Structure of the Unit Group of the Symmetric Group Algebra

N.Abhilash [#1], E.Nandakumar [*1]

[1]Department of Mathematics, SRM Institute of Science and Technology, Kattankulathur – 603203, Tamilnadu, India

[*]e-mail: nanda1611@gmail.com

Article Info
Page Number: 1070-1076
Publication Issue:
Vol. 72 No. 1 (2023)

Article History
Article Received: 15 October 2022
Revised: 24 November 2022
Accepted: 18 December 2022

Abstract: In this paper, we characterized the unit group for the semi-simple group algebra generated by the symmetric group and its order over the finite field. As an example, group S_7 is considered, and the unit group of the corresponding group algebra is classified for $p > 7$.

Keywords: Symmetric groups, Group algebra, Semi simplicity, Unit group.

Introduction

Let the finite field of order $q = p^k$, where p is the prime number is denoted by $\mathbb{K}$. Consider $\mathbb{K}G$ as the group algebra generated by G of order n over $\mathbb{K}$ and $\mathcal{U}(\mathbb{K}G)$ denote the collection of units in $\mathbb{K}G$. Here, $\mathcal{U}(\mathbb{K}G)$ is called the unit group of $\mathbb{K}G$. The study of unit groups is very much interesting and demanding and used in so many fields. For example, convolution codes were constructed by the units in [7],[8],[9] and unit groups were used to solve the various combinatorial number theoretical problems in [4].

In the past few years, the unit groups of different group algebras were studied and characterized. For G being a p-group, the structure of unit group was discussed in [14]. R.K.Sharma classified the unit group of the group algebra of some non-abelian group in [16], [17] and in [19], G.Tang also contributed to it. In [18], Swati Maheshwari characterized $\mathcal{U}(\mathbb{K}SL(2, Z_3))$. The unit group of the group algebra $\mathbb{K}A_4$ was characterized by Gildea in [5] and R.K.Sharma in [15]. In [2],[6],[10],[11] and [12], unit group of dihedral group algebra were discussed.

In [20], for the symmetric group algebra $\mathbb{K}S_5$, the unit group was characterized. But, if the size of the n in S_n increases, the complexity to solve the final equation $n_1^2 + n_2^2 + \cdots + n_r^2 = |G|$ will become very difficult. Therefore, Arvind (in [1]) introduced Brauer characters to estimate n_i rather than the usual methods.

In this paper, we characterized the unit group $\mathcal{U}(\mathbb{K}S_n)$ for the symmetric group algebra $\mathbb{K}S_n$ over the finite field $\mathbb{K}$, whenever the symmetric group algebra is semi-simple and we give an easy way to find the n_i's by using Bratteli diagram of symmetric group. Also, we give the complete classification of the unit group of $\mathbb{K}S_7$. Section 2 deals with the preliminaries while section 3 has the main result. The computation of the unit group of $\mathbb{K}S_7$ is given in section 4. The last section concluding in nature.

PRELIMINARIES

In this paper, $\mathbb{K}$ denotes the field of order $q = p^k$ and G denotes the finite group. The definitions and results given below are as in [3].

Definition 2.1. An element $x \in G$ is called p' elements, if $p \nmid |x|$, where $|x|$ is the order of x in G.

The least common multiple of the orders of all p' elements in G is denoted by s. The primitive s^{th} root of unity over $\mathbb{K}$ is denoted by θ. Therefore, $\mathbb{K}(\theta)$ is the splitting field over $\mathbb{K}$. Now, define the set

$$T_{G,\mathbb{K}} = \{t | \sigma(\theta) = \theta^t, where\ \sigma \in Gal(\mathbb{K}(\theta)/\mathbb{K})\}$$

Definition 2.2. For any p' element $x \in G$, $\gamma_x = \sum_{h \in C_x} h$, where C_x is the conjugacy class of x. Then, the cyclotomic $\mathbb{K}$-class of γ_x is given by,

$$S_{\mathbb{K}}(\gamma_x) = \left\{\gamma_{x^t} | t \in T_{G,\mathbb{K}}\right\}$$

Note 1. The set $T_{G,\mathbb{K}}$ equivalently defined as $T_{G,\mathbb{K}} = \left\{q^i mod\ s | 0 \leq i \leq d-1\right\}$, where $d = ord_s q$ as in [20] and it is helpful to find the order of cyclotomic $\mathbb{K}$-classes.

