SQUARES IN THE CENTRE OF THE GROUP ALGEBRA OF A SYMMETRIC GROUP

J. Murray*
Mathematics Department,
University College Dublin,
Belfield Dublin 4, Ireland.

Let $\mathcal{S}(n)$ be a finite symmetric group of degree n and let F be a perfect field of characteristic $p > 0$. We use $Z = Z(F\mathcal{S}(n))$ to denote the centre of the group algebra $F\mathcal{S}(n)$. If $\mathcal{X}$ is a subset of $\mathcal{S}(n)$ then $\mathcal{X}^+$ denotes its sum in $F\mathcal{S}(n)$. As is well known $\{\mathcal{K}^+ \mid \mathcal{K} \text{ a conjugacy class of } \mathcal{S}(n)\}$ forms an F-basis for Z. We use $Z_{p'}$ to denote the F-subspace of Z spanned by the p-regular class sums. The map $z \to z^p$ is a semi-linear transformation on Z, with respect to the automorphism $\lambda \to \lambda^p$ of F. Its image Z^p is an F-subalgebra of Z, and its kernel $\{z \in Z \mid z^p = 0\}$ is an ideal of Z. Our main result is:

Theorem 1. *Let $p = 2$. Then $Z^2 = Z_{2'}$. So $z \in Z$ is a square in Z if and only if z is an F-linear combination of 2-regular class sums.*

A p-block of $\mathcal{S}(n)$ is an indecomposable F-algebra, which is a direct summand of $F\mathcal{S}(n)$. Each p-block B of $\mathcal{S}(n)$ has an associated *weight* w and *p-core* α. So w is an integer between 0 and n/p, while α is a partition of $n - wp$ which has no *p-hooks*. See [JK81, 2.7 and 6.1] for definitions and proofs. The number $k(B)$ of irreducible characters associated to B equals the F-dimension of the centre $Z(B)$ of B, while the number $l(B)$ of irreducible Brauer characters equals the F-dimension of $Z_{2'} \cap Z(B)$. Set $Z(B)^2 = \{z^2 \mid z \in Z(B)\}$. The following is a block version of Theorem 1:

Theorem 2. *Let B be a 2-block of $\mathcal{S}(n)$, of weight w. Then $\dim(Z(B)^2)$ equals the number $P(w)$ of partitions of w.*

Proof. We have $Z(B)^2 = Z^2 \cap Z(B)$, since $Z(B)$ is commutative and unital. So $Z(B)^2 = Z_{2'} \cap Z(B)$, by Theorem 1. But $\dim(Z_{2'} \cap Z(B)) = l(B) = P(w)$, by [O80, 3.6]. This proves the result. □

Date: July 6, 2000.
1991 *Mathematics Subject Classification.* 20C20.
*the author was supported by an Enterprise Ireland research grant.

It seems unlikely that one could find an explicit formula for a square root of a 2-regular class sum (but see the proof of Proposition 9). We can at least show:

Theorem 3. *Each* 2*-regular class of* $\mathcal{S}(n)$ *occurs with odd multiplicity in the square of some involution class.*

In fact, for each 2-regular class of $\mathcal{S}(n)$, we can explicity describe a class of involutions for which this theorem holds. Our methods could be used to compute the square of any involution class sum of $\mathcal{S}(n)$.

For the rest of this paper we fix $g \in \mathcal{S}(n)$ and D a Sylow p-subgroup of $\mathbf{C}_{\mathcal{S}(n)}(g)$, and set $\mathrm{C} = \mathbf{C}_{\mathcal{S}(n)}(D)$. We use g_p ($g_{p'}$) to denote the p-part (p-regular part) of g. So g_p has p-power order, $g_{p'}$ has p'-order and $g = g_p g_{p'} = g_{p'} g_p$.

Our notation for subgroups, centralizers and normalizers is standard.

Proposition 4. $\mathrm{C} = \langle g_p \rangle \times N$, *for some group* N.

We defer the proof of Proposition 4 to the end of the paper, and proceed immediately to the proof of two corollaries. Corollary 6 will be needed in the proof of Theorem 1, while Corollary 5 may be of independent interest.

Let $a \in F\mathcal{S}(n)$ and $x \in \mathcal{S}(n)$. We use (a, x) to denote the coefficient of x in a. Set $\Omega(x) := \{y \in \mathcal{S}(n) \mid y^p = x\}$. If x has p'-order, we use $x^{1/p}$ to denote the unique element of $\Omega(x)$ that has p'-order.

Corollary 5. $Z_{p'}$ *is a subalgebra of* Z.

