Finite Metabelian Group Algebras

Shalini Gupta

Department of Mathematics, Punjabi University, Patiala, India

email: gupta_math@yahoo.com

Keywords: semisimple group algebra, primitive central idempotents, Wedderburn decomposition, metabelian groups.

Abstract. Given a finite metabelian group G, whose central quotient is abelian (not cyclic) group of order $p^2$, $p$ odd prime, the objective of this paper is to obtain a complete algebraic structure of semisimple group algebra $\mathbb{F}_q[G]$ in terms of primitive central idempotents, Wedderburn decomposition and the automorphism group.

1. Introduction

Let $F$ be a field and $G$ be a finite group such that the group algebra $F[G]$ is semisimple. A fundamental problem in the theory of group algebras is to understand the complete algebraic structure of semisimple group algebra $F[G]$. In the recent years, a lot of work has been done to solve this problem [1,2,5,7,8,9]. Bakshi et.al [3] have solved this problem for semisimple finite group algebra $\mathbb{F}_q[G]$, where $\mathbb{F}_q$ is a finite field of order $q$ and $G$ is a finite metabelian group. They further illustrated their algorithm by explicitly finding a complete set of primitive central idempotents, Wedderburn decomposition and the automorphism group of semisimple group algebra of certain groups whose central quotient is Klein’s four-group. In the present paper, a complete algebraic structure of semisimple group algebra $\mathbb{F}_q[G]$ for some finite groups $G$, whose central quotient, $G/Z(G)$, is the direct product of two cyclic groups of order $p$, $p$ odd prime, is obtained. It is known [6] that finitely generated groups $G$, whose central quotient is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ break into nine classes. The complete algebraic structure of $\mathbb{F}_q[G]$, for group $G$ in the two of the nine classes, is obtained in the present paper.

2. Notation

Let $G$ be a finite group of order coprime to $q$ and $\text{Irr}(G)$ denotes the set of all irreducible characters of $G$ over $\overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$. Let $H < K \leq G$ such that $K/H$ is cyclic of order $n$ and $T = N_G(H) \cap N_G(K)$, where $N_G(H)$ denotes the normalizer of $H$ in $G$. Let $\mathcal{C}(K/H)$ denotes the set of $q$-cyclotomic sets of $\text{Irr}(K/H)$ containing the generators of $\text{Irr}(K/H)$. Suppose that $T$ acts on $\mathcal{C}(K/H)$ by conjugation, then it is easy to see that stabilizer of any $\mathcal{C} \in \mathcal{C}(K/H)$ remains the same. Let $E_{\mathcal{C}}(K/H)$ denotes the stabilizer of any $\mathcal{C} \in \mathcal{C}(K/H)$ and let $\mathcal{R}(K/H)$ denotes the set of distinct orbits of $\mathcal{C}(K/H)$ under the action of $T$ on $\mathcal{C}(K/H)$. Observe that

$$|\mathcal{R}(K/H)| = \frac{\phi(n)|E_{\mathcal{C}}(K/H)|}{|T|\text{ord}_n(q)},$$

where $\text{ord}_n(q)$ denotes the order of $q$ modulo $n$. 

SciPress applies the CC-BY 4.0 license to works we publish: https://creativecommons.org/licenses/by/4.0/
For $C \in \mathcal{C}(K/H), \chi \in \mathcal{C}$ and $\zeta_n$ a primitive $n$th root of unity in $\mathbb{F}_q$, set

$$e_C(K/H) = |K|^{-1} \sum_{g \in K} \text{tr}_{F_q(\zeta_n)/F_q}(\chi(g))g^{-1},$$

and $e_C(G,K,H)$ as the sum of distinct $G$-conjugates of $e_C(K/H)$.