Proposition 2.1. There is an one-to-one correspondence between the simple components of $\frac{\mathbb{K}G}{J(\mathbb{K}G)}$ and the cyclotomic $\mathbb{K}$-classes in G, where $J(\mathbb{K}G)$ is the Jacobson radical.

Proposition 2.2. Let the Galois group $Gal(\mathbb{K}(\theta)/\mathbb{K})$ is cyclic and κ be the number of cyclotomic $\mathbb{K}$-classes in G. If $K_1, K_2, \cdots, K_\kappa$ are the simple components of $Z\left(\frac{\mathbb{K}G}{J(\mathbb{K}G)}\right)$ and $S_1, S_2, \cdots, S_\kappa$ are the cyclotomic $\mathbb{K}$-classes of G, then $|S_i| = [K_i : \mathbb{K}]$ with a suitable ordering of indices.

Lemma 2.1. [13] Let $\mathbb{K}G$ be a semi-simple group algebra and G' be the commutator subgroup of G. Then, $\mathbb{K}G \approx \mathbb{K}G_{G'} \oplus \triangle\,(G, G')$, where $\mathbb{K}G_{G'} = \mathbb{K}\left(\frac{G}{G'}\right)$ is the sum of all commutative simple components of $\mathbb{K}G$ and $\triangle\,(G, G')$ be the sum of all others.

Lemma 2.2. The commutator subgroup of S_n is $A_n, n \geq 3$.

Lemma 2.3. Let $\sigma \in S_n$ be the cycle of length l. Then, $\sigma^t, t \in \mathbb{Z}$ is also a cycle of length l if and only if $(t, l) = 1$.

Proposition 2.3. For the semi simple group algebra $\mathbb{K}G$, the set of irreducible representations and the conjugacy classes of G are in one-to-one correspondence with each other.

Main Result

Consider the symmetric group S_n, where $n! = p_1^{r_1} \cdot p_2^{r_2} \cdots p_\lambda^{r_\lambda}$, where p_i's are prime number and r_i's are their corresponding exponents. Let $\mathbb{K}_q$ be a finite field of order $q = p^k$, where char$(\mathbb{K}) = p$ and $p \nmid p_i$, for $i = 1,2,\cdots,\lambda$. Since $p \nmid n!$, the group algebra $\mathbb{K}_q S_n$ is semi-simple, by Maschke's theorem. Equivalently, $J(\mathbb{K}_q S_n) = 0$.

Lemma 3.1. Let $\sigma \in S_n$ be a l- cyclic permutation. Then, σ^t, where $t \in T_{S_n,\mathbb{K}}$ is also l-cyclic, if $(t,n) = 1$.

Proof. Here, $! = p_1^{r_1} \cdot p_2^{r_2} \cdots p_\lambda^{r_\lambda}$, where p_i's are prime number and r_i's are their corresponding exponents. And l must be less than or equal to n. Also, by note 1, $t = q^i mod\ s, 0 \le i \le d-1$ where $q = p^k$. Since $t \nmid n!, t \nmid l$. Hence the result follows from lemma 2.3.

Theorem 3.1. For $\mathbb{K}_q S_n$ defined above,

$$\mathbb{K}_q S_n \approx \mathbb{K}_q \oplus \mathbb{K}_q \oplus M_{n_1}(\mathbb{K}_q) \oplus M_{n_2}(\mathbb{K}_q) \oplus \cdots \oplus M_{n_{r-2}}(\mathbb{K}_q)$$

where $n_1, n_2, \cdots, n_{r-2}$ are determined by Brateli diagram of symmetric group.

