PRIMITIVE CENTRAL IDEMPOTENTS
OF FINITE GROUP RINGS OF SYMMETRIC GROUPS

HARALD MEYER

ABSTRACT. Let \( p \) be a prime. We denote by \( S_n \) the symmetric group of degree \( n \), by \( A_n \) the alternating group of degree \( n \) and by \( \mathbb{F}_p \) the field with \( p \) elements. An important concept of modular representation theory of a finite group \( G \) is the notion of a block. The blocks are in one-to-one correspondence with block idempotents, which are the primitive central idempotents of the group ring \( \mathbb{F}_q G \), where \( q \) is a prime power. Here, we describe a new method to compute the primitive central idempotents of \( \mathbb{F}_q G \) for arbitrary prime powers \( q \) and arbitrary finite groups \( G \). For the group rings \( \mathbb{F}_p S_n \) of the symmetric group, we show how to derive the primitive central idempotents of \( \mathbb{F}_p S_n \) from the idempotents of \( \mathbb{F}_p S_{n-1} \). Improving the theorem of Osima for symmetric groups we exhibit a new subalgebra of \( \mathbb{F}_p S_n \) which contains the primitive central idempotents. The described results are most efficient for \( p = 2 \). In an appendix we display all primitive central idempotents of \( \mathbb{F}_2 S_n \) and \( \mathbb{F}_4 A_n \) for \( n \leq 50 \) which we computed by this method.

INTRODUCTION AND NOTATION

Let \( p \) be a prime, let \( q = p^s \) for some \( s \in \mathbb{N} \) and let \( G \) be a finite group. For the finite field with \( q \) elements we write \( \mathbb{F}_q \), and \( \mathbb{F}_q G \) denotes the group ring of \( G \) over \( \mathbb{F}_q \). We use \( S_n \) and \( A_n \) for the symmetric and alternating group of degree \( n \), respectively. We write \( \mathbb{Z}_m \) for a cyclic group of order \( m \), and \( \mathbb{Z}_m \wr S_i \) for the wreath product of this group with \( S_i \). We use \( C_G(g) \) for the centralizer of \( g \in G \), and \( C_G(U) \) for the centralizer of \( U \subseteq G \). The centre of a group ring \( FG \) is denoted by \( Z(FG) \) and the radical of the centre by \( \text{Rad}(Z(FG)) \). We use \( \text{Irr}_G \) for the set of irreducible characters of \( G \). For block idempotents, i.e. the primitive central idempotents of \( \mathbb{F}_q G \), therefore it is important to find methods to compute the primitive central idempotents.

The usual method to compute primitive central idempotents is described in [8], Lemma 16.6. For this method it is necessary to compute the character table of \( G \) over the field \( \mathbb{C} \) of complex numbers first. For the symmetric group \( S_{50} \) it is known that there are 204226 characters over \( \mathbb{C} \), but there are only 5 primitive central idempotents of \( \mathbb{F}_2 S_{50} \). Due to the vast amount of data it is not possible to compute...
the character table of $S_{50}$, but it is possible to compute the 5 primitive central idempotents of $\mathbb{F}_2 S_{50}$ using the algorithm described in [12], 2.21. Thus we use the first part to give a description of this algorithm, which works for all finite group rings.

The specialization to symmetric and alternating groups allows us to speed up the algorithm. We do this by proving theoretical results about the group rings $\mathbb{F}_p S_n$ and their primitive central idempotents. To state the results we need the following notation: It is well known that the conjugacy classes of $S_n$ can be indexed by the partitions of $n$. We write $\mu = 1^{\alpha_1}, ..., n^{\alpha_n}$ for the partition

$$\mu = (1, \ldots, 1, 2, ..., 2, \ldots)$$

of $n$. The fact that $\mu$ is a partition of $n$ is abbreviated by $\mu \vdash n$. $C_\mu$ is the conjugacy class of $S_n$ belonging to $\mu$, and $C_\mu^+$ denotes the class sum of $C_\mu$ in $\mathbb{F}_p S_n$.

The $n$-tuple of multiplicities $(\alpha_1, \ldots, \alpha_n)$ appearing in $\mu$ is called the cycle type of the element $\sigma \in C_\mu$. We define

$$W(\mu) := \sum_{i=2}^{n} i \cdot \alpha_i$$

and call it the essential weight of the partition $\mu$. For our purpose it is convenient to ignore the parts equal to 1 in the partition, because an element like $(1, 2, 3) \in S_3$ is also an element of bigger symmetric groups. So we usually write $\mu = 2^{\alpha_2}, ..., n^{\alpha_n}$ for a partition and the corresponding class $C_\mu$ is a class of an arbitrary symmetric group $S_n$ with $n \geq W(\mu)$ depending on the context, i.e. $C_2$ denotes the conjugacy class of transpositions in every symmetric group $S_n$, $n \geq 2$. If we want to emphasize that $C_\mu$ is a class of a certain symmetric group $S_n$ we write $C_\mu|_{S_n}$ and also $C_\mu^+|_{S_n}$ for the class sum in $\mathbb{F}_p S_n$. The class multiplication coefficients $c_{\lambda \mu \nu} \in \mathbb{F}_p$ are defined via

$$C_\lambda^+ C_\mu^+ = \sum_{\nu \vdash n} c_{\lambda \mu \nu} C_\nu^+.$$ 

Here, the $c_{\lambda \mu \nu}$ depend on $n$, but to keep notation simple we usually suppress the $n$. In cases of ambiguity we write $c_{\lambda \mu \nu}|_{S_n}$ for the coefficient of $C_\nu^+|_{S_n}$ in $C_\lambda^+|_{S_n} \cdot C_\mu^+|_{S_n}$.

For an element

$$B = \sum_{g \in G} a_g g$$

of a group ring $\mathbb{F}_q G$ the support is the set $\text{supp } B := \{g \in G \mid a_g \neq 0\}$. The theorem of Osima mentioned above states that the support of primitive central idempotents of $\mathbb{F}_q G$ consists of $p'$-elements, i.e. elements of an order which is not divisible by $p$.

Usually these elements and the corresponding class sums are called $p$-regular, but in symmetric groups this expression is used for partitions $\mu = 1^{\alpha_1}, ..., n^{\alpha_n}$, where $\alpha_i < p$ for $i = 1, \ldots, n$. Thus we avoid using this expression for the classes and use the term ‘$p'$-conjugacy class’ instead for the conjugacy classes of $p'$-elements.

The corresponding partitions are usually called $p$-class regular, but we prefer to call them $p'$-partitions. Furthermore we define $p$-near-regular partitions and conjugacy classes: $\mu = 1^{\alpha_1}, ..., n^{\alpha_n}$ is called $p$-near-regular, when $\alpha_i < p$ for $i = 2, \ldots, n$ and the corresponding conjugacy classes are the $p$-near-regular classes. A theorem of Murray ([13], Corollary 5) states that the vector space

$$Z^G_{p'} := \langle C^+ \mid C \text{ is } p' - \text{conjugacy class of } G \rangle$$
is a subalgebra of the centre of \( \mathbb{F}_q G \), if \( G \) is a symmetric group. We also use the vector spaces
\[
Z^S_{p - \text{reg}} := \langle C^+_\mu \mid \mu \text{ is } p - \text{regular partition of } n \rangle
\]
and
\[
Z^S_{p - \text{nreg}} := \langle C^+ \mid C \text{ is } p - \text{near-regular conjugacy class of } S_n \rangle.
\]
Now we can state our main theorems. Section 2 is devoted to proving the following result.

**Theorem 1.** Let \( m < n \) and \( m \equiv n \mod p \). Let \( \delta \) be the homomorphism of vector spaces defined by

\[
\delta : Z^S_{p'} \rightarrow Z^S_p, \quad \delta(C^+_\mu) := \begin{cases} 
C^+_\mu \mid S_m, & \text{if } W(\mu) \leq m, \\
0, & \text{if } W(\mu) > m.
\end{cases}
\]

Then \( \delta \) is a homomorphism of algebras.

