The Module Theory of the 0-Hecke Algebra of the Symmetric Group

Redacted

Abstract

We study the module theory of the 0-Hecke algebra as Fayers [3] did. We specialise to the 0-Hecke algebra of the symmetric group, classifying its simple modules and studying its projective and injective modules.

Acknowledgements

I am grateful to my supervisor, Alex Fink, for his guidance, expertise and patience, through which I have been able to understand this project. I would not have been able to complete this project without him. I am also grateful to Matthew Fayers for suggesting this project and, more importantly, for inspiring me to see the beauty in abstract algebra.

1 Introduction

Let W be a Coxeter group. The *0-Hecke* algebra $\mathcal{H}_0(W)$ of W over the field $\mathbb{F}$ can be thought of as a 'deformation' of the group algebra $\mathbb{F}(W)$ in the following sense. The generators $\{h_i\}$ of $\mathcal{H}_0(W)$ are in bijection with the generators of W, satisfying the braid relations. But rather than the generators being involutions, they instead satisfy the quadratic relation $h_i^2 = -h_i$.

Norton [8] studied the 0-Hecke algebra $\mathcal{H}_0(W)$, studying its nilpotent radical, classifying its irreducible representations and decomposing it into its irreducible left ideals. Fayers [3] built on this work, presenting dualities and a correspondence between the projective and injective modules. In this work, we will present the results from [3], simplifying to the case where W is a symmetric group.

Any reader of this paper is assumed to have a good background in group and ring theory. Hungerford [5] covers much more than we will need in Chapters 1, 2 and 3. We will assume any group and ring theory results from Hungerford [5] without comment.

Since the reader is not assumed to be familiar with module theory, we start by briefly introducing modules, following [5, Section 4]. When then briefly introduce Coxeter groups, using $\mathcal{S}_n$ as a case study. We study useful properties of $\mathcal{S}_n$, following [7, Section 1]. All results stated are from [7], except for the few general results from [4, Section 5].

The final section studies the module theory of $\mathcal{H}_0(W)$ for the special case where W is a symmetric group, classifying the simple and studying projective and injective modules.

Throughout this paper, we will write fg for the composition of two functions f and g, omitting the $\circ$ symbol.

2 Module Theory

2.1 Modules and Module Homomorphisms

Definition 2.1.1. Let R be a ring with unity. A *left R-module* is an abelian group $(M, +)$ with a function $R \times M \to M$, $(r, m) \mapsto rm$ such that for all $r, s \in R$ and $m, n \in M$ the following hold.

M1) $r(m + n) = rm + rn$.
M2) $(r + s)m = rm + sm$.
M3) $r(sm) = (rs)m$.
M4) $1_R m = m$.

If R is a division ring and M is a left R-module, then M is a *left vector space*.

From now on, unless stated otherwise, R denotes a general ring with unity.

A right R-module (vector space resp.) M is defined in a similar way to left R-modules but with a function $M \times R \to M$, $(m, r) \mapsto mr$ satisfying i)−iv) for right multiplication. We will only consider left R-modules, and call them R-modules.

One notices that modules are 'vector spaces over rings', as opposed to the familiar notion of a vector space over a field. So in particular, every vector space over a field is a module of that field.

Since R is a group, we see that iii) and iv) define an action of R on M. So we will sometimes refer to the function as an R-action. Note that we specified + as the operation for M. However, we could just as easily have taken M to have any operation $\circ$.

Example 2.1.1. R is always a module over itself, with the module action being regular left multiplication. This is known as the *regular representation*. The trivial group $\{0\}$ is always an R-module with the module action given by $r0 = 0$ for all $r \in R$.

The following familiar properties from ring theory carry through to modules. If M is an R-module, and 0_M and 0_R are the additive identities of M and R respectively then

$$r0_M = 0_M, \qquad 0_r m = 0_M, \qquad (-r)m = -(rm) = r(-m).$$

for all $r \in R$ and $m \in M$.

From now on, we will denote 0_M, 0_R and the trivial module $\{0\}$ all by 0.

Example 2.1.2. Any abelian group G can be made into a $\mathbb{Z}$-module M by defining a function $R \times M \to M$ by

$$(m, n) \mapsto \begin{cases} \underbrace{m + \ldots + m}_{n \text{ times}} & \text{if } n > 0, \\ -(\underbrace{m + \ldots + m}_{n \text{ times}}) & \text{if } n < 0, \\ 0 & \text{otherwise.} \end{cases}$$

The reader may wish to verify that this really does define a $\mathbb{Z}$-module.

Example 2.1.3. Let R be a ring and I an ideal of R. Then I is an R-module with R-action being regular multiplication. Also, R/I is an abelian group so can be made into an R-module under the R-action $r(s+I) = (rs) + I$.

Since I is closed under multiplication in R, it is easy to see that is an R-module. Moreover, since the R-action of R/I is essentially just multiplication in R, it is also easy to see that R/I is an R-module, so we won't formally prove it.

The above example gives a flavour of the importance of module theory, as both ideals and quotient rings are modules. Thus, module theory combines results about both ideals and quotient rings.

Example 2.1.4. Recall that $R[x]$ is the polynomial ring of R. Let $M = C^0([a,b])$ be the set of continuous functions on $[a,b]$. This is an additive group. So we can make M into an $R[x]$-module as follows. Let $p = \sum_{i=0}^k a_i x^i \in R[x]$ and $f \in M$. Then define the $R[x]$-action by $p \cdot f = a_0 f$.

Note this is actually just scalar multiplication in disguise, and since M is a vector space (so is compatible with scalar multiplication), it follows that M is an $R[x]$-module.

Definition 2.1.2. Let M be an R-module and $N \subseteq M$. N is a *submodule* of M (denoted $N \leqslant M$) if N is an additive subgroup of M and $rn \in N$ for all $r \in R$ and $n \in N$. If R is a division ring, then any submodule of a vector space M is a *subspace*.

Example 2.1.5. If M is an R-module, then given any $m \in M$, the set $Rm = \{rm \mid r \in R\}$ is a submodule of M. We will give a proof of this in the next subsection.

Example 2.1.6. Let I be an ideal of R. Recall that both R and I are R-modules. Thus, $I \leqslant R$, by definition. So, in some sense, submodules generalise the notion of an ideal.

If R is clear from the context, then we will simply say N is a submodule of M.

Definition 2.1.3. Let M and N be R-modules. A function $\phi : M \to N$ is an R-module *homomorphism* if

i) $\phi(m+n) = \phi(m) + \phi(n)$ (ϕ is a group homomorphism),

ii) $\phi(rm) = r\phi(m)$ (ϕ is *R-linear*),

for all $r \in R$ and $m, n \in N$.

If ϕ is

i) injective, then ϕ is a *monomorphism*.

ii) surjective, then ϕ is a an *epimorphism*.

iii) bijective, then ϕ is an *isomorphism*.

From now on, we will simply call them homs. We will sometimes use *embedding* to mean monomorphism and *projection* to mean epimorphism. We denote by $\mathrm{Hom}_R(M,N)$ the set of all homs from M to N.

Definition 2.1.4. Let M be an R-module. The *dual module* of M is the R-module $M^* := \mathrm{Hom}_R(M,R)$.

We usually just say that M^* is the *dual* of M.

If M is a left R-module, then M^* is naturally a right R-module. We can define the R-action by $fr : m \to (f(m))r$ for all $f \in M^*$ and $m \in M$. Since f is a hom and $f(m)$ is in R, it follows that M^* satisfies the module axioms under this action.

Similarly, if M is right R-module, then the dual of M is $M^* := \mathrm{Hom}_R(M, R)$, which is a *left* R-module. (See Hungerford [5, Chapter 5, Section 4] for a full proof.)

Definition 2.1.5. Let $\phi : M \to N$ be a module hom. The *kernel* of ϕ is $\ker(\phi) = \{m \in M \mid \phi(m) = 0\}$ and the *image* of ϕ is $\mathrm{Im}(\phi) = \{\phi(m) \mid m \in M\}$.

The Isomorphism Theorems for groups can be extended to modules in a natural way. See [5, pp. 172–173] for the precise statement of each theorem. Similarly, a module hom ϕ is an embedding if and only if $\ker(\phi) = 0$.

Theorem 2.1.1. (Hungerford [5, Theorem 1.6].) *Let M be an R-module and $N \leqslant M$. Then M/N is an R-module with the R-action given by $r(m + N) = rm + N$.*

Proof. Firstly, since M is abelian, N is a normal subgroup of M, so M/N is well-defined. Now, suppose $m, m' \in M$ such that $m + N = m' + N$. Then, by the Coset Lemma, $m - m' \in N$, and since $N \leqslant M$, $r(m - m') \in N$, too. Therefore, $rm + N = rm' + N$ again by the Coset Lemma. Thus, the R-action is well-defined, and it follows that it satisfies the module axioms. □

Definition 2.1.6. Let $M_1, \ldots, M_k$ be R-modules. The *direct sum* of $M_1, \ldots, M_k$ is the R-module

$$M_1 \oplus \ldots \oplus M_k | = M_1 \times \ldots \times M_k$$

with addition given by

$$(m_1, \ldots, m_k) + (m'_1, \ldots, m'_k) = (m_1 + m'_1, \ldots, m_k + m'_k),$$

and R-action given by

$$r(m_1, \ldots, m_k) = (rm_1, \ldots, rm_k).$$

It is not too difficult to show that $M_1 \oplus \cdots \oplus M_k$ really is an R-module. This is left as an exercise to the reader.

Definition 2.1.7. Let $M = M_1 \oplus \cdots \oplus M_k$. The *canonical projection* is the map $\pi_i : \bigoplus M_j \to M_i$ and the *canonical injection* is the map $\iota_i : M_i \to \bigoplus M_j$.

The reader is left to check the π_i and ι_i are mutually inverse homs.

Definition 2.1.8. Let $\{M_1, \ldots, M_k\}$ be a family of submodules of an R-module M. Then M is the *direct sum* of $M_1, \ldots, M_k$ if

i) $M = M_1 \oplus \cdots \oplus M_k := \{m_1 + \cdots + m_k \mid m_i \in M_i\}$;

ii) $M_i \cap M_j = 0$ for all $i \neq j$.

When considering submodules and sums of modules, we will restrict to the finite case, although this is done without loss of generality (for the purposes of this paper).

Definition 2.1.9. Let $\mathbb{F}$ be a field. An $\mathbb{F}$-*algebra* is a ring R satisfying the following.

i) $(R, +)$ is a unitary $\mathbb{F}$-module.

ii) $\lambda(rs) = (\lambda r)s = r(\lambda s)$ for all $\lambda \in \mathbb{F}$ and $r, s \in R$.

2.2 Free Modules

Definition 2.2.1. Let N be a subset of an R-module M. The *span* of N, $\operatorname{span}(N)$, is the intersection of all submodules of M which contain N. If S is such an intersection then we say that N *spans* S or N is a *spanning set* for S.

The span of N is also called the *submodule generated by* N. If N is a singleton, then the submodule generated by N is *cyclic*. More generally, M is *finitely generated* if it is generated by a finite subset N.

