Serdica

Mathematical Journal

Сердика

Математическо списание

Serdica Math. J. **46** (2020), 253–260

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

WHEN THE WEDDERBURN DECOMPOSITION OF THE SEMISIMPLE GROUP ALGEBRA F_qG IMPLIES THAT OF $F_q(G \times C_2)$?

Gaurav Mittal, R. K. Sharma

Communicated by V. Drensky

Abstract. In this short note we give a condition under which the Wedderburn decomposition (WD) of the semisimple group algebra $F_q(G \times C_2)$ can be directly deduced from the WD of the semisimple group algebra F_qG, where F_q is a finite field with $\mathrm{char}(F_q) > 2$, G is an arbitrary finite group and C_2 is a group of order 2. To complement the abstract theory with an example, we determine the WD of the semisimple group algebra $F_q(A_5 \times C_2)$, where A_5 is the alternating group from that of F_qA_5.

Let F_q be the field with $q = p^k$ elements, where p is an odd prime and $k \in \mathbb{Z}^+$. It is well known that the group algebra F_qG of a finite group G is semisimple and therefore isomorphic to a direct sum of matrix rings over finite fields of characteristic p if and only if p does not divide $|G|$ [3]. To be more

2020 *Mathematics Subject Classification:* 20C05.
Key words: Wedderburn decomposition, group algebra.

precise, for a semisimple group algebra F_qG, we have $F_qG \cong \bigoplus_{t=1}^{j} M_{n_t}(F_{q_t})$. This decomposition of F_qG as a direct sum of matrix rings is known as Wedderburn decomposition (WD) [3]. In this paper, we study the following problem: Can we deduce the WD of the semisimple group algebra $F_q(G \times C_2)$ from the WD of F_qG, where F_q is a finite field, G is an arbitrary finite group and C_2 is a cyclic group of order 2.

In order to solve the above problem, first, we recall the procedure of determination of the WD of a semisimple group algebra F_qG. Let e denote the exponent of G, ζ be a primitive e^{th} root of unity and F be an arbitrary finite field. On the lines of [1], we define $I_F = \{n \mid \zeta \mapsto \zeta^n$ is an automorphism of $F(\zeta)$ over $F\}$. Since the Galois group $\mathrm{Gal}\big(F(\zeta), F\big)$ is a cyclic group, for any $\tau \in \mathrm{Gal}\big(F(\zeta), F\big)$ there exists a positive integer s which is invertible modulo e such that $\tau(\zeta) = \zeta^s$. In other words, I_F is a subgroup of the multiplicative group $\mathbb{Z}_e^*$. For any p-regular element $g \in G$, i.e. an element whose order is not divisible by p, let the sum of all conjugates of g be denoted by γ_g, and the cyclotomic F-class of γ_g be denoted by $S(\gamma_g) = \{\gamma_{g^n} \mid n \in I_F\}$.

Next, we recall some results which will be used in the proof of our main result.

Lemma 1 ([1])**.** *The number of simple components of $FG/J(FG)$ and the number of cyclotomic F-classes in G are equal.*

Lemma 2 ([1])**.** *Let ζ be defined as above and j be the number of cyclotomic F-classes in G. If $K_i, 1 \leq i \leq j$, are the simple components of the center of $FG/J(FG)$ and $S_i, 1 \leq i \leq j$, are the cyclotomic F-classes in G, then $|S_i| = [K_i : F]$ for each i after suitable ordering of the indices.*

Proposition 1 ([3])**.** *If FG is a semisimple group algebra and H is a normal subgroup of G, then $FG \cong F\big(G/H\big) \oplus \Delta(G, H)$, where $\Delta(G, H)$ is the left ideal of FG generated by the set $\{h - 1 \mid h \in H\}$.*

Let us now discuss a series of lemmas which will assist in proving our main result. Let $n(G)$ denote the number of conjugacy classes of a finite group G.