Let \( e_1, \ldots, e_r \) denote the primitive central idempotents of \( \mathbb{F}_p S_n \). Then \( \delta \) has the following properties:

1) If \( \delta(e_i) \neq 0 \), then \( \delta(e_i) \) is a primitive central idempotent of \( \mathbb{F}_p S_m \).
2) For every primitive central idempotent \( f \) of \( \mathbb{F}_p S_m \) there is an \( i \in \{1, \ldots, r\} \) such that \( f = \delta(e_i) \).

We remark that our Theorem 1 is related to Theorem 1.6 of [16].

In Section 3 we prove the following two theorems:

**Theorem 2.** \( Z^S_{p'} \cap Z^S_{p - \text{nreg}} \) is an algebra.

**Theorem 3.** The primitive central idempotents of \( \mathbb{F}_p S_n \) are contained in \( Z^S_{p'} \cap Z^S_{p - \text{nreg}} \), i.e. the support \( \text{supp} e_i \) of a primitive central idempotent \( e_i \) of \( \mathbb{F}_p S_n \) consists of \( p \)-near-regular \( p' \)-conjugacy classes.

These theorems help to speed up the program, so we were able to compute the primitive central idempotents of \( \mathbb{F}_2 S_n \) and \( \mathbb{F}_4 A_n \) for \( n \leq 50 \) using the computer algebra package GAP [2] and a program written in SYMMETRICA [10] provided by A. Kohnert. The Appendix contains the computational results.

We note that there is a theoretical result which provides one of the primitive central idempotents of the group rings \( \mathbb{F}_2 S_n \), if \( n \) is of the form \( n = \frac{m(m+1)}{2} \) with an integer \( m \). R. Gow proves in Theorem 3 of [3] that in this case one of the primitive central idempotents of \( \mathbb{F}_2 S_n \) has the form \( e = C^+ \), where \( C \) is the conjugacy class of elements corresponding to the partition \( (2m - 1, 2m - 5, 2m - 9, \ldots) \) of \( n \). We don’t use this result for our computations for symmetric groups, but we use it to determine the primitive central idempotents of \( \mathbb{F}_4 A_n \), because Gow also proves that this idempotent is the only idempotent of \( \mathbb{F}_2 S_n \) which splits in \( \mathbb{F}_4 A_n \).

1. **Computation of primitive central idempotents of finite group rings**

Let \( F \) be a splitting field for \( G \) of characteristic \( p > 0 \). We already mentioned that the usual method for computing the primitive central idempotents of a group ring \( FG \) uses the character table of \( G \) over \( C \). But what if we do not know the character table? Can we compute the idempotents within \( FG \)? The first observation is that we can assume \( F \) to be finite because every group has a finite splitting field of characteristic \( p \) according to a theorem of Brauer ([6], Theorem VII.2.6). Now if
FG is finite and \( B \in Z(FG) \), then the sequence \( (B^n)_{n \in \mathbb{N}} \) has to be periodic, i.e. there exist \( r, m \in \mathbb{N} \) such that \( B^r = B^{r+m} \). This idea can be used to construct central idempotents and leads to Algorithm [7] which is already described in [12]. The following theorem ([12], Satz 2.1) is the foundation of the algorithm. As we will need it in section 2, we prove it here again. Now let \( F \) be an arbitrary finite field of characteristic \( p > 0 \) and let \( \overline{F} \) denote the algebraic closure of \( F \). We will mention it explicitly if we assume \( F \) to be a splitting field for \( G \) or for \( Z(FG) \).

**Theorem 4.** Let \( B \in Z(FG) \) and let \( m \in \mathbb{N} \) be such that \( B^r = B^{r+m} \), for all \( r \in \mathbb{N} \) suitable large. Choose \( r = l \cdot m \), where \( l \neq 0 \) and suppose that \( m = p^s \cdot d \), where \( s \geq 0 \) and \( p \nmid d \). Let \( \zeta \in \overline{F} \) be a primitive \( d \)-th root of unity and put

\[
f_k := d^{-1} \sum_{i=0}^{d-1} (\zeta^k)^i B^{r+p^s \cdot i}
\]

for \( 0 \leq k \leq d-1 \). Then \( f_k = 0 \) or \( f_k \) is a central idempotent of \( F(\zeta^k)G \), the group ring of \( G \) over the field \( F(\zeta^k) \). For \( k \neq n \) we have \( f_kf_n = 0 \) in \( F(\zeta^k)G \). If \( B^r \neq 0 \), then there is a \( k \) such that \( f_k \neq 0 \) and \( B^r \) is a central idempotent itself.

**Proof.** For \( 0 \leq k \leq d-1 \) we define

\[
D_k := \sum_{i=0}^{d-1} (\zeta^k)^i B^{r+p^s \cdot i}.
\]

Now let \( w := \zeta^k \). Then we have \( w^d = 1 \) and get

\[
w^j B^{r+p^s \cdot j} \cdot D_k = \sum_{i=0}^{d-1} w^{i+j} B^{r+l \cdot m+p^s \cdot (i+j)} = D_k
\]

using the periodicity of the sequence \( (B^n)_{n \in \mathbb{N}} \). Hence we obtain \( D_k^2 = d \cdot D_k \), so \( f_k = d^{-1} D_k \) is 0 or a central idempotent in \( F(\zeta^k)G \).

If \( 0 \leq n \leq d-1 \) and \( n \neq k \), then

\[
D_k D_n = \sum_{i=0}^{d-1} (\zeta^k)^i (\zeta^m)^{-i} \left[ (\zeta^m)^i B^{r+p^s \cdot i} D_n \right] = D_n \cdot \sum_{i=0}^{d-1} (\zeta^{k-n})^i = 0.
\]

Therefore the \( f_k \) with \( f_k \neq 0 \) are orthogonal idempotents.

Finally, if \( B^r \neq 0 \), then

\[
\sum_{k=0}^{d-1} D_k = dB^r \neq 0,
\]

i.e. there is an \( f_k \neq 0 \). As the \( f_k \) are orthogonal we obtain

\[
(B^r)^2 = \left( \sum_{k=0}^{d-1} f_k \right)^2 = \sum_{k=0}^{d-1} f_k^2 = \sum_{k=0}^{d-1} f_k = B^r.
\]

A similar computation leads to the following corollary ([12], 2.3):

**Corollary 5.** Let \( e_1, \ldots, e_r \) be the primitive central idempotents of \( FG \). Then the span

\[
\langle e_1, \ldots, e_r \rangle_F = \{ B \in Z(FG) \mid B^{[F]} = B \}.
\]

The following theorem (see [12], Satz 2.17) is the foundation for our algorithm:
Theorem 6. Let $F$ be a splitting field for $Z(FG)$. Let $C_1, \ldots, C_k$ be the $p'$-conjugacy classes of $G$ and let $e_1, \ldots, e_r$ be the primitive central idempotents of $FG$. Then there is an $n_0 \in \mathbb{N}$ such that
\[ \langle e_1, \ldots, e_r \rangle_F = \left\langle (C_1^+)^{p_n}, \ldots, (C_k^+)^{p_n} \right\rangle_F \]
for all $n \geq n_0$.

Proof. Let $C_{k+1}, \ldots, C_c$ be the $p$-singular conjugacy classes of $G$, i.e. the classes of elements whose order is divisible by $p$. As the class sums $C_1^+, \ldots, C_c^+$ form a basis of $Z(FG)$, we get
\[ \langle e_1, \ldots, e_r \rangle_F = \left\langle (C_1^+)^{p_n}, \ldots, (C_c^+)^{p_n} \right\rangle_F \]
for all $n \in \mathbb{N}$ suitable large by [11], p. 434 (an elementary proof can be found in [12], Satz 2.11). According to the theorem of Osima ([8], Theorem 23.6) we know $\langle e_1, \ldots, e_r \rangle_F \subset \langle C_1^+, \ldots, C_k^+ \rangle_F$. Now let $n_0$ be a multiple of $|F|$, which is suitably large. Then
\[ \varphi : Z(FG) \longrightarrow Z(FG), B \longmapsto B^{p_n} \]
is a homomorphism of vector spaces, hence we obtain
\[ \langle e_1, \ldots, e_r \rangle_F = \varphi(\langle e_1, \ldots, e_r \rangle_F) \subset \left\langle (C_1^+)^{p_n}, \ldots, (C_k^+)^{p_n} \right\rangle_F \]
\[ \subset \left\langle (C_1^+)^{p_n}, \ldots, (C_c^+)^{p_n} \right\rangle_F = \langle e_1, \ldots, e_r \rangle. \]
Thus we get our statement for all $n \geq n_0$.