Proof. The group algebra $\mathbb{K}_q S_n$ is finite and so, Artinian. Therefore, by Wedderburn's theorem,

$$\mathbb{K}_q S_n \approx M_{n_1}(D_1) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_r}(D_r)$$

$$\mathbb{K}_q S_n \approx M_{n_1}(\mathbb{K}_{q^{m_1}}) \oplus M_{n_2}(\mathbb{K}_{q^{m_2}}) \oplus \cdots \oplus M_{n_r}(\mathbb{K}_{q^{m_r}})$$

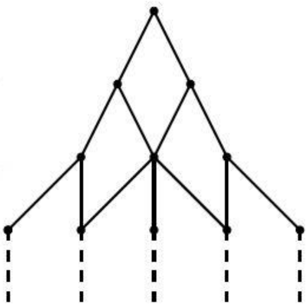
In the above decomposition, each component is pairwise inequivalent irreducible simple components of the group algebra. Use lemma 2.2, $\frac{S_n}{S_n'} \approx C_2$, the cyclic group of order two. Therefore, by lemma 2.1,

$$\mathbb{K}_q S_n \approx \mathbb{K}_q \oplus \mathbb{K}_q \oplus M_{n_1}(\mathbb{K}_{q^{m_1}}) \oplus M_{n_2}(\mathbb{K}_{q^{m_2}}) \oplus \cdots \oplus M_{n_{r-2}}(\mathbb{K}_{q^{m_{r-2}}})$$

The value of r is the number of simple components in the Wedderburn decomposition and by proposition 2.3, the value of r is equal to the number of partitions of n. By lemma 3.1, $\left|S_{\mathbb{K}_q}(\gamma_\sigma)\right| = 1$, for all $\sigma \in S_n$. Therefore, by proposition 2.2, $m_1 = m_2 = \cdots = m_r = 1$. Hence,

$$\mathbb{K}_q S_n \approx \mathbb{K}_q \oplus \mathbb{K}_q \oplus M_{n_1}(\mathbb{K}_q) \oplus M_{n_2}(\mathbb{K}_q) \oplus \cdots \oplus M_{n_{r-2}}(\mathbb{K}_q)$$

The value of n_i's in the above decomposition can be computed from the Bratelli's diagram of symmetric group.



In the above figure, dot represents the partitions of n arranged in the Lexicographic order from left to right. The number of paths from $n = 1$ to the desired partition gives the value of n_i's.

Corollary 3.1. Notations as above. The group $\mathcal{U}(\mathbb{K}_q S_n)$ is isomorphic to,

$$\mathcal{U}(\mathbb{K}_q S_n) \approx \mathbb{K}_q^* \oplus \mathbb{K}_q^* \oplus GL_{n_1}(\mathbb{K}_q) \oplus GL_{n_2}(\mathbb{K}_q) \oplus \cdots \oplus GL_{n_{r-2}}(\mathbb{K}_q)$$

Corollary 3.2. Notations as above. The order of $\mathcal{U}(\mathbb{K}_q S_n)$ is equal to,

$$\left|\mathcal{U}(\mathbb{K}_q S_n)\right| \approx \begin{cases} [q-1] \times [q-1] \times [(q^{n_1} - q^0)(q^{n_1} - q^1) \cdots (q^{n_1} - q^{n_1 - 1})] \times \\ [(q^{n_2} - q^0)(q^{n_2} - q^1) \cdots (q^{n_2} - q^{n_2 - 1})] \times \cdots \times \\ [(q^{n_{r-2}} - q^0)(q^{n_{r-2}} - q^1) \cdots (q^{n_{r-2}} - q^{n_{r-2} - 1})] \end{cases}$$

Note 2. The numerical values of $n_1, n_2, \cdots, n_{r-2}$ are determined by Brateli diagram of symmetric group.

