www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 3 No. 3 (2014), pp. 25-34.

www.ui.ac.ir

UNITS IN $\mathbb{F}_{2^k}D_{2n}$

N. MAKHIJANI*, R. K. SHARMA AND J. B. SRIVASTAVA

Communicated by Evgeny Vdovin

Abstract. Let $\mathbb{F}_qD_{2n}$ be the group algebra of D_{2n}, the dihedral group of order $2n$, over $\mathbb{F}_q = GF(q)$. In this paper, we establish the structure of $\mathcal{U}(\mathbb{F}_{2^k}D_{2n})$, the unit group of $\mathbb{F}_{2^k}D_{2n}$ and that of its normalized unitary subgroup $V_*(\mathbb{F}_{2^k}D_{2n})$ with respect to canonical involution $*$ when n is odd.

1. Introduction

Let FG be the group algebra of a finite group G over a field F and $\mathcal{U}(FG)$ be its unit group. The homomorphism $\varepsilon : FG \to F$ given by $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$ is called the augmentation map of FG. The group of normalized units of FG, denoted by $V(FG)$ consists of all the units in FG of augmentation 1. The anti-automorphism $g \mapsto g^{-1}$ of G extends linearly to an anti-automorphism $a \mapsto a^*$ of FG; this extension leaves $V(FG)$ setwise invariant and its restriction to $V(FG)$ followed by $v \mapsto v^{-1}$ gives an automorphism of $V(FG)$. The elements of $V(FG)$ fixed by this automorphism are the normalized unitary units of FG; they form a subgroup denoted by $V_*(FG)$. If F is a field of characteristic 2, then

$$V_*(FG) = \left\{\ v \in \mathcal{U}(FG) \mid v^* = v^{-1}\ \right\}.$$

In [1], A. Bovdi and L. Erdei described the unitary subgroup $V_*(\mathbb{F}_2G)$ for all groups G of order 8 and 16. The structure of $\mathbb{F}_{2^k}Q_8$ was established by L. Creedon and J. Gildea in [4], where Q_8 is the quaternion group of order 8. In [2], V. Bovdi and L. G. Kovács gave conditions on F and G for which $V_*(FG)$ is normal in $V(FG)$. Additionally in [3], V. Bovdi and A. L. Rosa determined the order of $V_*(\mathbb{F}_{2^k}G)$ for special cases of G. In [5], K. Kaur and M. Khan described the structure of $\mathcal{U}(\mathbb{F}_2D_{2p})$

MSC(2010): Primary: 16U60; Secondary: 20C05.

Keywords: Group Algebra, Unit Group, Unitary Units.

Received: 30 September 2013, Accepted: 26 January 2014.

*Corresponding author.

and $V_*(\mathbb{F}_2 D_{2p})$ for an odd prime p. In continuation to this investigation, we study the structure of $\mathcal{U}(\mathbb{F}_{2^k} D_{2n})$ and $V_*(\mathbb{F}_{2^k} D_{2n})$ for odd n.

The following presentation for D_{2n} shall be used

$$\langle\ a,\ b \mid a^n,\ b^2,\ b^{-1}ab = a^{-1}\ \rangle$$

2. Notations

We establish the basic notation where l and m are coprime integers, R is a ring, K is a field extension of F, $\alpha \in K$ is algebraic over F, $g \in G$ and X is any subset of G.

$ord_m(l)$	multiplicative order of l modulo m
$irr_F(\alpha)$	minimal polynomial of α over F
C_n	cyclic group of order n
F^*	$F \setminus \{0\}$
$\widehat{X}$	$\sum_{x \in X} x$
$\widehat{g}$	$\widehat{\langle\ g\ \rangle}$
G^m	external direct product of m copies of G
R^m	external direct sum of m copies of R
$M(n,F)$	algebra of all $n \times n$ matrices over the field F
$GL(n,F)$	general linear group of all $n \times n$ invertible matrices over the field F

3. Unit Group of $\mathbb{F}_{2^k} D_{2n}$

The following lemma is a consequence of some known facts.

