3.4.6 Corollary For each $l > k$,

(i) $\max_{g \in G}\{b_g(k,l+1)\} \leq \max_{g \in G}\{b_g(k,l)\}$;

(ii) $\min^+_{g \in G}\{b_g(k,l+1)\} \geq \frac{1}{|H_{l+1}|}\min^+_{g \in G}\{b_g(k,l)\}$ if $H_k \cdots H_l \neq H_k \cdots H_l H_{l+1}$;

(iii) $\min^+_{g \in G}\{b_g(k,l+1)\} \geq \min^+_{g \in G}\{b_g(k,l)\}$ if $H_k \cdots H_l = H_k \cdots H_l H_{l+1}$;

where min$^+$ denotes the minimum over the non-zero terms.

Using this we can obtain a uniform lower bound for $\min^+_g\{b_g(k,l)\}$.

3.4.7 Corollary For each k, l with $l > k$, $\min^+_{g \in G}\{b_g(k,l)\} \geq \frac{1}{|G|^{|G|}}$.

Proof:

Consider the increasing chain of subsets of G

$$H_k \subset H_k H_{k+1} \subset \cdots \subset H_k \cdots H_j \subset \cdots \subset H_k \cdots H_l.$$

We can pick $k = k_1 < \cdots < k_i < \cdots < k_r \le l$ such that for each $i \ge 2$, $H_k \cdots H_{k_i - 1} \neq H_k \cdots H_{k_i-1} H_{k_i}$ and for each $j \neq k_i$ for any i, $H_k \cdots H_{j-1} = H_k \cdots H_{j-1} H_j$. This gives us a maximal strictly increasing subchain

$$H_{k_1} \subsetneq H_{k_1} \cdots H_{k_2} \subsetneq \cdots \subsetneq H_{k_1} \cdots H_{k_i} \subsetneq \cdots \subsetneq H_{k_1} \cdots H_{k_r}$$

where

$$H_{k_1} \cdots H_{k_{i-1}} = H_{k_1} \cdots H_{k_{i-1}} H_{k_{i-1}+1} = \cdots = H_{k_1} \cdots H_{k_i - 1} \subsetneq H_n \cdots H_{k_i}.$$

Thus, by Corollary 3.4.6(ii)

$$\min_{g \in G}{}^{+} \{b_g(k, k_i)\} \ge \frac{1}{|H_{k_i}|} \min_{g \in G}{}^{+} \{b_g(k, k_i - 1)\}$$

and, by Corollary 3.4.6(iii),

$$\min_{g \in G}{}^{+} \{b_g(k, k_i - 1)\} \ge \min_{g \in G}{}^{+} \{b_g(k, k_i - 2)\} \ge \cdots \ge \min_{g \in G}{}^{+} \{b_g(k, k_{i-1})\}.$$

Hence,

$$\min_{g \in G}{}^{+} \{b_g(k, k_i)\} \ge \frac{1}{|H_{k_i}|} \min_{g \in G}{}^{+} \{b_g(k, k_{i-1})\}$$

and so, since $\min^+_{g \in G}\{b_g(k,k)\} = \frac{1}{|H_k|}$,

$$\min_{g \in G}{}^{+} \{b_g(k, l)\} \ge \min_{g \in G}{}^{+} \{b_g(k, k_r)\} \ge \frac{1}{|H_{k_r}| \cdots |H_{k_2}|} \min_{g \in G}{}^{+} \{b_g(k, k_1)\} = \frac{1}{|H_{k_1}| \cdots |H_{k_r}|}.$$

The result then follows since any strictly increasing chain of subsets of G can contain at most $|G|$ subsets, each of which has size at most $|G|$. □

3.4.8 Theorem $\lim_{k \to \infty} \widehat{H_1} \cdots \widehat{H_k} = \widehat{H}$.

Proof:

Define a sequence $\{n_i\}_{i=0}^{\infty}$ by $n_0 = 0$ and, for each $i \ge 1$, $n_i > n_{i-1}$ is such that

$$H_{n_{i-1}+1} \cdots H_{n_i} = H.$$

Note that such a sequence must exist by Corollary 3.4.4. Since by definition

$$H_1 \cdots H_{n_{i-1}} = H_{n_{i-1}+1} \cdots H_{n_i} = H,$$

for each $i > 1$, we have that $a_g(n_{i-1}) > 0$ and $b_g(n_{i-1} + 1, n_i) > 0$ for all $g \in H$ and $a_g(n_{i-1}) = 0$ and $b_g(n_{i-1} + 1, n_i) = 0$ for all $g \notin H$. Thus, for any $g, h \in H$ we have that

$$\sum_{x \in H} (a_{gx^{-1}}(n_{i-1}) - a_{hx^{-1}}(n_{i-1})) = \sum_{x \in G} a_{gx^{-1}}(n_{i-1}) - \sum_{x \in G} a_{hx^{-1}}(n_{i-1}) = 1 - 1 = 0$$

so $a_{gx^{-1}}(n_{i-1}) - a_{hx^{-1}}(n_{i-1}) < 0$ for at least one $x \in H$. Thus, if we let $T \subsetneq G$ be the set of all $x \in H$ such that $a_{gx^{-1}}(n_{i-1}) - a_{hx^{-1}}(n_{i-1}) \geq 0$ we see that

$$\begin{aligned}
& a_g(n_i) - a_h(n_i) \\
= & \sum_{x \in H} (a_{gx^{-1}}(n_{i-1}) - a_{hx^{-1}}(n_{i-1}))\, b_x(n_{i-1}+1, n_i) \\
< & \sum_{x \in T} (a_{gx^{-1}}(n_{i-1}) - a_{hx^{-1}}(n_{i-1}))\, b_x(n_{i-1}+1, n_i) \\
\leq & \left(\max_{h \in H}\{a_h(n_{i-1})\} - \min_{h \in H}\{a_h(n_{i-1})\}\right) \left(\sum_{x \in T} b_x(n_{i-1}+1, n_i)\right) \\
\leq & \left(\max_{h \in H}\{a_h(n_{i-1})\} - \min_{h \in H}\{a_h(n_{i-1})\}\right) (1 - \min_{g \in G}{}^{+}\{b_g(n_{i-1}+1, n_i)\}) \\
\leq & \left(\max_{h \in H}\{a_h(n_{i-1})\} - \min_{h \in H}\{a_h(n_{i-1})\}\right) \left(1 - \frac{1}{|G|^{|G|}}\right),
\end{aligned}$$

and so for each $i \geq 1$,

$$\max_{h \in H}\{a_h(n_i)\} - \min_{h \in H}\{a_h(n_i)\} < \left(1 - \frac{1}{|G|^{|G|}}\right) \left(\max_{h \in H}\{a_h(n_{i-1})\} - \min_{h \in H}\{a_h(n_{i-1})\}\right).$$

Consequently,

$$\max_{h \in H}\{a_h(n_i)\} - \min_{h \in H}\{a_h(n_i)\} < \left(1 - \frac{1}{|G|^{|G|}}\right)^i$$

and

$$\lim_{i \to \infty} \max_{h \in H}\{a_h(n_i)\} - \min_{h \in H}\{a_h(n_i)\} = 0.$$

Thus, since for each k there is some $n_i \geq k$ and

$$\max_{h \in H}\{a_h(n_i)\} - \min_{h \in H}\{a_h(n_i)\} \geq \max_{h \in H}\{a_h(k)\} - \min_{h \in H}\{a_h(k)\},$$

we also have

$$\lim_{k \to \infty} \max_{h \in H}\{a_h(k)\} - \min_{h \in H}\{a_h(k)\} = 0.$$

Finally, since $\max_{h \in H}\{a_h(k)\} \geq \frac{1}{|H|} \geq \min_{h \in H}\{a_h(k)\}$,

$$\lim_{k \to \infty} \max_{h \in H}\{a_h(k)\} = \frac{1}{|H|} = \lim_{k \to \infty} \min_{h \in H}\{a_h(k)\},$$

and therefore, since $a_g(k) = 0$ for all $g \notin H$ and for all k,

$$\lim_{k \to \infty} a_g(k) = \begin{cases} \frac{1}{|H|} & \text{if } g \in H \\ 0 & \text{if } g \notin H, \end{cases}$$

i.e. $\lim_{k \to \infty} \widehat{H_1} \cdots \widehat{H_k} = \widehat{H}$. □

3.4.9 Remark This result essentially follows from the theory of finite Markov chains and inhomogeneous products of non-negative matrices (see [2] and [17]). First note that without loss of generality we may assume $H = G$. For a subgroup H_i of G, the matrix corresponding to right multiplication by $\widehat{H_i}$ on FG is a non-negative doubly stochastic matrix. Further, if we let M_k be the matrix corresponding to $\widehat{H_{n_{k-1}+1}} \cdots \widehat{H_{n_k}}$ then, by Corollary 3.4.7 and the definition of n_k, the M_k are uniformly Markov. Hence, we have weak ergodicity at a geometric rate in the product $\lim_{k\to\infty} M_k \cdots M_1$, i.e. $[M_k \cdots M_1]_{i,s} - [M_k \cdots M_1]_{j,s} \to 0$ for each i, j and s as $k \to 0$. Thus, this shows that for each $g, h \in G$, $a_g(n_i) - a_h(n_i) \to 0$ as $i \to 0$. Finally, by Lemma 3.4.5, this in turn implies that $a_g(n) - a_h(n) \to 0$ as $n \to 0$.

