UNITS IN $F D_{2p^m}$

KULDEEP KAUR, MANJU KHAN

Abstract. In this note, we compute the order and provide the structure of the unit group $U(F D_{2p^m})$ of the group algebra $F D_{2p^m}$, where $F$ is a finite field of characteristic 2 and $D_{2p^m}$ is the dihedral group of order $2p^m$ such that $p$ is an odd prime. Further, we obtain the structure of the unitary subgroup $U_*(FD_{2p^m})$ with respect to canonical involution $*$ and prove that it is a normal subgroup of the unit group $U(F D_{2p^m})$.

INTRODUCTION

Let $FG$ be the group algebra of the group $G$ over the field $F$ and $U(FG)$ its unit group. Extending the anti-automorphism $g \mapsto g^{-1}$ of $G$ to the group algebra, we obtain the involution

$$x = \sum_{g \in G} x_g g \mapsto x^* = \sum_{g \in G} x_g g^{-1}$$

of $FG$, which we call canonical involution and is denoted by *. An element $x \in U(FG)$ is called unitary if $x^* = x^{-1}$. Let $U_u(FG)$ be the unitary subgroup consisting of all unitary elements of $U(FG)$. If $V(FG) = \{ \sum_{g \in G} a_g g \in U(FG) \mid \sum_{g \in G} a_g = 1 \}$ is the normalized unit group of the group algebra $FG$, then $U(FG) = V(FG) \times F^*$, where $F^*$

2000 Mathematics Subject Classification. 16U60, 20C05.
Key words and phrases. Unitary units; Unit Group; Group algebra.
is the set of all non zero elements of $F$. In particular, if $F$ is a finite field of characteristic 2, then the unitary subgroup $U_*(FG)$ is same as the unitary subgroup $V_*(FG)$. Interest in the group $U_*(FG)$ arose in algebraic topology and unitary $K$-theory [3].

Sandling [4] computed a basis for the normalized unit group $V(FG)$, if $G$ is a finite abelian $p$-group and $F$ is a finite field with $p$ elements. In [5] Sandling provided the generators and relators for each 2-group of order dividing 16 over finite field with 2 elements. Creedon and Gildea in [1] obtained the structure of $V(FD_8)$, where $D_8$ is a dihedral group of order 8 and $F$ is a finite field of characteristic 2. In [2], Kuldeep and Manju described the structure of the unit group $U(F_2D_{2p})$, where $F_2$ is the finite field with two elements and $D_{2p}$ is the dihedral group of order $2p$ for an odd prime $p$. They also computed the order and provided the structure of the unitary subgroup $U_*(F_2D_{2p})$ with respect to canonical involution $\ast$.

Our goal here is to study the structure of the unit group $U(FD_{2p^m})$ of the group algebra $FD_{2p^m}$ of the dihedral group $D_{2p^m}$ of order $2p^m$, where $p$ is an odd prime over a finite field $F$ of characteristic 2. We also provide the structure of the unitary subgroup $U_*(FD_{2p^m})$.

Throughout the paper, we assume that $F$ is a field with $2^n$ elements. The polynomial $x^{p^m} - 1$ can be written as

$$x^{p^m} - 1 = (x - 1) \prod_{s=1}^{m} \phi_{p^s}(x),$$

where $\phi_{p^s}(x)$ is the $p^s$-th cyclotomic polynomial over $F$. If $o_s$ denotes the order of $2^n$ modulo $p^s$, i.e., $o_s = o_{p^s}(2^n)$ for $1 \leq s \leq m$, and
$k_s$ denotes the number of irreducible factors of $\phi_{p^s}(x)$ over $F$, then $k_s = \frac{\phi(p^s)}{\phi_s}$, where $\phi$ denotes the Euler $\phi$-function. If $\alpha$ is a primitive $p^s$-th root of unity, then the polynomial $(x-\alpha)(x-\alpha^{2^n}) \cdots (x-\alpha^{(2^n)^{\phi_s-1}})$ is a minimal polynomial of $\alpha$ over $F$ and therefore, it is an irreducible factor of $\phi_{p^s}(x)$ over $F$.

**Unit Group of $FD_{2p^m}$**

In this section, we provide the order of the unit group $U(FD_{2p^m})$. Assume that $o_p(2^n) = d$. Clearly, $p$ and $d$ are relatively prime and $o_{p^2}(2^n)$ is either $d$ or $pd$. In general

**Lemma 1.** For an integer $i \geq 1$, if $o_{p^i}(2^n)$ is $d$, then $o_{p^{i+1}}(2^n)$ is either $d$ or $pd$.

**Proof.** Suppose that $o_{p^{i+1}}(2^n)$ is $t$. Then, $d|t$. Further, since $(2^n)^d = 1 \mod p^i$, it follows that $(2^n)^{dp} = 1 \mod p^{i+1}$. Therefore, $t|pd$. Hence, either $t = d$ or $t = pd$. □

**Lemma 2.** Assume that $o_{p^i}(2^n)$ is $d$. If $o_{p^{i+1}}(2^n)$ is $pd$, then $o_{p^k}(2^n)$ is $p^{k-i}d$ for all $k \geq i + 2$.

