East-West J. of Mathematics: Vol. 23, No 2 (2022) pp. 112-118
https://doi.org/10.36853/ewjm0389

A NOTE ON CENTRAL IDEMPOTENTS IN GROUP RING OF SYMMETRIC GROUP OVER $\mathbb{Z}_n$

Anuradha Sabharwal, Pooja Yadav and **R. K. Sharma**

Department of Mathematics,
University of Delhi, Delhi–110 007 India
e-mail: anuradha.sabharwal@gmail.com

Department of Mathematics,
Kamala Nehru College, University of Delhi, Delhi–110 007 India
e-mail: iitd.pooja@gmail.com

Department of Mathematics,
Indian Institute of Technology Delhi, Delhi–110 016 India
e-mail: rksharmaiitd@gmail.com

Abstract

The number of central idempotents in group ring $\mathbb{Z}_n[S_3]$ have been determined. Furthermore, some explicit form of central idempotents have also been obtained.

1 Introduction

The problem of computing central idempotents of rings and group rings is an important problem. It has drawn attention of many researchers. A central idempotent that cannot be written as the sum of two non zero orthogonal central idempotents is called a centrally primitive idempotent. Meyer [5] computed primitive central idempotents of $F_q[G]$ for arbitrary prime powers q, and arbitrary finite groups G. Aso, a well-known result of Osima [6, p.178] gives the explicit form for the primitive central idempotents in $K[G]$, when K is a field. Martínez [2] computed central irreducible idempotents of the dihedral group algebra $\mathbb{F}_q[D_{2n}]$. These papers do not provide all the central idempotents. In

---

Key words: central idempotents, group ring.
2010 AMS Mathematics Classification: 20C05, 16S34

this paper, we have determined the number of central idempotents in the group ring $\mathbb{Z}_n[S_3]$, the symmetric group S_3 over $\mathbb{Z}_n$ the ring of integers modulo n, for all positive integers n. Further, we provide an explicit form of these central idempotents.
Let G be a group and R be a ring, then the set of all linear combinations $\alpha = \sum_{g\in G} a_g g$ where $a_g \in R$ and only finitely many of the $a_g{}'s$ are non-zero is defined as group ring RG. Sum and product in group ring is given by $\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} (a_g + b_g)\, g$ and $\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} (a_g b_g)$ respectively. Group ring RG is a ring under addition and multiplication defined above. An element e of a ring is said to be an idempotent if $e^2 = e$. An idempotent e in a ring R is said to be a central idempotent if e commutes with every element of the ring R. For more basic results on group rings we refer to [3].

Definition 1. *A set of elements that are connected by an operation called conjugation forms a* ***conjugacy class****.*
Sum of elements in a conjugacy class is called the ***class sum*** *of the conjugacy class.*

Lemma 1.1 ([1], Theorem 3.6.2, p151)**.** *Let G be a group and R be a commutative ring. Then, the set of all class sums forms a basis of the center $\mathcal{Z}(R[G])$ of $R[G]$, over R.*

Example 1. *Symmetric group of degree 3 having presentation $S_3 = \langle \sigma, \tau | \tau^2 = \sigma^3 = 1,\ \sigma\tau = \tau^{-1}\sigma \rangle$, consists of 3 conjugacy classes. These are $\mathcal{C}_1 = \{1\}$ the idenditity element, $\mathcal{C}_2 = \{\tau, \tau\sigma, \tau\sigma^2\}$ containg all transpositions, and $\mathcal{C}_3 = \{\sigma, \sigma^2\}$ containing 3-cycles.*
Class sums in S_3 are $\gamma_1 = 1, \gamma_2 = \tau + \tau\sigma + \tau\sigma^2, \gamma_3 = \sigma + \sigma^2$ respectively. These form a basis of $\mathcal{Z}(R[S_3])$, over R. Therefore, any arbitrary element of $\mathcal{Z}(R[S_3])$ can be written as a linear combination of $\gamma_1, \gamma_2, \gamma_3$ over R.

In solving the system of equations, number theory plays an important role. The following result gives a unique solution to simultaneous linear congruences with coprime moduli.

Lemma 1.2 ([4],Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_l$ be integers with $\gcd(n_i, n_j) = 1$ whenever $i \neq j$. Let $n = n_1 n_2 \cdots n_l$ and $a_1, a_2, \ldots, a_l$ be integers. Then the system of linear congruences*

$$x \equiv a_i \mod n_i \ (1 \leq i \leq n_l)$$

has a simultaneous unique solution in $\mathbb{Z}_n$ given by $\bar{x} \equiv \sum_{i=1}^{l} a_i N_i y_i$, where $N_k = \frac{n}{n_k}$ and y_k is the unique solution of $N_k y \equiv 1 \mod n_k$.

