UNITS IN $F_2D_{2p}$

KULDEEP KAUR, MANJU KHAN

Abstract. Let $p$ be an odd prime, $D_{2p}$ be the dihedral group of order $2p$, and $F_2$ be the finite field with two elements. If $*$ denotes the canonical involution of the group algebra $F_2D_{2p}$, then bicyclic units are unitary units. In this note, we investigate the structure of the group $B(F_2D_{2p})$, generated by the bicyclic units of the group algebra $F_2D_{2p}$. Further, we obtain the structure of the unit group $U(F_2D_{2p})$ and the unitary subgroup $U_*(F_2D_{2p})$, and we prove that both $B(F_2D_{2p})$ and $U_*(F_2D_{2p})$ are normal subgroups of $U(F_2D_{2p})$.

INTRODUCTION

Let $FG$ be the group algebra of the group $G$ over the field $F$ and $U(FG)$ denotes its unit group. The anti-automorphism $g \mapsto g^{-1}$ of $G$ can be extended linearly to an anti-automorphism $a \mapsto a^*$ of the group algebra $FG$ known as canonical involution of $FG$. Let $U_*(FG)$ be the unitary subgroup consisting of the elements of $U(FG)$ that are inverted by canonical involution $*$. These elements are called unitary units in $FG$. If $F$ is a finite field of characteristic 2, then $U_*(FG)$ coincides with $V_*(FG)$; otherwise, it coincides with $V_*(FG) \times \langle -1 \rangle$. Here $V_*(FG)$ denotes the set of all unitary units in the normalized

2000 Mathematics Subject Classification. 16U60, 20C05.
Key words and phrases. Unitary units; Unit Group; Group algebra.
unit group $V(FG)$. Interest in the group $U_*(FG)$ arose in algebraic topology and unitary $K$-theory \cite{6}.

We are interested in the structure of the unit group $\mathcal{U}(F_2D_{2p})$ and the unitary subgroup $\mathcal{U}_*(F_2D_{2p})$. For a finite abelian $p$-group $G$ and the field $F$ with $p$ elements, R. Sandling \cite{7} gave the structure of $V(FG)$ and the structure of $V_*(FG)$ was obtained by A.A.Bovdi and A.A.Sakach in \cite{2} for a finite field $F$ of characteristic $p$. For a field $F$ with two elements and a 2-group $G$ up to order 16, R. Sandling \cite{8} gave the presentation for $V(FG)$. Later on, A.Bovdi and L. Erdei \cite{1} described the structure of the unitary subgroup $V_*(F_2G)$, where $G$ is a nonabelian group of order 8 and 16. In \cite{4} V. Bovdi and A. L. Rosa computed the order of the unitary subgroup of the group of units when $G$ is either an extraspecial 2-group or the central product of such a group with a cyclic group of order 4, and $F$ is a finite field of characteristic 2. In the same paper, they computed the order of the unitary subgroup $V_*(FG)$, where $G$ is a 2-group with an abelian subgroup $A$ of index 2 and an element $b$ such that $b$ inverts every element in $A$ and the order of $b$ is 2 or 4. V. Bovdi and T.Rozgonyi in \cite{3} described the structure of $V_*(F_2G)$, where the order of $b$ is 4.

For a dihedral group $G$ of order 6 and 10 and an arbitrary finite field $F$, the structure of the unit group $\mathcal{U}(FG)$ is described in \cite{9} and \cite{5}. Here we give the structure of the unit group $\mathcal{U}(F_2D_{2p})$ and the group $\mathcal{U}_*(F_2D_{2p})$. The bicyclic units of $F_2D_{2p}$ play an important role in finding the structure of unit group. We also study the structure of the group, $\mathcal{B}(F_2D_{2p})$, generated by bicyclic units of $F_2D_{2p}$. 
For an element \( g \in G \) of order \( n \), write \( \hat{g} = 1 + g + g^2 + \cdots + g^{n-1} \).

If \( g, h \in G, o(g) < \infty \), then

\[
\hat{u}_{g,h} = 1 + (g - 1)\hat{h}
\]

has an inverse \( \hat{u}_{g,h}^{-1} = 1 - (g - 1)\hat{h} \). Moreover, \( \hat{u}_{g,h} = 1 \) if and only if \( h \) is in the normalizer of \( \langle g \rangle \). The element \( \hat{u}_{g,h} \) is known as a bicyclic unit of the group algebra \( FG \) and the group generated by them is denoted by \( B(FG) \). Observe that all nontrivial bicyclic units of the group algebra \( F_2 D_{2p} \) are unitary units with respect to canonical involution.