This leads to the following algorithm for computing primitive central idempotents of finite group rings, which can be found in [12], 2.21. But the algorithm in [12] contains some minor gaps, which we fill here.

Algorithm 7. Let $G$ be a finite group and $p$ a prime. Let $F$ be a splitting field for $Z(FG)$ with char $F = p$. The computation of the primitive central idempotents of $FG$ can be accomplished by the following steps:

1) Compute the $p'$-conjugacy classes $C_1, \ldots, C_c$ of $G$.
2) For $i = 1, \ldots, b$, do the following: By computing successive powers of the class sum $C_i^+$, determine the minimal integers $r_1, m_i \geq 1$ such that $(C_i^+)^{r_1} = (C_i^+)^{r_1 + m_i}$, and $r_1$ is a multiple of $m_i$. Write $m_i = p^{s_i} \cdot d_i$, where $s_i \geq 0$ and $p \not| d_i$.
3) Compute the idempotents
\[ f_k^{(i)} := d_i^{-1} \sum_{j=0}^{d_i-1} (\zeta_i^k)^j (C_i^+)^{r_1 + p^{s_i} \cdot j} \]
for $1 \leq i < b$ and $0 \leq k \leq d_i - 1$, where $\zeta_i$ denotes a primitive $d_i$-th root of unity in a suitable extension of the field $\mathbb{F}_p$.
4) Choose a basis $f_1, \ldots, f_r$ of the mostly linear dependent set
\[ \left\{ f_k^{(i)} \mid 1 \leq i \leq b, \ 0 \leq k \leq d_i - 1 \right\}. \]
If $r = 1$, then $f_1$ is the only central idempotent of $FG$ and the computation is finished. For $r > 1$ we have to accomplish one more step:
5) For $i = 1, \ldots, r - 1$ do:
   \{ For $j = i + 1, \ldots, r$ do:
Then and thus \(C_m\) according to [11], p. 434, there is an Corollary 5 we obtain
\[
\text{Rad}(Z(FG)) = \left\langle C_1^+ - (C_1^+)p^n, ..., C_c^+ - (C_c^+)p^n \right\rangle \quad \text{(as a vector space)}.
\]

**Theorem 8.** Let \(F\) be a finite splitting field of characteristic \(p\) for \(Z(FG)\) with \(|F| = p^n\). Let \(C_1, ..., C_c\) be the conjugacy classes of \(G\) (here we need them all). Then
\[
\text{Rad}(Z(FG)) = \left\langle C_1^+ - (C_1^+)p^n, ..., C_c^+ - (C_c^+)p^n \right\rangle \quad \text{(as a vector space)}.
\]

**Proof.** Let \(e_1, ..., e_r\) be the primitive central idempotents of \(FG\). Let \(i \in \{1, ..., c\}\). According to [11], p. 434, there is an \(m \in \mathbb{N}\) with \((C_i^+)p^m \in \langle e_1, ..., e_r \rangle\). Using Corollary 5 we obtain
\[
\left(1 - (C_i^+)p^n\right)p^m = (C_i^+)p^m - \left((C_i^+)p^n\right)p^m = (C_i^+)p^m - (C_i^+)p^m = 0
\]
and thus \(C_i^+ - (C_i^+)p^n \in \text{Rad}(Z(FG))\).
Now we consider the map
\[ \varphi : Z(FG) \longrightarrow Z(FG), \quad \varphi(x) := x - x^{p^n}. \]
\( \varphi \) is a homomorphism of vector spaces. According to Corollary 5 the kernel is \( \langle e_1, \ldots, e_r \rangle \). The image is a subset of \( \text{Rad}(Z(FG)) \). By [8], Lemma 25.1, we obtain our statement.

**Remark 9.** We keep the notation of the last theorem. The proof of the preceding theorem also provides a method to compute the projection of an arbitrary element \( B \in Z(FG) \) to the vector spaces \( \langle e_1, \ldots, e_r \rangle \) and \( \text{Rad}(Z(FG)) \): Choose \( m = k \cdot n \), such that \( B^{p^m} \in \langle e_1, \ldots, e_r \rangle \) (this is true if \( p^m > c^n \)). Then \( B - B^{p^m} \in \text{Rad}(Z(FG)) \) and \( B - B^{p^m} \) are the projections of \( B \) to \( \langle e_1, \ldots, e_r \rangle \) and \( \text{Rad}(Z(FG)) \), respectively.

In the following sections we will see how we can improve the algorithm for symmetric groups.

### 2. Connections between primitive central idempotents of \( \mathbb{F}_p S_n \) for different \( n \)

The methods developed in the first section work for all finite groups and fields of characteristic \( p \), even in the case where \( p \nmid |G| \). But to apply the algorithm successfully to bigger symmetric groups we have to speed up the algorithm. In the algorithm we have to multiply sums of class sums. How can we do that quickly? If \( C_1, \ldots, C_m \) are the conjugacy classes of \( S_n \), then we get
\[
C_i^+ C_j^+ = \sum_{k=1}^{m} c_{ijk} C_k^+ \]
with coefficients \( c_{ijk} \in \mathbb{F}_p \). According to [3], Theorem 4.6, we know that
\[
c_{ijk} \equiv \frac{|C_i||C_j|}{[S_n]} \sum_{\chi \in \text{Irr}(S_n)} \chi(g_i) \chi(g_j) \chi(g_i^{-1}) \chi(1) \mod p,
\]
where \( g_i \in C_i \) for \( i \in \{1, \ldots, m\} \). So we can compute the class multiplication coefficients \( c_{ijk} \), if we know some parts of the character table of \( S_n \). Character values for symmetric groups can be computed very fast with the Murnaghan-Nakayama formula, see [7], 2.4.7, even for \( S_{50} \). But the number of class multiplication coefficients we have to compute must not be too big, if we want to get results for a group like \( S_{50} \). So we need theoretical results to reduce the work. A first result in this direction is a theorem of Murray ([14], Corollary 5): \( Z_{p'}^{S_n} \) is an algebra. So if we multiply class sums of \( p' \)-conjugacy classes we only need to compute the coefficients of \( p' \)-class sums. Due to Algorithm [7] we only need to consider \( p' \)-conjugacy classes, so we can use this result for all our computations. Here and in the following sections we will prove some more theorems which allow us to reduce the number of coefficients we need to compute.

The computations are simplified by the fact that \( \mathbb{F}_p \) is a splitting field for \( S_n \) according to [7], 2.1.12, so we can choose \( F = \mathbb{F}_p \).
Lemma 10. Let \( n > p \) and let \( \delta_n \) be the homomorphism of vector spaces defined by

\[
\delta_n : Z_{p^n}^S \longrightarrow Z_{p^n}^{S_{n-p}}, \quad C_\mu \mapsto \begin{cases} C_\mu |_{S_{n-p}}, & \text{if } W(\mu) \leq n - p, \\ 0, & \text{if } W(\mu) > n - p. \end{cases}
\]

Then \( \delta_n \) is a homomorphism of algebras.

Proof. We write \( S_{n-p} \) for the subgroup of \( S_n \) containing the permutations, which fix the numbers \( n - p + 1, \ldots, n \). Let \( \tau := (n - p + 1, \ldots, n) \in S_n \). Then for the centralizer we get \( C_{S_n}(\tau) = S_{n-p} \times \langle \tau \rangle \). Now let

\[
\text{Br}_\tau : Z(\mathbb{F}_p S_n) \longrightarrow Z(\mathbb{F}_p C_{S_n}(\tau))
\]

be the Brauer-homomorphism (see [15], Theorem 4.9). \( \text{Br}_\tau \) is a homomorphism of algebras with \( \text{Br}_\tau(C_\mu) = (C_\mu \cap C_{S_n}(\tau))^+ \). Thus \( \delta_n \) is the restriction of \( \text{Br}_\tau \) to \( Z_{p^n}^S \), and is therefore a homomorphism of algebras, by [14, Corollary 5].

