THE STRUCTURE OF SEMISIMPLE FINITE METABELIAN GROUP ALGEBRAS

SHALINI GUPTA

A Thesis submitted for the partial fulfilment
of the degree of
Doctor of Philosophy

Indian Institute of Science Education and Research Mohali
Department of Mathematics
Mohali-140306
February 2013

Dedicated to

Ashok Kumar Goyal,

Shruti and Aayush

Declaration

The work presented in this thesis has been carried out by me under the supervision of Professor Inder Bir S. Passi and Dr. Gurmeet K. Bakshi at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Date:
Place: Shalini Gupta

In our capacity as supervisors of the candidate's thesis work, we certify that the above statements by the candidate are true to the best of our knowledge.

Inder Bir S. Passi
(Supervisor)

Gurmeet K. Bakshi
(Supervisor)

Acknowledgement

I owe my deepest gratitude to my supervisors, Professor Inder Bir Singh Passi and Dr. Gurmeet Kaur Bakshi, for their guidance and encouragement.

I am thankful to the Director IISER Mohali, Professor N.Satyamurthy, Head of the Department of Mathematics, Professor Kapil Hari Paranjape, and the Mathematics faculty of Indian Institute of Science Education and Research for making available to me the excellent facilities of the Institute.

It is my pleasure to thank the faculty of the Centre for Advanced study in Mathematics, Panjab University, Chandigarh, in particular, Professor A.K.Bhandari and Professor S.K.Tomar, for graciously allowing me to use the library facilities of the department,

I am very grateful to the authorities of Punjabi University, Patiala, for granting me study leave for a period of three years.

Date:
Place: Shalini Gupta

Contents

Notation

G	a finite group
G'	the derived subgroup of G
$G^{(n)}$	the direct sum of n copies of G
$G_1 \rtimes G_2$	semidirect product of G_1 by G_2
$H \leq G$	H is a subgroup of G
$H \trianglelefteq G$	H is a normal subgroup of G
$[G : H]$	the index of the subgroup H in the group G
$N_G(H)$	the normalizer of the subgroup H in the group G
$\mathrm{core}(H)$	the largest normal subgroup of the group G contained in H, $H \leq G$
$R[G]$	the group ring of the group G with coefficients in the ring R
$\lvert S \rvert$	the cardinality of the set S
φ	Euler's phi-function
$\mathrm{ord}_n(q)$	the order of q modulo n
$\mathbb{Z}$	the ring of integers
$\mathbb{Z}_n$	the cyclic group of order n
$\mathbb{Z}_n^*$	the group of reduced residue classes modulo n
S_n	the symmetric group of degree n
$\mathbb{F}_q$	the finite field of order q
$\overline{\mathbb{F}}_q$	the algebraic closure of $\mathbb{F}_q$
$\mathrm{Irr}(G)$	the set of inequivalent irreducible characters of G over $\overline{\mathbb{F}}_q$
$\mathrm{Gal}(K/F)$	the Galois group of the field extension K/F
$M_n(F)$	the ring of all $n \times n$ matrices over the field F
$\mathrm{SL}_n(F)$	the group of matrices in $M_n(F)$ having determinant 1
$\ker(\chi)$	the kernel of χ, $\chi \in \mathrm{Irr}(G)$
$e(\chi)$	the primitive central idempotent of $\overline{\mathbb{F}}_q[G]$ determined by $\chi \in \mathrm{Irr}(G)$
$\mathbb{F}_q(\chi)$	the field obtained by adjoining the character values $\chi(g)$, $g \in G$, to the field $\mathbb{F}_q$
$e_{\mathbb{F}_q}(\chi)$	the primitive central idempotent of $\mathbb{F}_q[G]$ determined by $\chi \in \mathrm{Irr}(G)$
$\mathcal{G}(\chi)$	Galois group $\mathrm{Gal}(\mathbb{F}_q(\chi)/\mathbb{F}_q), \chi \in \mathrm{Irr}(G)$
$\square$	end (or omission) of proof

Introduction

Given a group G and a field F, one can define an F-algebra $F[G]$, called the group algebra of G over F, whose elements are the formal finite F-linear combinations of elements of G with addition defined coefficient-wise and multiplication defined via multiplication in G and distributivity. Group algebras constitute an important class of algebras with wide applications. A fundamental problem in the theory of group algebras is to understand their algebraic structure.

The classical approach to compute the primitive central idempotents of $F[G]$, in the semisimple case, i.e., when the characteristic of F does not divide the order of G, has been via character theory. If $\chi \in \mathrm{Irr}(G)$, the set of irreducible characters of G over $\overline{F}$, the algebraic closure of F, then

$$e(\chi) := \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g) g^{-1}$$

is a primitive central idempotent of $\overline{F}[G]$ and $\chi \mapsto e(\chi)$ is a 1-1 correspondence between $\mathrm{Irr}(G)$ and the set of all primitive central idempotents of $\overline{F}[G]$. The Galois group $\mathrm{Gal}(\overline{F}/F)$ acts on $\mathrm{Irr}(G)$ by setting

$$^{\sigma}\chi = \sigma \circ \chi, \quad \sigma \in \mathrm{Gal}(\overline{F}/F),\ \chi \in \mathrm{Irr}(G).$$

Let $\mathrm{orb}(\chi)$ denote the orbit of $\chi \in \mathrm{Irr}(G)$ under this action. Observe that $\mathrm{orb}(\chi)$ is equal to $\{^{\sigma}\chi \,|\, \sigma \in \mathrm{Gal}(F(\chi)/F)\}$, where $F(\chi)$ is the field obtained by adjoining to F, all the character values $\chi(g), g \in G$. It is known that, for any $\chi \in \mathrm{Irr}(G)$,

$$e_F(\chi) := \sum_{\psi \in \mathrm{orb}(\chi)} e(\psi) = \sum_{\sigma \in \mathrm{Gal}(F(\chi)/F)} e(^{\sigma}\chi)$$

is a primitive central idempotent of $F[G]$, called the primitive central idempotent associated with χ, and the map $\mathrm{orb}(\chi) \mapsto e_F(\chi)$ is a 1-1 correspondence between the set $\{\mathrm{orb}(\chi) \,|\, \chi \in \mathrm{Irr}(G)\}$ of orbits and the primitive central idempotents of $F[G]$.

In recent years the effort has been to carry out the computation of primitive central idempotents of $F[G]$ in terms of the subgroup structure of G [JLP03, OdRS06,

OdRS04, BdR07, GG11]. It is the latter approach that is pursued in this thesis, which is aimed as a contribution to understand the algebraic structure of semisimple finite group algebras of metabelian groups. It may be mentioned that the analogous study of rational group algebras has been carried out in [Her97, OdRS06, BKP13].

We begin our study of non-commutative semisimple finite group algebras $F[G]$ with the computation, in Chapter 1, of the primitive central idempotents when the group G is of order p_1p_2, where p_1 and p_2 are distinct primes [BGP11]. We next consider the case when G is an arbitrary metacyclic group [BGP] and conclude with the case when the group is an arbitrary metabelian group. Although, the case of metabelian groups contains the first two cases, the conclusion in the former cases, however, are more descriptive from the point of view of application.

In Chapter 2, we apply the preceeding computations of the primitive central idempotents to derive explicit Wedderburn decomposition and the group of automorphisms of the group algebras considered in Chapter 1.

Finally, in Chapter 3, we give several illustrative examples. In particular, we consider the group algebras of certain indecomposable groups G whose central quotient is the Klein four-group; thus providing a method for improving results in [FGPM10].

Chapter 1

Primitive Central Idempotents

The main result in this Chapter is the determination of a complete irredundant set of primitive central idempotents of the semisimple group algebra $\mathbb{F}_q[G]$, where G is an arbitrary finite metabelian group.

Commutative group algebras

We begin by recalling the primitive central idempotents of finite commutative semisimple group algebras. The explicit expressions for primitive central idempotents of the semisimple group algebra $\mathbb{F}_q[\mathbb{Z}_n]$, $n \geq 1$, have been computed in [SBDR04, SBDR08, BRS08]. We need the case when n is a prime and the description of primitive central idempotents, in this case, is as follows:

Proposition 1.1 *Let $\langle a \rangle$ be a cyclic group of prime order p and q a prime power, $p \nmid q$. Let $f = ord_p(q)$, $e = (p-1)/f$ and g a primitive root modulo p. The group algebra $\mathbb{F}_q[\langle a \rangle]$ has exactly the following $e+1$ distinct primitive (central) idempotents:*

$$\tfrac{1}{p}(1 + a + \cdots a^{p-1}),$$

$$\tfrac{1}{p}(f + \textstyle\sum_{j=0}^{p-2} \eta_{i+j} a^{g^j}), \quad 0 \leq i \leq e-1.$$

where $\eta_k = \sum_{j=0}^{f-1} \zeta^{g^k q^j}$, $k \geq 0$, and ζ is a primitive p-th root of unity in $\overline{\mathbb{F}}_q$; in particular, if $0 \leq m$, $m' \leq e-1$, $m \neq m'$, the tuples $(\eta_m, \eta_{m+1}, \ldots, \eta_{m+e+1})$ and $(\eta_{m'}, \eta_{m'+1}, \ldots, \eta_{m'+e+1})$ are distinct.

Let H and K be subgroups of G (not necessarily abelian) such that H is normal in K and K/H is cyclic. Then $\mathrm{Irr}(K/H)$ is a (multiplicative) cyclic group isomorphic to K/H of order coprime to q. The cyclic group $\langle q \rangle$ contained in $\mathbb{Z}^*_{[K:H]}$ acts on $\mathrm{Irr}(K/H)$ by setting $q.\chi = \chi^q$, $\chi \in \mathrm{Irr}(K/H)$. Recall that the orbits of this action

are called the *q-cyclotomic cosets* in $\mathrm{Irr}(K/H)$. It may be pointed out that if χ is generator of $\mathrm{Irr}(K/H)$, then so is every element in the orbit of χ. Define

$$\mathcal{C}(K/H) = \{C \,|\, C \text{ is an orbit of a generator } \chi \in \mathrm{Irr}(K/H)\}.$$

For $C \in \mathcal{C}(K/H)$, $\chi \in C$, following [BdR07], we set

$$\varepsilon_C(K,H) = |K|^{-1} \sum_{g \in K} (\mathrm{Tr}_{\mathbb{F}_q(\xi)/\mathbb{F}_q}(\chi(\overline{g})))g^{-1}, \tag{1.1}$$

where ξ is a primitive $|K/H|^{th}$ root of unity in $\overline{\mathbb{F}}_q$, $\mathrm{Tr}_{\mathbb{F}_q(\xi)/\mathbb{F}_q}$ is the trace of the extension $\mathbb{F}_q(\xi)/\mathbb{F}_q$, and for $g \in K$, $\overline{g} = gH$.

Observe that the group G acts on $\mathbb{F}_q[G]$ by conjugation. Let

$$e_C(G,\, K,\, H) = \quad \text{the sum of distinct } G\text{-conjugates of } \varepsilon_C(K,H). \tag{1.2}$$

The following result is due to Broche and Rio [BdR07].

Theorem 1.2 *Let $\mathbb{F}_q$ be a finite field and G a finite group of order coprime to q. Let $N \trianglelefteq G$ with G/N cyclic and let $C \in \mathcal{C}(G/N)$. Then*

(i) $\varepsilon_C(G,\, N)$ *is a primitive central idempotent of* $\mathbb{F}_q[G]$.

(ii) $\mathbb{F}_q[G]\varepsilon_C(G,\, N) \cong \mathbb{F}_q(\zeta_k)$, *where* ζ_k *is a primitive* k*-th root of unity in* $\overline{\mathbb{F}}_q$ *and* $k = [G : N]$.

(iii) $\varepsilon_C(G,\, N) = \varepsilon_D(G,\, N)$, $C,\, D \in \mathcal{C}(G/N)$, *if and only if* $C = D$.

Furthermore, in case G is abelian,

$$\{\varepsilon_C(G,\, N) \,|\, N \leq G,\, G/N \quad \textit{is cyclic and } C \in \mathcal{C}(G/N)\}$$

is a complete set of primitive central idempotents of $\mathbb{F}_q[G]$.

Irreducible characters of metacyclic groups

Let n, t, r, k be natural numbers with $r^t \equiv 1 \pmod{n}$, $kr \equiv k \pmod{n}$ and let G be the metacyclic group given by the presentation

$$G = \langle a, b \,|\, a^n = 1,\, b^t = a^k,\, b^{-1}ab = a^r \rangle. \tag{1.3}$$

Let $[n] = \{0, 1, \ldots, n-1\}$ and σ the permutation of $[n]$ defined by

$$i \mapsto ir \pmod{n}.$$

The cyclic group $\langle\sigma\rangle$ acts naturally on $[n]$. Let $[[n]]$ denote a complete set of representatives of the distinct orbits of $[n]$. For $i \in [n]$, let $\mathrm{orb}(i)$ denote the orbit of i and $l_i = |\,\mathrm{orb}(i)|$. Note that l_i is the order of r modulo $n/\gcd(i,\, n)$, and hence l_i divides t (as $r^t \equiv 1 \pmod n$). Let $s_i = t/l_i$ and ζ a primitive nt-th root of unity in $\overline{\mathbb{F}}_q$.

Let $i \in [n]$ and suppose $\gcd(i, n) = d$. For $0 \le j \le s_d - 1$, there exists a representation $T_{i,\,j} : G \longrightarrow GL(l_d,\, \overline{\mathbb{F}}_q)$ defined by

$$T_{i,\,j}(a) = \mathrm{diag}(\zeta^{-it},\, \zeta^{-itr}, \ldots, \zeta^{-itr^{l_d-1}}), \quad T_{i,\,j}(b) = \begin{bmatrix} 0 & 0 & \ldots & & 0 & \zeta^{-l_d(ik+nj)} \\ 1 & 0 & 0 & \ldots & & 0 \\ 0 & & \ddots & & & 0 \\ \vdots & & & & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 & 0 \end{bmatrix}.$$

Let $\chi_{i,\,j}$ denote the character of $T_{i,\,j}$. For a divisor d of n and a divisor l of $\frac{n}{d}s_d$, $d,\ l \ge 1$, let

$$X_{d,l} := \{(i,\, j) \,|\, i \in [[n]],\, \gcd(i, n) = d,\, 0 \le j \le s_d - 1,\, \gcd(\frac{i}{d}k + \frac{n}{d}j,\, \frac{n}{d}s_d) = l\}. \tag{1.4}$$

Theorem 1.3 [Bas79] *The set*

$$\{\chi_{i,\,j},\ (i,\, j) \in \bigcup_{d|n} \bigcup_{l|\frac{n}{d}s_d} X_{d,l}\}$$

is a complete set of irreducible characters of G over $\overline{\mathbb{F}}_q$.

We now proceed to compute the primitive central idempotents of $\mathbb{F}_q[G]$, where G is a metacyclic group of order nt with presentation given by (1.3). Our objective is to obtain explicit expressions for the idempotents entirely in terms of the numbers n, t, k, r and q. We will first consider the special case when n and t are primes.

Groups of order p_1p_2

Let G be a group of order p_1p_2, where p_1, p_2 are primes. If G is abelian, the primitive central idempotents of $\mathbb{F}_q[G]$ can be computed from Theorem 1.2. For explicit expressions of the idempotents, see [SBDR04, SBDR08, BRS08].

We thus assume throughout the rest of this Section that G is a non-abelian group of order p_1p_2 with $p_1 > p_2$, say. In this case, we must have $p_1 \equiv 1 \pmod{p_2}$. Let

$$G = \langle a, b \,|\, a^{p_1} = b^{p_2} = 1,\, b^{-1}ab = a^r \rangle, \tag{1.5}$$

where the multiplicative order of r modulo p_1 is p_2. Let $f_1 := \mathrm{ord}_{p_1}(q)$ and $f_2 := \mathrm{ord}_{p_2}(q)$ be the multiplicative orders of q modulo p_1 and p_2 respectively. Observe that $f_1 \,|\, p_1 - 1$ and $f_2 \,|\, p_2 - 1$. Let

$$e_1 := \frac{p_1 - 1}{f_1} \quad e_2 := \frac{p_2 - 1}{f_2}. \tag{1.6}$$

Let g_i be a primitive root modulo p_i and ζ_i, a primitive p_i-th root of unity in $\overline{\mathbb{F}}_q$, $i = 1, 2$. For $k \geq 0$, define

$$\eta_k^{(1)} := \sum_{j=0}^{f_1-1} \zeta_1^{g_1^k q^j}, \quad \eta_k^{(2)} := \sum_{j=0}^{f_2-1} \zeta_2^{g_2^k q^j}. \tag{1.7}$$

Observe that

$$\eta_{k+e_1}^{(1)} = \eta_k^{(1)}, \quad \eta_{k+e_2}^{(2)} = \eta_k^{(2)}.$$

Set

$$K := \mathbb{F}_q \left(\sum_{u=0}^{p_2-1} \zeta_1^{ir^u} \,|\, i = 1, 2, \ldots, p_1 - 1 \right). \tag{1.8}$$

For a group G of order $p_1 p_2$, Theorem 1.3 yields the following:

Proposition 1.4 *If G is a group given by the presentation (1.5), then it has exactly $p_2 + \frac{p_1-1}{p_2}$ irreducible characters over $\overline{\mathbb{F}}_q$, of which p_2 characters are of degree 1 and $\frac{p_1-1}{p_2}$ are of degree p_2.*

The non-trivial irreducible characters, ψ_m, $0 \leq m \leq p_2 - 2$, of degree 1 are given by

$$\psi_m(a^x b^y) = \zeta_2^{-g_2^m y}, \quad a^x b^y \in G, \quad 0 \leq m \leq p_2 - 2,$$

and the irreducible characters ϕ_n, $0 \leq n \leq \frac{p_1-1}{p_2} - 1$, of degree p_2 over $\overline{\mathbb{F}}_q$ are given by

$$\phi_n(a^x b^y) = \begin{cases} 0, & y \neq 0, \\ \sum_{j=0}^{p_2-1} \zeta_1^{-x g_1^{\frac{p_1-1}{p_2} j + n}}, & y = 0. \end{cases}$$

We now describe the primitive central idempotents of $\mathbb{F}_q[G]$ associated with the irreducible characters of degree 1. Let $\iota : G \to \overline{\mathbb{F}}_q$ be the trivial character of G.

Clearly

$$e_{\mathbb{F}_q}(\iota) = \frac{1}{p_1 p_2} \sum_{g \in G} g. \tag{1.9}$$

Lemma 1.5 *For* $0 \leq m \leq p_2 - 2$,

$$e_{\mathbb{F}_q}(\psi_m) = \frac{1}{p_1 p_2} \left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2} \eta^{(2)}_{m+j} \left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j} \right) \right),$$

and $e_{\mathbb{F}_q}(\psi_m) = e_{\mathbb{F}_q}(\psi_{m'})$ *if, and only if,* $m \equiv m' \pmod{e_2}$.

Proof. Let $0 \leq m \leq p_2 - 2$.

$$\begin{aligned}
e_{\mathbb{F}_q}(\psi_m) &= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\psi_m)/\mathbb{F}_q)} e({}^{\sigma}\psi_m) \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_2)/\mathbb{F}_q)} e({}^{\sigma}\psi_m), \qquad (\mathbb{F}_q(\psi_m) = \mathbb{F}_q(\zeta_2)) \\
&= \tfrac{1}{p_1 p_2} \left(\sum_{x=0}^{p_1-1} \sum_{y=0}^{p_2-1} \left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_2)/\mathbb{F}_q)} \sigma(\zeta_2^{g_2^m y}) \right) a^x b^y \right) \\
&= \tfrac{1}{p_1 p_2} \left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{y=1}^{p_2-1} \left(\sum_{i=0}^{f_2-1} (\zeta_2^{g_2^m y})^{q^i} \right) \left(\sum_{x=0}^{p_1-1} a^x b^y \right) \right) \\
&= \tfrac{1}{p_1 p_2} \left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2} \left(\sum_{i=0}^{f_2-1} (\zeta_2^{g_2^{m+j}})^{q^i} \right) \left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j} \right) \right) \\
&= \tfrac{1}{p_1 p_2} \left(f_2 \sum_{x=0}^{p_1-1} a^x + \sum_{j=0}^{p_2-2} \eta^{(2)}_{m+j} \left(\sum_{x=0}^{p_1-1} a^x b^{g_2^j} \right) \right).
\end{aligned}$$

Since $\eta^{(2)}_i = \eta^{(2)}_{i+e_2}$ for all $i \geq 0$, it follows that

$$e_{\mathbb{F}_q}(\psi_m) = e_{\mathbb{F}_q}(\psi_{m+e_2}).$$

Furthermore, in view of Proposition 1.1, $e_{\mathbb{F}_q}(\psi_m)$, for $0 \leq m \leq e_2 - 1$, are distinct. □

In the next Lemma, we describe the primitive central idempotents $e_{\mathbb{F}_q}(\phi_n)$, $0 \leq n \leq \frac{p_1-1}{p_2} - 1$, associated with non-linear irreducible characters.

Lemma 1.6 *(i) If $p_2 \mid f_1$, then, for $0 \le n \le \frac{p_1-1}{p_2} - 1$,*

$$e_{\mathbb{F}_q}(\phi_n) = \frac{p_2}{p_1[\mathbb{F}_q(\zeta_1) : K]} \left(f_1 + \sum_{k=0}^{p_1-2} \eta_{n+k}^{(1)} a^{g_1^k} \right)$$

and $e_{\mathbb{F}_q}(\phi_n) = e_{\mathbb{F}_q}(\phi_{n'})$ if, and only if, $n \equiv n' \pmod{e_1}$.