Proposition 2.2.1. *Let M be an R-module. If $N = \{m_1, \dots, m_k\} \subseteq M$, then the span of N is the set of all linear combinations of $m_1, \dots, m_k$ in R. That is,*

$$\operatorname{span}(N) = RN := \{r_1 m_1 + \cdots + r_k m_k \mid r_i \in R\}.$$

Proof. Let us first show that $\operatorname{span}(N)$ is itself a submodule of M. Write $\operatorname{span}(N) = M_1 \cap \cdots \cap M_k$, and let i range between 1 and k, so that $N \subseteq M_i \leqslant M$. We start by showing that $\operatorname{span}(N)$ is a subgroup, using the Subgroup Test.
S1. If $m, n \in \operatorname{span}(N)$, then $m, n \in M_i$, so $m + n \in M_i$, so $m + n \in \operatorname{span}(N)$.
S2. $0 \in M_i$ for each i, so $0 \in \operatorname{span}(N)$.
S3. If $m \in \operatorname{span}(N)$, then $m \in M_i$, so $-m \in M_i$, so $-m \in \operatorname{span}(N)$.
Also, given $r \in R$ and $m \in \operatorname{span}(N)$, $rm \in M_i$, so $rm \in \operatorname{span}(N)$, thus $\operatorname{span}(N)$ is closed under the R-action, whence $\operatorname{span}(N) \leqslant M$.

We now show that RN is also a submodule of M. Again, we first show that RN is a subgroup.
S1. If $m = \sum_{i=1}^k r_i m_i$ and $n = \sum_{i=1}^k r_i' m_i$ in RN, then

$$m + n = \sum_{i=1}^k r_i m_i + \sum_{i=1}^k r_i' m_i = \sum_{i=1}^k \left(r_i + r_i'\right) m_i \in RN.$$

S2. $0 = 0m_1 + \ldots + 0m_k \in RN$.
S3. For all $m \in RN$ as above, we claim $-m = \sum_{i=1}^k (-r_i) m_i$. Indeed,

$$m + (-m) = \sum_{i=1}^k r_i m_i + \sum_{i=1}^k (-r_i) m_i = \sum_{i=1}^k (r_i - r_i) m_i = \sum_{i=1}^k 0 m_i = 0,$$

and $-m \in RN$ since $-r \in R$. Similarly, $(-m) + m = 0$.

Moreover, $RN = r \sum_{i=1}^k r_i m_i = \sum_{i=1}^k (r r_i) m_i \in RN$ (as $r r_i \in R$), so RN is also closed under the R-action, so $RN \leqslant M$.

Now, $N \in \operatorname{span}(N)$, by definition of $\operatorname{span}(N)$. In particular, each $m_i \in \operatorname{span}(N)$ so $r m_i \in \operatorname{span}(N)$ (as $\operatorname{span}(N)$ is closed under the R-action), and $r_1 m_1 + \ldots + r_k m_k \in \operatorname{span}(N)$ (as $\operatorname{span}(N)$ is an additive group). Thus, $RN \subseteq \operatorname{span}(N)$. Furthermore, each $m_i \in RN$ (To see this, let $r_i = 1$ and $r_j = 0$ for all $j \neq i$.), so RN contains N. Thus, we also have $\operatorname{span}(N) \subseteq RN$. □

In the proof, we took N to be finite, but we could just as well have taken N to be infinite.

Letting $N = \{m\}$ for some m in M, we see that the cyclic submodule generated by N is Rm, as in Example 2.1.2, and that this really is a submodule of M.

Definition 2.2.2. Let M be an R-module, $N = \{m_1, \ldots, m_k\} \subseteq M$ and $m \in M$ be nonzero.

i) N is *linearly independent* if

$$\sum_{i=1}^{k} r_i m_i = 0$$

implies $r_i = 0$ for all i. Otherwise, N is *linearly dependent*.

ii) m is *torsion-free* if $rm = 0$ implies $r = 0$ for all $r \in R$. That is, $\{m\}$ is linearly independent as a subset of M.

Definition 2.2.3. Let M be an R-module. A *basis* for M is a subset of M which is linearly independent and spans M. An R-module M is *free* if it has at least one basis.

Theorem 2.2.2. (Hungerford [5, Theorem 2.4].) *Every vector space M over a division ring has a basis and thus is free. In particular, M has a basis $\mathcal{B}$ such that*

$$A \subseteq \mathcal{B} \subseteq C,$$

where A is linearly independent and C spans M.

Proof. The proof is beyond the scope of this work so we skip it. □

Note that, in general, it's not true that every spanning set contains a basis.

To see this, suppose that M is cyclic with m as its generator, ie., $\{m\}$ generates M. If m is not torsion-free, then $\{m\}$ is not linearly independent, and so is not a basis for M.

Another example is $\mathbb{Z}$ as a module over itself. Consider the subset $\{2, 3\}$. Then this subset generates $\mathbb{Z}$ (See *Numbers, Sets and Functions*, Exercise Sheet 1.) but is not linearly independent, since $-6 \cdot 2 + 4 \cdot 3 = 0$. Moreover, no subset of $\{2, 3\}$ spans $\mathbb{Z}$.

Lemma 2.2.3. (Hungerford [5, Lemma 2.3]) *Let M be a free R-module. Any basis of M is maximally linearly independent.*

Proof. Let $\mathcal{B} = \{m_1, \ldots, m_k\}$ be a basis for M. By maximally linearly independent, we mean that for any $m \in M$ with $m \notin \mathcal{B}$, the set $\{m_1, \ldots, m_k, m\}$ is linearly dependent. Indeed, given $m \in M$ not in $\mathcal{B}$, write $m = r_{m_1} m_1 + \cdots + r_{m_k} m_k$ with $r_{m_i} \in R$ for $i = 1, \ldots, k$. Then

$$\sum_{i=1}^{k} (-r_{m_i}) m_i + 1m = \sum_{i=1}^{k} (-r_{m_i}) m_i + \sum_{i=1}^{k} r_{m_i} m_i = \sum_{i=1}^{k} (-r_{m_i} + r_{m_i}) m_i = 0,$$

so $\{m_1, \ldots, m_k, m\}$ is linearly dependent since $r_{k+1} = 1 \neq 0$. □

Theorem 2.2.4. (Hungerford [5, Theorem 2.7].) *Let M be a free vector space over a division ring with basis $\mathcal{B}$. Then every other basis of M has cardinality $|\mathcal{B}|$. If $\mathcal{B}$ is infinite, then every other basis is also infinite.*

Proof. The proof of the theorem is standard so we skip it. It is easy to prove using the preceding lemma. □

In view of this theorem, we make the following definition.

Definition 2.2.4. Let M be a free vector space over a division ring R. The *dimension* $\dim_R(M)$ of M over R is the cardinality of any basis of M.

2.3 Sequences of Module Homomorphisms

Definition 2.3.1. A sequence of module homs $K \xrightarrow{\phi} L \xrightarrow{\psi} M$ is *exact* if $\mathrm{Im}(\phi) = \ker(\psi)$.

In the sequel, we will simply say 'exact sequence of modules' to mean 'exact sequence of module homs'.

Example 2.3.1. Let M and N be R-modules. Then the sequence

$$0 \to M \xrightarrow{\phi} N$$

is exact if and only if ϕ is an embedding. This is because the unique map $0 \to M$ has image 0, so we require $\ker(\phi) = 0$. That is, ϕ must be injective. Similarly,

$$M \xrightarrow{\phi} N \to 0$$

is exact if and only if ϕ is a projection. Reversing the above argument, the kernel of the unique map $N \to 0$ is all of N, so we require $\mathrm{Im}(\phi) = N$; that is, ϕ must be projective.

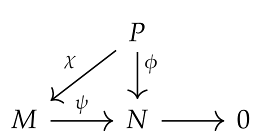
2.4 Projective and Injective Modules

Definition 2.4.1. An R-module P is *projective* if, given any exact sequence

$$M \xrightarrow{\psi} N \to 0$$

and hom $\phi : P \to N$, there exists a hom $\chi : P \to M$ such that $\phi = \psi\chi$.

This can be drawn in a commutative diagram, that is, the arrows commute, as follows.



Recall from Example 2.3.1 that ψ is a projection. So P is projective if, given any hom $\phi : P \to N$ and projection $\psi : M \to N$, there exists a hom $\chi : P \to M$ such that $\phi = \psi\chi$.

Theorem 2.4.1. (Hungerford [5, Theorem 3.2].) *Every free module is projective.*

Proof. Let P be a free module with basis $\mathcal{B} = \{p_1, \ldots, p_n\}$. Suppose we are given the following diagram

$$\begin{array}{ccccc} & & P & & \\ & & \big\downarrow{\scriptstyle \phi} & & \\ M & \xrightarrow{\ \psi\ } & N & \longrightarrow & 0 \end{array}$$

where ψ is an epimorphism. For each $p_i \in \mathcal{B}$, $\phi(p_i) \in N$. Since ψ is an epimorphism, there exist $m_i \in M$ for each $p_i \in \mathcal{B}$ such that $\psi(m_i) = \phi(p_i)$.

Since P is free, the map $\bar{\chi} : \mathcal{B} \to M$ given by $\bar{\chi}(p_i) = m_i$ can be extended to a hom as follows. Write $p \in P$ as $p = \sum_{i=1}^{k} r_i p_i$ and define $\chi(p) = \sum_{i=1}^{k} r_i \bar{\chi}(p_i)$. The map is well-defined since, if $p = \sum_{i=1}^{n} s_i p_i$ also, then $\sum_{i=1}^{n} r_i p_i - \sum_{i=1}^{n} s_i p_i = \sum_{i=1}^{n} (r_i - s_i) p_i = 0$. The reader is left to check that χ is really a hom.

Consequently, $\psi(\chi(p_i)) = \phi(p_i)$ for all i, so $\psi\chi = \phi : P \to N$, whence P is projective. □

Example 2.4.1. By Theorems 2.2.2 and 2.4.1, every vector space over a division ring is projective.

Theorem 2.4.2. (Hungerford [5, Proposition 3.8].) *Let P be a projective R-module. If $P = P_1 \oplus \cdots \oplus P_k$, then each P_i is projective for all $1 \leqslant i \leqslant k$.*

Proof. Let $P = P_1 \oplus \cdots \oplus P_k$ be projective. Let π_i and ι_i be the canonical projections and injections respectively. Suppose we are given the following diagram

$$\begin{array}{ccccc} & & P & & \\ & & {\scriptstyle \iota_i}\big\uparrow\big\downarrow{\scriptstyle \pi_i} & & \\ & & P_i & & \\ & & \big\downarrow{\scriptstyle \phi} & & \\ M & \xrightarrow{\ \psi\ } & N & \longrightarrow & 0 \end{array}$$

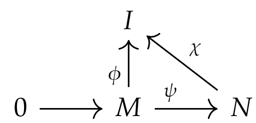
with ψ epimorphic. Since P is projective, there is a hom $\bar{\chi} : P \to M$ such $\psi\bar{\chi} = \phi \circ \pi_i$. Let $\chi = \psi\iota_i$ so that $\psi\chi = \psi\bar{\chi} \circ \iota_i = \phi \circ \pi_i \circ \iota_i = \phi$. Therefore, P_i is projective for all i. □

Definition 2.4.2. An R-module I is *injective* if, given any exact sequence

$$0 \to M \xrightarrow{\psi} N$$

and hom $\phi : M \to I$, there exists a hom $\chi : N \to I$ such that $\phi = \chi \circ \psi$.