Proof. Let $\mathcal{K}$ and $\mathcal{L}$ be p-regular classes of $\mathcal{S}(n)$, and suppose that $g_p \neq 1_{\mathcal{S}(n)}$. It is enough to show that $(\mathcal{K}^+\mathcal{L}^+, g) = 0$. Note that $g \notin N$, where N is the normal subgroup of $\mathbf{C}_{\mathcal{S}(n)}(D)$ given by Proposition 4. Now

$$\begin{aligned}(\mathcal{K}^+\mathcal{L}^+, g) &= ((\mathrm{C} \cap \mathcal{K})^+(\mathrm{C} \cap \mathcal{L})^+, g), \\ &\qquad \text{using the Brauer homomorphism, see [K91, (54)],} \\ &= 0, \quad \text{as } N \text{ contains every 2-regular element of C.}\end{aligned}$$

The corollary follows. ☐

Let m be a nonnegative integer. The proof of Corollary 5 actually shows that the F-subspace of Z spanned by the class sums of elements of $\mathcal{S}(n)$ whose p-parts have order p^m or less is a subalgebra of Z.

Corollary 6. $Z^p \subseteq Z_{p'}$.

Proof. Let $\mathcal{K}$ be a conjugacy class of $\mathcal{S}(n)$, and suppose that $g_p \neq 1_{\mathcal{S}(n)}$. It is enough to show that $((\mathcal{K}^+)^p, g) = 0$. By [K91, (55)], we have

$$((\mathcal{K}^+)^p, g) = (\mathcal{K}^+\Omega(g_p)^+, g_{p'}^{1/p}).$$

Now, D acts by conjugation on $\mathcal{K}$ and $\Omega(g_p)$, and centralizes $g_{p'}^{1/p}$. Thus

$$((\mathcal{K}^+)^p, g) \;=\; ((\mathrm{C}\cap\mathcal{K})^+(\mathrm{C}\cap\Omega(g_p))^+, g_{p'}^{1/p}).$$

But Proposition 4 implies that $\mathrm{C}\cap\Omega(g_p)$ is empty. The result follows. □

Corollary 6 implies the following, cf. [K91, (59)]:

Proposition 7. $\{z \in Z \mid z^p = 0\} = \{z \in Z \mid z\Omega(1_{\mathcal{S}(n)})^+ = 0\}$.

The analogues of Corollaries 5 and 6 hold for the alternating group $\mathcal{A}(n)$ also.

Proposition 8. *$Z(F\mathcal{A}(n))_{p'}$ is a subalgebra of $Z(F\mathcal{A}(n))$ and $Z(F\mathcal{A}(n))^p \subseteq Z(F\mathcal{A}(n))_{p'}$.*

Proof. Suppose that g is an element of $\mathcal{A}(n)$. If $p \neq 2$, then D is a Sylow p-subgroup of $C \cap \mathcal{A}(n) = \mathbf{C}_{\mathcal{A}(n)}(g)$. In particular,

$$\mathbf{C}_{\mathcal{A}(n)}(D) = \langle g_p \rangle \times M, \quad \text{for some group } M,$$

using Proposition 4. Thus $Z(F\mathcal{A}(n))^p \subseteq Z(F\mathcal{A}(n))_{p'}$ and $Z(F\mathcal{A}(n))_{p'}$ is a subalgebra of $Z(F\mathcal{A}(n))$, exactly as in the proofs of Corollaries 5 and 6.

Suppose now that $p = 2$. Let $\mathcal{K}$ be a conjugacy class of $\mathcal{A}(n)$. Then either $\mathcal{K}$ is a conjugacy class of $\mathcal{S}(n)$, or the elements of $\mathcal{K}$ have cycle type α, where α is a partition of n into unequal odd parts (see [JK81, 1.2.10]). In the former case we have

$$(\mathcal{K}^+)^2 \in Z_{2'} \cap Z(F\mathcal{A}(n)) = Z(F\mathcal{A}(n))_{2'},$$

using Corollary 6. In the latter case $\mathcal{K}$ has 2-defect zero. It is a theorem of Brauer that the class sums of 2-defect zero classes span an ideal Z_0 of $Z(F\mathcal{A}(n))$. Since Z_0 is contained in $Z(F\mathcal{A}(n))_{2'}$, it follows that $(\mathcal{K}^+)^2 \in Z(F\mathcal{A}(n))_{2'}$ in this case also.

The proof that $Z(F\mathcal{A}(n))_{2'}$ is a subalgebra of $Z(F\mathcal{A}(n))$ proceeds in a similar fashion. □

Let $\mu = (\mu_1, \mu_2, \ldots, \mu_t)$ be a partition of n. So $\mu_1 + \cdots + \mu_t = n$ and $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_t > 0$. We use $|\mu| = t$ to denote the number of parts of μ. The conjugacy classes of $\mathcal{S}(n)$ are parametrized by the partitions of n. The class corresponding to μ contains $(1, \ldots, \mu_1)(\mu_1{+}1, \ldots, \mu_1{+}\mu_2) \ldots (n{-}\mu_t{+}1, \ldots, n)$. Clearly this class is p-regular if and only if μ_i is coprime to p, for $i = 1, \ldots, t$.