Remark 11. If we define the homomorphism \( \delta_n \) of the preceding lemma for \( Z(\mathbb{F}_p S_n) \) we usually do not get a homomorphism of algebras: If \( C_\tau \) denotes the conjugacy class of \( \tau \) in \( S_n \), then \( C_\tau \cap C_{S_n}(\tau) \) is not contained in the subgroup \( S_{n-p} \) of \( C_{S_n}(\tau) \) and the same problem occurs for conjugacy classes of partitions containing \( p \). For example for the conjugacy class \( C_2 \) of transpositions it is easy to see that \((C_2^+)^2 = C_1^+ + C_3^+\) for \( n \equiv 2, 3 \mod 4 \) and \((C_2^+)^2 = C_3^+\) for \( n \equiv 0, 1 \mod 4 \).

Now we can prove our Theorem [1]

Proof of Theorem [1]. We keep the notation of Lemma 10. If \( m = n - k \cdot p \), then \( \delta \) is the composition of \( \delta_n, \delta_{n-p}, \ldots, \delta_{n-(k-1)p} \) and thus is a homomorphism of algebras. Therefore \( \{\delta(e_1), \ldots, \delta(e_r)\}\} \setminus \{0\} \) is a set of central orthogonal idempotents. We prove the remaining statements in several steps:

1) For every central idempotent \( f \in Z(\mathbb{F}_p S_m) \) there is a central idempotent \( e \in Z(\mathbb{F}_p S_n) \) with \( \delta(e) = f \):

We define a homomorphism \( \Delta \) of vector spaces by

\[
\Delta : Z(\mathbb{F}_p S_m) \longrightarrow Z(\mathbb{F}_p S_n), \quad C_\mu |_{S_m} \mapsto C_\mu |_{S_n}
\]

and put \( F := \Delta(f) \). Now let \( r, m \in \mathbb{N} \) such that \( Fr = Fr^m \) and \( r = l \cdot m \) for an \( l \in \mathbb{N} \). Let \( m = p^s \cdot d \) with \( p \nmid d \). We set

\[
e := d^{-1} \sum_{i=0}^{d-1} F_{p^s+i}.
\]

Then \( e \) is 0 or a central idempotent of \( \mathbb{F}_p S_n \) by Theorem [1]. We obtain

\[
\delta(e) = d^{-1} \sum_{i=0}^{d-1} \delta(F_{p^s+i}) = d^{-1} \sum_{i=0}^{d-1} f = f \neq 0,
\]

so \( e \neq 0 \) and \( \delta(e) = f \).

2) For every primitive central idempotent \( f \in Z(\mathbb{F}_p S_m) \) there is \( i \in \{1, \ldots, r\} \) with \( f = \delta(e_i) \):

By 1) there exists a central idempotent \( e \) of \( Z(\mathbb{F}_p S_n) \) with \( \delta(e) = f \). Now let \( e = \sum_{i=1}^{k} e_i \) be the decomposition of \( e \) in primitive central idempotents of
Then we have
\[ f = \delta(e) = \sum_{i=1}^{k} \delta(e_i), \]
and as \( \delta \) is a homomorphism of algebras, the \( \delta(e_i) \) are 0 or central orthogonal idempotents of \( Z(\mathbb{F}_p S_n) \). But \( f \) is primitive, therefore there is an \( i_0 \in \{1, \ldots, k\} \) such that \( \delta(e_{i_0}) \neq 0, \delta(e_j) = 0 \) for \( j \neq i_0 \) and we obtain \( f = \delta(e_{i_0}) \).

3) If \( e \in \{e_1, \ldots, e_r\} \) and \( \delta(e) = f \neq 0 \), then \( f \) is a primitive central idempotent of \( \mathbb{F}_p S_m \):

We assume that \( f \) is not primitive as a central idempotent. Then let \( f = \sum_{i=1}^{k} f_i \) be a decomposition of \( f \) in primitive central idempotents. By 2) there are primitive central idempotents \( e_1, \ldots, e_k \) of \( \mathbb{F}_p S_n \) with \( \delta(e_i) = f_i \). As \( \delta(e) = f \neq f_1 = \delta(e_1) \) we have \( e \neq e_1 \). Now both \( e \) and \( e_1 \) are different primitive central idempotents of \( \mathbb{F}_p S_n \), so they are orthogonal. Hence we obtain
\[ 0 = \delta(e \cdot e_1) = \delta(e) \cdot \delta(e_1) = f \cdot f_1 = f_1, \]
a contradiction.

Theorem allows us to write down the primitive central idempotents of \( \mathbb{F}_p S_n \) in a very compact way: For example, it will do to write down the primitive central idempotents of \( \mathbb{F}_2 S_{50} \) and \( \mathbb{F}_2 S_{48} \) to know the primitive central idempotents of \( \mathbb{F}_2 S_n \) for all \( n \leq 50 \). Furthermore our computations in connection with Theorem lead to statements like the following:

\[ C_{11} \notin \text{ supp } e \text{ for all primitive central idempotents } e \text{ of } \mathbb{F}_2 S_n, n \in \mathbb{N}, \]
because \( C_{11} \) is neither included in the support of the primitive central idempotents of \( \mathbb{F}_2 S_{11} \) nor in the according support in \( \mathbb{F}_2 S_{12} \).

For the computation of idempotents the most important part of Theorem is the fact that \( \delta \) is a homomorphism of algebras because this provides the following corollary:

**Corollary 12.** Let \( \lambda, \mu, \nu \) be \( \nu' \)-partitions of \( n \) with \( W(\mu) \geq W(\lambda) \). Let \( m \equiv n \mod p \) be minimal with \( W(\nu) \leq m \). Then for the class multiplication coefficient \( c_{\lambda\mu\nu}|_{S_n} \) we have
\[ c_{\lambda\mu\nu}|_{S_n} = \begin{cases} 
0, & \text{if } W(\nu) \leq W(\mu) - p \text{ or } W(\nu) > W(\mu) + W(\lambda), \\
\lambda \mu \nu|_{S_m}, & \text{if } W(\mu) - p < W(\nu) \leq W(\mu) + W(\lambda). 
\end{cases} \]

**Proof.** If \( \pi \in C_\lambda \) and \( \sigma \in C_\mu \), then \( \pi \) moves \( W(\lambda) \) points and \( \sigma \) moves \( W(\mu) \) points, so \( \pi \sigma \) moves at most \( W(\lambda) + W(\mu) \) points. Thus if \( W(\nu) > W(\lambda) + W(\mu) \), then obviously \( c_{\lambda\mu\nu}|_{S_n} = 0 \). Now let \( W(\nu) \leq W(\mu) - p \) and let \( \delta_n \) be as in Lemma As \( \delta_n \) is a homomorphism and \( \delta_n(C_\mu^+) = 0 \), but \( \delta_n(C_\nu^+) \neq 0 \), it follows that \( c_{\lambda\mu\nu}|_{S_n} = 0 \), in this case. The remaining statement is clear by applying \( \delta_n \).

3. A FURTHER SUBALGEBRA OF \( \mathbb{F}_p S_n \) CONTAINING THE IDEMPOTENTS

To prove Theorem [2] we need the following version of a lemma proved in [1], which is just a formulation of the statement that the Brauer homomorphism is an algebra homomorphism. Additionally it is a formulation of another theorem of Osima ([15 Theorem 4.1]): If \( C \) is a conjugacy class of \( G \) and \( g \in C \), then a
Sylow-$p$-subgroup of $C_G(g)$ is called a defect group of $C$. If $Z_D(FG)$ denotes the $F$-span of all class sums $C^+$ such that the defect groups of $C$ are contained in a $G$-conjugate of a certain $p$-subgroup $D$ of $G$, then $Z_D(FG)$ is an ideal of $Z(FG)$. But Lemma [13] is more detailed specifying elements and making a statement about the Sylow-$p$-subgroups of these elements. In the proof of Theorem [2] we apply this more detailed version of the theorem of Osima.