3. Metabelian group algebras

The notation used in [4] will be followed: For a normal subgroup $N$ of $G$, let $A_N/N$ be an abelian normal subgroup of $G/N$ of maximal order. Let $D_N$ be the set of subgroups $D/N$ of $A_N/N$ such that $A_N/D$ is cyclic and $T_{G/N}$ be the set of representatives of $D_N$ under the equivalence relation of conjugacy of subgroups of $G/N$. Define

$$S_{G/N} := \{(D/N, A_N/N) \mid D/N \in T_{G/N}, D/N \text{ core-free in } G/N\}.$$

Let

$$S := \{(N, D/N, A_N/N) \mid N \triangleleft G, S_{G/N} \neq \emptyset, (D/N, A_N/N) \in S_{G/N}\}.$$

We are now ready to recall the theorem describing the complete algebraic structure of semisimple finite metabelian group algebras:

Theorem 1 [3]: Let $G$ be a finite metabelian group of order coprime to $q$. Then,

(i) A complete set of primitive central idempotents of semisimple group algebra $\mathbb{F}_q[G]$ is given by the set $\{e_C(G, A_N, D) \mid (N, D/N, A_N/N) \in S, C \in \mathfrak{R}(A_N/D)\}$;

(ii) the simple component corresponding to primitive central idempotent $e_C(G, A_N, D)$ is

$$F_q[G]e_C(G, A_N, D) \cong M_{[\mathfrak{R}(A_N/D)]}(F_q^{ord(A_N,D)}),$$

where $M_n(R)$ denotes the ring of $n \times n$ matrices over the ring $R$ and

$$o(A_N, D) = \frac{\text{ord}\,(A_N, D) \cdot (q)}{[E_G(A_N, D) : A_N^D]}.$$ Moreover the number of such simple components is $|\mathfrak{R}(A_N,D)|$.

4. Groups whose central quotient is abelian (not cyclic) group of order $p^2$

Conelissen and Milies [6] have classified indecomposable finitely generated groups $G$, such that $G/Z(G) \cong C_p \times C_p$, into nine classes. In all of these classes, $G = \langle a, b, Z(G) \rangle$ with some more relations as described in following table:
It can be seen easily that $G$ is finite metabelian group only in five classes. Out of these five classes, we will give a complete algebraic structure of $\mathbb{F}_q[G]$, for $G = \mathfrak{G}_1$ and $\mathfrak{G}_2$ only. The rest of the cases can be dealt similarly. Throughout this section $\mathbb{F}_q$ is a finite field with $q$ elements and $\gcd(p,q) = 1$. Let $\text{ord}_p(q)$, the order of $q$ modulo $p$, be $f$ and $e = \frac{p-1}{f}$. Write $q^d = 1 + p^d c$, where $p$ does not divide $c$. Then for $l \geq 1$,

$$\text{ord}_p(q) = \begin{cases} f, & l \leq d, \\ fp^{l-d}, & l \geq d + 1. \end{cases}$$

### 4.1. Structure of $\mathbb{F}_q[\mathfrak{G}_1]$

Let $G$ be a group of type $\mathfrak{G}_1$. Thus $G$ has the following representation:

$$G = \langle a, b, c \mid a^p = b^p = c^p m = 1, b^{-1} a^{-1} ba = c^{p^{m-1}}, c \text{ central in } G \rangle (1)$$
where $p$ is prime and $m \geq 1$. For $p = 2$, the complete algebraic structure of $\mathbb{F}_q[G]$ can be read from [3]. Suppose $p$ is an odd prime. For $m \geq 2$, define

$$\begin{align*}
K_0 &= \langle 1 \rangle, 
K_1 := \langle c, a \rangle, 
K_2^{(i)} := \langle c, a' b \rangle, 
K_3^{(i)} := \langle a, b, c^p \rangle, 
0 \leq i \leq p - 1, \\
K_4^{(i,j)} := \langle a, c^p b^j \rangle, 
K_5^{(i,j)} := \langle b, c^p a^j \rangle, 
K_6^{(i,j,k)} := \langle c^p a^j, c^p b^k \rangle, 
0 \leq i \leq m - 2, 1 \leq j, k \leq p - 1.
\end{align*}$$