Lemma 3. *If $n(G) = r$, then $n(G \times C_2) = 2r$.*

P r o o f. Let $\{[g_i]\}_{i=1}^{r}$ be the conjugacy classes of G having representatives g_i and let $C_2 = \{e, \alpha\}$. Then, it is easy to see that the conjugacy classes of $G \times C_2$ are given by $\{[h_i]\}_{i=1}^{2r}$, where $h_i = (g_i, e)$ for $1 \leq i \leq r$ and $h_i = (g_{i-r}, \alpha)$ for $r + 1 \leq i \leq 2r$. $\square$

Lemma 4. *Let e be the exponent of a group G of odd order and $p^k \equiv a \pmod{e}$, where $0 < a < e$, p is an odd prime such that $p \nmid (\text{exponent}\,(G))$ and k is a positive integer. Then $p^k \equiv a \pmod{2e}$ or $p^k \equiv a + e \pmod{2e}$ accordingly as a is odd or even, respectively.*

Proof. Let us assume that $p^k \equiv b \pmod{2e}$ for some $0 \le b \le 2e$ which means that $p^k \equiv b \pmod{e}$. It is given that $p^k \equiv a \pmod{e}$, therefore, $b \equiv a \pmod{e}$. This asserts that b is either a or $a+e$, since $0 \le b \le 2e$. Further, if a is odd, then we must have $p^k \equiv a \pmod{2e}$, otherwise if $p^k \equiv a+e \pmod{2e}$, then p^k becomes even which is not so as p is odd. Similarly, if a is even, then we must have $p^k \equiv a + e \pmod{2e}$. □

Lemma 5. *Let e be an odd positive integer, $a \in \mathbb{Z}_e^*$ and $G_1 = \langle a \rangle$ be a subgroup of $\mathbb{Z}_e^*$ generated by a having order s.*

(1) *If a is odd, then the subgroup G_2 generated by a in $\mathbb{Z}_{2e}^*$; or*

(2) *if a is even, then the subgroup G_3 generated by $a+e$ in $\mathbb{Z}_{2e}^*$,*

is also of the order s. To be more precise, if $G_1 = \{1, a_1, \ldots, a_{s-1}\}$, then G_2 or $G_3 = \{1, b_1, \ldots, b_{s-1}\}$, where, for each i, $b_i = a_i$ or $a_i + e$ accordingly as a_i is odd or even.

Proof. It is clear by the properties of Euler's function φ that $|\mathbb{Z}_e^*| = |\mathbb{Z}_{2e}^*| = \varphi(e)$. Let x be the order of a in $\mathbb{Z}_{2e}^*$ for a odd. We need to prove that $x = s$. By definition, we have $a^x \equiv 1 \pmod{2e}$ which means $a^x \equiv 1 \pmod{e}$. But the order of a in $\mathbb{Z}_e^*$ is s which means that $x \ge s$. Let, if possible, $x > s$. This gives $a^s \not\equiv 1 \pmod{2e}$. Also $a^s \equiv 1 \pmod{e}$. On combining the last two congruences, we obtain that e divides $a^s - 1$ and $2e$ does not divide $a^s - 1$. But this is a contradiction since e is odd and it divides an even quantity $a^s - 1$ which means the quotient $\dfrac{a^s-1}{e}$ must be divisible by 2. Thus, $x = s$. A similar result also holds for a even. The rest part of the statement can be proved on the lines of proof of the Lemma 4. □

Lemma 6. *Let F_q be the field with $q = p^k$ elements, where p is an odd prime and $k \in \mathbb{Z}^+$. Let m number of representatives of conjugacy classes of G have $|S(\gamma_g)| = n$ (we use the general symbol g to denote a representative of G). Then, exactly $2m$ number of representatives of conjugacy classes of $H := G \times C_2$ have $|S(\gamma_h)| = n$.*

Proof. Let $\{[g_i]\}_{i=1}^m$ be the conjugacy classes of G having representatives g_i such that $|S(\gamma_{g_i})| = n$ for each i. We have already discussed that I_F is a subgroup of the multiplicative group $\mathbb{Z}_e^*$ in F_qG. In F_qH, I_F is a subgroup of the multiplicative group $\mathbb{Z}_{2e}^*$. To make a distinction, let $I_F^1 = I_F$ in F_qG and $I_F^2 = I_F$ in F_qH. Next, we consider the following two possibilities: (i) the exponent of G is even and (ii) the exponent of G is odd.