In the case of a finitely generated abelian group, the following result guarantees that an abelian group splits as a direct product of finitely many groups of the form $\mathbb{Z}_{p^k}$ for p prime,

Lemma 1.3 ([7],Fundamental Theorem of Finite Abelian Group)**.** *Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order.*

Let $n = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$ be the prime factorization of n. Since $\mathbb{Z}_n$ is a finite abelian group, by lemma 3,

$$\phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{n_l}}$$

is an isomorphism. Then for an element $a \in \mathbb{Z}_n$, is an idempotent in $\mathbb{Z}_n$ if and only if each $a \mod p_i^{n_i}$ is an idempotent in $\mathbb{Z}_{p_i^{n_i}}$. Using above two results we can calculate the number of idempotents in a finite ring.

Lemma 1.4. *The number of pairwise non congruent idempotents in $\mathbb{Z}_n$ is equal to 2^l.*

2 Central Idempotents

Theorem 2.1. *Let $n = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l}$ where p_i's are distinct primes and $n_1, n_2, \ldots, n_l$ are positive integers.*
Then the number of central idempotents in $\mathbb{Z}_n[S_3]$ is

(i) 2^{3l} *, if $p_i > 3 \;\forall\; 1 \leq i \leq l$.*

(ii) 2^{3l-1} *, if $p_1 = 2$ and $p_i > 3 \;\forall\; 2 \leq i \leq l$.*

(iii) 2^{3l-2} *, if $p_1 = 3$ and $p_i > 3 \;\forall\; 2 \leq i \leq l$.*

(iv) 2^{3l-3} *, if $p_1 = 2, p_2 = 3$ and $p_i > 3 \;\forall\; 3 \leq i \leq l$.*

Proof. $S_3 = \langle \sigma, \tau | \tau^2 = \sigma^3 = 1, \sigma\tau = \tau^{-1}\sigma \rangle$ has three conjugacy classes $\{1\}, \{\sigma, \sigma^2\}$ and $\{\tau, \tau\sigma, \tau\sigma^2\}$. By lemma 1, class sums of these conjugacy classes form a basis of center of $\mathbb{Z}_n[S_3]$, over $\mathbb{Z}_n$. That is,

$$\mathcal{Z}(\mathbb{Z}_n[S_3]) = \big\langle 1, \sigma + \sigma^2, \tau(1 + \sigma + \sigma^2) \big\rangle$$

Let e be a central idempotent in $\mathbb{Z}_n[S_3]$. Then, e can be expressed as

$$e = a \cdot 1 + b(\sigma + \sigma^2) + c(\tau(1 + \sigma + \sigma^2)) \text{ for some } a, b, c \in \mathbb{Z}_n$$

which can be written as

$$e = \alpha \cdot 1 + \beta(1 + \sigma + \sigma^2) + \gamma(1 + \sigma + \sigma^2 + \tau(1 + \sigma + \sigma^2)),$$

where $\alpha = a - b, \beta = b - c, \gamma = c \in \mathbb{Z}_n$. As e is an idempotent, $e^2 = e$. Comparing the coefficients of class sums in the equation $e^2 = e$, we get the following relations:

$$\alpha^2 = \alpha \quad (1)$$

$$3\beta^2 + 2\alpha\beta = \beta \quad (2)$$

$$6\gamma^2 + 2\alpha\gamma + 6\beta\gamma = \gamma \quad (3)$$

The values of α, β and γ give all the possible central idempotents in $\mathbb{Z}_n[S_3]$. By lemma 3, we observe that equation (1) has 2^l solutions for α. Let α_1 be an arbitrary solution of (1). Then equation (2) implies

$$3\beta^2 + 2\alpha_1\beta = \beta$$

$$\Longrightarrow \quad \beta[3\beta + (2\alpha_1 - 1)] = 0$$

$$\Longrightarrow \quad 3\beta^2 = -(2\alpha_1 - 1)\beta \quad (4)$$

Case(i) : If $p_i > 3 \ \forall \ 1 \leq i \leq l$
By fundamental theorem of finite abelian groups [7], the mapping

$$\phi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{n_l}}$$

defined by $\phi(a) = (a_1, a_2, \ldots, a_l)$ where each $a_i \equiv a \mod p_i^{n_i}$,
for all $a \in \mathbb{Z}_n$, is an isomorphism. For $\beta \in \mathbb{Z}_n$,

$$\phi(\beta) = (x_1, x_2, \ldots, x_l) \text{ where each } x_i \equiv \beta \mod p_i^{n_i}.$$