**Lemma 13.** Let $G$ be a finite group. Let $C_1, ..., C_s$ be the conjugacy classes of $G$ and let $C^+_1, ..., C^+_s$ be the corresponding class sums in $ZG$. Now let

$$C^+_i C^+_j = \sum_{k=1}^{s} a_{ijk} C^+_k.$$ 

If $a_{ijk} \neq 0 \mod p$, then for every element $z \in C_i$ and every Sylow-$p$-subgroup $P_z$ of $C_G(z)$ there are elements $x \in C_i$ and $y \in C_j$ as well as Sylow-$p$-subgroups $P_x$ of $C_G(x)$ and $P_y$ of $C_G(y)$, such that $xy = z$ and $P_z \leq P_x \cap P_y$.

**Proof.** See the proof of [1], Lemma 87.9.

**Proof of Theorem 2.** $Z_p^{S_n}$ is an algebra by Corollary 5 of [14]. Now let $(a_1, ..., a_n)$ and $(b_1, ..., b_n)$ be cycle types of $p$-near-regular $p'$-partitions $\sigma$ and $\tau$. We have to show that $C_{\sigma} \not\subseteq \text{supp}(C^+_{\sigma} C^+_{\tau})$ for $p'$-classes $C_{\sigma}$, which are not $p$-near-regular.

Let $(c_1, ..., c_n)$ be the cycle type of $\pi$. If $c_1 \geq p$ we can apply the Brauer-homomorphism and get

$$\text{Br}_{((1, ..., p))}(C^+_{\pi}) = C^+_{\pi} \neq 0,$$

where $\pi'$ has cycle type $(c_1 - p, c_2, ..., c_{n-p})$. Thus we get $c_{\sigma \tau \pi} | s_n = c_{\sigma' \tau' \pi'} | s_{n-p}$, where $C^+_{\sigma'} = \text{Br}_{((1, ..., p))}(C^+_{\sigma})$ and analogously for $C^+_{\tau'}$. Moreover, $C_{\sigma'}$ and $C_{\tau'}$ are $p$-near-regular $p'$-classes. Therefore we can assume that $c_1 < p$.

Now let $z \in C_\pi$ and $x \in C_\sigma$, $y \in C_\tau$ such that $xy = z$. It is well known that

(*)

$$C_{S_n}(x) \cong S_{a_1} \times (\mathbb{Z}_{a_2} \wr S_{a_2}) \times ... \times (\mathbb{Z}_{a_k} \wr S_{a_k})$$

and $|Z_k \wr S_k| = a_k! \cdot k^{a_k}$ ([17], 3.2.13). As $a_k < p$ for $k \geq 2$ and $a_k = 0$ for $p | k$ we obtain that $p$ divides $|C_{S_n}(x)|$ if and only if $a_1 \geq p$.

Hence the Sylow-$p$-subgroup of $C_{S_n}(x)$ is a subgroup of the subgroup isomorphic to $S_{a_1}$. This subgroup is the symmetric group on the set of numbers which are fixed by $x$. The same is true for $y$. Now let $P_x$, $P_y$ be Sylow-$p$-subgroups of $C_{S_n}(x)$, $C_{S_n}(y)$, respectively and let $P := P_x \cap P_y$. Then all numbers which are moved by an element of $P$ are fixed by $x$ and $y$ and therefore are fixed by $z$. But $c_1 < p$, so $z$ fixes less than $p$ numbers, i.e. no permutation of the fixed points of $z$ has order $p$. Thus we obtain $P_x \cap P_y = \{1\}$.

If $P_z$ is a Sylow-$p$-subgroup of $C_{S_n}(z)$, then $|P_z| > 1$ because there is an $i \geq 2$ such that $c_i \geq p$. Thus we obtain $P_z \not\subseteq P_x \cap P_y$ for all $x \in C_{\sigma}$, $y \in C_{\tau}$ with $xy = z$. By Lemma [14] we get $C_{\pi} \not\subseteq \text{supp}(C^+_{\sigma} C^+_{\tau})$.

Table 1 shows the dimension of $U_p := Z_{p^{S_n}} \cap Z_{p^{S_n}}$ for $p = 2, 3$ in comparison with the dimensions of $Z(F_p S_n)$ and $Z_{p^{S_n}}$.

The following remark is a special case of a more general theorem of Osima already mentioned above ([14], Theorem 4.1).

**Remark 14.** $Z_{p^{S_n}} \cap Z_{p^{S_n}}$ is an algebra.

For the rest of this section we fix the following notation:
As orbit of choice of $x_i$ Let $x$ be as in Notation 15. By $\sigma = (a_1, ..., a_n)$ we denote the cycle type of a $p'$-partition with $a_i \geq p$ for an $i \geq 2$, $a_j < p$ for $j < i$. $C_\sigma$ denotes the conjugacy class of elements of cycle type $\sigma$ in $S_n$. Thus the $p'$-partition $\sigma$ is not $p$-regular, but elements in $C_\sigma$ fix at most $p - 1$ symbols in $\{1, ..., n\}$.

The idea of the proof of Theorem 13 is the following: If the support of an idempotent $e$ contains $C_\sigma$, then the support also contains $\text{supp}(C_\sigma^+)$. The support of $(C_\sigma^+)^p$ can contain classes $C_\mu$, where $\mu$ is not $p$-regular. But if $(b_1, ..., b_n)$ is the cycle type of such a class $C_\mu$ and if $b_k \geq p$, then $k > i$, i.e. the position where the ‘irregularity’ occurs, grows. So a class $C_\sigma$ in the support of $e$ with a ‘minimal position of irregularity’ is not contained in the support of $e^p = e$, a contradiction.

For the proof of Theorem 13 we first collect the necessary information about $C_\sigma$ in several lemmas. We start with a lemma about the centralizers of an element of cycle type $\sigma$.

**Lemma 16.** Let $x \in C_\sigma$ and let $y \in C_{S_n}(x)$ have order $p$. Then $y$ is a product of $i$ or more commuting $p$-cycles.

**Proof.** As $y$ centralizes $x$, it permutes the orbits of $x$ on $\{1, ..., n\}$. Let $O$ be one orbit of $x$ which is not fixed by $y$. Then $O, yO, ..., y^{p-1}O$ are distinct orbits of $x$. Thus the cycle decomposition of $x$ consists of at least $p$ cycles of length $|O|$. Our choice of $x$ gives $|O| \geq i$, and $y$ is a product of at least $|O|$ commuting $p$-cycles.

**Corollary 17.** Let $\sigma$ be as in Notation 15, let $C_\mu \subset S_n$ be a $p'$-conjugacy class and let $\lambda = (c_1, ..., c_n)$ be the cycle type of a $p'$-partition with $C_\lambda \subset \text{supp}(C_\mu^+ C_\mu^+)$. Then $c_j < p$ for $2 \leq j < i$.

**Proof.** Let $x \in C_\mu$, $y \in C_\sigma$ and $z \in C_\lambda$. Suppose that $z$ contains at least $p$ commuting $j_0$-cycles in its cycle decomposition, where $j_0 < i$. Then an element permuting $p$ of the orbits of $z$ on $\{1, ..., n\}$ of length $j_0$ is an element in $C_{S_n}(z)$, and its cycle decomposition consists of $j_0$ commuting $p$-cycles. Thus every Sylow-$p$-subgroup $P_z$ of $C_{S_n}(z)$ contains an element of this cycle type. But $C_{S_n}(x)$ does not contain an element of such a cycle type according to Lemma 10. Hence if $P_z, P_y$ are Sylow-$p$-subgroups of $C_{S_n}(x), C_{S_n}(y)$, respectively, then $P_z \not\subset P_z \cap P_y$ and by Lemma 13 we obtain $C_\lambda \not\subset \text{supp}(C_\mu^+ C_\mu^+)$.

We remark that we just proved that a defect group of $C_\mu$ is not contained in a defect group of $C_\mu$ up to conjugacy, so Corollary 17 also follows by the theorem of Osima mentioned above (15, Theorem 4.1)).