For the possibility (i), exponent$(G \times C_2) = \mathrm{LCM}(\text{exponent}(G), 2)$ which means that exponent(H) = exponent(G). Therefore, $I_F^1 = I_F^2$ for both the group algebras F_qG and F_qH and contains only odd numbers that are co-prime to e. Consequently, we claim that the following $2m$ conjugacy classes of H given by $\{[h_i]\}_{i=1}^{2m}$, where $h_i = (g_i, e)$ for $1 \leq i \leq m$ and $h_i = (g_{i-m}, \alpha)$ for $m+1 \leq i \leq 2m$, where $C_2 = \{e, \alpha\}$ are such that $|S(\gamma_{h_i})| = n$ for each i. To see this claim, observe that by the definition for any h_i with $1 \leq i \leq m$,

$$S(\gamma_{h_i}) = \{\gamma_{h_i^s} \mid s \in I_F^2\} = \{\gamma_{(g_i,e)^s} \mid s \in I_F^2\} = \{\gamma_{(g_i^s,e)} \mid s \in I_F^2\},$$

which means that $|S(\gamma_{h_i})| = |S(\gamma_{g_i})| = n$ since $I_F^1 = I_F^2$. The same result is also true for $m+1 \leq i \leq 2m$ since the elements of I_F^2 are odd. Thus, the claim holds which proves the result for the possibility (i).

Next we move on to the second possibility: (ii) the exponent of G is odd. Here, we have exponent$(H) = 2\cdot$exponent (G). Let $q = p^k \equiv a \pmod{e}$. Then we have that $I_F^1 = (\langle a \rangle \pmod{e})$, i.e. I_F^1 is a subgroup generated by a in $\mathbb{Z}_e^*$. Then from Lemma 4 and 5 we conclude that modulo $2e$, I_F^2 is a subgroup generated by a or $a+e$ (accordingly as a is odd or even) in $\mathbb{Z}_{2e}^*$. Therefore, I_F^1 and I_F^2 have the same number of elements for both the group algebras F_qG and F_qH, however, the elements are not the same. Moreover, from Lemma 6, we know that if $I_F^1 = \{1, a_1, \ldots, a_{s-1}\}$, then $I_F^2 = \{1, b_1, \ldots, b_{s-1}\}$, where, for each i, $b_i = a_i$ or $a_i + e$ accordingly as a_i is odd or even.

Consequently, we claim that the following $2m$ conjugacy classes of H given by $\{[h_i]\}_{i=1}^{2m}$, where $h_i = (g_i, e)$ for $1 \leq i \leq m$ and $h_i = (g_{i-m}, \alpha)$ for $m+1 \leq i \leq 2m$, where $C_2 = \{e, \alpha\}$ are such that $|S(\gamma_{h_i})| = n$ for each i. To see this claim, observe that by definition for any h_i with $1 \leq i \leq m$,

$$S(\gamma_{h_i}) = \{\gamma_{h_i^s} \mid s \in I_F^2\} = \{\gamma_{(g_i,e)^s} \mid s \in I_F^2\} = \{\gamma_{(g_i^s,e)} \mid s \in I_F^2\}.$$

Note that we have already deduced that $s \in I_F^2$ is either a_i or $a_i + e$, where $a_i \in I_F^1$, and as the exponent of G is e, we have that $|S(\gamma_{h_i})| = |S(\gamma_{g_i})| = n$. For $m+1 \leq i \leq 2m$, we have

$$S(\gamma_{h_i}) = \{\gamma_{h_i^s} \mid s \in I_F^2\} = \{\gamma_{(g_i,\alpha)^s} \mid s \in I_F^2\} = \{\gamma_{(g_i^s,\alpha)} \mid s \in I_F^2\},$$

since every s in I_F^2 is an odd number. Thus, we again have that $|S(\gamma_{h_i})| = |S(\gamma_{g_i})| = n$. Hence, the result holds. □

We are now ready to state the main result of the paper.

Theorem 1. *Let F_q be the field with $q = p^k$ elements, where p is an odd prime and $k \in \mathbb{Z}^+$. Suppose that the WD of F_qG is known, i.e.*

$$F_qG \cong \bigoplus_{t=1}^{j_1} M_{n_t}(F_q) \bigoplus_{t=j_1+1}^{j_2} M_{n_t}(F_{q^2}) \bigoplus \cdots \bigoplus_{t=j_{n-1}+1}^{j_n} M_{n_t}(F_{q^n}), \tag{1}$$

where $j_i, n_t \in \mathbb{Z}^+$ for each i, t. Further, suppose that the following equation

$$\left(\sum_{t=1}^{j_1} x_t^2 + 2 \sum_{t=j_1+1}^{j_2} x_t^2 + \cdots + n \sum_{t=j_{n-1}+1}^{j_n} x_t^2 \right) - |G| = 0 \tag{2}$$