From equation (4), we have

$$3\beta^2 \equiv -(2\alpha_1 - 1)\beta \mod n$$

$$\Longleftrightarrow \quad 3x_i^2 \equiv -(2\alpha_1 - 1)x_i \mod p_i^{n_i} \quad \forall 1 \leq i \leq l$$

$$\Longleftrightarrow \quad x_i[3x_i + (2\alpha_1 - 1)] \equiv 0 \mod p_i^{n_i} \quad \forall 1 \leq i \leq l.$$

We claim that x_i and $3x_i + (2\alpha_1 - 1)$ cannot be zero divisors in $\mathbb{Z}_{p_l^{n_l}}$.
If possible, suppose $x_i \neq 0$ and $3x_i + (2\alpha_1 - 1) \neq 0$. Then $x_i = p_i^{\eta} r$ and $3x_i + (2\alpha_1 - 1) = p_i^{\varsigma} s$, where $p_i \nmid r$, $p_i \nmid s$ and $\eta + \varsigma \geq n_i$.

$$3p_i^{\eta} r + (2\alpha_1 - 1) = p_i^{\varsigma} s$$

without any loss of generality, let $\eta < \varsigma$, then

$$p_i^{\eta}[3r - p_i^{\varsigma - \eta} s] = -(2\alpha_1 - 1).$$

This implies that p_i^{η} is invertible in $\mathbb{Z}_{p_i^{n_i}}$. A contradiction. Therefore,

$$x_i \equiv 0 \quad \text{or} \quad 3x_i + (2\alpha_1 - 1) \equiv 0 \mod p_i^{n_i}$$

Since 3 is invertible in each $\mathbb{Z}_{p_i^{n_i}}$, there are 2^l possible values for β that satisfy equation (4). Let β_1 be one of these. Substituting $\alpha = \alpha_1$, and $\beta = \beta_1$ in equation (3), we get

$$\begin{aligned} & 6\gamma^2 + 2\alpha_1\gamma + 6\beta_1\gamma = \gamma \\ \Longrightarrow \quad & \gamma[6\gamma + (2\alpha_1 + 6\beta_1 - 1)\gamma] = 0 \end{aligned} \tag{5}$$

Further, since 6 is invertible in each $\mathbb{Z}_{p_i^{n_i}}$, by similar calculations we observe that there are 2^l possible values for γ satisfying (5). Hence there are $2^l \times 2^l \times 2^l$ solutions for the three simultaneous equations.
Thus, there are 2^{3l} central idempotents in this case.

Case(ii) : If $p_1 = 2$, $p_i > 3 \ \forall \ 2 \leq i \leq l$.
Note that 3 is invertible in each $\mathbb{Z}_{p_i^{n_i}}$. Therefore equation (4) have same solution for β as obtained in case(i). Though 6 is not invertible in $\mathbb{Z}_{p_1^{n_1}}$ but it is invertible in $\mathbb{Z}_{p_i^{n_i}}$ $\forall 2 \leq i \leq l$, therefore there are 2^{l-1} possible values for γ which satisfies equation (5). This gives that there are $2^l \times 2^l \times 2^{l-1}$ solutions for the three simultaneous equations.
Hence, there are 2^{3l-1} central idempotents in this case.

Case(iii) : If $p_1 = 3$, $p_i > 3 \ \forall \ 2 \leq i \leq l$.
Observe that 3 is not invertible in $\mathbb{Z}_{p_1^{n_1}}$ but 3 is invertible in $\mathbb{Z}_{p_i^{n_i}}$ $\forall 2 \leq i \leq l$. Hence there are 2^{l-1} possible values for β satisfying equation (4). Again, 6 is not invertible in $\mathbb{Z}_{p_1^{n_1}}$ but 6 is invertible in $\mathbb{Z}_{p_i^{n_i}}$ $\forall 2 \leq i \leq l$, we find that there are 2^{l-1} possible values for γ satisfying equation (5). Thus there are $2^l \times 2^{l-1} \times 2^{l-1} = 2^{3l-2}$ solutions for the three simultaneous equations.
And therefore there are 2^{3l-2} central idempotents in this case.