Let K be an arbitrary integral domain. In [M83], G. E. Murphy defines elements L_u in $K\mathcal{S}(n)$ by

$$L_u \;:=\; (1,u) \;+\; (2,u) \;+\; \cdots \;+\; (u-1,u),$$

where u is any integer between 2 and n, and each (v, u) is a transposition. For convenience, we set $L_1 := 1_{\mathcal{S}(n)}$.

Suppose that $1 \leq i < j < u$ or $u < i < j \leq n$. Then trivially $L_u\,(i, j) = (i, j)\,L_u$. In particular

$$L_u\,L_v = L_v\,L_u,$$

for all $u, v \in \{1, \ldots, n\}$. Also for $1 \leq u < n$, it can be shown that

$$L_u\,L_{u+1}\,(u, u+1) = (u, u+1)\,L_u\,L_{u+1}, \quad \text{and}$$
$$(L_u\, +\, L_{u+1})\,(u, u+1) = (u, u+1)\,(L_u\, +\, L_{u+1}).$$

Now 1, $L_u\,L_{u+1}$ and $L_u + L_{u+1}$ generate, as an algebra, the ring of symmetric polynomials in L_u and L_{u+1} over any commutative ring. It follows that the transposition $(u, u+1)$ commutes with any symmetric polynomial in L_u and L_{u+1}. Since $\{(u, u+1) \mid 1 \leq u < n\}$ generate $\mathcal{S}(n)$, we conclude that any symmetric polynomial in $L_2, \ldots, L_n$ lies in the centre $Z(K\mathcal{S}(n))$ of $K\mathcal{S}(n)$.

Let $P(n, p)$ denote the number of partitions of n into parts which are congruent to 1 modulo p.

Proposition 9. $\dim(Z^p) \geq P(n, p)$.

Proof. Let $\mu = (\mu_1, \mu_2, \ldots)$ be a partition of n. Suppose that $\mu_i > 1$ for $i = 1, \ldots, r$. Set X^μ as the sum, in $K\mathcal{S}(n)$, of all distinct products of the form

$$(L_{u_1})^{\mu_1 - 1}(L_{u_2})^{\mu_2 - 1} \ldots (L_{u_r})^{\mu_r - 1},$$

where $u_1, u_2, \ldots, u_r$ runs over all sets of r elements from $2, 3, \ldots, n$. If all parts of μ are 1, then set $X^\mu := 1_{\mathcal{S}(n)}$.

The main result of [M83, 1.9] is that if g is an element of $\mathcal{S}(n)$ of cycle type μ, then the coefficient of g in X^μ is 1, while if $\lambda = (\lambda_1, \lambda_2, \ldots)$ is the cycle type of any element of $\mathcal{S}(n)$ which occurs in X^μ, then either $|\mu| < |\lambda|$ or $\mu \lhd \lambda$, where $\lhd$ is the dominance relation on partitions. Murphy uses these facts to show that $\{X^\mu \mid \mu \text{ a partition of } n\}$ forms a K-basis for $Z(K\mathcal{S}(n))$.

Now consider when $K = F$ is a field of characteristic p. Let μ be a partition of n with $\mu_i \equiv 1 \,(\mathrm{mod}\, p)$, for $i = 1, \ldots, |\mu|$. Set $\lambda_i = (\mu_i - 1)/p + 1$, for $i = 1, \ldots, |\mu|$. Let λ be the partition of n whose first $|\mu|$ parts are $\lambda_1, \ldots, \lambda_{|\mu|}$, and whose remaining parts equal 1. Using the fact that the L_u commute, and the binomial theorem modulo p, we see that

$$(X^\lambda)^p = X^\mu.$$

The proposition now follows from the linear independence of the X^μ. □

We now give the proof of our main theorem.

proof of Theorem 1. Clearly $P(n,2)$ equals the number of 2-regular classes of $\mathcal{S}(n)$. So Proposition 9 implies that $\dim(Z^2) \geq \dim(Z_{2'})$. But $Z^2 \subseteq Z_{2'}$, by Corollary 6. The theorem follows. □

A partition is called 2-*singular* if at least one of its parts is even.

Corollary 10. $\dim\{z \in Z \mid z^2 = 0\}$ *equals the number of* 2-*singular partitions of* n.