UNIT GROUP OF $\mathbb{K}S_7$

Let $G = S_7$ and the order of $G = 7! = 7^1 \times 5^1 \times 3^2 \times 2^4$ and let $\mathbb{K}_q$ be the finite field of order q with characteristic $p(\neq 7,5,3,2)$. By Wedderburn decomposition theorem,

$$\mathbb{K}_q S_7 \approx M_{n_1}(D_1\,) \oplus M_{n_2}(D_2) \oplus \cdots \oplus M_{n_r}(D_r)$$

By Wedderburn little theorem,

$$\mathbb{K}_q S_7 \approx M_{n_1}(\mathbb{K}_{q^{m_1}}) \oplus M_{n_2}(\mathbb{K}_{q^{m_2}}) \oplus \cdots \oplus M_{n_r}(\mathbb{K}_{q^{m_r}})$$

$$\mathcal{U}(\mathbb{K}_q S_7) \approx GL_{n_1}(\mathbb{K}_{q^{m_1}}) \oplus GL_{n_2}(\mathbb{K}_{q^{m_2}}) \oplus \cdots \oplus GL_{n_r}(\mathbb{K}_{q^{m_r}})$$

The number of partitions of 7 is 15 and thus, $r = 15$.

$$\mathcal{U}(\mathbb{K}_q S_7) \approx GL_{n_1}(\mathbb{K}_{q^{m_1}}) \oplus GL_{n_2}(\mathbb{K}_{q^{m_2}}) \oplus \cdots \oplus GL_{n_{15}}(\mathbb{K}_{q^{m_{15}}})$$

Cyclic structure	**Order**
7	7
$6+1$	6

$5+2$	10
$5+1+1$	5
$4+3$	12
$4+2+1$	4
$4+1+1+1$	4
$3+3+1$	3
$3+2+2$	6
$3+2+1+1$	6
$3+1+1+1+1$	3
$2+2+2+1$	2
$2+2+1+1+1$	2
$2+1+1+1+1+1$	2
$1+1+1+1+1+1+1$	1

Since none of the order of the element in S_7 divides p, every element of S_7 is p' element. Therefore, the value of $s = 420$. For every $\sigma \in S_7, \gamma_\sigma$ is the sum of all conjugates of $\sigma \in S_7$, that is, the sum of all elements in S_7 having same cyclic structure with σ. By the definition of the set $T_{S_7,\mathbb{K}}$, observe that t does not divides n (refer note 3). Therefore, by lemma 3.1, $|S_{\mathbb{K}}(\gamma_\sigma)| = 1$, for all $\sigma \in S_7$ which gives $m + i = 1, 1 \leq i \leq r$.

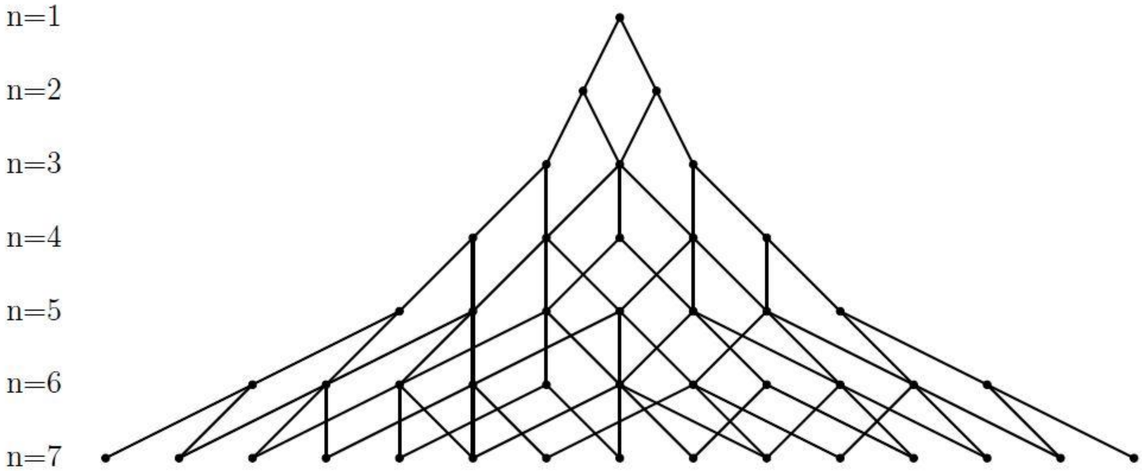
Note 3. For $q = 13, d = ord_{420}13$ =Smallest positive integer c such that $13^c \equiv 1 \; mod \; 420$. The value of d in this case is 4.