Let \( F_q \) be a finite field with \( q \) elements and \( n \) be a positive integer coprime with \( q \). If order of \( q \mod n \) is \( d \), then the set \( \{a_0, a_0q, \ldots a_0q^{d-1}\} \) of elements of \( \mathbb{Z}_n \) is said to be \( q \)-cycle modulo \( n \). Further, if \( \alpha \) is a primitive \( n \)-th root of unity, then the polynomial

\[
f_{a_0}(x) = (x - \alpha^{a_0})(x - \alpha^{a_0q}) \cdots (x - \alpha^{a_0q^{d-1}}),
\]

is an irreducible factor of \( \phi_n(x) \) over \( F_q \) is of degree \( d \). Hence, the number of irreducible factors of \( \phi_n(x) \) over \( F_q \) is \( \frac{\phi(n)}{d} \). Since \( F_2 \) is a field with 2 elements and \( D_{2p} \) is the dihedral group of order \( 2p \), it follows that if order of \( 2 \mod p \) is \( d \), then the number of irreducible factors of the cyclotomic polynomial \( \phi_p(x) \) over \( F_2 \) is \( \frac{\phi(p)}{d} \) and each irreducible factor is of degree \( d \).

**Unit Group of \( F_2 D_{2p} \)**

**Theorem 1.** Let \( G \) be the dihedral group

\[
D_{2p} = \langle a, b \mid a^p = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle.
\]
Suppose $V = \langle 1 + \overline{D_{2p}} \rangle$, where $\overline{D_{2p}}$ denotes the sum of all elements of $D_{2p}$. Then

$$U(F_2D_{2p})/V \cong \begin{cases} GL_2(F_{2^d}) \times GL_2(F_{2^d}) \cdots \times GL_2(F_{2^d}), & \text{if } d \text{ is even} \\ \underbrace{GL_2(F_{2^d}) \times GL_2(F_{2^d}) \cdots \times GL_2(F_{2^d})}_{\phi(p) \text{ copies}}, & \text{if } d \text{ is odd} \end{cases}$$

and hence $|U(F_2D_{2p})| = \begin{cases} 2((2^d - 1)(2^{2d} - 2^d))^{\phi(p)/d}, & \text{if } d \text{ is even} \\ 2((2^{2d} - 1)(2^{2d} - 2^d))^{\phi(p)/2d}, & \text{if } d \text{ is odd} \end{cases}$

We need the following lemmas:

**Lemma 2.** Let $p$ be an odd prime such that order of $2 \ mod \ p$ is $d$. If $\zeta$ is a primitive $p$-th root of unity, then $\zeta$ and $\zeta^{-1}$ are the roots of the same irreducible factor of $\phi_p(x)$ over $F_2$ if and only if $d$ is even.

**Proof.** Assume that $\zeta$ and $\zeta^{-1}$ are the roots of the same irreducible factor of $\phi_p(x)$ over $F_2$. It follows that $-1$ and $1$ are in same 2-cycle $mod \ p$ and so there exist some $t < d$ such that $2^t \equiv -1 \ mod \ p$. Hence order of $2^t \ mod \ p$ is 2. Further, since $2^d \equiv 1 \ mod \ p$, it implies that $(2^t)^d \equiv 1 \ mod \ p$. Hence $2|d$.

Conversely, let $d$ be even, say $d = 2t$. Then $2^t \equiv -1 \ mod \ p$ and hence $-1$ and $1$ are in same 2-cycle $mod \ p$. The result follows. \qed

**Lemma 3.** Let $\zeta$ be a primitive $p$-th root of unity. If order of $2 \ mod \ p$ is $d$, then $[F_2(\zeta + \zeta^{-1}) : F_2] = \frac{d}{2}$, if $d$ is even and $[F_2(\zeta + \zeta^{-1}) : F_2] = d$, if $d$ is odd and in this case $F_2(\zeta + \zeta^{-1}) = F_2(\zeta)$. 
Proof. We claim that \([F_2(\zeta) : F_2(\zeta + \zeta^{-1})] = 1\) or \(2\). If \([F_2(\zeta) : F_2(\zeta + \zeta^{-1})] = s > 2\), then the degree of the minimal polynomial of \((\zeta + \zeta^{-1})\) over \(F_2\) is \(\frac{d}{s}\), which is less than \(\frac{d}{2}\). Hence, there is a polynomial over \(F_2\) satisfied by \(\zeta\) of degree less than \(d\), which is impossible.