This can also be drawn in a commutative diagram, as follows.



One notices that in the commutative diagrams for projective and injective modules, the arrows are reversed (with M and N switched for ease of notation). Moreover, ψ is, in this case, an embedding, again by Example 2.4.1. This is known as *dualisation*. This means, in particular, that projective and injective modules are dual. That is, P is projective if and only if P^* is injective and P is injective if and only if P^* is projective.

This generalises to injectivity and surjectivity; there exists a surjection from a set A to a set B if and only if there exists an injection from B to A, and vice versa.

Proposition 2.4.3. (Hungerford [5, Proposition 3.7]) *Let I be an injective R-module. If $I = I_1 \oplus \cdots \oplus I_k$, then each I_i is injective for all $1 \leqslant i \leqslant k$.*

Proof. The result follows from carefully dualising the proof of Theorem 2.4.2. □

Example 2.4.2. Consider $\mathbb{R}^2$ as an $\mathbb{R}$-module with the standard basis $\{e_1, e_2\}$. Write $\langle e_1 \rangle$ for the span of e_1. Then $\langle e_1 \rangle$ is an injective $\mathbb{R}$-module since $\langle e_1 \rangle \oplus \langle e_2 \rangle = \mathbb{R}^2$ and $\langle e_1 \rangle \cap \langle e_2 \rangle = 0$.

Definition 2.4.3. A ring is *self-injective* if it is injective as a module over itself.

2.5 Projective Covers and Injective Hulls

Definition 2.5.1. Let M be an R-module. N is a *superfluous submodule* of M if, given any submodule L of M,

$$L + N = M \Rightarrow L = M.$$

Example 2.5.1. The trivial module 0 is a superfluous submodule of any R-module.

Definition 2.5.2. Let M and N be an R-modules. A *superfluous epimorphism* of M is a surjection $\phi : M \to N$ such that $\ker(\phi)$ is a superfluous submodule of M.

Example 2.5.2. Any module isomorphism $\phi : M \to N$ is a superfluous epimorphism since ϕ is necessarily an epimorphism and $\ker(\phi) = 0$, as ϕ is injective, so $\ker(\phi)$ is a superfluous submodule of N.

Definition 2.5.3. A *projective cover* of an R-module M is a pair (P, ϕ), where P is projective and $\phi : P \to M$ is a superfluous epimorphism of P.

By Benson [1, page 9] the projective cover is unique up to isomorphism. We will write $P(M)$ to denote the projective cover of M in the future.

We require ϕ to be superfluous so that P is the 'smallest' projective module which covers M, in the sense that no proper submodule Q of P would cover M. This is because superfluity of ϕ means, informally, that ϕ is only surjective on P, and isn't surjective when restricted to any submodule of P.

Example 2.5.3. Suppose M is free and $M \cong N$ as modules under ϕ. Then N is projective by Theorem 2.4.1 and ϕ is a superfluous isomorphism as in Example 2.5.2, so (N, ϕ) is a projective cover of M.

Definition 2.5.4. Let M be an R-module. N is an *essential submodule* of M if, given any submodule L of M,

$$L \cap N = 0 \Rightarrow L = 0.$$

We also say M is an *essential extension* of N.

The idea of superfluous and essential submodules is that superfluous submodules are 'small' submodules of M whilst essential submodules are 'big' submodules of M.

Example 2.5.4. Any R-module M is an essential submodule of itself.

Definition 2.5.5. Let M be an R-module. $I = I(M)$ is the *injective hull* of M if M is an essential submodule of I and I is injective.

Every module has an injective hull, since every module may be embedded into an injective module. However, a projective cover may not always exist for a module.

2.6 Simple Modules

Definition 2.6.1. Let M be an R-module. Then M is *simple* if its only submodules are 0 and M.

Definition 2.6.2. Let M be an R-module. A *composition series* of M is a series of submodules

$$M = M_0 > \ldots > M_k = 0$$

such that M_i/M_{i+1} is simple for all i.

Similar to the Isomorphism Theorems, the Jordan-Hölder Theorem also holds for composition series of modules. Therefore, any two composition series of M have the same length and same factors, up to isomorphism and reordering.

Proposition 2.6.1. *Let M and M' be R-modules and $N \leqslant M$. If M and M' have composition series, then so do M/N and $M \oplus M'$.*

Proof. We use an argument from Rotman [9] and [12].

Let

$$M = M_0 > \ldots > M_k = 0$$

and

$$M' = M'_0 > \ldots > M'_l = 0$$

be composition series for M and M' respectively. Then we can explicitly construct the following composition series for $M \oplus M'$:

$$M \oplus M' > M_1 \oplus M' > \ldots > M_k \oplus M' > M_k \oplus M'_1 > \ldots M_k \oplus M'_l > 0 \oplus 0.$$

Note that under the canonical projection π, $M' \cong 0 \oplus M' = \ker(\pi)$, so $M_i \cong (M_i \oplus M')/M'$. Thus, there exist quotient maps $M_i \oplus M' \to M_i \to M_i/M_{i+1}$ which are all epimorphisms. One can check that M_{i+1} is in the kernel of the composition, whence $(M_i \oplus M')/(M_{i+1} \oplus M') \cong M_i/M_{i+1}$ for each i. Therefore, it follows that each $(M_i \oplus M')/(M_{i+1} \oplus M')$ is simple.

Now, let $\overline{M}_0 = M/N$ and for $i = 1, \ldots, k$, let $\overline{M}_i = \{m + N \mid m \in M_i\}$. Then

$$M/N = \overline{M}_0 \geqslant \ldots \geqslant \overline{M}_k = 0$$

is a series of M/N (since each $\overline{M}_i$ is abelian). The quotient maps $M_i \to \overline{M}_i \to \overline{M}_i/\overline{M}_{i+1}$ are epimorphisms, and since M_{i+1} is in the kernel of the composition, $M_i/M_{i+1} \cong \overline{M}_i/\overline{M}_{i+1}$. Thus, each $\overline{M}_i/\overline{M}_{i+1}$ is simple. □

Definition 2.6.3. Let M be an R-module and $\{N_1, \ldots, N_k\}$ be a complete collection of its simple submodules. The *socle* of M is the R-module

$$\operatorname{soc}(M) = N_1 \oplus \cdots \oplus N_k.$$

Lemma 2.6.2. *Every simple module is the socle of its injective hull.*

Proof. We use an argument from [11].

Let M be a simple module and $I = I(M)$. Then, in particular, M is an essential submodule of I. So given any non-trivial $J \leqslant I$, we have $M \cap J \neq 0$. But we showed in Proposition 2.2.1 that the intersection of submodules is itself a submodule. We also have $M \cap J \leqslant M \leqslant I$. Thus, since M is simple, this implies $M \cap J = M$; that is, M is contained in J. This means, in particular, that M is the only simple submodule of I. Therefore, $\operatorname{soc}(I) = M$. □

Theorem 2.6.3. *Let M be a nontrivial R-module. Then M is simple if and only if M is a cyclic module with any nonzero element as its generator.*

Proof. First suppose M is simple. Let $m \in M$ be nonzero and consider Rm. Then Rm is a cyclic submodule of M, by Proposition 2.2.1. Since M is simple, we must have $Rm = 0$ or $Rm = M$. Since $m \neq 0$, $Rm \neq 0$ (as $m = 1m \in Rm$), so $Rm = M$.

Now assume M is a cyclic module with any nonzero element as its generator. Let N be a nonzero submodule of M and let $m \in N$ be nonzero. Then, since N is a submodule of M, it follows that $rm \in N$ for all $r \in R$ and $m \in N$. Therefore,

$$Rm \subseteq N \subseteq M.$$

But, by assumption, m generates M. Thus, $Rm = M$ so $N = M$. □

3 Special Properties of $\mathcal{S}_n$

In this section, we will introduce some important properties of $\mathcal{S}_n$ which will be useful when studying the 0-Hecke Algebra. First, let us reintroduce $\mathcal{S}_n$.

3.1 $\mathcal{S}_n$ as a Coxeter Group

Definition 3.1.1. The *symmetric group* of order n is the group $\mathcal{S}_n$ generated by the set $S = \{s_1, \ldots, s_{n-1}\}$ such that $(s_i s_j)^{m_{ij}} = e$ for all $s_i, s_j \in S$, where $m_{ii} = 1$ and $m_{ij} = m_{ji}$ for all $j \neq i$.

Let's see how this coincides with the familiar definition of $\mathcal{S}_n$.

The symmetric group $\mathcal{S}_n$ is generated by $n-1$ transpositions $s_1, \ldots, s_{n-1}$, where $s_i = (i \;\; i+1)$, each with order 2 (so they are *involutions*). This is because any transposition $(i \;\; j)$ can be written as

$$(i \;\; j) = s_i s_{i+1} \ldots s_{j-1} \ldots s_{i+1} s_i,$$

and any element can be written as a product of transpositions.

Furthermore, if $1 \leqslant i \neq j \leqslant n-1$, then each product $s_i s_j$ of the transpositions s_i and s_j has order 3 if $s_i s_j$ is a 3-cycle, and order 2 otherwise. Moreover, $s_j s_i$ is a 3-cycle only if $s_i s_j$ is a 3-cycle, and if not, then $s_i s_j = s_j s_i$.

Any group which satisfies Definition 2.1.1 is called a *Coxeter group*. Some familiar examples are the Klein four-group and the dihedral group of order n. We are only interested in $\mathcal{S}_n$ as a Coxeter group. Throughout this chapter, we will introduce properties of $\mathcal{S}_n$ which are general properties of all Coxeter groups.

See Humphreys [4, Section 5] for a general discussion on Coxeter Groups.

3.2 The Length Function

From now on, $W = \mathcal{S}_{n+1}$ and $S = \{s_1, \ldots, s_n \mid s_i = (i \;\; i+1)\}$. (This simply means that W is generated by n elements rather than $n-1$.)

Recall that the subgroup generated by S is the set $\langle s_1, \ldots, s_n \rangle$ of all products of elements from

$$\left\{ s_1^{\pm 1}, \ldots, s_n^{\pm 1} \right\}.$$

Since the s_i's generate W, $\langle s_1, \ldots, s_n \rangle = W$ and since $s_i^{-1} = s_i$, each element $w \in W$ can be written as a product $w = s_{r_1} \cdots s_{r_k}$ of possibly non-distinct elements in S. We are interested in the case where i is minimal.