Lemma 3.1. *Let $(q,m) = 1$, ξ be a primitive mth root of unity over $\mathbb{F}_q$ and $d_m = ord_m(q)$. Then ξ and ξ^{-1} are conjugates over $\mathbb{F}_q$ if and only if d_m is even and $q^{d_m/2} \equiv -1 \bmod m$. Moreover*

$$\mathbb{F}_q[\xi + \xi^{-1}] \cong \begin{cases} \mathbb{F}_{q^{d_m/2}} & \text{if } d_m \text{ is even and } q^{d_m/2} \equiv -1 \bmod m \\ \mathbb{F}_{q^{d_m}} & \text{otherwise} \end{cases}$$

Proof. From ([6], Theorem 2.21, pp. 53), it is known that automorphisms of $\mathbb{F}_q(\xi)$ over $\mathbb{F}_q$ are determined by their action on ξ and given by the assignments

$$\begin{array}{ccc} \xi & \mapsto & \xi \\ \xi & \mapsto & \xi^q \\ & \vdots & \\ \xi & \mapsto & \xi^{q^{d_m-1}} \end{array}$$

Thus ξ and ξ^{-1} are conjugates over $\mathbb{F}_q$ if and only if $q^l \equiv -1 \bmod m$ for some $l \in \mathbb{N}$. The rest follows. $\square$

In what follows, $q = 2^k$.

Theorem 3.2. *Let G be the dihedral group of order $2n$, n odd. Then*

$$\mathcal{U}(\mathbb{F}_q D_{2n}) \cong \; C_2^k \times C_{q-1} \times \prod_{m|n,\; m>1} GL(2, \mathbb{F}_{q^{e_m}})^{\frac{\varphi(m)}{2e_m}}$$

where

$$e_m = \begin{cases} d_m/2 & \text{if } d_m \text{ is even and } q^{d_m/2} \equiv -1 \bmod m \\ d_m & \text{otherwise} \end{cases}$$

and $d_m = ord_m(q)$.

Proof. Let $\Phi_l(X)$ denote the l-th cyclotomic polynomial

$$\Phi_l(X) = \prod_{0<j\leq l,\; (j,l)=1} (x - \xi^j)$$

where ξ is a primitive l-th root of unity over $\mathbb{F}_q$.

It is known that

$$\Phi_l(X) = f_{l,1}(X) \cdots f_{l,s_l}(X)$$

where the polynomials $f_{l,i}(X) \in \mathbb{F}_q[X]$ are irreducible over $\mathbb{F}_q$ $\forall\, i,\; 1 \leq i \leq s_l = \dfrac{\varphi(l)}{d_l}$.

Let m be a divisor of n, $m > 1$. Also, let

$$B_m = \begin{cases} s_m & \text{if } d_m \text{ is even and } q^{d_m/2} \equiv -1 \bmod m \\ s_m/2 & \text{otherwise} \end{cases}$$

and $\xi_{m,i}$ be a root of $f_{m,i}$ for each $i,\; 1 \leq i \leq s_m$.

If $B_m = s_m/2$, then in view of Lemma 3.1, we suppose that

$$\xi_{m, \frac{s_m}{2}+i} = \xi_{m,i}^{-1} \;\forall\, i,\; 1 \leq i \leq B_m$$

Let $E_1 = \mathbb{F}_q$ and $E_m = \bigoplus_{j=1}^{B_m} M\left(2, \mathbb{F}_q[\, \xi_{m,j} + \xi_{m,j}^{-1} \,]\right)$.

We now define the following $\mathbb{F}_q$-algebra homomorphisms

(a) $\theta_1 : \mathbb{F}_q D_{2n} \to E_1$ by the assignment $a \mapsto 1,\; b \mapsto 1$.