Now, if \(d\) is even, then by last lemma, we obtain a polynomial of degree \(d\) satisfied by \(\zeta\) and \(\zeta^{-1}\). It implies that there is a polynomial of degree \(d - 1\) satisfied by \(\zeta + \zeta^{-1}\). Hence \([F_2(\zeta + \zeta^{-1}) : F_2] < d\) and therefore, \([F_2(\zeta) : F_2(\zeta + \zeta^{-1})] = 2\). Further, if \(d\) is odd, then \([F_2(\zeta) : F_2(\zeta + \zeta^{-1})] \neq 2\). Hence \(F_2(\zeta) = F_2(\zeta + \zeta^{-1})\) and so \([F_2(\zeta + \zeta^{-1}) : F_2] = d\). \(\Box\)

Proof of the Theorem. Let the cyclotomic polynomial

\[
\phi_p(x) = f_1(x)f_2(x)\ldots f_s(x)
\]

be the product of irreducible factors over \(F_2\), where \(s = \frac{\phi(p)}{d}\). Assume that \(\gamma_i\) is a root of irreducible factor \(f_i(x)\) over \(F_2\). Define a matrix representation of \(D_{2p}\),

\[
T_{\gamma_i} : D_{2p} \to M_2(F_2(\gamma_i + \gamma_i^{-1}))
\]

by the assignment

\[
a \mapsto \begin{pmatrix} 0 & 1 \\ 1 & \gamma_i + \gamma_i^{-1} \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & 0 \\ \gamma_i + \gamma_i^{-1} & 1 \end{pmatrix}
\]

If \(d\) is even, then define \(T = T_0 \oplus T_{\gamma_1} \oplus T_{\gamma_2} \oplus \cdots \oplus T_{\gamma_s}\), the direct sum of the given representations \(T_{\gamma_i}, 1 \leq i \leq s\), and \(T_0\) is the trivial representation of \(D_{2p}\) over \(F_2\) of degree 1.
Suppose \( d \) is odd. Lemma (2) implies that \( \gamma_i \) and \( \gamma_i^{-1} \) are roots of the different irreducible factors of \( \phi_p(x) \). If \( \gamma_i^{-1} \) is a root of \( f_j(x) \), then choose \( \gamma_j = \gamma_i^{-1} \). Without loss of generality, assume that \( \gamma_1, \gamma_2, \ldots, \gamma_{s'} \) are the roots of distinct irreducible factors of \( \phi_p(x) \) such that \( \gamma_i \neq \gamma_j^{-1} \) for \( 1 \leq i, j \leq s' \). Then define \( T = T_0 \oplus \bigoplus_{i=1}^{s'} T_{\gamma_i} \), the direct sum of all distinct matrix representation. Therefore,

\[
T : D_{2p} \to \mathcal{U}(F_2 \oplus M_2(F_2(\gamma_1 + \gamma_1^{-1}))) \oplus \cdots \oplus M_2(F_2(\gamma_k + \gamma_k^{-1})))
\]

given by

\[
a \mapsto \begin{pmatrix} 1, \begin{pmatrix} 0 & 1 \\ 1 & \gamma_1 + \gamma_1^{-1} \end{pmatrix} \end{pmatrix}, \cdots, \begin{pmatrix} 0 & 1 \\ 1 & \gamma_k + \gamma_k^{-1} \end{pmatrix}
\]

and

\[
b \mapsto \begin{pmatrix} 1, \begin{pmatrix} 1 & 0 \\ \gamma_1 + \gamma_1^{-1} & 1 \end{pmatrix} \end{pmatrix}, \cdots, \begin{pmatrix} 1 & 0 \\ \gamma_k + \gamma_k^{-1} & 1 \end{pmatrix}
\]

is a group homomorphism, where \( k = s = \frac{\phi(p)}{d} \), if \( d \) is even and \( k = s' = \frac{\phi(p)}{2d} \) if \( d \) is odd.