We need the following result on blocks of symmetric groups:

Proposition 11. *Let* B *be a* p*-block of* $\mathcal{S}(n)$*, of weight* w*. Then* $Z(B) \cong Z(B_0)$*, where* B_0 *is the principal* p*-block of* $\mathcal{S}(pw)$*.*

Proof. The principal p-block B_0 of $\mathcal{S}(pw)$ has empty core and weight w. M. Enguehard [E90] has shown that there exists a *perfect isometry* between any two p-blocks of finite symmetric groups that have the same weight. This implies, among other things, that the centres of B and B_0 are isomorphic. □

Let B be a p-block of $\mathcal{S}(n)$, let $J(B)$ denote the Jacobson radical of $Z(B)$, and let p^t denote the exponent of a defect group of B. Using Proposition 11, and (59) of [K91], we see that

$$z^{p^t} = 0, \qquad \text{for each } z \in J(B).$$

This can be sharpened to:

Theorem 12. *There exists* $z \in J(B)$ *with* $z^{p^{t-1}} \neq 0$*.*

First we need two lemmas.

Let G be a finite group. For each positive integer m, define

$$\begin{aligned} \Omega_m &:= \{x \in G \mid x^{p^m} = 1_G\} \\ \Lambda_m &:= \{x \in G \mid o(x) = p^m\} \;=\; \Omega_m \backslash \Omega_{m-1} \\ \Delta_m &:= \{x \in G \mid x_p \in \Lambda_m\}. \end{aligned}$$

Lemma 13. *Let* e *be an idempotent in* $Z(FG)$*. Then*

$$e\,\Lambda_m^+ \;=\; (e, 1_G)\,\Lambda_m^+ \;+\; (\textit{terms involving non } p\textit{-elements of } \Delta_m).$$

Proof. Let $x \in G$ have order p^m. It follows from a well-known result of Iizuka (see [K91, (61)]) that the support of $e\,\Lambda_m^+$ is contained in Δ_m. So it is enough to show that $(e\,\Lambda_m^+, x) = (e, 1_G)$. We have

$$\begin{aligned}(e\,\Lambda_m^+, x) &= (e\,\Omega_m^+, x) \;-\; (e\,\Omega_{m-1}^+, x)\\ &= (e^{p^t}, x^{p^t})^{p^{-t}} \;-\; (e^{p^{t-1}}, x^{p^{t-1}})^{p^{-t+1}}, \quad \text{by (55) of [K91]}\\ &= (e, 1_G)^{p^{-t}} \;-\; (e, x^{p^{t-1}})^{p^{-t+1}}\\ &= (e, 1_G), \quad \text{as } (e, 1_G) \in GF(p) \text{ and as } e \text{ is supported}\\ &\qquad\qquad \text{on the } p\text{-regular elements of } G.\end{aligned}$$

□

Lemma 14. *Let c be an m-cycle, where $m \geq 2$, and let t be a transposition that does not commute with c. Then tc is an $(m-1)$-cycle, an $(m+1)$-cycle, or a product of two commuting cycles whose combined length is m.*

Proof. This is a routine calculation. □

Proof of Theorem 12. Let e be the unique idempotent in $Z(B)$, and let ω denote the epimorphism $B \to F$ which has kernel $J(B)$. Using Proposition 11, we may assume that B is the principal p-block of $\mathcal{S}(n)$.

Let τ be the class of transpositions in $\mathcal{S}(n)$, and let m be a positive integer. We may write

$$\tau^+ e \;=\; i \;+\; j,$$

where $i = \omega(\tau^+)e \in GF(p)e$ and $j \in J(B)$. If m is a positive integer then

$$(\tau^+ e)^{p^m} \;=\; i^{p^m} \;+\; j^{p^m} \;=\; i \;+\; j^{p^m}.$$

So the proposition will follow if we show that $(\tau^+ e)^{p^{t-1}} \neq (\tau^+ e)^{p^t}$.

Let u be a (p^{t+1})-cycle in $\mathcal{S}(n)$. Then $u^{1/p}$ is also a (p^{t+1})-cycle. Using [K91, (55)], and the fact that $(\tau^+ e\,\Omega_m^+, u) \in GF(p)$, we see that

$$((\tau^+ e)^{p^m}, u) \;=\; (\tau^+ e\,\Omega_m^+, u).$$

It follows that

$$\begin{aligned}((\tau^+ e)^{p^t}, u) - ((\tau^+ e)^{p^{t-1}}, u) &= (\tau^+ e\,\Omega_t^+, u) - (\tau^+ e\,\Omega_{t-1}^+, u)\\ &= (\tau^+ e\,\Lambda_t^+, u).\end{aligned} \tag{15}$$