has a unique solution in $(\mathbb{Z}^+)^{j_n}$ given by $(n_1, n_2, \ldots, n_{j_1}, n_{j_1+1}, \ldots, n_{j_n})$. Then the WD of $F_q(G \times C_2)$ is the following:

$$F_q(G \times C_2) \cong \bigoplus_{t=1}^{j_1} M_{n_t}(F_q) \bigoplus_{t=j_1+1}^{j_2} M_{n_t}(F_{q^2}) \bigoplus \cdots \bigoplus_{t=j_{n-1}+1}^{j_n} M_{n_t}(F_{q^n})$$
$$\bigoplus_{t=1}^{j_1} M_{n_t}(F_q) \bigoplus_{t=j_1+1}^{j_2} M_{n_t}(F_{q^2}) \bigoplus \cdots \bigoplus_{t=j_{n-1}+1}^{j_n} M_{n_t}(F_{q^n}).$$

P r o o f. It is given that

$$F_qG \cong \bigoplus_{t=1}^{j_1} M_{n_t}(F_q) \bigoplus_{t=j_1+1}^{j_2} M_{n_t}(F_{q^2}) \bigoplus \cdots \bigoplus_{t=j_{n-1}+1}^{j_n} M_{n_t}(F_{q^n}).$$

From the above WD, we can easily see that F_qG has j_n simple components which means that G has j_n cyclotomic F-classes (see Lemma 1). Also, by utilizing Lemma 2, we conclude that j_1 representatives of conjugacy classes of G have $|S(\gamma_g)| = 1$ (we keep the general notation γ_g for each element g), $2(j_2 - j_1)$ representatives of G have $|S(\gamma_g)| = 2$ (since if for conjugates $a, b \in G$, $S(\gamma_a) = \{\gamma_a, \gamma_b\}$ then $S(\gamma_b) = \{\gamma_a, \gamma_b\}$ but we only need to consider the cyclotomic F-class either for γ_a or γ_b, not for both), $\ldots$, $n(j_n - j_{n-1})$ representatives of G have $|S(\gamma_g)| = n$. Incorporate Lemma 6 to see that $2j_1$ representatives of $G \times C_2$ have $|S(\gamma_g)| = 1$, $4(j_2 - j_1)$ representatives of $G \times C_2$ have $|S(\gamma_g)| = 2, \ldots, 2n(j_n - j_{n-1})$ representatives of $G \times C_2$ have $|S(\gamma_g)| = n$.

To this end, let us now talk about the WD of $F_q(G \times C_2)$. Suppose that $n(G) = r$. Then Lemmas 1 and 2 (with $J(FG) = 0$) imply that

$$r = j_1 + 2(j_2 - j_1) + \cdots + n(j_n - j_{n-1}).$$

In virtue of Lemma 3 we have $n(G \times C_2) = 2r$. We rewrite the above equation as

$$2r = (2j_1) + 2(2(j_2 - j_1)) + \cdots + n(2(j_n - j_{n-1})).$$

Consequently, we have

$$F_q(G \times C_2) \cong \bigoplus_{t=1}^{2j_1} M_{z_t}(F_q) \bigoplus_{t=2j_1+1}^{2j_2} M_{z_t}(F_{q^2}) \bigoplus \cdots \bigoplus_{t=2j_{n-1}+1}^{2j_n} M_{z_t}(F_{q^n}), \tag{3}$$

where $j_i, z_t \in \mathbb{Z}^+$ for each i, t. Observe that C_2 is a normal subgroup of $G \times C_2$. Using this fact Proposition 1 yields:

$$F(G \times C_2) \cong FG \oplus \Delta(G \times C_2, C_2). \tag{4}$$

On utilizing (1) in (4) and the comparing the result with (3) gives (after reordering of indices, if required)

$$F_q(G \times C_2) \cong \bigoplus_{t=1}^{j_1} M_{n_t}(F_q) \bigoplus_{t=j_1+1}^{j_2} M_{n_t}(F_{q^2}) \bigoplus \cdots \bigoplus_{t=j_{n-1}+1}^{j_n} M_{n_t}(F_{q^n})$$

$$\bigoplus_{t=1}^{j_1} M_{z_t}(F_q) \bigoplus_{t=j_1+1}^{j_2} M_{z_t}(F_{q^2}) \bigoplus \cdots \bigoplus_{t=j_{n-1}+1}^{j_n} M_{z_t}(F_{q^n}).$$