**Theorem 2.** A complete set of primitive central idempotents of semisimple group algebra $\mathbb{F}_q[G]$, $G$ of type $G_1$, is given as follows:

**Primitive central idempotents of $\mathbb{F}_q[G]$ for $m = 1$:**

$$e_c(G,G,G), \ C \in \mathcal{R}(G/G);$$
$$e_c(G,G,\langle c, a' b \rangle), \ C \in \mathcal{R}(G/\langle c, a' b \rangle), \ 0 \leq i \leq p - 1;$$
$$e_c(G,G,\langle a, c \rangle), \ C \in \mathcal{R}(G/\langle a, c \rangle);$$
$$e_c(G,\langle a, c \rangle, \langle a \rangle), \ C \in \mathcal{R}(\langle a, c \rangle/\langle a \rangle).$$

**Primitive central idempotents of $\mathbb{F}_q[G]$ for $m \geq 2$:**

$$e_c(G,K_1,\langle a \rangle), \ C \in \mathcal{R}(K_1/\langle a \rangle);$$
$$e_c(G,G,K_1), \ C \in \mathcal{R}(G/K_1);$$
$$e_c(G,G,K_2^{(i)}), \ C \in \mathcal{R}(G/K_2^{(i)}) \ 0 \leq i \leq p - 1;$$
$$e_c(G,G,K_3^{(i)}), \ C \in \mathcal{R}(G/K_3^{(i)}) \ 0 \leq i \leq p - 1;$$
$$e_c(G,G,K_4^{(i,j)}), \ C \in \mathcal{R}(G/K_4^{(i,j)}) \ 0 \leq i \leq m - 2, 1 \leq j \leq p - 1;$$
$$e_c(G,G,K_5^{(i,j)}), \ C \in \mathcal{R}(G/K_5^{(i,j)}) \ 0 \leq i \leq m - 2, 1 \leq j \leq p - 1;$$
$$e_c(G,G,K_6^{(i,j,k)}), \ C \in \mathcal{R}(G/K_6^{(i,j,k)}) \ 0 \leq i \leq m - 2, 1 \leq j, k \leq p - 1.$$

To prove this Theorem, we first need to find the normal subgroups of $G$.

**Lemma 1.** Let $G$ be a group as defined in (1) and $\mathcal{N}$ be the set of distinct normal subgroups of $G$. Then

(i) For $m = 1$, $\mathcal{N} = \{\langle 1 \rangle, \langle c \rangle, \langle c, a \rangle, \langle c, a, b \rangle, \langle c, a' b \rangle \} \ 0 \leq i \leq p - 1\}$ and $\mathcal{S} = \{\langle 1 \rangle, \langle a, c \rangle, \langle c, a, b \rangle, \langle c, a' b \rangle, \langle c^p a, c^p b \rangle, \langle c^p a', c^p b' \rangle, \langle c^p a^j, c^p b^k \rangle \}$

(ii) For $m \geq 2$, $\mathcal{N} = \{\langle c^p a \rangle, \langle c^p a', c^p b \rangle, \langle c^p a', c^p b' \rangle \}$

and $\mathcal{S} = \{\langle \rangle, \langle c, a \rangle, \langle c, a', b \rangle \}$ \ $0 \leq i \leq m - 1 \}$ $\cup$ \ $\langle c^p a \rangle, \langle c^p a', c^p b \rangle, \langle c^p a', c^p b' \rangle, \langle c^p a^j, c^p b^k \rangle \}$ 1 $\leq j \leq p - 1 \}$ $\cup$ \ $\langle c^p a \rangle, \langle c^p a', c^p b \rangle, \langle c^p a', c^p b' \rangle, \langle c^p a^j, c^p b^k \rangle \}$ 1 $\leq j \leq p - 1 \}$ $\cup$ \ $\langle \rangle, \langle c, a \rangle, \langle c, a', b \rangle \}$ 1 $\leq j \leq p - 1 \}$. 


