GENERATORS FOR THE CENTRE OF THE GROUP ALGEBRA
OF A SYMMETRIC GROUP

JOHN MURRAY

Abstract. The ring of symmetric functions is used to obtain an explicit set of
generators for the centre of the integral group algebra of a symmetric group,
different to those given by H. K. Farahat and G. Higman. This generating set
is used to show that the centre of the 2-modular group algebra is generated
by certain sums of 2-classes.

Proper subalgebras of the centre of the 2-modular group algebra are studied
in the context of symmetric functions. These include the algebra that is the
span of the 2-regular class sums, and the algebra that is generated by the
involution class sums. Various related subalgebras of the modular ring of
symmetric functions are shown to be polynomial algebras, and furnished with
explicit sets of algebraically independent generators.

1. Introduction

Let $S_n$ be the symmetric group on $n$ symbols. H. K. Farahat and G. Higman [FH]
exhibited a set of generators for the centre $Z(ZS_n)$ of the integral group ring $ZS_n$,
and introduced an infinite dimensional filtered algebra whose structure constants
are integer valued rational functions. A. -A. A. Jucys [J] used their methods to
show that $Z(ZS_n)$ coincides with the ring $A_{n-1}$ of integer symmetric polynomials
in certain elements of $ZS_n$. A different, and independent, proof of the same result
was given by G. E. Murphy in [Mpy]. We will refer to these generating elements
(whose definition is recalled in (6.1) below) as the JM-elements of $ZS_n$. Murphy’s
proof shows that the $Q$-algebra generated by the JM-elements coincides with the $Q$-
span of a complete set of primitive idempotents for $QS_n$. Theorem 1.9 in [Mpy] also
furnishes $Z(ZS_n)$ with an explicit $Z$-basis involving monomial symmetric functions
in the JM-elements.

The Farahat-Higman generators are the elementary symmetric polynomials in
the JM-elements. As Jucys himself mentioned, any other set of generators for the
algebra of integral symmetric functions gives a corresponding set of generators for
$Z(ZS_n)$. In this paper we give an explicit generating set that is related to the
complete symmetric polynomials.

Let $F$ be a field of characteristic 2. By an $n$-class we mean a conjugacy class
whose elements have $n$-power order, for $n \geq 1$. Using our generating set, we prove
in Theorem 3.8 that the centre $Z(FS_n)$ of the group algebra $FS_n$ is generated by
the 2-class sums of $S_n$. Theorem 4.6 gives a method of finding an explicit set of 2-
class sums that generate $Z(FS_n)$. The only involution classes that occur in this set
are products of powers of 2 commuting transpositions. The modular representation

Date: Submitted - January 15, 2002,
1991 Mathematics Subject Classification. 05E05, 20C05, 20C30.
theory of $S_n$ shows that no set of $p$-class sums can generate the centre of the group algebra of $S_n$ over a field of odd characteristic $p > 0$.

It is noteworthy that both the Farahat and Higman paper, and the Murphy paper, include proofs of the so-called Nakayama Conjecture that gives a combinatorial classification of the $p$-blocks of $S_n$. Our results have some consequences for the $2$-blocks of $S_n$. Specifically, we show in Section 5 that each 2-block idempotent can be expressed as a polynomial, with coefficients in $F$, in the involution class sums of $S_n$.

The latter part of the paper is concerned with various proper subalgebras of $Z(FS_n)$. The author showed in [M] that, for each each $N > 0$, the span of the class sums of elements of $S_n$ whose order is not divisible by $2^N$ forms a subalgebra of $Z(FS_n)$. When $N = 1$, we obtain an algebra spanned by the sums of those conjugacy classes containing elements of odd order. We give explicit generators for this algebra in Section 7. There is a related subalgebra of the modular ring of symmetric functions, $\Lambda \otimes F$, which we call the 2-regular class symbol algebra (an element in a group is said to be 2-regular if it has odd order). We show that this algebra is a polynomial algebra, and furnish it with an explicit set of algebraically independent generators.

There has been some interest in recent times in representing the operation of multiplication by the sum of all transpositions, by means of differential operators acting on symmetric functions. See [LT], for instance. Here we are interested in all involution classes of $S_n$. In Section 8, we define and study the involution class symbol algebra. This is a subalgebra of $\Lambda \otimes F$ that is related to the algebra generated by all involution class sums. In Theorem 8.9 we exhibit an algebraically independent subset of the involution class symbol algebra. We suspect, but cannot yet prove, that this set actually generates the algebra.

The final section of the paper is devoted to showing that the 2-regular class symbol algebra and the involution class symbol algebra together generate a polynomial subalgebra of $\Lambda \otimes F$. This algebra is the span of the symmetric functions defined in (9.6). Although this is a theorem about the 2-modular ring of symmetric functions, we suspect that the corresponding conjugacy class sums span a subalgebra of $Z(FS_n)$. Indeed, a central theme of this paper is that there is a closer than expected correspondence between the 2-modular ring of symmetric functions and the centre of the 2-modular group algebra of a symmetric group.

2. THE CLASS SYMBOL ALGEBRA

Throughout this paper, $n$ denotes an arbitrary positive integer, and $F$ denotes a field of characteristic $2$.

Let $S_\infty$ be the group of finitary permutations on $\mathbb{N} = \{1, 2, \ldots\}$ i.e. the group of bijections on the set of positive integers that fix all but a finite number of integers. We regard $S_n$ as the set of permutations in $S_\infty$ that fix $\{n+1, n+2, \ldots\}$ elementwise. So $S_1 \leq S_2 \leq \ldots$, and $S_\infty = \bigcup_{n=1}^{\infty} S_n$.

We employ the notation and methods of I. G. Macdonald [Mac]. A partition is a nonincreasing sequence $\lambda = [\lambda_1 \geq \lambda_2 \geq \ldots]$ of nonnegative integers whose sum $|\lambda| = \lambda_1 + \lambda_2 + \ldots$ is finite. Call $\lambda$ a partition of $n$, and write $\lambda + n$, if $|\lambda| = n$. The nonzero terms of $\lambda_1, \lambda_2, \ldots$ are called the parts of $\lambda$. Let $a_i$ be the number of parts of $\lambda$ that equal $i$, for $i \geq 1$. The multi-index notation $\lambda = [i^{a_1}, j^{a_2}, \ldots]$, where $i$ is omitted if $a_i = 0$, will be employed throughout. We use $l(\lambda)$ to denote the number
of parts of \( \lambda \). The number of ways of arranging the parts of \( \lambda \) is

\[
u_{\lambda} = \frac{l(\lambda)!}{\prod_i n_i!}.
\]

Two elements of \( S_\infty \) are conjugate if and only if they are conjugate in any subgroup \( S_n \) that contains them both. The conjugacy classes of \( S_n \) and of \( S_\infty \) are labelled by partitions, but in different ways. If \( \lambda \) is a partition of \( n \), we let \( K(\lambda) \) be the conjugacy class of \( S_n \) whose elements have cycle type \( \lambda \). The modified cycle type of the elements of \( K(\lambda) \) is the partition \( \mu = [\lambda_1 - 1, \ldots, \lambda_{l(\lambda)} - 1, 0, \ldots] \). If \( \sigma \in S_n \), the cycle type of \( \sigma \) depends on \( n \), whereas the modified cycle type of \( \sigma \) does not. We let \( c_\mu \) denote the set of elements of \( S_\infty \) that have modified cycle type \( \mu \). Then \( c_\mu \) is a conjugacy class of \( S_\infty \), and each conjugacy class of \( S_\infty \) arises in this way. In particular, the identity permutation belongs to \( c_{[]} \), where \([\ ]\) is the empty partition. For \( m \geq 1 \), set \( c_\mu(m) := c_\mu \cap S_m \). Then \( c_\mu(n) = K(\lambda) \), while \( c_\mu(m) \) is the empty set, if \( |\mu| + l(\mu) > m \).

We identify \( K(\lambda) \) or \( c_\mu(n) \) with the sum of the elements of the corresponding class of \( S_n \) in \( Z(ZS_n) \). The empty sum is, by fiat, zero. For partitions \( \mu \) and \( \nu \) we have

\[
c_\mu(n) c_\nu(n) = \sum_\rho \alpha_{\mu\nu}^\rho c_\rho(n),
\]

where \( \rho \) ranges over all partitions and \( \alpha_{\mu\nu}^\rho \) are integers that depend on \( n \). Farahat and Higman [FH] have shown that the integer \( \alpha_{\mu\nu}^\rho \) is zero if \( |\rho| > |\mu| + |\nu| \), is independent of \( n \), if \( |\rho| = |\mu| + |\nu| \), and is a rational function of \( n \), if \( |\rho| < |\mu| + |\nu| \).

A \( Z \)-order is a \( Z \)-algebra that is free as \( Z \)-module. The Macdonald class symbol algebra \( G \) is the \( Z \)-order that is freely generated by the \( S_\infty \)-class symbols \( \{c_\mu\} \), where the multiplication is induced from

\[
c_\mu c_\nu = \sum_{|\rho| = |\mu| + |\nu|} \alpha_{\mu\nu}^\rho c_\rho.
\]

A typical element of \( G \) has the form \( g = \sum_\mu \alpha_\mu c_\mu \), where \( \mu \) ranges over a finite set of partitions, and each \( \alpha_\mu \) is an integer. We use \( g(n) \) to denote the element \( \sum \alpha_\mu c_\mu(n) \) of \( Z(ZS_n) \). For \( i \leq n \), let \( Z(ZS_n)_i \) be the \( Z \)-submodule of \( Z(ZS_n) \) that is spanned by those nonzero \( c_\lambda(n) \) with \( |\lambda| < i \).