Let λ_t denote the class of p^t-cycles in $\mathcal{S}(n)$. Suppose that $t \in \tau$ and $x \in \Delta_m$ and $tx = u$. Then $x = tu$ contains a p^t-cycle in its cycle decomposition. So x is a p^t-cycle, using Lemma 14. It then follows from Lemma 13 that

$$(\tau^+ e\,\Lambda_t^+, u) \;=\; (e, 1)\,(\tau^+ \lambda_t^+, u). \tag{16}$$

A direct calculation shows that

$$|\{ (t,l) \in \tau \times \lambda_t \mid tl = u \}| = p^t - 1. \tag{17}$$

We conclude from (15), (16) and (17) that

$$((\tau^+ e)^{p^t}, u) - ((\tau^+ e)^{p^{t-1}}, u) = -(e,1).$$

But $(e,1) \neq 0_F$, by a theorem of Brauer. So $(\tau^+ e)^{p^{t-1}} \neq (\tau^+ e)^{p^t}$. This completes the proof. □

Let $J(Z)$ denote the Jacobson radical of Z, and let p^t denote the p-exponent of $\mathcal{S}(n)$. Suppose that $p = 2$. If $n = 4$ then $z^{p^{t-1}+1} = 0$, for all $z \in J(Z)$, while if $n = 6$, there exists $z \in J(Z)$ with $z^{p^t-1} \neq 0$. So Theorem 12 is best possible. On the other hand, the dihedral group D_8 of order 8 has 2-exponent 4, yet $z^2 = 0$ for each $z \in J(Z(FD_8))$. So Theorem 12 does not generalize to all finite groups.

Corollary 18. *Let $J(Z)$ denote the Jacobson radical of Z, and let p^t denote the p-exponent of $\mathcal{S}(n)$. Then $\dim_F(J(Z)^{p^{t-1}})$ is greater that or equal to the number of p-blocks of $\mathcal{S}(n)$ that have weight greater than or equal to p^{t-1}.*

Proof. Suppose that B is a p-block of $\mathcal{S}(n)$, of weight $w \geq p^{t-1}$. Now by [JK81, 6.2.39], a defect group D of B is isomorphic to a wreath product of a cyclic group of order p and a Sylow p-subgroup of a Symmetric group of degree w. But $w < p^t$. So the p-adic decomposition of w contains p^{t-1} with non-zero multiplicity. It follows that D has a direct factor isomorphic to a Sylow p-subgroup of $\mathcal{S}(p^t)$. Hence D has exponent p^t. The corollary now follows from Theorem 12. □

Theorem 19. *Let p be an odd prime. Then $Z^p \lneq Z_{p'}$.*

Proof. Let τ be the class of transpositions in $\mathcal{S}(n)$. So $\tau^+ \in Z_{p'}$. Suppose that there exists $z \in Z$ with $z^p = \tau^+$. Then $z^{p^t} = (\tau^+)^{p^{t-1}}$ lies in the $GF(p)$-span of the block idempotents of Z, using [K91, (59)]. So $(z^{p^t})^p = z^{p^t}$. However,

$$(z^{p^t})^p = (\tau^+)^{p^t} \neq (\tau^+)^{p^{t-1}} = z^{p^t},$$

by the proof of Theorem 12. This contradiction shows that no such z exists. □

proof of Theorem 3. Let g be a 2-regular element of $\mathcal{S}(n)$ and let t be an involution which inverts g. If X is a $\langle g \rangle$-orbit on $\{1, \ldots, n\}$, then so too is Xt. So either X is stabilized by $\langle t \rangle$, or t contains the $|X|$-transpositions $\{(x, xt) \mid x \in X\}$ in its cycle decomposition. Suppose that X is stabilized by $\langle t \rangle$. Then t fixes some point, say x_0, in X, since $|X|$ is odd and $\langle t \rangle$

is a 2-group. It follows from the fact that t inverts g that t contains the $(|X|-1)/2$-transpositions $\{(x_0g^j, x_0g^{|X|-j}) \mid j = 1, \dots (|X|-1)/2\}$ in its cycle decomposition.

Suppose that g has a_i orbits of size i, and that exactly b_i of these are stabilized by $\langle t\rangle$. Then the number of transpositions in t is

$$\sum b_i \frac{(i-1)}{2} + \frac{(a_i - b_i)}{2} i \; = \; \sum \frac{a_i i - b_i}{2}. \tag{20}$$

Moreover,

$$\sum (a_i i - b_i)/2 \; \leq \; \sum a_i(i-1)/2, \tag{21}$$

with equality if and only if $b_i = a_i$, for all i.