**Proof.** Let $o_{p^{i+2}}(2^n)$ be $t$. Then, it is clear that $pd|t$ and $d|t$. Further, since $(2^n)^d \equiv 1 \mod p^i$, there is an integer $s$ such that $(2^n)^d = 1 + sp^i$ and so $(2^n)^{dp} \equiv 1 + sp^{i+1} \mod p^{i+2}$. As $o_{p^{i+1}}(2^n)$ is $pd$, it follows that $(p,s) = 1$ and so $(2^n)^{dp} \not\equiv 1 \mod p^{i+2}$. Also $(2^n)^{pd} \equiv 1$ modulo $p^{i+1}$, which entails that $o_{p^{i+2}}(2^n) = p^{i+2}$. Therefore $t|p^{i+2}$. Hence $o_{p^{i+2}}(2^n)$ is $p^2d$. In a similar way one can prove for any integer $k \geq (i + 3)$. □
Lemma 3. Let $o_p^k(2^n) = d$, for $1 \leq k \leq i$ and $o_{p^i+1}(2^n) = pd$. If $\zeta$ is a primitive $p^m$-th root of unity, then $\zeta^j$ and $\zeta^{-j}$ are roots of the same irreducible polynomial over $F$ if and only if $2|d$.

Proof. First, assume that $\zeta^j$ and $\zeta^{-j}$ are roots of the same irreducible polynomial over $F$. If $j = kp^r, (k, p) = 1$, then it is clear that $\zeta^j$ is primitive $p^{m-r}$-th root of unity. Therefore, $\zeta^j$ and $\zeta^{-j}$ are roots of $\phi_{p^{m-r}}(x)$. Hence, $-1 \equiv 1(2^n)^t \mod p^{m-r}$, where $1 \leq t \leq o_{m-r} - 1$. Thus $o_{p^{m-r}}(2^{nt}) = 2$. Further, since $(2^n)^{o_{m-r}} \equiv 1 \mod p^{m-r}$, it follows that $2|o_{m-r}$. From lemma (2), we get

$$o_{m-r} = \begin{cases} d, & \text{if } m - r \leq i \\ p^{m-r-1}d, & \text{if } m - r > i \end{cases}$$

As $(2, p) = 1$, we obtain that $d$ is even.

To prove the converse part, it is enough to show that if $d$ is even then there exists an integer $t$ such that $-1 \equiv (2^n)^t \mod p^{m-r}$ for any $j = kp^r, (k, p) = 1$. For that, if $d = 2t$, then $(2^n)^{2t} = 1 \mod p^{m-r}$ or $(2^n)^{p^{m-r-2t}} = 1 \mod p^{m-r}$. Since $-1$ is the only element of order 2 in $\mathbb{Z}_{p^{m-r}}$, it follows that $(2^n)^t \equiv -1 \mod p^{m-r}$ or $(2^n)^{p^{m-r-2t}} \equiv -1 \mod p^{m-r}$. □

Lemma 4. Let $o_p^k(2^n) = d$ for $1 \leq k \leq i$ and $o_{p^i+1}(2^n) = pd$. If $d$ is even, then for any $j$, $[F(\zeta^p + \zeta^{-p}) : F] = \frac{o_{m-1}}{2}$, and if $d$ is odd, then $[F(\zeta^p + \zeta^{-p}) : F] = o_{m-j}$ and in this case $F(\zeta^p + \zeta^{-p}) = F(\zeta^p)$.

Proof. If $[F(\zeta^p + \zeta^{-p}) : F] = s < \frac{o_{m-1}}{2}$, then there exists a polynomial of degree $2s < o_{m-j}$ satisfied by $\zeta^p$, which is a contradiction. Therefore
Theorem 5. Let $D_{2p^m}$ be the dihedral group

$$D_{2p^m} = \langle a, b \mid a^{p^m} = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle.$$

Assume that $o_{p^k}(2^n) = d$, for $1 \leq k \leq i$ and $o_{p^{i+1}}(2^n) = pd$. If $o_r = o_{p^r}(2^n)$, then the order of the unit group $\mathcal{U}(F_{2p^m})$ is

$$2^n(2^n - 1) \prod_{r=1}^{m} ((q_r^2 - 1)(q_r^2 - q_r))^{k'_r},$$

where $q_r = \begin{cases} 2^{\frac{np}{d}}, & \text{if } d \text{ is even} \\ 2^{np}, & \text{if } d \text{ is odd} \end{cases}$ and $k'_r = \begin{cases} k_r, & \text{if } d \text{ is even} \\ k_r, & \text{if } d \text{ is odd} \end{cases}$.

Proof. Let $f_{1,p^j}(x), f_{2,p^j}(x), \ldots, f_{k_j,p^j}(x)$ be the distinct irreducible factors of the cyclotomic polynomial $\Phi_{p^j}(x)$ over $F$, where $k_j = \frac{\Phi(p^j)}{d} = \frac{p^j-1(p-1)}{d}$, for $1 \leq j \leq i - 1$ and $k_j = \frac{p^i-1(p-1)}{d}$ for $i \leq j \leq m$. If $\gamma_1$ and $\gamma_2$ denote roots of distinct irreducible factors of $\Phi_{p^i}(x)$ over $F$, then $\gamma_1 = \zeta^{p^{m-j}J_1}$ and $\gamma_2 = \zeta^{p^{m-j}J_2}$ for some integer $J_1$ and $J_2$ such that $(J_1, p) = 1$ and $(J_2, p) = 1$. Choose $\gamma'_1 = \zeta^{p^{m-j-1}J_1}$ and $\gamma'_2 = \zeta^{p^{m-j-1}J_2}$, then $\gamma'_1$ and $\gamma'_2$ are roots of $\Phi_{p^{i+1}}(x)$ over $F$. If $\gamma'_1$ and $\gamma'_2$ are roots of the same irreducible factors of $\Phi_{p^{i+1}}(x)$ then there exists $t$ such that
\[ J_1 = (2^n)^t J_2 \mod p^j + 1. \] Hence, \( J_1 = (2^n)^t J_2 \mod p^j \), which is a contradiction. Hence, \( \gamma'_1 \) and \( \gamma'_2 \) are roots of distinct irreducible factors of \( \phi_{p^j+1}(x) \) over F.