**Lemma 2.2.** Suppose that \( g_1, g_2, \ldots \) are elements of \( G \) that generate \( G \) as a \( Z \)-order. Then the non-zero \( g_1(n), g_2(n), \ldots \) generate \( Z(ZS_n) \) as a \( Z \)-algebra.

**Proof.** It is enough to show that \( c_\lambda(n) \in Z[g_1(n), g_2(n), \ldots] \) for each partition \( \lambda \). We prove this using induction on \( i = |\lambda| \). If \( i = 0 \), then \( \lambda \) is the empty partition and \( c_\lambda(n) = 1 \). Suppose then that \( i > 0 \) and that \( c_\mu(n) \in Z[g_1(n), g_2(n), \ldots] \), whenever \( \mu \) is a partition with \( |\mu| < i \). By hypothesis there exists \( f \in Z[x_1, x_2, \ldots] \) such that \( f(g_1, g_2, \ldots) = c_\lambda \). An inductive argument using (2.1) shows that

\[
f(g_1(n), g_2(n), \ldots) \equiv c_\lambda(n) \pmod{Z(ZS_n)_i}.
\]

The lemma now follows from the inductive hypothesis. \( \square \)

I. G. Macdonald has shown that \( G \) is isomorphic to a polynomial ring in a countable number of variables. Specifically, let \( \Lambda \) be the ring of symmetric functions in the variables \( x_1, x_2, \ldots \) over \( Z \). Then there exists a \( Z \)-basis \( \{g_\lambda\} \) for \( \Lambda \) such that the map \( \phi : \Lambda \to G \), defined by \( \phi(g_\lambda) = c_\lambda \), is a ring isomorphism. Let \( e_n \in \Lambda \) denote the \( n \)-th elementary symmetric function. Then \( e_1, e_2, \ldots \) are algebraically
independent over \( \mathbb{Z} \), and \( \Lambda = \mathbb{Z}[e_1, e_2, \ldots] \). From now on we will not distinguish between \( G \) and \( \Lambda \), and we identify \( c_\lambda \) with the symmetric function \( g_\lambda \).

If \( \lambda \) is a partition, let \( m_\lambda \) denote the monomial symmetric function of type \( \lambda \). The \( n \)-th complete symmetric function \( h_n \) is \( \sum_{\lambda \vdash n} m_\lambda \). The symmetric functions \( h_1, h_2, \ldots \) are algebraically independent and \( \Lambda = \mathbb{Z}[h_1, h_2, \ldots] \). Indeed, the map \( \tau \) that interchanges \( e_i \) and \( h_i \), for \( i \geq 1 \), is an involutory automorphism of \( \Lambda \). For each partition \( \lambda \), set \( h_\lambda := \prod_{i\geq 0} h_\lambda \). The generating function \( H(x) = \sum_{n\geq 0} h_n x^n \) is given (somewhat informally) by the following infinite product of power series:

\[
H(x) = \prod_{n \geq 1} \left(1 - x_n x\right)^{-1}.
\]

The power sum symmetric functions are defined as follows. Set \( p_n := m_{[n]} \), and for each partition \( \lambda \), define \( p_\lambda := \prod p_\lambda \). Then the \( p_n \) are algebraically independent, and \( \{ p_\lambda \} \) forms a basis for \( \Lambda \otimes \mathbb{Q} \) (but not for \( \Lambda \). The power series \( P(x) = \sum p_n x^{n-1} \) satisfies the equation \( P(x) = H'(x)/H(x) \) (see [Mac]). In particular,

\[
n h_n = \sum_{i=1}^{n} p_i h_{n-i}.
\]

Let \( <,> \) denote the nondegenerate symmetric bilinear form on \( \Lambda \) such that

\[
< h_\lambda, m_\mu > = \delta_{\lambda \mu}
\]

for all partitions \( \lambda \) and \( \mu \). Let \( f_\lambda \) denote the symmetric function that is \( <,> \)-dual to \( c_\lambda \). The \( f_\lambda \) are sometimes called the forgotten symmetric functions. Since \( \tau(c_\lambda) = h_\lambda \), and it is known that \( <,> \) is \( \tau \)-invariant, we have \( \tau(f_\lambda) = m_\lambda \).

The following theorem [Mac, I.2.24], which we restate here for the convenience of the reader, characterizes the \( c_\lambda \):

**Theorem 2.3.** Let \( \{ h_\lambda \} \) be the \( \mathbb{Z} \)-basis of \( \Lambda \) that is \( <,> \)-dual to \( \{ c_\lambda \} \). Set \( \mu_\lambda := h_{\mu(\lambda)} \) for \( n \geq 1 \). Then the map \( h_n \mapsto \mu_n \) induces a \( \mathbb{Z} \)-algebra involutory automorphism of \( \Lambda \). In particular \( \mu_n = \prod h_{\lambda_n} \), for each partition \( \lambda \). Let \( H^*(x) = \sum_{n \geq 0} h_n x^n \) be the generating function for the \( \mu_n \). Then \( H^*(x) \) is the Lagrange inverse of \( H(x) \) i.e. if \( y := xH^*(x) \), then \( x = yH(y) \).

If \( \{ \alpha_\lambda \} \) and \( \{ \beta_\lambda \} \) are \( \mathbb{Z} \)-bases of \( \Lambda \), indexed by partitions, we let \( M(\alpha, \beta) \) denote the change of basis matrix from \( \{ \alpha_\lambda \} \) to \( \{ \beta_\lambda \} \) i.e.

\[
\alpha_\lambda = \sum_{\mu} M(\alpha, \beta)_\lambda, \mu \beta_\mu.
\]

Note that \( M(\beta, \alpha) = M(\alpha, \beta)^{-1} \). Also if \( \{ \alpha'_\lambda \} \) and \( \{ \beta'_\lambda \} \) are the \( <,> \)-dual bases to \( \{ \alpha_\lambda \} \) and \( \{ \beta_\lambda \} \), and \( \dagger \) denotes matrix transposition, then

\[
M(\alpha', \beta') = M(\beta, \alpha)^\dagger,
\]

If \( n \geq 1 \), we use \( \mathcal{L}(n) \) to denote the number of digits that equal 1 in the binary expansion of \( n \). So \( n \) is a sum of \( \mathcal{L}(n) \) distinct nonnegative powers of 2. We use \( \nu(n) \) to denote the highest power of 2 that divides \( n \). Note that \( \mathcal{L}(2n) = \mathcal{L}(n) \) and that \( \nu(n!) = n - \mathcal{L}(n) \).
3. Generators for the class symbol algebra

Catalan numbers appear frequently in the combinatorics of symmetric functions. The \( n \)-th Catalan number \( C_n \) is the integer

\[
C_n := \frac{1}{n+1} \binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1}.
\]

**Lemma 3.1.** \( C_n \) is odd if and only if \( n+1 \) is a power of 2.

**Proof.** This follows from

\[
\nu(C_n) = \nu((2n)!) - \nu((n+1)!) - \nu(n!)
= (2n - \mathcal{L}(2n)) - (n + 1 - \mathcal{L}(n+1)) - (n - \mathcal{L}(n))
= \mathcal{L}(n+1) - 1.
\]

\[\square\]

For each partition \( \lambda \), set

\[
C_\lambda := \prod_i C_{\lambda_i}.
\]

Our interest in the \( C_\lambda \) arises from:

**Proposition 3.2.**

\[
e_n = (-1)^n \sum_{\lambda \vdash n} C_\lambda c_\lambda,
\]
\[
h_n = (-1)^n \sum_{\lambda \vdash n} c_\lambda.
\]

**Proof.** Let \( \lambda \) be a partition of \( n \). Since \( e_n = m_{[n^*]} \), we have

\[
M(e, c)_{[n], \lambda} = M(m, c)_{[n], \lambda} = M(h^*, h)_{\lambda, [n^*]}, \text{ using (2.4)}
= \prod_i M(h^*, h)_{[\lambda_i], [n^*]}
\]

Macdonald has shown in [Mac, I.2.24] that

\[
h_n^* = \sum_{\lambda \vdash n} \frac{(-1)^{l(\lambda)}}{n+1} \binom{n + l(\lambda)}{n} u_\lambda h_\lambda.
\]

So

\[
(3.4) \quad M(h^*, h)_{[n], [n^*]} = \frac{(-1)^n}{n+1} \binom{n + n}{n} u_{[n^*]} = (-1)^n C_n.
\]

The identity for \( e_n \) follows from (3.3) and (3.4).