Extend this group homomorphism \( T \) to the algebra homomorphism

\[
T' : F_2 D_{2p} \to F_2 \oplus M_2(F_2(\gamma_1 + \gamma_1^{-1}))) \oplus \cdots \oplus M_2(F_2(\gamma_k + \gamma_k^{-1}))),
\]

where \( M_2(F_2(\gamma_i + \gamma_i^{-1}))) \) is the algebra of \( 2 \times 2 \) matrices over the field \( F_2(\gamma_i + \gamma_i^{-1}) \).
Note that the representation $T_{\gamma_i}$ is equivalent to $S_{\gamma_i}$, where

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

Hence, for $x \in D_{2p}, T_{\gamma_i}(x) = M_i S_{\gamma_i}(x) M_i^{-1}$, where $M_i = \begin{pmatrix} 1 & 1 \\ \gamma_i & \gamma_i^{-1} \end{pmatrix}$.

Suppose that $x = \sum_{i=0}^{p-1} \alpha_i a^i + \sum_{i=0}^{p-1} \beta_i a^i b \in \text{Ker} T'$. Then $T'(x) = 0$ implies that

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

and for $1 \leq j \leq k, \gamma_j$ and $\gamma_j^{-1}$ satisfies the polynomials $g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{p-1} x^{p-1}$ and $h(x) = \beta_0 + \beta_1 x + \cdots + \beta_{p-1} x^{p-1}$ over $F_2$. It follows that irreducible factors of $\phi_p(x)$ are factors of $g(x)$ and $h(x)$.

Further, since all factors are co-prime, it follows that $\phi_p(x)$ divides $g(x)$ and $h(x)$ and hence $\alpha_i = \alpha_j$, and $\beta_i = \beta_j$, $0 \leq i, j \leq p - 1$. Thus, from equation (1), we have $\alpha_i = \beta_i, 0 \leq i \leq p - 1$ and therefore $\text{Ker} T' = F_2 \widehat{D}_{2p}$.

Further, the dimension of $(F_2 D_{2p}/F_2 \widehat{D}_{2p})$ and $F_2 \bigoplus_{i=1}^{k} M_2(F_2(\gamma_i + \gamma_i^{-1}))$ over $F_2$ are same. Hence

$$F_2 D_{2p}/F_2 \widehat{D}_{2p} \cong F_2 \bigoplus_{i=1}^{k} M_2(F_2(\gamma_i + \gamma_i^{-1})).$$

Since $F_2 \widehat{D}_{2p}$ is nilpotent, $T'$ induces an epimorphism

$$T'' : \mathcal{U}(F_2 D_{2p}) \to \prod_{i=1}^{k} GL_2(F_2(\gamma_i + \gamma_i^{-1}))$$
such that $\ker T'' = \langle 1 + \widehat{D_{2p}} \rangle$. Hence

$$U(F_2D_{2p})/\langle 1 + \widehat{D_{2p}} \rangle \cong \prod_{i=1}^k \text{GL}_2(F_2(\gamma_i + \gamma_i^{-1}))$$

and therefore the result follows.

**Structure of $\mathcal{B}(F_2D_{2p})$**

**Theorem 4.** Let $p$ be an odd prime such that order of $2 \mod p$ is $d$. Then, the group generated by the bicyclic units, i.e.,

$$\mathcal{B}(F_2D_{2p}) \cong \begin{cases} 
\text{SL}_2(F_{2^d}) \times \cdots \times \text{SL}_2(F_{2^d}), & \text{if } d \text{ is even} \\
\text{SL}_2(F_{2^d}) \times \cdots \times \text{SL}_2(F_{2^d}), & \text{if } d \text{ is odd} 
\end{cases}$$

where $\text{SL}_2(F)$ is the special linear group of degree 2 over $F$.

We need the following lemmas:

**Lemma 5.** $D_{2p} \cap \mathcal{B}(F_2D_{2p}) = \langle a \rangle$.

*Proof.** Since $D_{2p}$ is in the normalizer of $\mathcal{B}(F_2D_{2p})$, it implies that $\mathcal{B}(F_2D_{2p}) \cap D_{2p}$ is a normal subgroup of $D_{2p}$. Therefore, it is either a trivial subgroup or $\langle a \rangle$.