Choose \( \gamma_{1j} \) as a root of the irreducible factor \( f_{j,p}(x) \) of \( \phi_p(x) \), where \( 1 \leq j \leq k_1 \). Therefore \( \gamma_{1j} = \zeta^{p^{n-1} J_j} \), \( (J_j, p) = 1 \). Let \( \gamma^{(l)}_{11}, \gamma^{(l)}_{12}, \ldots, \gamma^{(l)}_{1k_1} \) denote roots of distinct irreducible factors of \( \phi_{p^l}(x) \) over F, for \( 1 \leq l \leq m \), where \( \gamma^{(1)}_{1j} = \gamma_{1j} \) and \( \gamma^{(l)}_{1j} = \zeta^{p^{n-1} J_j} \), \( 1 \leq j \leq k_1 \). Since the number of irreducible factors of \( \phi_{p^l}(x) \) is \( k_2 = pk_1 \), without loss of generality, assume that \( \gamma^{(l)}_{1j} \) is a root of \( f_{j,p^l}(x) \) for \( 1 \leq j \leq k_1 \) and \( 1 \leq l \leq m \).

Further, in a similar way, choose \( \gamma_{2j} \) from the irreducible factor \( f_{j,p^2} \) of \( \phi_{p^2}(x) \), where \( k_1 < j \leq k_2 \).

If \( \gamma_{rs} \) denotes the root of the irreducible factor \( f_{s,p^r}(x) \) of \( \phi_{p^r}(x) \) for \( 1 \leq r \leq i, 1 \leq s \leq k_r \).

Define \( \gamma_{rs} = \begin{cases} \gamma^{(r)}_{1s}, & \text{if } 1 \leq s \leq k_1 \\ \gamma^{(r-1)}_{2s}, & \text{if } k_1 < s \leq k_2 \\ \vdots \\ \gamma^{(1)}_{rs}, & \text{if } k_r - 1 < s \leq k_r, \end{cases} \)

where \( \gamma^{(1)}_{rs} = \gamma_{rs} \).

Since \( k_i = k_{i+1} = \cdots = k_m \), consider for \( i + 1 \leq r \leq m, 1 \leq s \leq k_i \)

\[ \gamma_{rs} = \begin{cases} \gamma^{(r)}_{1s}, & \text{if } 1 \leq s \leq k_1 \\ \gamma^{(r-1)}_{2s}, & \text{if } k_1 < s \leq k_2 \\ \vdots \\ \gamma^{(r-i+1)}_{is}, & \text{if } k_{i-1} < s \leq k_i. \end{cases} \]
Define a matrix representation $T_{rs}$ of $D_{2p^m}$,

$$T_{rs} : D_{2p^m} \to M_2(F(\gamma_{rs} + \gamma_{rs}^{-1}))$$

by the assignment

$$a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & \gamma_{rs} + \gamma_{rs}^{-1} \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & 0 \\ \gamma_{rs} + \gamma_{rs}^{-1} & 1 \end{pmatrix}$$

If $d$ is even, then define $T = T_0 \oplus \bigoplus_{r=1}^{m} T_{rs}$, the direct sum of the given representations $T_{rs}, 1 \leq r \leq m, 1 \leq s \leq k_r$, and $T_0$ is the trivial representation of $D_{2p^m}$ over $F$ of degree 1.

Suppose $d$ is odd. Then lemma (4) implies that $\gamma_{rs}$ and $\gamma_{rs}^{-1}$ are roots of different irreducible factors of $\phi_{p^r}(x)$. If $\gamma_{rs}^{-1}$ is a root of $f_{j,p^r}(x)$, then choose $\gamma_{rj} = \gamma_{rs}^{-1}$. Without loss of generality, assume that $\{\gamma_{rs} | 1 \leq r \leq m, 1 \leq s \leq k_r\}$ are roots of distinct irreducible factors of $\phi_{p^r}(x)$ such that $\gamma_{rj} \neq \gamma_{rs}^{-1}$ for $1 \leq j, s \leq \frac{k_r}{2}$. Then, define $T = T_0 \oplus \bigoplus_{r=1}^{m} T_{rs}$, the direct sum of all distinct matrix representations. Therefore, the map

$$T : D_{2p^m} \to F \oplus \bigoplus_{r=1}^{m} \bigoplus_{s=1}^{k_r'} M_2(F(\gamma_{rs} + \gamma_{rs}^{-1}))$$

is a group homomorphism, where $k_r' = \begin{cases} k_r, & \text{if } d \text{ is even} \\ \frac{k_r}{2}, & \text{if } d \text{ is odd} \end{cases}$.

By extending this group homomorphism linearly over $F$, we obtain an algebra homomorphism

$$T' : FD_{2p^m} \to F \oplus \bigoplus_{r=1}^{m} \bigoplus_{s=1}^{k_r'} M_2(F(\gamma_{rs} + \gamma_{rs}^{-1})).$$
Consider the matrix representation $S_{rs}$ of $D_{2p^m}$ defined as follows:

$$S_{rs}(a) = \begin{pmatrix} \gamma_{rs} & 0 \\ 0 & \gamma_{rs}^{-1} \end{pmatrix}, \quad S_{rs}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$ 

Note that for any $x \in D_{2p^m}$, $T_{rs}(x) = M_{rs}S_{rs}(x)M_{rs}^{-1}$, where $M_{rs} = \begin{pmatrix} 1 & 1 \\ \gamma_{rs} & \gamma_{rs}^{-1} \end{pmatrix}$.