Since \( \tau(e_n) = h_n \) and \( \tau(m_{[n^*]}) = f_{[n^*]} \), we have \( h_n = f_{[n^*]} \). So

\[
M(h, c)_{[n], \lambda} = M(f, c)_{[n^*], \lambda} = M(h^*, e)_{\lambda, [n^*]}, \text{ using (2.4)}
= \prod_i M(h^*, e)_{[\lambda_i], [n^*]}
\]

\[
(3.5)
\]
We adopt Macdonald’s methods to express $h_n^*$ in terms of the $e_\lambda$. Recall from Theorem 2.3 that if $y = xH(x)$, then $x = yH^*(y)$. So
\[ dx = \sum_{n \geq 0} (n + 1) h_n^* y^n dy. \]
It follows that $(n + 1)h_n^*$ equals the residue (coefficient of $y^{-1}$) of $dz/y^{n+1}$. Let $E(x) = \sum_{n \geq 0} e_n x^n$ be the generating function for the $e_n$. Then $H(x) = 1/E(-x)$. So $y = x/E(-x)$, whence $dz/y^{n+1} = dxE(-x)^{n+1}/x^{n+1}$. Thus $(n + 1)h_n^*$ equals the coefficient of $x^n$ in $E(-x)^{n+1}$. Since the $e_n$ are algebraically independent, we deduce that
\[ h_n^* = \frac{(-1)^n}{n + 1} \sum_{\lambda \vdash n} \binom{n + 1}{l(\lambda)} u_\lambda e_\lambda. \]
In particular
\[ M(h^*, e)[\nu] = \frac{(-1)^n}{n + 1} \binom{n + 1}{n} u_{[1^n]} = (-1)^n. \]
The identity for $h_n$ follows from (3.5) and (3.7).

We use this to prove a result about the 2-modular group algebra of $S_n$.

**Theorem 3.8.** Let $F$ be a field of characteristic 2, and let $\mathcal{L}(n)$ be the number of digits that equal 1 in the binary expansion of $n$. For $i = 1, \ldots, n - \mathcal{L}(n)$, set
\[ K_i := \sum K \in Z(FS_n), \]
where $K$ ranges over the 2-classes of $S_n$ whose cycle decomposition contains $n - i$ cycles. Then $K_1, \ldots, K_{n - \mathcal{L}(n)}$ generate the $F$-algebra $Z(FS_n)$.

**Proof.** It is enough to prove the result for $F = GF(2)$. We have $\Lambda = \mathbb{Z}[e_1, e_2, \ldots]$. So the nonzero terms in $e_1(n), e_2(n) \ldots$ generate the $\mathbb{Z}$-algebra $Z(\mathbb{Z}S_n)$ by Lemma 2.2. Reduction modulo 2 induces an epimorphism $Z(\mathbb{Z}S_n) \twoheadrightarrow Z(FS_n)$. Using Lemma 3.1 and Proposition 3.2, we see that the image of $e_i(n)$ in $Z(FS_n)$ coincides with $K_i$, for $i \geq 1$. Suppose that $S_n$ has a 2-class whose cycle type contains $n - i$ parts. Then $n$ is a sum of $n - i$ powers of 2. So $n - i \geq \mathcal{L}(n)$, whence $i \leq n - \mathcal{L}(n)$. It follows that $K_i = 0$, for $i > n - \mathcal{L}(n)$. This completes the proof of the theorem.

4. **Generators for the modular group algebra**

In this section we prove a more precise form of Theorem 3.8. Our first result translates Theorem 4.3 of [FH] into the language of symmetric functions.

**Proposition 4.1.** Let $\lambda$ be a partition of $n$. Then
\[ M(c, h)_{\lambda}[\nu] = (-1)^{l(\lambda)} \binom{n - 1 + l(\lambda)}{n - 1} u_\lambda. \]

**Proof.** We have
\[ M(c, h)_{\lambda}[\nu] = M(m, h^*)[\nu, \lambda] = M(p, h^*)[\nu, \lambda]. \]
Recall that $P(x) = H'(x)/H(x)$, and that if $y = xH(x)$, then $x = yH^*(y)$. Thus
\[ \frac{dy}{y} = \frac{H(x) + xH'(x)}{xH(x)} dx = \left( \frac{1}{x} + P(x) \right) dx. \]
It follows that $p_n$ is the residue of $dy/yx^n = dy/y^{n+1}H^*(y)^n$, which in turn is the coefficient of $y^n$ in $H^*(y)^{-n}$. Write $H^*(y) = 1 + H^*_+(y)$. Then
\[
H^*(y)^{-n} = \sum_{l \geq 0} \left( \frac{-n}{l} \right) H^*_+(y)^l.
\]
Since the $h^*_+$ are algebraically independent, it follows that
\[
(4.3) \quad p_n = \sum_{\lambda \vdash n} (-1)^l(\lambda) \left( \frac{n-1 + l(\lambda)}{n-1} \right) u_\lambda h^*_+.
\]
The proposition follows from (4.2) and (4.3).

Next we show that each positive integer has a particular representation as a sum of terms of the form $2^i - 1$, for $i \geq 1$. We begin with some technical results.

Let $S$ denote the set of sequences $s = \cdots s_{2i} s_0$, where each $s_i$ is one of the symbols $\{1, 0, -1, -2, \ldots \}$, and there are only a finite number of occurrences of 1. For each $i > 0$, let $s_{\geq i}$ denote the subsequence $\cdots s_{i+2} s_{i+1} s_i$ of $s$. We associate two numerical values to $s$. These are
\[
|s| := \left| \left\{i \geq 0 \mid s_i = 1 \right\} \right|, \quad \text{and} \quad \sum s := \sum_{i=0}^{\infty} \text{sgn}(s_i)2^i(2|s| - 1), \quad \text{a formal sum}.
\]

**Lemma 4.4.** Let $s \in S$ be such that for each $i \geq 0$, either
\begin{enumerate}[label=(\roman*)]
  \item $s_i = 1$ \quad or
  \item $s_i = -|s_{\geq i}|$.
\end{enumerate}
Then $\sum s = 2|s| - 1$.

**Proof.** Since $|s|$ is finite, there is a minimal $N = N(s) \geq 0$, such that $s_n = 0$ when $n \geq N$. We prove the lemma using induction on $N$. The base case $N = 0$ is trivial.

Suppose that $N > 0$. Then $N(s_{\geq 1}) < N$. The inductive hypothesis gives $\sum s_{\geq 1} = 2^{|s_{\geq 1}|} - 1$, and the definition gives $\sum s = 2 \sum s_{\geq 1} + \text{sgn}(s_0)(2^{|s|} - 1)$. If $s_0 = 1$, then $|s_{\geq 1}| = |s| - 1$, and $\sum s = 2(2^{|s_{\geq 1}|} - 1) + (2^{|s|} - 1) = 2^{|s|} - 1$. Otherwise $s_0 = -|s|$ and $|s_{\geq 1}| = |s|$. In this case we have $\sum s = 2(2^{|s_{\geq 1}|} - 1) - (2^{|s|} - 1) = 2^{|s|} - 1$. This completes the proof.

**Lemma 4.5.** Let $s \in S$ be such that for each $i \geq 0$, either
\begin{enumerate}[label=(\roman*)]
  \item $s_i = 1$ \quad or
  \item $s_j \neq 1$, for some $j < i$, and $s_i = -|s_{\geq i}|$ \quad or
  \item $s_j = 1$, for all $j < i$, and $s_i = -|s_{\geq i}| - 1$.
\end{enumerate}
Then $\sum s = -1$.

**Proof.** There exists $i \geq 0$ such that $s_j = 1$ for all $j < i$, and $s_{\geq i}$ has initial term $s_i = -|s_{\geq i}| - 1 = 1 - |s| - 1$. Let $x$ be the word that is obtained from $s$ by replacing $s_i$ by $-|s_{\geq i}|$. Then $x$ satisfies the criteria of Lemma 4.4, and $|x| = |s|$. We compute
\[
\sum s = \sum x + 2^i(2^{|s|} - 1) - 2^i(2^{|s|} + 1 - i) - 1 = 2^{|s|} - 1 + 2^{|s|} - 2^{|s|+1}, \quad \text{using Lemma 4.4}
\]
\[
= -1.
\]
Theorem 4.6. There exist nonnegative integers $e_1, e_2, \ldots$ such that $\lambda = [2^{e_1} - 1, 2^{e_2} - 1, \ldots]$ is a partition of $n$ and $M(c, h)_{\lambda, [n]}$ is odd.

Proof. Since $P(x) = H(x)/H(x)$ and $H(x) = 1/E(-x)$, we have $-P(-x) = E'(x)/E(x)$. Also $\tau(h_n) = e_n$. It follows that $\tau(p_n) = (-1)^e p_n$. Thus from $p_n = m_{[n]}$, and $\tau(m_{[n]}) = f_{[n]}$, we get $f_{[n]} = (-1)^e p_n$. Now for $\mu$ a partition, we have

$$M(c, e)_{\mu, [n]} = M(f, h^*)_{\mu, [n]} = (-1)^e M(p, h^*)_{\mu, [n]}$$

$$\equiv M(c, h)_{\mu, [n]} \pmod{2}, \quad \text{see (4.2)}.$$

The first statement of Proposition 3.2 then implies that $\sum_{\mu} M(c, h)_{\mu, [n]}$ is odd, where $\mu$ runs over all partitions of $n$ with $\mu_i + 1$ a power of 2, for all $i$. The theorem follows immediately from this. As an alternative proof, we will explicitly construct a partition of $n$ with the desired properties.

Let $b$ denote the sequence $b_i b_i b_0$ such that $n - 1 = \sum b_i 2^i$ is the binary expansion of $n - 1$. As before, $b_{\geq i}$ is the truncated sequence $b_{i+2} b_{i+1} b_i$. We construct a sequence $s = \ldots s_2 s_1 s_0 \in S$ as follows. For $i \geq 0$, set

$$s_i := \begin{cases} 1, & \text{if } b_i = 1; \\ -|b_{\geq i}|, & \text{if } b_i = 0, \text{ for some } j < i; \\ -|b_{\geq i}| - 1, & \text{if } b_i = 0, \text{ for all } j < i. \end{cases}$$

Then $s$ satisfies the criteria of Lemma 4.5.