We claim that $b \notin D_{2p} \cap \mathcal{B}(F_2D_{2p})$. For that we define a map

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

such that

$$f(a^i) = 1 \text{ and } f(a^i b) = g, 0 \leq i \leq p - 1.$$
Unit Group of $F_2D_{2p}$

Note that it is a group homomorphism and we can extend this linearly to an algebra homomorphism $f'$ from $F_2D_{2p}$ to $F_2\langle g \rangle$. It is easy to see that the image of the bicyclic units under $f'$ is 1. If $b \in \mathcal{B}(F_2D_{2p})$, then $f'(b) = 1$, which is not possible. Therefore, $b \notin \mathcal{B}(F_2D_{2p})$. This shows that $D_{2p} \cap \mathcal{B}(F_2D_{2p}) \neq D_{2p}$.

Also observe that

$$u_{ab,a}u_{ab,a^2} \cdots u_{ab,a^l} = ab(1 + \widehat{D_{2p}})$$

and

$$u_{b,a}u_{b,a^2} \cdots u_{b,a^l} = b(1 + \widehat{D_{2p}}),$$

where $u_{a,b,a^i} = 1 + (a^i + a^{-i})(1 + a^ib)$ is a bicyclic unit of the group algebra $F_2D_{2p}$ and $l = \frac{p-1}{2}$. It implies that

$$a = u_{ab,a}u_{ab,a^2} \cdots u_{ab,a^l}u_{b,a} \cdots u_{b,a^2}u_{b,a}.$$ 

Hence, $D_{2p} \cap \mathcal{B}(F_2D_{2p}) = \langle a \rangle$. □

**Lemma 6.** For $1 \leq i \leq k$, let $\gamma_i$ be the primitive $p$-th root of unity described in the proof of the Theorem 1. Then the minimal polynomials of $\gamma_i + \gamma_i^{-1}, 1 \leq i \leq k$, are distinct.

**Proof.** Suppose that $d$ is even. If $\zeta$ is a primitive $p$-th root of unity, then $[F_2(\zeta + \zeta^{-1}) : F_2] = \frac{d}{2}$. Assume that

$$f(x) = a_0 + a_1x + \cdots + a_{\frac{d}{2}}x^{\frac{d}{2}}$$

is the minimal polynomial over $F_2$ satisfied by both $\gamma_i + \gamma_i^{-1}$ and $\gamma_j + \gamma_j^{-1}$ for $i \neq j$. It implies that there is a polynomial of degree $d$ over $F_2$
satisfied by both $\gamma_i$ and $\gamma_j$. This is a contradiction, because the minimal polynomials of $\gamma_i$ and $\gamma_j$ over $F_2$ are co-prime. Hence the result follows.

Further, if $d$ is odd, then $[F_2(\zeta + \zeta^{-1}) : F_2] = d$. Let $f(x)$ be the minimal polynomial over $F_2$ satisfied by both $\gamma_i + \gamma_i^{-1}$ and $\gamma_j + \gamma_j^{-1}$ for $i \neq j$. It follows that there is a polynomial $g(x)$ of degree $2d$ over $F_2$ satisfied by $\gamma_i, \gamma_j, \gamma_j$ and $\gamma_j^{-1}$. Since $d$ is odd, the minimal polynomials of $\gamma_i^{\pm 1}$ and $\gamma_j^{\pm 1}$ over $F_2$ are co-prime. Hence the product of the minimal polynomials divides $g(x)$, which is a contradiction. This completes the proof of the lemma.

□

**Proof of the theorem:** Observe that the image of the bicyclic units of the group algebra $F_2D_{2p}$ are in $\prod_{i=1}^{k} SL_2(F_2(\gamma_i + \gamma_i^{-1}))$ under the map $T''$. Suppose $T'''$ is the restricted map of $T''$ to $B(F_2D_{2p})$, i.e.,

$$T''' : B(F_2D_{2p}) \rightarrow \prod_{i=1}^{k} SL_2(F_2(\gamma_i + \gamma_i^{-1}))$$

such that $T'''(x) = T''(x)$ for $x \in B(F_2D_{2p})$. Then $kerT''' \leq kerT''$. Since $b \notin B(F_2D_{2p})$ and $u_{b,a}u_{b,a^2} \cdots u_{b,a^l} = b(1 + \overline{D_{2p}})$, it follows that $kerT''' = \{1\}$.