(ii) If $p_2 \nmid f_1$, then, for $0 \le n \le \frac{p_1-1}{p_2} - 1$,

$$e_{\mathbb{F}_q}(\phi_n) = \frac{1}{[\mathbb{F}_q(\zeta_1) \,:\, K]\, p_1} \left(f_1 p_2 + \sum_{i=0}^{p_1-2} \left(\sum_{j=0}^{p_2-1} \eta_{n+i+j\frac{e_1}{p_2}}^{(1)} \right) a^{g^i} \right)$$

and $e_{\mathbb{F}_q}(\phi_n) = e_{\mathbb{F}_q}(\phi_{n'})$ if, and only if, $n \equiv n' \pmod{\frac{e_1}{p_2}}$.

Proof. Observe that $\mathbb{F}_q(\phi_n) = K$ for all $n \ge 0$, where K is as defined in equation (1.8). Therefore,

$$\begin{aligned}
[\mathbb{F}_q(\zeta_1) : K] e_{\mathbb{F}_q}(\phi_n) &= [\mathbb{F}_q(\zeta_1) : K] \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{F}_q)} e({}^{\sigma}\phi_n) \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_1)/\mathbb{F}_q)} e({}^{\sigma}\phi_n) \\
&= \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_1)/\mathbb{F}_q)} \left(\tfrac{p_2}{p_1 p_2} \sum_{x=0}^{p_1-1} \sigma(\phi_n(a^{-x})) a^x \right) \\
&= \tfrac{p_2}{p_1 p_2} \sum_{x=0}^{p_1-1} \sum_{j=0}^{p_2-1} \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(\zeta_1)/\mathbb{F}_q)} \sigma \left(\zeta_1^{x g_1^{\frac{p_1-1}{p_2} j+n}} \right) a^x \\
&= \tfrac{1}{p_1} \sum_{x=0}^{p_1-1} \sum_{j=0}^{p_2-1} \sum_{l=0}^{f_1-1} \left(\zeta_1^{x g_1^{\frac{p_1-1}{p_2} j+n}} \right)^{q^l} a^x \\
&= \tfrac{1}{p_1} \left(f_1 p_2 + \sum_{i=0}^{p_1-2} \sum_{j=0}^{p_2-1} \sum_{l=0}^{f_1-1} \left(\zeta_1^{g_1^{\frac{p_1-1}{p_2} j+n+i}} \right)^{q^l} a^{g_1^i} \right). \qquad (1.10)
\end{aligned}$$

Case I : $p_2 \,|\, f_1$**.**

In this case, $g_1^{\frac{p_1-1}{p_2}.j} \in \langle q \rangle \subseteq \mathbb{Z}_{p_1}^*$ for all j, $0 \leq j \leq p_2 - 1$. Therefore, $\sum_{l=0}^{f_1-1} \left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}j+n+i}} \right)^{q^l} = \sum_{l=0}^{f_1-1} \left(\zeta_1^{g_1^{n+i}} \right)^{q^l} = \eta_{n+i}^{(1)}$ for $0 \leq j \leq p_2 - 1$. Substituting in equation (1.10), we get

$$\begin{aligned}
[\mathbb{F}_q(\zeta_1) : K] e_{\mathbb{F}_q}(\phi_n) &= \frac{1}{p_1} \left(f_1 p_2 + \sum_{i=0}^{p_1-2} \sum_{j=0}^{p_2-1} \eta_{n+i}^{(1)} a^{g_1^i} \right) \\
&= \frac{1}{p_1} \left(f_1 p_2 + p_2 \sum_{i=0}^{p_1-2} \eta_{n+i}^{(1)} a^{g_1^i} \right) \\
&= \frac{p_2}{p_1} (f_1 + \sum_{i=0}^{p_1-2} \eta_{n+i}^{(1)} a^{g_1^i}).
\end{aligned}$$

Since the right side of the above equation is non-zero, it follows that $[\mathbb{F}_q(\zeta_1) : K]$ is invertible in $\mathbb{F}_q$ and, consequently,

$$e_{\mathbb{F}_q}(\phi_n) = \frac{p_2}{[\mathbb{F}_q(\zeta_1) : K]\, p_1} \left(f_1 + \sum_{i=0}^{p_1-2} \eta_{n+i}^{(1)} a^{g_1^i} \right).$$

Since $\eta_i^{(1)} = \eta_{i+e_1}^{(1)}$ for all $i \geq 0$, we have

$$e_{\mathbb{F}_q}(\phi_n) = e_{\mathbb{F}_q}(\phi_{n+e_1}).$$

Also, in view of Proposition 1.1, $e_{\mathbb{F}_q}(\phi_n)$, $0 \leq n \leq e_1 - 1$, are all distinct.

Case II : $p_2 \nmid f_1$**.**

For $1 \leq j \leq p_2 - 1$, let j' be the remainder obtained on dividing $f_1 j$ by p_2. We observe that $\left(g_1^{\frac{p_1-1}{p_2}j - \frac{e_1}{p_2}j'} \right)^{f_1} = g_1^{e_1 f_1 \frac{f_1 j - j'}{p_2}} \equiv 1 \pmod{p_1}$. This gives $g_1^{\frac{p_1-1}{p_2}j - \frac{e_1}{p_2}j'} \in \langle q \rangle \subseteq \mathbb{Z}_{p_1}^*$. Hence, $\sum_{l=0}^{f_1-1} \left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}j+n+i}} \right)^{q^l} = \sum_{l=0}^{f_1-1} \left(\zeta_1^{g_1^{\frac{e_1}{p_2}j'+n+i}} \right)^{q^l} = \eta_{n+i+\frac{e_1}{p_2}j'}$. Note that as j runs through 1 to $p_2 - 1$, so does j'. Therefore,

$$\sum_{j=1}^{p_2-1} \sum_{l=0}^{f_1-1} \left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}j+n+i}} \right)^{q^l} = \sum_{j'=1}^{p_2-1} \eta_{n+i+\frac{e_1}{p_2}j'}. \tag{1.11}$$

From equations (1.10) and (1.11), we obtain

$$\begin{aligned}
[\mathbb{F}_q(\zeta_1):K]e_{\mathbb{F}_q}(\phi_n) &= \frac{1}{p_1}\left(f_1p_2+\sum_{i=0}^{p_1-2}\sum_{j=0}^{p_2-1}\sum_{l=0}^{f_1-1}\left(\zeta_1^{g_1^{\frac{p_1-1}{p_2}j+n+i}}\right)^{q^l}a^{g^i}\right)\\
&= \frac{1}{p_1}\left(f_1p_2+\sum_{i=0}^{p_1-2}\left(\sum_{l=0}^{f_1-1}(\zeta_1^{g_1^{n+i}})^{q^l}+\sum_{j=1}^{p_2-1}\sum_{l=0}^{f_1-1}(\zeta_1^{g_1^{\frac{p_1-1}{p_2}j+n+i}})^{q^l}\right)a^{g^i}\right)\\
&= \frac{1}{p_1}\left(f_1p_2+\sum_{i=0}^{p_1-2}\left(\eta_{n+i}^{(1)}+\sum_{j=1}^{p_2-1}\eta_{n+i+\frac{e_1}{p_2}j}^{(1)}\right)a^{g^i}\right)\\
&= \frac{1}{p_1}\left(f_1p_2+\sum_{i=0}^{p_1-2}\left(\sum_{j=0}^{p_2-1}\eta_{n+i+j\frac{e_1}{p_2}}^{(1)}\right)a^{g^i}\right).
\end{aligned} \tag{1.12}$$

We next see that the right side of equation (1.12) is non-zero. Suppose not, then

$$\eta_{n+i}^{(1)}+\eta_{n+i+\frac{e_1}{p_2}}^{(1)}+\eta_{n+i+2.\frac{e_1}{p_2}}^{(1)}+\cdots+\eta_{n+i+(p_2-1)\frac{e_1}{p_2}}^{(1)}=0$$

for $0\le i\le p_1-2$. In particular,

$$\begin{aligned}
\eta_0^{(1)}+\eta_{\frac{e_1}{p_2}}^{(1)}+\eta_{2.\frac{e_1}{p_2}}^{(1)}+\cdots+\eta_{(p_2-1)\frac{e_1}{p_2}}^{(1)} &= 0\\
\eta_1^{(1)}+\eta_{1+\frac{e_1}{p_2}}^{(1)}+\eta_{1+2.\frac{e_1}{p_2}}^{(1)}+\cdots+\eta_{1+(p_2-1)\frac{e_1}{p_2}}^{(1)} &= 0\\
\cdots&\\
\eta_{\frac{e_1}{p_2}-1}^{(1)}+\eta_{\frac{e_1}{p_2}-1+\frac{e_1}{p_2}}^{(1)}+\eta_{\frac{e_1}{p_2}-1+2.\frac{e_1}{p_2}}^{(1)}+\cdots+\eta_{\frac{e_1}{p_2}-1+(p_2-1)\frac{e_1}{p_2}}^{(1)} &= 0.
\end{aligned}$$

On adding the above system of equations, we get $\eta_0^{(1)}+\eta_1^{(1)}+\cdots+\eta_{e_1-1}^{(1)}=0$, which is a contradiction, since $\sum_{i=0}^{e_1-1}\eta_i^{(1)}=-1$. Consequently, $[\mathbb{F}_q(\zeta_1):K]$ is invertible in $\mathbb{F}_q$ and

$$e_{\mathbb{F}_q}(\phi_n)=\frac{1}{[\mathbb{F}_q(\zeta_1):K]\,p_1}\left(f_1p_2+\sum_{i=0}^{p_1-2}\left(\sum_{j=0}^{p_2-1}\eta_{n+i+j\frac{e_1}{p_2}}^{(1)}\right)a^{g^i}\right).$$

It is clear from the above expression that

$$e_{\mathbb{F}_q}(\phi_n)=e_{\mathbb{F}_q}(\phi_{(n+\frac{e_1}{p_2})}).$$

That the idempotents $e_{\mathbb{F}_q}(\phi_n)$, $0 \leq n \leq \frac{e_1}{p_2} - 1$ are all distinct is a consequence of the following:

Lemma 1.7 *For $0 \leq n$, $n' \leq \frac{e_1}{p_2} - 1$, $n \neq n'$, there exists i, $0 \leq i \leq p_1 - 2$, such that*

$$\sum_{j=0}^{p_2-1} \eta^{(1)}_{n+i+j\frac{e_1}{p_2}} \neq \sum_{j=0}^{p_2-1} \eta^{(1)}_{n'+i+j\frac{e_1}{p_2}}.$$

Proof. Let $\theta_i := \frac{1}{p_1}(f_1 + \sum_{j=0}^{p_1-2} \eta^{(1)}_{i+j} a^{g_1^j}), \quad 0 \leq i \leq e_1 - 1$ be the primitive central idempotents of $\mathbb{F}_q[\langle a \rangle]$ as given in Proposition 1.1. Suppose the Lemma is not true, i.e., we have

$$\sum_{j=0}^{p_2-1} \eta^{(1)}_{n+i+j\frac{e_1}{p_2}} = \sum_{j=0}^{p_2-1} \eta^{(1)}_{n'+i+j\frac{e_1}{p_2}}$$

for $0 \leq i \leq p_1 - 2$. It then follows that

$$\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} = \sum_{j=0}^{p_2-1} \theta_{k+n'-n+j\frac{e_1}{p_2}}$$

for $0 \leq k \leq \frac{e_1}{p_2} - 1$. Therefore,

$$\begin{aligned}
\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} &= \left(\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} \right)^2 \\
&= \left(\sum_{i=0}^{p_2-1} \theta_{k+i.\frac{e_1}{p_2}} \right) \left(\sum_{j=0}^{p_2-1} \theta_{k+n'-n+j\frac{e_1}{p_2}} \right) \\
&= \sum_{i=0}^{p_2-1} \sum_{j=0}^{p_2-1} \theta_{k+i\frac{e_1}{p_2}} \theta_{k+n'-n+j\frac{e_1}{p_2}}.
\end{aligned}$$

However, for $0 \leq i, j \leq p_2 - 1$, $n \neq n'$, the idempotent $\theta_{k+i\frac{e_1}{p_2}}$ is orthogonal to $\theta_{k+n'-n+j\frac{e_1}{p_2}}$. Thus we have

$$\sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} = 0, \quad 0 \leq k \leq \frac{e_1}{p_2} - 1.$$

Adding these equations, we get

$$\sum_{k=0}^{\frac{e_1}{p_2}-1} \sum_{j=0}^{p_2-1} \theta_{k+j\frac{e_1}{p_2}} = 0.$$

Now the left hand side of the above equation is equal to $\sum_{i=0}^{e_1-1}\theta_i$. We thus have a contradiction, since

$$\sum_{i=0}^{e_1-1}\theta_i = 1 - \frac{1}{p_1}\sum_{i=0}^{p_1-1} a^i \neq 0. \ \square$$

As a result of the foregoing Lemmas, we have the following:

Theorem 1.8 [BGP11] *Let G be a group given by the presentation (1.5).*

(i) If $p_2 \mid f_1$, then $\mathbb{F}_q[G]$ has exactly the following e_1+e_2+1 distinct primitive central idempotents:

$$\tfrac{1}{p_1p_2}\sum_{g\,G} g,$$

$$\tfrac{1}{p_1p_2}\left(f_2\sum_{x=0}^{p_1-1}a^x + \sum_{j=0}^{p_2-2}\eta^{(2)}_{m+j}\left(\sum_{x=0}^{p_1-1}a^x b^{g_2^j}\right)\right), \quad 0\le m\le e_2-1,$$

$$\tfrac{p_2}{p_1\,[\mathbb{F}_q(\zeta_1):K]}\left(f_1+\sum_{k=0}^{p_1-2}\eta^{(1)}_{n+k}a^{g_1^k}\right), \quad 0\le n\le e_1-1.$$

(ii) If $p_2 \nmid f_1$, then $\mathbb{F}_q[G]$ has exactly the following $\frac{e_1}{p_2}+e_2+1$ distinct primitive central idempotents:

$$\tfrac{1}{p_1p_2}\sum_{g\in G} g,$$

$$\tfrac{1}{p_1p_2}\left(f_2\sum_{x=0}^{p_1-1}a^x + \sum_{j=0}^{p_2-2}\eta^{(2)}_{m+j}\left(\sum_{x=0}^{p_1-1}a^x b^{g_2^j}\right)\right), \quad 0\le m\le e_2-1,$$

$$\tfrac{1}{p_1\,[\mathbb{F}_q(\zeta_1):K]}\left(f_1p_2+\sum_{i=0}^{p_1-2}\left(\sum_{j=0}^{p_2-1}\eta^{(1)}_{n+i+j\frac{e_1}{p_2}}\right)a^{g_1^i}\right), \quad 0\le n\le \tfrac{e_1}{p_2}-1. \ \square$$

Metacyclic groups

Let G be a metacyclic group given by the presentation

$$G = \langle a, b \,|\, a^n = 1,\, b^t = a^k,\, b^{-1}ab = a^r\rangle,$$

where n, t, r, k are natural numbers with $r^t \equiv 1 \pmod n$, $kr \equiv k \pmod n$. Let q be a prime power coprime to nt. The cyclic group $\langle q \rangle$ contained in $\mathbb{Z}_n^*$ acts on $[n]$ by setting $q.i = qi \pmod n$, $i \in [n]$. Let $C(q,\, i,\, n)$ denote the orbit of $i \in [n]$.

For $d|n$ and $l|\frac{n}{d}s_d$, define

- $f_d := |C(q,\, d,\, n)|$.
- $h_{d,\,l} := |C(q, l, \frac{n}{d}s_d)|$.
- $g_{d,\,l} := \gcd(f_d, h_{d,\,l})$.
- $\ell_{d,\,l} := \operatorname{lcm}(f_d, h_{d,\,l})$.
- $k_{d,\,l}$:= the smallest positive integer m such that $r^m \equiv (q^{g_{d,\,l}})^x \pmod{\frac{n}{d}}$ for some integer x.
- $v_{d,\,l} := \frac{s_d}{\gcd(l,\, s_d)}$.

For $d|n$, $l|\frac{n}{d}s_d$, $(i,\, j) \in X_{d,\,l}$, where $X_{d,\,l}$ is as defined in equation (1.4), $0 \le x \le n-1$ and $0 \le y \le s_d - 1$, define

- $u_{d,\,l}(i,\, j)$:= the solution of the congruence $\frac{i}{d}x \equiv -\frac{\frac{i}{d}k + \frac{n}{d}j}{\gcd(l,\, s_d)} \pmod{\frac{n}{d}}$.
- $C_{d,\,l}(i,\, j)$:= the q-cyclotomic coset of the character in $\operatorname{Irr}(\langle a, b^{l_d}\rangle / \langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle)$ given by

$$a + \langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle \mapsto \zeta^{-it},\ b^{l_d} + \langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle \mapsto \zeta^{-l_d(ik+nj)},$$

  where $u = u_{d,\,l}(i,\, j)$, $v = v_{d,\,l}$ and ζ is a primitive nt-th root of unity in $\overline{\mathbb{F}}_q$.
- $A_{d,\,l}(i,\, j,\, x,\, y) := \frac{\ell_{d,\,l}}{g_{d,\,l}|C(q^{g_{d,l}}, (ik+nj)y, ns_d)||C(q^{g_{d,l}}, ix, n)|}$,
- $\alpha_{d,\,l}(i,\, j,\, x,\, y) :=$
  $A \sum_{\alpha=0}^{k_{d,\,l}-1} \sum_{\beta=0}^{g_{d,\,l}-1} \left(\sum_{z \in C(q^{g_{d,l}}, ixr^\alpha, n)} (\zeta^{tz})^{q^\beta} \right) \left(\sum_{w \in C(q^{g_{d,l}}, (ik+nj)y,\, ns_d)} (\zeta^{l_d w})^{q^\beta} \right)$, where
  $A = A_{d,\,l}(i,\, j,\, x,\, y)$.

Given $d \,|\, n,\ l \,|\, \frac{n}{d}s_d$ and $(i,\, j), (i',\, j') \in X_{d,\,l}$, we say that $(i', j') \sim (i,\, j)$ if there exists an integer λ such that

(i) $i'k + nj' \equiv (ik + nj)q^\lambda \pmod{ns_d}$,
(ii) $\operatorname{orb}(i') = \operatorname{orb}(iq^\lambda)$, i.e., $i' \equiv iq^\lambda r^\mu \pmod n$, for some $\mu \ge 0$.

It is easy to see that the relation $\sim$ defined above on $X_{d,\,l}$ is an equivalence relation. Let $[X_{d,\,l}]$ denote a set of representatives of distinct equivalence classes of $X_{d,\,l}$ under the above equivalence relation.

With the group G and the notation as above, the following result gives a complete set of primitive central idempotents of $\mathbb{F}_q[G]$.

Theorem 1.9 [BGP] (i) *Let* $d|n$, $l|\frac{n}{d}s_d$ *and* $(i,\,j) \in X_{d,\,l}$. *Let* $u = u_{d,\,l}(i,\,j)$, $v = v_{d,\,l}$, *and* $C = C_{d,\,l}(i,\,j)$. *Then*

$$e_{\mathbb{F}_q}(\chi_{i,\,j}) = e_C(G, \langle a, b^{l_d}\rangle, \langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle) = \frac{1}{ns_d}\sum_{x=0}^{n-1}\sum_{y=0}^{s_d-1}\alpha_{d,\,l}(i,\,j,\,x,\,y)\,a^x b^{y\,l_d}. \quad (1.13)$$

(ii) $\{e_{\mathbb{F}_q}(\chi_{i,\,j}) \mid (i,\,j) \in \bigcup_{d|n}\bigcup_{l|\frac{n}{d}s_d}[X_{d,\,l}]\}$ *is a complete set of primitive central idempotents of* $\mathbb{F}_q[G]$.

We will prove the above result in a number of steps.

Let G be a finite group of order coprime to q and $N \trianglelefteq G$. Let ψ be a linear character on N and let C be the q-cyclotomic coset of $\overline{\psi} \in \mathrm{Irr}(N/\ker\psi)$, where $\overline{\psi}$ is the corresponding character of $N/\ker\psi$ given by $\overline{g} = g\ker\psi \mapsto \psi(g)$. Let $\chi = \psi^G$. With this notation we have the following:

Theorem 1.10 *If* $\chi \in \mathrm{Irr}(G)$, *then*

(i) $e_{\mathbb{F}_q}(\psi) = \varepsilon_C(N,\,\ker\psi)$.

(ii) $e_{\mathbb{F}_q}(\chi) = e_C(G,\,N,\,\ker\psi)$.

Proof. (i) Let η be a primitive $|N/\ker\psi|^{th}$ root of unity in $\overline{\mathbb{F}}_q$. We have

$$\begin{aligned}
e_{\mathbb{F}_q}(\psi) &= \frac{1}{|N|}\sum_{g\in N}\sum_{\tau\in\mathcal{G}(\psi)}\tau(\psi(g^{-1}))g,\\
&= \frac{1}{|N|}\sum_{g\in N}\sum_{\tau\in\mathcal{G}(\psi)}\tau(\overline{\psi}((\overline{g})^{-1}))g,\\
&= \frac{1}{|N|}\sum_{g\in N}\sum_{\tau\in\mathrm{Gal}(\mathbb{F}_q(\eta)/\mathbb{F}_q)}\tau(\overline{\psi}((\overline{g})^{-1}))g, \quad (\mathcal{G}(\psi)=\mathrm{Gal}(\mathbb{F}_q(\eta)/\mathbb{F}_q)),\\
&= \frac{1}{|N|}\sum_{g\in N}\mathrm{Tr}_{\mathbb{F}_q(\eta)/\mathbb{F}_q}(\overline{\psi}((\overline{g})^{-1}))g,\\
&= \varepsilon_C(N,\ker\psi).
\end{aligned}$$

This proves (i).