**Lemma 18.** Let $\pi$ be a product of $i$ commuting $p$-cycles, where $i$ is coprime to $p$. Then all $p'$-elements of the same cycle type contained in $C_{S_{p-1}}(\pi)$ are conjugate in $C_{S_{p-1}}(\pi)$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>dim $Z(F_p S_n)$</th>
<th>dim $Z_{p^n}^S$</th>
<th>dim $U_2$</th>
<th>dim $Z_{p^n}^S$</th>
<th>dim $U_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>42</td>
<td>10</td>
<td>7</td>
<td>22</td>
<td>18</td>
</tr>
<tr>
<td>20</td>
<td>627</td>
<td>64</td>
<td>30</td>
<td>202</td>
<td>129</td>
</tr>
<tr>
<td>30</td>
<td>5604</td>
<td>296</td>
<td>95</td>
<td>1225</td>
<td>622</td>
</tr>
<tr>
<td>40</td>
<td>37338</td>
<td>1113</td>
<td>260</td>
<td>5834</td>
<td>2405</td>
</tr>
<tr>
<td>50</td>
<td>204226</td>
<td>3658</td>
<td>632</td>
<td>23603</td>
<td>8008</td>
</tr>
</tbody>
</table>

**Table 1.**
Proof. \( C_{S_p}^i(\pi) \cong Z_p \wr S_i \) (see (\( \ast \))) is a semidirect product of a \( p \)-group (generated by the cycles of \( \pi \)) and a copy of \( S_i \). Using the explicit description of the conjugacy classes of \( Z_p \wr S_i \) in \([9], 3.2, 3.13\) we can deduce that every \( p' \)-element of \( C_{S_p}^i(\pi) \) is conjugate in \( C_{S_p}^i(\pi) \) to an element of the copy of \( S_i \). Therefore the projection \( C_{S_p}^i(\pi) \rightarrow S_i \) induces a bijection between the \( p' \)-classes of the two groups. Due to \([7], 4.1.18, 4.2.17\) this bijection maps a \( p' \)-element of cycle type \((p\lambda_1, \ldots, p\lambda_i)\) to an element of cycle type \((\lambda_1, \ldots, \lambda_i)\). Thus we obtain our result.

Corollary 19. We keep the notation of Lemma 18 Let \( g \in C_{S_p}^i(\pi) \) be a \( p' \)-element and let \( \chi \in \text{Irr}_{C_{S_p}^i(\pi)} \). Then \( \chi(g) \in \mathbb{Z} \).

Proof. Let \( m \in \mathbb{N} \) with \( \text{gcd}(m, \text{ord} g) = 1 \). By Lemma 18 the elements \( g \) and \( g^m \) are conjugate in \( C_{S_p}^i(\pi) \), thus we obtain \( \chi(g) \in \mathbb{Z} \) for \( \chi \in \text{Irr}_{C_{S_p}^i(\pi)} \) using \([3], V.13.7.b\) and \([4], 6.3b, 6.4a\).

Remark 20. With the notation of Lemma 18 the vector space \( Z_{p'}^{C_{S_p}^i(\pi)} \) is an algebra.

Proof. \( Z_{p'}^{S_p} \) is an algebra by Corollary 5 of \([13]\), and the Brauer homomorphism

\[
\text{Br}(\pi) : Z(\mathbb{F}_p S_p) \rightarrow Z(\mathbb{F}_p C_{S_p}^i(\pi))
\]

is a projection. By Lemma 18 this projection is surjective: If \( C \) is a \( p' \)-class of \( S_p \), then \( C \cap C_{S_p}^i(\pi) = 0 \) or \( C \cap C_{S_p}^i(\pi) \) is a \( p' \)-class of \( C_{S_p}^i(\pi) \).

Lemma 21. Let \( \pi \) and \( i \) be as in Lemma 18 Let \( C \subset C_{S_p}^i(\pi) \) be the conjugacy class of elements of cycle type \((c_1, \ldots, c_{pi})\), where \( c_i = p \) and \( c_j = 0 \) for \( j \neq i \). Then \((C^+)^2 = 0 \) in \( \mathbb{F}_p C_{S_p}^i(\pi) \).

Proof. \( \text{supp}(C^+) \) consists of \( p' \)-elements according to Remark 20 Now let \( D \subset C_{S_p}^i(\pi) \) be a \( p' \)-conjugacy class. According to \([4], 4.6\), the coefficient \( a_{CCD} \) of \( D^+ \) in \((C^+)^2 \subset Z C_{S_p}^i(\pi) \) is

\[
a_{CCD} = \frac{|C|}{|C_{S_p}^i(\pi)|} \sum_{\chi \in \text{Irr}_{C_{S_p}^i(\pi)}} \chi^2(g) \cdot \frac{\chi(h^{-1})}{\chi(1)},
\]

where \( g \in C \) and \( h \in D \). By Corollary 19 we know that \( \chi(g) \) and \( \chi(h^{-1}) \) are integers. Using \([9], 3.9\), we obtain

\[
\frac{|C|}{|C_{S_p}^i(\pi)|} = \frac{(p^{i-1} \cdot (i-1)!)^2}{p^i \cdot i!} = \frac{p^{i-2}(i-1)!}{i}.
\]

The group \( C_{S_p}^i(\pi) \cong (\mathbb{Z}_p)^i \rtimes S_i \) contains an abelian normal subgroup of order \( p^i \), so by a theorem of Ito \((4), 19.9\) we get

\[
\chi(1) \mid |C_{S_p}^i(\pi) : (\mathbb{Z}_p)^i| = \frac{p^i \cdot i!}{p^i} = i!.
\]

As \( p \mid i \) this provides \( a_{CCD} = 0 \mod p \) for \( i > 2 \). For \( i = 2 \) the centralizer of \( \pi \) is a group of order \( 2p^2 \). Therefore the product of two elements of \( C \) is an element of the Sylow-\( p \)-subgroup of \( C_{S_p}^i(\pi) \), i.e. \( C \nsubseteq \text{supp}(C^+)^2 \). As \( p \mid |C| \) provides \( 1 \nsubseteq \text{supp}(C^+)^2 \), we obtain \( a_{CCD} = 0 \mod p \) for the case \( i = 2 \), because \( \{1\} \) and \( C \) are the only \( p' \)-classes of \( C_{S_p}^i(\pi) \) in this case.
We remark that the fact that $C^+$ is nilpotent can already be deduced from [13, 4.7].

**Lemma 22.** Let $\sigma, i$ be as in Notation [15] and let $\mu = (b_1, ..., b_n)$ be the cycle type of a $p'$-partition with $b_i \geq p$. Then $C_\mu \not\subseteq \text{supp}(C^+_p)$.

**Proof.** There are elements $x \in C_\sigma$ and $y \in C_\mu$ such that
\[
\pi = (1, 2, ..., p)(p + 1, ..., 2p)\cdot (i - 1)p + 1, ..., ip)
\]
is an element of $CS_n(x)$ and of $CS_n(y)$. We apply the Brauer-homomorphism
\[
\text{Br}_{(\pi)} : Z(F_p, S_n) \longrightarrow Z(F_p, CS_n(\pi))
\]
and get
\[
C_\mu \subset \text{supp}(C^+_\sigma)^p \iff \text{supp}\left(\text{Br}_{(\pi)}(C_\mu)^p \subset \text{supp}(\text{Br}_{(\pi)}(C^+_\sigma))^p\right),
\]
as $\text{Br}_{(\pi)}(C_\mu)^p \neq 0$.

The coefficient $a_\mu$ of $C^+_\mu$ in $(C^+_\sigma)^p \in \mathbb{Z}S_n$ is the number of solutions $(g_1, ..., g_p)$ of the equation
\[
g_1 \cdot \cdot \cdot g_p = y,
\]
where $g_i \in C_\sigma \cap CS_n(\pi)$. Using the decomposition $CS_n(\pi) \cong CS_{n-i} \times S_{n-i}$ we can write $g_i = g_i \cdot \cdot \cdot g_i$ and $y = y_1 \cdot \cdot \cdot y_2$ with $g_i \cdot \cdot \cdot g_i \in C_\sigma$ and $g_i \cdot \cdot \cdot g_i \in S_{n-i}$ and obtain equations
\[
g_{1,1}g_{2,1}...g_{p,1} = y_1, \quad g_{1,2}...g_{p,2} = y_2.
\]
If $r_1, r_2$ denote the number of solutions of the first and second equation, respectively, then $a_\mu = r_1 \cdot r_2$. We show that $r_1 \equiv r_2 \mod p$.