Further, it is known that

$$SL_2(F_2(\zeta + \zeta^{-1})) = \left\langle \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \mid u, v \in F_2(\zeta + \zeta^{-1}) \right\rangle.$$

To prove $T'''$ is onto, it is sufficient to prove that the elements of the
form
\[
\left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right), \ldots, \left( \begin{pmatrix} 1 & 0 \\ u_i & 1 \end{pmatrix} \right), \ldots, \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)
\]
and
\[
\left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right), \ldots, \left( \begin{pmatrix} 1 & v_i \\ 0 & 1 \end{pmatrix} \right), \ldots, \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)
\]
where \(u_i, v_i \in F_2(\gamma_i + \gamma_i^{-1})\) have a preimage in \(\mathcal{B}(F_2D_{2p})\) under \(T''''\) for all \(1 \leq i \leq k\).

Assume that \(y_i = \prod_{j=1, j \neq i}^{k} f_j'((\gamma_i + \gamma_i^{-1})^j)\), such that \(f_j'(x)\) is the minimal polynomial of \((\gamma_j + \gamma_j^{-1})^j\) over \(F_2\). If \(g(x) = \prod_{j=1, j \neq i}^{k} f_j'(x)\), then \(g(\gamma_j + \gamma_j^{-1}) = 0\) for \(1 \leq j \leq k, j \neq i\) and \(g(\gamma_i + \gamma_i^{-1}) = y_i\), a nonzero element of \(F_2(\gamma_i + \gamma_i^{-1})\).

Take \(\{y_i, y_i(\gamma_i + \gamma_i^{-1}), \ldots, y_i(\gamma_i + \gamma_i^{-1})^{t-1}\}\) as a basis of \(F_2(\gamma_i + \gamma_i^{-1})\) over \(F_2\), where \(t = [F_2(\gamma_i + \gamma_i^{-1}) : F_2]\). Therefore, any element \(u_i\) of \(F_2(\gamma_i + \gamma_i^{-1})\) can be written as \(u_i = y_i \sum_{j=0}^{t-1} \alpha_j(\gamma_i + \gamma_i^{-1})^j\). Assume that \(u'(x) = g(x)u(x)\), where \(u(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{t-1} x^{t-1} \in F_2[x]\) and therefore \(u'(x) \in F_2[x]\). It is clear that \(u'(\gamma_i + \gamma_i^{-1}) = u_i\) and \(u'(\gamma_j + \gamma_j^{-1}) = 0\) for \(1 \leq j \leq k, j \neq i\). Further, if \(u'(x) = a_0 + a_1 x + \cdots + a_m x^m\), then the generator \(X_i\), whose \(i\)-th component is \(\begin{pmatrix} 1 & 0 \\ u_i & 1 \end{pmatrix}\) and other components are the identity matrix, can be written as \(X_i = e_0 e_1 \cdots e_m\). Here \(e_j\) is an element of \(\prod_{i=1}^{k} SL_2(F_2(\gamma_i + \gamma_i^{-1}))\) such that
the $r$-th component of $e_j$ is \[
\begin{pmatrix}
1 & 0 \\
a_j(\gamma_r + \gamma_r^{-1})^j & 1
\end{pmatrix},
\] for $0 \leq j \leq m$, $1 \leq r \leq k$. Now we will prove that the preimage of $e_j$ is in $\mathcal{B}(F_2D_{2p})$ under the map $T'''$.

If $a_j = 0$, then it is trivial. Now assume that $a_j = 1$. Suppose that $M = (M_1, M_2, \ldots, M_k)$, where $M_r = \begin{pmatrix} 1 & 1 \\ \gamma_r & \gamma_r^{-1} \end{pmatrix}$. If

\[(\gamma_r + \gamma_r^{-1})^{j-1} = b_0 + \sum_{s=1}^{l-1} b_s(\gamma_r^s + \gamma_r^{-s}),\]

where $b_i \in F_2$ then the $r$-th component of $M^{-1}e_jM$ is

\[
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix} + (b_0 + \sum_{s=1}^{l-1} b_s(\gamma_r^s + \gamma_r^{-s})) \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.
\]