For each $i \geq 0$, set $a_i := \sum \{2^j \mid j \geq 0 \text{ and } s_j = -i\}$. Lemma 4.5 shows that

$$\sum_{i \geq 0} b_i 2^i - \sum_{i \geq 0} a_i (2^i - 1) = \sum s = -1.$$ 

But $\sum b_i 2^i = n - 1$. It follows that

$$\sum_{i \geq 0} a_i (2^i - 1) = n.$$ 

Note that $n - 1 + \sum a_i = 2^r - 1$, where $2^{r-1} \leq n < 2^r$. The construction of $a_i$ shows that

$$r = L(n + 1) + \sum a_i = L(n - 1) + \sum L(a_i).$$

Let $\lambda$ denote the partition of $n$, whose parts are all of the form $2^i - 1$, for $i \geq 1$, where the multiplicity of $2^i - 1$ is $a_i$. It follows from Proposition 4.1 that $M(c, h)_{\lambda, [n]}$ is odd. \hfill \square

Corollary 4.7. Let $F$ be a field of characteristic 2, and let $r$ be the largest positive integer such that $2^r \leq n < 2^{r+1}$. Then there exist 2-classes $L_1, \ldots, L_{2^r-1}$ of $S_n$, whose sums generate the algebra $Z(FS_n)$. These classes can be chosen so that $L_i$ contains $n - i$ cycles, and $L_i$ is an involution class if and only if $i$ is a power of 2.

Proof. For $i \geq 1$, let $\lambda^i$ be the partition of $i$, constructed by the method of Theorem 4.6, such that $M(c, h)_{\lambda^i, [n]}$ is odd. Then clearly $\{c_{\lambda^i} \mid i \geq 1\}$ form a set of algebraically independent generators for $A$. It follows that the images of the nonzero $c_{A'}(n)$ generate $Z(FS_n)$.

Let $i$ be the largest positive integer such that $2^i \leq n$. The proof of Theorem 4.6 shows that $l(\lambda^i) = 2^{r-1} - 1$. Set $L_i = c_{A'}(n)$. Then $L_i$ is a conjugacy class of $S_n$ if and only if $i + l(\lambda^i) = 2^{r-1} \leq n$. This occurs if and only if $i < 2^r$. Now $L_i$ is an involution class if and only if all parts of $\lambda^i$ are 1. The construction of $\lambda^i$ shows that this occurs if and only if $i$ is a power of 2. \hfill \square
The table below demonstrates the construction of the 2-classes of $S_{16}$ that is given in the proof of Theorem 4.6.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$b$</th>
<th>$s$</th>
<th>$\lambda$</th>
<th>Class of $S_{16}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0 -1</td>
<td>$[1]$</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0 -1 -1</td>
<td>$[2]$</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0 1 -2</td>
<td>$[3]$</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0 -1 1</td>
<td>$[4]$</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td>0 -1 -2</td>
<td>$[3, 12]$</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1</td>
<td>0 1 -2</td>
<td>$[3, 12]$</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>1</td>
<td>0 1 -3</td>
<td>$[7]$</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>1</td>
<td>1 -1 1</td>
<td>$[18]$</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>0</td>
<td>1 -1 -2</td>
<td>$[3, 16]$</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>0</td>
<td>1 -2 1</td>
<td>$[3, 14]$</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>0</td>
<td>1 1 -3</td>
<td>$[7, 14]$</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>0</td>
<td>1 -2 1</td>
<td>$[3, 14]$</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>1</td>
<td>1 1 -3</td>
<td>$[7, 32]$</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>1</td>
<td>1 1 -3</td>
<td>$[7, 32]$</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1 1 -4</td>
<td>$[15]$</td>
</tr>
</tbody>
</table>

5. 2-BLOCKS OF SYMMETRIC GROUPS

Each finite dimensional $F$-algebra $A \neq 0$ has a decomposition

$$A = B_1 \oplus \cdots \oplus B_r$$

into a direct sum of a number $r$ of nonzero indecomposable $F$-algebras $B_i$. These are called the blocks of $A$. Let $e_i$ denote the multiplicative identity of the algebra $B_i$, for $1 \leq i \leq r$. Then $e_i$ is called the block idempotent of $B_i$. It is known that

$$1_A = e_1 + \cdots + e_r$$

is a decomposition of $1_A$ into a sum of pairwise orthogonal primitive central idempotents. When $A$ is a group algebra, each block of $A$ has associated to it a family of 2-subgroups of the group, known as its defect groups. These groups can be defined using the support of the block idempotent.

Suppose now that $A$ is split over $F$. Then the centre $Z(A)$ decomposes into

$$Z(A) = N \oplus E,$$

as $F$-algebras, where $N$ is the nilradical of $Z(A)$, and $E = F e_1 + \cdots + F e_r$ is the maximal semisimple subalgebra of $Z(A)$. The projection map $\rho : Z(A) \to E$, with respect to this decomposition, is given by

$$\rho(z) = \sum_{i=1}^r \omega_i(z)e_i, \quad \text{for } z \in Z(A),$$

where $\omega_i : Z(A) \to F$ is the unique irreducible $F$-representation of $Z(A)$ whose kernel does not contain $B_i$. The map $\omega_i$ is called the central character of $B_i$. It is known that $\rho(z)$ is contained in the subalgebra of $Z(A)$ that is generated by $z$. 

9
In this section we prove two results about the block algebras of $FS_n$. Our first result is known. It is a consequence of the Nakayama Conjecture, the theorem that classifies the $p$-blocks of symmetric groups using the $p$-cores of partitions.

**Proposition 5.1.** Let $F$ be a field of characteristic 2 and let $D$ be a 2-subgroup of $S_n$. Then $FS_n$ has at most one block with defect group $D$.

*Proof.* We use standard block-theoretic notation. See for instance [NT]. Let $G$ be an arbitrary finite group, let $p$ be a prime, and let $k$ be a field of characteristic $p$. Suppose that $B$ is a block of $kG$, with central character $\omega_B$ and defect group $P$. The *Brauer correspondent* $b$ of $B$ is a block of $kN_G(P)$, whose central character $\omega_b$ satisfies

$$\omega_b(K) = \omega_b \circ Br_P(K) = \omega_b(K \cap C_G(P)), \quad \text{for all classes } K \text{ of } G,$$

where $Br_P$ denotes the *Brauer homomorphism* with respect to $P$. A result of J. Green implies that $\omega_b$ vanishes on class sums of elements whose $p$-parts are not contained in $P$. Also $\omega_b(L^+) = [L]$, for each conjugacy class $L$ of $N_G(P)$ that is contained in $Z(P)$. It follows that if $K$ is a class of $p$-elements of $G$, then

$$\omega_B(K) = |K \cap Z(P)| 1_F.$$

This argument is due to G. R. Robinson.

We specialize to $G = S_n$ and $P = D$. The previous section shows that the 2-class sums generate $Z(FS_n)$, and the previous paragraph shows that the values of $\omega_B$ on the 2-class sums are determined by $D$. It follows that $\omega_B$ is determined by $D$. But $B$ is determined by $\omega_B$. We conclude that $B$ is the unique block of $FS_n$ that has defect group $D$. \hfill \Box

We now present the main result of this section.

**Theorem 5.3.** Let $F$ be a field of characteristic 2. Then each idempotent in $Z(FS_n)$ lies in the algebra that is generated by the involution class sums of $S_n$.

*Proof.* Let $B$ be a 2-block of $S_n$. The Nakayama Conjecture endows $B$ with a positive integer $w < n/2$ called its *weight*. Let $w = \sum_i 2^{a_i}$ be the 2-adic decomposition of $w$. Let $W_0$ denote the cyclic group of order 2, and define $W_i$ for $i > 0$, inductively by $W_i := W_{i-1} \cdot W_0$. Set $D := \prod_i W_{a_i}$. Then $D$ is isomorphic to a Sylow 2-subgroup of $S_{2w}$, and each defect group of $B$ is isomorphic to $D$. An inductive argument shows that $Z(W_i)$ is cyclic of order 2, whence $Z(D)$ is elementary abelian. In fact, the centre of a defect group contains exactly one involution that is a product of $2w$ commuting transpositions, for each $a_i \neq 0$, and these involutions form a basis for the centre. It follows from (5.2) that $\omega_B$ vanishes on the sum of any 2-class whose elements have order divisible by 4.

Let $Z(FS_n) = N \otimes E$ and $\rho : Z(FS_n) \to E$ be as above. Suppose that $L_1, L_2, \ldots$ are 2-classes of $S_n$ whose sums generate the algebra $Z(FS_n)$. Then clearly $\rho(L_1), \rho(L_2), \ldots$ generate the algebra $E$. The previous paragraph shows that $\rho(L_i) = 0$ unless $L_i$ is a class of involutions. It follows that $E$ is contained in the algebra generated by the involution class sums in the list $L_1, L_2, \ldots$. \hfill \Box

Corollary 4.7 can be used to strengthen this theorem, in an obvious way.
6. MURPHY-JUCYS ELEMENTS

For positive integers \( i \neq j \), let \((i,j)\) denote the permutation in \( S_\infty \) that transposes \( i \) and \( j \). Define the JM-elements of \( \mathbb{Z}S_\infty \) as
\[
J_u := (1,u) + (2,u) + \ldots + (u-1,u), \quad \text{for } u = 2, \ldots n.
\]
If \( f \) is a polynomial in the variables \( x_1, x_2, \ldots \), we use \( f(l;n) \) to denote the evaluation of \( f \) at \( x_1 = l_2, x_2 = l_3, \ldots, x_{n-1} = l_n, x_n = 0, x_{n+1} = 0, \ldots \). So \( f(l;n) \) lies in \( \mathbb{Z}S_n \).