(b) $\theta_m : \mathbb{F}_q D_{2n} \to E_m$ given by

$$a \mapsto \left(\begin{bmatrix} 0 & 1 \\ 1 & \xi_{m,j} + \xi_{m,j}^{-1} \end{bmatrix} \right)_{j=1}^{B_m}, \; b \mapsto \left(\begin{bmatrix} 1 & \xi_{m,j} + \xi_{m,j}^{-1} \\ 0 & 1 \end{bmatrix} \right)_{j=1}^{B_m}$$

Let $\theta : \mathbb{F}_q D_{2n} \to \underset{m|n}{\oplus} E_m$ be defined as

$$\theta = \underset{m|n}{\oplus} \theta_m$$

We claim that $ker\ \theta = \mathbb{F}_q\widehat{D_{2n}}$.

Let $A = \sum_{i=0}^{n-1} \alpha_i a^i + \sum_{i=0}^{n-1} \beta_i b a^i \in ker\ \theta$ and $F(X) = \sum_{i=0}^{n-1} \alpha_i X^i,\ G(X) = \sum_{i=0}^{n-1} \beta_i X^i \in \mathbb{F}_q[X]$.

Since

$$\begin{bmatrix} 0 & 1 \\ 1 & \xi_{m,j} + \xi_{m,j}^{-1} \end{bmatrix} = Z_{m,j}^{-1} \begin{bmatrix} \xi_{m,j} & 0 \\ 0 & \xi_{m,j}^{-1} \end{bmatrix} Z_{m,j} \text{ and}$$
$$\begin{bmatrix} 1 & \xi_{m,j} + \xi_{m,j}^{-1} \\ 0 & 1 \end{bmatrix} = Z_{m,j}^{-1} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} Z_{m,j}$$

where

$$Z_{m,j} = \begin{bmatrix} 1 & \xi_{m,j} \\ 1 & \xi_{m,j}^{-1} \end{bmatrix} \in M\left(2, \mathbb{F}_q[\xi_{m,j}]\right),$$

therefore

$$\begin{bmatrix} F(\xi_{m,j}) & G(\xi_{m,j}^{-1}) \\ G(\xi_{m,j}) & F(\xi_{m,j}^{-1}) \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

for all $(m,j) \in \mathcal{A}$, where $\mathcal{A} = \{\ (m,j)\ \mid m \mid n,\ m > 1 \text{ and } 1 \le j \le B_m\ \}$.

Thus $F(X) = \alpha(1 + X + \cdots + X^{n-1})$ and $G(X) = \beta(1 + X + \cdots + X^{n-1})$ for some $\alpha,\ \beta \in \mathbb{F}_q$. Since $F(1) + G(1) = 0$, $\alpha = \beta$. As a result $A = \alpha\widehat{D_{2n}}$ as claimed.

Also

$$dim_{\mathbb{F}_q} \underset{m|n}{\oplus} E_m = 1 + 2 \sum_{m>1,\ m|n} \varphi(m) = 1 + 2(n-1) = 2n - 1$$

shows that θ is onto and hence $J(\mathbb{F}_q D_{2n}) \subseteq ker\ \theta$. But $dim_{\mathbb{F}_q} J(\mathbb{F}_q D_{2n}) \ge 1$. Thus $J(\mathbb{F}_q D_{2n}) = ker\ \theta$.

Using Wedderburn Malcev theorem, we have

$$\begin{aligned} \mathcal{U}(\mathbb{F}_q D_{2n}) &\cong (1 + J(\mathbb{F}_q D_{2n})) \rtimes \left(\frac{\mathbb{F}_q D_{2n}}{J(\mathbb{F}_q D_{2n})}\right) \\ &\cong C_2^k \times C_{q-1} \times \prod_{m|n,\ m>1} GL(2, \mathbb{F}_{q^{e_m}})^{\frac{\varphi(m)}{2e_m}} \end{aligned}$$

□

4. Structure of $V_*(\mathbb{F}_q D_{2n})$

For any $g, h \in G$,

$$\mu_{g,h} = 1 + (g-1)h\widehat{g}$$

is called a bicyclic unit of FG and

(a) $\mu_{g,h}^{-1} = 1 - (g-1)h\widehat{g}$

(b) $\mu_{g,h} = 1 \Leftrightarrow h^{-1}gh \in \langle\ g\ \rangle$

We denote the group generated by the bicyclic units of FG by $\mathcal{B}(FG)$.

