Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **45** (2019), 217–224

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ON UNIT GROUP OF GROUP ALGEBRA OF PAULI'S GROUP OVER ANY FINITE FIELD OF ODD CHARACTERISTICS

Gaurav Mittal

Communicated by V. Drensky

Abstract. In this article, we characterize the unit group of the group algebra $\mathbb{F}_qG$ where $\mathbb{F}_q$ is a finite field with $q = p^k$ elements for prime $p > 2$ and G is the Pauli group of order 16.

1. Introduction. Let $\mathbb{F}_qG$ denote the group algebra of the finite group G over the of finite field $\mathbb{F}_q$ with $q = p^k$ elements for an odd prime, where p, k is any positive integer. We refer to [16] for elementary definitions and applications about group algebras. The description of the units of $\mathbb{F}_qG$ is a classical problem and very important from the applications point of view. Hurley in [9] suggested the construction of convolutional codes from the units in group rings. Many researchers from the latest decades have made great efforts in the description of these units. We shall discuss some of the literature survey of these efforts. Perlis and Walker in [17] studied the structure of FG for a finite abelian group G and

2010 *Mathematics Subject Classification:* 16U60, 20C05.
Key words: unit group, finite field, Wedderburn decomposition.

a finite field F. For dihedral groups, the structure of the unit group $U(FG)$ is discussed in [4, 7, 15, 13] where F is a finite field. Sharma et al. gave the structure of $U(FG)$ for the alternating group A_4 and the symmetric group S_3 in [18, 19], respectively. For some of the other non-abelian groups the structure of the unit groups of FG is established in [12, 21, 1, 2, 14, 20, 6].

Bakshi et al. [2] determined the Wedderburn decomposition of F_qG for a metabelian group G and a finite field F. The technique employed there involves the computation of primitive central idempotents which further involves the determination of strongly Shoda pair (H_1, H_2) [7, Definition 5] and the q-cyclotomic coset of the set $\mathrm{Irr}(H_2/H_1)$ of irreducible characters of H_2/H_1 over the algebraic closure $\overline{F}$ of F, corresponding to a generator of $\mathrm{Irr}(H_2/H_1)$, see [3, Theorem 7]. In this paper, we completely characterize $\mathbb{F}_qG$ and its unit group for all $p > 2$, when G is the Pauli group of order 16, without using strongly Shoda pair (H_1, H_2) and q-cyclotomic coset of the set $\mathrm{Irr}(H_2/H_1)$. For $p = 2$, Gildea [6] determined the structure of the unit group of the group algebra of the Pauli group. In this way the description of the unit group of the group algebra of the Pauli group over any finite field is complete. Note that the Pauli group of order 16 is isomorphic to $C_4 \circ D_8$, i.e., the central product of a cyclic group of order 4 and the dihedral group of order 8 where the central product of two groups a is way of producing a group from two smaller groups. See, for instance, [8] for its formal definition.

2. Preliminaries. Let $\mathbb{F}$ denote an arbitrary finite field, e is the exponent of G, and η a primitive e^{th} root of unity. Further as in [5], we define

$$I_{\mathbb{F}} = \{n \mid \eta \mapsto \eta^n \text{ is an automorphism of } \mathbb{F}(\eta) \text{ over } \mathbb{F}\}.$$

Clearly, $I_{\mathbb{F}}$ is a subgroup of the multiplicative group $\mathbb{Z}_e^*$ (the group of integers which are invertible with respect to multiplication modulo e) because the Galois group $\mathrm{Gal}\big(\mathbb{F}(\eta), \mathbb{F}\big)$ is a cyclic group and for any $\tau \in \mathrm{Gal}\big(\mathbb{F}(\eta), \mathbb{F}\big)$, there exists a positive integer $z \in \mathbb{Z}_e^*$ such that $\tau(\eta) = \eta^z$. An element $g \in G$ is p-regular provided p is not a factor of its order. Now, for any p-regular element $g \in G$, let the sum of all conjugates of g be denoted by γ_g, and the cyclotomic $\mathbb{F}$-class of γ_g be denoted by

$$S(\gamma_g) = \{\gamma_{g^n} \mid n \in I_{\mathbb{F}}\}.$$

The number of cyclotomic $\mathbb{F}$-classes and the cardinality of $S(\gamma_g)$ will be computed later on for the characterization of the unit groups.