(ii) Let $\{x_1, x_2, \ldots, x_m\}$ be a transversal of N in G. We have

$$\begin{aligned}
[\mathbb{F}_q(\psi):\mathbb{F}_q(\chi)]e_{\mathbb{F}_q}(\chi) &= \frac{\chi(1)[\mathbb{F}_q(\psi):\mathbb{F}_q(\chi)]}{|G|}\sum_{g\in G}\sum_{\tau\in\mathcal{G}(\chi)}\tau(\chi(g^{-1}))g,\\
&= \frac{[G:N]}{|G|}\sum_{g\in G}\sum_{\tau\in\mathcal{G}(\psi)}\tau(\chi(g^{-1}))g,\\
&= \frac{1}{|N|}\sum_{g\in N}\sum_{\tau\in\mathcal{G}(\psi)}\sum_{i=1}^{m}\tau(\psi(x_i^{-1}g^{-1}x_i))g,\\
&= \sum_{i=1}^{m}x_i\left(\frac{1}{|N|}\sum_{g\in N}\sum_{\tau\in\mathcal{G}(\psi)}\tau(\psi(g^{-1}))g\right)x_i^{-1},\\
&= \sum_{i=1}^{m}x_i e_{\mathbb{F}_q}(\psi)x_i^{-1},\\
&= \sum_{i=1}^{m}x_i\varepsilon_C(N,\ker\psi)x_i^{-1},\\
&= [\mathrm{Cen}_G(\varepsilon_C(N,\ker\psi)):N]\sum_{j=1}^{m'}y_j\varepsilon_C(N,\ker\psi)y_j^{-1},
\end{aligned}$$

where $\mathrm{Cen}_G(\varepsilon_C(N,\ker\psi))$ denotes the centralizer of $\varepsilon_C(N,\ker\psi)$ in G, and $\{y_1, y_2, \ldots, y_{m'}\}$ is a transversal of $\mathrm{Cen}_G(\varepsilon_C(N,\ker\psi))$ in G. As $\sum_{j=1}^{m'}y_j\varepsilon_C(N,\ker\psi)y_j^{-1}$,

being a sum of distinct primitive central idempotents of $\mathbb{F}_q[N]$, is a non-zero idempotent, it follows that,

$$[\mathbb{F}_q(\psi) : \mathbb{F}_q(\chi)] = [\mathrm{Cen}_G(\varepsilon_C(N, \ker\psi)) : N], \tag{1.14}$$

and

$$e_{\mathbb{F}_q}(\chi) = \sum_{j=1}^{m'} y_j \varepsilon_C(N, \ker\psi) y_j^{-1} = e_C(G, N, \ker\psi).$$

This completes the proof of (ii). $\square$

Let $d|n,\ l|\frac{n}{d}s_d$ and $(i, j) \in X_{d,l}$. Let $\psi_{i,j} : \langle a, b^{l_d}\rangle \to \overline{\mathbb{F}}_q$ be the linear character of $\langle a, b^{l_d}\rangle$ given by $\psi_{i,j}(a) = \zeta^{-it}$ and $\psi_{i,j}(b^{l_d}) = \zeta^{-l_d(ik+nj)}$. It is easy to see that $\chi_{i,j}$ is induced from the linear character $\psi_{i,j}$ of $\langle a, b^{l_d}\rangle$.

Lemma 1.11 *Let $d|n,\ l|\frac{n}{d}s_d$ and $(i, j) \in X_{d,l}$. Then*

$$e_{\mathbb{F}_q}(\psi_{i,j}) = \varepsilon_C(\langle a, b^{l_d}\rangle, \langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle) = \frac{1}{ns_d}\sum_{x=0}^{n-1}\sum_{y=0}^{s_d-1}\beta_{x,y}\, a^x b^{y l_d}, \tag{1.15}$$

where

$$\beta_{x,y} \;=\; A_{d,l}(i, j, x, y)\sum_{\beta=0}^{g_{d,l}-1}\left(\sum_{z\in C(q^{g_{d,l}}, ix, n)}(\zeta^{tz})^{q^\beta}\right)\left(\sum_{w\in C(q^{g_{d,l}}, (ik+nj)y, ns_d)}(\zeta^{l_d w})^{q^\beta}\right),$$

u, v, $A_{d,l}(i, j, x, y)$ and the q-cyclotomic coset C are as in the statement of Theorem 1.9.

Proof. The first equality of equation (1.15) follows from Theorem 1.10, if we show that

$$\ker(\psi_{i,j}) = \langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle, \tag{1.16}$$

where u and v are as in the statement. Now, $\psi_{i,j}(a^{\frac{n}{d}}) = \zeta^{-i\frac{n}{d}t} = \zeta^{-n\frac{i}{d}t} = 1$. Also $\psi_{i,j}(a^u b^{l_d v}) = \zeta^{-iut}\zeta^{-l_d v(ik+nj)} = 1$. Thus $a^{\frac{n}{d}}$ and $a^u b^{l_d v}$ belong to $\ker(\psi_{i,j})$. Therefore, $\langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle \subseteq \ker(\psi_{i,j})$. As $\langle a, b^{l_d}\rangle/\ker(\psi_{i,j}) \cong \langle\zeta^{dt}, \zeta^{ldl_d}\rangle$ and $|\langle\zeta^{dt}, \zeta^{ldl_d}\rangle| = \mathrm{lcm}(\frac{n}{d}, \frac{ns_d}{ld}) = \frac{n}{d}\frac{s_d}{\gcd(s_d,l)} = \frac{n}{d}v$, it follows that $|\ker(\psi_{i,j})| = \frac{ds_d}{v}$. Also note that $|\langle a^{\frac{n}{d}}, a^u b^{l_d v}\rangle| = \frac{ds_d}{v}$. Thus the equality in (1.16) follows.

We now prove the second equality of equation (1.15). We have

$$e_{\mathbb{F}_q}(\psi_{i,j}) = \frac{1}{ns_d}\sum_{g\in\langle a, b^{l_d}\rangle}\sum_{\tau\in\mathcal{G}(\psi_{i,j})}\tau(\psi_{i,j}(g^{-1}))g.$$

Since $\mathbb{F}_q(\psi_{i,j}) = \mathbb{F}_q(\zeta^{it}, \zeta^{l_d(ik+nj)}) = \mathbb{F}_q(\zeta^{dt}, \zeta^{ldl_d})$, it follows that

$$[\mathbb{F}_q(\psi_{i,j}) : \mathbb{F}_q] = \mathrm{lcm}(f_d, h_{d,l}) = \ell_{d,l}, \tag{1.17}$$

and

$$e_{\mathbb{F}_q}(\psi_{i,j}) = \frac{1}{ns_d} \sum_{g \in \langle a, b^{l_d} \rangle} \sum_{\tau \in \mathcal{G}(\psi_{i,j})} \tau(\psi_{i,j}(g^{-1}))g = \frac{1}{ns_d} \sum_{x=0}^{n-1} \sum_{y=0}^{s_d-1} \beta_{x,y} a^x b^{l_d y}, \tag{1.18}$$

where

$$\begin{aligned}
\beta_{x,y} &= \sum_{\tau \in \mathrm{Gal}(\mathbb{F}_{q^{\ell_{d,l}}}/\mathbb{F}_q)} \tau(\psi_{i,j}(b^{-l_d y} a^{-x})) \\
&= \sum_{\tau \in \mathrm{Gal}(\mathbb{F}_{q^{\ell_{d,l}}}/\mathbb{F}_q)} \tau(\zeta^{itx} \zeta^{l_d(ik+nj)y}) \\
&= \sum_{\nu=0}^{\ell_{d,l}-1} \zeta^{itxq^\nu} \zeta^{l_d(ik+nj)yq^\nu} \\
&= \sum_{\gamma=0}^{-1+\ell_{d,l}/h_{d,l}} \sum_{\delta=0}^{-1+h_{d,l}} \zeta^{itxq^{\delta+\gamma h_{d,l}}} \zeta^{l_d(ik+nj)yq^{\delta+\gamma h_{d,l}}} \\
&= \sum_{\delta=0}^{-1+h_{d,l}} \left(\sum_{\gamma=0}^{-1+\ell_{d,l}/h_{d,l}} \left(\zeta^{itxq^{\gamma h_{d,l}}}\right)^{q^\delta} \right) \zeta^{l_d(ik+nj)yq^\delta}, \\
&\qquad \text{as } l_d(ik+nj)q^{h_{d,l}} \equiv l_d(ik+nj) \pmod{nt}, \\
&= \frac{\ell_{d,l}}{h_{d,l}|C(q^{h_{d,l}}, ix, n)|} \sum_{\delta=0}^{-1+h_{d,l}} \left(\sum_{z \in C(q^{h_{d,l}}, ix, n)} (\zeta^{tz})^{q^\delta} \right) \zeta^{l_d(ik+nj)yq^\delta}.
\end{aligned}$$

We now show that

$$C(q^{h_{d,l}}, ix, n) = C(q^{g_{d,l}}, ix, n). \tag{1.19}$$

As $g_{d,l}$ divides $h_{d,l}$, we clearly have $C(q^{h_{d,l}}, ix, n) \subseteq C(q^{g_{d,l}}, ix, n)$. In order to see that the right hand side of (1.19) is contained in its left hand side, we write $g_{d,l} = x_0 f_d + y_0 h_{d,l}$, where x_0 and y_0 integers, and note that for any integer $z_0 \geq 0$,

$$ixq^{z_0 g_{d,l}} = ixq^{z_0 x_0 f_d} q^{z_0 y_0 h_{d,l}} \equiv ixq^{z_0 y_0 h_{d,l}} \pmod{n}. \tag{1.20}$$

Since the left hand side of (1.20) is an arbitrary element of $C(q^{g_{d,l}}, ix, n)$ and the right hand side of (1.20) belongs to $C(q^{h_{d,l}}, ix, n)$, it follows that $C(q^{g_{d,l}}, ix, n) \subseteq C(q^{h_{d,l}}, ix, n)$ and hence (1.19) is proved.

In view of (1.19), $\beta_{x,\,y}$ now becomes

$$\begin{aligned}
&= \frac{\ell_{d,\,l}}{h_{d,l}|C(q^{g_{d,\,l}},ix,n)|}\sum_{\delta=0}^{-1+h_{d,\,l}}\left(\sum_{z\in C(q^{g_{d,\,l}},ix,n)}(\zeta^{tz})^{q^\delta}\right)\zeta^{l_d(ik+nj)yq^\delta}\\
&= \frac{\ell_{d,\,l}}{h_{d,l}|C(q^{g_{d,\,l}},\,ix,\,n)|}\sum_{\mu=0}^{-1+h_{d,\,l}/g_{d,\,l}}\sum_{\beta=0}^{g_{d,\,l}-1}\left(\sum_{z\in C(q^{g_{d,\,l}},ix,n)}(\zeta^{tzq^{\mu g_{d,\,l}}})^{q^\beta}\right)(\zeta^{l_d(ik+nj)yq^{\mu g_{d,\,l}}})^{q^\beta}\\
&= \frac{\ell_{d,\,l}}{h_{d,l}|C(q^{g_{d,\,l}},\,ix,\,n)|}\sum_{\mu=0}^{-1+h_{d,\,l}/g_{d,\,l}}\sum_{\beta=0}^{g_{d,\,l}-1}\left(\sum_{z\in C(q^{g_{d,\,l}},\,ix,\,n)}(\zeta^{tz})^{q^\beta}\right)(\zeta^{l_d(ik+nj)yq^{\mu g_{d,\,l}}})^{q^\beta}\\
&= \frac{\ell_{d,\,l}}{h_{d,l}|C(q^{g_{d,\,l}},\,ix,\,n)|}\sum_{\beta=0}^{g_{d,\,l}-1}\left(\sum_{z\in C(q^{g_{d,\,l}},\,ix,\,n)}(\zeta^{tz})^{q^\beta}\right)\left(\sum_{\mu=0}^{-1+h_{d,\,l}/g_{d,\,l}}(\zeta^{l_d(ik+nj)yq^{\mu g_{d,\,l}}})^{q^\beta}\right)\\
&= A_{d,l}(i,\,j,\,x,\,y)\sum_{\beta=0}^{g_{d,\,l}-1}\left(\sum_{z\in C(q^{g_{d,\,l}},\,ix,\,n)}(\zeta^{tz})^{q^\beta}\right)\left(\sum_{w\in C(q^{g_{d,\,l}},\,(ik+nj)y,\,ns_d)}(\zeta^{l_d w})^{q^\beta}\right),
\end{aligned}$$

where $A_{d,l}(i,\,j,\,x,\,y)$ is as in the statement. Now substituting the above expression of $\beta_{x,\,y}$ in (1.18), we obtain the second equality of equation (1.15). $\square$

Lemma 1.12 *Let $d|n,\ l|\frac{n}{d}s_d$ and $(i,\,j)\in X_{d,\,l}$.*

(i) For $s\geq 0$, let $j_s\equiv j+\frac{ik(1-r^s)}{n}\pmod{s_d}$. Then $(ir^s,j_s)\in X_{d,\,l}$ and

$$b^s e_{\mathbb{F}_q}(\psi_{i,\,j})b^{-s}=e_{\mathbb{F}_q}(\psi_{ir^s,\,j_s}).$$

(ii) $\mathrm{Cen}_G(e_{\mathbb{F}_q}(\psi_{i,\,j}))=\langle a,\,b^{k_{d,\,l}}\rangle$ and $\{1,\,b,\,\ldots,\,b^{k_{d,\,l}-1}\}$ is a transversal of $\mathrm{Cen}_G(e_{\mathbb{F}_q}(\psi_{i,\,j}))$ in G.

Proof. *(i)* Since $\gcd(r,\,n)=1$, we have $\gcd(ir^s,\,n)=\gcd(i,\,n)=d$ and

$$\begin{aligned}
\frac{ir^s}{d}k+\frac{n}{d}j_s &\equiv \frac{ir^s}{d}k+\frac{n}{d}(j+\frac{ik(1-r^s)}{n})\pmod{\frac{n}{d}s_d}\\
&\equiv \frac{i}{d}k+\frac{n}{d}j\pmod{\frac{n}{d}s_d}.
\end{aligned}$$

Thus $\gcd(\frac{ir^s}{d}k+\frac{n}{d}j_s,\,\frac{n}{d}s_d)=\gcd(\frac{i}{d}k+\frac{n}{d}j,\,\frac{n}{d}s_d)=l$. Hence $(ir^s,\,j_s)\in X_{d,\,l}$. Now, by Lemma 1.11, we get that the coefficient of a^xb^{lay} in the expression of $e_{\mathbb{F}_q}(\psi_{ir^s,\,j_s})$ is

$$A_{d,l}(i,\,j,\,x,\,y)\sum_{\beta=0}^{g_{d,\,l}-1}\left(\sum_{z\in C(q^{g_{d,\,l}},\,ir^sx,\,n)}(\zeta^{tz})^{q^\beta}\right)\left(\sum_{w\in C(q^{g_{d,\,l}},\,(ik+nj)y,\,ns_d)}(\zeta^{l_d w})^{q^\beta}\right),$$

which is same as the coefficient of $a^x b^{l_d y}$ in the expression of $b^s e_{\mathbb{F}_q}(\psi_{i,j}) b^{-s}$. Thus (i) is proved.

(ii) Since $e_{\mathbb{F}_q}(\psi_{i,j})$ is a central idempotent of $\mathbb{F}_q[\langle a,\, b^{l_d}\rangle]$, we have $\langle a,\, b^{l_d}\rangle \subseteq \mathrm{Cen}_G(e_{\mathbb{F}_q}(\psi_{i,j}))$. Let $b^s \in \mathrm{Cen}_G(e_{\mathbb{F}_q}(\psi_{i,j}))$. Then $b^s e_{\mathbb{F}_q}(\psi_{i,j}) b^{-s} = e_{\mathbb{F}_q}(\psi_{i,j})$. Therefore, by (i),

$$e_{\mathbb{F}_q}(\psi_{ir^s,\,j_s}) = e_{\mathbb{F}_q}(\psi_{i,j}), \tag{1.21}$$

which, by Lemma 1.11, gives that

$$\varepsilon_{C'}(\langle a, b^{l_d}\rangle, \ker(\psi_{ir^s,\,j_s})) = \varepsilon_C(\langle a, b^{l_d}\rangle, \ker(\psi_{i,j})), \tag{1.22}$$

where C' is the q-cyclotomic coset of $\mathrm{Irr}(\langle a, b^{l_d}\rangle/\ker(\psi_{ir^s,\,j_s}))$ containing $\overline{\psi}_{ir^s,\,j_s}$. Also equation (1.21) implies that $\psi_{ir^s,\,j_s} = \tau \circ \psi_{i,j}$, for some $\tau \in \mathcal{G}(\psi_{i,j})$. This gives that $\ker(\psi_{ir^s,\,j_s}) = \ker(\psi_{i,j})$. Consequently, we get from equation (1.22), that $\varepsilon_{C'}(\langle a, b^{l_d}\rangle, \ker(\psi_{i,j})) = \varepsilon_C(\langle a, b^{l_d}\rangle, \ker(\psi_{i,j}))$. This gives, by Theorem 1.2(iii), that $C = C'$, i.e., $\psi_{ir^s,\,j_s} = {\psi_{i,j}}^{q^c}$, for some integer $c \geq 1$. Now evaluating both $\psi_{ir^s,\,j_s}$ and ${\psi_{i,j}}^{q^c}$ at a and b^{l_d}, we obtain that

$$ik + nj \equiv (ik + nj)q^c \pmod{ns_d},$$

and

$$ir^s \equiv iq^c \pmod{n}.$$

The first congruence implies that $h_{d,l} \,|\, c$ and consequently, the second congruence yields $k_{d,l} \,|\, s$. However, it is easily seen that $b^{k_{d,l}} \in \mathrm{Cen}_G(e_{\mathbb{F}_q}(\psi_{i,j}))$. Therefore, we obtain that $\{1,\, b,\, \ldots,\, b^{k_{d,l}-1}\}$ is a transversal of $\mathrm{Cen}_G(e_{\mathbb{F}_q}(\psi_{i,j}))$ in G. $\square$

Proof of Theorem 1.9. (i) It follows from Theorem 1.10 and Lemmas 1.11, 1.12 that

$$e_{\mathbb{F}_q}(\chi_{i,j}) = \sum_{s=0}^{k_{d,l}-1} b^s e_{\mathbb{F}_q}(\psi_{i,j}) b^{-s} = \sum_{s=0}^{k_{d,l}-1} e_{\mathbb{F}_q}(\psi_{ir^s,\,j_s}). \tag{1.23}$$

Now substituting the expression of $e_{\mathbb{F}_q}(\psi_{ir^s,\,j_s})$ obtained from Lemma 1.11, we get the required expression of $e_{\mathbb{F}_q}(\chi_{i,j})$.

(ii) Let $d|n$, $l|\frac{n}{d}s_d$, $(i,\, j)$, $(i',\, j') \in X_{d,l}$ be such that $(i',\, j') \sim (i,\, j)$. Then it follows immediately from the expressions of $e_{\mathbb{F}_q}(\chi_{i,j})$ and $e_{\mathbb{F}_q}(\chi_{i',j'})$ given by (i) that $e_{\mathbb{F}_q}(\chi_{i,j}) = e_{\mathbb{F}_q}(\chi_{i',j'})$.

Conversely, let $(i,\, j)$, $(i',\, j') \in \bigcup_{d|n} \bigcup_{l|\frac{n}{d}s_d} X_{d,l}$ be such that

$$e_{\mathbb{F}_q}(\chi_{i,j}) = e_{\mathbb{F}_q}(\chi_{i',j'}). \tag{1.24}$$

In order to prove (ii), we need to show that there exist integers $d,\, l \geq 1$, $d|n$, $l|\frac{n}{d}s_d$ such that $(i,\, j)$, $(i',\, j') \in X_{d,l}$ and $(i',\, j') \sim (i,\, j)$. Equation (1.24) implies

$$\chi_{i',\,j'} = \tau \circ \chi_{i,\,j}, \tag{1.25}$$

for some $\tau \in \mathcal{G}(\chi_{i,\,j})$. This gives that $\chi_{i,\,j}$ and $\chi_{i',\,j'}$ have the same degrees, i.e., $l_i = l_{i'}$. Also it follows from equation (1.25) that $\ker(\chi_{i',\,j'}) = \ker(\chi_{i,\,j})$, which implies that $\langle a^{n/\gcd(i',\,n)}\rangle = \ker(\chi_{i',\,j'}) \cap \langle a\rangle = \ker(\chi_{i,\,j}) \cap \langle a\rangle = \langle a^{n/\gcd(i,\,n)}\rangle$. Consequently, $\gcd(i',\, n) = \gcd(i,\, n) = d$, say.

Let $l = \gcd(\frac{i}{d}k + \frac{n}{d}j, \frac{n}{d}s_d)$ and $l' = \gcd(\frac{i'}{d}k + \frac{n}{d}j', \frac{n}{d}s_d)$. By Lemma 1.11 and equations (1.23), (1.24), we have $\sum_{s=0}^{k_{d,\,l}-1} e_{\mathbb{F}_q}(\psi_{ir^s,\,j_s}) = \sum_{s=0}^{k_{d,\,l'}-1} e_{\mathbb{F}_q}(\psi_{i'r^s,\,j'_s})$, which holds if, and only if,

$$e_{\mathbb{F}_q}(\psi_{i,\,j}) = e_{\mathbb{F}_q}(\psi_{i'r^s,\,j'_s}), \tag{1.26}$$

for some $s \geq 0$, i.e.,

$$\varepsilon_C(\langle a,\, b^{l_d}\rangle,\, \ker(\psi_{i,\,j})) = \varepsilon_{C'}(\langle a,\, b^{l_d}\rangle,\, \ker(\psi_{i'r^s,\,j'_s})). \tag{1.27}$$

Also equation (1.26) implies that

$$\psi_{i'r^s,\,j'_s} = \tau \circ \psi_{i,\,j}, \tag{1.28}$$

for some $\tau \in \mathcal{G}(\psi_{i,\,j})$, which gives that $\ker(\psi_{i'r^s,\,j'_s}) = \ker(\psi_{i,\,j})$. Consequently, equation (1.27) and Theorem 1.2(iii) gives that $C = C'$. Therefore, $\psi_{i'r^s,\,j'_s} = {\psi_{i,\,j}}^{q^c}$, for some $c \geq 0$ which yields, by evaluating $\psi_{i'r^s,\,j'_s},\ {\psi_{i,\,j}}^{q^c}$ at a and b^{l_d}, that $l = l'$ and $(i',\, j') \sim (i,\, j)$. This completes the proof of (ii). $\square$

Metabelian groups

Let G be a finite group and H a subgroup of G. We set

$$\hat{H} = \frac{1}{|H|}\sum_{h \in H} h$$

and let

$$\mathcal{M}(G/H) = \quad \text{the set of minimal normal subgroups of } G \text{ containing } H \text{ properly.}$$

Let $\varepsilon(K,\, H)$ be the element of the rational group algebra $\mathbb{Q}[G]$ given by

$$\varepsilon(K,\, H) = \begin{cases} \prod_{M/H \in \mathcal{M}(K/H)} (\hat{H} - \hat{M}), & \text{if } H \neq K, \\ \hat{K}, & \text{if } H = K. \end{cases}$$

Definition 1.13 *A strongly Shoda pair of G is a pair $(K,\, H)$ of subgroups of G with the properties that*
(i) $H \leq K \trianglelefteq N_G(H)$,
(ii) K/H *is cyclic and a maximal abelian subgroup of* $N_G(H)/H$,
(iii) the different G-conjugates of $\varepsilon(K,\, H)$ are mutually orthogonal.