It is important to note that if $G = D_{2n}$, then $\mu_{a^i,h} = 1\ \forall\ h \in G$ and $1 \leq i \leq n-1$. Thus $\mathcal{B}(\mathbb{F}_q G)$ is generated by the set

$$\begin{aligned} &\left\{\ \mu_{a^ib,h} \mid 0 \leq i \leq n-1,\ h \in G\ \right\} \\ = &\left\{\ 1 + \left(a^j + a^{-j}\right)\left(1 + a^ib\right)\ \mid 0 \leq i \leq n-1,\ 1 \leq j \leq \frac{n-1}{2}\right\} \end{aligned}$$

In [5], it is shown that if $d = ord_p(2)$, then the structure of $\mathcal{B}(\mathbb{F}_2 D_{2p})$ is given by

$$\mathcal{B}(\mathbb{F}_2 D_{2p}) \cong \begin{cases} SL(2, \mathbb{F}_{2^{d/2}})^{\frac{p-1}{d}} & \textit{if } d \textit{ is even} \\ SL(2, \mathbb{F}_{2^d})^{\frac{p-1}{2d}} & \textit{if } d \textit{ is odd} \end{cases}$$

We shall now alter the proof for the same in [5] to see how the result gets generalized.

Let $\mathcal{B}_1$ be the subgroup of $\mathcal{U}(\mathbb{F}_q D_{2n})$ generated by the set

$$\left\{\ 1 + \alpha\left(a^j + a^{-j}\right)\left(1 + a^ib\right)\ \mid 0 \leq i \leq n-1,\ 1 \leq j \leq \frac{n-1}{2},\ \alpha \in \mathbb{F}_q\right\}$$

We shall need the following lemma.

Lemma 4.1. *Let L be an algebraic extension of F and $\alpha,\ \beta_1, \cdots, \beta_n \in L$ such that α is not an F-conjugate of $\beta_i\ \forall\ i,\ 1 \leq i \leq n$. Then for each $\gamma \in F[\alpha]$, there exists $f_\gamma(x) \in F[x]$ such that*

$$\begin{aligned} f_\gamma(\alpha) &= \gamma, \\ f_\gamma(\beta_i) &= 0\ \forall\ i,\ 1 \leq i \leq n \end{aligned}$$

Proof. Let $g(x) = \prod_{i=1}^{n} P_i(x)$, where $P_i(X) = irr_F(\beta_i)$.

If $\delta = g(\alpha)$ and $[F[\alpha] : F] = m$, then $\gamma = \delta \sum_{j=0}^{m-1} a_i\alpha^i$ for some $a_i \in F$. The lemma follows if we take $f_\gamma(x) = g(x) \sum_{j=0}^{m-1} a_i x^i \in F[x]$. □

Theorem 4.2. *If n is odd, then*

$$\mathcal{B}_1 \ \cong \prod_{m|n,\ m>1} SL(2, \mathbb{F}_{q^{e_m}})^{\frac{\varphi(m)}{2e_m}}$$

where

$$e_m = \begin{cases} d_m/2 & \text{if } d_m \text{ is even and } q^{d_m/2} \equiv -1 \ mod\ m \\ d_m & \text{otherwise} \end{cases}$$

and $d_m = ord_m(q)$.

Proof. Let $\theta' = \left(\underset{m|n,\ m>1}{\oplus} \theta_m \right)\Big|_{\mathcal{U}(\mathbb{F}_q D_{2n})}$ and $\theta'' = \theta'|_{\mathcal{B}_1}$. For any $X \in \mathcal{B}_1$,

$$\begin{aligned} \theta''(X)^2 &= \theta''(X^2) \\ &= \theta''(1) \\ &= (I_{2\times 2}, \cdots, I_{2\times 2}) \end{aligned}$$

Thus $\theta''(\mathcal{B}_1) \subseteq \prod_{m|n,\ m>1} SL(2, \mathbb{F}_{q^{e_m}})^{\frac{\varphi(m)}{2e_m}}$.