Let $x = \sum_{i=0}^{p^m-1} \alpha_i a^i + \sum_{i=0}^{p^m-1} \beta_i a^i b \in KerT'$. Then, the equation $T'(x) = 0$ implies that

$$\sum_{i=0}^{p^m-1} \alpha_i + \sum_{i=0}^{p^m-1} \beta_i = 0 \quad (1)$$

and $\gamma_{rs}, \gamma_{rs}^{-1}, 1 \leq r \leq m, 1 \leq s \leq k_r'$ are roots of the polynomials $g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{p^m-1}x^{p^m-1}$ and $h(x) = \beta_0 + \beta_1 x + \cdots + \beta_{p^m-1}x^{p^m-1}$ over $F$. It follows that irreducible factors of $\phi_{p^r}(x)$ are factors of $g(x)$ and $h(x)$ for all $1 \leq r \leq m$. Further, since the irreducible factors $\phi_{p^r}(x)$ are co-prime, it follows that $\phi_p(x)\phi_{p^2}(x)\cdots\phi_{p^m}(x)$ divides $g(x)$ and $h(x)$, i.e., $1 + x + x^2 + \cdots + x^{p^m-1}$ divides $g(x)$ and $h(x)$, and hence $\alpha_i = \alpha_j$, and $\beta_i = \beta_j, 0 \leq i, j \leq p^m-1$. Thus, from equation (1), we have $\alpha_i = \beta_i, 0 \leq i \leq p^m-1$ and therefore $KerT' = F\overline{D_{2p^m}}$. Since dimensions of $(F\overline{D_{2p^m}}/F\overline{D_{2p^m}})$ and $F^{m \bigoplus \bigoplus}_{r=1} M_{2}(F(\gamma_{rs} + \gamma_{rs}^{-1}))$ over $F$ are equal, we obtain

$$\frac{F\overline{D_{2p^m}}}{F\overline{D_{2p^m}}} \cong F^{m \bigoplus \bigoplus_{r=1} M_{2}(F(\gamma_{rs} + \gamma_{rs}^{-1}))}. $$

Note that $F\overline{D_{2p^m}}$ is a nilpotent ideal and hence $T'$ induces an epimorphism $T'' : \mathcal{U}(F\overline{D_{2p^m}}) \to F^* \times \prod_{r=1}^{m} \prod_{s=1}^{k'_r} GL_2(F(\gamma_{rs} + \gamma_{rs}^{-1}))$ such that
kerT'' = 1 + \overline{F D_{2p^m}}. Thus

$$\mathcal{U}(\overline{F D_{2p^m}}) \cong F^* \times \prod_{r=1}^{m} \prod_{s=1}^{k'_r} GL_2(F(\gamma_{rs} + \gamma_{rs}^{-1})).$$

and hence the result follows.

\[\square\]

\textbf{Structure of The Unitary Subgroup} \(\mathcal{U}_*(FD_{2p^m})\)

In this section, we study the structure of the unitary subgroup \(\mathcal{U}_*(FD_{2p^m})\) with respect to canonical involution \(*\). We also prove that the unit group \(\mathcal{U}(FD_{2p^m})\) is the direct product of the unitary subgroup with a central subgroup.

Let \(f(x)\) be a monic irreducible polynomial of degree \(n\) over \(F_2\) such that \(F \cong F_2[x]/\langle f(x) \rangle\) and let \(\alpha\) be the residue class of \(x\) modulo \(\langle f(x) \rangle\). Let us define the set \(B\) as follows:

\[B = \{1 + \alpha^i (a^j + a^{-j})(1 + a^k b) \mid 0 \leq i \leq n-1, 1 \leq j \leq \frac{p^m - 1}{2}, 0 \leq k \leq p^m - 1\}\.

Clearly, \(B \subseteq U_*(FD_{2p^m})\). Let \(\mathcal{B}(FD_{2p^m})\) denote the group generated by \(B\). The following theorem provides the structure of this group.

\textbf{Theorem 6.} Let \(o_{p^k}(2^n) = d\), for \(1 \leq k \leq i\) and \(o_{p^{i+1}}(2^n) = pd\). Then,

\[\mathcal{B}(FD_{2p^m}) \cong \prod_{r=1}^{m} \prod_{s=1}^{k'_r} SL_2(F(\gamma_{rs} + \gamma_{rs}^{-1})),\]

where \(SL_2(K)\) is the special linear group of degree 2 over the field \(K\).

We will need the following results:

\textbf{Lemma 7.} \(D_{2p^m} \cap \mathcal{B}(FD_{2p^m}) = \langle a \rangle\).
Proof. Since $D_{2p^m}$ is in the normalizer of $B(FD_{2p^m})$, it implies that $B(FD_{2p^m}) \cap D_{2p^m}$ is a normal subgroup of $D_{2p^m}$. Therefore, it is either a trivial subgroup or $\langle a^{p^i} \rangle$, for $0 \leq i \leq m - 1$. Let us define a map

$$f : D_{2p^m} \rightarrow \langle g | g^2 = 1 \rangle$$

such that $f(a^i) = 1$ and $f(a^i b) = g$, $0 \leq i \leq p^m - 1$. Note that it is a group homomorphism and we can extend this linearly to an algebra homomorphism $f'$ from $FD_{2p^m}$ to $F(g)$. It is easy to see that the image of the elements of $B$ under $f'$ is 1 and therefore $b \notin B(FD_{2p^m})$. Hence, $D_{2p^m} \cap B(FD_{2p^m}) \neq D_{2p^m}$. Further, observe that

$$u_{ab,a} u_{ab,a^2} \cdots u_{ab,a^{p^m-1}} = ab(1 + \hat{D}_{2p^m})$$

and

$$u_{b,a} u_{b,a^2} \cdots u_{b,a^{p^m-1}} = b(1 + \hat{D}_{2p^m}),$$

where $u_{a,b,a^i} = 1 + (a^i + a^{-i})(1 + a^j b)$. Consequently,

$$a = u_{ab,a} u_{ab,a^2} \cdots u_{ab,a^{p^m-1}} u_{ab,a^{p^m-1-1}} \cdots u_{b,a^2} u_{b,a}. $$