Given a set $\mathcal{X}$ of representatives for the orbits of $\langle g\rangle$ on $\{1, \dots, n\}$, there is a unique involution s which inverts g and centralizes all members of $\mathcal{X}$. Let $\mathcal{T}$ be the conjugacy class of $\mathcal{S}(n)$ which contains s, and suppose that $t \in \mathcal{T}$ inverts g. By (20), the cycle decomposition of s, and hence t, consists of $\sum_i a_i(i-1)/2$ transpositions. But then (21) implies that t fixes an element from each $\langle g\rangle$-orbit. We deduce that

$$|\{t \in \mathcal{T} \mid g^t = g^{-1}\}| \; := \; \prod i^{a_i}$$

equals the number of sets of representatives for the orbits of $\langle g\rangle$ on $\{1, \dots, n\}$. A standard argument gives

$$((\mathcal{T}^+)^2, g) \; = \; |\{t \in \mathcal{T} \mid g^t = g^{-1}\}|\, 1_F.$$

The theorem now follows from the fact that $\prod i^{a_i}$ is odd. □

It remains to prove Proposition 4. First we need some notation for subgroups of $\mathcal{S}(n)$. Much of this is taken from [R93, 1.6].

Let X and Y be finite sets. We use $\mathcal{S}(X)$ to denote the group of all permutations of X. By convention all permutations act on the right. Let H be a subgroup of $\mathcal{S}(X)$. If $h \in H$ and $y_0 \in Y$, we can define a permutation $h(y_0)$ of $X \times Y$ via

$$(x,y)h(y_0) := \begin{cases} (xh, y), & \text{if } y = y_0, \\ (x,y), & \text{if } y \neq y_0, \end{cases} \qquad \text{for all } (x,y) \in X \times Y.$$

The map $h \to h(y_0)$ gives an injection $H \hookrightarrow \mathcal{S}(X \times Y)$, whose image we denote by $H(y_0)$. We let H^Y denote the group generated by $\{H(y_0) \mid y_0 \in Y\}$. So H^Y isomorphic to the external direct product of $|Y|$ copies of H.

Suppose that we have a collection of disjoint finite sets $\{X_y \mid y \in Y\}$ and groups $\{H_y \leq \mathcal{S}(X_y) \mid y \in Y\}$, indexed by the elements of Y. Then $\prod_{y \in Y} H_y$

denotes the group generated by $\{H_y(y) \mid y \in Y\}$. So $\prod_{y\in Y} H_y$ is an embedding of the external direct product of the groups H_y in $\mathcal{S}(\cup_y X_y)$.

Let K be a subgroup of $\mathcal{S}(Y)$. For $k \in K$, we can define a permutation k^* of $X \times Y$ via

$$(x,y)k^* := (x, yk), \quad \text{for all } (x,y) \in X \times Y.$$

The map $k \to k^*$ gives an injection $K \hookrightarrow \mathcal{S}(X \times Y)$, whose image we denote by $\Delta(K,X)$ (and $\Delta(K,n)$, if $|X| = n$). In particular, $\Delta(K,X) \cong K$.

The *wreath product* $H \wr K$ of H with K is the subgroup of $\mathcal{S}(X \times Y)$ generated by H^Y and $\Delta(K,X)$. A quick calculation shows that $h(y_0)^{k^*} = h(y_0 k)$, for each $y_0 \in Y$, $h \in H$ and $k \in K$. It follows that H^Y is a normal subgroup of $H \wr K$. We call H^Y the *base group* of $H \wr K$. Also $H^Y \cap \Delta(K,X) = \{1\}$. So $H \wr K$ is isomorphic to a semi-direct product of H^Y with K.

If m is a positive integer, we will use Z_m to denote the cyclic subgroup of $\mathcal{S}(m)$ generated by an m-cycle. The following is crucial to be proof of Proposition 4:

Proposition 22. *Let m and n be positive integers with h.c.f.$(m,n) = 1$. Then $Z_m \wr \mathcal{S}(n) = \Delta(Z_m, n) \times N$, for some group N.*

Proof. Let h be a generator of Z_m. A typical element of $Z_m \wr \mathcal{S}(n)$ is of the form $\prod_{i=1}^n h(i)^{\alpha_i}\sigma^*$, with $\sigma \in \mathcal{S}(n)$, and $0 \le \alpha_i \le m-1$, for $i = 1, \ldots, n$. Define $\theta : Z_m \wr \mathcal{S}(n) \to Z_m$, by

$$\theta(\prod_{i=1}^n h(i)^{\alpha_i}\sigma^*) \;=\; \prod_{i=1}^n h^{\alpha_i}.$$

Then θ is a group homomorphism, since $h(i)^{\sigma^*} = h(i\sigma)$, for $i = 1, \ldots, n$, and $\sigma \in \mathcal{S}(n)$.