According to Lemma [18] there is exactly one conjugacy class $C \subset CS_{\mu}(\pi)$ of elements of cycle type $(c_1, ..., c_m)$ with $c_i \neq 0$ and $c_j = 0$ for $j \neq i$, and in fact $c_i = p$ for this class. Let $g_i = g_i \cdot \cdot \cdot g_i$ be a decomposition of an element $g_i \in C_\sigma \cap CS_n(\pi)$. We prove that $g_{i,1} \in C$ and that for every element $g_{i,1} \in C$ there exists an element $g_{i,1} \in S_{n-i}$ such that $g_{i,1} \cdot \cdot \cdot g_{i,1} \in C_\sigma \cap CS_n(\pi)$. Thus we have to count the number of solutions $(g_{1,1}, ..., g_{1,1})$ of the first equation, where $g_{1,1} \in C$ for all $t$. Then we prove that $y_1 \in C$ as well and that therefore $r_1$ is the coefficient of $C^+$ in $(C^+_p)^p$.

All $p'$-elements in $CS_{\mu}(\pi) \setminus \{1\}$ have a cycle type of the form $(p_1, ..., p_d)$. As $a_j < p$ for $1 \leq j < i$ we obtain $g_{1,1} \in C$ for all $g_i = g_i \cdot \cdot \cdot g_i \in CS_n(\pi) \cap C_\sigma$ and for every $g_{1,1} \in C$ there exists a $g_{i,1} \cdot \cdot \cdot g_{i,1} \in S_{n-i}$ such that $g_i = g_i \cdot \cdot \cdot g_i \in CS_n(\pi) \cap C_\sigma$.

Now let $\lambda = (b_1, ..., b_n)$ be the cycle type of a $p'$-partition with $C_\lambda \subset \text{supp}(C^+_\sigma)^k$.

Using induction and Corollary [17] we see that $b_j < p$ for all $j < i$. This also provides $y_1 \in C$ for all $y = y_1 \cdot \cdot \cdot y_2 \in CS_n(\pi)$ such that $r_1 \equiv r_2 \mod p$.

**Corollary 23.** Let $\sigma, i$ be as in Notation [15] and let $\mu = (b_1, ..., b_n)$ be the cycle type of a $p'$-partition with $C_\mu \subset \text{supp}(C^+_\sigma)^p$. Then $b_j < p$ for $1 \leq j \leq i$.

**Proof.** For $1 \leq j < i$ the statement $b_j < p$ follows by induction and Corollary [14] Lemma [22] provides $b_i < p$.

**Proof of Theorem 3.** We consider a minimal counterexample in the following sense: For a given prime $p$ let $n$ be minimal such that a primitive central idempotent $e \in F_pS_n$ exists with $e \not\in Z_{p'}^{S_n} \cap Z_{p-nreg}^{S_n}$. According to a theorem of Osima [8, 7.4] we know that $e \in Z_{p-nreg}^{S_n}$, therefore there is a $p'$-partition $\sigma$ of cycle type $(a_1, ..., a_n)$
with $a_i \geq p$ for some $i \geq 2$, such that $C_\sigma \subset \supp e$. Now we choose $\sigma$ to be the partition, where $i \geq 2$ is minimal with $a_i \geq p$ under all partitions with $C_\sigma \subset \supp e$.

Let $e = \sum_{C_\tau \subset \supp e} a_\tau C_\tau^+$. Then

\[ e = e^p = \sum_{C_\tau \subset \supp e} a_\tau^p (C_\tau^+)^p = \sum_{C_\tau \subset \supp e} a_\tau (C_\tau^+)^p. \]

For conjugacy class sums $C_\tau^+ \in Z_{p^m}^{S_n} \cap Z_{p-nreg}^{S_n}$ we know $(C_\tau^+)^p \in Z_{p^m}^{S_n} \cap Z_{p-nreg}^{S_n}$ by Theorem 2 thus $C_\sigma \not\subset \supp (C_\tau^+)^p$ for these $\tau$. Now let $(b_1, \ldots, b_n)$ be the cycle type of a partition $\tau$ with $C_\tau \subset \supp e$ and $b_j \geq p$ for some $j \geq 2$. Using Theorem 1 and the minimality of $n$ we get that $b_1 < p$ for all these $\tau$. Now let $j$ be minimal with $b_j \geq p$ for the given $\tau$. If $j \geq i$, then $C_\sigma \not\subset \supp (C_\tau^+)^p$ according to Corollary 23. As we choose $i$ to be minimal there is no $\tau$ such that $C_\tau \subset \supp e$ and $b_j \geq p$ for a $j$ with $2 \leq j < i$. Hence we obtain

\[ C_\sigma \not\subset \supp e^p = \supp e, \]

a contradiction.

Now we want to use the theorems we proved to speed up the algorithm described in Algorithm 7 for the computation of the primitive central idempotents of finite group rings of symmetric and alternating groups. For symmetric groups the number $r$ of primitive central idempotents of $F_p S_n$ can be computed using Nakayamas Conjecture, [7], 6.1.21. To compute the primitive central idempotents of $F_p S_n$ we use Algorithm 7 with the following changes:

- We compute the $p$-near-regular $p'$-conjugacy classes in step 1) of Algorithm 7.
- We subsume steps 2), 3) and 4) of Algorithm 7 in a loop and check if the basis computed in 4) already has $r$ elements. If this is the case we do not need to compute further idempotents and we can continue with step 5.
- For step 2) and step 5) of Algorithm 7 it is necessary to compute the product of class sums in $F_p S_n$. We compute the class multiplication coefficients over the field $\mathbb{C}$ of complex numbers according to [1], Theorem 4.6, using a program written in SYMMETRICA ([10]) provided by A. Kohnert and then reduce them modulo $p$. As we are multiplying class sums of $p$-near-regular $p'$-classes we only have to compute coefficients $c_{ijk}$ of $p$-near regular $p'$-classes $C_k$ according to Theorem 2. We also use Corollary 12 to reduce the number of coefficients we have to compute.
- We store the products of class sums because they usually occur several times during the computation.

Considering the changes described above we see that the best situation occurs for $p = 2$, because in this case the numbers of $p'$-classes and of $p$-near-regular classes both are much smaller than for all other primes (see Table 1). But there are even more possibilities to speed up the program for $p = 2$. The step of Algorithm 7 consuming the most time is step 5), because the idempotents $f_i$ are sums of many class sums and it takes a long time to compute a product $f_i \cdot f_j$. The philosophy for $p = 2$ is to compute only squares of class sums if possible. So for $p = 2$ we also made the following changes of Algorithm 7:
These changes allowed us to compute the primitive central idempotents of $F$ true for all idempotents of $F$ also the primitive central idempotents of $S$. The time needed to compute the idempotents of $F$ dual core computer with two Opteron 265 1.8GHz processors. Approximately the $n \leq 50$. The results can be seen in the Appendix. For our computations we used a The necessary information about the primitive central idempotents of the group rings $F_2 S_n$ can be found in corollaries 4 and 5 of [3]: If $n$ is not of the form $n = \frac{m(m+1)}{2}$ with an integer $m$, then the primitive central idempotents of $F_2 S_n$ are also the primitive central idempotents of $F_2 A_n$. If $n = \frac{m(m+1)}{2}$, then this is also true for all idempotents of $F_2 S_n$ except for one. In this case $c = C^+$ is a primitive central idempotent of $F_2 S_n$ according to Theorem 3 of [3], where $C$ is the conjugacy class of elements corresponding to the partition $(2m - 1, 2m - 5, 2m - 9, ...)$ of $n$. These changes allowed us to compute the primitive central idempotents of $F_2 S_n$ for $n \leq 50$. The results can be seen in the Appendix. For our computations we used a dual core computer with two Opteron 265 1.8GHz processors. Approximately the time needed to compute the idempotents of $S_{n+2}$ using the results of the computation for $S_n$ is twice the time needed for the computation of the idempotents for $S_n$. So it takes about 7s to carry out the computation for $S_{20}$, 4m for $S_{30}$, 3h31m for $S_{40}$ and 10d7h14m for $S_{50}$ using the results for $S_{28}$, $S_{38}$ and $S_{48}$, respectively.