3.4.10 Corollary Let $\{H_k\}_{k=1}^{\infty}$ be an arbitrary sequence of subgroups of G, then

$$\lim_{k\to\infty} \widehat{H_1} \cdots \widehat{H_k} = \widehat{H_1} \cdots \widehat{H_n} \widehat{H}$$

for some n such that for each $i > n$ there exists $j > i$ with $H_j = H_i$ and where H is the subgroup generated by $\{H_k\}_{k=n+1}^{\infty}$.

Proof:

It suffices to show that such an n exists since then the result follows from Theorem 3.4.8 using the sequence $\{H_k\}_{k=n+1}^{\infty}$.

Let K be an arbitrary subgroup of G, then either there exists some $m(K)$ such that $H_j \neq K$ for all $j > m(K)$ or, for any i, there exists $j > i$ with $H_j = K$. Since there are only a finite number of subgroups of G we can set $n = \max_K m(K)$, where the maximum is taken over the subgroups of the first type. Then we see that for any subgroup H_i with $i > n$, H_i must be of the second type, i.e. there exists some $j > i$ with $H_j = H_i$. □

Chapter 4

Application to Coxeter Groups and Finite Groups with BN-pair

In this chapter we give two examples of well known irreducible characters which can be expressed as alternating sums of permutation characters, the sign character for Coxeter groups and the Steinberg character for finite groups with BN-pair, and show that we can use permutation modules to construct FG-modules which afford these characters.

4.1 Coxeter Groups

4.1.1 Definition A *Coxeter group* is a finite group W with a presentation

$$W = \langle s_1, \ldots s_n : (s_i s_j)^{m_{i,j}} = 1, 1 \leq i, j \leq n \rangle ,$$

where the $\{m_{i,j}\}$ are positive integers such that

(i) $m_{i,i} = 1$;

(ii) $m_{i,j} > 1$ if $i \neq j$; and

(iii) $m_{j,i} = m_{i,j}$ for all $1 \leq i, j \leq n$.

Let $S = \{s_1, \ldots, s_n\}$, then the pair (W, S) is called a *Coxeter system*.

4.1.2 Example Let $W = S_{n+1}$, the symmetric group on $n + 1$ letters. For $1 \leq i \leq n$, define $s_i = (i \quad i+1)$ then W has a presentation given by

$$W = \langle s_1, \ldots, s_n : (s_i s_j)^{m_{i,j}} = 1, 1 \leq i, j \leq n \rangle$$

where

$$m_{i,j} = \begin{cases} 3 & \text{if } |i-j| = 1, \\ 2 & \text{otherwise.} \end{cases}$$

The following are standard definitions and results for Coxeter groups; see [3] Chapitre VI or [8] for proofs.

4.1.3 Definition Let $w \in W$, then the *length* of w, denoted $l(w)$, is the minimum number of factors needed to express w as a product the s_i, i.e.

$$l(w) = \min\{r : w = s_{i_1} \cdots s_{i_r} \text{ with } s_{i_1}, \ldots, s_{i_r} \in S\}.$$

The expression $w = s_{i_1} \cdots s_{i_r}$ is said to be in *reduced form* if $r = l(w)$.

In particular we have that $l(s_i) = 1$ for each $s_i \in S$ and $l(1) = 0$. Further, $l(w)$ satisfies the following properties:

4.1.4 Proposition Let $w, w' \in W$. Then

(i) $l(w^{-1}) = l(w)$;

(ii) $l(ww') \leq l(w) + l(w')$;

(iii) $l(ww') \geq |l(w) - l(w')|$.

4.1.5 Corollary Let $w \in W$ and $s \in S$. Then $l(sw) = l(w) \pm 1$.

We now define certain subgroups of W generated by elements of S.

4.1.6 Definition Let (W, S) be a Coxeter system and let J be a subset of S. Define W_J to be the subgroup $W_J = \langle J \rangle$. In particular $W_\emptyset = \{1\}$ and $W_S = W$.

Then we see that the subgroups W_J have the following properties:

4.1.7 Proposition Let (W, S) be a finite Coxeter system and $I, J \subset S$. Then

(i) $W_I \leq W_J$ if and only if $I \subset J$;

(ii) $W_I \cap W_J = W_{I \cap J}$;

(iii) $\langle W_I, W_J \rangle = W_{I \cup J}$.

4.2 The Sign Character

4.2.1 Definition Let W be a Coxeter group, then the sign character $\epsilon : W \to F$ is defined to be

$$\epsilon(w) = (-1)^{l(w)}$$

for each $w \in W$.

By Corollary 3.2.2, we know that if we define $u \in FW$ to be the self-adjoint idempotent

$$u = \frac{1}{|W|} \sum_{w \in W} (-1)^{l(w)} w$$

then ϵ is afforded by the FW-module FWu. We will now construct this module using permutation modules.

4.2.2 Definition Let (W, S) be a Coxeter system and let M be the FW-module in the orthogonal decomposition

$$FW = M \oplus \left(\sum_{i=1}^{n} FW\widehat{W_{\{s_i\}}} \right).$$

4.2.3 Theorem $M = FWu$.

Proof:

For each i, let $W_i = W_{\{s_i\}}$. By Lemma 2.1.16,

$$M = FW(1 - \widehat{W_1}) \cap \cdots \cap FW(1 - \widehat{W_n}).$$

and so $M = FWe$ where $e = (1 - \widehat{W_1}) \wedge \cdots \wedge (1 - \widehat{W_n})$. Now, since

$$s_i(1 - \widehat{W_i}) = s_i \left(\frac{1}{2} - \frac{1}{2} s_i \right) = \frac{1}{2} s_i - \frac{1}{2} = (-1) \left(\frac{1}{2} - \frac{1}{2} s_i \right) = (-1)(1 - \widehat{W_i}),$$

we see that

$$s_i e = s_i(1 - \widehat{W_i})e = (-1)(1 - \widehat{W_i})e = (-1)e.$$

Thus, for any $w = s_{i_1} \cdots s_{i_{l(w)}} \in W$,

$$we = s_{i_1} \cdots s_{i_{l(w)}} e = (-1) \cdots (-1)e = (-1)^{l(w)} e.$$

Hence, we see that $FWe = Fe$, i.e. $\dim_F(M) \le 1$.

On the other hand, since $wu = (-1)^{l(w)}u$ for each $w \in W$, we see that for each $1 \leq i \leq n$

$$(1 - \widehat{W_i})u = \left(\frac{1}{2} - \frac{1}{2}s_1\right)u = \frac{1}{2}u - \frac{1}{2}s_1 u = \frac{1}{2}u + \frac{1}{2}u = u.$$

Thus, by Lemma 2.1.15(iv), $ue = u$ and $FWu \subset FWe$. Hence $M = FWu$. □

4.2.4 Remark Solomon, in [18], expressed the sign character as an alternating sum of permutation characters

$$\epsilon = \sum_{J \subset S} (-1)^{|J|}(1_{W_J})^W;$$

see, for example, [8] Section 66.

4.3 Finite Groups with BN-pair

4.3.1 Definition Let G be a finite group, then it has a BN-pair if it has subgroups B and N such that

(i) $G = \langle B, N \rangle$;

(ii) $B \cap N$ is normal in N;

(iii) $W = N/(B \cap N)$ is generated by a set $S = \{s_1, \cdots, s_n\}$ of elements such that $s_i^2 = 1$;

(iv) $sBw \subset BwB \cup BswB$ for all $s \in S$ and $w \in W$;

(v) $sBs \not\subseteq B$ for all $s \in S$.

Since the double cosets $B\overline{w}B$ are independent of the choice of coset representative $\overline{w}$ for w we denote them simply as BwB.