Next, we recall two results from [5]. The first one relates the number of simple components of $\mathbb{F}G/J(\mathbb{F}G)$ with the number of cyclotomic $\mathbb{F}$-classes. Here $J(\mathbb{F}G)$ denotes the Jacobson radical of $\mathbb{F}G$. The second result is about the cardinality of a cyclotomic $\mathbb{F}$-class in G.

Theorem 2.1. *The number of simple components of* $\mathbb{F}G/J(\mathbb{F}G)$ *and the number of cyclotomic* $\mathbb{F}$*-classes in* G *are equal.*

Theorem 2.2. *Let* $\mathrm{Gal}(F(\eta)/F)$ *be cyclic and* j *be the number of cyclotomic* $\mathbb{F}$*-classes in* G*. If* K_i*,* $1 \leq i \leq j$*, are the simple components of the center of* $\mathbb{F}G/J(\mathbb{F}G)$ *and* S_i*,* $1 \leq i \leq j$*, are the cyclotomic* $\mathbb{F}$*-classes in* G*, then* $|S_i| = [K_i : \mathbb{F}]$ *for each* i *after suitable ordering of the indices if required.*

For the description of the structure of the unit group $U(\mathbb{F}G)$, we need to determine the Weddeeburn decomposition of the group algebra $\mathbb{F}G$ or, in other words, we need to determine the simple components of $\mathbb{F}G$. At this point, we can always claim $\mathbb{F}$ to be one of the simple components in the decomposition of $\mathbb{F}G/J(\mathbb{F}G)$. We give a simple proof of the same for the sake of completeness.

Lemma 2.1. *Let* S_1 *and* S_2 *be finite dimensional algebras over* $\mathbb{F}$*. Further, let* S_2 *be semisimple and* g *be an epimorphism of* S_1 *onto* S_2*. Then we have* $S_1/J(S_1) \cong S_3 + S_2$ *where* S_3 *is some semisimple* $\mathbb{F}$*-algebra.*

Proof. From [10, Chapter 1, Proposition 6.16], we have $J(S_1) \subseteq \mathrm{Ker}(g)$. This means that there exists a $\mathbb{F}$-algebra homomorphism g_1 from $S_1/J(S_1)$ to S_2 which is also onto. In other words, we have

$$g_1 : S_1/J(S_1) \longmapsto S_2 \text{ defined by } g_1(s + J(S_1)) = g(s), \qquad s \in S_1.$$

As $S_1/J(S_1)$ is semisimple, there exists an ideal I of $S_1/J(S_1)$ such that

$$S_1/J(S_1) = \mathrm{Ker}(g_1) \oplus I.$$

Our claim is that $I \cong S_2$. Note that any element $s \in S_1/J(S_1)$ can be uniquely written as $s = s_1 + s_2$ where $s_1 \in \mathrm{Ker}(g_1), s_2 \in I$. So, define

$$g_2 : S_1/J(S_1) \mapsto \mathrm{Ker}(g_1) \oplus S_2 \text{ by } g_2(s) = (s_1, g_1(s_2)).$$

Since $\mathrm{Ker}(g_1)$ is a semisimple algebra over $\mathbb{F}$ and S_2 is an isomorphic $\mathbb{F}$-algebra, claim and the result hold. □

Note that if $J(\mathbb{F}G) = 0$, then the above lemma implies that $\mathbb{F}$ is one of the simple components of $\mathbb{F}G$. Further, we characterize the set $I_{\mathbb{F}}$ defined in the beginning of this section.

Theorem 2.3 ([11, Theorem 2.21])**.** *Let* $\mathbb{F}$ *be a finite field with prime power order* q*. If* e *is such that* $\gcd(e, q) = 1$*,* η *a primitive* e^{th} *root of unity and* $|q|$ *is the order of* q *modulo* e*, then modulo* e *we have*

$$I_{\mathbb{F}} = \{1, q, q^2, \ldots, q^{|q|-1}\}.$$

The next result is Proposition 3.6.11 from [16] and is handy in determination of the commutative simple components in the Wedderburn decomposition of $\mathbb{F}G$.

Theorem 2.4. *If RG is a semisimple group algebra, then*

$$RG \cong R(G/G') \oplus \Delta(G, G'),$$

where G' is the commutator subgroup of G, $R(G/G')$ is the sum of all commutative simple components of RG, and $\Delta(G, G')$ is the sum of all others.