Let $H \trianglelefteq K \leq G$ be such that K/H is cyclic. Let $g \in G$. For a character ψ of K, let $\psi^{(g)}$ denote the character of $K^{(g)} := g^{-1}Kg$ defined by $\psi^{(g)}(x) = \psi(gxg^{-1})$. Clearly $\ker(\psi) = H$ if, and only if, $\ker(\psi^{(g)}) = H^{(g)}$. Therefore, the map π given by $\psi \mapsto \psi^{(g)}$ defines a bijection between the generators of $\mathrm{Irr}(K/H)$ and those of $\mathrm{Irr}(K^{(g)}/H^{(g)})$. Note that if C is the q-cyclotomic coset of ψ then $C^{(g)} := \pi(C)$ is the q-cyclotomic coset of $\psi^{(g)}$. Thus π in turn induces a bijection $\pi^{(g)} : \mathcal{C}(K/H) \to \mathcal{C}(K^{(g)}/H^{(g)})$ given by $C \mapsto C^{(g)}$.

Let $N = N_G(H) \cap N_G(K)$. Define an action of N on $\mathcal{C}(K/H)$ as follows:

$$g.C = C^{(g)},\ g \in N,\ C \in \mathcal{C}(K/H).$$

Note that under this action the stabilizer of any $C \in \mathcal{C}(K/H)$ remains the same. For $C \in \mathcal{C}(K/H)$, let Orb(C) denote the orbit of C and

$$E_G(K/H) = \quad \text{the stablizer of } C.$$

Let

$$R(K/H) = \text{ the set of representatives of distinct orbits of } \mathcal{C}(K/H).$$

Define

$$o(K,\, H) = \frac{\mathrm{ord}_{[K:H]}(q)}{[E_G(K/H) : K]}. \tag{1.29}$$

The following result is due to Broche and Rio [BdR07].

Theorem 1.14 *Let $\mathbb{F}_q$ be a finite field of order q and G a finite group of order coprime to q. Let $(K,\, H)$ be a strongly Shoda pair of G and $C \in \mathcal{C}(K/H)$. Then*
(i) $\mathrm{Cen}_G(\varepsilon_C(K,\, H)) = E_G(K/H)$.
(ii) $e_C(G,\, K,\, H)$ *is a primitive central idempotent of* $\mathbb{F}_q[G]$.
(iii) $\mathbb{F}_q[G]e_C(G,\, K,\, H) \cong M_{[G:K]}(\mathbb{F}_{q^{o(K,\, H)}})$.

Furthermore, if G is an abelian-by-supersolvable group, the every primitive central idempotent of $\mathbb{F}_q[G]$ is of the form $e_C(G,\, K,\, H)$, for a strongly Shoda pair $(K,\, H)$ of G and $C \in \mathcal{C}(K/H)$.

Let G be a finite metabelian group of order coprime to q. Let

- $\mathcal{A}$:= a fixed maximal abelian subgroup of G containing G'.
- $\mathcal{T}$:= the set of all subgroups D of G with $D \leq \mathcal{A}$ and $\mathcal{A}/D$ cyclic.

For D_1, $D_2 \in \mathcal{T}$, we say that D_1 is equivalent to D_2 if there exists $g \in G$ such that $D_2 = g^{-1}D_1g$. Let

- $\mathcal{T}_G$:= a set of representatives of the distinct equivalence classes of $\mathcal{T}$.

For $D \in \mathcal{T}$, let

- K_D := a fixed maximal element of $\{K \mid \mathcal{A} \leq K \leq G,\ K' \leq D\}$.
- $\mathcal{R}(D)$:= the set of those linear representations of K_D over $\overline{\mathbb{F}}_q$ whose restriction to $\mathcal{A}$ has kernel D.
- $\mathcal{R}_C(D)$:= a complete set of those representations in $\mathcal{R}(D)$ which are not mutually G-conjugate.

The following result is proved in [BKP13] for complex irreducible representations. However, the analogous proof works for the irreducible representations of G over $\overline{\mathbb{F}}_q$.

Theorem 1.15 [BKP13] *Let G be a finite metabelian group with $\mathcal{A}$ and $\mathcal{T}_G$ as defined above. Then*

$$\Omega = \{\rho^G,\ \rho \in \mathcal{R}_C(D),\ D \in \mathcal{T}_G\},$$

is a complete set of inequivalent irreducible representations of G over $\overline{\mathbb{F}}_q$.

Furthermore, $\rho^G \in \Omega$ is faithful if, and only if, D is core-free.

For $N \trianglelefteq G$ with

$$\mathcal{A}_N/N = \text{ a maximal abelian subgroup of } G/N \text{ containing } (G/N)',$$

define

$$\mathcal{S}_{G/N} = \{(D/N,\, \mathcal{A}_N/N) \mid D/N \in \mathcal{T}_{G/N},\, D/N \text{ core-free in } G/N\}.$$

Let

$$\mathcal{S} := \{(N,\, D/N,\, \mathcal{A}_N/N) \mid N \trianglelefteq G,\, \mathcal{S}_{G/N} \neq \emptyset,\, (D/N,\, \mathcal{A}_N/N) \in \mathcal{S}_{G/N}\}.$$

The following is our main result on the primitive central idempotents of a semisimple finite group algebra of a metabelian group.

Theorem 1.16 *Let $\mathbb{F}_q$ be a finite field with q elements and G a finite metabelian group of order coprime to q. Then*

$$\{e_C(G,\, \mathcal{A}_N,\, D) \mid (N,\, D/N,\, \mathcal{A}_N/N) \in \mathcal{S},\, C \in \mathcal{R}(\mathcal{A}_N/D)\}$$

is a complete set of primitive central idempotents of $\mathbb{F}_q[G]$.

Proof. Let

$$\mathfrak{S} := \{((N,\, D/N,\, \mathcal{A}_N/N),\, C) \,|\, (N,\, D/N,\, \mathcal{A}_N/N) \in \mathcal{S},\, C \in \mathcal{R}(\mathcal{A}_N/D)\}. \quad (1.30)$$

If $((N,\, D/N,\, \mathcal{A}_N/N),\, C) \in \mathfrak{S}$, then, by ([BKP13], Lemma 6), $(\mathcal{A}_N,\, D)$ is a strongly Shoda pair in G, and therefore, by Theorem 1.14 (ii), $e_C(G,\, \mathcal{A}_N,\, D)$ is a primitive central idempotent of $\mathbb{F}_q[G]$. Thus we have a map

$$\pi : ((N,\, D/N,\, \mathcal{A}_N/N),\, C) \mapsto e_C(G,\, \mathcal{A}_N,\, D)$$

from $\mathfrak{S}$ to a complete set of primitive central idempotents of $\mathbb{F}_q[G]$. In order to prove the Theorem, we need to prove that π is 1-1 and onto.

To show that π is onto, let e be a primitive central idempotent of $\mathbb{F}_q[G]$. We have $e = e_{\mathbb{F}_q}(\chi)$, for some $\chi \in \mathrm{Irr}(G)$. Let τ be a representation affording χ and $N = \ker \tau$. Let $\overline{\tau}$ be the corresponding faithful representation of G/N. By Theorem 1.15, it follows that there exists a unique pair $(D/N,\, \mathcal{A}_N/N) \in S_{G/N}$ and a representation $\overline{\rho}$ of $\mathcal{A}_N/N$ with kernel D/N such that $\overline{\tau} = \overline{\rho}^{G/N}$. This yields $\chi = \psi^G$, where ψ is the character afforded by $\rho : \mathcal{A}_N \to \overline{\mathbb{F}}_q$ given by $\rho(x) = \overline{\rho}(xN)$. Since $\ker \psi = D$, by Theorem 1.10, we have

$$e_{\mathbb{F}_q}(\chi) = e_C(G,\, \mathcal{A}_N,\, D), \quad (1.31)$$

where $C \in \mathcal{R}(\mathcal{A}_N/D)$ is the q-cyclotomic coset of $\overline{\psi}$ and consequently π is onto.

To show that π is 1-1, let $((N,\, D/N,\, \mathcal{A}_N/N),\, C)$ and $((\tilde{N},\, \tilde{D}/\tilde{N},\, \mathcal{A}_{\tilde{N}}/\tilde{N}),\, \tilde{C}) \in \mathfrak{S}$ be such that

$$e_C(G,\, \mathcal{A}_N,\, D) = e_{\tilde{C}}(G,\, \mathcal{A}_{\tilde{N}},\, \tilde{D}). \quad (1.32)$$

Let $\rho \in \mathcal{R}_C(D)$, $\tilde{\rho} \in \mathcal{R}_{\tilde{C}}(\tilde{D})$ and χ and $\tilde{\chi}$ be the character afforded by ρ^G and $\tilde{\rho}^G$ respectively. By Theorem 1.10, $e_{\mathbb{F}_q}(\chi) = e_C(G,\, \mathcal{A}_N,\, D)$ and $e_{\mathbb{F}_q}(\tilde{\chi}) = e_{\tilde{C}}(G,\, \mathcal{A}_{\tilde{N}},\, \tilde{D})$. Therefore, equation (1.32) implies that $e_{\mathbb{F}_q}(\chi) = e_{\mathbb{F}_q}(\tilde{\chi})$, which, in turn, implies that

$$\tilde{\chi} = \sigma \circ \chi,\ \sigma \in \mathcal{G}(\chi). \quad (1.33)$$

Consequently, $\tilde{N} = \ker(\tilde{\chi}) = \ker(\chi) = N$. Also, by going modulo N, it follows from equation (1.33) and Theorem 1.15, that D/N and $\tilde{D}/N$ are conjugate in G/N.

This gives $D/N = \tilde{D}/N$, i.e., $D = \tilde{D}$. Next, if $\{z_1, z_2, \ldots, z_k\}$ is a transversal of $E_G(\mathcal{A}_N/D)$ in G, then, by Theorem 1.14(i) and equation (1.32), we have

$$\sum_{j=1}^{k} \varepsilon_{C^{(z_j)}}(\mathcal{A}_N, D^{(z_j)}) = \sum_{j=1}^{k} \varepsilon_{\tilde{C}^{(z_j)}}(\mathcal{A}_N, D^{(z_j)}). \tag{1.34}$$

Since both the sides of the above equation are primitive central idempotents in $\mathbb{F}_q[\mathcal{A}_N]$, it follows that, for some j, $1 \leq j \leq k$,

$$\varepsilon_C(\mathcal{A}_N, D) = \varepsilon_{\tilde{C}^{(z_j)}}(\mathcal{A}_N, D^{(z_j)}). \tag{1.35}$$

However, by Theorem 1.2, $\varepsilon_C(\mathcal{A}_N, D) = e_{\mathbb{F}_q}(\rho)$, and $\varepsilon_{\tilde{C}^{(z_j)}}(\mathcal{A}_N, \tilde{D}^{(z_j)}) = e_{\mathbb{F}_q}(\tilde{\rho}^{(z_j)})$. Therefore, we have by equation (1.35), $e_{\mathbb{F}_q}(\rho) = e_{\mathbb{F}_q}(\tilde{\rho}^{(z_j)})$, which, as before, gives $D = \ker \rho = \ker \tilde{\rho}^{(z_j)} = \tilde{D}^{(z_j)} = D^{(z_j)}$, i.e., $z_j \in N_G(D)$. Consequently, $\mathrm{Orb}(C) = \mathrm{Orb}(\tilde{C})$. This proves that π is 1-1. $\square$

We now illustrate Theorem 1.16 with its application to metacyclic groups; thus obtaining an alternative set of primitive central idempotents of $\mathbb{F}_q[G]$ with G given by presentation (1.3).

For a divisor v of n, let

- $o_v = \mathrm{ord}_v(r)$.
- $G_{o_v} = \langle a, b^{o_v} \rangle$.
- $\mathcal{B}_{o_v} = \{(w, i, c) \in \mathbb{Z}^3 \,|\, w > 0,\, w \,|\, n,\, w \,|\, r^{o_v} - 1,\, o_v c > 0\,, o_v c \,|\, t,\, w \,|\, k + i\frac{t}{o_v c}\}$.

Let

$$\mathfrak{N} = \{(v, i, c) \in \mathbb{Z}^3 \mid v > 0,\, v|n,\, c > 0,\, c|t,\, 0 \leq i \leq v-1,\, v|k+i\frac{t}{c},\, o_v \,|\, c \text{ and } v \,|\, i(r-1)\}.$$

For $(v, i, c) \in \mathfrak{N}$, define

- $H_{v,i,c} = \langle a^v, a^i b^c \rangle$.
- $X_{v,i,c} = \{(v, \alpha, \beta) \,|\, \beta o_v \mid c,\, \alpha\frac{c}{\beta o_v} \equiv i \pmod v,\, \beta = \frac{c\,\gcd(\alpha(r-1), v)}{v o_v},$ $\gcd(v, \alpha, \beta) = 1$ and $(v, \alpha, \beta) \in \mathcal{B}_{o_v}\}$.

Define a relation, denoted $\sim$, on $X_{v,i,c}$ as follows:

For $(v, \alpha_1, \beta_1), (v, \alpha_2, \beta_2) \in X_{v,i,c}$, we say that $(v, \alpha_1, \beta_1) \sim (v, \alpha_2, \beta_2) \Leftrightarrow \beta_1 = \beta_2$ and $\alpha_1 \equiv \alpha_2 r^j \pmod v$ for some j. It is easy to see that $\sim$ is an equivalence relation on $X_{v,i,c}$. Let $\mathfrak{X}_{v,i,c}$ denote the set of distinct equivalence classes of $X_{v,i,c}$ under the equivalence relation $\sim$.

Theorem 1.17 *Let $\mathbb{F}_q$ be a finite field with q elements and G the group given by the presentation (1.3). If* $\gcd(q,\, nt) = 1$, *then*

$$\bigcup_{(v,\,i,\,c)\in\mathfrak{N}} \{e_C(G,\, G_{o_v},\, H_{v,\,\alpha,\,\beta o_v}),\ \mid\ (v,\,\alpha,\,\beta)\in\mathfrak{X}_{v,\,i,\,c},\ C\in\mathcal{R}(G_{o_v}/H_{v,\,\alpha,\,\beta o_v})\}$$

is a complete set of primitive central idempotents of the group algebra $\mathbb{F}_q[G]$.

We prove it in a number of steps.

Lemma 1.18 *$H_{v,\,i,\,c},\ (v,\,i,\,c)\in\mathfrak{N}$, are all the distinct normal subgroups of G.*

Proof. Let $N \trianglelefteq G$. Suppose $N\cap\langle a\rangle = \langle a^v\rangle, v \mid n,\ v > 0$. Now, if $N/N\cap\langle a\rangle$, as a subgroup of $G/\langle a\rangle$, is generated by $\langle b^c\langle a\rangle\rangle,\ c > 0,\ c \mid t$, then clearly,

$$N = \langle a^v,\, a^ib^c\rangle \text{ for some } i,\ 0\le i\le v-1. \tag{1.36}$$

Now N being a normal subgroup of G, we must have $b^{-1}a^ib^cb,\ a^{-1}a^ib^ca$ and $(a^ib^c)^{t/c}$ all belong to N. This gives

$$v \mid i(r-1),\ o_v \mid c,\ v \mid k + i\frac{t}{c}. \tag{1.37}$$

Consequently, equations (1.36) and (1.37) yield that $(v,\, i,\, c)\in\mathfrak{N}$ and $N = H_{v,\,i,\,c}$.

Conversely, it is easy to see that for any $(v,\, i,\, c)\in\mathfrak{N}$, $H_{v,\,i,\,c}$ is normal subgroup of G. Furthermore,

$$|H_{v,\,i,\,c}| = \frac{nt}{vc}. \tag{1.38}$$

In order to complete the proof of the Lemma, we need to show that $H_{v,\,i,\,c},\ (v,\,i,\,c)\in\mathfrak{N}$, are distinct. Let $(v_1,\, i_1,\, c_1),\ (v_2,\, i_2,\, c_2)\in\mathfrak{N}$ be such that $H_{v_1,\,i_1,\,c_1} = H_{v_2,\,i_2,\,c_2}$. Then $\langle a^{v_1}\rangle = H_{v_1,\,i_1,\,c_1}\cap\langle a\rangle = H_{v_2,\,i_2,\,c_2}\cap\langle a\rangle = \langle a^{v_2}\rangle$ implies that $v_1 = v_2 = v$, say. Also, in view of equation (1.38), $|H_{v,\,i_1,\,c_1}/\langle a^v\rangle| = |H_{v,\,i_2,\,c_2}/\langle a^v\rangle|$ implies that $c_1 = c_2 = c$, say. Further, $a^{i_2}b^c\in H_{v,\,i_2,\,c}$, $a^{i_1}b^c\in H_{v,\,i_1,\,c}$ and $H_{v,\,i_1,\,c} = H_{v,\,i_2,\,c}$ gives that $a^{i_1-i_2}\in H_{v,\,i_1,\,c}\cap\langle a\rangle = \langle a^v\rangle$. Hence $i_2\equiv i_1 \pmod{v_1}$, i.e., $i_1 = i_2$. This proves the Lemma. □

Lemma 1.19 *Let $(v,\, i,\, c)\in\mathfrak{N}$ and $N = H_{v,\,i,\,c}$. Then*

(i) G_{o_v}/N is a maximal abelian subgroup of G/N containing $(G/N)'$.

(ii) H/N is a subgroup of G_{o_v}/N with cyclic quotient and H/N core-free in $G/N \Leftrightarrow H = H_{v,\,\alpha,\,\beta o_v},\ (v,\,\alpha,\,\beta)\in X_{v,\,i,\,c}$.

Proof. (i) By ([CR06], p.336), $G'_{o_v} = \langle a^{r^{o_v}-1}\rangle$. Since $v \,|\, r^{o_v} - 1$, we have $G'_{o_v} \leq \langle a^v\rangle \leq N$ and therefore G_{o_v}/N is abelian. Furthermore G_{o_v}/N contains $(G/N)'$ as $G' = \langle a^{r-1}\rangle \leq \langle a,\, b^{o_v}\rangle = G_{o_v}$. Thus G_{o_v}/N is an abelian subgroup of G/N containing $(G/N)'$.

If $o_v = 1$, then clearly, $G_{o_v}/N = G/N$ is a maximal abelian subgroup of G/N containing $(G/N)'$. Let $o_v > 1$. Suppose that K/N is an abelian subgroup of G/N with $G_{o_v}/N \leq K/N \leq G/N$. Since $o_v > 1$, G/N is not abelian. Thus $K/N \lneq G/N$. Now $K \cap \langle a\rangle = \langle a\rangle$ implies that $K = \langle a,\, b^j\rangle$ for some $j \,|\, o_v$. However, $K' \leq N$ implies that $\langle a^{r^j-1}\rangle \leq N$, which gives that $v \,|\, r^j - 1$, i.e., $o_v \,|\, j$. Thus $j = o_v$ and $K/N = G_{o_v}/N$. This proves (i).

(ii) Let H/N be a subgroup of G_{o_v}/N with cyclic quotient. By ([OdRS06], Lemma 2.2), we have

$$H = H_{u,\,\alpha,\,\beta o_v},\ (u,\,\alpha,\,\beta) \in \mathcal{B}_{o_v} \text{ and } \gcd(u,\,\alpha,\,\beta) = 1.$$

Since $N \leq H$, we must have $a^v \in H$ and $a^i b^c \in H$, which holds, if, and only if,

$$u \,|\, v,\ \beta o_v \,|\, c \text{ and } \alpha\frac{c}{\beta o_v} \equiv i \pmod{u}. \tag{1.39}$$

We claim that

$$\text{core}(H) = \langle a^u,\, a^{\alpha\frac{\delta}{\beta o_v}} b^\delta\rangle,\ \delta = \frac{\beta u o_v}{\gcd(\alpha(r-1),\, u)}.$$

Let $K = \langle a^u,\, a^{\alpha\frac{\delta}{\beta o_v}} b^\delta\rangle$ with δ as above. Since $(u,\, \alpha\frac{\delta}{\beta o_v},\, \delta) \in \mathfrak{N}$, by Lemma 1.18, it follows that K is a normal subgroup of G. Since $ab^{o_v}a^{-1}b^{-o_v} \in \langle a^v\rangle$, we have $a^{\alpha\frac{\delta}{\beta o_v}} b^\delta (a^\alpha b^{\beta o_v})^{-\frac{\delta}{\beta o_v}} \in \langle a^v\rangle$. Thus K is a subgroup of $H_{u,\,\alpha,\,\beta o_v} = H$.