4.3.2 Example Let $G = \mathrm{GL}_{n+1}(\mathbb{Z}/p\mathbb{Z})$ and define

$$B = \{[m_{i,j}] \in G : m_{i,j} = 0, i > j\}$$

and

$$N = \{[m_{i,j}] \in G : \text{for each } 1 \leq i \leq n,\ m_{i,j} \neq 0 \text{ for some } j \text{ and } m_{i,k} = 0 \text{ for } k \neq j\}.$$

Then we find that these give a BN-pair for G, and further

$$\begin{aligned} W &= \{[m_{i,j}] \in G : \text{for each } 1 \leq i \leq n,\ m_{i,j} = 1 \text{ for some } j \text{ and } m_{i,k} = 0 \text{ for } k \neq j\} \\ &\simeq S_n. \end{aligned}$$

Again, the following are standard definitions and results for finite groups with BN-pair; see [3] Chapitre IV, [4] or [8].

4.3.3 Theorem Let G be a finite group with BN-pair, then

$$G = \bigsqcup_{w \in W} BwB.$$

4.3.4 Lemma (W, S) is a Coxeter system, and further for all $s_i \in S$ and $w \in W$,

(i) If $l(s_i w) \geq l(w)$, then $s_i B w \subset B s_i w B$;

(ii) If $l(s_i w) \leq l(w)$, then $s_i B w \not\subset B s_i w B$.

4.3.5 Corollary W has a presentation $W = \langle s_1, \cdots, s_n : (s_i s_j)^{m_{ij}} = 1 \rangle$.

Since the (B, B)-double cosets of G are parameterised by the Coxeter group W, we can use the subgroups W_J of W to construct subgroups of G containing B.

4.3.6 Definition Let $J \subset S$, and define $P_J = BW_JB$.

We see that the subgroups P_J have properties similar to the properties for W_J given in Proposition 4.1.7.

4.3.7 Proposition Let $I, J \subset S$, then

(i) $P_I \leq P_J$ if and only if $I \leq J$;

(ii) $P_I \cap P_J = P_{I \cap J}$;

(iii) $\langle P_I, P_J \rangle = P_{I \cup J}$.

Further, we define a particular subring of FG which is related to the group ring FW of W.

4.3.8 Definition Let G be a finite group with BN-pair and define the *Hecke ring* $\mathcal{H}_F(G, B)$ to be

$$\mathcal{H}_F(G, B) = \widehat{B} FG \widehat{B}.$$

In a similar way to Lemma 3.3.5 we see, $\mathcal{H}_F(G, B)$ has an F-basis given by the (B, B)-double cosets of G.

4.3.9 Lemma $\mathcal{H}_F(G,B)$ has F-basis $\{\beta_w\}_{w\in W}$ where

$$\beta_w = q(w)\widehat{B}w\widehat{B}$$

and

$$q(w) = \frac{|BwB|}{|B|}.$$

In particular, multiplication of the basis elements is given in the following way:

4.3.10 Theorem For each $s_i \in S$ and $w \in W$,

$$\beta_{s_i}\beta_w = \begin{cases} \beta_{s_i w} & \text{if } l(s_i w) > l(w), \\ q(s_i)\beta_{s_i w} + (q(s_i)-1)\beta_w & \text{if } l(s_i w) < l(w). \end{cases}$$

This in turn leads to a presentation of the Hecke ring in terms of generators and relations which is obtained from the presentation of W as a Coxeter group.

4.3.11 Theorem $\mathcal{H}_F(G,B)$ is generated by the elements $\{\beta_{s_i}\}_{s_i\in S}$ with relations

$$\beta_{s_i}^2 = q(s_i)1 + (q(s_i)-1)\beta_{s_i}$$

and

$$\begin{aligned} (\beta_{s_i}\beta_{s_j})^{k_{i,j}} &= (\beta_{s_j}\beta_{s_i})^{k_{i,j}} & \text{if } m_{i,j} = 2k_{i,j}, \\ (\beta_{s_i}\beta_{s_j})^{k_{i,j}}\beta_{s_i} &= (\beta_{s_j}\beta_{s_i})^{k_{i,j}}\beta_{s_j} & \text{if } m_{i,j} = 2k_{i,j}+1. \end{aligned}$$

4.4 The Steinberg Character

4.4.1 Remark In [19], Steinberg defined for $\mathrm{GL}_n(\mathbf{F}_q)$ an irreducible subrepresentation of $\mathrm{Ind}_B^G\rho_1$ with degree $q^{n(n-1)/2}$, i.e. the highest power of q dividing the order of $\mathrm{GL}_n(\mathbf{F}_q)$. Later, in [20], Steinberg extended this construction to other linear groups and in [21] gave a corresponding $\mathbb{C}G$-submodule of $\mathbb{C}G\widehat{B}$ for all finite groups with BN-pair. Curtis, in [5], then gave a construction for the character St of this module using a correspondence between the irreducible characters of G and of W. In particular, he showed that the Steinberg character corresponded to the sign character of W and so, using Solomon's formula, that it could be expressed as an alternating sum of permutation characters

$$\mathrm{St} = \sum_{J\subset S}(-1)^{|J|}(1_{P_J})^G.$$

The construction of the Steinberg character which we will use was given by Curtis, Iwahori and Kilmoyer in [7].

We first state some standard results which we will need for the construction; see [6] for proofs.

4.4.2 Theorem Let ζ be an irreducible character of $\mathbb{C}G$ such that $(\zeta, (1_B)^G) > 0$. Then the restriction $\zeta_{\mathcal{H}_{\mathbb{C}}(G,B)}$ is an irreducible character of $\mathcal{H}_{\mathbb{C}}(G, B)$ of degree $(\zeta, (1_B)^G)$. Conversely, each irreducible character ϕ of $\mathcal{H}_{\mathbb{C}}(G, B)$ is the restriction to $\mathcal{H}_{\mathbb{C}}(G, B)$ of a unique irreducible character ζ of $\mathbb{C}G$.

Note that this is essentially a character theoretic version of Corollaries 2.3.5 and 2.3.6. In the case where ϕ is a linear character, the following result gives us a construction for the corresponding self-adjoint idempotent.

4.4.3 Theorem Let $\phi : \mathcal{H}_{\mathbb{C}}(G, B) \to \mathbb{C}$ be a homomorphism. Then ϕ is the restriction to $\mathcal{H}_{\mathbb{C}}(G, B)$ of a unique irreducible character ζ of G such that $(\zeta, (1_B)^G) = 1$. Moreover,

$$u = \frac{\zeta(1)}{|G : B|} \sum_{w \in W} \frac{1}{q(w)} \phi(\beta_{w^{-1}}) \beta_w$$

is a primitive idempotent in $\mathbb{C}G$ such that $\mathbb{C}Gu$ affords ζ.

Now, consider the homomorphism $\phi : \mathcal{H}_{\mathbb{C}}(G, B) \to \mathbb{C}$ given by

$$\phi(\beta_w) = (-1)^{l(w)}$$

for each $w \in W$. Using the presentation for $\mathcal{H}_{\mathbb{C}}(G, B)$ given in Theorem 4.3.11 it is clear that this is indeed a homomorphism. Thus, by Theorem 4.4.2 it is the restriction of a unique irreducible character of G, the Steinberg character St. Further, by Theorem 4.4.3 St is afforded by the $\mathbb{C}G$-module $\mathbb{C}Gu$ where

$$u = \frac{\mathrm{St}(1)}{|G : B|} \sum_{w \in W} \frac{(-1)^{l(w)}}{q(w)} \beta_w.$$

We now prove that the ϕ is afforded by the $\mathcal{H}_F(G, B)$-module $\mathcal{H}_F(G, B)u$ and therefore that the Steinberg character is afforded by the FG-module FGu with $u \in FG$ defined above.

4.4.4 Proposition $u \in FG$ is the self-adjoint idempotent such that $\mathcal{H}_F(G, B)u$ affords the character $\phi : \mathcal{H}_F(G, B) \to F$ defined by

$$\phi(\beta_w) = (-1)^{l(w)}.$$

Proof:

First fix $1 \leq i \leq n$ and denote by W' the set of all $w \in W$ which cannot be expressed in reduced form as $w = s_i w'$ for some $w' \in W$. Then, clearly we have that $W = W' \sqcup s_i W'$, since if $w \in W$ is such that $w = s_i w'$ is in reduced form for some $w' \in W$, then we must have that $w' \in W'$.