Now $ker\ \theta'' \subseteq ker\ \theta' = \{\ 1 + \alpha\widehat{D_{2n}} \mid \alpha \in \mathbb{F}_q\ \}$. Let $\alpha \in \mathbb{F}_q$ such that

$$1 + \alpha\widehat{D_{2n}} \in ker\ \theta'' \subseteq \mathcal{B}_1$$

If $\tau : \mathbb{F}_q D_{2n} \to \mathbb{F}_q(D_{2n}/\langle\ a\ \rangle)$ be the $\mathbb{F}_q$-algebra homomorphism determined by the map

$$a \mapsto \bar{1},\ b \mapsto \bar{b},$$

then

$$\begin{aligned} & \tau(X) = \bar{1}\ \forall\ X \in \mathcal{B}_1 \\ \Rightarrow\ & \tau(1 + \alpha\widehat{D_{2n}}) = \bar{1} \\ \Rightarrow\ & \bar{1} + \alpha(\bar{1} + \bar{b}) = \bar{1} \\ \Rightarrow\ & (1+\alpha)\bar{1} + \alpha\bar{b} = \bar{1} \end{aligned}$$

which is possible only if $\alpha = 0$. Thus $ker\ \theta'' = (1)$.

It remains to show that $\theta'' : \mathcal{B}_1 \to \prod_{(m,j)\in\mathcal{A}} SL(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}])$ is onto.

Choose $\alpha \in \mathbb{F}_q^*,\ t \geq 0$.

Also let $A^{\alpha,t} = (A^{\alpha,t}_{m,j}) \in \prod_{(m,j)\in\mathcal{A}} SL(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}])$ such that

$$A^{\alpha,t}_{m,j} = \begin{pmatrix} 1 & \alpha(\xi_{m,j} + \xi_{m,j}^{-1})^t \\ 0 & 1 \end{pmatrix}$$

Then

$$\begin{aligned} & Z_{m,j}A^{\alpha,t}_{m,j}Z^{-1}_{m,j} \\ = \;& (\xi_{m,j}+\xi^{-1}_{m,j})^{-1}\begin{pmatrix} 1 & \xi_{m,j} \\ 1 & \xi^{-1}_{m,j}\end{pmatrix}\begin{pmatrix} 1 & \alpha(\xi_{m,j}+\xi^{-1}_{m,j})^t \\ 0 & 1\end{pmatrix}\begin{pmatrix} \xi^{-1}_{m,j} & \xi_{m,j} \\ 1 & 1\end{pmatrix} \\ = \;& \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} + \alpha(\xi_{m,j}+\xi^{-1}_{m,j})^{t-1}\begin{pmatrix} 1 & 1 \\ 1 & 1\end{pmatrix} \end{aligned} \tag{4.1}$$

Notice that for any $u \in \mathbb{N}$,

$$(\xi_{m,j}+\xi^{-1}_{m,j})^u = \sum_{i=0}^{\lfloor \frac{u-1}{2}\rfloor} c_{u,i}\left(\xi^{u-2i}_{m,j}+\xi^{-(u-2i)}_{m,j}\right), \text{ where } c_{u,i} = {}^uC_i \bmod 2$$

Thus for any $t \geq 0$,

$$(\xi_{m,j}+\xi^{-1}_{m,j})^{t-1} = c_0 + \sum_i c_i\left(\xi^{i}_{m,j}+\xi^{-i}_{m,j}\right),\ c_i \in \mathbb{F}_2$$

Equation (4.1) reduces to

$$\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} + \left(d_0 + \sum_i d_i\left(\xi^{i}_{m,j}+\xi^{-i}_{m,j}\right)\right)\begin{pmatrix} 1 & 1 \\ 1 & 1\end{pmatrix},\ d_i = \alpha c_i$$

Let

$$\begin{aligned} X_{\alpha,t} &= 1 + d_0(1+b) + \sum_i d_i\left(a^i + a^{-i}\right)(1+b) \\ &= (1+d_0(1+b))(1+\sum_i d_i(a^i+a^{-i})(1+b)) \end{aligned}$$

Then $\theta'(X_{\alpha,t}) = A^{\alpha,t}$.