3. Unit group of $\mathbb{F}_q G$ where G is Pauli group of order 16.

In this section, we give our main result which is the characterization of the unit group of the finite group algebra $\mathbb{F}_q G$, where G is the Pauli group of order 16 and $p > 2$. The Pauli group G is a matrix group consisting of the Pauli matrices

$$I_2, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

together with the product of these matrices with $\pm i$ and -1. Observe that G has 10 conjugacy classes as discussed below:

1. Four conjugacy classes have only one element in their class. Representatives of these classes are $g_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $g_2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $g_3 = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}$, $g_4 = \begin{bmatrix} -i & 0 \\ 0 & -i \end{bmatrix}$. Also note that $|g_1| = 1$, $|g_2| = 2$, $|g_3| = |g_4| = 4$.

2. Each of the remaining 6 conjugacy classes with respective representatives $\{g_5, g_7, g_9, g_{11}, g_{13}, g_{15}\}$ have two elements. Explicitly, these classes are

$$\left\{ g_5 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \ g_6 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\}, \quad \left\{ g_7 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \ g_8 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\},$$

$$\left\{ g_9 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \ g_{10} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}, \quad \left\{ g_{11} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \ g_{12} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\},$$

$$\left\{ g_{13} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \ g_{14} = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \right\}, \quad \left\{ g_{15} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}, \ g_{16} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \right\}.$$

Also $|g_5| = |g_7| = |g_{13}| = 2, |g_9| = |g_{11}| = |g_{15}| = 4$.

Clearly, the exponent of G is 4 and as p is an odd prime, $\gcd(|G|, p) = 1$ which further implies that $J(\mathbb{F}_q G) = 0$. Now, before moving on to the Wedderburn decomposition of $\mathbb{F}_q G$, first we give the Wedderburn decomposition of $\mathbb{F}_q(C_2 \times C_2 \times C_2)$ for $p > 2$.

Lemma 3.1. *The Wedderburn decomposition of $\mathbb{F}_q H$ with $H = C_2 \times C_2 \times C_2$, where C_2 is a cyclic group of order 2, for $p > 2$ is $\mathbb{F}_q^{\oplus 8}$.*

Proof. Clearly, H has exponent 2. Further, being abelain each element of H is itself a conjugacy class and as $p > 2$, we have $J(\mathbb{F}_qH) = 0$. Therefore, the Wedderburn decomposition of $\mathbb{F}_qH$ is

$$\mathbb{F}_qH \cong \mathbb{F}_q \overset{7}{\underset{s=1}{\oplus}} M_{n_s}(\mathbb{F}_s),$$

where for each s, $\mathbb{F}_s$ is a finite extension of $\mathbb{F}_q$, $n_s \geq 1$. Now since $\mathbb{F}_qH$ is abelian, we have $n_s = 1$ for each s and hence the above implies

$$\mathbb{F}_qH \cong \mathbb{F}_q \overset{7}{\underset{r=1}{\oplus}} \mathbb{F}_r.$$

Since p is an odd, this means $p^k \equiv 1 \pmod 2$ for any k. Thus $I_{\mathbb{F}} = \{1\}$ and hence Theorems 2.1 and 2.2 imply that

$$\mathbb{F}_qH \cong \mathbb{F}_q^{\oplus 8}. \qquad \square$$

Theorem 3.1. *The Wedderburn decomposition of* $\mathbb{F}_qG$, *for* $p > 2$, *where* G *is the Pauli group of order* 16 *is as follows:*

(1) *If* $p \equiv 1 \pmod 4$ *and* k *is any positive integer or* $p \equiv 3 \pmod 4$ *and* k *is even, then*

$$\mathbb{F}_qG \cong \mathbb{F}_q^{\oplus 8} \oplus M_2(\mathbb{F}_q) \oplus M_2(\mathbb{F}_q).$$

(2) *If* $p \equiv 3 \pmod 4$ *and* k *is odd, then*

$$\mathbb{F}_qG \cong \mathbb{F}_q^{\oplus 8} \oplus M_2(\mathbb{F}_{q^2}).$$

Proof. Since $J(\mathbb{F}_qG) = 0$, the Wedderburn decomposition of $\mathbb{F}_qG$ is given by

$$\mathbb{F}_qG \cong \overset{r}{\underset{t=1}{\oplus}} M_{s_t}(\mathbb{F}_t),$$

where for each t, $\mathbb{F}_t$ is a finite extension of $\mathbb{F}_q$, $s_t \geq 1$. So, the Wedderburn decomposition of $\mathbb{F}_qG$ can be completely known if we know the integers s_t, and $\mathbb{F}_t$ for each t from 1 to r. Incorporating Lemma 2.1 and re-ordering the indexes (if needed) we obtain

$$\mathbb{F}_qG \cong \mathbb{F}_q \overset{r-1}{\underset{t=1}{\oplus}} M_{s_t}(\mathbb{F}_t). \tag{1}$$