Proof. It can be seen easily that in (i) and (ii), the subgroups listed are distinct and normal in $G$. Also if $N \triangleleft G$, then it can be shown easily, as in [[3], Lemma 4], that $N$ is one of the subgroups listed in the statement of Lemma.

Observe that in both (i) and (ii), for $N = \langle i \rangle$, $A_i / N = \langle c, a \rangle$. Hence $S_{G/N} = \{(a) : \langle c, a \rangle)\}$. Moreover for non-identity normal subgroup $N$ of $G$, the derived group of $G$, $G' = \langle c^{p-1} \rangle$ is contained in $N$, thus $G/N$ is abelian and hence $A_i / N = G/N$. Thus for all non-identity normal subgroups $N$ of $G$,

$$S_{G/N} = \begin{cases} \{(a) : \langle c, a \rangle)\}, & \text{if } G/N \text{ is cyclic}, \\ \phi, & \text{otherwise}. \end{cases}$$

Thus to complete the proof, we need to find only those $N \in \mathcal{N}$ for which $G/N$, is cyclic. In (i), the subgroups $\langle c, a \rangle, \langle c, a, b \rangle, \langle c, a' b \rangle$, $0 \leq i \leq p - 1$ have cyclic quotient with $G$, whereas in (ii), the following normal subgroups have cyclic quotient with $G$:

$$K_1, K_2^{(i)}, K_3^{(i)}, 0 \leq i \leq p - 1,$$

$$K_4^{(i, j)}, K_5^{(i, j)}, K_6^{(i, j, k)}, 0 \leq i \leq m - 2, 1 \leq j, k \leq p - 1.$$

Thus the proof of the lemma is complete.

Proof of Theorem 2. The list of primitive central idempotents of group algebra $\mathbb{F}_q[G]$ can now be easily obtained with the help of Theorem 1 and Lemma 1.

Theorem 3. The Wedderburn decomposition and the automorphism group of semisimple group algebra $\mathbb{F}_q[G]$, $G$ of type $\mathfrak{G}_1$, are given as follows:

**Wedderburn decomposition**

$$\mathbb{F}_q[G] \cong \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q^{(p+1)e} \oplus M_p(\mathbb{F}_q)^{(e)}, & m = 1, \\ \mathbb{F}_q \oplus \mathbb{F}_q^{(m+1)e} \oplus \mathbb{F}_q^{(p^{m-1}e)} \oplus M_p(\mathbb{F}_q)^{(e)}, & 2 \leq m \leq d, \\ \mathbb{F}_q \oplus \mathbb{F}_q^{(d+1-e)} \oplus \sum_{i=d+1}^{m-1} \mathbb{F}_q^{(p^{d+1-e})} \oplus M_p(\mathbb{F}_q^{(p^{d-1}e)}), & m \geq d + 1. \end{cases}$$

**Automorphism group**

$$\text{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} \left( \mathbb{Z}_f^{(p+1)e} \ltimes S_{(p+1)e} \right) \oplus \left( (SL_p(\mathbb{F}_q) \ltimes \mathbb{Z}_f)^{(e)} \ltimes S_e \right), m = 1, \\ \left( \mathbb{Z}_f^{(p^{m+1}e)} \ltimes S_{(p^{m+1}e)} \right) \oplus \left( (SL_p(\mathbb{F}_q) \ltimes \mathbb{Z}_f)^{(p^{m-1}e)} \ltimes S_{p^{m-1}e} \right), 2 \leq m \leq d, \\ \left( \mathbb{Z}_f^{(p^{d+2}e)} \ltimes S_{p^{d+2}+d} \right) \oplus \sum_{i=d+1}^{m} \left( (SL_p(\mathbb{F}_q) \ltimes \mathbb{Z}_f)^{(p^{d+1}e)} \ltimes S_{p^{d+1}e} \right), m \geq d + 1. \end{cases}$$

where $\mathbb{Z}_m$ denotes the cyclic group of order $m$, $S_n$ denotes the symmetric group of degree $n$ and for a group $H$, $H^{(n)}$ a direct sum of $n$ copies of $H$. 