In order to show that $\text{core}(H) = K$, we need to show that K is the largest normal subgroup of G contained in $H = H_{u,\,\alpha,\,\beta o_v}$. Let L be a normal subgroup of G contained in $H_{u,\,\alpha,\,\beta o_v}$. By Lemma 1.18, $L = H_{w,\,\gamma,\,f}$ for some $(w,\,\gamma,\,f) \in \mathfrak{N}$. Since $\langle a^w\rangle = L \cap \langle a\rangle \leq H_{u,\,\alpha,\,\beta o_v} \cap \langle a\rangle = \langle a^u\rangle$, it follows that $u \,|\, w$. Next observe that an arbitray element of $H_{u,\,\alpha,\,\beta o_v}$ is of the type $a^j b^s$ with $\beta o_v \,|\, s$ and $j \equiv \alpha\frac{s}{\beta o_v} \pmod{u}$. Therefore, $L = H_{w,\,\gamma,\,f}$ is a subgroup of $H_{u,\,\alpha,\,\beta o_v}$ if, and only if, $\beta o_v \,|\, f$ and $\gamma \equiv \alpha\frac{f}{\beta o_v} \pmod{u}$. Since $\gamma(r-1) \equiv 0 \pmod{w}$, we have $\alpha\frac{f}{\beta o_v}(r-1) \equiv 0 \pmod{\text{u}}$. This gives that $\delta \,|\, f$ and consequently $L = H_{w,\,\gamma,\,f}$ is contained in $K = \langle a^u,\, a^{\alpha\frac{\delta}{\beta o_v}} b^\delta\rangle$. This proves that K is the largest normal subgroup of G contained in $H_{u,\,\alpha,\,\beta o_v}$, which proves the claim.

It is now immediate from the claim that H/N is core-free in G/N if, and only if, $u = v$ and $\delta = c$. This proves (ii). $\square$

Lemma 1.20 *Let* $(v,\, i,\, c) \in \mathfrak{N}$ *and* $(v,\, \alpha_1,\, \beta_1)$, $(v,\, \alpha_2,\, \beta_2) \in X_{v,i,c}$. *Then* $H_{v,\,\alpha_1,\,\beta_1 o_v}$ *and* $H_{v,\,\alpha_2,\,\beta_2 o_v}$ *are conjugate in* G *if, and only if,* $\beta_1 = \beta_2$ *and* $\alpha_1 \equiv \alpha_2 r^j \pmod{v}$, *for some* j.

Proof. Suppose

$$H_{v,\,\alpha_1,\,\beta_1 o_v} = g^{-1} H_{v,\,\alpha_2,\,\beta_2 o_v} g, \quad g = a^i b^j \in G. \tag{1.40}$$

Then, in particular, in view of equation (1.38), we have

$$|H_{v,\,\alpha_1,\,\beta_1 o_v}| = \frac{nt}{v\beta_1 o_v} = \frac{nt}{v\beta_2 o_v} = |H_{v,\,\alpha_2,\,\beta_2 o_v}|,$$

i.e.,

$$\beta_1 = \beta_2.$$

Further equation (1.40) holds, if, and only if,

$$(a^i b^j)^{-1} a^{\alpha_2} b^{\beta_1 o_v} a^i b^j \in H_{v,\,\alpha_1,\,\beta_1 o_v}.$$

Since $ab^{o_v}a^{-1}b^{-o_v} \in \langle a^v \rangle$, we have $(a^i b^j)^{-1} a^{\alpha_2} b^{\beta_1 o_v} a^i b^j (a^{\alpha_2 r^j} b^{\beta_1 o_v})^{-1} \in \langle a^v \rangle \subseteq H_{v,\,\alpha_1,\,\beta_1 o_v}$, which yields that

$$\alpha_1 \equiv \alpha_2 r^j \pmod{v}$$

and proves the Lemma. □

Proof of Theorem 1.17. By Lemma 1.18, $H_{v,i,c}$, $(v,\, i,\, c) \in \mathfrak{N}$, are all the distinct normal subgroups of G. For $(v,\, i,\, c) \in \mathfrak{N}$, and $N = H_{v,i,c}$, Lemma 1.19 implies that

$$S_{G/N} = \{(H_{v,\,\alpha,\,\beta o_v}/N,\, G_{o_v}/N) \,|\, (v,\, \alpha,\, \beta) \in \mathfrak{X}_{v,i,c}\}.$$

Therefore, we have

$$\mathcal{S} = \bigcup_{(v,i,c)\in\mathfrak{N}} \{(H_{v,i,c},\, H_{v,\,\alpha,\,\beta o_v}/N,\, G_{o_v}/N) \,|\, (v,\, \alpha,\, \beta) \in \mathfrak{X}_{v,i,c}\}$$

and consequently, Theorem 1.16 yields the required result. □

Chapter 2

Wedderburn Decomposition and Automorphism Group

Let $\mathbb{F}_q$ be a finite field with q elements. In this Chapter, we compute the Wedderburn decomposition and the group of automorphisms of $\mathbb{F}_q[G]$, where G is a finite metabelian group of order coprime to q. We compute the explicit Wedderburn decomposition. The standard results on automorphisms of finite dimensional algebras yield the corresponding group of automorphisms and we omit the details.

We continue with the notation introduced in Chapter 1. We denote by $\mathrm{Aut}(\mathbb{F}_q[G])$, the group of $\mathbb{F}_q$-automorphisms of $\mathbb{F}_q[G]$. For $\chi \in \mathrm{Irr}(G)$, let $A(\chi) := \mathbb{F}_q[G]e_{\mathbb{F}_q}(\chi)$.

Groups of order p_1p_2

Theorem 2.1 [BGP11] *Let $G = \langle a, b \,|\, a^{p_1} = b^{p_2} = 1,\, b^{-1}ab = a^r\rangle$ be a group of order p_1p_2, where p_1 and p_2 are primes, $p_2 \,|\, p_1 - 1$, and r is an element of order p_2 in $\mathbb{Z}_{p_1}^*$. Suppose* $\gcd(q,\, p_1p_2) = 1$. *Then*

$$(i) \quad \mathbb{F}_q[G] \cong \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_{q^{f_2}}^{(e_2)} \oplus M_{p_2}(\mathbb{F}_{q^u})^{(e_1)}, & p_2 | f_1, \\ \mathbb{F}_q \oplus \mathbb{F}_{q^{f_2}}^{(e_2)} \oplus M_{p_2}(\mathbb{F}_{q^{f_1}})^{(\frac{e_1}{p_2})}, & p_2 \nmid f_1, \end{cases}$$

where $u = \frac{f_1}{p_2}$.

$$(ii)\quad \mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} (\mathbb{Z}_{f_2}^{(e_2)} \rtimes S_{e_2}) \oplus (H_1^{(e_1)} \rtimes S_{e_1}), & p_2 \mid f_1,\ f_2 \neq 1, \\ S_{e_2+1} \oplus (H_1^{(e_1)} \rtimes S_{e_1}), & p_2 \mid f_1,\ f_2 = 1, \\ (\mathbb{Z}_{f_2}^{(e_2)} \rtimes S_{e_2}) \oplus (H_2^{(\frac{e_1}{p_2})} \rtimes S_{e_1/p_2}), & p_2 \nmid f_1,\ f_2 \neq 1, \\ S_{e_2+1} \oplus (H_2^{(\frac{e_1}{p_2})} \rtimes S_{e_1/p_2}), & p_2 \nmid f_1,\ f_2 = 1, \end{cases}$$

where $H_1 = \mathrm{SL}_{p_2}(\mathbb{F}_{q^u}) \rtimes \mathbb{Z}_u,\ u = \frac{f_1}{p_2}$ *and* $H_2 = \mathrm{SL}_{p_2}(\mathbb{F}_{q^{f_1}}) \rtimes \mathbb{Z}_{f_1}$.

Proof. Let

$$\tilde{e} := \begin{cases} e_1, & p_2 \mid f_1, \\ \frac{e_1}{p_2}, & p_2 \nmid f_1. \end{cases} \tag{2.1}$$

By Theorem 1.8, $e_{\mathbb{F}_q}(\iota)$, $e_{\mathbb{F}_q}(\psi_m), e_{\mathbb{F}_q}(\phi_n)$, $0 \leq m \leq e_2 - 1$, $0 \leq n \leq \tilde{e} - 1$ constitute a complete set of distinct primitive central idempotents of $\mathbb{F}_q[G]$. Therefore,

$$\mathbb{F}_q[G] \cong A(\iota) \oplus A(\psi_0) \oplus \cdots \oplus A(\psi_{e_2-1}) \oplus A(\phi_0) \oplus \cdots \oplus A(\phi_{\tilde{e}-1}).$$

We have $e_{\mathbb{F}_q}(\iota) = \frac{1}{p_1 p_2} \sum_{g \in G} g$ and $A(\iota, \mathbb{F}_q) = \mathbb{F}_q[G] e_{\mathbb{F}_q}(\iota) \cong \mathbb{F}_q$.

For $0 \leq m \leq e_2 - 1$, ψ_m being a linear character, $A(\psi_m)$ is commutative and so $A(\psi_m)$ is equal to its centre. But, in view of ([Yam74], Proposition 1.4) , the centre of $A(\psi_m)$ is isomorphic to $\mathbb{F}_q(\psi_m) = \mathbb{F}_q(\zeta_2)$. Hence $A(\psi_m) \cong \mathbb{F}_q(\zeta_2)$ for $0 \leq m \leq e_2 - 1$.

For $0 \leq i \leq \tilde{e} - 1$, by Wedderburn structure theorem, $A(\phi_i) \cong M_{n_i}(D_i)$, where D_i is a finite field containing $\mathbb{F}_q$, and $n_i \geq 1$. By ([Yam74], Proposition 1.4), the centre of $A(\phi_i)$ is isomorphic to $\mathbb{F}_q(\phi_i)$, therefore, we have $D_i \cong \mathbb{F}_q(\phi_i)$. However, for $1 \leq i \leq n$, $\mathbb{F}_q(\phi_i) = K$, where K is as defined in equation (1.8). Observe that $A(\phi_i)$, $0 \leq i \leq \tilde{e} - 1$, are all isomorphic as $\mathbb{F}_q$-vector spaces. Therefore, it follows that $n_0 = n_1 = \cdots = n_{\tilde{e}} = \tilde{n}$, say. Consequently, $A(\phi_i) \cong M_{\tilde{n}}(K)$ for $0 \leq i \leq \tilde{e} - 1$ and

$$\mathbb{F}_q[G] \cong \mathbb{F}_q \oplus \mathbb{F}_q(\zeta_2)^{(e_2)} \oplus M_{\tilde{n}}(K)^{(\tilde{e})}. \tag{2.2}$$

Furthermore,

$$Z(\mathbb{F}_q[G]) \cong \mathbb{F}_q \oplus \mathbb{F}_q(\zeta_2)^{(e_2)} \oplus K^{(\tilde{e})}, \tag{2.3}$$

where $Z(\mathbb{F}_q[G])$ is the centre of $\mathbb{F}_q[G]$.

Observe that $[\mathbb{F}_q(\zeta_2) : \mathbb{F}_q] = \mathrm{ord}_{p_2}(q) = f_2$, thus on comparing the dimension over $\mathbb{F}_q$ on both sides of (2.3), we obtain that

$$p_2 + \frac{p_1 - 1}{p_2} = 1 + e_2 f_2 + \tilde{e}[K : \mathbb{F}_q],$$

which gives that

$$[K : \mathbb{F}_q] = \begin{cases} \frac{f_1}{p_2}, & p_2 \mid f_1 \\ f_1, & p_2 \nmid f_1. \end{cases} \tag{2.4}$$

and now comparing the dimension over $\mathbb{F}_q$ on both sides of (2.2), we obtain that

$$p_1 p_2 = 1 + e_2 f_2 + \tilde{n}^2 \tilde{e}[K : \mathbb{F}_q],$$

which gives that $\tilde{n} = p_2$. Thus (i) is proved.

(ii) follows from (i) and the standard results on automorphisms of finite dimensional algebras [Lam01]. □

Metacyclic groups

The following Theorem follows from Theorems 1.9(ii) and 1.14(iii). However, we give a simpler proof, in this case, using the ideas contained in ([OdRS04], Theorem 2.1).

Theorem 2.2 [BGP] *Let n, t, r, k be natural numbers with $r^t \equiv 1 (mod\, n)$, $kr \equiv k (mod\, n)$ and let G be a metacyclic group given by presentation*

$$G = \langle a, b \mid a^n = 1,\, b^t = a^k,\, b^{-1}ab = a^r \rangle.$$

Suppose that $\gcd(q,\, nt) = 1$. *Then*

$$\mathbb{F}_q[G] \cong \bigoplus_{d \mid n} \bigoplus_{l \mid \frac{n}{d} s_d} M_{l_d}(\mathbb{K}_{d,\,l})^{(n_{d,\,l})},$$

where $\mathbb{K}_{d,\,l}$ is the field extension of $\mathbb{F}_q$ of degree $\frac{\ell_{d,\,l} k_{d,\,l}}{l_d}$ and $n_{d,\,l} = |[X_{d,\,l}]|$.

Proof. By Wedderburn theorem,

$$\mathbb{F}_q[G] e_{\mathbb{F}_q}(\chi_{i,\,j}) \cong M_\kappa(\mathbb{K}), \tag{2.5}$$

where $\mathbb{K}$ is a finite field containing $\mathbb{F}_q$. Comparing the centre of the algebras on both sides of (2.5), it follows that $\mathbb{K}$ is isomorphic to the centre of $\mathbb{F}_q[G] e_{\mathbb{F}_q}(\chi_{i,\,j})$. However, by ([Yam74], Proposition 1.4), the centre of $\mathbb{F}_q[G] e_{\mathbb{F}_q}(\chi_{i,\,j})$ is isomorphic to $\mathbb{F}_q(\chi_{i,\,j})$. Therefore

$$[\mathbb{K} : \mathbb{F}_q] = [\mathbb{F}_q(\chi_{i,\,j}) : \mathbb{F}_q].$$

By equations (1.14), (1.17) and Lemma 1.12(ii), we have

$$[\mathbb{F}_q(\chi_{i,\,j}) : \mathbb{F}_q] = \frac{[\mathbb{F}_q(\psi_{i,\,j}) : \mathbb{F}_q]}{[\mathrm{Cen}_G(e_{\mathbb{F}_q}(\psi_{i,\,j})) : \langle a,\, b^{l_d} \rangle]} = \frac{\ell_{d,\,l} k_{d,\,l}}{l_d}$$

and hence,

$$[\mathbb{K} : \mathbb{F}_q] = \frac{\ell_{d,l} k_{d,l}}{l_d} \quad \text{and} \quad \mathbb{K} \cong \mathbb{K}_{d,l}.$$

Since by equation (1.17), the dimension of $\mathbb{F}_q[\langle a, b^{l_d}\rangle]e_{\mathbb{F}_q}(\psi_{ir^\gamma, j_\gamma})$ over $\mathbb{F}_q$, $\dim_{\mathbb{F}_q}(\mathbb{F}_q[\langle a, b^{l_d}\rangle]e_{\mathbb{F}_q}(\psi_{ir^\gamma, j_\gamma}))$, equals $\ell_{d,l}$, it follows from equation (1.23) that $\dim_{\mathbb{F}_q}(\mathbb{F}_q[G]e_{\mathbb{F}_q}(\chi_{i,j})) = k_{d,l} l_d \ell_{d,l}$. Therefore, comparing the dimension of the algebras over $\mathbb{F}_q$ on both sides of (2.5), we obtain that

$$k_{d,l} l_d \ell_{d,l} = \kappa^2 \dim_{\mathbb{F}_q} \mathbb{K} = \frac{\kappa^2 \ell_{d,l} k_{d,l}}{l_d},$$

which gives $\kappa = l_d$ and the Theorem is thus proved. □

Metabelian groups

Let G be a metabelian group of order coprime to q and let ξ be a primitive $|G|$-th root of unity in $\overline{\mathbb{F}}_q$. We use the notation introduced in Section 1.5 of Chapter 1. Let $(N,\, D/N,\, \mathcal{A}_N/N) \in \mathcal{S}$. Then $\mathcal{A}_N/D$ is a cyclic group generated by aD, say. Let $x_1, x_2, \ldots, x_t$ be a transversal of $\mathcal{A}_N$ in G, and r_i, $1 \le i \le t$, be integers such that $x_i^{-1} a x_i D = a^{r_i} D$. Let $\zeta = \xi^{|G|/[\mathcal{A}_N : D]}$, and $\mathcal{K}(N,\, D/N,\, \mathcal{A}_N/N)$ be the subfield of $\overline{\mathbb{F}}_q$ obtained by adjoining the t elements $\sum_{i=1}^{t} \zeta^{j r_i}$, $1 \le j \le t-1$ to $\mathbb{F}_q$. It is easily seen that the field $\mathcal{K}(N,\, D/N,\, \mathcal{A}_N/N)$ is independent of the choice of transversal of $\mathcal{A}_N$ in G.

For $d | [G : G']$ and $l | [\mathbb{F}_q(\xi) : \mathbb{F}_q]$, let $\mathcal{S}_{d,l}$ be the set of those $(N,\, D/N,\, \mathcal{A}_N/N) \in \mathcal{S}$ such that

(*i*) $[G : \mathcal{A}_N] = d$,

(*ii*) $[\mathcal{K}(N,\, D/N,\, \mathcal{A}_N/N) : \mathbb{F}_q] = l$.

Clearly $\mathcal{S}_{d,l}$, $d | [G : G']$, $l | [\mathbb{F}_q(\xi) : \mathbb{F}_q]$, are disjoint and $\mathcal{S} = \bigcup_{\substack{d \,|\, [G:G'] \\ l \,|\, [\mathbb{F}_q(\xi):\mathbb{F}_q]}} \mathcal{S}_{d,l}$.

Theorem 2.3 *With the above notation,*

(*i*) $\mathbb{F}_q[G] \cong \bigoplus_{\substack{d | [G:G'] \\ l | [\mathbb{F}_q(\xi):\mathbb{F}_q]}} M_d(\mathbb{F}_{q^l})^{(\alpha_{d,l})}$,

(*ii*) $\mathrm{Aut}(\mathbb{F}_q[G]) \cong \bigoplus_{\substack{d \,|\, [G:G'] \\ l \,|\, [\mathbb{F}_q(\xi):\mathbb{F}_q]}} K_{d,l}^{(\alpha_{d,l})} \rtimes S_{\alpha_{d,l}}$,

where $K_{d,l} = \mathrm{SL}_d(\mathbb{F}_{q^l}) \rtimes \mathbb{Z}_l$ *and* $\alpha_{d,l} = \sum_{(N,\, D/N,\, \mathcal{A}_N/N) \in S_{d,l}} |R(\mathcal{A}_N/D)|$.

Proof. (i) It follows from Theorems 1.14(iii) and 1.16 that for $((N,\ D/N,\ \mathcal{A}_N/N), C) \in \mathfrak{S}$, where $\mathfrak{S}$ is as defined in equation (1.30),

$$\mathbb{F}_q[G]e_C(G,\ \mathcal{A}_N,\ D) \cong M_{[G:\mathcal{A}_N]}(\mathbb{F}_{q^{o(\mathcal{A}_N,\ D)}})$$

Thus we have,

$$\begin{aligned}
\mathbb{F}_q[G] &\cong \bigoplus_{((N,\ D/N,\ \mathcal{A}_N/N),\ C)\in\mathfrak{S}} \mathbb{F}_q[G]e_C(G,\ \mathcal{A}_N,\ D) \\
&\cong \bigoplus_{(N,\ D/N,\ \mathcal{A}_N/N)\in\mathcal{S}} \ \bigoplus_{C\in R(\mathcal{A}_N/D)} \mathbb{F}_q[G]e_C(G,\ \mathcal{A}_N,\ D) \\
&\cong \bigoplus_{(N,\ D/N,\ \mathcal{A}_N/N)\in\mathcal{S}} \ \bigoplus_{C\in R(\mathcal{A}_N/D)} M_{[G:\mathcal{A}_N]}(\mathbb{F}_{q^{o(\mathcal{A}_N,\ D)}}) \\
&\cong \bigoplus_{\substack{d\mid[G:G'] \\ l\mid[\mathbb{F}_q(\xi):\mathbb{F}_q]}} \ \bigoplus_{(N,\ D/N,\ \mathcal{A}_N/N)\in\mathcal{S}_{d,\ l}} \ \bigoplus_{C\in R(\mathcal{A}_N/D)} M_{[G:\mathcal{A}_N]}(\mathbb{F}_{q^{o(\mathcal{A}_N,\ D)}}) \\
&\cong \bigoplus_{\substack{d\mid[G:G'] \\ l\mid[\mathbb{F}_q(\xi):\mathbb{F}_q]}} \ \bigoplus_{(N,\ D/N,\ \mathcal{A}_N/N)\in\mathcal{S}_{d,\ l}} M_{[G:\mathcal{A}_N]}(\mathbb{F}_{q^{o(\mathcal{A}_N,\ D)}})^{(|R(\mathcal{A}_N/D)|)}
\end{aligned}$$

For $d \mid [G:G'],\ l \mid [\mathbb{F}_q(\xi):\mathbb{F}_q]$, and $(N,\ D/N,\ \mathcal{A}_N/N) \in \mathcal{S}_{d,l}$, we show that

$$o(\mathcal{A}_N,\ D) = [\mathcal{K}(N,\ D/N,\ \mathcal{A}_N/N) : \mathbb{F}_q] = l. \tag{2.6}$$

If $\rho \in \mathcal{R}_C(D)$ and χ is the character afforded by ρ^G, then, by Theorem 1.14(i) and equation (1.14),

$$[E_G(\mathcal{A}_N/D) : \mathcal{A}_N] = [\mathbb{F}_q(\zeta) : \mathbb{F}_q(\chi)].$$

However, note that

$$\mathbb{F}_q(\chi) = \mathcal{K}(N,\ D/N,\ \mathcal{A}_N/N).$$

Therefore, we have,

$$[\mathcal{K}(N,\ D/N,\ \mathcal{A}_N/N) : \mathbb{F}_q] = [\mathbb{F}_q(\zeta) : \mathbb{F}_q]/[E_G(\mathcal{A}_N/D) : \mathcal{A}_N] = o(\mathcal{A}_N,\ D).$$

This proves (2.6) and we thus have

$$\begin{aligned}
\mathbb{F}_q[G] &\cong \bigoplus_{\substack{d\mid[G:G'] \\ l\mid[\mathbb{F}_q(\xi):\mathbb{F}_q]}} \ \bigoplus_{(N,\ D/N,\ \mathcal{A}_N/N)\in\mathcal{S}_{d,\ l}} M_d(\mathbb{F}_{q^l})^{(|R(\mathcal{A}_N/D)|)} \\
&\cong \bigoplus_{\substack{d\mid[G:G'] \\ l\mid[\mathbb{F}_q(\xi):\mathbb{F}_q]}} M_d(\mathbb{F}_{q^l})^{(\alpha_{d,\ l})},
\end{aligned}$$

where $\alpha_{d,\,l} = \sum_{(N,\,D/N,\,\mathcal{A}_N/N)\in\mathcal{S}_{d,\,l}} |R(\mathcal{A}_N/D)|$. This proves (i).