Hence, $D_{2p^m} \cap B(FD_{2p^m}) = \langle a \rangle$. □

Lemma 8. If $\gamma_{rs}$ denotes the root of the irreducible factor $f_{s,p^r}$ of the cyclotomic polynomial $\phi_{p^r}(x)$ over $F$, then the minimal polynomials of $\gamma_{rs_1} + \gamma_{rs_1}^{-1}$ and $\gamma_{rs_2} + \gamma_{rs_2}^{-1}$ are distinct.

Proof. First assume that $r_1 = r_2 = r$. Then, if $d$ is even, we have $[F(\gamma_{rs_i} + \gamma_{rs_i}^{-1}) : F] = \frac{\phi}{2}$, where $1 \leq i \leq 2$. Let $f(x) = a_0 + \cdots + a_{\frac{\phi}{2}} x^{\frac{\phi}{2}}$ be the minimal polynomial over $F$ satisfied by both $\gamma_{rs_1} + \gamma_{rs_1}^{-1}$ and $\gamma_{rs_2} + \gamma_{rs_2}^{-1}$. It follows that $\gamma_{rs_1}$ and $\gamma_{rs_2}$ satisfy the same minimal polynomial
over $F$. This is a contradiction, because the irreducible factors $f_{s_1,p}$ and $f_{s_2,p}$ are coprime. Next, if $d$ is odd, then $[F(\gamma_{rs_1} + \gamma_{rs_1}^{-1}) : F] = o_r$. Therefore, the degree of the minimal polynomial of $\gamma_{rs_1} + \gamma_{rs_1}^{-1}$ over $F$ is $o_r$. Since $\gamma_{rs_1}$ and $\gamma_{rs_1}^{-1}$ are roots of different irreducible factors of $\phi_p(x)$ with degree $o_r$ and the factors are co-prime, it implies that the minimal polynomials of $\gamma_{rs_1} + \gamma_{rs_1}^{-1}$ and $\gamma_{rs_2} + \gamma_{rs_2}^{-1}$ are distinct.

Now assume that $r_1 < r_2$. If $i < r_1 < r_2$, then the degree of the minimal polynomial of $\gamma_{r_1 s_1} + \gamma_{r_1 s_1}^{-1}$ is $d_2^{-i}$ and the degree of the minimal polynomial of $\gamma_{r_2 s_2} + \gamma_{r_2 s_2}^{-1}$ is $\frac{p^{r_2 - id_2}}{2}$, if $d$ is even. Otherwise the degrees are $p^{r_1 - id}$ and $p^{r_2 - id}$, respectively. Hence, their minimal polynomials are distinct.

Now, if $r_1 \leq i < r_2$, then the degree of the minimal polynomial of $\gamma_{r_1 s_1} + \gamma_{r_1 s_1}^{-1}$ is $d$ and the degree of the minimal polynomial of $\gamma_{r_2 s_2} + \gamma_{r_2 s_2}^{-1}$ is $\frac{p^{r_2 - id}}{2}$, if $d$ is even. Otherwise the degree of the minimal polynomials are $d$ and $p^{r_1 - id}$, respectively. Hence, the result follows. In a similar way one can prove for other cases as well. □

**Proof of the theorem:** Observe that the image of elements of $B$ are in $\prod_{r=1}^{m} \prod_{s=1}^{k_r} SL_2(F(\gamma_{rs} + \gamma_{rs}^{-1}))$ under the map $T''$. Suppose $T'''$ is the restricted map of $T''$ to $B(FD_{2p^m})$, i.e.,

$$T''' : B(FD_{2p^m}) \rightarrow \prod_{r=1}^{m} \prod_{s=1}^{k_r} SL_2(F(\gamma_{rs} + \gamma_{rs}^{-1}))$$

such that $T'''(x) = T''(x)$ for $x \in B(FD_{2p^m})$. Therefore, $ker T''' \leq ker T'' = 1 + FD_{2p^m}$. Consider the element $t_{\alpha} = 1 + \alpha \tilde{D}_{2p^m}$, where $\alpha$ is a non zero element of $F$. Now, if $\alpha \neq 1$, then the length of $1 + \alpha \tilde{D}_{2p^m}$
is $2p^m$. Since the length of each element of $B(FD_{2p^m})$ is odd, it follows that $t_α \notin B(FD_{2p^m})$. Further, if $α = 1$, then the element $1 + \overline{D_{2p^m}}$ can be written as $1 + \overline{D_{2p^m}} = bu_{b,a}u_{b,a^2} \cdots u_{b,a^{p^m-1}}$. Since $b \notin B(FD_{2p^m})$, it follows that $\ker T'' = \{1\}$.