If

$$\begin{aligned} Z_{\alpha,t} &= \prod_{i=1}^{\frac{n-1}{2}}(1+d_0(a^i+a^{-i})(1+b)) = 1 + d_0(1+b) + d_0\widehat{D_{2n}} \text{ and} \\ Y_{\alpha,t} &= Z_{\alpha,t}(1+\sum_i d_i(a^i+a^{-i})(1+b)), \end{aligned}$$

then $\theta'(Y_{\alpha,t}) = \theta'(X_{\alpha,t}) = A^{\alpha,t}$ and $Y_{\alpha,t} \in \mathcal{B}_1$. Thus $\theta''(Y_{\alpha,t}) = A^{\alpha,t}$.

By ([7], Theorem 3.2.10)

$$SL(2,F) = \left\langle \begin{pmatrix} 1 & x \\ 0 & 1\end{pmatrix}, \begin{pmatrix} 1 & 0 \\ y & 1\end{pmatrix} \;\middle|\; x,\ y \in F\right\rangle$$

In order to show that θ'' is onto, we find an inverse image for the generators of $\prod_{(m,j)\in\mathcal{A}} SL(2,\mathbb{F}_q[\xi_{m,j}+\xi^{-1}_{m,j}])$. We begin with a generator of the type

$$C = \left(I_{2\times 2}, \cdots, I_{2\times 2}, \begin{pmatrix} 1 & x_{u,v} \\ 0 & 1\end{pmatrix}, I_{2\times 2}, \cdots, I_{2\times 2}\right)$$

where $x_{u,v} \in \mathbb{F}_q[\xi_{u,v} + \xi_{u,v}^{-1}]$ and the rest will be similar.

By Lemma 4.1, there exists $P_{u,v}(x) \in \mathbb{F}_q[x]$ such that

(1) $P_{u,v}(\xi_{u,v} + \xi_{u,v}^{-1}) = x_{u,v}$
(2) $P_{u,v}(\xi_{m,j} + \xi_{m,j}^{-1}) = 0 \ \forall \ (m,j) \neq (u,v)$

Let $P_{u,v}(x) = \sum\limits_{i=0}^{w} \alpha_i^{u,v} x^i$. This gives $x_{u,v} = \sum\limits_{i=0}^{w} \alpha_i^{u,v} (\xi_{u,v} + \xi_{u,v}^{-1})^i$. Now consider

$$\prod_{i=0}^{w} A^{\alpha_i^{u,v},i} = \left(\prod_{i=0}^{w} A_{m,j}^{\alpha_i^{u,v},i} \right) = (B_{m,j})$$

where

$$B_{m,j} = \begin{pmatrix} 1 & P_{u,v}(\xi_{m,j} + \xi_{m,j}^{-1}) \\ 0 & 1 \end{pmatrix}$$

Thus

$$\theta'' \left(\prod_{i=1}^{w} Y_{\alpha_i^{u,v},i} \right) = C$$

and we are done. □

Having obtained the structure of the subgroup $\mathcal{B}_1$, it becomes obvious to figure out how the subgroups $V_*(\mathbb{F}_q D_{2n})$ and $\mathcal{B}_1$ are related. The next theorem determines the same.

Theorem 4.3. $V_*(\mathbb{F}_q D_{2n}) \cong \mathcal{B}_1 \times \left(1 + \mathbb{F}_q \widehat{D_{2n}}\right)$

Proof. Since $q = 2^k$,

$$GL\left(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]\right) \ = \ SL\left(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]\right) \ \times \ \mathcal{Z}\left(GL\left(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]\right)\right)$$

where it is known that

$$\mathcal{Z}\left(GL\left(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]\right)\right) = \left\{ \begin{pmatrix} \alpha_{m,j} & 0 \\ 0 & \alpha_{m,j} \end{pmatrix} \ \middle| \ \alpha_{m,j} \in \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]^* \right\}$$

Hence

$$\mathcal{U}(\mathbb{F}_q D_{2n}) \cong (1 + \mathbb{F}_q \widehat{D_{2n}}) \times \mathbb{F}_q^* \times \prod_{(m,j) \in \mathcal{A}} SL\left(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]\right) \ \times \ \mathcal{Z}\left(GL\left(2, \mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]\right)\right)$$

Let $\mathbb{F}_q^* = \langle \ \zeta \ \rangle$ and $\mathbb{F}_q[\xi_{m,j} + \xi_{m,j}^{-1}]^* = \langle \ \zeta_{m,j} \ \rangle$.