(ii) It follows immediately from (i). $\square$

Chapter 3

Misc. Examples

In this Chapter, we give several examples of the computation of primitive central idempotents, Wedderburn decomposition and the group of automorphisms of semisimple finite group algebras.

We continue with the notation used in Chapters 1 and 2.

3.1 $G := \langle a, b \,|\, a^{2^m} = b^2 = 1,\ b^{-1}ab = a^{2^{m-1}-1} \rangle,\ m \geq 2.$

Let λ be the highest power of 2 dividing $q-1$ (resp. $q+1$) if $q \equiv 1 \pmod 4$ (resp. $q \equiv -1 \pmod 4$). Observe that for any integer $\alpha \geq 2$, $\mathrm{ord}_{2^\alpha}(q)$, the order of q modulo 2^α, is given by

$$\mathrm{ord}_{2^\alpha}(q) = \begin{cases} 2^{\alpha-\lambda}, & \alpha \geq \lambda+1,\ q \equiv 1 \text{ or } -1 \,(\mathrm{mod}\, 4), \\ 1, & 2 \leq \alpha \leq \lambda,\ q \equiv 1 \pmod 4, \\ 2, & 2 \leq \alpha \leq \lambda,\ q \equiv -1 \pmod 4. \end{cases}$$

Let $T = \{\beta \in \mathbb{Z} \,|\, 0 \leq \beta \leq m-2,\ q^u \equiv 2^{m-1}-1 \pmod{2^{m-\beta}} \text{ for some integer } u \geq 1\}$. For $0 \leq \beta \leq m-2$, let $T_\beta \subseteq \mathbb{Z}^*_{2^{m-\beta}}$ be such that T_β (resp. $T_\beta \cup (2^{m-1}-1)T_\beta$) is a left transversal of $\langle q \rangle$ in $\mathbb{Z}^*_{2^{m-\beta}}$ according as $\beta \in T$ (resp. $\beta \notin T$).

By Theorems 1.9, 2.2 and 2.3, we have the following:

Primitive central idempotents

Case I : $q \equiv 1 \pmod 4$

$\underline{m \geq \lambda + 1 \ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1});$
$e_{\mathbb{F}_q}(\chi_{2^{m-1},0}), e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ s \in T_\beta,\ (|T_\beta| = 2^{\min(m-\beta,\,\lambda)-2}), 0 \leq \beta \leq m-2.$

$\underline{3 \leq m \leq \lambda \ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ s \in T_\beta,\ (|T_\beta| = 2^{m-\beta-2}),\ 0 \leq \beta \leq m-2.$

$\underline{m = 2 \ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{1,0}),\ e_{\mathbb{F}_q}(\chi_{3,0}),\ e_{\mathbb{F}_q}(\chi_{1,1}),\ e_{\mathbb{F}_q}(\chi_{3,1}).$

Case II : $q \equiv -1 \pmod 4$

$\underline{m = \lambda + 1 \ ;}$
$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ s \in T_\beta,\ (|T_\beta| = 2^{m-\beta-2}),\ 0 \leq \beta \leq m-2.$

$\underline{m > \lambda + 1 \ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ s \in T_\beta, (|T_\beta| = 2^{\min(m-\beta,\,\lambda)-2}),\ 0 \leq \beta \leq m-2.$

$\underline{3 \leq m \leq \lambda;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{s,0}),\ s \in T_0, (|T_0| = 2^{m-3});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ s \in T_\beta, (|T_\beta| = 2^{m-\beta-2}),\ 1 \leq \beta \leq m-2.$

$\underline{m = 2 \ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2,0}),\ e_{\mathbb{F}_q}(\chi_{2,1}),\ e_{\mathbb{F}_q}(\chi_{1,0}),\ e_{\mathbb{F}_q}(\chi_{1,1}).$

Wedderburn decomposition

Case I : $q \equiv 1 \pmod 4$

$\underline{m \geq \lambda + 1 \ ;}$

$$\mathbb{F}_q^{(4)} \bigoplus_{\beta=0}^{m-\lambda-1} M_2(\mathbb{F}_{q^{2^{m-\beta-\lambda}}})^{(2^{\lambda-2})} \bigoplus M_2(\mathbb{F}_q)^{(2^{\lambda-1}-1)}.$$

$\underline{3 \leq m \leq \lambda \ ;}$

$$\mathbb{F}_q^{(4)} \bigoplus M_2(\mathbb{F}_q)^{(2^{m-1}-1)}.$$

$\underline{m = 2 \ ;}$

$$\mathbb{F}_q^{(8)}.$$

Case II : $q \equiv -1 \pmod 4$

$\underline{m = \lambda + 1 \ ;}$

$$\mathbb{F}_q^{(4)} \bigoplus M_2(\mathbb{F}_q)^{(2^{m-1}-1)}.$$

$\underline{m > \lambda + 1 \ ;}$

$$\mathbb{F}_q{}^{(4)} \bigoplus_{\beta=0}^{m-\lambda-1} M_2(\mathbb{F}_{q^{2^{m-\beta-\lambda}}})^{(2^{\lambda-2})} \bigoplus M_2(\mathbb{F}_q)^{(2^{\lambda-1}-1)}.$$

$\underline{3 \leq m \leq \lambda;}$

$$\mathbb{F}_q^{(4)} \bigoplus M_2(\mathbb{F}_{q^2})^{(2^{m-3})} \bigoplus M_2(\mathbb{F}_q)^{(2^{m-2}-1)}.$$

$\underline{m = 2;}$

$$\mathbb{F}_q{}^{(4)} \bigoplus \mathbb{F}_{q^2}^{(2)}.$$

Automorphism group

Case I : $q \equiv 1 \pmod 4$

$\underline{m \geq \lambda + 1\ ;}$

$$S_4 \bigoplus_{\beta=0}^{m-\lambda-1} (H_\beta{}^{(2^{\lambda-2})} \rtimes S_{2^{\lambda-2}}) \bigoplus (SL_2(\mathbb{F}_q)^{(2^{\lambda-1}-1)} \rtimes S_{2^{\lambda-1}-1}),$$

where $H_\beta = SL_2(\mathbb{F}_{q^{2^{m-\beta-\lambda}}}) \rtimes \mathbb{Z}_{2^{m-\beta-\lambda}}$.

$\underline{3 \leq m \leq \lambda\ ;}$

$$S_4 \bigoplus (SL_2(\mathbb{F}_q)^{(2^{m-1}-1)} \rtimes S_{2^{m-1}-1}).$$

$\underline{m = 2\ ;}$

$$S_8.$$

Case II : $q \equiv -1 \pmod 4$

$\underline{m = \lambda + 1\ ;}$

$$S_4 \bigoplus (SL_2(\mathbb{F}_q)^{(2^{m-1}-1)} \rtimes S_{2^{m-1}-1}).$$

$\underline{m > \lambda + 1\ ;}$

$$S_4 \bigoplus_{\beta=0}^{m-\lambda-1} (H_\beta{}^{(2^{\lambda-2})} \rtimes S_{2^{\lambda-2}}) \bigoplus (SL_2(\mathbb{F}_q)^{(2^{\lambda-1}-1)} \rtimes S_{2^{\lambda-1}-1}),$$

where $H_\beta = SL_2(\mathbb{F}_{q^{2^{m-\beta-\lambda}}}) \rtimes \mathbb{Z}_{2^{m-\beta-\lambda}}$.

$\underline{3 \leq m \leq \lambda;}$

$$S_4 \bigoplus \Big((SL_2(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2)^{(2^{m-3})} \rtimes S_{2^{m-3}} \Big) \bigoplus (SL_2(\mathbb{F}_q)^{(2^{m-2}-1)} \rtimes S_{2^{m-2}-1}).$$

$\underline{m = 2;}$

$$S_4 \bigoplus (\mathbb{Z}_2{}^{(2)} \rtimes S_2).$$

3.2 $G := \langle a, b \,|\, a^{2^m} = b^2 = 1,\ b^{-1}ab = a^{2^{m-1}+1} \rangle,\ m \geq 2.$

Let $U = \{\beta \in \mathbb{Z} \,|\, 0 \leq \beta \leq m-2, q^u \equiv 2^{m-1}+1 \pmod{2^{m-\beta}} \text{ for some integer } u \geq 1\}$. For $0 \leq \beta \leq m-2$, let $U_\beta \subseteq \mathbb{Z}^*_{2^{m-\beta}}$ be such that U_β (resp. $U_\beta \cup (2^{m-1}+1)U_\beta$) is a left transversal of $\langle q \rangle$ in $\mathbb{Z}^*_{2^{m-\beta}}$ according as $\beta \in U$ (resp. $\beta \notin U$). Let λ be as in Example 3.1.

By Theorems 1.9, 2.2 and 2.3, we have the following:

Primitive central idempotents

Case I : $q \equiv 1 \pmod 4$

$\underline{m \geq \lambda + 1\ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{s,0}),\ s \in U_0,\ (|U_0| = 2^{\lambda-1});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ e_{\mathbb{F}_q}(\chi_{2^\beta s,1}),\ s \in U_\beta,\ (|U_\beta| = 2^{\min(m-\beta,\,\lambda)-1}),\ 1 \leq \beta \leq m-2.$

$\underline{2 \leq m \leq \lambda\ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{s,0}),\ s \in U_0,\ (|U_0| = 2^{m-2});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ e_{\mathbb{F}_q}(\chi_{2^\beta s,1}),\ s \in U_\beta,\ (|U_\beta| = 2^{m-\beta-1}),\ 1 \leq \beta \leq m-2.$

Case II : $q \equiv -1 \pmod 4$

$\underline{m > \lambda + 1\ ;}$
$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{s,0}),\ s \in U_0,\ (|U_0| = 2^{\lambda-1});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ e_{\mathbb{F}_q}(\chi_{2^\beta s,1}), s \in U_\beta,\ (|U_\beta| = 2^{\min(m-\beta,\,\lambda)-1}),\ 1 \leq \beta \leq m-2.$

$\underline{3 \leq m \leq \lambda + 1\ ;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},0}),\ e_{\mathbb{F}_q}(\chi_{2^{m-1},1});$
$e_{\mathbb{F}_q}(\chi_{s,0}),\ s \in U_0, (|U_0| = 2^{m-3});$
$e_{\mathbb{F}_q}(\chi_{2^\beta s,0}),\ e_{\mathbb{F}_q}(\chi_{2^\beta s,1}),\ s \in U_\beta, (|U_\beta| = 2^{m-\beta-2}),\ 1 \leq \beta \leq m-2.$

$\underline{m = 2;}$

$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{2,0}),\ e_{\mathbb{F}_q}(\chi_{2,1}),\ e_{\mathbb{F}_q}(\chi_{1,0}).$

Wedderburn decomposition

Case I : $q \equiv 1 \pmod 4$

$\underline{m = \lambda + 1\ ;}$

$$\mathbb{F}_q{}^{(2^m)} \bigoplus M_2(\mathbb{F}_q)^{(2^{m-2})}.$$

$\underline{m > \lambda + 1\ ;}$

$$\mathbb{F}_q{}^{(2^{\lambda+1})} \bigoplus_{\beta=1}^{m-\lambda-1} \mathbb{F}_{q^{2^{m-\beta-\lambda}}}^{(2^\lambda)} \bigoplus M_2(\mathbb{F}_{q^{2^{m-\lambda-1}}})^{(2^{\lambda-1})}.$$

$\underline{2 \leq m \leq \lambda;}$

$$\mathbb{F}_q^{(2^m)} \bigoplus M_2(\mathbb{F}_q)^{(2^{m-2})}.$$

Case II : $q \equiv -1 \pmod 4$

$\underline{m > \lambda + 1\ ;}$

$$\mathbb{F}_q{}^{(4)} \bigoplus_{\beta=1}^{m-\lambda-1} \mathbb{F}_{q^{2^{m-\beta-\lambda}}}^{(2^\lambda)} \bigoplus \mathbb{F}_{q^2}^{(2^\lambda-2)} \bigoplus M_2(\mathbb{F}_{q^{2^{m-\lambda-1}}})^{(2^{\lambda-1})}.$$

$\underline{3 \leq m \leq \lambda + 1 \ ;}$

$$\mathbb{F}_q^{(4)} \bigoplus \mathbb{F}_{q^2}^{(2^{m-1}-2)} \bigoplus M_2(\mathbb{F}_{q^2})^{(2^{m-3})}.$$

$\underline{m = 2;}$

$$\mathbb{F}_q^{(4)} \bigoplus M_2(\mathbb{F}_q).$$

Automorphism group

Case I : $q \equiv 1 \pmod 4$

$\underline{m = \lambda + 1 \ ;}$

$$S_{2^m} \bigoplus (SL_2(\mathbb{F}_q)^{(2^{m-2})} \rtimes S_{2^{m-2}}).$$

$\underline{m > \lambda + 1 \ ;}$

$$S_{2^{\lambda+1}} \bigoplus_{\beta=1}^{m-\lambda-1} (\mathbb{Z}_{2^{m-\beta-\lambda}}{}^{(2^\lambda)} \rtimes S_{2^\lambda}) \bigoplus (H^{(2^{\lambda-1})} \rtimes S_{2^{\lambda-1}}),$$

where $H = SL_2(\mathbb{F}_{q^{2^{m-\lambda-1}}}) \rtimes \mathbb{Z}_{2^{m-\lambda-1}}$.

$\underline{2 \leq m \leq \lambda;}$

$$S_{2^m} \bigoplus (SL_2(\mathbb{F}_q)^{(2^{m-2})} \rtimes S_{2^{m-2}}).$$

Case II : $q \equiv -1 \pmod 4$

$\underline{m > \lambda + 1 \ ;}$

$$S_4 \bigoplus (\mathbb{Z}_2{}^{(2^{\lambda+1}-2)} \rtimes S_{2^{\lambda+1}-2}) \bigoplus_{\beta=1}^{m-\lambda-2} (H_\beta{}^{(2^\lambda)} \rtimes S_{2^\lambda}) \bigoplus (H^{(2^{\lambda-1})} \rtimes S_{2^{\lambda-1}}),$$

where $H_\beta = \mathbb{Z}_{2^{m-\beta-\lambda}}$ and $H = SL_2(\mathbb{F}_{q^{2^{m-\lambda-1}}}) \rtimes \mathbb{Z}_{2^{m-\lambda-1}}$.

$\underline{3 \leq m \leq \lambda + 1 \ ;}$

$$S_4 \bigoplus (\mathbb{Z}_2{}^{(2^{m-1}-2)} \rtimes S_{2^{m-1}-2}) \bigoplus (H^{(2^{m-3})} \rtimes S_{2^{m-3}}),$$

where $H = SL_2(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2$.

$\underline{m = 2;}$

$$S_4 \bigoplus SL_2(\mathbb{F}_q).$$

3.3 $G = D_{2n}$, the dihedral group of order $2n$.

We determine the structure of $\mathbb{F}_q[G]$, when $G := \langle a, b \,|\, a^n = b^2 = 1,\ b^{-1}ab = a^{-1} \rangle$ is dihedral group of order $2n$. Suppose that $\gcd(q, 2n) = 1$. Let

$$S = \{d \,|\, d|n,\ q^u \equiv -1 \pmod{\frac{n}{d}} \text{ for some integer } u \geq 1\}.$$

For a divisor d of n, $d \geq 1$, let $f_d = \mathrm{ord}_{n/d}(q)$ and $T_d \subseteq \mathbb{Z}^*_{n/d}$ be such that T_d (resp. $\pm T_d$) is a left transversal of $\langle q \rangle$ in $\mathbb{Z}^*_{n/d}$ if $d \in S$ (resp. $d \notin S$). Note that

$$|T_d| = \begin{cases} \frac{\varphi(\frac{n}{d})}{f_d}, & d \in S, \\ \\ \frac{\varphi(\frac{n}{d})}{2f_d}, & d \notin S. \end{cases}$$

Given $l \,|\, \mathrm{ord}_n(q)$, let S_l be the set of those divisors d of n such that

(i) $d \neq n, \frac{n}{2}$,

(ii) $f_d = \begin{cases} l, & d \notin S, \\ 2l, & d \in S. \end{cases}$

Thus Theorems 1.9, 2.2 and 2.3 yield the following:

Primitive central idempotents

$\underline{n \text{ odd};}$

$$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{dk,0}),\ d|n,\ d \neq n,\ k \in T_d.$$

n even ;

$e_{\mathbb{F}_q}(\chi_{0,0})$, $e_{\mathbb{F}_q}(\chi_{0,1})$, $e_{\mathbb{F}_q}(\chi_{\frac{n}{2},0})$, $e_{\mathbb{F}_q}(\chi_{\frac{n}{2},1})$, $e_{\mathbb{F}_q}(\chi_{dk,0})$, $d|n$, $d \neq n$, $n/2$, $k \in T_d$.

Wedderburn decomposition

n odd;

$$\mathbb{F}_q^{(2)} \bigoplus_{d \notin S} M_2(\mathbb{F}_{q^{f_d}})^{(\frac{\varphi(\frac{n}{d})}{2f_d})} \bigoplus_{d \in S,\, d \neq n} M_2(\mathbb{F}_{q^{f_d/2}})^{(\frac{\varphi(\frac{n}{d})}{f_d})}.$$

n even;

$$\mathbb{F}_q^{(4)} \bigoplus_{d \notin S} M_2(\mathbb{F}_{q^{f_d}})^{(\frac{\varphi(\frac{n}{d})}{2f_d})} \bigoplus_{d \in S,\, d \neq n, \frac{n}{2}} M_2(\mathbb{F}_{q^{f_d/2}})^{(\frac{\varphi(\frac{n}{d})}{f_d})}.$$

Automorphism group

n odd;

$$S_2 \bigoplus_{l | \mathrm{ord}_n(q)} \left((SL_2(\mathbb{F}_{q^l}) \rtimes \mathbb{Z}_l)^{(\alpha_{d,\,l})} \rtimes S_{\alpha_{d,\,l}} \right)$$

n even;

$$S_4 \bigoplus_{l | \mathrm{ord}_n(q)} \left((SL_2(\mathbb{F}_{q^l}) \rtimes \mathbb{Z}_l)^{(\alpha_{d,\,l})} \rtimes S_{\alpha_{d,\,l}} \right),$$

where $\alpha_{d,\,l} = \sum_{d \in S_l} \frac{\varphi(\frac{n}{d})}{2l}$.

3.4 $G = Q_{4n}$, the quaternion group of order $4n$.

We determine the structure of $\mathbb{F}_q[G]$, when $G := \langle a, b \,|\, a^{2n} = 1,\ b^2 = a^n,\ b^{-1}ab = a^{-1}\rangle$ is the quaternion group of order $4n$. Suppose that $\gcd(q, 4n) = 1$. Let

$$V = \{d \,|\, d|2n,\ q^u \equiv -1 \pmod{\frac{2n}{d}} \text{ for some integer } u \geq 1\}.$$

For a divisor d of $2n$, $d \geq 1$, let $o_d = \mathrm{ord}_{2n}(q)$ and $V_d \subseteq \mathbb{Z}^*_{2n/d}$ be such that V_d (resp. $\pm V_d$) is a left transversal of $\langle q \rangle$ in $\mathbb{Z}^*_{2n/d}$ according as $d \in V$ (resp. $d \notin V$). Note that

$$|V_d| = \begin{cases} \frac{\varphi(\frac{2n}{d})}{o_d}, & d \in V, \\ \\ \frac{\varphi(\frac{2n}{d})}{2o_d}, & d \notin V. \end{cases}$$

Given $l \,|\, \mathrm{ord}_{2n}(q)$, let U_l be the set of those divisors d of n such that

(i) $d \neq n, 2n$,

(ii) $o_d = \begin{cases} l, & d \notin V, \\ 2l, & d \in V. \end{cases}$

Theorems 1.9, 2.2 and 2.3 yield the following:

Primitive central idempotents

Case I : $q \equiv 1 \pmod 4$**)**

$$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{n,0}),\ e_{\mathbb{F}_q}(\chi_{n,1}),\ e_{\mathbb{F}_q}(\chi_{dk,0}),\ d \,|\, 2n,\ d \neq n,\ 2n,\ k \in V_d.$$

Case II : $q \equiv -1 \pmod 4$**)**

n odd;

$$e_{\mathbb{F}_q}(\chi_{0,0}),\ e_{\mathbb{F}_q}(\chi_{0,1}),\ e_{\mathbb{F}_q}(\chi_{n,0}),\ e_{\mathbb{F}_q}(\chi_{dk,0}),\ d|2n,\ d \neq n,\ 2n,\ k \in V_d.$$

n even;

$e_{\mathbb{F}_q}(\chi_{0,0})$, $e_{\mathbb{F}_q}(\chi_{0,1})$, $e_{\mathbb{F}_q}(\chi_{n,0})$, $e_{\mathbb{F}_q}(\chi_{n,1})$, $e_{\mathbb{F}_q}(\chi_{dk,0})$, $d \mid 2n$, $d \neq n,\, 2n$, $k \in V_d$.