It is known that

$$SL_2(F(\zeta + \zeta^{-1})) = \left\langle \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}, \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix} \right| u, v \in F(\zeta + \zeta^{-1})\right\rangle.$$

For onto of $T''$, choose an element $U_{rs}$ from $\prod_{r=1}^{m} \prod_{s=1}^{k_r'} SL_2(F(\gamma_{rs} + \gamma_{rs}^{-1}))$, where the component of $U_{rs}$ corresponding to the matrix representation $T_{rs}$ is

$$\begin{pmatrix} 1 & 0 \\ u_{rs} & 1 \end{pmatrix},$$

such that $u_{rs} \in F(\gamma_{rs} + \gamma_{rs}^{-1})$ and the remaining components are identity matrices. Let $y_{rs} = \prod_{t=1}^{m} \prod_{j=1}^{k_t'} f_{t,j}'(\gamma_{rs} + \gamma_{rs}^{-1})$, where $f_{t,j}'(x)$ is the minimal polynomial of $\gamma_{tj} + \gamma_{tj}^{-1}$ over $F$. If we define

$$g(x) = \prod_{t=1}^{m} \prod_{j=1}^{k_t'} f_{t,j}'(x),$$

then $g(\gamma_{tj} + \gamma_{tj}^{-1}) = 0$ for $1 \leq t \leq m$, $1 \leq j \leq k_t'$, and $t \neq r$ and $j \neq s$ and $g(\gamma_{rs} + \gamma_{rs}^{-1}) = y_{rs}$, a nonzero element of $F(\gamma_{rs} + \gamma_{rs}^{-1})$. Choose $\{y_{rs}, y_{rs}(\gamma_{rs} + \gamma_{rs}^{-1}), \ldots, y_{rs}(\gamma_{rs} + \gamma_{rs}^{-1})^{t_r-1}\}$ as a basis of $F(\gamma_{rs} + \gamma_{rs}^{-1})$ over $F$, where $t_r = [F(\gamma_{rs} + \gamma_{rs}^{-1}) : F]$. Thus, the element $u_{rs}$ can be written as

$$u_{rs} = y_{rs} \sum_{q=0}^{t_r-1} \beta_q(\gamma_{rs} + \gamma_{rs}^{-1})^q.$$

Assume that $u'(x) = g(x)u(x)$, where $u(x) = \beta_0 + \beta_1x + \cdots + \beta_{t_r-1}x^{t_r-1}$, a polynomial over $F$. Now $u'(\gamma_{rs} + \gamma_{rs}^{-1}) = u_{rs}$ and $u'(\gamma_{tj} + \gamma_{tj}^{-1}) = 0$ for $1 \leq t \leq m, 1 \leq j \leq k_t', t \neq r$ and $j \neq s$. If $u'(x) = a_0 + a_1x + \cdots + a_kx^k$, then $U_{rs}$ can be written as $U_{rs} = e_0e_1 \cdots e_k$, where $e_h$ is an element of
\[
\prod_{t=1}^{m} \prod_{j=1}^{k_t'} SL_2(F(\gamma_{tj} + \gamma_{tj}^{-1}))\]

such that the component \(e_h^{(t,j)}\) of \(e_h\) corresponding to the matrix representation \(T_{tj}\) is

\[
\begin{pmatrix}
1 & 0 \\
a_h(\gamma_{tj} + \gamma_{tj}^{-1})^h & 1
\end{pmatrix},
\]

for \(0 \leq h \leq k\) and for \(1 \leq t \leq m, 1 \leq j \leq k_t'\). Now we will prove that the preimage of \(e_h\) is in \(B(FD_{2p^m})\) under the map \(T''\).

If \(a_h = 0\), then it is clear that the preimage of \(e_h\) is in \(B(FD_{2p^m})\). If \(a_h \neq 0\), then choose \(M\) from \(\prod_{t=1}^{m} \prod_{j=1}^{k_t'} GL_2(F(\gamma_{tj} + \gamma_{tj}^{-1}))\), such that the component \(M_{tj}\) corresponding to the matrix representation \(T_{tj}\) is

\[
M_{tj} = \begin{pmatrix}
1 & 1 \\
\gamma_{tj} & \gamma_{tj}^{-1}
\end{pmatrix},
\]

for \(1 \leq t \leq m, 1 \leq j \leq k_t'\). Note that

\[
M_{tj}^{-1}e_h^{(t,j)}M_{tj} = \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix} + a_h(\gamma_{tj} + \gamma_{tj}^{-1})^{h-1} \begin{pmatrix}
1 & 1 \\
1 & 1
\end{pmatrix}.
\]

Now \((\gamma_{tj} + \gamma_{tj}^{-1})^{h-1} = b_0 + \sum_{q=1}^{k} b_q((\gamma_{tj})^q + (\gamma_{tj})^{-q}),\)

where \(b_i \in F_2\) and

\[
k = \begin{cases}
h - 1, & \text{if } h > 0 \\
\frac{p^m - 1}{2}, & \text{if } h = 0
\end{cases}
\]

Hence,

\[
M_{tj}^{-1}e_h^{(t,j)}M_{tj} = \begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix} + (b_0 + \sum_{q=1}^{k} b_q'(\gamma_{tj}^q + \gamma_{tj}^{-q})) \begin{pmatrix}
1 & 1 \\
1 & 1
\end{pmatrix},
\]

where \(b_q' = a_h b_q \in F\) and the component of \(M^{-1}e_h M\) corresponding to the matrix representation \(T_{tj}\) is \(M_{tj}^{-1}e_h^{(t,j)}M_{tj}\). If

\[
\alpha = 1 + (b_0 + \sum_{q=1}^{k} b_q'(a^q + a^{-q}))(1 + b),
\]
then $T''(\alpha) = e_h$, because $S_{tj}(x) = M_{tj}^{-1}T_{tj}(x)M_{tj} \forall x \in D_{2p^m}$. Now, if $b'_0 = 0$, then