$$T_{S_7,\mathbb{K}} = \{13^i \; mod \; 420 | i = 0,1,2,3\} = \{1,13,97,169\}$$

For $q = 41, d = ord_{420}41$ =Smallest positive integer c such that $41^c \equiv 1 \; mod \; 420$. The value of d in this case is 2.

$$T_{S_7,\mathbb{K}} = \{41^i \; mod \; 420 | i = 0,1\} = \{1,41\}$$

The Bratteli's diagram for $n = 7$ is given below.



Therefore, from left $n_1 = 1, n_2 = 6, n_3 = 14, n_4 = 15, n_5 = 14, n_6 = 35, n_7 = 20, n_8 = 21, n_9 = 21, n_{10} = 35, n_{11} = 15, n_{12} = 14, n_{13} = 14, n_{14} = 6, n_{15} = 1$. Hence, by corollary 1,

$$\mathcal{U}(\mathbb{K}_q S_n) \approx \begin{cases} \mathbb{K}_q^* \oplus \mathbb{K}_q^* \oplus GL_6(\mathbb{K}_q) \oplus GL_6(\mathbb{K}_q) \oplus GL_{14}(\mathbb{K}_q) \oplus GL_{14}(\mathbb{K}_q) \oplus GL_{14}(\mathbb{K}_q) \oplus GL_{14}(\mathbb{K}_q) \oplus \\ GL_{15}(\mathbb{K}_q) \oplus GL_{15}(\mathbb{K}_q) \oplus GL_{20}(\mathbb{K}_q) \oplus GL_{21}(\mathbb{K}_q) \oplus GL_{21}(\mathbb{K}_q) \oplus GL_{35}(\mathbb{K}_q) \oplus GL_{35}(\mathbb{K}_q) \end{cases}$$

By corollary 3.2, the order of the unit group is given by,

$$|\mathcal{U}(\mathbb{K}_q S_n)| \approx \begin{cases} [q-1] \times [q-1] \times [(q^6-1)(q^6-q)\cdots(q^6-q^5)] \times \cdots \times \\ [(q^{35}-1)(q^{35}-q)\cdots(q^{35}-q^{34})] \end{cases}$$

Conclusion

This paper characterized the unit group of the semi simple symmetric group algebra $\mathbb{K}_q S_n$ uniquely using the Bratelli's diagram of symmetric groups. With this, the unit group of group algebra generated by all finite groups can be computed uniquely according to Cayley's theorem. This work paved the way for the researchers to find the restriction of symmetric group to its subgroups in order to compute the dimensions of irreducible representations of the subgroups of symmetric group.