Wedderburn decomposition

Case I : $q \equiv 1 \pmod 4$

$$\mathbb{F}_q^{(4)} \bigoplus_{d \notin V} M_2(\mathbb{F}_{q^{o_d}})^{(\frac{\varphi(\frac{2n}{d})}{2o_d})} \bigoplus_{\substack{d \in V, \\ d \neq n,\, 2n}} M_2(\mathbb{F}_{q^{o_d/2}})^{(\frac{\varphi(\frac{2n}{d})}{o_d})}.$$

Case II : $q \equiv -1 \pmod 4$

n odd;

$$\mathbb{F}_q^{(2)} \bigoplus \mathbb{F}_{q^2} \bigoplus_{d \notin V} M_2(\mathbb{F}_{q^{o_d}})^{(\frac{\varphi(\frac{2n}{d})}{2o_d})} \bigoplus_{\substack{d \in V, \\ d \neq n,\, 2n}} M_2(\mathbb{F}_{q^{o_d/2}})^{(\frac{\varphi(\frac{2n}{d})}{o_d})}$$

n even;

$$\mathbb{F}_q^{(4)} \bigoplus_{d \notin V} M_2(\mathbb{F}_{q^{o_d}})^{(\frac{\varphi(\frac{2n}{d})}{2o_d})} \bigoplus_{\substack{d \in V, \\ d \neq n,\, 2n}} M_2(\mathbb{F}_{q^{o_d/2}})^{(\frac{\varphi(\frac{2n}{d})}{o_d})}.$$

Automorphism group

Case I : $q \equiv 1 \pmod 4$

$$S_4 \bigoplus_{l \mid \mathrm{ord}_{2n}(q)} \left((SL_2(\mathbb{F}_{q^l}) \rtimes \mathbb{Z}_l)^{(\beta_{d,\,l})} \rtimes S_{\beta_{d,\,l}} \right)$$

Case II : $q \equiv -1 \pmod 4$

n odd;

$$S_2 \bigoplus \mathbb{Z}_2 \bigoplus_{l|\mathrm{ord}_{2n}(q)} \left((SL_2(\mathbb{F}_{q^l}) \rtimes \mathbb{Z}_l)^{(\beta_{d,\,l})} \rtimes S_{\beta_{d,\,l}} \right),$$

n even;

$$S_4 \bigoplus_{l|\mathrm{ord}_{2n}(q)} \left((SL_2(\mathbb{F}_{q^l}) \rtimes \mathbb{Z}_l)^{(\beta_{d,\,l})} \rtimes S_{\beta_{d,\,l}} \right),$$

where $\beta_{d,\,l} = \sum_{d \in U_l} \frac{\varphi(\frac{2n}{d})}{2l}$.

3.5 $G := \langle a,\, b,\, x \,|\, a^p = b^p = a^{-1}b^{-1}ab = x^2 = 1, x^{-1}ax = a^{-1},\, x^{-1}bx = b^{-1} \rangle$, p odd prime

Observe that the normal subgroups of G are $G = \langle a,\, b,\, x \rangle$, $G' = \langle a,\, b \rangle$, $N_i = \langle a^i b \rangle$, $0 \le i \le p-1$, $N_p = \langle a \rangle$ and $\langle 1 \rangle$. It is easy to see that

$$S_{G/G} = \{(\langle 1 \rangle,\, \langle 1 \rangle)\},\ S_{G/G'} = \{(\langle 1 \rangle,\, G/G')\}$$

and

$$S_{G/N_i} = \{(\langle 1 \rangle,\, G'/N_i)\},\ 0 \le i \le p.$$

This gives

$$\mathcal{S} = \{(G, \langle 1 \rangle,\, \langle 1 \rangle)\} \cup \{(G', \langle 1 \rangle,\, G/G')\} \cup \{(N_i, \langle 1 \rangle,\, G'/N_i),\ 0 \le i \le p\}.$$

Observe that, $R(G/G)$ and $R(G/G')$ has precisely one q-cyclotomic coset, call it C and C', say. For $0 \le i \le p$, $R(G'/N_i)$ has $\frac{p-1}{f}$ q-cyclotomic cosets, if $-1 \in \langle q \rangle \pmod p$; and $\frac{p-1}{2f}$ q-cyclotomic cosets, if $-1 \notin \langle q \rangle \pmod p$, where f is the order of q modulo p. Direct calculations yield that for each $(N, D/N, A_N/N) \in \mathcal{S}$, the corresponding $o(\mathcal{A}_N,\, D)$ and $|R(\mathcal{A}_N/D)|$ are as follows:

$(N,\, D/N,\, \mathcal{A}_N/N)$	$o(\mathcal{A}_N,\, D)$	$\lvert R(\mathcal{A}_N/D)\rvert$
$(G, \langle 1 \rangle, \langle 1 \rangle)$	1	1
$(G', \langle 1 \rangle, G/G')$	1	1
$(N_i,\, \langle 1 \rangle,\, G'/N_i), 0 \le i \le p$	$\begin{cases} f/2, & -1 \in \langle q \rangle \pmod p, \\ f, & -1 \notin \langle q \rangle \pmod p. \end{cases}$	$\begin{cases} \frac{p-1}{f}, & -1 \in \langle q \rangle \pmod p, \\ \frac{p-1}{2f}, & -1 \notin \langle q \rangle \pmod p. \end{cases}$

Thus Theorems 1.16 and 2.3 yield the following:

Primitive central idempotents

$$e_C(G,G,G),\ C \in \mathcal{R}(G/G);$$
$$e_{C'}(G,G,G'),\ C' \in \mathcal{R}(G/G');$$
$$e_{C_i}(G,G',N_i),\ C_i \in \mathcal{R}(G'/N_i), 0 \le i \le p.$$

Wedderburn decomposition

$$\mathbb{F}_q[G] \cong \begin{cases} \mathbb{F}_q^{(2)} \bigoplus M_2(\mathbb{F}_{q^{f/2}})^{(\frac{p^2-1}{f})}, & -1 \in \langle q \rangle \pmod p, \\ \\ \mathbb{F}_q^{(2)} \bigoplus M_2(\mathbb{F}_{q^f})^{(\frac{p^2-1}{2f})}, & -1 \notin \langle q \rangle \pmod p. \end{cases}$$

Automorphism group

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong S_2 \bigoplus \left(H^{(\kappa)} \rtimes S_\kappa\right),$$

where $H = \mathrm{SL}_2(\mathbb{F}_{q^\alpha}) \rtimes \mathbb{Z}_\alpha$,

$$\alpha = \begin{cases} f/2, & -1 \in \langle q \rangle \pmod p, \\ f, & -1 \notin \langle q \rangle \pmod p. \end{cases}$$

and

$$\kappa = \begin{cases} \frac{p^2-1}{f}, & -1 \in \langle q \rangle \pmod p, \\ \frac{p^2-1}{2f}, & -1 \notin \langle q \rangle \pmod p. \end{cases}.$$

3.6 Groups G of the type $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The groups G of the type $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, where $Z(G)$ denotes the centre of group G, arose in the work of Goodaire [Goo83] while studying Moufang loops and then subsequently appeared in the work of several authors [GPMS09, JRM05, JRM06, LSS09]. It is known ([GJPM96], Chapter 5) that any group with $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is the direct product of an indecomposable group (with this property) and an abelian group. Moreover the finite indecomposable groups with $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ break into five classes as follows:

Group	Generators	Relations
D_1	x, y, t	$x^2, y^2, t^{2^m}, y^{-1}x^{-1}yxt^{2^{m-1}}, t$ central , $m \geq 1$
D_2	x, y, t	$x^2t^{-1}, y^2t^{-1}, t^{2^m}, y^{-1}x^{-1}yxt^{2^{m-1}}, t$ central , $m \geq 1$
D_3	x, y, t_1, t_2	$x^2, y^2t_2^{-1}, t_1^{2^{m_1}}, t_2^{2^{m_2}}, y^{-1}x^{-1}yxt_1^{2^{m_1-1}}, t_1, t_2$ central , $m_1, m_2 \geq 1$
D_4	x, y, t_1, t_2	$x^2t_1^{-1}, y^2t_2^{-1}, t_1^{2^{m_1}}, t_2^{2^{m_2}}, y^{-1}x^{-1}yxt_1^{2^{m_1-1}}, t_1, t_2$ central , $m_1, m_2 \geq 1$
D_5	x, y, t_1, t_2, t_3	$x^2t_2^{-1}, y^2t_3^{-1}, t_1^{2^{m_1}}, t_2^{2^{m_2}}, t_3^{2^{m_3}}, y^{-1}x^{-1}yxt_1^{2^{m_1-1}}, t_1, t_2, t_3$ central , $m_1, m_2, m_3 \geq 1$

It thus becomes important to investigate the group algebra $\mathbb{F}_q[D_i]$, $1 \leq i \leq 5$.

3.6.1 Groups G of type D_1.

Observe that for $m = 1$, G is isomorphic to D_8, the dihedral group of order 8, and the structure of group algebra $\mathbb{F}_q[D_8]$ can be read from Example 3.3.

Let $m \geq 2$, Define
$N_0 := \{e\}$, $N_1 := \langle t, x\rangle$, $N_2 := \langle t, y\rangle$, $N_3 := \langle t, xy\rangle$, $N_4^{(\alpha)} := \langle t^{2^\alpha}, x, y\rangle$,
$N_5^{(\beta)} := \langle t^{2^{m-1}}, x, yt^{2^\beta}\rangle$, $N_6^{(\beta)} := \langle t^{2^{m-1}}, xt^{2^\beta}, y\rangle$, $N_7^{(\beta)} := \langle t^{2^\beta}x, t^{2^\beta}y\rangle$,
$0 \leq \alpha \leq m-1$, $0 \leq \beta \leq m-2$.

Let λ be the highest power of 2 dividing $q-1$ (resp. $q+1$) according as $q \equiv 1 \pmod 4$ (resp. $q \equiv -1 \pmod 4$).

Ferraz, Goodaire and Milies ([FGPM10], Theorem 3.1) proved that the Wedderburn decomposition of $\mathbb{F}_q[G]$, G of type D_1, contains at least $8m-10$ simple components. If $q \equiv 3 \pmod 8$, then this number is acheived with $8m-12$ fields and 2 quaternion algebras, each necessarily a ring of 2×2 matrices. We improve this result of Ferraz et.al. by providing a concrete description of $\mathbb{F}_q[G]$, G of type D_1, in the following Theorem:

Theorem 3.1 *A complete set of primitive central idempotents, Wedderburn decomposition and the automorphism group of $\mathbb{F}_q[G]$, G of type D_1, $m \geq 2$, is given by :*

(i)

Primitive central idempotents

$e_C(G,\, N_1,\, \langle x\rangle)$, $C \in R(N_1/\langle x\rangle)$;
$e_C(G,\, G,\, N_i)$, $C \in R(G/N_i)$, $1 \le i \le 3$;
$e_C(G,\, G,\, N_4^{(\alpha)})$, $C \in R(G/N_4^{(\alpha)})$, $0 \le \alpha \le m-1$;
$e_C(G,\, G,\, N_j^{(\beta)})$, $C \in R(G/N_j^{(\beta)})$, $0 \le \beta \le m-2$, $5 \le j \le 7$.

(ii)

Wedderburn decomposition

$\underline{q \equiv 1 \pmod 4}$

$$\mathbb{F}_q[G] \cong \begin{cases} {\mathbb{F}_q}^{(2^{m+1})} \bigoplus {M_2(\mathbb{F}_q)}^{(2^{m-1})}, & m \le \lambda, \\ {\mathbb{F}_q}^{(2^{m+1})} \bigoplus {M_2(\mathbb{F}_{q^2})}^{(2^{m-2})}, & m = \lambda+1, \\ {\mathbb{F}_q}^{(2^{\lambda+2})} \bigoplus_{\alpha=\lambda+1}^{m-1} {\mathbb{F}_{q^{2^{\alpha-\lambda}}}}^{(2^{\lambda+1})} \bigoplus {M_2(\mathbb{F}_{q^{2^{m-\lambda}}})}^{(2^{\lambda-1})}, & m \ge \lambda+2. \end{cases}$$

$\underline{q \equiv -1 \pmod 4}$

$$\mathbb{F}_q[G] \cong \begin{cases} {\mathbb{F}_q}^{(8)} \bigoplus {\mathbb{F}_{q^2}}^{(2^m-4)} \bigoplus {M_2(\mathbb{F}_{q^2})}^{(2^{m-2})}, & 2 \le m \le \lambda+1, \\ {\mathbb{F}_q}^{(8)} \bigoplus {\mathbb{F}_{q^2}}^{(2^m-4)} \bigoplus {M_2(\mathbb{F}_{q^4})}^{(2^{m-3})}, & m = \lambda+2, \\ {\mathbb{F}_q}^{(8)} \bigoplus {\mathbb{F}_{q^2}}^{(2^{\lambda+2}-4)} \bigoplus_{\alpha=\lambda+2}^{m-1} {\mathbb{F}_{q^{2^{\alpha-\lambda}}}}^{(2^{\lambda+1})} \bigoplus {M_2(\mathbb{F}_{q^{2^{m-\lambda}}})}^{(2^{\lambda-1})}, & m \ge \lambda+3. \end{cases}$$

(iii)

Automorphism group

$\underline{q \equiv 1 \pmod 4}$

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} S_{2^{m+1}} \bigoplus (\mathrm{SL}_2(\mathbb{F}_q)^{(2^{m-1})} \rtimes S_{2^{m-1}}), & m \le \lambda, \\ S_{2^{m+1}} \bigoplus \left((\mathrm{SL}_2(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2)^{(2^{m-2})} \rtimes S_{2^{m-2}} \right), & m = \lambda+1, \\ S_{2^{\lambda+2}} \bigoplus_{\alpha=\lambda+1}^{m-1} (\mathbb{Z}_{2^{\alpha-\lambda}}{}^{(2^{\lambda+1})} \rtimes S_{2^{\lambda+1}}) \bigoplus \mathcal{H}_\lambda, & m \ge \lambda+2, \end{cases}$$

$\underline{q \equiv -1 \pmod 4}$

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} S_8 \bigoplus (\mathbb{Z}_2{}^{(2^m-4)} \rtimes S_{2^m-4}) \bigoplus ((\mathrm{SL}_2(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2)^{(2^{m-2})} \rtimes S_{2^{m-2}}), & m \le \lambda+1, \\ S_8 \bigoplus (\mathbb{Z}_2{}^{(2^m-4)} \rtimes S_{2^m-4}) \bigoplus ((\mathrm{SL}_2(\mathbb{F}_{q^4}) \rtimes \mathbb{Z}_4)^{(2^{m-3})} \rtimes S_{2^{m-3}}), & m = \lambda+2, \\ S_8 \bigoplus (\mathbb{Z}_2{}^{(2^{\lambda+2}-4)} \rtimes S_{2^{\lambda+2}-4}) \bigoplus_{\alpha=\lambda+2}^{m-1} (\mathbb{Z}_{2^{\alpha-\lambda}}{}^{(2^{\lambda+1})} \rtimes S_{2^{\lambda+1}}) \bigoplus \mathcal{H}_\lambda, & m \ge \lambda+3, \end{cases}$$

where $\mathcal{H}_\lambda = (\mathrm{SL}_2(\mathbb{F}_{q^{2^{m-\lambda}}}) \rtimes \mathbb{Z}_{2^{m-\lambda}})^{(2^{\lambda-1})} \rtimes S_{2^{\lambda-1}}$.

In order to prove the above Theorem, we first need to compute all the normal subgroups of $G,\ G$ of type D_1.

Lemma 3.2 *All the distinct non-identity normal subgroups of G are given by:*

(i) $\langle t^{2^\alpha}, x\rangle$, $\langle t^{2^\alpha}, y\rangle$, $\langle t^{2^\alpha}, xy\rangle$, $\langle t^{2^\alpha}, x, y\rangle$;
(ii) $\langle t^{2^\beta}x\rangle$, $\langle t^{2^\beta}y\rangle$, $\langle t^{2^{m-1}}, t^{2^\beta}xy\rangle$, $\langle t^{2^{m-1}}, x, t^{2^\beta}y\rangle$, $\langle t^{2^{m-1}}, t^{2^\beta}x, y\rangle$, $\langle t^{2^\beta}x, t^{2^\beta}y\rangle$;
(iii) $\langle t^{2^\gamma}\rangle$,

where $0 \leq \alpha \leq m-1,\ 0 \leq \beta \leq m-2$ *and* $0 \leq \gamma \leq m-1$.

Proof. Observe that all the subgroups listed in the statement are distinct and normal in G.

Let N be a normal subgroup of G not contained in $\langle t\rangle$. If $N \neq \langle 1\rangle$, then it is easy to see that $\langle t^{2^{m-1}}\rangle \leq N$. Therefore $N \cap \langle t\rangle = \langle t^{2^v}\rangle$, $0 \leq v \leq m-1$. Since $N/N \cap \langle t\rangle$ is isomorphic to subgroup of $G/\langle t\rangle$, which is generated by $x\langle t\rangle$, $y\langle t\rangle$, it follows that $N/N \cap \langle t\rangle$ is isomorphic to one of the following: $\langle x\langle t\rangle\rangle$, $\langle y\langle t\rangle\rangle$, $\langle xy\langle t\rangle\rangle$ or $\langle x\langle t\rangle, y\langle t\rangle\rangle$.

Case I : $N/\langle t^{2^v}\rangle \cong \langle x\langle t\rangle\rangle$

In this case, $N = \langle t^{2^v}, t^{2^i}x\rangle$, for some i, $0 \leq i \leq v \leq m-1$.

If $i = v$, then $N = \langle t^{2^v}, x\rangle$. Since $N \trianglelefteq G$, $xt^{2^{m-1}} = y^{-1}xy \in N$, implies that $t^{2^{m-1}} \in N \cap \langle t\rangle = \langle t^{2^v}\rangle$, which is possible only if $v \leq m-1$.

If $i < v$, then $N = \langle t^{2^v}, t^{2^i}x\rangle = \langle t^{2^i}x\rangle$ as $t^{2^v} \in \langle t^{2^i}x\rangle$. Further $xt^{2^i+2^{m-1}} = y^{-1}t^{2^i}xy \in N$ implies that $t^{2^{m-1}} \in \langle t^{2^v}\rangle$. Hence $v \leq m-1$ and $i \leq m-2$. Thus in this case, either

$$N = \langle t^{2^i}, x\rangle,\ 0 \leq i \leq m-1 \tag{3.1}$$

or

$$N = \langle t^{2^i}x\rangle,\ 0 \leq i \leq m-2. \tag{3.2}$$

Case II: $N/\langle t^{2^v}\rangle \cong \langle y\langle t\rangle\rangle$.

Computation analogous to those in Case I yield that

$$N = \langle t^{2^i}y\rangle, 0 \leq i \leq m-2 \tag{3.3}$$

or

$$N = \langle t^{2^i}, y\rangle,\ 0 \leq i \leq m-1. \tag{3.4}$$

Case III: $N/\langle t^{2^v}\rangle \cong \langle xy\langle t\rangle\rangle$.

In this case $N = \langle t^{2^v},\, t^{2^i}xy\rangle$ for $0 \le i \le v \le m-1$.

If $i = v$, then $N = \langle t^{2^v},\, xy\rangle$. Since N is a normal subgroup of G, $xyt^{2^{m-1}} = y^{-1}xyy \in N$, implies that $t^{2^{m-1}} \in N \cap \langle t\rangle = \langle t^{2^v}\rangle$, which is possible only if $v \le m-1$.

If $i < v$, then $N = \langle t^{2^v},\, t^{2^i}xy\rangle$, $0 \le i \le m-2$. Since $\langle t^{2^{m-1}},\, t^{2^i}xy\rangle \le \langle t^{2^v},\, t^{2^i}xy\rangle$ and

$$t^{2^v} = \begin{cases} (t^{2^i}xy)^{2^{v-i}}t^{2^{m-1}}, & \text{if } v-i = 1, \\ (t^{2^i}xy)^{2^{v-i}}, & \text{if } v-i \ge 2, \end{cases}$$

it follows that $\langle t^{2^v},\, t^{2^i}xy\rangle = \langle t^{2^{m-1}},\, t^{2^i}xy\rangle$.

Thus in this case, either

$$N = \langle t^{2^i},\, xy\rangle,\ 0 \le i \le m-1 \tag{3.5}$$

or

$$N = \langle t^{2^{m-1}},\, t^{2^i}xy\rangle,\ 0 \le i \le m-2. \tag{3.6}$$

Case IV: $N/\langle t^{2^v}\rangle \cong \langle x\langle t\rangle,\, \langle y\langle t\rangle\rangle$.

In this case, N is one of the following forms:

(a) $\langle t^{2^v},\, x,\, y\rangle$;
(b) $\langle t^{2^v},\, t^{2^i}x,\, y\rangle$ for some i, $0 \le i \le v-1$;
(c) $\langle t^{2^v},\, x,\, t^{2^i}y\rangle$ for some i, $0 \le i \le v-1$;
(d) $\langle t^{2^v},\, t^{2^i}x,\, t^{2^i}y\rangle$ for some i, $0 \le i \le v-1$;
(e) $\langle t^{2^v},\, t^{2^i}x,\, t^{2^j}y\rangle$ for some $1 \le i, j \le v-1$, $i \ne j$.