Consider the generator $\delta := \prod_{i=1}^n h(i)$ of $\Delta(Z_m, n)$. Since h.c.f.$(m,n) = 1$, it follows that $\theta(\delta) = h^n$ is a generator of Z_m. So θ is onto, and $\ker(\theta) \cap \Delta(Z_m,n) = \{1\}$. But $\Delta(Z_m,n)$ is central in $Z_m \wr \mathcal{S}(n)$. We conclude that

$$Z_m \wr \mathcal{S}(n) \;=\; \Delta(Z_m,n) \times N, \quad \text{where } N = \ker(\theta).$$

□

Let

$$\mathrm{Fix}(H) \;:=\; \{x \in X \mid xh = x, \text{ for all } h \in H\},$$
$$\mathrm{Mov}(H) \;:=\; \{x \in X \mid xh \neq x, \text{ for some } h \in H\}.$$

Lemma 23. $\mathbf{C}_{\mathcal{S}(X)}(H) = \mathbf{C}_{\mathcal{S}(\mathrm{Mov}(H))}(H) \times \mathcal{S}(\mathrm{Fix}(H))$. *If* $\mathrm{Fix}(H) = \phi$ *then* $\mathbf{C}_{\mathcal{S}(X \times Y)}(H^Y) = \mathbf{C}_{\mathcal{S}(X)}(H)^Y$.

Proof. Both statements are obvious. □

Lemma 24. *Suppose that K acts transitively on Y. Then*

$$\mathbf{C}_{\mathcal{S}(X\times Y)}(\Delta(K,X)) = \mathbf{C}_{\mathcal{S}(Y)}(K) \wr \mathcal{S}(X).$$

Proof. It is clear that $\mathbf{C}_{\mathcal{S}(Y)}(K) \wr \mathcal{S}(X) \subseteq \mathbf{C}_{\mathcal{S}(X\times Y)}(\Delta(K,X))$.

For each $x \in X$, the set $x \times Y := \{(x,y) \mid y \in Y\}$ is a $\Delta(K,X)$-orbit on $X \times Y$. Moreover, each $\Delta(K,X)$-orbit equals $x \times Y$, for some $x \in X$.

Let $x \in X$ and $\sigma \in \mathbf{C}_{\mathcal{S}(X\times Y)}(\Delta(K,X))$. The previous paragraph implies that $(x \times Y)\sigma = x\sigma_1 \times Y$, for some $\sigma_1 \in \mathcal{S}(X)$. So for $y \in Y$ we have

$$(x,y)\sigma = (x\sigma_1, y\sigma_x),$$

where $\sigma_x \in \mathcal{S}(Y)$ depends on x. An easy calculation shows that $\sigma_x \in \mathbf{C}_{\mathcal{S}(Y)}(K)$. So $\sigma = \sigma_1^* \prod_{x\in X} \sigma_x$ lies in $\mathbf{C}_{\mathcal{S}(Y)}(K) \wr \mathcal{S}(X)$. The lemma follows. □

Corollary 25. *Suppose that H fixes no element of X and that K acts transitively on Y. Then $\mathbf{C}_{\mathcal{S}(X\times Y)}(H \wr K) = \Delta(\mathbf{C}_{\mathcal{S}(X)}(H), Y)$.*

Proof. We have

$$\begin{aligned}
\mathbf{C}_{\mathcal{S}(X\times Y)}(H \wr K) &= \mathbf{C}_{\mathcal{S}(X\times Y)}(H^Y) \cap \mathbf{C}_{\mathcal{S}(X\times Y)}(\Delta(K,X)), \\
&\qquad \text{using the definition of wreath product,} \\
&= \mathbf{C}_{\mathcal{S}(X)}(H)^Y \cap \mathbf{C}_Y(K) \wr \mathcal{S}(X), \quad \text{by Lemmas 23 and 24,} \\
&= \langle c(y_0) \mid c \in \mathbf{C}_{\mathcal{S}(X)}(H), y_0 \in Y \rangle \cap \Delta(\mathcal{S}(X), Y) \\
&= \Delta(\mathbf{C}_{\mathcal{S}(X)}(H), Y).
\end{aligned}$$

□

Recall that g is an element of $\mathcal{S}(n)$ and that D is a Sylow p-subgroup of $\mathrm{C} = C_{\mathcal{S}(n)}(g)$. We use the above results to compute $\mathbf{C}_{\mathcal{S}(n)}(D)$. Suppose that g has a_i cycles of length i in its cycle decomposition, for $i = 1, 2, \ldots, n$.

Lemma 26. $\mathrm{C} \cong \prod_{i=1}^{n} Z_i \wr \mathcal{S}(a_i)$.

Proof. This is 4.1.19 of [JK81]. □

If n is an integer, write n_p for the p-part of n and $n_{p'}$ for the p-regular part of n. So $n = n_p n_{p'}$, and n_p is a power of p, while $n_{p'}$ is coprime to p. Let $a_i = \sum b_{ij} p^j$ be the base p-expansion of a_i, and let $P(a_i)$ be a Sylow p-subgroup of $\mathcal{S}(a_i)$. It is know that

$$P(a_i) \cong \prod P(p^j)^{b_{ij}}, \tag{27}$$

where $P(p^j)$ is a Sylow p-subgroup of $\mathcal{S}(p^j)$. Here we restrict j to those values for which $b_{ij} \neq 0$. Also $P(p^j)$ is a transitive subgroup of $\mathcal{S}(p^j)$, and the centre $\mathbf{Z}(P(p^j))$ of $P(p^j)$ coincides with $\mathbf{C}_{\mathcal{S}(p^j)}(P(p^j))$.