$$\alpha = 1 + \sum_{q=1}^{k} b'_q (a^q + a^{-q})(1 + b) = \prod_{q=1}^{k} (1 + b'_q(a^q + a^{-q})(1 + b)),$$

which is a product of the elements of $B$. Next, if $b'_0 \neq 0$, then consider

$$T''(\alpha) = T''(1 + b'_0(1 + b) + \sum_{q=1}^{k} (a^q + a^{-q})(1 + b))$$

$$= T''(1 + b'_0(1 + b)T''(\prod_{q=1}^{k} (1 + (a^q + a^{-q})(1 + b))).$$

Further, since $\widehat{D}_{2p^m} \in \ker T'$, therefore

$$T'(1 + b'_0(1 + b)) = T'((1 + b'_0(1 + b))(1 + \widehat{D}_{2p^m}))$$

$$= T'(1 + b'_0(1 + b + \widehat{D}_{2p^m}))$$

$$= \prod_{i=1}^{\frac{m}{2}-1} T'(1 + b'_0(a^i + a^{-i})(1 + b)),$$

is an element of $T''(B(FD_{2p^m}))$. Then, $e_h$ has a preimage in $B(FD_{2p^m})$. in a similar way, one can prove for other generators as well. Hence

$$B(FD_{2p^m}) \cong \prod_{r=1}^{m} \prod_{s=1}^{k'_r} SL_2(F(\gamma_{rs} + \gamma_{rs}^{-1})).$$

**Theorem 9.** The unitary subgroup $U_*(FD_{2p^m})$ of the group algebra $FD_{2p^m}$ is the direct product of the subgroup $B(FD_{2p^m})$ with the group $1 + \widehat{D}_{2p^m}$. Further, $U(FD_{2p^m}) = U_*(FD_{2p^m}) \times \prod_{r=1}^{m} \prod_{s=1}^{k'_r} \langle x_{rs} \rangle \times \langle x \rangle$, where $x$ and $x_{rs}$ are invertible elements in the center of the group algebra.
Units in $FD_{2p^m}$ such that the order of $x$ is $2^n - 1$ and the order of $2^{nt_r} - 1$, if $d$ is odd, otherwise $2^{n\left(\frac{d}{2}\right)} - 1$.

Proof. Let $F(\gamma_{rs} + \gamma_{rs}^{-1})^* = \langle \eta_{rs} \rangle$ be a cyclic group of order $2^{nt_r} - 1$, where $t_r = [F(\gamma_{rs} + \gamma_{rs}^{-1}) : F]$. Then,

$$GL_2(F(\gamma_{rs} + \gamma_{rs}^{-1})) = SL_2(F(\gamma_{rs} + \gamma_{rs}^{-1})) \times \left\{ \begin{pmatrix} \eta_{rs}^j & 0 \\ 0 & \eta_{rs}^j \end{pmatrix} \mid 1 \leq j \leq 2^{nt_r} - 1 \right\}.$$ 

Since $\eta_{rs} \in F(\gamma_{rs} + \gamma_{rs}^{-1})$ and \{y_{rs}, y_{rs}(\gamma_{rs} + \gamma_{rs}^{-1}), \ldots, y_{rs}(\gamma_{rs} + \gamma_{rs}^{-1})^{t_r - 1}\} is a basis of $F(\gamma_{rs} + \gamma_{rs}^{-1})$, it implies that $\eta_{rs} = y_{rs}h_{rs}(\gamma_{rs} + \gamma_{rs}^{-1}) = h'_{rs}(\gamma_{rs} + \gamma_{rs}^{-1})$, where $h_{rs}(x) \in F[x]$ and $h'_{rs}(x) = g(x)h_{rs}(x)$. Further, note that $h'_{rs}(\gamma_{tj} + \gamma_{tj}^{-1}) = 0$ for $t \neq r$ and $j \neq s$. If $\alpha_{rs}$ denotes the constant term of the polynomial $h'_{rs}(x)$ over $F$, then the image of $h'_{rs}(a + a^{-1})$ under the map $T'$ is $X_{rs}$, where the first component of $X_{rs}$ is $\alpha_{rs}$ and the component corresponding to the matrix representation $T_{rs}$ is $
abla$ \begin{pmatrix} \eta_{rs} & 0 \\ 0 & \eta_{rs} \end{pmatrix} \nabla and all the remaining components are zero matrices.