Further, any odd prime p is either of the form $4z + 1$ where the integer $z \geq 1$ or $4z + 3$ where $z \geq 0$. So, now we consider both the possibilities. If $p \equiv 1 \pmod 4$ and k is any positive integer, then clearly

$$q = p^k \equiv 1 \pmod 4.$$

So, we have $|S(\gamma_g)| = 1$ for each $g \in G$ as $I_{\mathbb{F}} = \{1\}$. Now from (3.1), Theorems 2.1 and 2.2 we derive

$$\mathbb{F}_q G \cong \mathbb{F}_q \bigoplus_{t=1}^{9} M_{s_t}(\mathbb{F}_q).$$

Computing dimensions on both sides we obtain

$$15 = \sum_{t=1}^{9} s_t^2.$$

The only possible values of s_i's satisfying the above equation are $s_i = 1$ for $1 \leq i \leq 7$ and $s_i = 2$ for $8 \leq i \leq 9$. Thus, whenever $p \equiv 1 \pmod 4$, we have

$$\mathbb{F}_q G \cong \mathbb{F}_q^{\oplus 8} \oplus M_2(\mathbb{F}_q) \oplus M_2(\mathbb{F}_q). \tag{2}$$

Now we move on to the possibility $p \equiv 3 \pmod 4$. First let k be even. Then this means $q = p^k \equiv 1 \pmod 4$ and hence the Wedderburn decomposition of $\mathbb{F}_q G$ is similar to that in (3.2). If k is odd, then clearly

$$q = p^k \equiv 3 \pmod 4.$$

So, $I_{\mathbb{F}} = \{1, 3\}$ and this implies that

$$S(\gamma_{g_3}) = \{\gamma_{g_3}, \gamma_{g_4}\},$$

and $S_{\gamma_g} = \gamma_g$ for every other representative g. Therefore from (3.1), Theorems 2.1 and 2.2 we derive

$$\mathbb{F}_q G \cong \mathbb{F}_q \bigoplus_{t=1}^{7} M_{s_t}(\mathbb{F}_q) \oplus M_{s_8}(\mathbb{F}_{q^2}).$$

By the dimension formula, we have

$$15 = \sum_{t=1}^{7} s_t^2 + 2s_8^2.$$

From the above, we obtain two possibilities for s_i's. One is $s_i = 1$ for $1 \leq i \leq 5$, $s_6 = s_7 = 2$, $s_8 = 1$ and other one is $s_i = 1$ for $1 \leq i \leq 7$, $s_8 = 2$. Accordingly, we have

$$\mathbb{F}_q G \cong \mathbb{F}_q^{\oplus 8} \oplus M_2(\mathbb{F}_q) \oplus M_2(\mathbb{F}_q) \oplus \mathbb{F}_{q^2}$$

or

$$\mathbb{F}_q G \cong \mathbb{F}_q^{\oplus 8} \oplus M_2(\mathbb{F}_{q^2}).$$

Now observe that the commutator subgroup of G is isomorphic to C_2 and G/G' is isomorphic to $C_2 \times C_2 \times C_2$. So by Lemma 3.1 and Theorem 2.4, we conclude that from the choices obtained above, we have

$$\mathbb{F}_q G \cong \mathbb{F}_q^{\oplus 8} \oplus M_2(\mathbb{F}_{q^2}). \qquad \square$$

The following is now straightforward.

Corollary 3.1. *The unit group of* $\mathbb{F}_q G$*, for* $p > 2$*, where* G *is the Pauli group of order* 16 *is*

(1) *If* $p \equiv 1 \pmod 4$ *and* k *is any positive integer or* $p \equiv 3 \pmod 4$ *and* k *is even, then*

$$U(\mathbb{F}_q G) \cong (\mathbb{F}_q^*)^{\times 8} \times GL_2(\mathbb{F}_q) \times GL_2(\mathbb{F}_q).$$

(2) *If* $p \equiv 3 \pmod 4$ *and* k *is odd, then*

$$U(\mathbb{F}_q G) \cong (\mathbb{F}_q^*)^{\times 8} \times GL_2(\mathbb{F}_{q^2}).$$