By extending the matrix representation $S_{\gamma_r}$ to an algebra homomorphism over $F_2$, we obtain that this element is an image of $\alpha$ under the algebra homomorphism $S_{\gamma_r}$, where $\alpha = 1 + (b_0 + \sum_{s=1}^{l-1} b_s(a^s + a^{-s}))(1 + b)$. Since $S_{\gamma_r}(\alpha) = M_r^{-1}T_{\gamma_r}(\alpha)M_r$, it follows that $e_j = T''(\alpha)$. If $b_0 = 0$, then

\[\alpha = \prod_{s=1}^{l-1} (1 + b_s(a^s + a^{-s})(1 + b)),\]

is product of bicyclic units of the group algebra $F_2D_{2p}$. Now if $b_0 = 1$, then

\[\alpha = b \prod_{s=1}^{l-1} (1 + b_s(a^s + a^{-s})(1 + b)).\]

Since $b(1 + \widehat{D_{2p}}) = u_{b,a} \ldots u_{b,a^l}$ and $1 + \widehat{D_{2p}}$ is in the kernel of $T''$, it implies that $\alpha(1 + \widehat{D_{2p}})$ is the preimage of $e_j$ under the map $T'''$. 
Therefore, the preimage of $X_i$ is in $\mathcal{B}(F_2D_{2p})$. Similarly we can prove the same thing for other generators. Then

$$\prod_{i=1}^{k} SL_2(F_2(\gamma_i + \gamma_i^{-1})) = T''''(\mathcal{B}(F_2D_{2p})).$$

Hence

$$\mathcal{B}(F_2D_{2p}) \cong \prod_{i=1}^{k} SL_2(F_2(\gamma_i + \gamma_i^{-1}))$$

and so

$$|\mathcal{B}(F_2D_{2p})| = \begin{cases} (2^d(2^d - 1))^k & \text{if } d \text{ is even} \\ (2^d(2^{2d} - 1))^k & \text{if } d \text{ is odd.} \end{cases}$$

### The structure of Unitary Subgroup and Unit Group

**Theorem 7.** The unitary subgroup $\mathcal{U}_*(F_2D_{2p})$ of the group algebra $F_2D_{2p}$ is the semidirect product of the normal subgroup $\mathcal{B}(F_2D_{2p})$ with the group $\langle b \rangle$. Further, $\mathcal{U}(F_2D_{2p}) = \mathcal{U}_*(F_2D_{2p}) \times \prod_{i=1}^{k} \langle z_i \rangle$, where $z_i$ is an invertible element in the center of the group algebra $F_2D_{2p}$ of order $2^d - 1$, if $d$ is even; otherwise it is of order $2^d - 1$.

**Proof.** Since $GL_2(F_2(\gamma + \gamma^{-1}))$ is the direct product of $SL_2(F_2(\gamma + \gamma^{-1}))$ with the group consisting of all nonzero scalar matrices, we have

$$\mathcal{U}(F_2D_{2p})/V \cong \prod_{i=1}^{k} (SL_2(F_2(\gamma_i + \gamma_i^{-1}))) \times (F_2(\gamma_i + \gamma_i^{-1}))^*I_{2 \times 2}),$$
where $F_2(\gamma + \gamma^{-1})^*$ is the group of all nonzero elements of $F_2(\gamma + \gamma^{-1})$.

Let $F_2(\gamma_i + \gamma_i^{-1})^* = \langle \eta_i \rangle$ for $1 \leq i \leq k$. Since $y_i = \prod_{j=1 \atop j \neq i}^{k} f_j'(\gamma_i + \gamma_i^{-1})$ is a non zero element of $F_2(\gamma_i + \gamma_i^{-1})$, take $\{y_i, y_i(\gamma_i + \gamma_i^{-1}), \ldots, y_i(\gamma_i + \gamma_i^{-1})^{t-1} \}$ as a basis of $F_2(\gamma_i + \gamma_i^{-1})$ over $F_2$. Here $t = \frac{d}{2}$ when $d$ is even; otherwise $t = d$. Therefore, $\eta_i = y_i h_i(\gamma_i + \gamma_i^{-1}) = h_i'(\gamma_i + \gamma_i^{-1})$, where $h_i(x)$ and $h_i'(x) \in F_2[x]$. Also note that $h_i'(\gamma_j + \gamma_j^{-1}) = 0$ for $i \neq j$. If the constant coefficient of $h_i'(x)$ is $\alpha \eta_i$, then the image of $h_i'(a + a^{-1})$ under the map $T'$ is the element $x_i'$ such that the first component of $x_i'$ is $\alpha \eta_i$, $(i+1)$-th component is $\begin{pmatrix} \eta_i & 0 \\ 0 & \eta_i \end{pmatrix}$ and all the remaining components are zero matrix. Further, if $y_0(x) = \prod_{i=1}^{k} f_i'(x)$, then $y_0(\gamma_i + \gamma_i^{-1}) = 0, 1 \leq i \leq k$ and the constant coefficient of $y_0(x)$ is 1. It follows that the image of $y_0(a + a^{-1})$ under the map $T'$ is the element whose first component is 1 and remaining components are zero. Choose $x_i$ such that $(i+1)$-th component is $\begin{pmatrix} \eta_i & 0 \\ 0 & \eta_i \end{pmatrix}$ and the remaining components are identity matrix. If $z_i$ denotes a preimage of $x_i$, then either