**Proof of Theorem 3.** In order to find the Wedderburn decomposition of \( \mathbb{F}_q[G] \), we need to find the simple component corresponding to each primitive central idempotent. More precisely, for each \( (N, D/N, A_N/N) \in S, C \in \mathfrak{R}(A_N/D) \), we need to calculate \( o(A_N, D) \) and \( |\mathfrak{R}(A_N/D)| \), as given by the following tables:

**Case I :** \( m = 1 \)

| \( (N, D|N, A_N/N) \) | \( E_G(A_N/D) \) | \( o(A_N, D) \) | \( |\mathfrak{R}(A_N/D)| \) |
|-----------------|-------------|-------------|-----------------|
| \( \langle 1 \rangle, \langle a \rangle, \langle (a, c) \rangle \) | \( \langle a, c \rangle \) | \( f \) | \( e \) |
| \( \langle (c, a), \langle 1 \rangle, G/\langle c, a \rangle \rangle \) | \( G \) | \( f \) | \( e \) |
| \( \langle (1), G, \langle 1 \rangle \rangle \) | \( G \) | \( 1 \) | \( 1 \) |
| \( \langle (c, a'b), \langle 1 \rangle, G/\langle c, a'b \rangle \rangle \rangle \) | \( 0 \leq i \leq p - 1 \) | \( G \) | \( f \) | \( e \) |

**Case II :** \( m \geq 2 \)

| \( (N, D|N, A_N/N) \) | \( E_G(A_N/D) \) | \( o(A_N, D) \) | \( |\mathfrak{R}(A_N/D)| \) |
|-----------------|-------------|-------------|-----------------|
| \( (K_0, \langle a \rangle, K_1) \) | \( K_1 \) | \( \begin{cases} f, & m \leq d, \\ fp^{d-i}, & m \geq d + 1. \end{cases} \) | \( \begin{cases} p^{m-i}e, & m \leq d, \\ p^{d-i}e, & m \geq d + 1. \end{cases} \) |
| \( (K_1, K_0, G/K_1) \) | \( G \) | \( f \) | \( e \) |
| \( (K_2(i), K_0, G/K_2(i)) \) | \( G \) | \( f \) | \( e \) |
| \( (K_3(i), K_0, G/K_3(i)) \) | \( G \) | \( \begin{cases} 1, & i = 0 \\ f, & 1 \leq i \leq d \\ fp^{d-i}, & i \geq d + 1 \end{cases} \) | \( \begin{cases} 1, & i = 0, \\ p^{i-1}e, & 1 \leq i \leq d, \\ p^{d-i}e, & i \geq d + 1. \end{cases} \) |
| \( (K_4(i,j), K_0, G/K_4(i,j)) \) | \( G \) | \( \begin{cases} f, & i \leq d - 1, \\ fp^{d-i+1}, & i \geq d. \end{cases} \) | \( \begin{cases} p^ie, & i \leq d - 1, \\ p^{d-i}e, & i \geq d. \end{cases} \) |
| \( (K_5(i,j), K_0, G/K_5(i,j)) \) | \( G \) | \( \begin{cases} f, & i \leq d - 1, \\ fp^{d-i+1}, & i \geq d. \end{cases} \) | \( \begin{cases} p^ie, & i \leq d - 1, \\ p^{d-i}e, & i \geq d. \end{cases} \) |
| \( (K_6(i,j,k), K_0, G/K_6(i,j,k)) \) | \( G \) | \( \begin{cases} f, & i \leq d - 1, \\ fp^{d-i+1}, & i \geq d. \end{cases} \) | \( \begin{cases} p^ie, & i \leq d - 1, \\ p^{d-i}e, & i \geq d. \end{cases} \) |

Now, the required Wedderburn decomposition and automorphism group can be easily read from these two tables and [3, Theorem 3].
4.2. Structure of $\mathbb{F}_q[\mathfrak{G}_2]$ 