Thus, for each $w \in W'$ we see that

$$\begin{aligned} \beta_{s_i}(q(s_i)\beta_w - \beta_{s_i w}) &= q(s_i)\beta_{s_i}\beta_w - \beta_{s_i}\beta_{s_i w} \\ &= q(s_i)\beta_{s_i w} - q(s_i)\beta_w - (q(s_i) - 1)\beta_{s_i w} \\ &= (-1)(q(s_i)\beta_w - \beta_{s_i w}). \end{aligned}$$

In addition,

$$u = \frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{(-1)^{l(w)}}{q(w)}\beta_w = \frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W'}\frac{(-1)^{l(w)}}{q(s_i w)}(q(s_i)\beta_w - \beta_{s_i w}),$$

so we see that

$$\begin{aligned} \beta_{s_i} u &= \frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W'}\frac{(-1)^{l(w)}}{q(s_i w)}\beta_{s_i}(q(s_i)\beta_w - \beta_{s_i w}) \\ &= \frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W'}\frac{(-1)^{l(w)}}{q(s_i w)}(-1)(q(s_i)\beta_w - \beta_{s_i w}) \\ &= (-1)u. \end{aligned}$$

Thus, since it is true for each $1 \leq i \leq n$, for any $w = s_{i_1} \cdots s_{i_{l(w)}} \in W$ we get

$$\beta_w u = \beta_{s_{i_1}} \cdots \beta_{s_{i_{l(w)}}} u = (-1)\cdots(-1)u = (-1)^{l(w)}u.$$

Hence $\mathcal{H}_F(G,B)u = Fu$ affords the character ϕ. Now, u is clearly self-adjoint and

$$\begin{aligned} u^2 &= \frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{(-1)^{l(w)}}{q(w)}\beta_w u \\ &= \frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{(-1)^{l(w)}}{q(w)}(-1)^{l(w)}u \\ &= \left(\frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{1}{q(w)}\right)u. \end{aligned}$$

So

$$u' = \left(\frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{1}{q(w)}\right)^{-1} u$$

must be the self-adjoint idempotent such that $\mathcal{H}_F(G,B)u'$ affords ϕ. Consequently, $u' \in FG$ must also be the self-adjoint idempotent such that FGu' affords the Steinberg character St. Therefore, by Corollary 3.2.5,

$$\begin{aligned}
\mathrm{St}(1) &= |G|u'_1 \\
&= |G|\left(\frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{1}{q(w)}\right)^{-1} u_1 \\
&= |G|\left(\frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{1}{q(w)}\right)^{-1} \frac{\mathrm{St}(1)}{|G:B|}\frac{1}{|B|} \\
&= \mathrm{St}(1)\left(\frac{\mathrm{St}(1)}{|G:B|}\sum_{w\in W}\frac{1}{q(w)}\right)^{-1}.
\end{aligned}$$

Thus, we must have that $u' = u$, i.e. $u \in FG$ is the self-adjoint idempotent such that $\mathcal{H}_F(G,B)u$ affords the character ϕ, and further that

$$\mathrm{St}(1) = |G:B|\left(\sum_{w\in W}\frac{1}{q(w)}\right)^{-1},$$

which corresponds to the formula given in [6] Theorem 3.1. □

4.4.5 Corollary $u \in FG$ is the self-adjoint idempotent such that FGu affords the Steinberg character St.

In an analogous way to the sign character for Coxeter groups, we construct the $\mathcal{H}_F(G,B)$-module affording ϕ using modules of the form $\mathcal{H}_F(G,B)\widehat{P}$ for subgroups P of G containing B.

4.4.6 Definition Let G be a finite group with BN-pair and define X to be the $\mathcal{H}_F(G,B)$-submodule of $\mathcal{H}_F(G,B)$ in the orthogonal decomposition

$$\mathcal{H}_F(G,B) = X \oplus \sum_{i=1}^{n} \mathcal{H}_F(G,B)\widehat{P_{\{s_i\}}}.$$

4.4.7 Theorem $X = \mathcal{H}_F(G,B)u$.

Proof:

If we define $P_i = P_{\{s_i\}}$, we see that

$$X = \mathcal{H}_F(G,B)(\widehat{B} - \widehat{P_1}) \cap \cdots \cap \mathcal{H}_F(G,B)(\widehat{B} - \widehat{P_n})$$

and so $X = \mathcal{H}_F(G,B)e$ where $e = (\widehat{B} - \widehat{P_1}) \wedge \cdots \wedge (\widehat{B} - \widehat{P_n})$. In particular, we see that for each $1 \le i \le n$, $\widehat{P_i}(\widehat{B} - \widehat{P_i}) = \widehat{P_i} - \widehat{P_i} = 0$ and so $\widehat{P_i}e = \widehat{P_i}(\widehat{B} - \widehat{P_i})e = 0$. Now $P_i = P_{\{s_i\}} = B\langle s_i\rangle B = B \sqcup Bs_iB$. Thus,

$$\widehat{P_i} = \frac{1}{|P_i|}\sum_{x\in P_i} x = \frac{1}{|P_i|}\sum_{x\in B} x + \frac{1}{|P_i|}\sum_{x\in Bs_iB} x = \frac{1}{|P_i : B|}(\beta_1 + \beta_{s_i}).$$

So, since $\widehat{P_i}e = 0$ for each i, $(\beta_1 + \beta_{s_i})e = 0$ and $\beta_{s_i}e = (-1)(\beta_1)e = (-1)e$. Hence, for any $w = s_{i_1}\cdots s_{i_{l(w)}} \in W$

$$\beta_w e = \beta_{s_{i_1}} \cdots \beta_{s_{i_{l(w)}}} e = (-1)\cdots(-1)e = (-1)^{l(w)}e.$$

So $\mathcal{H}_F(G,B)e = Fe$, i.e. $\dim_F(X) \le 1$.

Further, since $\beta_{s_i}u = (-1)u$ for each i, we see that

$$\begin{aligned}(\widehat{B} - \widehat{P_i})u &= \left(\frac{|P_i : B| - 1}{|P_i : B|}\beta_1 - \frac{1}{|P_i : B|}\beta_{s_i}\right)u \\ &= \frac{|P_i : B| - 1}{|P_i : B|}\beta_1 u - \frac{1}{|P_i : B|}\beta_{s_i}u \\ &= \frac{|P_i : B| - 1}{|P_i : B|}u + \frac{1}{|P_i : B|}u \\ &= u.\end{aligned}$$

Thus, by Lemma 2.1.15(iv), $ue = u$, and $\mathcal{H}_F(G,B)u \subset \mathcal{H}_F(G,B)e$. Hence $X = \mathcal{H}_F(G,B)u$. □

Immediately from this result we can construct the FG-module affording the Steinberg character using only permutation modules.

4.4.8 Definition Let M be the FG-module in the orthogonal decomposition

$$FG\widehat{B} = M \oplus \sum_{i=1}^{n} FG\widehat{P_i}.$$

4.4.9 Lemma $M = FGu$

Proof:

Again, we see that

$$M = FG(\widehat{B} - \widehat{P_1}) \cap \cdots \cap FG(\widehat{B} - \widehat{P_n})$$

and so $M = FGe$ where $e = (\widehat{B} - \widehat{P_1}) \wedge \cdots \wedge (\widehat{B} - \widehat{P_n})$. By Theorem 4.4.7 we see that $\mathcal{H}_F(G,B)e = \mathcal{H}_F(G,B)u$ and thus, by the uniqueness of the self-adjoint idempotents $e = u$, i.e. $M = FGu$. □

Chapter 5

Application to $\mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$

In a similar way to Chapter 4, we examine the irreducible character of $\mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$ given by Hill in [11] as an analogue of the Steinberg character for $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. In particular, we construct certain subgroups of $\mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$ and use them to construct an FG-module which affords this character and then express the character as an alternating sum of permutation characters.

5.1 Preliminaries

Define $R = R_h = \mathbb{Z}/p^h\mathbb{Z}$, then R_h has a unique maximal ideal pR_h and every ideal of R_h is of the form $p^a R_h$ for some $0 \leq a \leq h$. We can define a map $v : R_h \to \{0,..,h\}$ by $v(r) = a$ if and only if $r \in p^a R_h$ and $r \neq p^{a+1} R_h$, and $v(0) = h$. In particular, the map v satisfies the following properties:

5.1.1 Lemma Let $r, s \in R_h$. Then

(i) $v(r) = 0$ if and only if $r \in R_h^\times$;

(ii) $v(rs) = \min(v(r) + v(s), h)$;

(iii) $v(r+s) \geq \min(v(r), v(s))$;

(iv) If $v(r) \neq v(s)$ then $v(r+s) = \min(v(r), v(s))$.

More importantly, we can define a ring epimorphism

$$\Delta_a : R_h \to R_a; r \mapsto \begin{cases} r & \text{if } v(r) < a \\ 0 & \text{if } v(r) \geq a. \end{cases}$$

Then, $\ker \Delta_a = p^a R_h$ and so $|p^a R_h| = p^{h-a}$.