Before we proceed further, we shall need the following polynomials in $\mathbb{F}_q[x]$:

1. For each $(m,j) \in \mathcal{A}$, $Q_{m,j} \in \mathbb{F}_q[x]$ such that

$$Q_{m,j}(\xi_{m,j} + \xi_{m,j}^{-1}) = \zeta_{m,j}$$
$$Q_{m,j}(\xi_{u,v} + \xi_{u,v}^{-1}) = 0 \ \forall \ (u,v) \in \mathcal{A} \text{ such that } (u,v) \neq (m,j)$$

2. $g(x) = \prod\limits_{(m,j) \in \mathcal{A}} p_{m,j}(x)$, where $p_{m,j}(x) = irr_{\mathbb{F}_q}(\xi_{m,j} + \xi_{m,j}^{-1})$

3. $g'(x) = g(0)^{-1}g(x)$

4. $h_{(m,j)}(x) = \sum\limits_{\substack{(u,v)\in\mathcal{A}\\(u,v)\neq(m,j)}} Q_{u,v}(x)^{q^{e_u}-1} + Q_{m,j}(x)$

5. $H_{(m,j)}(x) = h_{(m,j)}(x) + (1 + h_{(m,j)}(0))g'(x)$

6. $h'(x) = \sum\limits_{(u,v)\in\mathcal{A}} Q_{u,v}(x)^{q^{e_u}-1}$

7. $H'(x) = h'(x) + (\zeta + h'(0))g'(x)$

Now for each $(m, j) \in \mathcal{A}$, let

$$\begin{aligned} R_{m,j} &= H_{m,j}(a + a^{-1}) \\ S &= H'(a + a^{-1}) \end{aligned}$$

Then

$$\begin{aligned} \theta(R_{m,j}) &= \theta\left(\ H_{m,j}(a + a^{-1})\ \right) \\ &= H_{m,j}\left(\ \theta(a + a^{-1})\ \right) \\ &= (1, U^{m,j}),\ \text{where} \\ & \quad U^{m,j}_{u,v} = \begin{cases} \begin{pmatrix} \zeta_{m,j} & 0 \\ 0 & \zeta_{m,j} \end{pmatrix} & \text{if } (u,v) = (m,j) \\ I_{2\times2} & \text{otherwise} \end{cases} \\ \theta(S) &= H^{'}\left(\ \theta(a + a^{-1})\ \right) = (\zeta, I_{2\times2}, \cdots, I_{2\times2}) \end{aligned}$$

Therefore $R_{m,j},\ S \in \mathcal{U}(\mathbb{F}_qD_{2n})$ and hence $\theta'(R_{m,j}) = \theta(R_{m,j})$ and $\theta'(S) = \theta(S)$.

Observe that $\mathcal{Z}\left(\ \mathcal{U}(\mathbb{F}_qD_{2n})\ \right) \cong (1 + \mathbb{F}_q\widehat{D_{2n}}) \times\ \mathbb{F}_q^* \ \times \prod\limits_{m\ |\ n,\ m>1} \left(\ \mathbb{F}^*_{q^{e_m}}\right)^{\frac{\varphi(m)}{2e_m}}$.

As a result, the following hold true.