Definition 3.2.1. Let $w \in W$ and write $w = s_{r_1} \cdots s_{r_k}$ with k minimal.

i) The *length* of w is k.

ii) The expression $s_{r_1} \cdots s_{r_k}$ is a *reduced expression* for w.

iii) The *length function* of W is the function $\ell : W \to \mathbb{N}$ which maps $w \mapsto k$ if $s_{r_1} \cdots s_{r_k}$ is a reduced expression for w.

Example 3.2.1. In W, the identity element e has length 0 as it is the product of no generators, and any $s_i \in S$ has length 1.

Example 3.2.2. Consider $\mathcal{S}_6$ with the usual generating set. Let $w = (1\ 5)(2\ 3\ 4) \in \mathcal{S}_6$. Then a reduced expression for w is

$$w = (1\ 2)(2\ 3)(3\ 4)(4\ 5)(4\ 3)(3\ 2)(2\ 1)(2\ 3)(3st4),$$

so $\ell(w) = 9$.

Lemma 3.2.1. (Humphreys, [4, p. 108].) *Let ℓ be the length function on W. Let w and w' be any elements in W and let s_i be any generator in S. Then*
i) $\ell\left(w^{-1}\right) = \ell(w)$.
ii) $\ell(w) = 1 \Leftrightarrow w = s_i$.
iii) $\ell(ww') \leqslant \ell(w) + \ell(w')$.
iv) $\ell(ww') \geqslant \ell(w) - \ell(w')$.
v) $\ell(w) - 1 \leqslant \ell(s_i w) \leqslant \ell(w) + 1$.

Proof. Let $w, w' \in W$ and $s_i \in S$.
i) Suppose a reduced expression for w is $w = s_{r_1} \cdots s_{r_k}$. Then, $w^{-1} = s_{r_k} \cdots s_{r_1}$ and $\ell\left(w^{-1}\right) \leqslant \ell(w)$. Now, suppose a reduced expression for w^{-1} is $s_{r_l} \cdots s_{r_1}$, so $w = s_{r_1} \cdots s_{r_l}$. Then $\ell(w) \leqslant \ell\left(w^{-1}\right)$.
ii) Trivial.
iii) Let $w = s_{r_1} \cdots s_{r_k}$ and $w' = s'_{r_1} \cdots s'_{r_l}$ be reduced expressions for w and w' respectively. Then $\ell(w) = k$ and $\ell(w') = l$. Also, $s_{r_1} \cdots s_{r_k} s'_{r_1} \cdots s'_{r_l}$ is an expression for ww' with $k + l$ factors. Thus,

$$\ell(ww') \leqslant k + l = \ell(w) + \ell(w').$$

iv) We have

$$\ell(w) = \ell(ww'(w')^{-1}) \leqslant \ell(ww') + \ell(w'),$$

so

$$\ell(w) - \ell(w') \leqslant \ell(ww').$$

v) Simply combine iii) and iv) to conclude

$$\ell(w) - 1 = \ell(w) - \ell(s_i) \leqslant \ell(s_i w) \leqslant \ell(w) + \ell(s_i) = \ell(w) + 1.$$ □

Corollary 3.2.2. (Humphreys [4, p. 108].) *The 'sign' homomorphism $\phi_{\text{sign}} \mid W \to \{1, -1\}$, which sends even permutations to 1 and odd permutations to -1, is given by $\phi(w) = (-1)^{\ell(w)}$ for all $w \in W$. Thus, $\ell(s_i w) = \ell(w) \pm 1$ for any $s_i \in S$.*

Proof. Each generator s_i is odd, and $\ell(s_i) = 1$. Thus,

$$\phi_{\text{sign}}(s_i) = -1 = (-1)^1 = (-1)^{\ell(s_i)}.$$

Now, given any $w \in W$, let $s_{r_1} \cdots s_{r_k}$ be a reduced expression for w (so $\ell(w) = k$). Then

$$\phi_{\text{sign}}(w) = \phi_{\text{sign}}(s_{r_1}) \cdots \phi_{\text{sign}}(s_{r_k}) = (-1)^k = (-1)^{\ell(w)}.$$

Moreover, $\phi_{\text{sign}}(s_i w) = \phi_{\text{sign}}(s_i)\phi_{\text{sign}}(w) = -\phi_{\text{sign}}(w)$ implies $\ell(s_i w) \neq \ell(w)$, so it follows from Lemma 2.2.1 v) that $\ell(s_i w) = \ell(w) \pm 1$. The same clearly holds for $\ell(w s_i)$. □

Proposition 3.2.3. (Fayers [3, Lemma 2.3].) *There exists a unique $w_0 \in W$ such that $\ell(w_0) \geqslant \ell(w)$ for all $w \in W$. Moreover,*

$$\ell(w_0 w) = \ell(w_0) - \ell(w) = \ell(w w_0).$$

In particular, w_0 is an involution.

We claim that $w_0 = (1\ n)(2\ (n-1))...(\lfloor n/2 \rfloor\ \lceil n/2 \rceil + 1)$. Note w_0 is a product of $\lfloor n/2 \rfloor$ disjoint transpositions and can be written with $\frac{n(n-1)}{2}$ generating transpositions. In order to show that w_0 is the longest element in W, we require some results which are proven in the next section, so we will delay the proof until then. However, note that w_0 is an involution, by construction.

Lemma 3.2.4. (Fayers [3, Proposition 2.4].) *The conjugation action of w_0 on $\mathcal{S}_n$ is given by $w_0 s_i w_0 = s_{n-i}$.*

Proof. Denote by $w_0 \cdot s_i$ the conjugation action of w_0 on $\mathcal{S}_n$.

We have $w_0 = (1\ n)(2\ (n-1))...(\lfloor n/2 \rfloor\ \lceil n/2 \rceil + 1)$. Notice, firstly, from how w_0 was constructed, that $(k\ l)$ is a disjoint cycle of w_0 if and only if $k + l = n + 1$. Also, if $i \neq k$ and $l \neq i + 1$, then $w_0 \cdot s_i$ fixes k and l, since $(k\ l)$ appears twice in $w_0 \cdot s_i$, so $w_0 \cdot s_i \mid k \mapsto l \mapsto k$, and $l \mapsto k \mapsto k$. Finally, since $w_0 \cdot s_i$ is a transposition, it transposes two (and only two) numbers. So if we find two numbers which $w_0 \cdot s_i$ doesn't fix, then we have found $w_0 \cdot s_i$,

Now, for all $1 \leqslant i \leqslant n-1$, $w_0 \cdot s_i$ transposes $n - i$ and $n - i + 1$. This is because $(i\ (n-i+1))$ and $((i+1)\ (n-i))$ are disjoint cycles of w_0, since $i + (n-i+1) = n+1$ and $(i+1) + (n-i) = n+1$. Also,

$$\begin{aligned} w_0 \cdot s_i : n-i+1 &\mapsto i \mapsto i+1 \mapsto n-i \\ n-i &\mapsto i+1 \mapsto i \mapsto n-i+1 \end{aligned}$$

so $w_0 \cdot s_i = ((n-i)\ (n-i+1)) = s_{n-i}$. □

3.3 The Strong Exchange Condition

In this section, we will state and prove the Strong Exchange Condition. But before we can do that, we must introduce some preliminary ideas. We will proceed as Mathas did in [7, Section 1], and so all proofs are adapted from him.

Throughout this section, $T = \{w s_i w^{-1} \mid w \in W,\ s_i \in S\}$ is the set of transpositions in W.

Definition 3.3.1. Let $w \in W$ and denote by $\mathcal{P}(W)$ the power set of W. The *reflection cocycle* of W is the function $N : W \longrightarrow \mathcal{P}(W)$ given by

$$N(w) = \{(i\ j) \in W \mid i < j, w(i) > w(j)\}.$$

Example 3.3.1. $N(e) = \emptyset$ and $N(s_i) = \{s_i\}$, since, for each i, $s_i(i) = i+1$ and $s_i(i+1) = i$, and s_i fixes every other $j \neq i, i+1$.

Lemma 3.3.1. (Mathas [7, Lemma 1.2].) *Let $v, w \in W$ and denote by Δ the symmetric difference of sets. Then $N(vw) = N(v) \,\Delta\, vN(w)v^{-1}$.*

Proof. We proceed by induction on $\ell(v)$.

Let $\ell(v) = 1$, so $v = s_i \in S$, and let $w = (j\ k) \in W$. Then we claim that $s_i(j\ k)s_i = (s_i(j)\ s_i(k))$. This is trivially true if $i \neq j, k \neq i+1$ or $(j\ k) = s_i$, since $s_i w s_i = w$ and s_i either fixes both j and k or transposes them.

If $j = i, k \neq i+1$ then

$$\begin{aligned} s_i(j\ k)s_i |\ & i \mapsto i+1 \mapsto i \\ & i+1 \mapsto i = j \mapsto k \\ & k \mapsto j = i \mapsto i+1, \end{aligned}$$

so $s_i(j\ k)s_i = s_i(i\ k)s_i = (i+1\ k) = (s_i(i)\ s_i(k))$. Similarly, if $j \neq i, k = i+1$, then $s_i w s_i = (j\ i) = (s_i(j)\ s_i(k))$. So the claim holds in each case, therefore, the hypothesis is true for the base case.

Now suppose $\ell(v) > 1$ and that the induction hypothesis holds for all integers $\ell(u) < \ell(v)$. Since $\ell(v) > 1$, it follows that $v = s_i u$ where $s_i \in S$ and $u \in W$ with $\ell(u) = \ell(v) - 1$. We can find such a u by letting $s_i = s_{r_1}$ where $s_{r_1} \cdots s_{r_k}$ is some reduced expression for v. In particular, $N(v) = N(s_i u) = N(s_i) \,\Delta\, s_i N(u) s_i$, so

$$\begin{aligned} N(vw) = N(s_i u w) = N(s_i(uw)) &= N(s_i) \,\Delta\, s_i N(uw) s_i \\ &= N(s_i) \,\Delta\, s_i N(u) s_i \,\Delta\, s_i u N(w) u^{-1} s_i \\ &= N(v) \,\Delta\, s_i u N(w)(s_i u)^{-1} \\ &= N(v) \,\Delta\, vN(w)v^{-1}. \end{aligned}$$ □

Proposition 3.3.2. (Mathas [7, Proposition 1.3].) *Let $w \in W$. Then*

i) $\ell(w) = |N(w)|$.

ii) $N(w) = \{t \in T \mid \ell(tw) < \ell(w)\}$.

Proof. Let $w \in W$.

i) Let $s_{r_1} \cdots s_{r_k}$ be a reduced expression for w. For each $1 \leqslant i \leqslant k$, let $t_i = s_{r_1} \cdots s_{r_{i-1}} s_{r_i} s_{r_{i-1}} \cdots s_{r_1}$. Recall we showed that t_i is a transposition at the beginning of this section. Then, by Lemma 3.3.1,

$$\begin{aligned} N(w) &= N(s_{r_1} \cdots s_{r_k}) \\ &= N(s_{r_1}) \,\Delta\, s_{r_1} N(s_{r_2} \cdots s_{r_k}) s_{r_1} \\ &= N(s_{r_1}) \,\Delta\, s_{r_1}(N(s_{r_2}) \,\Delta\, s_{r_2} N(s_{r_3} \cdots s_{r_k}) s_{r_2}) s_{r_1}. \end{aligned}$$

Repeatedly iterating this process, we get

$$N(w) = \{t_1\} \,\Delta \cdots \Delta\, \{t_k\},$$

since $N(s_i) = \{s_i\}$ for each s_i, and so conjugating $N(s_i)$ by some s_j means simply conjugating s_i by s_j, which gives some transposition t_j.