Observe that for $0 \le i \le v-1$,

$$\langle t^{2^v},\, t^{2^i}x,\, y\rangle = \langle t^{2^{m-1}},\, t^{2^i}x,\, y\rangle,$$

$$\langle t^{2^v},\, x,\, t^{2^i}y\rangle = \langle t^{2^{m-1}},\, x,\, t^{2^i}y\rangle,$$

and

$$\langle t^{2^v},\, t^{2^i}x,\, t^{2^i}y\rangle = \langle t^{2^{m-1}},\, t^{2^i}x,\, t^{2^i}y\rangle.$$

Also for $1 \le i, j \le v-1$, $i \ne j$,

$$\langle t^{2^v},\, t^{2^i}x,\, t^{2^j}y\rangle = \begin{cases} \langle t^{2^i}x,\, y\rangle, & \text{if } i < j, \\ \langle x,\, t^{2^j}y\rangle, & \text{if } j < i. \end{cases}$$

Thus we have proved that any normal subgroup of G not contained in $\langle t\rangle$ is one of the forms given in (i) and (ii) of the statement. This proves the Lemma. $\square$

In order to apply Theorem 1.16 to a group G of type D_1, we compute $S_{G/N}$ for all normal subgroups N of G.

Clearly if $N = \langle 1\rangle$, $S_{G/N} = \{(\langle x\rangle, \langle t, x\rangle)\}$.

Suppose N is a non-identity normal subgroup of G, then N is one of the subgroups listed in Lemma 3.2. Since $G' = \langle t^{2^{m-1}}\rangle \leq N$, we have $\mathcal{A}_N/N = G/N$ and the corresponding

$$S_{G/N} = \begin{cases} \{(\langle 1\rangle, G/N)\}, & \text{if } G/N \text{ is cyclic,} \\ \emptyset, & \text{otherwise.} \end{cases}$$

Next we see that among all the normal subgroups N of G stated in Lemma 3.2, only the following subgroups N satisfy the condition that G/N is cyclic;

$$N_i,\ N_4^{(\alpha)},\ N_j^{(\beta)},\ 1 \leq i \leq 3,\ 0 \leq \alpha \leq m-1,\ 5 \leq j \leq 7,\ 0 \leq \beta \leq m-2.$$

Therefore $\mathcal{S} = \{(N_0, \langle x\rangle, N_1)\} \cup \{(N_i, \langle 1\rangle, G/N_i) \mid 1 \leq i \leq 3\} \cup \{(N_4^{(\alpha)}, \langle 1\rangle, G/N_4^{(\alpha)}) \mid 0 \leq \alpha \leq m-1\} \cup \{(N_j^{(\beta)}, \langle 1\rangle, G/N_j^{(\beta)}) \mid 0 \leq \beta \leq m-2\}$. This proves (i).

In order to prove (ii) and (iii), we first note that for any integer $\gamma \geq 2$,

$$\mathrm{ord}_{2^\gamma}(q) = \begin{cases} 2^{\gamma-\lambda}, & \gamma \geq \lambda+1,\ q \equiv 1 \text{ or } -1 (\mathrm{mod}\, 4), \\ 1, & \gamma \leq \lambda\ , q \equiv 1 (\mathrm{mod}\, 4), \\ 2, & \gamma \leq \lambda,\ q \equiv -1 (\mathrm{mod}\, 4). \end{cases}$$

Direct calculations yield that for each $(N, D/N, A_N/N) \in \mathcal{S}$, the corresponding $o(\mathcal{A}_N, D)$ and $|R(\mathcal{A}_N/D)|$ are as given by the following tables:

Case I : $q \equiv 1 \pmod 4$**.**

$(N,\, D/N,\, \mathcal{A}_N/N)$	$o(\mathcal{A}_N,\, D)$	$\lvert R(\mathcal{A}_N/D)\rvert$
$(N_i,\, \langle 1\rangle,\, G/N_i)$, $1 \le i \le 3$	1	1
$(N_4^{(0)},\, \langle 1\rangle,\, G/N_4^{(0)})$,	1	1
$(N_4^{(\alpha)},\, \langle 1\rangle,\, G/N_4^{(\alpha)})$, $1 \le \alpha \le m-1$	$\begin{cases} 2^{\alpha-\lambda}, & \alpha \ge \lambda+1, \\ 1, & \alpha \le \lambda \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \alpha \ge \lambda+1, \\ 2^{\alpha-1}, & \alpha \le \lambda \end{cases}$
$(N_j^{(\beta)},\, \langle 1\rangle,\, G/N_j^{(\beta)})$, $5 \le j \le 7,\, 0 \le \beta \le m-2$	$\begin{cases} 2^{\beta+1-\lambda}, & \beta \ge \lambda, \\ 1, & \beta \le \lambda-1 \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \beta \ge \lambda, \\ 2^{\beta}, & \beta \le \lambda-1 \end{cases}$
$(N_0,\, \langle x\rangle,\, N_1)$	$\begin{cases} 2^{m-\lambda}, & m \ge \lambda+1, \\ 1, & m \le \lambda \end{cases}$	$\begin{cases} 2^{\lambda-1}, & m \ge \lambda+1, \\ 2^{m-1}, & m \le \lambda \end{cases}$

Case II : $q \equiv -1 \pmod 4$.

$(N,\, D/N,\, \mathcal{A}_N/N)$	$o(\mathcal{A}_N,\, D)$	$\lvert R(\mathcal{A}_N/D)\rvert$
$(N_i,\, \langle 1\rangle,\, G/N_i)$, $1 \le i \le 3$	1	1
$(N_4^{(\alpha)},\, \langle 1\rangle,\, G/N_4^{(\alpha)})$, $0 \le \alpha \le 1$	1	1
$(N_4^{(\alpha)},\, \langle 1\rangle,\, G/N_4^{(\alpha)})$, $2 \le \alpha \le m-1$	$\begin{cases} 2^{\alpha-\lambda}, & \alpha \ge \lambda+2, \\ 2, & \alpha \le \lambda+1 \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \alpha \ge \lambda+2, \\ 2^{\alpha-2}, & \alpha \le \lambda+1 \end{cases}$
$(N_j^{(0)},\, \langle 1\rangle,\, G/N_j^{(0)})$, $5 \le j \le 7$,	1	1
$(N_j^{(\beta)},\, \langle 1\rangle,\, G/N_j^{(\beta)})$, $5 \le j \le 7,\, 1 \le \beta \le m-2$	$\begin{cases} 2^{\beta+1-\lambda}, & \beta \ge \lambda+1, \\ 2, & \beta \le \lambda \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \beta \ge \lambda+1, \\ 2^{\beta-1}, & \beta \le \lambda \end{cases}$
$(N_0,\, \langle x\rangle,\, N_1)$	$\begin{cases} 2^{m-\lambda}, & m \ge \lambda+1, \\ 2, & m \le \lambda \end{cases}$	$\begin{cases} 2^{\lambda-1}, & m \ge \lambda+2, \\ 2^{m-2}, & m \le \lambda+1 \end{cases}$

Thus, Theorem 2.3 with the help of above two tables yield (ii) and (iii).

3.6.2 Groups G of type D_2.

Observe that for $m = 1$, D_2 is isomorphic to Q_8, the quaternion group of order 8 and the structure of group algebra $\mathbb{F}_q[Q_8]$ can be read from Example 3.4.

Let $m \geq 2$. Define
$K_0 := \{e\}$, $K_1 := \langle x \rangle$;
${K_2}^{(\alpha)} := \langle x^{2^\alpha}, x^{2^\alpha - 1}y \rangle$, ${K_3}^{(\beta)} := \langle x^{2^\beta}, x^{2^{\beta-1}-1}y \rangle$,
$0 \leq \alpha \leq m$, $1 \leq \beta \leq m$.

Let λ be the highest power of 2 dividing $q-1$ (resp. $q+1$) according as $q \equiv 1 \pmod 4$ (resp. $q \equiv -1 \pmod 4$).

Ferraz, Goodaire and Milies proved ([FGPM10], Theorem 3.2) that the Wedderburn decomposition of $\mathbb{F}_q[G]$, G of type D_2, contains at least $4m$ simple components. If $q \equiv 3 \pmod 8$, then this number is acheived with $4m-2$ fields and 2 quaternion algebras, each necessarily a ring of 2×2 matrices. The following Theorem improves this result of Ferraz et.al.

Theorem 3.3 *A complete set of primitive central idempotents, Wedderburn decomposition and the automorphism group of $\mathbb{F}_q[G]$, G of type D_2, $m \geq 2$, is given by :*

(i)

Primitive central idempotents

$e_C(G, K_1, K_0)$, $C \in R(K_1/K_0)$;
$e_C(G, G, K_1)$, $C \in R(G/K_1)$;
$e_C(G, G, K_2^{(\alpha)})$, $C \in R(G/{K_2}^{(\alpha)})$, $0 \leq \alpha \leq m$;
$e_C(G, G, K_3^{(\beta)})$, $C \in R(G/K_3^{(\beta)})$, $1 \leq \beta \leq m$.

(ii)

Wedderburn decomposition

$\underline{q \equiv 1 \pmod 4}$

$$\mathbb{F}_q[G] \cong \begin{cases} {\mathbb{F}_q}^{(2^{m+1})} \bigoplus {M_2(\mathbb{F}_q)}^{(2^{m-1})}, & m \leq \lambda, \\ {\mathbb{F}_q}^{(2^{\lambda+1})} \bigoplus_{\alpha=\lambda+1}^{m} {\mathbb{F}_{q^{2^{\alpha-\lambda}}}}^{(2^\lambda)} \bigoplus {M_2(\mathbb{F}_{q^{2^{m-\lambda}}})}^{(2^{\lambda-1})}, & m \geq \lambda+1. \end{cases}$$

$\underline{q \equiv -1 \pmod 4}$

$$\mathbb{F}_q[G] \cong \begin{cases} {\mathbb{F}_q}^{(4)} \bigoplus {\mathbb{F}_{q^2}}^{(2^m-2)} \bigoplus {M_2(\mathbb{F}_{q^2})}^{(2^{m-2})}, & 2 \leq m \leq \lambda+1, \\ {\mathbb{F}_q}^{(4)} \bigoplus {\mathbb{F}_{q^2}}^{(2^{\lambda+1}-2)} \bigoplus_{\alpha=\lambda+2}^{m} {\mathbb{F}_{q^{2^{\alpha-\lambda}}}}^{(2^\lambda)} \bigoplus {M_2(\mathbb{F}_{q^{2^{m-\lambda}}})}^{(2^{\lambda-1})}, & m \geq \lambda+2. \end{cases}$$

(iii)

Automorphism group

$\underline{q \equiv 1 \pmod 4}$

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} S_{2^{m+1}} \bigoplus (\mathrm{SL}_2(\mathbb{F}_q)^{(2^{m-1})} \rtimes S_{2^{m-1}}), & m \leq \lambda, \\ S_{2^{\lambda+1}} \bigoplus_{\alpha=\lambda+1}^{m} (\mathbb{Z}_{2^{\alpha-\lambda}}{}^{(2^{\lambda})} \rtimes S_{2^{\lambda}}) \bigoplus \mathcal{H}_{\lambda}, & m \geq \lambda+1, \end{cases}$$

$\underline{q \equiv -1 \pmod 4}$

$$\mathrm{Aut}(\mathbb{F}_q[G]) \cong \begin{cases} S_4 \bigoplus (\mathbb{Z}_2{}^{(2^m-2)} \rtimes S_{2^m-2}) \bigoplus ((\mathrm{SL}_2(\mathbb{F}_{q^2}) \rtimes \mathbb{Z}_2)^{(2^{m-2})} \rtimes S_{2^{m-2}}), & m \leq \lambda+1, \\ S_4 \bigoplus (\mathbb{Z}_2{}^{(2^{\lambda+1}-2)} \rtimes S_{2^{\lambda+1}-2}) \bigoplus_{\alpha=\lambda+2}^{m} (\mathbb{Z}_{2^{\alpha-\lambda}}{}^{(2^{\lambda})} \rtimes S_{2^{\lambda}}) \bigoplus \mathcal{H}_{\lambda}, & m \geq \lambda+2, \end{cases}$$

where $\mathcal{H}_{\lambda} = (\mathrm{SL}_2(\mathbb{F}_{q^{2^{m-\lambda}}}) \rtimes \mathbb{Z}_{2^{m-\lambda}})^{(2^{\lambda-1})} \rtimes S_{2^{\lambda-1}}$.

Proof. We have

$$G = \langle x, y \mid x^{2^{m+1}} = 1, y^2 = x^2, y^{-1}xy = x^{2^m+1} \rangle.$$

By Lemma 1.18, the non-identity normal subgroups of G are given by

(i) $\langle x^{2^\alpha} \rangle$, $\langle x^{2^\alpha}, x^{2^\alpha-1}y \rangle$, $0 \leq \alpha \leq m$,
(ii) $\langle x^{2^\beta}, x^{2^{\beta-1}-1}y \rangle$, $1 \leq \beta \leq m$.

Also, Lemmas 1.19 and 1.20 yield that

$\mathcal{S} = \{(K_0, \langle 1 \rangle, K_1)\} \cup \{(K_1, \langle 1 \rangle, G/K_1)\} \cup \{(K_2{}^{(\alpha)}, \langle 1 \rangle, G/K_2{}^{(\alpha)}) \mid 0 \leq \alpha \leq m\} \cup \{(K_3{}^{(\beta)}, \langle 1 \rangle, G/K_3{}^{(\beta)}) \mid 1 \leq \beta \leq m\}$.

Therefore, (i) follows from Theorem 1.17.

For each $(N, D/N, A_N/N) \in \mathcal{S}$, the corresponding $o(\mathcal{A}_N, D)$ and $|R(\mathcal{A}_N/D)|$ in the case $q \equiv 1 \pmod 4$ or $q \equiv -1 \pmod 4$ are as follows:

Case I : $q \equiv 1 \pmod 4$.

$(N,\, D/N,\, \mathcal{A}_N/N)$	$o(\mathcal{A}_N,\, D)$	$\lvert R(\mathcal{A}_N/D)\rvert$
$(K_1,\, \langle 1\rangle,\, G/K_1)$,	1	1
$(K_2{}^{(0)},\, \langle 1\rangle,\, G/K_2{}^{(0)})$,	1	1
$(K_2{}^{(\alpha)},\, \langle 1\rangle,\, G/K_2{}^{(\alpha)})$, $1 \le \alpha \le m$	$\begin{cases} 2^{\alpha-\lambda}, & \alpha \ge \lambda+1, \\ 1, & \alpha \le \lambda \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \alpha \ge \lambda+1, \\ 2^{\alpha-1}, & \alpha \le \lambda \end{cases}$
$(K_3{}^{(\beta)},\, \langle 1\rangle,\, G/K_3{}^{(\beta)})$, $1 \le \beta \le m$	$\begin{cases} 2^{\beta-\lambda}, & \beta \ge \lambda+1, \\ 1, & \beta \le \lambda \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \beta \ge \lambda+1, \\ 2^{\beta-1}, & \beta \le \lambda \end{cases}$
$(K_0,\, \langle 1\rangle,\, K_1)$	$\begin{cases} 2^{m-\lambda}, & m \ge \lambda+1, \\ 1, & m \le \lambda \end{cases}$	$\begin{cases} 2^{\lambda-1}, & m \ge \lambda+1, \\ 2^{m-1}, & m \le \lambda \end{cases}$

Case II : $q \equiv -1 \pmod 4$.

$(N,\, D/N,\, \mathcal{A}_N/N)$	$o(\mathcal{A}_N,\, D)$	$\lvert R(\mathcal{A}_N/D)\rvert$
$(K_1,\, \langle 1\rangle,\, G/K_1)$,	1	1
$(K_2^{(\alpha)},\, \langle 1\rangle,\, G/K_2^{(\alpha)})$, $0 \le \alpha \le 1$	1	1
$(K_2^{(\alpha)},\, \langle 1\rangle,\, G/K_2^{(\alpha)})$, $2 \le \alpha \le m$	$\begin{cases} 2^{\alpha-\lambda}, & \alpha \ge \lambda+2, \\ 2, & \alpha \le \lambda+1 \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \alpha \ge \lambda+2, \\ 2^{\alpha-2}, & \alpha \le \lambda+1 \end{cases}$
$(K_3^{(1)},\, \langle 1\rangle,\, G/K_3^{(1)})$,	1	1
$(K_3^{(\beta)},\, \langle 1\rangle,\, G/K_3^{(\beta)})$, $2 \le \beta \le m$	$\begin{cases} 2^{\beta-\lambda}, & \beta \ge \lambda+2, \\ 2, & \beta \le \lambda+1 \end{cases}$	$\begin{cases} 2^{\lambda-1}, & \beta \ge \lambda+2, \\ 2^{\beta-2}, & \beta \le \lambda+1 \end{cases}$
$(K_0,\, \langle 1\rangle,\, K_1)$	$\begin{cases} 2^{m-\lambda}, & m \ge \lambda+2, \\ 2, & m \le \lambda+1 \end{cases}$	$\begin{cases} 2^{\lambda-1}, & m \ge \lambda+2, \\ 2^{m-2}, & m \le \lambda+1 \end{cases}$

Thus Theorem 2.3 , with the help of above two tables yield (ii) and (iii). $\square$

Remark: The above analysis of the structure of $\mathbb{F}_q[G],\ G$ of type $D_1,\ D_2$, provides a method for computing the algebraic structure of $\mathbb{F}_q[G]$, for finite group G whose central quotient is Klein four-group. It will thus naturally be of interest to compute the algebraic structure of $\mathbb{F}_q[G],\ G$ of type $D_i,\ i = 3, 4, 5$.

Bibliography

[Bas79] B. G. Basmaji, *Complex representations of metacyclic groups*, Amer. Math. Monthly **86** (1979), no. 1, 47–48.

[BdR07] Osnel Broche and Ángel del Río, *Wedderburn decomposition of finite group algebras*, Finite Fields Appl. **13** (2007), no. 1, 71–79.

[BGP] Gurmeet K. Bakshi, Shalini Gupta, and Inder Bir S. Passi, *The structure of finite semisimple metacyclic group algebras*, J. Ramanujan Math Soc. (to appear).

[BGP11] ———, *Semisimple metacyclic group algebras*, Proc. Indian Acad.Sci.(Math Sci.) **121** (2011), no. 4, 379–396.

[BKP13] Gurmeet K. Bakshi, Ravindra S. Kulkarni, and Inder Bir S. Passi, *The rational group algebra of a finite group*, J. Algebra Appl. **12** (2013), no. 3.

[BRS08] Gurmeet K. Bakshi, Madhu Raka, and Anuradha Sharma, *Idempotent generators of irreducible cyclic codes*, Number theory & discrete geometry, Ramanujan Math. Soc. Lect. Notes Ser., vol. 6, Ramanujan Math. Soc., Mysore, 2008, pp. 13–18.

[CR06] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing, Providence, RI, 2006, Reprint of the 1962 original.

[FGPM10] Raul A. Ferraz, Edgar G. Goodaire, and César Polcino Milies, *Some classes of semisimple group (and loop) algebras over finite fields*, J. Algebra **324** (2010), no. 12, 3457–3469.

[GG11] Inneke V. Gelder and Olteanu G., *Finite group algebras of nilpotent groups: A complete set of orthogonal primitive central idempotents*, Finite Fields Appl. **17** (2011), no. 2, 157–165.

[GJPM96] Edgar G. Goodaire, Eric Jespers, and César Polcino Milies, *Alternative loop rings*, North-Holland Mathematics Studies, vol. 184, North-Holland Publishing Co., Amsterdam, 1996.

[Goo83] Edgar G. Goodaire, *Alternative loop rings*, Publ. Math. Debrecen **30** (1983), no. 1-2, 31–38.

[GPMS09] A. Giambruno, C. Polcino Milies, and Sudarshan K. Sehgal, *Lie properties of symmetric elements in group rings*, J. Algebra **321** (2009), no. 3, 890–902.

[Her97] Allen Herman, *On the automorphism groups of rational group algebras of metacyclic groups*, Comm. Algebra **25** (1997), no. 7, 2085–2097.

[JLP03] Eric Jespers, Guilherme Leal, and Antonio Paques, *Central idempotents in the rational group algebra of a finite nilpotent group*, J. Algebra Appl. **2** (2003), no. 1, 57–62.

[JRM05] Eric Jespers and Manuel Ruiz Marín, *Antisymmetric elements in group rings*, J. Algebra Appl. **4** (2005), no. 4, 341–353.

[JRM06] ———, *On symmetric elements and symmetric units in group rings*, Comm. Algebra **34** (2006), no. 2, 727–736.

[Lam01] T. Y. Lam, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001.

[LSS09] Gregory T. Lee, Sudarshan K. Sehgal, and Ernesto Spinelli, *Lie properties of symmetric elements in group rings. II*, J. Pure Appl. Algebra **213** (2009), no. 6, 1173–1178.

[OdRS04] Aurora Olivieri, Ángel del Río, and Juan Jacobo Simón, *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra **32** (2004), no. 4, 1531–1550.

[OdRS06] Aurora Olivieri, Á. del Río, and Juan Jacobo Simón, *The group of automorphisms of the rational group algebra of a finite metacyclic group*, Comm. Algebra **34** (2006), no. 10, 3543–3567.

[SBDR04] Anuradha Sharma, Gurmeet K. Bakshi, V.C. Dumir, and Madhu Raka, *Cyclotomic numbers and primitive idempotents in the ring* $GF(q)[x]/x^{p^n} - 1$, Finite Fields Appl. **10** (2004), no. 4, 653–673.

[SBDR08] ———, *Irreducible cyclic codes of length* 2^n, Ars Combin **86** (2008).

[Yam74] Toshihiko Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Mathematics, Vol. 397, Springer-Verlag, Berlin, 1974.

Index

Curriculum Vitae

Name:	Shalini Gupta
Date of Birth:	15-03-1978
Nationality:	Indian
Qualification:	M.Sc (Hons.School) (Mathematics) Panjab University, Chandigarh (1999)
Affiliation:	Assistant Professor Department of Mathematics Punjabi University Patiala
E-mail :	*shalinigupta@iisermohali.ac.in*