Observe that if group $G$ is of type $\mathfrak{G}_2$, then it has the following presentation:

$$G = \langle a, b \mid a^{p^{m+1}} = 1, b^p = a^p, b^{-1}a^{-1}ba = a^{p^{m+1}}, a^p \text{ central in } G \rangle,$$

where $p$ is a prime and $m \geq 1$. For $p = 2$, the complete algebraic structure of $\mathbb{F}_q[G]$ can be read from [3]. Suppose $p$ is an odd prime. For $m \geq 1$, set:

$$L_0 := \langle 1 \rangle, L_1 := \langle a \rangle, L_2^{(i)} := \langle a^{p^i} \rangle, 1 \leq i \leq m, L_3 := \langle a, b \rangle,$$

$$L_4 := \langle a^p, a^2b \rangle, 0 \leq i \leq p - 1,$$

$$L_5^{(i,j)} := \langle a^{p^i}, a^{p^{i-1}}b \rangle, 2 \leq i \leq m, 1 \leq j \leq p.$$

The following Theorems give a complete algebraic structure of semisimple group algebra $\mathbb{F}_q[G]$:

**Theorem 4.** A complete set of primitive central idempotents of semisimple group algebra $\mathbb{F}_q[G]$, $G$ of type $\mathfrak{G}_2$, is given as follows:

**Primitive central idempotents of $\mathbb{F}_q[G]$**

$$e_C(G, G, G), C \in \mathbb{R}(G/G);$$

$$e_C(G, G, L_1), C \in \mathbb{R}(G/L_1);$$

$$e_C(G, G, L_2), C \in \mathbb{R}(G/L_2);$$

$$e_C(G, L_1, L_0), C \in \mathbb{R}(L_1/L_0);$$

$$e_C(G, L_4^{(i)}), C \in \mathbb{R}(G/L_4^{(i)}), 0 \leq i \leq p - 1;$$

$$e_C(G, L_5^{(i,j)}), C \in \mathbb{R}(G/L_5^{(i,j)}), 2 \leq i \leq m, 1 \leq j \leq p.$$

**Proof of Theorem 4.** In view of Theorem 1, to find a complete list of primitive central idempotents of $\mathbb{F}_q[G]$ we first need to list all normal subgroups of $G$. It can be seen easily that the set $\mathcal{N}$ of distinct normal subgroups of $G$ is equal to

$$\{L_0, L_1, L_2^{(i)}, 1 \leq i \leq m, L_3, L_4^{(i)}, 0 \leq i \leq p - 1, L_5^{(i,j)}, 2 \leq i \leq m, 1 \leq j \leq p\}.$$

For $N = L_0$, $A_N/N = L_1$. Hence $S_{G/N} = \{\langle L_0, L_1 \rangle\}$. Moreover, for non-identity $N \in \mathcal{N}, S_{G/N}$ is non-empty if and only if $G/N$ is cyclic. The following $N \in \mathcal{N}$ have cyclic quotient with $G$:

$$L_1, L_3, L_4^{(i)}, 0 \leq i \leq p - 1, L_5^{(i,j)}, 2 \leq i \leq m, 1 \leq j \leq p.$$

Thus (i) follows from Theorem 1.

**Theorem 5.** The Wedderburn decomposition and the automorphism group of semisimple group algebra $\mathbb{F}_q[G]$, $G$ of type $\mathfrak{G}_2$, are as follows:

**Wedderburn decomposition**

$$\mathbb{F}_q[G] \cong \begin{cases} 
\mathbb{F}_q \bigoplus \mathbb{F}_q \left( \frac{p^{m+1}}{f} \right) \bigoplus \mathbb{M}_p \left( \mathbb{F}_q \right)^{(p^{m+1}-1)e}, & m \leq d - 1, \\
\mathbb{F}_q \bigoplus \sum_{i=d+1}^{m} \mathbb{F}_{q^{p^d}(p^d)} \left( \frac{p^{d+1}-1}{f} \right) \bigoplus \mathbb{M}_p \left( \mathbb{F}_{q^{p^m-p^d}} \right)^{(p^{d+1}-1)e}, & m \geq d. \end{cases}$$
Automorphism group

\[ Aut(F_q[G]) \cong \left\{ \begin{array}{l}
(\mathbb{Z}_f \left( \frac{p^{m+1}-1}{f} \right) \rtimes S_f(\frac{p^{m+1}-1}{f})) \oplus \\
(SL_p(F_q) \ltimes \mathbb{Z}_f)(p^{m-1}e) \rtimes S_{p^{m-1}e}, \ m \leq d - 1 \\
(\mathbb{Z}_f \left( \frac{p^{d+1}-1}{f} \right) \rtimes S_f(\frac{p^{d+1}-1}{f})) \oplus \sum_{i=d+1}^{m}(\mathbb{Z}_f p^{i-d}(p^d e) \rtimes S_{p^d e}) \oplus \\
(SL_p(F_q f^{p^m-d}) \ltimes \mathbb{Z}_f f^{p^m-d})(p^{d-1}e) \rtimes S_{p^d-1}e, \ m \geq d.
\end{array} \right. \]

Proof of Theorem 5. We will first find \( E_G(L_1/L_0) \). Observe that \( |L_1/L_0| = p^{m+1} \) and \( L_1 \subseteq E_G(L_1/L_0) \subseteq G \). Let \( m \leq d - 1 \). In this case, \( b \in E_G(L_1/L_0) \), if and only if \( \zeta^{p^m+1} = \zeta^d \) for some \( i, 1 \leq i \leq f \), where \( \zeta \) is a primitive \( p^{m+1} \) th root of unity. This implies that \( p^m + 1 = q^i \) (mod \( p^{m+1} \)), i.e., \( p = \frac{f}{\gcd(i, f)} \), which gives that \( p \) divides \( p - 1 \), a contradiction. Hence in this case \( E_G(L_1/L_0) = L_1 \). For \( m \geq d \), \( E_G(L_1/L_0) = G \). Thus we have the following:

| \( (N, D/N, A_N/N) \) | \( E_G(A_N/D) \) | \( \alpha(A_N/D) \) | \( |\mathcal{R}(A_N/D)| \) |
|-----------------------------|----------------|----------------|----------------|
| \((G, L_0, L_0)\)          | \(G\)           | 1              | 1              |
| \((L_1, L_0, G/L_1)\)      | \(G\)           | \(f\)          | \(e\)          |
| \((L_4^{(i)}, L_0, G/L_4^{(i)})\), 0 \leq i \leq p - 1 | \(G\)           | \(f\)          | \(e\)          |
| \((L_5^{(i,j)}, L_0, G/L_5^{(i,j)})\), 2 \leq i \leq m, 1 \leq j \leq p | \(G\)           | \(\begin{array}{l}
(f, \ i \leq d, \\
p^i f^{d-j}, \ i \geq d + 1.
\end{array}\) | \(\begin{array}{l}
p^{i-1}e, \ i \leq d, \\
p^{d-j}e, \ i \geq d + 1.
\end{array}\) |
| \((L_0, L_0, L_1)\)        | \(\begin{array}{l}
L_1, \ m \leq d - 1, \\
G, \ m \geq d.
\end{array}\) | \(\begin{array}{l}
f, \ m \leq d - 1, \\
p^{m-d}e, \ m \geq d.
\end{array}\) | \(\begin{array}{l}
p^{m-1}e, \ m \leq d - 1, \\
p^{d-1}e, \ m \geq d.
\end{array}\) |

The Wedderburn decomposition and automorphism group of \( F_q[G] \) can now be easily read with the help of this table and [3, Theorem 3].

Acknowledgment

The author is grateful to the referees for their valuable suggestions which have helped to write the paper in the present form.
References