We claim that $t_i \neq t_j$ if $i \neq j$. If not, then, for some $1 \leqslant i < j \leqslant k$, we have $t_i = t_j$. Also,

$$\begin{aligned} t_i w &= s_{r_1} \cdots s_{r_{i-1}} s_{r_i} s_{r_{i-1}} \cdots s_{r_1} s_{r_1} \cdots s_{r_k} \\ &= s_{r_1} \cdots s_{r_{i-1}} s_{r_{i+1}} \cdots s_{r_k}, \end{aligned}$$

since $s_{r_1} \cdots s_{r_i}$ is a sub-expression of a reduced expression for w, so all of these factors cancel out. Similarly, $t_j w = s_{r_1} \cdots \hat{s}_{r_j} \cdots s_{r_k}$ where the hat denotes the omission of that element. Therefore,

$$\begin{aligned} w = t_i t_j w &= s_{r_1} \cdots s_{r_{i-1}} s_{r_i} s_{r_{i-1}} \cdots s_{r_1} s_{r_1} \cdots s_{r_{j-1}} s_{r_j} s_{r_{j-1}} \cdots s_{r_1} w \\ &= s_{r_1} \cdots \hat{s}_{r_i} \cdots \hat{s}_{r_j} \cdots s_{r_k} \end{aligned}$$

implying $\ell(w) < k$. This is a contradiction, so each t_i is distinct, so $N(w) = \{t_1, \ldots, t_k\}$ and $|N(w)| = k = \ell(w)$.

ii) Note firstly that $t \in N(t)$ for all $t \in T$. To see this, write $t = (i\ j)$ so that $i < j$. But $t(i) = j > i = t(j)$, so $t \in N(t)$.

Now, let $N(w) = \{t_1, \ldots, t_k\}$ as in the proof of i). We proved that $t_j w = s_{r_1} \cdots \hat{s}_{r_j} \cdots s_{r_k}$ for each t_j, whence $\ell(t_j w) < \ell(w)$. Thus, $N(w) \subseteq \{t \in T \mid \ell(tw) < \ell(w)\}$. On the other hand, let $t \in T$ with $t \notin N(w)$. By Lemma 3.3.1, $N(tw) = N(t)\, \Delta\, tN(w)t$. We know $t \in N(t)$, and by supposition, $t \notin N(w)$, so $t \notin tN(w)t$. Thus, $t \in N(tw) \subseteq \{t \in T \mid \ell(ttw) < \ell(tw)\}$. Therefore, $\ell(ttw) = \ell(w) < \ell(tw)$. □

We can now prove Lemma 3.2.2.

Proof (of Lemma 3.2.2)**.** Recall that $w_0 = (1\ n)(2\ (n-1))...(\lfloor n/2 \rfloor\ \lceil n/2 \rceil + 1)$.

To prove the first part, we use an argument from [10]. Note that there are $\frac{n(n-1)}{2}$ pairs $(i\ j) \in W$ with $i < j$. There are $n-1$ pairs $(1\ 2), (1\ 3), \ldots (1\ n)$, $n-2$ pairs $(2\ 3), (2\ 4) \ldots (2\ n)$, ..., and one pair $(n-1\ n)$. Summing all of these gives

$$(n-1) + (n-2) + \cdots + 1 = \sum_{k=1}^{n-1} k = \frac{n(n-1)}{2} \text{ pairs.}$$

Thus for any $w \in W$, we have $N := \frac{n(n-1)}{2} \geqslant \ell(w) = |N(w)|$, as there are at most N pairs $(i\ j)$ with $w(i) > w(j)$. Since w_0 has exactly N such pairs (in its reduced expression), it follows that $\ell(w_0) = N$. In particular, $\ell(w_0) \geqslant \ell(w)$ for all $w \in W$.

Now, $\ell(ww_0) \geqslant \ell(w)_0) - l(w)$, by Lemma 3.2.1. So we require to show that $\ell(ww_0) \leqslant \ell(w_0) - \ell(w)$. We will do so by induction on $\ell(w_0) - \ell(w)$, using an argument from [2]. Let $w \in W$.

If $\ell(w) = \ell(w_0)$, then $w = w_0$, so $\ell(ww_0) = \ell(e) = 0$. (This holds, in particular, for w_0^{-1}, whence w_0 is an involution.)

Now suppose $\ell(w) < \ell(w_0)$. Choose some $s_i \in S$ and let $w' := s_i w$ such that $\ell(w') > \ell(w)$. In particular, $\ell(w') = \ell(w) + 1$. We can do this since $\ell(w)$ is not maximal, so we can increase it. So, $\ell(w_0) - \ell(w') < \ell(w_0) - \ell(w)$, thus the induction hypothesis holds for $\ell(w_0) - \ell(w')$. That is, $\ell(w'w_0) = \ell(w_0) - \ell(w')$. Moreover,

$\ell(ww_0) = \ell(s_i s_i w w_0) = \ell(s_i w' w_0) \leqslant \ell(w' w_0) + 1$. Therefore,

$$\begin{aligned}\ell(ww_0) \leqslant \ell(w'w_0) + 1 &= \ell(w_0) - \ell(w') + 1\\ &= \ell(w_0) - (\ell(w) + 1) + 1\\ &= \ell(w_0) - \ell(w).\end{aligned}$$

Finally, noting that $w^{-1}w_0 = (w_0 w)^{-1}$, we have

$$\ell(w_0 w) = \ell(w^{-1}w_0) = \ell(w_0) - \ell(w^{-1}) = \ell(w_0) - \ell(w). \qquad \square$$

We are now ready to introduce the Strong Exchange Condition.

Theorem 3.3.3. (Strong Exchange Condition.) *Let $w = s_{r_1} \cdots s_{r_k}$ be a reduced expression for w. If $t \in T$ satisfies $\ell(tw) < \ell(w)$, then there exists an i with $1 \leqslant i \leqslant k$ such that*

$$tw = s_{r_1} \cdots \hat{s}_{r_i} \cdots s_{r_k},$$

where $\hat{s}_{r_i}$ denotes the omission of s_{r_i}. Furthermore, $t = t_i$ (as in Proposition 3.3.2), and if the expression for w is reduced, then i is unique.

Proof. For $1 \leqslant i \leqslant k$, let t_i be as in the proof of Proposition 3.3.2. Then $N(w) = \{t_1\} \,\Delta \cdots \Delta\, \{t_k\}$ by Lemma 3.3.1 and $t \in N(w)$ by Proposition 3.3.2 ii). Recall we showed that $N(w) = \{t_1, \ldots, t_k\}$, so $t = t_i$ for some i. We also showed that, in this case, $t_i w = s_{r_1} \cdots \hat{s}_{r_i} \cdots s_{r_k}$, and that the omitted s_{r_i} is unique. $\square$

Corollary 3.3.4. Mathas [7, Corollary 1.7] *Let $w \in W$ and $s_i \in S$. Then $\ell(s_i w) < \ell(w)$ if and only if w has a reduced expression starting with s_i.*

Proof. Suppose $\ell(s_i w) < \ell(w)$ and let $s_{r_1} \cdots s_{r_k}$ be a reduced expression for w. Then $s_i w = s_i s_{r_1} \cdots \hat{s}_{r_j} \cdots s_{r_k}$ for some j, using the Strong Exchange Condition, so $w = s_i s_{r_1} \cdots \hat{s}_{r_j} \cdots s_{r_k}$ which is reduced as it has length k. The converse is easy to prove and left to the reader. $\square$

The last two results listed will be important in the next section.

Theorem 3.3.5. (Matsumoto's Theorem.) *Two expressions $s_{r_1} \cdots s_{r_k}$ and $s'_{r_1} \cdots s'_{r_l}$ are both reduced expressions for some $w \in W$ if and only if one can be transformed into the other using only the braid relations.*

Proof. See Mathas [7, pp. 4–5]. $\square$

Lemma 3.3.6. *Let $w \in W$ and $s_i, s_j \in S$ such that s_i and s_j commute. Then $\ell(s_j w) > \ell(w)$ and $\ell(s_i s_j w) = \ell(w)$ and if and only $\ell(s_i w) < \ell(w)$ and $\ell(s_j s_i w) = \ell(w)$.*

Proof. Firstly, if $\ell(s_i s_j w) < \ell(s_j w)$, then $s_i \in N(s_j w)$, by Proposition 3.3.2. Now, consider $N(w)$. We have

$$N(w) = N(s_j s_j w) = N(s_j) \,\Delta\, s_j N(s_j w) s_j = \{s_j\} \,\Delta\, s_j N(s_j w) s_j,$$

by Lemma 3.3.1. Since $s_i \in N(s_j w)$, $s_j s_i s_j \in s_j N(s_j w) s_j$, so $s_j s_i s_j \in N(w)$ because $s_j s_i s_j \notin \{s_j\}$. But s_i and s_j commute, so $s_i s_j = s_j s_i$. Therefore, $s_j s_i s_j = (s_j)^2 s_i = s_i \in N(w)$, and if $\ell(s_i s_j w) = \ell(w)$, then $\ell(s_j s_i w) = \ell(w)$ since $s_i s_j w = s_j s_i w$. The converse follows from reversing the preceding arguments. $\square$

4 The Module Theory of the 0-Hecke Algebra

4.1 The 0-Hecke Algebra

Definition 4.1.1. Let $\mathbb{F}$ be a field. The *0-Hecke algebra* $\mathcal{H}_0(W)$ is the associative $\mathbb{F}$-algebra with generators $h_1, \ldots, h_n$ satisfying the following relations.
i) $(h_i)^2 = -h_i$.
ii) $h_i h_j = h_j h_i$ for all $j \neq i \pm 1$.
iii) $h_i h_{i+1} h_i = h_{i+1} h_i h_{i+1}$.

From now on, we will write $\mathcal{H}$ for $\mathcal{H}_0(W)$. $\mathcal{H}$ is part of a larger family of algebras called *Iwahori-Hecke algebras*. See [6] for a general discussion on Iwahori-Hecke algebras.

Note that the generators of $\mathcal{H}$ are in bijection with the generators of W. For any $w \in W$, let $s_{r_1} \cdots s_{r_k}$ be a reduced expression for w. Define $h_w = h_{r_1} \cdots h_{r_k}$. By Matsumoto's Theorem, this is well-defined as it's independent of the reduced expression for w. If $w = e$, then $h_w = 1_{\mathbb{F}}$.

Theorem 4.1.1. (Fayers [3, Theorem 2.1].) *Let $w \in W$ and $s_i \in S$. Then $h_{s_i} = h_i$ and*

$$h_i h_w = \begin{cases} h_{s_i w} & \text{if } \ell(s_i w) > \ell(w)), \\ -h_w & \text{if } \ell(s_i w) < \ell(w)). \end{cases}$$

Moreover, as an $\mathbb{F}$-module, $\mathcal{H}$ has a basis $\{h_w \mid w \in W\}$.