The necessary information about the primitive central idempotents of the group rings $F_2 A_n$ can be found in corollaries 4 and 5 of [3]: If $n$ is not of the form $n = \frac{m(m+1)}{2}$ with an integer $m$, then the primitive central idempotents of $F_2 S_n$ are also the primitive central idempotents of $F_2 A_n$. If $n = \frac{m(m+1)}{2}$, then this is also true for all idempotents of $F_2 S_n$ except for one. In this case $c = C^+$ is a primitive central idempotent of $F_2 S_n$ according to Theorem 3 of [3], where $C$ is the conjugacy class of elements corresponding to the partition $(2m - 1, 2m - 5, 2m - 9, ...)$ of $n$. • It turned out that we get the right number of idempotents using 1 and the powers of the class sums $C_i^+, C_j^+, ... , C_{(r-2)+3}^+$. We didn’t prove that the powers of these class sums always generate the vector space spanned by the primitive central idempotents, but the program will stop if it doesn’t find enough linear independent idempotents. • In step 2) we compute $(C_i^+)^{2^k}$ until $(C_i^+)^{2^k} = (C_i^+)^{2^{k+1}}$ building only squares of class sums. Then $f_i := (C_i^+)^{2^k}$ is the idempotent occuring in step 3). We keep in mind that $f_i$ ”comes from” $C_i$ for step 5). • We store all class multiplication coefficients, because we can use them for bigger symmetric groups according to Corollary [2]. • The products $f_i \cdot f_j$ occurring in step 5) are computed in the following way: We kept in mind that $f_i$ came from $C_i$ and $f_j$ came from $C_j$. So instead of multiplying $f_i$ and $f_j$ directly—both are usually large sums of class sums—we multiply $C_i^+$ and $C_j^+$ and compute $(C_i^+ C_j^+)^{2^k}$ until $(C_i^+ C_j^+)^{2^k} = (C_i^+ C_j^+)^{2^{k+1}}$. Then $f_i \cdot f_j = (C_i^+ C_j^+)^{2^k}$. The advantage of this procedure is that we only have to compute squares of class sums and no mixed products except $C_i^+ C_j^+$. We store all squares we compute, because they usually occur several times. If we replace an idempotent $f_i$ by $f_i \cdot f_j$ or by a sum of idempotents, then we have to keep in mind that our new idempotent comes from $C_i^+ C_j^+$ or from a sum of class sums. Here we get a delicate problem: After several steps of the loop in step 5) our idempotents are powers of expressions like $(C_i^+)^2 \cdot C_j^+ + (C_k^+)^3 \cdot C_m^+ + C_n^+ \cdot (C_m^+)^2 + ...$. In every step the expressions become longer and the multiplying of two such expressions takes more and more time. Therefore we have to keep these expressions simple: The idempotent generated by $(C_i^+)^2 \cdot C_j^+$ is also generated by $C_i^+ \cdot C_j^+$ so we have to filter out powers in our expressions. If we do that we will see that the idempotents generated by the summands $(C_k^+)^3 \cdot C_m^+$ and $C_n^+ \cdot (C_m^+)^2$ in the expression above are the same, so we can delete those summands from our expression. Thus for every idempotent $f_i$ we store such an expression, and this expression has to be updated and simplified whenever we replace an idempotent $f_i$ by a product or a sum of idempotents.
This idempotent $e$ splits in a sum of two primitive central idempotents of $F_{2k}A_n$. As the class $C$ splits in two conjugacy classes $C_-$ and $C_+$ of $A_n$ we can compute the remaining primitive central idempotents of $F_{2k}A_n$ by computing the powers of the class sums $C_-$ and $C_+$. For alternating groups the field $F_2$ is not always a splitting field, but at least $F_4$ is a splitting field for $A_n$ according to Corollary B of [12]. Thus it may happen that the two idempotents are not elements of $F_2A_n$, but they are elements of $F_4A_n$. The results show that our Theorems 1, 2, 3 are not true for alternating groups.

ACKNOWLEDGEMENTS

The author thanks A. Kerber and W. Müller for fruitful discussions about this topic, A. Kohnert for providing programs computing the class multiplication coefficients of symmetric and alternating groups, A. Konovalor for help with a lot of questions concerning GAP, and the referee for a lot of helpful comments and suggestions.

APPENDIX

Here our notation is slightly different to the notation in the rest of the article: If $\mu = 2^{a_2}, ..., n^{a_n}$ is a partition we write $2^{a_2}, ..., n^{a_n}$ for the class sum $C_+^{\mu}$ in $F_2S_m$, where $m \geq W(\mu)$. According to Theorem I one can easily deduce the primitive central idempotents of $F_2S_n$ for $n < 49$ from the primitive central idempotents of $F_2S_{50}$ and $F_2S_{59}$. To simplify that task we added tokens of the form $|_{16}$ to indicate where the primitive central idempotent of $F_2S_{16}$ ends.

Primitive central idempotents of $F_2S_n$ for $n$ odd and $n \leq 49$:

Primitive central idempotents of $F_2S_n$ for $n$ even and $n \leq 50$:

\[ c_1 = \frac{1}{30} \left( 47 + 5 \cdot 5a + 7 \cdot 5a + 9 + 5 \cdot 10 + 15 + 7 \cdot 9 + 5 \cdot 11 + 7 \cdot 13 + 14 + 5 \cdot 13 + 24 + 7 \cdot 9 + 13 + 5 \cdot 11 + 17 + 7 \cdot 13 + 19 + 5 \cdot 11 + 19 + 9 + 5 \cdot 13 + 21 + 7 \cdot 9 + 13 + 17 + 3 \cdot 5 \cdot 9 + 13 + 19 + 5 \cdot 11 + 17 + 3 \cdot 5 \cdot 9 + 13 + 19 \right) \]

\[ c_2 = \frac{1}{30} \left( 47 + 5 \cdot 5a + 7 \cdot 5a + 9 + 5 \cdot 10 + 15 + 7 \cdot 9 + 5 \cdot 11 + 7 \cdot 13 + 14 + 5 \cdot 13 + 24 + 7 \cdot 9 + 13 + 5 \cdot 11 + 17 + 7 \cdot 13 + 19 + 5 \cdot 11 + 19 + 9 + 5 \cdot 13 + 21 + 7 \cdot 9 + 13 + 17 + 3 \cdot 5 \cdot 9 + 13 + 19 \right) \]
For alternating groups \( F_4 \) is always a splitting field. The primitive central idempotents of \( F_4 A_n \) are the primitive central idempotents of \( F_2 S_n \) except for one case: If \( n = \frac{3m(m+1)}{2} \), then there is an idempotent \( e = C^+ \) of \( F_2 S_n \), where \( C \) is the conjugacy class corresponding to the partition \((2m - 1, 2m - 5, 2m - 9, \ldots)\) of \( n \). This idempotent splits in two primitive central idempotents \( f_1 \) and \( f_2 \) of \( F_2 A_n \). We computed these two idempotents. If a class \( C \) of \( S_n \) splits in two conjugacy classes of \( A_n \), then we write \( C_- \) and \( C_+ \) for the \( A_n \)-classes. \( \zeta \) denotes a generator of \( F_4 \) over \( F_2 \). To save space we only write \( f_1 \), the second idempotent \( f_2 \) can easily be computed via \( f_2 = f_1 + 2m - 1, 2m - 5, 2m - 9, \ldots + 2m - 1, 2m - 5, 2m - 9, \ldots \).
References


Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
E-mail address: harald.meyer@uni-bayreuth.de