Now define $G = G(h) = GL(n, R_h)$ to be the group consisting of all invertible n by n matrices with entries in R_h. Then Δ_a induces a group epimorphism

$$\delta_a : G(h) \to G(a); [r_{i,j}]_{i,j} \mapsto [\Delta_a(r_{i,j})]_{i,j}$$

which has kernel $K(a) = \{I + M_n(p^a R_h)\}$. By definition $K(a)$ is a normal subgroup of $G(h)$ and $G(h)/K(a) \simeq G(a)$.

5.1.2 Lemma $|G(h)| = p^{n^2 h - n(n+1)/2} \prod_{k=1}^{n} (p^k - 1)$.

Proof:
$G(h)/K(a) \simeq G(a)$ implies that $|G(h)| = |G(a)| \cdot |K(a)|$. In particular for $a = 1$ we get that

$$\begin{aligned} |G(h)| &= |K(1)| \cdot |G(1)| \\ &= p^{n^2(h-1)} p^{n(n-1)/2} (p^n - 1) \cdots (p - 1) \\ &= p^{n^2 h - n(n+1)/2} \prod_{k=1}^{n} (p^k - 1). \end{aligned}$$

□

Similarly, define $B = B_n = \{[r_{i,j}]_{i,j} \in G : r_{i,j} = 0 \text{ for } j > i\}$, i.e. the subgroup of G consisting of upper triangular matrices. By restriction we get a group epimorphism $\delta_a : B(h) \to B(a)$ with kernel $B(h) \cap K(a)$ and so, $B(h)/(B(h) \cap K(a)) \simeq B(a)$.

5.1.3 Lemma $|B(h)| = p^{n(n+1)h/2 - n} (p - 1)^n$.

Proof:
Again, $B(h)/(B(h) \cap K(a)) \simeq B(a)$ implies that $|B(h)| = |B(h) \cap K(a)| \cdot |B(a)|$. In particular, for $a = 1$,

$$\begin{aligned} |B(h)| &= |B(h) \cap K(1)| \cdot |B(1)| \\ &= p^{n(n+1)(h-1)/2} p^{n(n-1)/2} (p - 1)^n \\ &= p^{n(n+1)h/2 - n} (p - 1)^n. \end{aligned}$$

□

5.1.4 Corollary $|G(h) : B(h)| = p^{n(n-1)(h-1)/2} \prod_{k=1}^{n-1} (p^k + p^{k-1} + \cdots + 1)$.

5.2 The $n = 2$ Case

We now investigate the case $n = 2$ fully and decompose the permutation module $FG\widehat{B}$ into irreducibles. Since $FG\widehat{B}$ has F-basis $\{t\widehat{B}\}_{t\in\mathcal{T}}$ where $\mathcal{T}$ is a left transversal for B in G, we will first find the left cosets of B in G.

5.2.1 Lemma The left cosets of B in G are $\begin{bmatrix}1 & 0\\ r & 1\end{bmatrix}B$, for $r \in R_h$, and $\begin{bmatrix}s & 1\\ 1 & 0\end{bmatrix}B$, for $v(s) > 0$.

Proof:
Let $[r_{i,j}] \in G$. Then if $v(r_{1,1}) = 0$,

$$\begin{bmatrix}1 & 0\\ r_{2,1}{r_{1,1}}^{-1} & 1\end{bmatrix}\begin{bmatrix}r_{1,1} & r_{1,2}\\ 0 & r_{2,2} - {r_{1,1}}^{-1}r_{1,2}r_{2,1}\end{bmatrix} = \begin{bmatrix}r_{1,1} & r_{1,2}\\ r_{2,1} & r_{2,2}\end{bmatrix}$$

and if $v(r_{1,1}) > 0$ then we must have that $v(r_{2,1}) = 0$ and $v(r_{1,1}{r_{2,1}}^{-1}) > 0$, in which case

$$\begin{bmatrix}r_{1,1}{r_{2,1}}^{-1} & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}r_{1,2} & r_{2,2}\\ 0 & r_{1,2} - r_{1,1}{r_{2,1}}^{-1}r_{2,2}\end{bmatrix} = \begin{bmatrix}r_{1,1} & r_{1,2}\\ r_{2,1} & r_{2,2}\end{bmatrix}.$$

Now, since $|G : B| = p^h + p^{h-1}$ these must all be distinct left cosets. □

Similarly, since we will again be considering the subring $\widehat{B}FG\widehat{B}$ of FG, we also find the (B, B)-double cosets of B in G.

5.2.2 Lemma The (B, B)-double cosets in G are

$$B\begin{bmatrix}1 & 0\\ p^a & 1\end{bmatrix}B = \bigsqcup_{v(r)=a}\begin{bmatrix}1 & 0\\ r & 1\end{bmatrix}B$$

for $1 \le a \le h$, and

$$B\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}B = \bigsqcup_{v(r)=0}\begin{bmatrix}1 & 0\\ r & 1\end{bmatrix}B \bigsqcup_{v(s)>0}\begin{bmatrix}s & 1\\ 1 & 0\end{bmatrix}B.$$

Proof:
Let $v(r) = 0$ and $0 \le a \le h$, then we see that

$$\begin{bmatrix}1 & 0\\ 0 & r\end{bmatrix}\begin{bmatrix}1 & 0\\ p^a & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & r^{-1}\end{bmatrix} = \begin{bmatrix}1 & 0\\ p^a r & 1\end{bmatrix}$$

and, for $a = 0$ and $v(s) > 0$,

$$\begin{bmatrix}-1 & 1+s\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix} = \begin{bmatrix}s & 1\\ 1 & 0\end{bmatrix}.$$

Hence, we see that for $1 \leq a \leq h$

$$\dot{\bigsqcup_{v(r)=a}} \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix} B \subset B \begin{bmatrix} 1 & 0 \\ p^a & 1 \end{bmatrix} B$$

and for $a = 0$,

$$\bigsqcup_{v(r)=0} \begin{bmatrix} 1 & 0 \\ r & 1 \end{bmatrix} \bigsqcup_{v(s)>0} \begin{bmatrix} s & 1 \\ 1 & 0 \end{bmatrix} B \subset B \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} B.$$

In particular, this means that

$$G = \bigcup_{a=0}^{h} B \begin{bmatrix} 1 & 0 \\ p^a & 1 \end{bmatrix} B.$$

Finally, suppose that $[b_{i,j}], [b'_{i,j}] \in B$, then for $0 \leq a \leq h$

$$\begin{bmatrix} b_{1,1} & b_{1,2} \\ 0 & b_{2,2} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ p^a & 1 \end{bmatrix} \begin{bmatrix} b'_{1,1} & b'_{1,2} \\ 0 & b'_{2,2} \end{bmatrix} = \begin{bmatrix} b_{1,1}b'_{1,1} + p^a b_{1,2}b'_{1,1} & b_{1,1}b'_{1,2} + b_{1,2}b'_{2,2} + p^a b_{1,2}b'_{1,2} \\ p^a b_{2,2}b'_{1,1} & b_{2,2}b'_{2,2} + p^a b_{2,2}b'_{1,2} \end{bmatrix}.$$

So, since $v(p^a b_{2,2} b'_{1,1}) = a$, the double cosets must be distinct. □

Note that we can characterise the (B, B)-double cosets in the following way:

5.2.3 Corollary For $0 \leq a \leq h$,

$$B \begin{bmatrix} 1 & 0 \\ p^a & 1 \end{bmatrix} B = \left\{ \begin{bmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \end{bmatrix} \in G : v(r_{2,1}) = a \right\}.$$

Now, we can use the (B, B)-double cosets to define subgroups of G containing B.

5.2.4 Definition For each $0 \leq a \leq h$, define

$$H_a = \bigsqcup_{k=a}^{h} B \begin{bmatrix} 1 & 0 \\ p^k & 1 \end{bmatrix} B.$$

5.2.5 Lemma For each $0 \leq a \leq h$, H_a is a subgroup of G.

Proof:

From Corollary 5.2.3

$$H_a = \left\{ \begin{bmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \end{bmatrix} \in G : v(r_{2,1}) \geq a \right\}.$$

Thus, for any $[r_{i,j}], [s_{i,j}] \in H_a$,

$$\begin{bmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \end{bmatrix} \begin{bmatrix} s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2} \end{bmatrix} = \begin{bmatrix} r_{1,1}s_{1,1} + r_{1,2}s_{2,1} & r_{1,1}s_{1,2} + r_{1,2}s_{2,2} \\ r_{2,1}s_{1,1} + r_{2,2}s_{2,1} & r_{2,1}s_{1,2} + r_{2,2}s_{2,2} \end{bmatrix} \in H_a$$

since $v(r_{2,1}s_{1,1} + r_{2,2}s_{2,1}) \geq \min\{v(r_{2,1}) + v(s_{1,1}), v(r_{2,2}) + v(s_{2,1})\} \geq a$. □

In particular, the subgroups H_a have the following properties:

5.2.6 Lemma Let $0 \leq a, b \leq h$, then

(i) $H_a \leq H_b$ if and only if $a \geq b$;

(ii) $H_a \cap H_b = H_{\max(a,b)}$;

(iii) $\langle H_a, H_b \rangle = H_{\min(a,b)}$.