Define $Y(x) = \prod_{t=1}^{m} \prod_{j=1}^{k'_t} f'_{t,j}(x)$, where $f'_{t,j}(x)$ is the minimal polynomial of $\gamma_{tj} + \gamma_{tj}^{-1}$ over $F$. Without loss of generality, one can take that the constant coefficient of $Y(x)$ is 1. Note that $Y(\gamma_{tj} + \gamma_{tj}^{-1}) = 0$, $1 \leq t \leq m, 1 \leq j \leq k'_t$. Therefore, the image of $Y(a + a^{-1})$ under the map $T'$ is the element whose first component is 1 and all the remaining components are zero matrices. Next, we will find a preimage of $Z_{rs}$ where $Z_{rs}$ is the element of $F^* \times \prod_{t=1}^{m} \prod_{j=1}^{k'_t} GL_2(F(\gamma_{tj} + \gamma_{tj}^{-1}))$ such that its first component is 1, the component corresponding to the matrix.
representation $T_{rs}$ is \( \begin{pmatrix} \eta_{rs} & 0 \\ 0 & \eta_{rs} \end{pmatrix} \) and all the remaining components are identity matrices. Take
\[
z_{rs} = \sum_{t=1}^{m} \sum_{j=1}^{k'_t} h'_{tj}(a + a^{-1})^{2^{nt_r} - 1}.
\]
The image of $z_{rs}$ under the map $T'$ is the element whose first component is either 0 or 1 and the component corresponding to the matrix representation $T_{rs}$ is \( \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \) and all the remaining components are identity matrices. If we define $z'_{rs} = z_{rs} + h'_{rs}$, then it is clear that the image of $z'_{rs}$ is the element whose first component is either $\alpha_{rs}$ or $1 + \alpha_{rs}$ and the component corresponding to the matrix representation $T_{rs}$ is \( \begin{pmatrix} \eta_{rs} & 0 \\ 0 & \eta_{rs} \end{pmatrix} \) and all the remaining components are identity matrices. Therefore, $z'_{rs} + (1 + \alpha_{rs}) Y(a + a^{-1})$ or $z'_{rs} + \alpha_{rs} Y(a + a^{-1})$ is a preimage of the element $Z_{rs}$ which lies in the center of $FD_{2^pm}$. If $F^* = \langle \eta \rangle$, then the element $z = \sum_{t=1}^{m} \sum_{j=1}^{k'_t} h'_{tj}(a + a^{-1})^{2^{nt_r} - 1} + \eta Y(a + a^{-1})$ or $z = \sum_{t=1}^{m} \sum_{j=1}^{k'_t} h'_{tj}(a + a^{-1})^{2^{nt_r} - 1} + (1 + \eta) Y(a + a^{-1})$ is a preimage of the element $Z_{rs}$ which lies in the center of $FD_{2^pm}$. If $F^* = \langle \eta \rangle$, then the element $z = \sum_{t=1}^{m} \sum_{j=1}^{k'_t} h'_{tj}(a + a^{-1})^{2^{nt_r} - 1} + \eta Y(a + a^{-1})$ or $z = \sum_{t=1}^{m} \sum_{j=1}^{k'_t} h'_{tj}(a + a^{-1})^{2^{nt_r} - 1} + (1 + \eta) Y(a + a^{-1})$ is a preimage of the element $Z \in F^* \times \prod_{t=1}^{m} \prod_{j=1}^{k'_t} GL_2(F(\gamma_{tj} + \gamma_{tj}^{-1}))$, whose first component is $\eta$ and all the remaining components are identity matrices. Therefore, there are elements $x_{rs}$ of order $2^{nt_r} - 1$ and an element $x$ of order $2^n - 1$ in $U(FD_{2^pm})$. Since $\langle x_{rs} \rangle \cap \langle x_{tj} \mid 1 \leq t \leq m, 1 \leq s \leq k'_t, t \neq r \text{ and } j \neq s \rangle = \{1\}$, take $W = \prod_{t=1}^{m} \prod_{j=1}^{k'_t} \langle x_{tj} \rangle$. Note that $\langle x \rangle \cap W = \{1\}$. 

The order of the group $\langle x \rangle \times W$ is odd and is contained in the center of $FD_{2p^m}$, therefore $W \cap U_s(FD_{2p^m}) = \{1\}$. By comparing the order, we obtain that $U(FD_{2p^m}) = W \times \langle x \rangle \times (B(FD_{2p^m}) \times (1 + \widehat{D}_{2p^m}))$ and therefore, $U_s(FD_{2p^m}) = B(FD_{2p^m}) \times (1 + \widehat{D}_{2p^m})$. The group $1 + \widehat{D}_{2p^m} = \prod_{i=0}^{n-1} \langle 1 + \alpha^i \widehat{D}_{2p^m} \rangle$, is an elementary abelian 2-group. 

**Corollary 10.** The commutator subgroup $U'(FD_{2p^m}) = U'_s(FD_{2p^m})$. Also, $U'(FD_{2p^m})$ is a normal subgroup of $B(FD_{2p^m})$.

**Proof.** Since $U(FD_{2p^m}) = W \times \langle x \rangle \times U_s(FD_{2p^m})$ such that $W \times \langle x \rangle$ is in the center of $FD_{2p^m}$, it follows that $U'(FD_{2p^m}) = U'_s(FD_{2p^m})$. Further, because $U_s(FD_{2p^m}) = B(FD_{2p^m}) \times (1 + \widehat{D}_{2p^m})$ and $(1 + \widehat{D}_{2p^m})$ lies in the center of $FD_{2p^m}$, it implies that $U'_s(FD_{2p^m}) \leq B(FD_{2p^m}) \leq U_s(FD_{2p^m})$ providing us with the result. □

**References**

[1] L. Creedon and J. Gildea. The structure of the unit group of the group algebra $F_2 D_8$. *Canad. Math. Bull.*, 54(2):237–243, 2011.

[2] K. Kaur and M. Khan. Units in $F_2 D_{2p}$. *Journal of Algebra and Its Applications*, to appear.

[3] S. P. Novikov. Algebraic construction and properties of Hermitian analogs of $K$-theory over rings with involution from the viewpoint of Hamiltonian formalism. Applications to differential topology and the theory of characteristic classes. I. II. *Izv. Akad. Nauk SSSR Ser. Mat.*, 34:253–288; ibid. 34 (1970), 475–500, 1970.

[4] R. Sandling. Units in the modular group algebra of a finite abelian $p$-group. *J. Pure Appl. Algebra*, 33(3):337–346, 1984.

[5] R. Sandling. Presentations for unit groups of modular group algebras of groups of order 16. *Math. Comp.*, 59(200):689–701, 1992.
E-mail address: kuldeepk@iitrpr.ac.in, manju@iitrpr.ac.in

DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF TECHNOLOGY ROPAR, NANGAL ROAD, RUPNAGAR - 140 001