Proof. Clearly, $h_{s_i} = h_i$, by definition.

Now, suppose $\ell(s_i w) > \ell(w)$. Then $\ell(s_i w) = \ell(w) + 1$, so $s_i s_{r_1} \cdots s_{r_k}$ is a reduced expression for $s_i w$ and

$$h_{s_i w} = h_{s_i} h_{r_1} \cdots h_{r_k} = h_i h_{r_1} \cdots h_{r_k} = h_i h_w.$$

And if $\ell(s_i w) < \ell(w)$, then $s_i \cdots s_{r_k}$ is a reduced expression for w by Corollary 3.3.4, so $h_w = h_i \cdots h_{r_k}$. Thus, using $s_i \cdots s_{r_k}$ as the reduced expression for w, we have

$$h_i h_w = h_{s_i} h_w = h_{s_i} h_{s_i} \cdots h_{r_k} = (h_{s_i})^2 \cdots h_{r_k} = -h_{s_i} \cdots h_{r_k} = -h_w.$$

Now, recall that the $h_i's$ and $s_i's$ are in bijection. So given any $h \in H$, we can write it minimally as $h = h_{r_1} \cdots h_{r_k} = h_{s_{r_1}} \cdots h_{s_{r_k}} = h_w$ where $w \in W$ and $s_{r_1} \cdots s_{r_k}$ is a reduced expression for this w. Thus, it follows that $h = h_w$, and so $\{h_w \mid w \in W\}$ spans $\mathcal{H}$.

Now, suppose R is an $\mathbb{F}$-algebra with basis $\{e_w | w \in W\}$. Using an argument from Mathas [7, Theorem 1.13], we shall show that $\mathrm{Hom}_{\mathbb{F}}(R, R)$ admits a subalgebra $\mathcal{R}$ generated by elements which satisfy i), ii) and iii) from Definition 4.1.1. Let $\vartheta_1, \ldots, \vartheta_n \in \mathrm{Hom}_{\mathbb{F}}(R, R)$ be given by

$$\vartheta_i(e_w) = \begin{cases} e_{s_i w} & \text{if } \ell(s_i w) > \ell(w), \\ -e_w & \text{if } \ell(s_i w) < \ell(w), \end{cases}$$

for all $1 \leqslant i \leqslant n$. We claim that $\mathcal{R} \cong \mathcal{H}$.

Firstly, suppose $\ell(s_i w) > \ell(w)$ (so $\ell(s_i(s_i w)) < \ell(s_i w)$). Then

$$\vartheta_i(\vartheta_i(e_w)) = \vartheta_i(e_{s_i w}) = -e_{s_i w}.$$

And if $\ell(s_i w) < \ell(w)$, then

$$\vartheta_i(\vartheta_i(e_w)) = \vartheta_i(-e_w) = e_w.$$

So, overall,

$$\vartheta_i(\vartheta_i(e_w)) = \begin{cases} -e_{s_i w} & \text{if } \ell(s_i w) > \ell(w), \\ e_w & \text{if } \ell(s_i w) < \ell(w), \end{cases}$$

from which it follows that $\vartheta_i^2 = -\vartheta_i$.

Now, let us show that $\vartheta_i \vartheta_j = \vartheta_j \vartheta_i$ for $j \neq i \pm 1$, and we leave showing $\vartheta_i \vartheta_{i+1} \vartheta_i = \vartheta_{i+1} \vartheta_i \vartheta_{i+1}$ to the reader. (Note that $s_i s_j = s_j s_i$ in this case.) Either $\ell(s_i s_j w) = \ell(w)$ or $\ell(s_i s_j w) = \ell(w) \pm 2$. Let us list the all cases for $\vartheta_i(\vartheta_j(e_w))$ and $\vartheta_j(\vartheta_i(e_w))$.

First, suppose $\ell(s_j w) > \ell(w)$. Then

$$\vartheta_i(\vartheta_j(e_w)) = \begin{cases} e_{s_i s_j w} & \text{if } \ell(s_i s_j w) > \ell(s_j w), \\ -e_{s_j w} & \text{if } \ell(s_i s_j w) < \ell(s_j w). \end{cases}$$

Second, suppose $\ell(s_j w) < \ell(w)$. Then

$$\vartheta_i(\vartheta_j(e_w)) = \begin{cases} -e_{s_i w} & \text{if } \ell(s_i s_j w) > \ell(s_j w), \\ e_w & \text{if } \ell(s_i s_j w) < \ell(s_j w). \end{cases}$$

Now suppose $\ell(s_i w) > \ell(w)$. Then

$$\vartheta_j(\vartheta_i(e_w)) = \begin{cases} e_{s_j s_i w} & \text{if } \ell(s_j s_i w) > \ell(s_i w), \\ -e_{s_i w} & \text{if } \ell(s_j s_i w) < \ell(s_i w). \end{cases}$$

Finally, if $\ell(s_i w) < \ell(w)$, then

$$\vartheta_i(\vartheta_j(e_w)) = \begin{cases} -e_{s_j w} & \text{if } \ell(s_j s_i w) > \ell(s_i w), \\ e_w & \text{if } \ell(s_j s_i w) < \ell(s_i w). \end{cases}$$

If $\ell(s_i s_j w) = \ell(w) + 2$, then $\ell(s_j w) > \ell(w)$ and $\ell(s_i s_j w) > \ell(s_j w)$, so $\vartheta_i(\vartheta_j(e_w)) = e_{s_i s_j w}$. And since $s_i s_j = s_j s_i$, we have $\ell(s_j s_i w) = \ell(w) + 2$, so $\ell(s_i w) > \ell(w)$ and $\ell(s_j s_i w) > \ell(s_i w)$, whence $\vartheta_j(\vartheta_i(e_w)) = e_{s_j s_i w} = e_{s_i s_j w} = \vartheta_i(\vartheta_j(e_w))$.

Similarly, if $\ell(s_i s_j w) = \ell(w) - 2$, then $\vartheta_i(\vartheta_j(e_w)) = \vartheta_i(-e_w) = e_w = \vartheta_j(\vartheta_i(e_w))$.

If $\ell(s_i s_j w) = \ell(w)$, then assume first that $\ell(s_j w) > \ell(w)$. By Lemma 3.3.6, this implies $\ell(s_i w) < \ell(w)$ and $\ell(s_j s_i w) = \ell(w)$. Therefore, $\ell(s_i s_j w) < \ell(s_j w)$ and $\ell(s_j s_i w) > \ell(s_i w)$, so

$$\vartheta_i(\vartheta_j(e_w)) = \vartheta_i(e_{s_j w}) = -e_{s_j w} = \vartheta_j(-e_w) = \vartheta_j(\vartheta_i(e_w)).$$

Similarly, if $\ell(s_j w) < \ell(w)$, then, by Lemma 3.3.6, $\ell(s_i w) > \ell(w)$. Thus applying the same argument, we also have $\vartheta_i(\vartheta_j(e_w)) = \vartheta_j(\vartheta_i(e_w))$.

So $\mathcal{R}$ and $\mathcal{H}$ are generated by elements both satisfying the same defining relations, so there is a surjective algebra hom $\Theta : \mathcal{H} \to \mathcal{R}$ given by $\Theta(h_i) = \vartheta_i$. Furthermore, given $w \in W$ with reduced expression $s_{r_1} \cdots s_{r_k}$, define $\vartheta_w := \vartheta_{r_1} \cdots \vartheta_{r_k}$. Then $\Theta(h_w) = \vartheta_w$. (By Matsumoto's Theorem, this is independent of the reduced expression for W.) Observe that $\vartheta_w(e_e) = \vartheta_{r_1} \cdots \vartheta_{r_k}(e_e) = \vartheta_{r_1} \cdots \vartheta_{r_{k-1}}(e_{s_{r_k}}) = \ldots = e_{s_{r_1} \cdots s_{r_k}} = e_w$.

We are now able to show that $\{h_w \,|\, w \in W\}$ is a linearly independent set. Suppose $h := \sum_{w \in W} \lambda_w h_w = 0$, where $\lambda_w \in \mathbb{F}$. Then $\vartheta(h) = \sum_{w \in W} \lambda_w \vartheta_w = 0$ in $\mathcal{R}$. Therefore, in R,

$$\sum_{w \in W} \lambda_w e_w = \sum_{w \in W} \lambda_w \vartheta_w(e_e) = 0.$$

Since $\{e_w \,|\, w \in W\}$ is a basis for R, we must have $\lambda_w = 0$ for all $w \in W$, so $\{h_w \,|\, w \in W\}$ is a linearly independent set, and so a basis for $\mathcal{H}$. This also implies that Θ is an isomorphism, as it implies $\ker(\Theta) = 0$. □

Corollary 4.1.2. (Norton [8, Corollary 1.4].) *Let $w, w' \in W$. Then*
i) $h_w h_{w'} = \pm h_{w''}$ for some $w'' \in W$ with $\ell(w'') \geqslant \ell(w')$.
ii) $h_w h_{w'} = h_{ww'}$ if and only if $\ell(ww') = \ell(w) + \ell(w')$.

Proof. Let $w, w' \in W$. Let $s_{r_1} \cdots s_{r_k}$ be a reduced expression for w and $s'_{r_1} \cdots s'_{r_l}$ be a reduced expression for w'.

i) Then

$$h_w h_{w'} = h_{s_{r_1}} \cdots h_{s_{r_k}} h_{w'}.$$

By Theorem 4.1.1, multiplying $h_{w'}$ by any $h_{s_{r_i}}$ on the left either equals $h_{s_{r_i} w'}$ or $-h_{w'}$. In particular, multiplying $h_{w'}$ on the left by a generator can't decrease the length of w'. Thus, doing this for each s_{r_i} in the reduced expression for w, we have $h_w h_{w'} = \pm h_{w''}$, with $\ell(w'') \geqslant \ell(w')$.

ii) First suppose $\ell(ww') = \ell(w) + \ell(w')$. Then since $\ell(ww') = k + l$, it follows that $s_{r_1} \cdots s_{r_k} s'_{r_1} \cdots s'_{r_l}$ is a reduced expression for ww', so

$$h_{ww'} = h_{s_{r_1}} \cdots h_{s_{r_k}} h_{s'_{r_1}} \cdots h_{s'_{r_l}} = h_w h_{w'}.$$

Now suppose $h_w h_{w'} = h_{ww'}$. Then

$$h_{ww'} = h_{s_{r_1}} \cdots h_{s_{r_k}} h_{s'_{r_1}} \cdots h_{s'_{r_l}}.$$

This implies that $s_{r_1} \cdots s_{r_k} s'_{r_1} \cdots s'_{r_l}$ is a reduced expression for ww', so $\ell(ww') = k + l = \ell(w) + \ell(w')$. □

We can now give an example of a 0-Hecke algebra using Theorem 4.1.1.