Proof:
These results are clear from the definition of H_a. □

Using these subgroups we construct the following FG-submodules of $FG\widehat{B}$.

5.2.7 Definition For each $1 \leq a \leq h$ define M_a to be the FG-module in the orthogonal decomposition

$$FG\widehat{H_a} = M_a \oplus FG\widehat{H_{a-1}}$$

and define $M_0 = FG\widehat{H_0} = FG\widehat{G}$.

We will show that these are irreducible FG-modules. To do this, in the same way as for the Steinberg character, we consider the subring $\widehat{B}FG\widehat{B}$ of FG.

5.2.8 Definition Define the *Hecke ring* $\mathcal{H}_F(G, B)$ to be

$$\mathcal{H}_F(G, B) = \widehat{B}FG\widehat{B}.$$

Again, the Hecke ring has an F-basis parameterised by the (B, B)-double cosets in G.

5.2.9 Lemma $\mathcal{H}_F(G, B)$ has F-basis $\{\beta_a\}_{a=0}^{h}$ where

$$\beta_a = q_a \widehat{B} \begin{bmatrix} 1 & 0 \\ p^a & 1 \end{bmatrix} \widehat{B}$$

with $q_0 = p^h$, $q_h = 1$ and $q_a = p^{h-a} - p^{h-a-1}$ for $1 \leq a \leq h - 1$.

Proof:

Since $\mathcal{H}_F(G,B) = \widehat{B}FG\widehat{B}$ it is clearly spanned by $\left\{\widehat{B}x\widehat{B}\right\}_{x\in G}$. However, for each $g \in BxB$ there exist $b, b' \in B$ such that $g = bxb'$, and so $\widehat{B}g\widehat{B} = \widehat{B}bxb'\widehat{B} = \widehat{B}x\widehat{B}$. Thus, $\mathcal{H}_F(G,B)$ is spanned by $\left\{\widehat{B}x\widehat{B}\right\}_{x\in D}$ where D is a complete set of (B,B)-double coset representatives in G. Further, by Lemma 3.3.4

$$\widehat{B}x\widehat{B} = \widehat{B}x\widehat{B}x^{-1}x = \widehat{B}x\widehat{Bx^{-1}}x = \widehat{BxBx^{-1}}x = \widehat{BxB}.$$

Thus, since the coefficient of g in $\widehat{BxB}$ is 0 for $g \notin BxB$ and non-zero for $g \in BxB$, we must have that $\left\{\widehat{B}x\widehat{B}\right\}_{x\in D}$ is linearly independent and therefore is an F-basis for $\mathcal{H}_F(G,B)$. The result then follows from Lemma 5.2.2. □

We now use the subgroups H_a to define the $\mathcal{H}_F(G,B)$-modules corresponding to the FG-modules M_a.

5.2.10 Definition Define N_a to be the $\mathcal{H}_F(G,B)$-module in the orthogonal decomposition

$$\mathcal{H}_F(G,B)\widehat{H_a} = N_a \oplus \mathcal{H}_F(G,B)\widehat{H_{a-1}}$$

and $N_0 = \mathcal{H}_F(G,B)\widehat{H_0} = \mathcal{H}_F(G,B)\widehat{G}$.

Note that $M_a = FGe_a$ and $N_a = \mathcal{H}_F(G,B)e_a$ where

$$e_a = \begin{cases} \widehat{H_a} - \widehat{H_{a-1}} & \text{if } a \neq 0 \\ \widehat{H_0} & \text{if } a = 0, \end{cases}$$

and so N_a is indeed the $\mathcal{H}_F(G,B)$-module corresponding to the FG-submodule M_a of $FG\widehat{B}$ in the sense of Corollary 2.3.5. Further, the $\mathcal{H}_F(G,B)$-module N_a is irreducible for each a by the following:

5.2.11 Lemma $\mathcal{H}_F(G,B)e_a = Fe_a$.

Proof:

In the case where $a = 0$ we see that $e_0 = \widehat{G}$ and so $\mathcal{H}_F(G,B)e_0 = F\widehat{G}$. So, we will now assume that $a > 0$.

Let $b \geq a$, then we see that

$$\beta_b e_a = q_b\left(\widehat{B}\begin{bmatrix}1 & 0\\ p^b & 1\end{bmatrix}\widehat{B}\right)(\widehat{H_a} - \widehat{H_{a-1}}) = q_b(\widehat{H_a} - \widehat{H_{a-1}}) = q_b e_a.$$

Now, for any $b < a$,

$$\widehat{H_b}e_a = \widehat{H_b}(\widehat{H_a} - \widehat{H_{a-1}}) = 0.$$

In addition,

$$H_b = H_{b+1} \sqcup \left(B \begin{bmatrix} 1 & 0 \\ p^b & 1 \end{bmatrix} B \right),$$

so $\beta_b = p^{h-b}\widehat{H_b} - p^{h-b-1}\widehat{H_{b+1}}$. Thus

$$\beta_b e_a = p^{h-b}\widehat{H_b} e_a - p^{h-b-1}\widehat{H_{b+1}} e_a = \begin{cases} -p^{h-a} e_a & \text{if } b = a-1, \\ 0 & \text{if } b < a-1. \end{cases}$$

□

Thus we see that we can decompose $\mathcal{H}_F(G, B)$ into irreducible $\mathcal{H}_F(G, B)$-modules.

5.2.12 Corollary $\mathcal{H}_F(G, B) = N_h \oplus \cdots \oplus N_0$.

Proof:
Clearly $N_a \cap N_{a'} = \emptyset$ for $a \neq a'$ since $e_a \neq e_{a'}$, and so the result follows since $\dim_F(N_a) = 1$ by Lemma 5.2.11 and $\dim_F H_F(G, B) = h + 1$ by Lemma 5.2.9. □

Further, we must have that each M_a is an irreducible FG-module.

5.2.13 Corollary For each a, M_a is an irreducible FG-module with character

$$\chi_a = \begin{cases} (1_{H_a})^G - (1_{H_{a-1}})^G & \text{if } a \neq 0, \\ 1_G & \text{if } a = 0. \end{cases}$$

Proof:
Irreducibility follows from Corollary 2.3.6 and the character from Corollary 3.2.6. □

Hence, we get the following decomposition of $FG\widehat{B}$ into irreducible FG-modules.

5.2.14 Corollary $FG\widehat{B} = M_h \oplus \cdots \oplus M_0$.

Proof:
This follows from the corresponding decomposition for $\mathcal{H}_F(G, B)$. □

Now consider the following FG-submodule of $FG\widehat{B}$.

5.2.15 Definition For each h define

$$M = \begin{cases} M_h \oplus M_{h-2} \oplus \cdots \oplus M_0 & \text{if } h \cong 0 \bmod 2, \\ M_h \oplus M_{h-2} \oplus \cdots \oplus M_1 & \text{if } h \cong 1 \bmod 2. \end{cases}$$

5.2.16 Lemma $\chi_M = \sum_{a=0}^{h} (-1)^{h-a} (1_{H_a})^G$.

5.2.17 Corollary $\chi_M(1) = p^h$.

5.2.18 Remark Lees, in [15], constructs a virtual character S_G, which is an analogue of the Steinberg character for $\mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$, and that can be expressed as an alternating sum of permutation characters

$$S_G = \sum_{(k)} (-1)^{|(k)|} (1_{H_{(k)}})^G$$

where $H_{(k)}$ are certain subgroups of G containing B. For the case where $n = 2$, these subgroups are exactly the subgroups H_a constructed above and we see that $S_G = \chi_M$.

5.3 The Subgroups K_J

Now, for the general case we construct certain subgroups of G which contain B in a manner similar to the construction of the subgroups P_J for a finite groups with BN-pair. First we start by constructing subgroups of G which are analogous to the subgroups W_J.

5.3.1 Definition For each $1 \leq i \leq n-1$ define

$$x_i(r) = \begin{bmatrix} I_{i-1} & & & \\ & 1 & 0 & \\ & r & 1 & \\ & & & I_{n-1-i} \end{bmatrix}$$

and, in particular, for each $1 \leq i \leq n-1$, let $\sigma_i = x_i(p^{h-1})$.