$$z_i = \sum_{j=1 \atop j \neq i}^{k} h_j'(a + a^{-1})^{2^t-1} + h_i'(a + a^{-1})$$

or

$$z_i = \sum_{j=1 \atop j \neq i}^{k} h_j'(a + a^{-1})^{2^t-1} + h_i'(a + a^{-1}) + y_0(a + a^{-1})$$

which are in the center of $U(F_2D_{2^p})$ of order $2^t - 1$. Further, since $\langle z_i \rangle \cap \langle z_j \mid 1 \leq j \leq k, j \neq i \rangle = \{1\}$, take $W = \prod_{i=1}^{k} \langle z_i \rangle$. Also, note that
$W \cap U_*(F_2D_{2p}) = \{1\}$ and therefore $U(F_2D_{2p}) = W \times (B(F_2D_{2p}) \rtimes \langle b \rangle)$ and $U_*(F_2D_{2p}) = B(F_2D_{2p}) \rtimes \langle b \rangle)$. \(\square\)

**Corollary 8.** The group generated by bicyclic units $B(F_2D_{2p})$ and the unitary subgroup $U_*(F_2D_{2p})$ are normal subgroups of $U(F_2D_{2p})$.

**Corollary 9.** The commutator subgroup $U'(F_2D_{2p}) = U'_*(F_2D_{2p})$. Also, $U'(F_2D_{2p})$ is a normal subgroup of $B(F_2D_{2p})$.

**Proof.** Since $U(F_2D_{2p}) = W \times U_*(F_2D_{2p})$ such that $W$ is in the center of $F_2D_{2p}$, it follows that $U'(F_2D_{2p}) = U'_*(F_2D_{2p})$. Further, since $U_*(F_2D_{2p}) = B(F_2D_{2p}) \rtimes \langle b \rangle$ and $b$ is in the normalizer of $B(F_2D_{2p})$, it implies that $U'_*(F_2D_{2p}) \leq B(F_2D_{2p}) \leq U_*(F_2D_{2p})$ and hence the result follows. \(\square\)

**References**

[1] A. Bovdi and L. Erdei. Unitary units in modular group algebras of 2-groups. *Comm. Algebra*, 28(2):625–630, 2000.

[2] A. A. Bovdi and A. A. Sakach. The unitary subgroup of the multiplicative group of the modular group algebra of a finite abelian $p$-group. *Mat. Zametki*, 45(6):23–29, 110, 1989.

[3] V. Bovdi and T. Rozgonyi. On the unitary subgroup of modular group algebras. *ArXiv e-prints*, March 2008.

[4] Victor Bovdi and A. L. Rosa. On the order of the unitary subgroup of a modular group algebra. *Comm. Algebra*, 28(4):1897–1905, 2000.

[5] Manju Khan. Structure of the unit group of $FD_{10}$. *Serdica Math. J.*, 35(1):15–24, 2009.
[6] 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.

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

[8] Robert Sandling. Presentations for unit groups of modular group algebras of
groups of order 16. Math. Comp., 59(200):689–701, 1992.

[9] R. K. Sharma, J. B. Srivastava, and Manju Khan. The unit group of $FS_3$. Acta
Math. Acad. Paedagog. Nyházi. (N.S.), 23(2):129–142, 2007.

E-mail address: kuldeepk@iitrpr.ac.in, manju@iitrpr.ac.in

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