Example 4.1.1. Let $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$ and $W = S_2$. Note that W is generated by (1 2). Write 1 and h for the basis elements of $\mathcal{H}(W)$. Then $\mathcal{H}(W) = \{0, 1, h, 1+h\}$. We are working in characteristic 2, whence $2h = 2(1 + h) = 0$. Moreover, $-1_{\mathbb{F}} = 1_{\mathbb{F}}$, so $h^2 = -h = h$. and $(1 + h)^2 = 1^2 + h^2 = 1 + h$. (Note this makes $\mathcal{H}(W)$ a boolean algebra.) Thus, the addition table for $\mathcal{H}(W)$ is

$+$	0	1	h	$1+h$
0	0	1	h	$1+h$
1	1	0	$1+h$	h
h	h	$1+h$	0	1
$1+h$	$1+h$	h	1	0

and the multiplication table is

$\cdot$	0	1	h	$1+h$
0	0	0	0	0
1	0	1	h	$1+h$
h	0	h	h	0
$1+h$	0	$1+h$	0	$1+h$

4.2 Simple $\mathcal{H}$-Modules

Define the following order on the elements of W:

$$e \leqslant w_1 \ldots \leqslant w_{N-1} \leqslant w_N = w_0,$$

where $N := (n+1)! - 1$. If w_i and w_j have the same length, then write them in any order. Write $w > w'$ Let $h_0 := 1_{\mathbb{F}} = h_e$ and rewrite the basis of H as $\{h_i \mid 0 \leqslant i \leqslant N\}$ in bijection with the elements of W. Note, in particular, that $h_1, \ldots, h_n$ are still the generators of $\mathcal{H}$.

Lemma 4.2.1. (Norton [8, Section 2].) *Let $M_0 := \mathcal{H}$ and for $1 \leqslant i \leqslant N$, define M_i to be the $\mathbb{F}$-module with basis $\{h_j \mid j \geqslant i\}$. Then each M_i is an $\mathcal{H}$-module.*

Proof. It suffices to show that each M_i is a left ideal of $\mathcal{H}$.

Let $h \in \mathcal{H}$ and $h_i \in M_i$. Write $h = \lambda_0 h_0 + \ldots + \lambda_N h_N$. We must show that $hh_i \in M_i$. Fix some j such that $0 \leqslant j \leqslant N$. Then by Corollary 4.1.2, $h_j h_i = \pm h_k$ with $k \geqslant i$. Thus, $\pm h_j h_i$ is a basis element of M_i, and so $\lambda h_j h_i$ is an element of M_i. Thus, $hh_i = \lambda_0 h_0 h_i + \cdots + \lambda_N h_N h_i \in M_i$, whence M_i is an ideal of $\mathcal{H}$. □

Theorem 4.2.2. (Fayers [3, Theorem 2.2].) *For each subset J of $\{1, \ldots, n\}$, let M_J be the $\mathcal{H}$-module with basis $\{h\}$ and $\mathcal{H}$-action given by*

$$h_j h = \begin{cases} -h & \text{if } j \in J, \\ 0 & \text{if } j \notin J \end{cases}$$

Then $\{M_J \mid J \subseteq \{1, \ldots, n\}\}$ is a complete set of simple $\mathcal{H}$-modules.

Proof. We will follow Norton's proof from [8, Section 3].

From Lemma 4.2.1, we have the following series of $\mathcal{H}$-ideals:

$$\mathcal{H} = M_0 \geqslant M_1 \geqslant \ldots \geqslant M_N = h_N\mathcal{H} \geqslant 0.$$

This is a natural composition series of $\mathcal{H}$, and so each M_i/M_{i+1} is a one-dimensional $\mathcal{H}$-module. Therefore, by Theorem 2.6.2, these are simple modules. In fact, these are all of the simple $\mathcal{H}$-modules.

To see this, let M be a finitely generated $\mathcal{H}$-module with m generators. Then there exists a projection $\phi : \mathcal{H}^k \to M$, so M is (isomorphic to) a quotient module of $\mathcal{H}^m$. This is because $\mathcal{H}^k/\ker(\phi) \cong M$, by the First Isomorphism Theorem.

But from the given composition series of $\mathcal{H}$, by Proposition 2.6.1, we can produce a composition series of $\mathcal{H}^m$ with the same property. Similarly, this induces a composition series of its quotient module M, which will, again, have the same property as the composition series of $\mathcal{H}^m$. This shows that M can't be simple unless it's one-dimensional.

Now, each M_i/M_{i+1} has a 1-dimensional basis $\{h_{w_j} + M_{i+1}\} =: [h_{w_j}]$. The $\mathcal{H}$-action is given by $h_{s_i}[h_{w_j}] = [h_{s_i}h_{w_j}]$, by Theorem 2.1.1. And by Theorem 3.1.1, $h_{s_i}h_{w_j}$ equals either $h_{s_iw_j}$ or $-h_{w_j}$. But $h_{s_iw_j} \in M_{i+1}$, so in this case, $[h_{s_i}h_{w_j}] = [0] = 0 \in M_i/M_{i+1}$. Thus, overall, $h_{s_i}[h_{w_j}] = 0$ or $h_{s_i}h_{w_j} = -[h_{w_j}]$.

We must show that this action and the $\mathcal{H}$-action from the theorem are equivalent. For any $J \subseteq \{1, \ldots, n\}$, let W_J be the subgroup of W generated by $S_J := \{s_j \mid j \in J\} \subseteq S$. Let w_{N_J} be the unique longest element in $W(J)$. For such a w_{N_J}, we have $\{i \in \{1, \ldots, n\} \mid s_iw_{N_J} < w_{N_J}\} = J$. That is, if w_{N_J} generates a simple module, then the $\mathcal{H}$-action on that module will be exactly as described in the theorem. We showed that there are 2^{N+1} simple $\mathcal{H}$-modules, and there are exactly 2^{N+1} of these elements w_{N_J}.

Moreover, given the construction of the ideals, each ideal will contain a w_{N_J} for some J, so w_{N_j} will generate that ideal. So given any $J \subseteq \{1, \ldots, n\}\}$, arbitrarily choose $i \in \{0, \ldots, N\}$ so that M_i/M_{i+1} is generated by w_{N_J}, and let $M_J := M_i/M_{i+1}$. Then $\{M_J \mid J \subseteq \{1, \ldots, n\}\}$ is a complete set of simple $\mathcal{H}$-modules. □

4.3 Automorphisms and Duality

In this section, we list some automorphisms and dualities which will be useful in the next section.

Definition 4.3.1. Let R be a $\mathbb{F}$-algebra. A hom $\phi : R \to R$ is an *anti-automorphism* if ϕ satisfies $\phi(rs) = \phi(s)\phi(r)$ for all $r, s \in R$, together with the remaining ring homomorphism axioms and $\mathbb{F}$-linearity.

Proposition 4.3.1. (Fayers [3, Proposition 3.2].) *There is an automorphism of $\mathcal{H}$ given by*

$$\psi : h_i \mapsto h_{w_N s_i w_N},$$

and an anti-automorphism given by

$$\chi : h_i \mapsto h_i$$

for $i = 1, \dots, n$.

Proof. Let us check that ψ preserves the defining relations for $\mathcal{H}$. Recall that $w_N s_i w_N = s_{n+1-i}$, so $\psi(h_i) = h_{n+1-i}$. Therefore, $(\psi(h_i))^2 = -h_{n+1-i} = -\psi(h_i)$. Furthermore, if $j \neq i \pm 1$, then

$$\psi(h_i h_j) = h_{n+1-i} h_{n+1-j} = h_{n+1-j} h_{n+1-i} = \psi(h_j h_i).$$

This follows since $n+1-j \neq (n+1-i) \pm 1$ if $j \neq i \pm 1$. Finally, it is easy to see that

$$\psi(h_i h_{i+1} h_i) = h_{n+1-i} h_{n+2-i} h_{n+1-i} = h_{n+2-i} h_{n+1-i} h_{n+2-i} = \psi(h_{i+1} h_i h_{i+1}).$$

The reader is left to check the same holds for χ. □

Now suppose M is an $\mathcal{H}$-module.

We define $\overline{M}$ to be the module with the same underlying vector space as M, but with the $\mathcal{H}$-action given by

$$hm = \psi(h)m,$$

for all $h \in \mathcal{H}$ and $m \in M$.

We also define $M^\diamond$ to be the vector space dual to M, with the $\mathcal{H}$-action given by

$$(hf)(m) = f(\chi(h)m),$$

for all $h \in \mathcal{H}$, $f \in M^\diamond$ and $m \in M$. Finally, we define $M^\circ = (\overline{M})^\diamond \cong \overline{M^\diamond}$.

Proposition 4.3.2. (Fayers [3, Proposition 3.3].) *Let* $J \subseteq \{1, \dots, n\}$ *and* M_J *be as in Theorem 4.2.2. Then* $M_J^\diamond \cong M_J$ *and* $\overline{M}_J \cong (M_J)^\circ$.

Proof. If we can prove the first equivalence, then the second follows by definition. Since M_J is one-dimensional, $(M_J)^*$ is also one-dimensional and hence, simple. So $\dim_{\mathcal{H}}(M_J) = \dim_{\mathcal{H}}((M_J)^*)$, and M_J and $(M_J)^*$ have the same $\mathcal{H}$-action. Therefore, $M_J \cong (M_J)^*$ and the result follows. □

4.4 Projective and Injective $\mathcal{H}$-Modules

Definition 4.4.1. Let R be an $\mathbb{F}$-algebra. R is *Frobenius* if there exists a linear map $\phi : R \to \mathbb{F}$ such that $\ker(\phi)$ contains no left or right ideal of R.

Proposition 4.4.1. (Fayers, [3, Proposition 4.1].) *$\mathcal{H}$ is Frobenius.*

Proof. Define $\phi : \mathcal{H} \to \mathbb{F}$ by mapping

$$\phi\left(h_{w_i}\right) = \begin{cases} -1 & \text{if } w_i = w_N, \\ 0 & \text{otherwise,} \end{cases}$$

and extending by linearity.

Let $I_{\mathcal{H}}$ and ${}_{\mathcal{H}}I$ be left and right ideals of $\mathcal{H}$. We must show that $I_{\mathcal{H}}, {}_{\mathcal{H}}I \notin \ker(\phi)$.