A. A. Jucys [1] has shown the following:

**Lemma 6.2.** \( Z(\mathbb{Z}S_n) \) coincides with the ring of symmetric polynomials in \( l_2, \ldots, l_n \). In particular \( Z(\mathbb{Z}S_n) = \mathbb{Z}[e_1(l;n), \ldots, e_{n-1}(l;n)] \). In terms of the class sums,
\[
e_i(l;n) = \sum_{\lambda^i} c_\lambda(n). \quad \text{for } i = 1, \ldots, n - 1.
\]

The following result gives a connection between the ring of symmetric polynomials in the Jucys elements and Macdonald’s class symbol algebra. Recall that \( \tau \) is an involutory automorphism of \( \Lambda \) that interchanges \( e_i \) and \( h_i \) for \( i \geq 1 \).

**Theorem 6.3.** Let \( g \in \Lambda \) be a homogeneous symmetric function of degree \( i \). Then
\[
g(l;n) \equiv (-1)^i \tau(g)(n) \pmod{Z(\mathbb{Z}S_n)_i}.
\]

**Proof.** Proposition 3.2 and Lemma 6.2 imply that \( e_i(l;n) = (-1)^i h_i(n) \), for each \( i \geq 1 \). Let \( \lambda \) be a partition. An inductive argument using (2.1) gives
\[
e_i(l;n) \equiv (-1)^{|\lambda|} h_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_{|\lambda|}}.
\]
But \( h_\lambda = \tau(e_\lambda) \). The proposition follows, as the \( e_\lambda \) form a \( \mathbb{Z} \)-basis for \( \Lambda \).

**Corollary 6.4.** Let \( \lambda \) be a partition. Then
\[
m_\lambda(l;n) \equiv (-1)^{|\lambda|} f_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_{|\lambda|}};
\]
\[
h_\lambda(l;n) \equiv (-1)^{|\lambda|} e_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_{|\lambda|}}.
\]
In particular, if \( i \geq 1 \) then
\[
h_i(l;n) \equiv \sum_{\lambda^i} C_\lambda c_\lambda(n) \pmod{Z(\mathbb{Z}S_n)_i}.
\]

**Proof.** The first statement uses the fact that \( \tau(m_\lambda) = f_\lambda \). The other statements use Proposition 3.2.

7. THE 2-REGULAR CLASS SYMBOL ALGEBRA

Recall that \( F \) is a field of characteristic 2. A conjugacy class of \( S_n \) is said to be 2-regular if all its elements have odd order. The author showed in [M, Corollary 5] that the \( F \)-span of the class sums of the \( 2 \)-regular classes forms a subalgebra of \( Z(\mathbb{F}S_n) \). We call this algebra the \( 2 \)-regular algebra of \( Z(\mathbb{F}S_n) \). (More generally the centre of the \( p \)-modular group algebra of \( S_n \) has a \( p \)-regular subalgebra, for each prime \( p \).)

We call a partition with all parts even a \( 2 \)-partition. So a class of \( S_n \) is \( 2 \)-regular if and only if its modified cycle type is a \( 2 \)-partition. It follows from (2.1) and the previous paragraph that the \( F \)-span of \( \{ c_\lambda \mid \lambda \text{ is a } 2 \text{-partition} \} \) forms a subalgebra of \( \Lambda \otimes F \), which we shall call the \( 2 \)-regular class symbol algebra. The purpose of this section is to show that this is a polynomial subalgebra of \( \Lambda \otimes F \). This fact will be used to give explicit generators for the \( 2 \)-regular subalgebra of \( Z(\mathbb{F}S_n) \).
We extend the notation for Catalan numbers slightly by setting \( C_q = 0 \), whenever \( q \in \mathbb{Q} \setminus \mathbb{Z} \). For each pair \( \lambda/n \), with \( \lambda \) a partition and \( n \) a positive integer, define
\[
C_{\lambda/n} := \prod_i C_{\lambda_i/n}.
\]

**Proposition 7.1.** \( h_n^2 \equiv \sum_{\lambda \vdash 2n} C_{\lambda/2} c_\lambda \mod 2 \).

**Proof.** We have \( e_n = m_{[1^*]} \). So \( e_n^2 \equiv m_{[2^*]} \mod 2 \). Applying the automorphism \( \tau \), we get \( h_n^2 \equiv f_{[2^*]} \mod 2 \). Now if \( \lambda \) is a partition of \( 2n \), then
\[
M(h, c)_{[\lambda], \lambda} \equiv M(f, c)_{[\lambda], \lambda} \mod 2
\]
\[
= M(h^*, c)_{[\lambda], [\lambda^*]}, \text{ by } (2.4)
\]
\[
= \left\{ \begin{array}{ll}
\prod_{i \geq 1} M(h^*, c)_{[\lambda_i], [\lambda_i/2]}, & \text{if } \lambda_i \text{ is even for all } i \geq 1; \\
0, & \text{otherwise.}
\end{array} \right.
\]
Equation (3.6) gives
\[
M(h^*, c)_{[2n], [2n]} = \frac{(-1)^{2n}}{2n+1} \binom{2n+1}{n} u_{[2^*]} = C_n.
\]
The proposition follows from (7.2) and (7.3). \( \square \)

**Corollary 7.4.** Let \( F \) be a field of characteristic 2. Then the 2-regular class symbol algebra coincides with the polynomial algebra \( F[h_1^2, h_2^2, \ldots] \).

**Proof.** Lemma 3.1 implies that if \( j \geq 1 \), then \( C_{j/2} \) is odd if and only if \( j + 2 \) is a power of 2. It then follows from Proposition 7.1 that
\[
h_i^2 \equiv \sum c_\lambda \mod 2,
\]
for each \( i \geq 1 \), where \( \lambda \) ranges over the partitions of \( 2i \) with each part \( \lambda_j \) of the form \( 2^q - 2 \), for some \( q > 0 \). This shows that the subalgebra of \( \Lambda \otimes F \) generated by the images of \( h_1^2, h_2^2, \ldots \) is contained in the 2-regular class symbol algebra.

There is an obvious bijection between the 2-partitions of \( 2i \) and the partitions of \( 2i \) whose parts occur with even multiplicities. It then follows from a consideration of Z-ranks, and the previous paragraph, that the images of \( \{ h_1^2, h_2^2, \ldots \} \) form an algebraically independent generating set for the 2-regular class symbol algebra. \( \square \)

**Theorem 7.5.** Let \( F \) be a field of characteristic 2. For \( i = 1, \ldots, \lfloor \frac{n}{2} \rfloor \), set
\[
R_i := \sum K \in Z(FS_n),
\]
where \( K \) ranges over the conjugacy classes of \( S_n \) whose cycle decomposition consists of \( n - 2i \) cycles, each of length \( 2^e - 1 \), for some \( e \geq 0 \). Then \( R_1, \ldots, R_{\lfloor \frac{n}{2} \rfloor} \) generate the 2-regular algebra of \( Z(FS_n) \).

**Proof.** The element \( R_i \) coincides with the image of \( h_i^2(n) \) in \( Z(FS_n) \). Suppose that \( S_n \) has a conjugacy class that contains \( 2i \) cycles. Then \( 2i \leq n \). So \( i \leq \lfloor \frac{n}{2} \rfloor \). Since \( \{ h_1^2, h_2^2, \ldots \} \) generate the 2-regular class symbol subalgebra in \( \Lambda \otimes F \), it follows that \( \{ R_1, \ldots, R_{\lfloor \frac{n}{2} \rfloor} \} \) generate the 2-regular subalgebra of \( Z(FS_n) \). \( \square \)
8. The involution class symbol algebra

Let $t_n$ denote the conjugacy class of $S_\infty$ containing the involutions that are products of $n$ commuting transpositions. So $t_0 := 1$, and $t_i := 0$ for $i < 0$. If $\lambda$ is a partition, set

$$t_\lambda := \prod_i t_{\lambda_i}.$$ 

Also put $t_{[\lambda]} := 1$. Recall that $F$ is a field of characteristic 2. The images of $\{t_\lambda \mid \lambda \text{ a partition}\}$ span a subalgebra of $\Lambda \otimes F$. We call this algebra the involution class symbol algebra. We do not know whether it is a polynomial algebra. In Theorem 8.9 we exhibit a set of algebraically independent involution class symbols. It is possible that these elements actually generate the involution class symbol algebra. In Section 9 we will show that a slightly larger subalgebra of $\Lambda \otimes F$ is a polynomial algebra.

**Proposition 8.1.** $t_n = (-1)^n \sum_{\lambda \vdash n} C_\lambda m_\lambda$.

**Proof.** The map that interchanges $h_n$ and $h_n^*$ is an involutory automorphism of $\Lambda$. (But note that it does not preserve the bilinear form $\langle , \rangle$.) It follows that

$$M(c, m) = M(h, h^*)^t = M(h^*, h)^t = M(m, c).$$

Thus

$$M(t_n, m)[n, \lambda] = M(c, m)[n, \lambda] = M(m, c)[n, \lambda] = M(e, m)[n, \lambda].$$

The result now follows from Proposition 3.2. \hfill $\Box$

Set $D_n := \left( \frac{2n - 1}{n - 1} \right)$. Our interest in $D_n$ is partially due to the next lemma.