Case(iv) : If $p_1 = 3$, $p_2 = 2$, $p_i > 3 \ \forall \ 3 \leq i \leq l$.
Again 3 is not invertible in $\mathbb{Z}_{p_1^{n_1}}$ but being invertible in $\mathbb{Z}_{p_i^{n_i}}$ $\forall 2 \leq i \leq l$, we get 2^{l-1} possible values for β satisfying equation (4). Next, 6 is not invertible in $\mathbb{Z}_{p_1^{n_1}}$ and $\mathbb{Z}_{p_2^{n_2}}$ but 6 is invertible in $\mathbb{Z}_{p_i^{n_i}}$ $\forall 3 \leq i \leq l$, there are 2^{l-2} possible values for γ which satisfy equation (5). This gives $2^l \times 2^{l-1} \times 2^{l-2}$ solutions for the three simultaneous equations.
Hence, there are 2^{3l-3} central idempotents in this case. □

Corollary 1. *Central idempotents in $\mathbb{Z}_n[S_3]$ are of the form*

$$\alpha + \beta(1 + \sigma + \sigma^2) + \gamma(1 + \sigma + \sigma^2 + \tau(1 + \sigma + \sigma^2)),$$

where

1. *α is an idempotent in $\mathbb{Z}_n$, and each one is precisely of the form $\sum_{k=1}^{l} h_k\epsilon_k + m\mathbb{Z}$, where $\epsilon_k \in \{0,1\}$ and $h_k \in \left(\prod_{i=1,i\neq k}^{l} p_i^{n_i}\right)\mathbb{Z}$ such that $h_k - 1 \in p_k^{n_k}\mathcal{Z}$.*

2. *β is the simultaneous solution of the system of linear congruences*

$$\beta \equiv a_i \mod p_i^{n_i} \quad (1 \leq i \leq l),$$

where (for each α),

- *$a_i \in \{0, -(2\alpha - 1)(3^{-1} \mod p_i^{n_i}) \mod n\}$ $\forall\ 1 \leq i \leq l$ in cases (i) and (ii), and*
- *$a_1 = 0, a_i \in \{0, -(2\alpha - 1)(3^{-1} \mod p_i^{n_i}) \mod n\}$ $\forall\ 2 \leq i \leq l$ in cases (iii) and (iv).*

Using Chinese Remainder theorem [4], the solution of the above system of linear congruences is given by $\bar{\beta} \equiv \sum_{i=1}^{l} a_i P_i x_i$ where

- *$P_k = \frac{n}{p_k^{n_k}}$*
- *x_k is the unique solution of $P_k x \equiv 1 \mod p_k^{n_k}$*

3. *γ is the solution of the system of linear congruences*

$$\gamma \equiv b_i \mod p_i^{n_i} \quad (1 \leq i \leq l),$$

where (for each α and β),

- *$b_i \in \{0, -(2\alpha + 6\beta - 1)(6^{-1} \mod p_i^{n_i}) \mod n\}$ $\forall\ 1 \leq i \leq l$ in case (i), and*
- *$b_1 = 0, b_i \in \{0, -(2\alpha + 6\beta - 1)(6^{-1} \mod p_i^{n_i}) \mod n\}$ $\forall\ 2 \leq i \leq l$ in cases (ii) and (iii), and*
- *$b_1 = 0, b_2 = 0, b_i \in \{0, -(2\alpha + 6\beta - 1)(6^{-1} \mod p_i^{n_i}) \mod n\}$ $\forall\ 3 \leq i \leq l$ in case (iv).*

References

[1] C. Polcino Milies and S. K. Sehgal, *An introduction to group rings*, Algebra and Applications, 1, Kluwer Academic Publishers, Dordrecht, 2002. MR1896125

[2] F. E. Brochero Martínez, Structure of finite dihedral group algebra, Finite Fields Appl. **35** (2015), 204–214. MR3368809

[3] D. S. Passman, *The algebraic structure of group rings*, Pure and Applied Mathematics, Wiley-Interscience, New York, 1977. MR0470211

[4] D. M. Burton, *Elementary number theory*, Allyn and Bacon, Inc., Boston, MA, 1976. MR0567138

[5] H. Meyer, Primitive central idempotents of finite group rings of symmetric groups, Math. Comp. **77** (2008), no. 263, 1801–1821. MR2398795

[6] M. Osima, On blocks of characters of the symmetric group, Proc. Japan Acad. **31** (1955), 131–134. MR0076771

[7] J. A. Gallian, *Contemporary Abstract Algebra*, Narosa, 1999.