1. The only elements of order 2 in $\mathcal{Z}\left(\ \mathcal{U}(\mathbb{F}_qD_{2n})\ \right)$ are of the type $1 + \alpha\widehat{D_{2n}},\ \alpha \in \mathbb{F}_q$.
2. If $G_1 = \langle\ S, R_{m,j}\ \ |\ (m,j) \in \mathcal{A}\ \rangle$, then $G_1 \leq \mathcal{Z}\left(\ \mathcal{U}(\mathbb{F}_qD_{2n})\ \right)$ and $|\ G_1\ |$ is odd
3. $G_1 \cap V_*(\mathbb{F}_qD_{2n}) = (1)$ and hence $G_1 \cap \left(\mathcal{B}_1 \times (1 + \mathbb{F}_q\widehat{D_{2n}})\right) = (1)$
4. $|\ G_1\ | \geq |\ \theta'(G_1)\ | = (q-1) \times \prod\limits_{m|n,\ m>1} (q^{e_m} - 1)^{\frac{\varphi(m)}{2e_m}}$
5. $$\begin{aligned} |\ \mathcal{U}(\mathbb{F}_qD_{2n})\ | &\geq\ |\ G_1\ \times\ \mathcal{B}_1\ \times\ (1 + \mathbb{F}_q\widehat{D_{2n}})\ | \\ &\geq\ q(q-1)\ \times \prod_{m|n,\ m>1} \left(\ (q^{e_m} - 1)\ \ |\ SL(2, \mathbb{F}_{q^{e_m}})\ |\ \right)^{\frac{\varphi(m)}{2e_m}} \\ &=\ q(q-1)\ \times \prod_{m|n,\ m>1} |\ GL(2, \mathbb{F}_{q^{e_m}})\ |^{\frac{\varphi(m)}{2e_m}} \end{aligned}$$

$$= \mid \mathcal{U}(\mathbb{F}_q D_{2n}) \mid$$

6. $V_*(\mathbb{F}_q D_{2n}) \;=\; \mathcal{B}_1 \;\times\; (1 + \mathbb{F}_q \widehat{D_{2n}})$
7. $\mathcal{U}(\mathbb{F}_q D_{2n}) \;\cong\; V_*(\mathbb{F}_q D_{2n}) \times \mathbb{F}_q^* \times \prod_{m|n,\ m>1} \left(\mathbb{F}_{q^{e_m}}^* \right)^{\frac{\varphi(m)}{2e_m}}$

and hence the proof. □

5. Concluding Remarks

Remark 5.1. *Note that for any odd prime p and $i \in \mathbb{N}$, $ord_{p^{i+1}}(q) = ord_{p^i}(q)$ or $p \times ord_{p^i}(q)$. Hence*

$$\mathcal{U}(\mathbb{F}_q[D_{2p^n}]) \cong C_2^k \times C_{q-1} \times \prod_{1 \leq m \leq n} GL(2, \mathbb{F}_{q^{e_m}})^{\frac{\varphi(p^m)}{2e_m}}$$

where

$$e_m = \begin{cases} d_m/2 & \text{if } d \text{ is even} \\ d_m & \text{if } d \text{ is odd} \end{cases}$$

d_m being the multiplicative order of q modulo p^m $\forall\ 1 \leq m \leq n$ and $d = d_1$.

References

[1] A. A. Bovdi and L. Erdei, Unitary units in the modular group algebra of groups of order 16, *Technical Reports Debrecen*, **96** no. 4 (1996) 57–72.

[2] V. A. Bovdi and L. G. Kovács, Unitary units in modular group algebras, *Manuscr. Math.*, **84** no. 1 (1994) 57-72.

[3] V. Bovdi and A. L. Rosa, On the order of the unitary subgroup of a modular group algebra, *Comm. Algebra*, **28** no. 4 (2000) 1897–1905.

[4] L. Creedon and J. Gildea, Unitary units of the group algebra $\mathbb{F}_{2^k} Q_8$, *Internat. J. Algebra Comput.*, **19** no. 2 (2009) 283-286.

[5] K. Kaur and M. Khan, Units in $F_2 D_{2p}$, *J. Algebra Appl.*, **13** no. 2 2014 pp. 9 http://dx.doi.org/10.1142/S0219498813500904.

[6] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 2000.

[7] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts **80**, Springer-Verlag, New York, 1996.

Neha Makhijani

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India

Email: `nehamakhijani@gmail.com`

R. K. Sharma

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India

Email: `rksharmaiitd@gmail.com`

J. B. Srivastava

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi, India

Email: `jbsrivas@gmail.com`