Here $\mathbb{F}_q^*$ *is the unit group of* $\mathbb{F}_q$ *and* $GL_2(\mathbb{F}_q)$*,* $GL_2(\mathbb{F}_{q^2})$ *are the general linear groups of* 2×2 *invertible matrices over the fields* $\mathbb{F}_q$ *and* $\mathbb{F}_{q^2}$*, respectively.*

REFERENCES

[1] G. K. Bakshi, S. Gupta, I. B. S. Passi. The structure of finite semisimple metacyclic group algebras. *J. Ramanujan Math. Soc.* **28**, *2* (2013), 141–158.

[2] G. K. Bakshi, S. Gupta, I. B. S. Passi. The algebraic structure of finite metabelian group algebra. *Comm. Algebra* **43**, *6* (2015), 2240–2257.

[3] O. Broche, Á. del Río. Wedderburn decomposition of finite group algebras. Finite Fields Appl. **13**, *1* (2007), 71–79.

[4] L. Creedon, J. Gildea. The structure of the unit group of the group algebra $\mathbb{F}_{2^k} D_8$. *Canad. Math. Bull.* **54**, *2* (2011), 237–243.

[5] R. A. Ferraz. Simple components of the center of $\mathbb{F}G/J(\mathbb{F}G)$. *Comm. Algebra* **36**, *9* (2008), 3191–3199.

[6] J. Gildea. The structure of the unit group of the group algebra of Pauli's group over any field of characteristic 2. *Int. J. Algebra Comput.* **20**, *5* (2010), 721–729.

[7] J. Gildea, F. Monaghan. Units of some group algebras of groups of order 12 over any finite field of characteristics 3. *Algebra Discrete Math.* **11**, *1* (2011), 46–58.

[8] D. Gorenstein. Finite groups, 2nd ed. New York: Chelsea Publishing Co., 1980.

[9] T. Hurley. Convolutional codes from units in matrix and group rings. *Int. J. Pure Appl. Math.* **50**, *3* (2009), 431–463.

[10] G. Karpilovsky. The Jacobson radical of group algebras. North-Holland Mathematics Studies, vol. **135**. Notas de Matematica [Mathematical Notes], vol. **115**. Amsterdam, North-Holland Publishing Co., 1987.

[11] R. Lidl, H. Niederreiter. Introduction to finite fields and their applications. New York, Cambridge University Press, 1986.

[12] S. Maheshwari, R. K. Sharma. The unit group of group algebra $\mathbb{F}SL(2,\mathbb{Z}_3)$. *J. Algebra Comb. Discrete Struct. Appl.* **3**, *1* (2015), 1–6.

[13] N. Makhijani, R. K. Sharma, J. B. Srivastava. A note on units in $\mathbb{F}_{p^m}D_{2p^n}$. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)* **30**, *1* (2014), 17–25.

[14] N. Makhijani, R. K. Sharma, J. B. Srivastava. The unit group of algebra of circulant matrices. *Int. J. Group Theory* **3**, *4* (2014), 13–16.

[15] N. Makhijani, R. K. Sharma, J. B. Srivastava. Units in finite dihedral and quaternion group algebras. J. Egyptian Math. Soc. **24**, *1* (2016), 5–7.

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

[17] S. Perlis, G. L. Walker. Abelian group algebras of finite order. *Trans. Amer. Math. Soc.* **68** (1950), 420–426.

[18] R. K. Sharma, J. B. Srivastava, M. Khan. The unit group of $\mathbb{F}A_4$. *Publ. Math. Debrecen* **71**, *1–2* (2007), 21–26.

[19] R. K. Sharma, J. B. Srivastava, M. Khan. The unit group of $\mathbb{F}S_3$. *Acta Math. Acad. Paedagog. Nyházi. (N.S.)* **23**, *2* (2007), 129–142.

[20] R. K. Sharma, P. Yadav. The unit group of $\mathbb{Z}_pQ_8$. *Algebras Groups Geom.* **25**, *4* (2008), 425–429.

[21] G. Tang, Y. Wei, Nanning, Y. Li. Units group of group algebras of some small groups. *Czechoslovak Math. J.* **64(139)**, *1* (2014), 149–157.

Department of Mathematics
Indian Institute of Technology Roorkee
Roorkee, India
e-mail: `gmittal@ma.iitr.ac.in`

Received January 29, 2019