Clearly, the $x_i(r)$ satisfy the following properties:

5.3.2 Lemma Let $r, s \in R$, then

(i) $x_i(r)x_i(s) = x_i(r+s)$;

(ii) $x_i(r)x_j(s) = x_j(s)x_i(r)$ if $|i-j| > 1$;

(iii) $x_i(r)x_{i+1}(s) = x_{i+1}(s)x_i(r)$ if $rs = 0$.

5.3.3 Definition Let $J \subset S = \{1, \ldots, n-1\}$, and define $V_J = \langle \sigma_j : j \in J \rangle$.

5.3.4 Lemma Let $J \subset S$, then if $J = \{j_1, \ldots, j_k\}$, with $j_1 < \cdots < j_k$,

$$V_J = \{x_{j_1}(r_1) \cdots x_{j_k}(r_k) : v(r_i) \geq h-1\}.$$

Proof:

By Lemma 5.3.2, for each i, j, $\sigma_i\sigma_j = \sigma_j\sigma_i$ and, for each a, $\sigma_j^a = x_j(p^{h-1}a)$. Consequently, each element of V_J is of the form $x_{j_1}(p^{h-1}a_1)\cdots x_{j_k}(p^{h-1}a_k)$. Conversely, if $v(r) \geq h-1$ then $r = p^{h-1}a$ and $x_j(r) = \sigma_j^a \in V_J$. □

5.3.5 Corollary $|V_J| = p^{|J|}$.

Immediately from Lemma 5.3.4 we see that the subgroups V_J satisfy the following properties:

5.3.6 Lemma Let $I, J \subset S$, then

(i) $V_I \leq V_J$ if and only if $I \subset J$;

(ii) $V_I \cap V_J = V_{I\cap J}$;

(iii) $V_I V_J = V_{I\cup J}$;

Using the subgroups V_J, we define subgroups of G which contain B.

5.3.7 Definition Let $J \subset S$ and define $K_J = BV_JB$.

5.3.8 Lemma $K_J = V_JB$.

Proof:

Clearly, $V_JB \subset BV_JB = K_J$. Now, let m denote the $n-j$ by j matrix with $(1,j)$-th entry p^{h-1} and 0's elsewhere. Then for any $v(p^{h-1}r) \geq h-1$,

$$x_j(p^{h-1}r) = \begin{bmatrix} I_j & 0 \\ rm & I_{n-j} \end{bmatrix}.$$

Further, for each $b \in B_j$, $mb = b_{1,1}m$ and for each $b'' \in B_{n-j}$, $b''m = b''_{n-j,n-j}m$. Hence, for each $\begin{bmatrix} b & b' \\ 0 & b'' \end{bmatrix} \in B$,

$$\begin{aligned} & \begin{bmatrix} b & b' \\ 0 & b'' \end{bmatrix} \begin{bmatrix} I_j & 0 \\ rm & I_{n-j} \end{bmatrix} \\ = & \begin{bmatrix} b + b'rm & b' \\ b''_{n-j,n-j}rm & b'' \end{bmatrix} \\ = & \begin{bmatrix} I_j & 0 \\ (b_{1,1})^{-1}b''_{n-j,n-j}rm & I_{n-j} \end{bmatrix} \begin{bmatrix} b + b'rm & b' \\ 0 & b'' - (b_{1,1})^{-1}b''_{n-j,n-j}rmb' \end{bmatrix} \end{aligned}$$

and so, for each $b = [b_{i,j}] \in B$ we have that

$$bx_j(p^{h-1}r) = x(p^{h-1}rb_{1,1}{}^{-1}b_{n,n})b'$$

for some $b' \in B$, where $v(b_{1,1}{}^{-1}b_{n,n}) = 0$. Consequently, for any $x_{j_1}(r_1)\cdots x_{j_k}(r_k) \in V_J$ we see that

$$bx_{j_1}(r_1)\cdots x_{j_k}(r_k) = x_{j_1}(r_1')\cdots x_{j_k}(r_k')b'$$

for some $b' \in B$ and some $v(r_i') = v(r_i)$. Hence $BV_J \subset V_JB$ and $K_J = BV_JB \subset V_JB$. □

5.3.9 Corollary K_J is a group.

Proof:
$K_JK_J = (V_JB)(V_JB) = V_J(BV_JB) = V_JV_JB = V_JB = K_J$. □

5.3.10 Corollary $|K_J| = p^{|J|}|B|$.

Proof:
Suppose that $x_{j_1}(r_1)\cdots x_{j_k}(r_k)B = x_{j_1}(s_1)\cdots x_{j_k}(s_k)B$ then

$$(x_{j_1}(r_1)\cdots x_{j_k}(r_k))^{-1}x_{j_1}(s_1)\cdots x_{j_k}(s_k) = x_{j_1}(s_1 - r_1)\cdots x_{j_k}(s_k - r_k) \in B$$

and $r_i = s_i$ for each i. Hence

$$K_J = V_JB = \bigsqcup_{g \in V_J} gB$$

and $|K_J| = |V_J| \cdot |B| = p^{|J|}|B|$. □

In particular, we see that the subgroups K_J satisfy properties similar to those in Lemma 5.3.6.

5.3.11 Lemma Let $I, J \subset S$, then

1. $K_I \leq K_J$ if and only if $I \subset J$;
2. $K_I \cap K_J = K_{I\cap J}$;
3. $K_IK_J = K_{I\cup J}$.

Proof:
The results follow directly from the corresponding results for V_J. □

Clearly the subgroups K_J are not all the subgroups of G containing B. In particular, consider the following definition from [15]:

5.3.12 Definition Let $(k) = (k_1, \ldots, k_{n-1})$ be such that $0 \leq k_i \leq h$ for each i and define $k_{i,j} = \max\{k_r : j \leq r < i\}$ for $1 \leq j < i \leq n$. Then let

$$H_{(k)} = \{[m_{i,j}] \in G : v(m_{i,j}) = k_{i,j} \text{ for } 1 \leq j < i \leq n\}.$$

The $H_{(k)}$ are also subgroups of G containing B, by [15] Lemma 4.4, but as we see from the following example, K_J is not necessarily of the form $H_{(k)}$ for some (k).

5.3.13 Example Let $n = 3$ and $h = 2$, then the subgroup $P_{\{1,2\}}$ is given by

$$P_{\{1,2\}} = \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ 0 & a_{3,2} & a_{3,3} \end{bmatrix} \in G : v(a_{2,1}), v(a_{3,2}) \geq 1 \right\}$$

whereas the subgroups $H_{(k)}$ are

$$\begin{aligned}
H_{(2,2)} &= B \\
H_{(2,1)} &= \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ 0 & a_{2,2} & a_{2,3} \\ 0 & a_{3,2} & a_{3,3} \end{bmatrix} \in G : v(a_{3,2}) \geq 1 \right\} \\
H_{(1,2)} &= \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ 0 & 0 & a_{3,3} \end{bmatrix} \in G : v(a_{2,1}) \geq 1 \right\} \\
H_{(1,1)} &= \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{2,1} & a_{3,3} \end{bmatrix} \in G : v(a_{2,1}), v(a_{3,1}), v(a_{2,1}) \geq 1 \right\} \\
H_{(2,0)} &= \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ 0 & a_{2,2} & a_{2,3} \\ 0 & a_{3,2} & a_{3,3} \end{bmatrix} \in G \right\} \\
H_{(0,2)} &= \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ 0 & 0 & a_{3,3} \end{bmatrix} \in G \right\} \\
H_{(1,0)} &= \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{2,1} & a_{3,3} \end{bmatrix} \in G : v(a_{2,1}), v(a_{3,1}) \geq 1 \right\} \\
H_{(0,1)} &= \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{2,1} & a_{3,3} \end{bmatrix} \in G : v(a_{3,1}), v(a_{2,1}) \geq 1 \right\} \\
H_{(0,0)} &= G.
\end{aligned}$$

Thus we see that $P_{\{1,2\}}$ is not of the form $H_{(k)}$ for any (k).

5.4 An Analogue of the Steinberg Character

In [11], Hill defines a character St_h, which is an analogue of the Steinberg character for $\mathrm{GL}_n(\mathbb{Z}/p^h\mathbb{Z})$ but is different from the character given by Lees in [15]. In particular, Hill shows that St_h is an irreducible character such that

$$(\mathrm{St}_h, (1_P)^G) = \begin{cases} 1 & \text{if } P = B \\ 0 & \text{if } P \gneq B \end{cases}$$

and, further, that

$$\mathrm{St}_h(1) = p^{(h-1)n(n-1)/2-(n-1)} \prod_{k=2}^{n} (p^k - 1).$$

We will now construct an FG-module which affords this character and use the corresponding self-adjoint idempotent to show that St_h can be expressed as an alternating sum of permutation character over the subgroups K_J defined in the previous section.