Let $h \in \mathcal{H}$ be nonzero. We must find $j, k \in \mathcal{H}$ such that $\phi(jh), \phi(hk) \neq 0$. Write $h = \lambda_0 h_{w_0} + \ldots + \lambda_N h_{w_N}$ and let w_i be the element of maximal length such that $h_i = h_{w_i}$ has a nonzero coefficient. Let $j = h_{w_N w_i^{-1}}$ and $k = h_{w_i^{-1} w_N}$. Then, by Corollary 4.1.2, $jh_{w_i} = h_{W_N} = h_{w_i}k$, since

$$\ell(w_N w_i^{-1} w_i) = \ell(w_N) - \ell(w_i^{-1} w_i) = \ell(w_N) + \ell(w_i^{-1} w_i),$$

because $\ell(w_i^{-1} w_i) = 0$. Moreover, if $j \neq i$, then $jh_{w_j}, h_{w_j}k \neq h_{w_N}$ because

$$\ell(w_N w_i^{-1} w_j) = \ell(w_N) - \ell(w_i^{-1} w_j) \neq \ell(w_N).$$

Thus, $\phi(jh), \phi(hk) \neq 0$, so $\phi(jh), \phi(hk) \notin \ker(\phi)$, so $\mathcal{H}$ is Frobenius. □

Proposition 4.4.2. (Fayers [3, Proposition 4.2].) *Let ϕ be the linear map defined in the proof of Proposition 4.4.1. Then, for any $h, j \in \mathcal{H}$, we have $\phi(hj) = \phi(\psi(j)h)$.*

Proof. By linearity, it suffices to only check the case where $h = h_{w_i}$ and $j = h_{w_j}$. By Corollary 4.1.2, $\phi(hj) = 1$ if and only if $hj = h_{w_N}$, and $hj = h_{w_N}$ if and only if $j = h_{w_i^{-1} w_N}$. Similarly, $\phi(\psi(j)h) = 1$ if and only if $\psi(j) = h_{w_N w_i^{-1}}$. But $\psi(j) = h_{w_N w_j w_N}$, so $\phi(hj) = 1$ if and only if $j = \phi(\psi(j)h) = 1$. This is because if $j = h_{w_i^{-1} w_N}$, then $\psi(j) = h_{w_N w_i^{-1} w_N w_N} = h_{w_N w_i^{-1}}$. Similarly, if $j = h_{w_N w_i^{-1}}$, then $\psi(j) = h_{w_i^{-1} w_N}$. □

Lemma 4.4.3. (Benson [1, Proposition 1.6.2].) *Let R be an $\mathbb{F}$-algebra. If R is Frobenius, then R is self-injective. Moreover, any finitely generated R-module is projective if and only if it is injective.*

Proof. We will only prove the lemma for the case where $R = \mathcal{H}$.

Write ${}_{\mathcal{H}}\mathcal{H}$ when considering $\mathcal{H}$ as a left $\mathcal{H}$-module and write $\mathcal{H}_{\mathcal{H}}$ when considering $\mathcal{H}$ as a right $\mathcal{H}$-module. We showed that $\mathcal{H}$ is free, so by Proposition 2.4.1, $\mathcal{H}$ is projective. Therefore, if we show that ${}_{\mathcal{H}}\mathcal{H} \cong (\mathcal{H}_{\mathcal{H}})^*$, then, by duality, this will imply that $\mathcal{H}$ is injective.

Recall that $(\mathcal{H}_{\mathcal{H}})^* = \mathrm{Hom}(\mathcal{H}, \mathbb{F})$ is a natural left $\mathcal{H}$-module. Define a hom $\vartheta : {}_{\mathcal{H}}\mathcal{H} \to (\mathcal{H}_{\mathcal{H}})^*$ given by $\vartheta(h) : j \to \phi(jh)$, where ϕ is the linear map from Proposition 4.4.1. Then

$$\vartheta(h + h')(j) = \phi(j(h + h')) = \phi(jh) + \phi(jh') = \vartheta(h) + \vartheta(h'),$$

so ϑ is a hom. We showed in Proposition 4.4.1 that $\phi(jh) \neq 0$ whenever $h \neq 0$. Thus, $\ker(\vartheta) = 0$, so ϑ is injective. Thus, ϑ must also be surjective, since $\dim_{\mathbb{F}}({}_{\mathcal{H}}\mathcal{H}) = \dim_{\mathbb{F}}((\mathcal{H}_{\mathcal{H}})^*)$, as $\mathcal{H}$ is finitely generated.

Since $\mathcal{H}$ is self-injective, it follows that an $\mathcal{H}$-module M is projective if and only if M^* is projective. And, by duality, M^* is projective if and only if M is injective. □

Definition 4.4.2. Let R be an $\mathbb{F}$-algebra. An element $e \in R$ is an *idempotent* if $e^2 = e$.

Note that in ring theory, e is used to denote an idempotent, whereas in group theory, e is used to denote the identity.

If ϑ is a module hom and e is an idempotent, then $\vartheta(e)$ is an idempotent, since $\vartheta(e)^2 = \vartheta(e^2) = \vartheta(e)$.

Lemma 4.4.4. (Benson [1, Lemma 1.3.3].) *Let R be an $\mathbb{F}$-algebra, M be an R-module and e be an idempotent in R. Then*

$$eM \cong Hom_R(Re, M).$$

Proof. Define a map $\vartheta : eM \to \mathrm{Hom}_R(Re, M)$ given by $\vartheta(em) : re \mapsto rem$. To see that ϑ is a hom, suppose $m, n \in M$. Then

$$(\vartheta(em + en))(re) = (\vartheta(e(m + n)))(re) = re(m + n) = rem + ren = (\vartheta(em) + \vartheta(en))(re).$$

Now define $\bar{\vartheta} : \mathrm{Hom}_R(Re, M) \to eM$ given by $\bar{\vartheta}(f) = f(e)$ for all $f \in \mathrm{Hom}_R(Re, M)$. Again, $\bar{\vartheta}$ is a hom. Let $f, g \in \mathrm{Hom}_R(Re, M)$. Then

$$\bar{\vartheta}(f + g) = (f + g)(e) = f(e) + g(e) = \bar{\vartheta}(f) + \bar{\vartheta}(g).$$

It remains to show ϑ and $\bar{\vartheta}$ are inverses. Indeed, if $f \in \mathrm{Hom}_R(Re, M)$, then $f(e) = f(1e) = em$, so

$$(\vartheta(\bar{\vartheta}(f)))(re) = \vartheta(f(e))(re) = \vartheta(em)(re) = rem = f(em).$$

And if $m \in M$, then $\bar{\vartheta}(\vartheta(em)) = em$, since $\vartheta(em) : e \mapsto em$. □

Proposition 4.4.5. (Fayers [3, Proposition 4.5].) *For each simple module M_J of $\mathcal{H}$, we have*

$$P(M_J) \cong I(\overline{M}_J).$$

Hence, for any projective module P of $\mathcal{H}$, we have $P^\circ \cong P$.

Proof. Let M_J be any simple $\mathcal{H}$-module. Then M_J has an injective cover $I = I(M_J)$. But I is also projective, and since M_J embeds into I minimally, it follows that I covers M_J minimally, so $I = P(M_J)$. Thus, by Lemma 2.6.4, $\mathrm{soc}(P)$ is simple whenever $P = P(M_J)$.

Now, by Norton [8, Theorem 4.20], for each subset J of $\{1, \ldots, n\}$, there exist idempotents $q_J \in \mathcal{H}$ such that $\mathcal{H}q_J$ are ideals and

$$\mathcal{H} \cong \bigoplus_J \mathcal{H}q_J.$$

Since $\mathcal{H}$ is free, Theorem 2.4.2 implies that each $\mathcal{H}q_J$ is a projective $\mathcal{H}$-module. Moreover, $\mathcal{H}q_J$ is finitely generated, and thus injective, too. Thus, $\mathcal{H}q_J \cong P = P(M_J)$ for the simple $\mathcal{H}$-module M_J.

We then have $H\psi(q_J) \cong \overline{P} = P(\overline{M}_J)$. Also, $\mathrm{soc}(P)q_J$ is a left ideal of $\mathcal{H}$ (as it is a submodule of $\mathcal{H}$), so there exists some $p \in \mathrm{soc}(P)$ such that

$$0 \neq \phi(pq_J) = \phi(\psi(q_J)p),$$

where the first equality holds since $\mathcal{H}$ is Frobenius and the second follows from Proposition 4.4.2. Thus,

$$0 \neq \psi(q_J)\mathrm{soc}(P) \cong \mathrm{Hom}_R(H\psi(q_J), \mathrm{soc}(P)) \cong \mathrm{Hom}_R(\overline{P}, \mathrm{soc}(P)),$$

by Lemma 3.4.4. So there is a nonzero hom from $\overline{P}$ to $\mathrm{soc}(P)$. And since $\mathrm{soc}(P)$ is simple, there is an isomorphism from $\mathrm{soc}(P)$ to the simple submodule $\overline{M}_J$ of $\overline{P}$. Note that $\overline{M}_J \leqslant \overline{P}$ since $\overline{P}$ projects on $\overline{M}_J$, meaning $\overline{M}_J$ embeds into $\overline{P}$. Therefore, $\overline{M}_J$ is isomorphic to its image in $\overline{P}$, which is a submodule of $\overline{P}$. Therefore, $P(M_J) = I(\overline{M}_J) \cong I((M_J)^\circ)$, since $\overline{M}_J \cong (M_J)^\circ$, by Proposition 4.3.3. Moreover, since $\mathcal{H} \cong \mathcal{H}^\circ$ (by Fayers [3, Proposition 3.4]), it follows that $\mathcal{H}q_J \cong (\mathcal{H}q_J)^\circ$ for all q_J.

Now, consider the case where P is any projective module (so $\mathrm{soc}(P)$ is not necessarily simple). Then

$$P = P_1 \oplus \cdots \oplus P_k,$$

where $\mathrm{soc}(P_i)$ is simple for each $1 \leqslant i \leqslant k$. But we showed that this means that $P_i = P(M_{J_i}) \cong I((M_{J_i})^\circ)$ for each P_i, where $M_{J_1}, \ldots, M_{J_k}$ are all simple $\mathcal{H}$-modules. Finally, since P° is the sum of injective modules with simple socles (as the dual of P), we have

$$P^\circ = I((M_{J_1})^\circ) \oplus \cdots \oplus I((M_{J_k})^\circ),$$

from which it follows that $P \cong P^\circ$. □

Bibliography

[1] D Benson, *Representations and cohomology I*, Cambridge University Press, Cambridge, 1991.

[2] A Björner, F Brenti, *Combinatorics of Coxeter Groups*, Springer-Verlag, New York, 2000.

[3] M Fayers, 0-Hecke algebras of finite Coxeter groups, *J. Pure Appl. Algebra*, **199** (2005), 27–41.

[4] J Humphreys, *Reflection Groups and Coxeter Groups*, Cambridge University Press, Cambridge, 1990.

[5] T Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[6] N Iwahori, H Matsumoto, On some Bruhat decomposition and the structure of the Hecke rings of p-adic Chevalley groups, *Publ. Math. Inst. Hautes Etudes Sci*, **25** (1965), 5–48.

[7] A Mathas, *Iwahori-Hecke Algebras and Schur Algebras of the Symmetric Group*, American Mathematical Society, Providence, 1999.

[8] P Norton, 0-Hecke algebras, *J. Aust. Math. Soc.*, **27** (1979), 337–357.

[9] J Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, New York, 1994.

[10] https://math.stackexchange.com/a/3579104/729653, *math.stackexchange.com*, 12/03/2020.

[11] https://math.stackexchange.com/a/1004741/729653, *math.stackexchange.com*, 08/04/2020.

[12] https://math.stackexchange.com/a/259496/729653, *math.stackexchange.com*, 05/05/2020