**Lemma 8.2.** Let $C(x) = \sum_{n=0}^\infty (-1)^n C_n x^n$. Then $C'(x)/C(x) = \sum_{n=1}^\infty (-1)^n D_n x^{n-1}$.

**Proof.** The binomial theorem can be used to show that

$$C(x) = \frac{-1 + \sqrt{1 + 4x}}{2x}.$$ 

So $xC(x)^2 + C(x) - 1 = 0$. Differentiating, we get

$$\frac{C'(x)}{C(x)} = \frac{-C(x)}{1 + 2xC(x)} = \frac{1 - \sqrt{1 + 4x}}{2x} = \left(1 + 4x\right)^{-1/2} - 1.$$ 

The result follows from another application of the binomial theorem. \hfill $\Box$

Let $T(x) = \sum_{n \geq 0} t_n x^n$ and set $D(x) := T'(x)/T(x) = \sum_{n \geq 1} d_n x^{n-1}$. So $\{d_n\}$ are symmetric functions that satisfy

$$nt_n = \sum_{i=1}^n d_i t_{n-i}.$$ 

(8.3)

Recall that $p_n = m_n$. Our next result was inspired by Proposition 1.2 of [W].

**Proposition 8.4.** $d_n = (-1)^n D_n p_n$. 

13
Proof. Clearly $T(x) = \prod_{i \geq 1} C(x_i x)$. So
\[
\frac{T'(x)}{T(x)} = \frac{d}{dx} \left[ \ln T(x) \right] = \sum_{i=1}^{\infty} \frac{d}{dx} \left[ \ln C(x_i x) \right]
\]
\[
= \sum_{i=1}^{\infty} \frac{C'(x_i x)}{C(x_i x)} x_i = \sum_{i=1}^{\infty} D(x_i x) x_i, \quad \text{by Lemma 8.2}
\]
\[
= \sum_{n=1}^{\infty} (-1)^n D_n p_n x^{n-1}.
\]
\[\square\]

The above Proposition can be used to show that $\{t_n \mid n \geq 1\}$ is a set of algebraically independent generators of $\Lambda \otimes \mathbb{Q}$. We omit the details.

Next we determine the parity of $D_n$.

**Lemma 8.5.** Let $n$ be a positive integer. Then $D_n$ is odd if and only if $n$ is a power of 2.

**Proof.** This follows from
\[
\nu(D_n) = \nu((2n - 1)! n!) - \nu((n - 1)! n!) - \nu(n!)
\]
\[
= \nu((2n)! n! - 2n) - \nu(n! n) + \nu(n) - \nu(n!)
\]
\[
= (2n - \mathcal{L}(n)) - 2(n - \mathcal{L}(n)) - 1
\]
\[
= \mathcal{L}(n) - 1.
\]
\[\square\]

This allows us to prove the following:

**Corollary 8.6.** Then the involution class symbol algebra is generated by the images of $\{t_n \mid n \geq 1, n \text{ is even or } n = 1\}$ in $\Lambda \otimes F$.

**Proof.** Suppose that $n \geq 0$. We use induction on $n$ to show that
\[
t_{2n+1} \equiv \sum_{i \geq 1} t_{1}^{i-1} t_{2n+2-2i} \pmod{2}.
\]
If $n = 0$ this equality is trivial. So suppose that $n > 0$. Equation 8.3 and Proposition 8.4 imply that
\[
(2n + 1) t_{2n+1} = \sum_{i=1}^{2n+1} (-1)^i D_i p_i t_{2n+1-i}.
\]
It then follows from Lemma 8.5 that
\[
t_{2n+1} \equiv \sum_{i \geq 0} p_i t_{2n+1-i} \pmod{2}
\]
But $p_{2n} \equiv t_1^{2n} \pmod{2}$. So the inductive hypothesis gives
\[
t_{2n+1} \equiv \sum_{i \geq 0} \sum_{j \geq 1} t_1^{i+j-1} t_{2n+2-j-2i} \pmod{2}.
\]
Let $i \neq j$ be positive integers. The terms in the above sum arising from $(i,j)$ and $(j,i)$ are the same. So they cancel. We conclude that
\[
t_{2n+1} = \sum_{i \geq 0} t_1^{2i+2i-1} t_{2n+2-2i-2i} \pmod{2}
\]
\[
= \sum_{i \geq 1} t_1^{2i-1} t_{2n+2-2i}.
\]

Next we refine our knowledge of the parity of $D_n$.

**Lemma 8.7.** Let $n$ be a positive integer. Then $(D_n^2 - D_{2n})/2$ is an integer. This integer is odd if and only if $n$ is a power of 2 or a sum of two distinct powers of 2.

**Proof.** Since $L(n) = L(2n)$, it follows from Lemma 8.5 that $D_n$ and $D_{2n}$ have the same parity. In particular $(D_n^2 - D_{2n})/2$ is an integer.

Suppose that $L(n) \geq 3$. Then $(D_n^2 - D_{2n})/2$ is even, since both $D_n$ and $D_{2n}$ are divisible by 4.

Suppose that $L(n) = 2$. Then $D_n$ and $D_{2n}$ are congruent to 2 modulo 4. So $D_n^2$ is divisible by 4 and $(D_n^2 - D_{2n})/2$ is odd.

Finally, suppose that $n$ is a power of 2. Then $D_n$ is odd. So $D_n^2$ is congruent to 1 modulo 4. We prove that $D_{2n}$ is congruent to 3 modulo 4 by induction. The base case is $D_2 = 3$. The inductive step follows from
\[
D_{2n} = \frac{(2n-1)(2n-3) \cdots (2n-(2n-1))}{D_n}
\]
\[
\equiv \frac{(-1)(-3) \cdots (-2n+1)}{(-1)(-3) \cdots (-2n+1)} D_n \equiv D_n \pmod{4}.
\]

We conclude that $(D_n^2 - D_{2n})/2$ is odd in this case.

If $\alpha$ and $\beta$ are partitions, let $\alpha \cup \beta$ denote the partition that is formed by arranging the parts of $\alpha$ and $\beta$ in nonincreasing order.

If $|\alpha| = |\beta| = n$, write $\alpha \prec \beta$ if $l(\alpha) > l(\beta)$ or $l(\alpha) = l(\beta)$ and $\alpha$ precedes $\beta$ in the reverse lexicographic order. Then $\prec$ is a total order and

(i) Every partition of $n$ precedes $[n]$;

(ii) $[n^2]$ is the immediate predecessor of $[2n]$.

Moreover, if $\alpha, \beta, \gamma, \delta$ are partitions with $\alpha \prec \gamma$ and $\beta \prec \delta$, then $\alpha \cup \beta \prec \gamma \cup \delta$.

Suppose that $n$ is 1 or an even integer. Define the partition
\[
\epsilon(n) := \begin{cases} [n], & \text{if } n \text{ is a power of } 2, \\ \lfloor (n/2)^2 \rfloor, & \text{if } n \text{ is not a power of } 2. \end{cases}
\]

For $\lambda$ a partition with each part even or equal to 1, set
\[
\epsilon(\lambda) := \bigcup_{i \geq 1} \epsilon(\lambda_i).
\]

Then the map $\lambda \rightarrow \epsilon(\lambda)$ is injective.

We now prove the main result of this section.
Theorem 8.9. Let $F$ be a field of characteristic 2. Then
\[
\{t_n \mid n \text{ is a power of } 2 \text{ or a sum of two distinct even powers of } 2\}
\]
is algebraically independent, when considered as a subset of $\Lambda \otimes F$.

Proof. Let $n \geq 1$. Then $M(t, h)[n^2][n^2] = M(e, h)[1^2][1^2] = (-1)^n D_n$, using Proposition 4.1. It then follows from Lemma 8.5, and (i) of (8.8), that, modulo 2,
\[
(8.10) \quad t_n \equiv \begin{cases} h_n + \sum \{\text{certain } h_\mu \text{ with } \mu < [n]\}, & \text{if } n \text{ is a power of } 2; \\ \sum \{\text{certain } h_\mu \text{ with } \mu < [n]\}, & \text{otherwise}. \end{cases}
\]
Now suppose that $n$ is not a power of 2. We have $m[n^2] = (p[n^2] - p[2n])/2$. So
\[
M(t, h)[2n][n^2] = M(e, h)[1^2][n^2] = M(m, h^*)[n^2][1^2] \quad \text{by (2.4)}
\]
\[
= (M(p, h^*)[n^2][1^2] - M(p, h^*)[2n][1^2])/2
\]
\[
= (D_n^2 - D_{2n})/2, \quad \text{using (4.3)}.
\]
It then follows from Lemma 8.7, (ii) of (8.8), and (8.10), that, modulo 2,
\[
(8.11) \quad t_n \equiv \begin{cases} h_{[(n/2)^2]} + \sum \{\text{certain } h_\mu \text{ with } \mu < [(n/2)^2]\}, & \text{if } n \text{ is a sum of two distinct even powers of } 2; \\ \sum \{\text{certain } h_\mu \text{ with } \mu < [(n/2)^2]\}, & \text{otherwise}. \end{cases}
\]
Let $\lambda$ be a partition, such that each part $\lambda_i$ is a power of 2 or a sum of two even powers of 2. It follows from (8.10) and (8.11) that
\[
t_\lambda \equiv h_{[(\lambda)^2]} + \sum \{\text{certain } h_\mu \text{ with } \mu < \lambda\} \quad \text{mod } 2.
\]
The theorem now follows from the injectivity of $\epsilon$. \qed

9. A POLYNOMIAL SUBALGEBRA OF THE CLASS SYMBOL ALGEBRA

Recall that $F$ is a field of characteristic 2. In this the final section we show that the smallest subalgebra of $\Lambda \otimes F$ that contains both the involution class symbol algebra and the 2-regular class symbol algebra is a polynomial algebra. We furnish it with a set of algebraically independent generators in Theorem 9.8. In view of Theorem 8.9, Corollary 9.10 provides evidence that the involution class symbol algebra is itself a polynomial algebra.