5.4.1 Definition Let M be the FG-module in the orthogonal decomposition

$$FG\widehat{B} = M \oplus \sum_{i=1}^{n-1} FG\widehat{K_{\{i\}}}.$$

5.4.2 Lemma The self-adjoint idempotent $e \in FG$ such that $M = FGe$ is

$$e = \sum_{J \subset S} (-1)^{|J|} \widehat{K_J}.$$

Proof:

From Lemma 5.3.11(iv), for each $I, J \subset K$, $K_I K_J = K_{I \cup J} = K_J K_I$. Thus, by Lemma 3.3.4 we have the similar result that $\widehat{K_I}\widehat{K_J} = \widehat{K_{I\cup J}} = \widehat{K_J}\widehat{K_I}$ and hence, we must also have that $(\widehat{B} - \widehat{K_I})(\widehat{B} - \widehat{K_J}) = (\widehat{B} - \widehat{K_J})(\widehat{B} - \widehat{K_I})$. In particular, this shows that for each $1 \leq i, j \leq n$, $(\widehat{B} - \widehat{K_{\{i\}}})(\widehat{B} - \widehat{K_{\{j\}}}) = (\widehat{B} - \widehat{K_{\{j\}}})(\widehat{B} - \widehat{K_{\{i\}}})$ and the result then follows from Lemma 2.4.1 since we know that $M = FGe$ where

$$\begin{aligned} e &= (\widehat{B} - \widehat{K_{\{1\}}}) \wedge \cdots \wedge (\widehat{B} - \widehat{K_{\{n-1\}}}) \\ &= (\widehat{B} - \widehat{K_{\{1\}}}) \cdots (\widehat{B} - \widehat{K_{\{n-1\}}}) \\ &= \sum_{k=0}^{n-1} \sum_{i_1 < \cdots < i_k} (-1)^k \widehat{K_{\{i_1\}}} \cdots \widehat{K_{\{i_k\}}} \\ &= \sum_{k=0}^{n-1} \sum_{i_1 < \cdots < i_k} (-1)^k \widehat{K_{\{i_1,\ldots,i_k\}}} \\ &= \sum_{J \subset S} (-1)^{|J|} \widehat{K_J}. \end{aligned}$$

□

Now, since we can express the self-adjoint idempotent for M as an alternating sum of group sums, we must therefore also be able to express the character afforded by M as a corresponding alternating sum of permutation characters.

5.4.3 Corollary $\chi_M = \sum_{J \subset S} (-1)^{|J|} (1_{K_J})^G$.

Proof:
This follows from Corollary 3.2.6. □

Further, note that the degree of this character is the same as the degree of the character given by Hill.

5.4.4 Lemma $\chi_M(1) = p^{(h-1)n(n-1)/2-(n-1)}(p^n - 1) \cdots (p^2 - 1)$.

Proof:
From Corollary 5.4.3, we see

$$\begin{aligned}
\chi_M(1) &= \sum_{J \subset S} (-1)^{|J|} (1_{K_J})^G(1) \\
&= \sum_{J \subset S} (-1)^{|J|} |G : K_J| \\
&= \sum_{J \subset S} (-1)^{|J|} \frac{|G : B|}{|K_J : B|} \\
&= \frac{|G : B|}{p^{n-1}} \sum_{J \subset S} (-1)^{|J|} p^{(n-1)-|J|} \\
&= \frac{|G : B|}{p^{n-1}} \sum_{k=0}^{n-1} \binom{n-1}{k} (-1)^k p^{(n-1)-k} \\
&= \frac{|G : B|}{p^{n-1}} (p-1)^{n-1}.
\end{aligned}$$

So, using Corollary 5.1.4, we get

$$\begin{aligned}
\chi_M(1) &= \left(p^{(h-1)n(n-1)/2} \prod_{k=1}^{n-1} (p^k + p^{k-1} + \cdots + 1) \right) p^{-(n-1)} (p-1)^{n-1} \\
&= p^{(h-1)n(n-1)/2-(n-1)} \prod_{k=2}^{n} (p^k - 1).
\end{aligned}$$

□

Consequently, we see that the character afforded by M is in fact the character constructed by Hill.

5.4.5 Corollary $\mathrm{St}_h = \chi_M$.

Proof:
We see that

$$\begin{aligned}(\mathrm{St}_h, \chi_M) &= (\mathrm{St}_h, \sum_{J \subset S} (-1)^{|J|} (1_{K_J})^G) \\ &= \sum_{J \subset S} (-1)^{|J|} (\mathrm{St}_h, (1_{K_J})^G) \\ &= (\mathrm{St}_h, (1_B)^G) \\ &= 1.\end{aligned}$$

Thus, by Corollary 3.1.10, since St_h is an irreducible character,

$$\chi_M = \mathrm{St}_h + \zeta$$

for some character ζ of G. Further, $\chi_M(1) = \mathrm{St}_h(1)$ implies that $\zeta(1) = 0$, i.e. we must have that $\chi_M = \mathrm{St}_h$. □

5.4.6 Remark Since St_h is an irreducible character which is afforded by M, M must be an irreducible FG-module. More importantly, we see that we can express the character constructed by Hill as an alternating sum of permutation characters

$$\mathrm{St}_h = \sum_{J \subset S} (-1)^{|J|} (1_{K_J})^G,$$

which is analogous to the formula given by Curtis in [5] for the Steinberg character of a finite group with BN-pair.

Further, since $e \in FK_S$ we must have that M is induced from the irreducible FK_S-module $FK_S e$. In particular, we see that

$$\mathrm{St}_h = \left(\sum_{J \subset S} (-1)^{|J|} (1_{K_J})^{K_S} \right)^G .$$

Note that this is not true for the Steinberg character of a finite group with BN-pair, since by the construction of $u \in FG$, the self-adjoint idempotent such that FGu affords the Steinberg character, $u \notin FH$ for any proper subgroup of G. □

Bibliography

[1] Anderson, F. W. and Fuller, K. R. : Rings and categories of modules, Springer-Verlag, New York, 1992.

[2] Berman, A. and Plemmons, R. J. : Nonnegative matrices in the mathematical sciences, Academic Press, New York, 1979.

[3] Bourbaki, N. : Groupes at algèbres de Lie, IV, V, VI, Hermann, Paris, 1968.

[4] Carter, R. W. : Finite groups of Lie type: conjugacy classes and irreducible characters, Wiley, New York, 1985.

[5] Curtis, C. W. : The Steinberg character of a finite group with a $(B - N)$ pair, J. Algebra **4** (1966), 433-441.

[6] Curtis, C. W. and Fossum, T. V. : On centralizer rings and characters of representations, Math. Zeitschr. **107** (1968), 402-406.

[7] Curtis, C. W., Iwahori, N. and Kilmoyer, R. W. : Hecke algebras and characters of parabolic type of finite groups with BN-pairs, Publ. Math. I.H.E.S. **40** (1971), 81-116.

[8] Curtis, C. W. and Reiner, I. : Methods of representation theory - with applications to finite groups and orders, Vol. II, Wiley, New York, 1987.

[9] Dornhoff, L. : Group representation theory, Part A, Dekker, New York, 1971.

[10] Golan, J. S. : Foundations of linear algebra, Kluwer Academic Publishers, Boston, 1995.

[11] Hill, G. : Regular elements and regular characters of $\mathrm{GL}_n(\mathcal{O})$, J. Algebra **174** (1995), 610-635.

[12] Isaacs, I. M. : Character theory of finite groups, Academic Press, New York, 1976.

[13] Lam, T. Y. : A first course in noncommutative rings, Springer-Verlag, New York, 1991.

[14] Lax, P. D. : Linear algebra, Wiley, New York, 1997.

[15] Lees, P. : A Steinberg representation for $GL_n(\mathbb{Z}/p^h\mathbb{Z})$, Proc. London Math. Soc. **37** (1978), 459-490.

[16] Serre, J. P. : Linear representations of finite groups, Springer-Verlag, New York, 1977.

[17] Seneta, E. : Non-negative matrices and Markov chains, Springer-Verlag, New York, 1981.

[18] Solomon, L. : The orders of the finite Chevalley groups, J. Algebra **3** (1966), 376-393.

[19] Steinberg, R. : A geometric approach to the representations of the full linear group over a Galois field, Trans. Amer. Math. Soc. **71** (1951), 274-282.

[20] Steinberg, R. : Prime power representations of finite linear groups, Can. J. Math. **8** (1956), 580-591.

[21] Steinberg, R. : Prime power representations of finite linear groups II, Can. J. Math. **9** (1957), 347-351.