References

1. N. Arvind, S. Panja, Unit group of some finite semi-simple group algebras, J. Egypt. Math. Soc., 30, Article No. 17, 2022.
2. L.Creedon and J. Gildea, The structure of the unit group of the group algebra $F_{2^k}D_8$. Canad. Math. Bull., 54(2):237-243, 2011.
3. R.A. Ferraz, Simple components of center of $\frac{FG}{J(FG)}$. Comm. Algebra, 36(9):3191- 3199, 2008.
4. Aoudni, Y., Donald, C., Farouk, A., Sahay, K. B., Babu, D. V., Tripathi, V., & Dhabliya, D. (2022). Cloud security based attack detection using transductive learning integrated with

hidden markov model. Pattern Recognition Letters, 157, 16-26. doi:10.1016/j.patrec.2022.02.012
5. Dhabliya, D. (2021). Delay-tolerant sensor network (DTN) implementation in cloud computing. Paper presented at the Journal of Physics: Conference Series, , 1979(1) doi:10.1088/1742-6596/1979/1/012031 Retrieved from www.scopus.com
6. Dhabliya, D. (2019). Security analysis of password schemes using virtual environment. International Journal of Advanced Science and Technology, 28(20), 1334-1339. Retrieved from www.scopus.com
7. W. D. Gao, A. Geroldinger, F. Halter-Koch, Group algebras of finite abelian groups and their applications to combinatorial problems, Rocky Mountain J.Math., 39 (2008), 805-823.
8. Gildea, The structure of the unit group of the group algebra $F_{2^k}A_4$. Czechoslo-vak. Math. J., 61(136)(2):531-539, 2011.
9. Gildea, F. Monaghan, Units of some group algebras of groups of order 12 over any finite field of characteristic 3, Algebra Discrete Math. 11(1) (2011) 46-58.
10. T. Hurley, Group rings and rings of matrices, Int. J. Pure Appl. Math. 31 (2006), no. 3, 319-335.
11. T. Hurley, Convolutional codes from units in matrix and group rings, Int. J. Pure Appl. Math. 50 (2009), no. 3, 431-463.
12. P. Hurley, T. Hurley, Codes from zero-divisors and units in group rings, Interna-tional Journal of Information and Coding Theory (IJICOT), Vol. 1, No. 1, 20.
13. N. Makhijani,R.K. Sharma, and J.B. Srivastava, The unit group of finite group algebra of a generalized dihedral group. Asian European J. Math., 7(2):1450034, 2014.
14. N. Makhijani, R. K. Sharma, J. B. Srivastava, A note on units in $F_{p^m}D_{2p^n}$, Acta Math. Acad. Paedagog. Nyhzi. 30(1) (2014) 17-25.
15. N. Makhijani, R. K.Sharma, J. B. Srivastava, The unit group of F_qD_{30}, Serdica Math. J. 41(2-3) (2015) 185-198.
16. C.P. Miles, S.K. Sehgal, An Introduction to Group Rings, Kluwer Academic Pub-lishers, Dordrcht, 2002.
17. R. Sandling, Units in the modular group algebra of a finite abelian p-group, J. Pure Appl. Algebra, 33 (1984), 337-346.
18. R. K. Sharma, J. B. Srivastava, M. Khan, The unit group of FA_4, Publ. Math. Debrecen 71(1-2) (2007) 21-26.
19. R. K. Sharma, J. B. Srivastava, M. Khan, The unit group of FS_3, Acta Math. Acad. Paedagog. Nyhzi. 23(2) (2007) 129-142.
20. R. K. Sharma, P. Yadav, The unit group of Z_pQ_8, Algebras Groups Geom. 25(4) (2008) 425-429.
21. Swati Maheshwari, R.K.Sharma, The unit group of the group algebra $F_qSL(2,Z_3)$, J. Algebra Comb. Discrete Appl. 3(1) (2015) 1-6.
22. G. Tang, Y. Wei, Nanning, Y. Li, Units group of group algebras of some small groups, Czechoslovak Math. J. 64(1) (2014) 149-157.
23. Yogesh Kumar, R. K. Sharma and J. B. Srivastava,The structure of the unit group of the group algebra FS_5 where F is a finite field with Char $F = p > 5$, ActaMath. Acad. Paedagog. Nyh azi. (N.S.), 33(2) (2017),187-191.