For any $\sigma \in S_\infty$, we may write $\sigma = \sigma_2\sigma_2' = \sigma_2\sigma_2''$, where $\sigma_2$ has order a power of 2 and $\sigma_2'$ has odd order. We call $\sigma_2$ the 2-part of $\sigma$, and $\sigma_2'$ the 2-regular part of $\sigma$. The 2-regular parts of the elements of a class of $S_\infty$ form a single 2-regular conjugacy class. We call the set of classes whose 2-regular parts lie in a given 2-regular class $K$ the 2-regular section of $S_\infty$ that contains $K$.

Let $\lambda$ be a partition and let $N \geq 1$. Extending the notion of a 2-partition, we call a partition $\lambda$ a $2^N$-partition if
\[
\lambda_i \not\equiv -1 \pmod{2^N}, \quad \text{for all } i \geq 1.
\]
Then $\{c_{\lambda} \mid \lambda \text{ is a } 2^N\text{-partition}\}$ are the conjugacy classes of $S_\infty$ whose elements have order not divisible by $2^N$. It follows from (2.1), and the remark after Corollary 5 in [M], that these symbols form an $F$-basis for a subalgebra of $\Lambda \otimes F$. We call this algebra the $2^N$-regular class symbol algebra.

Let $\approx$ be the equivalence relation generated on the set of partitions by:

(i) If $n \geq 1$ then $[2n + 1] \approx [n^2, 1]$;
(ii) If $\alpha, \beta, \gamma, \delta$ are partitions, with $\alpha \approx \gamma$ and $\beta \approx \delta$, then $\alpha \cup \beta \approx \gamma \cup \delta$.  

16
Both of the following Lemmas are fairly obvious consequences of the definition of $\approx$.

**Lemma 9.1.** Each $\approx$ equivalence classes contains a unique partition with all odd parts equal to 1.

**Lemma 9.2.** Let $\lambda, \mu$ be partitions of $n$. Then $\lambda \approx \mu$ if and only if $c_\lambda$ and $c_\mu$ are contained in the same 2-regular section of $S_\infty$.

Following Farahat and Higman, we define

$$m(\sigma) := \sum (|N| - 1), \quad \text{for } \sigma \in S_\infty,$$

where $N$ runs over all orbits of $\sigma$ on $\mathbb{N}$. We call any expression $\sigma = \sigma_1 \ldots \sigma_m$, where $\sigma_1, \ldots, \sigma_m \in S_\infty$, and $\sum m(\sigma_i) = m(\sigma)$, a minimal factorization of $\sigma$. Every $\sigma$ has a minimal factorization into transpositions. If $N$ is an orbit of $\sigma$ on $\mathbb{N}$, we will use $\sigma^N$ for the element of $S_\infty$ that agrees with $\sigma$ on $N$, and fixes all element of $\mathbb{N}\setminus N$. So $\sigma^N \in S_M$, where $M = \max i$.

The next two lemmas can be deduced from Lemma 3.5 of [FH].

**Lemma 9.3.** Let $\sigma = \sigma_1 \ldots \sigma_m$ be a minimal factorization of $\sigma$. Then each orbit of $\sigma$ is a union of orbits of the $\sigma_i$.

**Lemma 9.4.** Let $\sigma = \sigma_1 \ldots \sigma_m$ be a minimal factorization of $\sigma$. Suppose that $N$ is a union of orbits of $\sigma$. Then $\sigma^N = \sigma_1^N \ldots \sigma_m^N$ is a minimal factorization of $\sigma^N$.

We also need a technical lemma that concerns the multiplication of the class symbols $c_\mu$. Let $\{\mu^i\}$ be a sequence of partitions with $\sum |\mu^i| = n$. We may write

$$\prod c_{\mu^i} = \sum_{\lambda \vdash n} |P\{\{c_{\mu^i}\}; c_\lambda\}| c_\lambda,$$

where, for $\sigma$ a fixed element of $c_\lambda$,

$$P\{\{c_{\mu^i}\}; c_\lambda\} = \{(\sigma_1, \sigma_2, \ldots) \in c_{\mu^1} \times c_{\mu^2} \times \cdots \mid \prod \sigma_i = \sigma\}.$$

**Lemma 9.5.** Suppose that $\lambda = \alpha \cup \beta$, where $\alpha$ and $\beta$ are partitions. Then

$$|P\{\{c_{\mu^i}\}; c_\lambda\}| = \sum |P\{\{c_{\mu^i}\}; c_\alpha\}| \times |P\{\{c_{\mu^i}\}; c_\beta\}|,$$

where $\{\{\rho^i\}; \{\nu^i\}\}$ range over all pairs of sequences of partitions for which $\rho^i \cup \nu^i = \mu^i$, for all $i \geq 1$, and $\sum |\rho^i| = |\alpha|$ and $\sum |\nu^i| = |\beta|$.

**Proof.** We demonstrate a bijection

$$P\{\{c_{\mu^i}\}; c_\lambda\} \longleftrightarrow \bigcup P\{\{c_{\mu^i}\}; c_\alpha\} \times P\{\{c_{\nu^i}\}; c_\beta\}.$$

Let $\sigma \in c_\lambda$. Then there exists a partition $\mathbb{N} = N \cup M$, with $N^\sigma = N$ and $M^\sigma = M$, such that $\sigma^N \in c_\alpha$ and $\sigma^M \in c_\beta$. Suppose that $\{\sigma_i\} \in P\{\{c_{\mu^i}\}; c_\lambda\}$. Then $\sigma_i = \sigma_i^N \sigma_i^M$ for $i \geq 1$, and $\sigma^N = \prod \sigma_i^N$ and $\sigma^M = \prod \sigma_i^M$, using Lemma 9.4. Now $\sigma_i^N \in c_{\mu^i}$ and $\sigma_i^M \in c_{\nu^i}$, for some partitions $\rho^i, \nu^i$. Clearly $\rho^i \cup \nu^i = \mu^i$ and $(\sigma_i^N) \in P\{\{c_{\mu^i}\}; c_\alpha\}$ and $(\sigma_i^M) \in P\{\{c_{\nu^i}\}; c_\beta\}$. The map

$$(\sigma_i) \rightarrow ((\sigma_i^N), (\sigma_i^M))$$

is reversible. This establishes the required bijection, and completes the proof. \qed
We now concentrate on 4-partitions. Let $\nu$ be a 4-partition. Set
\begin{equation}
  k_{\nu} := \sum \{ c_\mu \mid \mu \text{ is a 4-partition of } |\nu| \text{ and } \mu \approx \nu \}.
\end{equation}
The first example where $k_{\nu} \neq c_\nu$ occurs with $\nu = [5]$. Then $k_{[5]} = q_3 + q_{2^2,1}$.

**Proposition 9.7.** Let $F$ be a field of characteristic 2. Let $\lambda$ be a partition and let $\mu$ be a 2-partition. Then the product $t_\lambda c_\mu$ lies in the $F$-span of
\begin{equation}
  \{ k_\nu \mid \nu \text{ is a 4-partition of } |\lambda| + |\mu| \}.
\end{equation}

**Proof.** Since $[1^n]$ and $\mu$ are 4-regular, it follows that $t_\lambda c_\mu$ is contained in the 4-
regular class symbol algebra. Also, if $\alpha$ and $\beta$ are partitions with $\alpha \cup \beta = [1^n]$, then
$\alpha = [1^n]$ and $\beta = [1^{n-m}]$, for some $m$. Similarly, if $\alpha \cup \beta = \mu$, then both $\alpha$ and $\beta$
are 2-regular. Using Lemma 9.5, and the definition of $k_\nu$, it is enough to show that
\begin{equation}
  |P(t_\lambda c_\mu; q_{4n+1})| \equiv |P(t_\lambda c_\mu; c_{[2n]^2,1})| \pmod{2},
\end{equation}
whenever $|\lambda| + |\mu| = 4n + 1$, for some $n \geq 0$. This follows from Claim 1 and Claim 2 below. \hfill \Box

**Claim 1.** Let $|\lambda| + |\mu| = 4n + 1$. We claim that either $P(t_\lambda c_\mu; q_{4n+1})$ has even
cardinality or there is a unique $j \geq 1$ such that $\lambda_j$ is odd, in which case
\begin{equation}
  |P(t_\lambda c_\mu; q_{4n+1})| \equiv |P(t_{\lambda_1}, \ldots, t_{\lambda_{j-1}}, \lambda_j, \ldots, \mu; c_{[2n]^2})| \pmod{2}.
\end{equation}

**Proof.** Let $\sigma \in S_4$ have modified cycle type $[4n+1]$. We may assume that $\sigma \in S_{4n+2}$. Then $\sigma$ has a single orbit on $\{1, \ldots, 4n+2\}$. Now $|\mu|$ is even, since all parts of $\mu$ are even, while $4n+1$ is odd. It follows that $\lambda_j$ is odd, for some $j \geq 1$. By a slight abuse of notation, we may assume that $\lambda_1$ is odd.