It is worth to mention that in the above WD, the only variables need to find out are $z_i, 1 \leq i \leq j_n$. Apply the dimension formula in the above WD to see that

$$|G \times C_2| = 2|G| = \left(\sum_{t=1}^{j_1} x_t^2 + 2 \sum_{t=j_1+1}^{j_2} x_t^2 + \cdots + n \sum_{t=j_{n-1}+1}^{j_n} x_t^2 \right)$$

$$+ \left(\sum_{t=1}^{j_1} z_t^2 + 2 \sum_{t=j_1+1}^{z_2} z_t^2 + \cdots + n \sum_{t=j_{n-1}+1}^{j_n} z_t^2 \right).$$

Due to (1) (applying the dimension formula in it), the above can be written as

$$|G| = \sum_{t=1}^{j_1} z_t^2 + 2 \sum_{t=j_1+1}^{z_2} z_t^2 + \cdots + n \sum_{t=j_{n-1}+1}^{j_n} z_t^2.$$

Finally, employ (2) in above to deduce that $z_i = n_i$ for $1 \leq i \leq j_n$. This completes the proof. □

In order to see the worthiness of the theory developed in this paper, we consider a group algebra and show that the conditions of Theorem 1 are satisfied by it.

Consider the alternating group $A_5 = \langle a, b | a^2, b^3, (ab)^5 \rangle$ for $a = (1,2)(3,4)$ and $b = (1,3,5)$. Note that A_5 has 5 conjugacy classes, with representatives $1, a, b, ab$ and $(ab)^2$. For any $p > 5$, the WD of $F_q A_5$ is already deduced in [2, Theorem 4.1]. However, in order to see how the conditions of Theorem 1 are satisfied by the group algebra $F_q A_5$, we quickly find its WD. For $q = p^k$ with $p > 5$, we have the following two possibilities: (i) $q \equiv \pm 1 \pmod 5$. (ii) $q \equiv \pm 2 \pmod 5$. For the case (i), we have $S(\gamma_g) = \gamma_g$ for each representative g of the conjugacy classes of A_5. Therefore, Lemmas 1 and 2 imply that $F_q A_5 \cong \bigoplus_{r=1}^{5} M_{n_r}(\mathbb{F}_q)$. Applying the dimension formula in this yields $60 = \sum_{n_r=1}^{5} n_r^2$, $n_r \geq 1$. This equation has a unique solution given by $(1,3,3,4,5)$. Therefore, due to Theorem 1, we have

$$F_q(A_5 \times C_2) \cong F_q^2 \oplus M_3(F_q)^4 \oplus M_4(F_q)^2 \oplus M_5(F_q)^2.$$

For the case (ii), we have $S(\gamma_{ab}) = \{\gamma_{ab}, \gamma_{(ab)^2}\}$ and $S(\gamma_g) = \gamma_g$ for the rest of the representatives g of the conjugacy classes of A_5. Therefore, Lemmas 1 and 2 imply that $F_q A_5 \cong \bigoplus_{r=1}^{3} M_{n_r}(\mathbb{F}_q) \oplus M_{n_4}(\mathbb{F}_{q^2})$. Applying the dimension formula in this yields $60 = \sum_{n_r=1}^{3} n_r^2 + 2n_4^2, n_r \geq 1$. This equation has a unique solution given by $(1,4,5,3)$. Therefore, due to Theorem 1, we have

$$F_q(A_5 \times C_2) \cong F_q^2 \oplus M_4(F_q)^2 \oplus M_5(F_q)^2 \oplus M_3(F_q)^2.$$

REFERENCES

[1] R. A. Ferraz. Simple components of the center of $FG/J(FG)$. *Comm. Algebra* **36** (2008), 3191–3199.

[2] N. Makhijani, R. K. Sharma, J. B. Srivastava. A note on the structure of $\mathbb{F}_{p^k} A_5 / J(\mathbb{F}_{p^k} A_5)$. *Acta Sci. Math. (Szeged)* **82**, *1–2* (2016), 29–43.

[3] C. Polcino Milies, S. K. Sehgal. An Introduction to Group Rings. Algebra and Applications, vol. **1**. Dordrecht, Kluwer Academic Publishers, 2002.

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

R. K. Sharma
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi, India
e-mail: rksharmaiitd@gmail.com

Received November 18, 2020