See (9) in [O86] for another version of the following lemma:

Lemma 28. $D \cong \prod_{i_p \neq 1} \prod_j (\Delta(Z_{i_p}, i_{p'}) \wr P(p^j))^{b_{ij}} \times \prod_{i_p=1} \Delta(P(a_i), i)$.

Proof. This follows from Lemma 26, (27), and the definition of the wreath product. Note that $\Delta(Z_{i_p}, i_{p'})$ is a Sylow p-subgroup of Z_i. □

Proposition 29.

$$\begin{aligned}\mathbf{C}_{\mathcal{S}(n)}(D) \cong & \prod_{i_p \neq 1} \prod_j \Delta(Z_{i_p} \wr \mathcal{S}(i_{p'}), p^j)^{b_{ij}} \\ & \times \prod_{i_p=1} \prod_{j>0} (\mathbf{Z}(P(p^j)) \wr \mathcal{S}(i))^{b_{ij}} \times \mathcal{S}(\sum_{i_p=1} i b_{i0}).\end{aligned}$$

Proof. Suppose that $1 \leq i \leq n$ and $i_p \neq 1$. Then

$$\begin{aligned}\mathbf{C}_{\mathcal{S}(ip^j)}(\Delta(Z_{i_p}, i_{p'}) \wr P(p^j)) &= \Delta(\mathbf{C}_{\mathcal{S}(i)}(\Delta(Z_{i_p}, i_{p'})), p^j), \quad \text{by Corollary 25} \\ &= \Delta(\mathbf{C}_{\mathcal{S}(i_p)}(Z_{i_p}) \wr \mathcal{S}(i_{p'}), p^j), \quad \text{by Lemma 24} \\ &= \Delta(Z_{i_p} \wr \mathcal{S}(i_{p'}), p^j).\end{aligned}$$

If $i_p = 1$, we have $\Delta(P(a_i), i) = \{1_{\mathcal{S}(ib_{i0})}\} \times \prod_{j>0} \Delta(P(p^j), i)^{b_{ij}}$, and $\Delta(P(p^j), i)$ has no fixed points for $j > 0$. Also

$$\begin{aligned}\mathbf{C}_{\mathcal{S}(ip^j)}(\Delta(P(p^j), i)) &= \mathbf{C}_{\mathcal{S}(p^j)}(P(p^j)) \wr \mathcal{S}(i), \quad \text{by Lemma 24} \\ &= \mathbf{Z}(P(p^j)) \wr \mathcal{S}(i).\end{aligned}$$

The proposition now follows from repeated applications of Lemma 23. □

proof of Proposition 4. It follows from Propositions 22 and 29 that

$$\mathbf{C}_{\mathcal{S}(n)}(D) = \prod_{i_p \neq 1} \prod_j \Delta(Z_{i_p}, i_{p'} p^j)^{b_{ij}} \times M$$

for some subgroup M of $\mathcal{S}(n)$. Also, the projection of g_p onto each factor $\Delta(Z_{i_p}, i_{p'} p^j)$ generates that factor. The proposition now follows from standard properties of finite abelian groups. □

1. Acknowledgement

I am most grateful to Gordan James for pointing out how [M83, 1.9] might be used to prove Proposition 9.

References

[E90] M. Enguehard, *Isométries parfaites entre blocs de groupes symétriques*, S.M.F. Astérisque Vol. 181–182 (1990), p157–171.

[JK81] G. James, A. Kerber, *The representation theory of the symmetric group,* Encycl. of Math. and Applic. 16, Addison-Wesley Publ. Co., London, 1981.

[K91] B. Külshammer, *Group-theoretical descriptions of ring-theoretical invariants of group algebras*, Progress in Math. 95 (1991), 425-442.

[M83] G. E. Murphy, *The Idempotents of the Symmetric Group and Nakayama's Conjecture*, J. Algebra 81 (1983), 258–265.

[O80] J. B. Olsson, *Lower Defect Groups*, Comm. Alg. 8, No. 3 (1980), 261-288.

[O86] J. B. Olsson, *Lower Defect Groups in Symmetric Groups*, J. Algebra 104, 37–56 (1986).

[R93] D. J. S. Robinson, *A course in the theory of groups,* Graduate Texts in Math. 80, Springer-Verlag, New York, 1993.

E-mail address: jcmurray@eircom.net