Let $a = \sigma^{2n+1}$. Then $a \in t_{[2n+1]}$ is an involution. Moreover, $a$ generates a Sylow
2-subgroup of the centralizer of $\sigma$ in $S_{4n+2}$. There exists $b \in t_{[2n]}$ that inverts $\sigma$.
Clearly $K = \langle a, b \rangle$ is elementary abelian of order 4. Assume that $4n+1, 4n+2$
are the unique symbols fixed by $b$. Then $K$ acts without fixed points on $\{1, \ldots, 4n\}$.

Let $((\sigma_i), h) \in P(t_{\lambda_1} c_\mu; q_{4n+1})$. For $i \geq 1$, set $b_i := \sigma_{i-1} \sigma_{i-2} \ldots \sigma_2 \sigma_1 b$. Define
\begin{equation}
  ((\sigma_i), h)^a = ((\sigma_i^a), h^a)
\end{equation}
and
\begin{equation}
  ((\sigma_i), h)^b = ((\sigma_i^b), (h^{-1})^a b).
\end{equation}
A long but routine check establishes that both $((\sigma_i), h)^a$ and $((\sigma_i), h)^b$
are elements of $P(t_{\lambda_1} c_\mu; q_{4n+1})$, and that this induces an action of the group $K$ on $P(t_{\lambda_1} c_\mu; q_{4n+1})$. This generalization of the Brauer homomorphism was discovered
by R. Gow. See [G] for further details.

Since $K$ is a 2-group, the cardinality of the set $P(t_{\lambda_1} c_\mu; q_{4n+1})$ is equivalent,
modulo 2, to the number of ordered tuples $((\sigma_i), h) \in P(t_{\lambda_1} c_\mu; q_{4n+1})$ such that
\begin{equation}
  \sigma_i^a = \sigma_i, \quad \sigma_i^b = \sigma_i, \quad \text{for all } i \geq 1, \quad \text{and } h^a = h \text{ and } h^{b_i} = h^{-1}.
\end{equation}
Assume that there is such a tuple $((\sigma_i), h)$. Then $\sigma_1 \in t_{\lambda_1}$, and $\sigma_i^a = \sigma_1$ and $\sigma_i^b = \sigma_i^a h = \sigma_1$. The 4-group $K$ has $n$ orbits on $\{1, \ldots, 4n\}$, and it acts regularly
on each orbit. Let $x$ be one of these orbits. Since $\sigma_1 \in C(K)$, either $\sigma_1$ fixes
each element of $x$, or $\sigma_1$ fixed no element of $x$. We deduce that the number of elements
of $\{1, \ldots, 4n\}$ that are fixed by $\sigma_1$ is divisible by 4. But
\begin{equation}
  \lambda_1 = (4n + 2 - \#\{\text{fixed points of } \sigma_1\})/2.
\end{equation}
Since $\lambda_1$ is odd, it follows that $\sigma_1$ contains the transposition $(4n+1, 4n+2)$ in
its cycle decomposition. Now $\prod \sigma_i h = \sigma$ is a minimal factorization of $\sigma$. So
(4n + 1, 4n + 2) can only occur in the cycle decomposition of \(\sigma_1\). We deduce that \(\lambda_i\) is even for \(i \geq 2\). Also \((4n + 1, 4n + 2)\) has modified cycle type \([(2n)^2, 1]\), and \((4n + 1, 4n + 2)\sigma_1 \in t_{\lambda_1^{-1}}\). Claim 1 follows easily from this.

**Claim 2.** Let \(|\lambda| + |\mu| = 4n + 1\). We claim that either \(P(t_{\lambda_1}, c_{\mu}; c_{[(2n)^2, 1]}\) has even cardinality or there is a unique \(j \geq 1\) such that \(\lambda_j\) is odd, and that

\[
P(t_{\lambda_1}, c_{\mu}; c_{[(2n)^2, 1]}) \equiv |P(t_{\lambda_1}, \ldots, t_{\lambda_{j-1}}, \ldots, c_{\mu}; c_{[(2n)^2]})| \pmod{2}.
\]

**Proof.** As in Claim 1, we may assume that \(\lambda_1\) is odd. Let \(\sigma \in S_{4n}\) have modified cycle type \([(2n)^2, 1]\). We may assume that \(\sigma \in S_{4(n+1)}\) and that \(x = \{1, \ldots, 2n+1\}\), \(y = \{2n+2, \ldots, 4n+2\}\) and \(z = \{4n+3, 4n+4\}\) are the 3 orbits of \(\sigma\). Let \(a \in t_{2n+1}\) be an involution that centralizes \(\sigma\). So \(a\) interchanges the elements of \(x\) and \(y\), and fixes both elements of \(z\).

Suppose that \(P(t_{\lambda_1}, c_{\mu}; c_{[(2n)^2, 1]}\) has odd cardinality. By an argument simpler than that used in Claim 1, there exists \((\{\sigma_i\}, h) \in \prod t_{\lambda_i} \times c_{\mu} \times \prod c_{\mu} \times h = \sigma\), and \(\sigma_i^h = \sigma_i\), for all \(i \geq 1\), and \(h^a = h\). Let \(j \in x\). Set \(k = a(j)\). Suppose that \(\sigma_1(j) \neq j\). Then \(\sigma_1(k) = a(\sigma_1(j)) \neq k\). Also \(k \in y\). We deduce that the cycle decomposition of \(\sigma_1\) contains the pair of transpositions \((j, \sigma_1(j))(k, \sigma_1(k))\). As \(\sigma_1\) has an odd number \(\lambda_1\) of transpositions in its cycle decomposition, it follows that \(\sigma_1\) contains the transposition \((4n + 3, 4n + 4)\). The proof of Claim 2 now proceeds along the same lines as that of Claim 1.

We now prove the main result of this section.

**Theorem 9.8.** Let \(F\) be a field of characteristic 2. Then the smallest subalgebra of \(\Lambda \otimes F\) that contains the involution class algebra and the 2-regular class algebra coincides with the \(F\)-span of \(\{k_\nu \mid \nu\) is a 4-partition\}. This algebra is a polynomial algebra with algebraically independent generating set

\[
\{t_n \mid n \geq 1 \text{ is a power of 2}\} \cup \{h_n^2 \mid n \geq 1 \text{ is not a power of 2}\}.
\]

**Proof.** It follows from (8.10) that the images of the elements of \(\{t_n \mid \mathcal{L}(n) = 1\} \cup \{h_n^2 \mid \mathcal{L}(n) > 1\}\) form an algebraically independent set in \(\Lambda \otimes F\).

Let \(A\) be the subalgebra of \(\Lambda \otimes F\) generated by the involution class symbol algebra and the 2-regular class symbol algebra. Let \(A_n\) be the \(Z\)-span of \(\{c_\lambda \mid \lambda \vdash n\}\). For \(\lambda\) a partition, and \(i \geq 1\), recall that \(a_i(\lambda)\) denotes the multiplicity of \(i\) as a part of \(\lambda\). The first paragraph shows that \(\dim_F(A \cap A_n)\) is not smaller than the cardinality of the set

\[
\{\lambda \vdash n \mid \mathcal{L}(i) = 1 \text{ or } a_i(\lambda) \text{ is even, for each } i \geq 1\}.
\]

There is an obvious bijection between this set and the set

\[
\{\nu \vdash n \mid \text{ all odd parts of } \nu \text{ equal } 1\}.
\]

This bijection sends \(\lambda \rightarrow \nu\), where

\[
a_i(\nu) = \begin{cases} a_i(\lambda), & \text{if } i \text{ is a power of 2;} \\ 0, & \text{if } i > 1 \text{ is odd;} \\ a_i/2(\lambda)/2, & \text{otherwise.} \end{cases}
\]

It now follows from Proposition 9.7 and Lemma 9.1 that \(A\) coincides with the \(F\)-span of \(\{k_\nu \mid \nu\) is a 4-partition\}. Moreover, \(A\) is generated by the elements of \(\{t_n \mid \mathcal{L}(n) = 1\} \cup \{h_n^2 \mid \mathcal{L}(n) > 1\}\). This completes the proof of the theorem.

\[\square\]
Note 9.9. A similar argument shows that
\[ \{ t_2^m \mid n \geq 0 \} \cup \{ t_2^{m+2m} \mid n > m > 0 \} \cup \{ h_6^n \mid n \geq 1, \mathcal{L}(n) > 2 \} \]
also form a set of algebraically independent generators for the $F$-algebra spanned by \( \{ k_v \mid v \text{ is a 4-partition} \} \).

Corollary 9.10. $t_{14}$ lies in the $F$-algebra generated by $t_1, t_2, t_4, t_6, t_8, t_{10}, t_{12}$.

Proof. We have $\mathcal{L}(14) = 2$. Note 9.9 implies that $t_{14}$ can be written as an $F$-polynomial in $\{ t_1, t_2, t_4, t_8 \} \cup \{ t_6, t_{10}, t_{12} \} \cup \{ h_7 \}$. However (8.10) and (8.11) show that $M(t, h)_{\lambda, \mu} = 0$, for each partition $\lambda$ of 14. The result follows immediately from this.

\[ \square \]

10. Acknowledgement

I thank Arun Ram for alerting me to the existence of Farahat and Higman's results, and for providing me with a copy of Jucys' paper. Thanks are also due to the organizers of the Representations of Finite Groups meeting held at the Mathematisches Forschungsinstitut Oberwolfach, in March 2001.

References


Mathematics Department, National University of Ireland, Maynooth, Co. Kildare, Ireland

E-mail address: jsmurray@maths.may.ie