ISOMORPHISM PROBLEM OF UNITARY SUBGROUPS OF GROUP ALGEBRAS

ZSOŁT BALOGH, VICTOR BOVDI

Dedicated to the memory of Professor János Kurdics

Abstract. Let \( V_*(FG) \) be the normalized unitary subgroup of the modular group algebra \( FG \) of a finite \( p \)-group \( G \) over a finite field \( F \) with the classical involution \( * \). We investigate the isomorphism problem for the group \( V_*(FG) \), that asks when the group \( V_*(FG) \) is determined by its group algebra \( FG \). We confirm it for classes of finite abelian \( p \)-groups, 2-groups of maximal class and non-abelian 2-groups of order at most 16.

1. Introduction and Results

Let \( V(FG) \) be the group on normalized units of the group algebra \( FG \) of a finite group \( G \) over a field \( F \). In 1947 R.M. Thrall proposed the following problem: For a given group \( G \) and the field \( F \), determine all groups \( H \) such that \( FH \) is isomorphic to \( FG \) over \( F \). In the special case when \( G \) is a \( p \)-group and \( F \) is a field of characteristic \( p \) this problem is called isomorphism problem of modular group algebras. The modular isomorphism problem has been investigated by several authors. It has long been known \[17\] that the group algebra \( FG \) of a finite abelian \( p \)-group determines \( G \). This result was extended in \[7\] to countable abelian \( p \)-groups by Berman. The most general result of the isomorphism problem related to abelian basic groups can be found in \[21\]. For non-abelian group algebras, this problem was investigated in \[1, 2, 3, 18, 22, 23, 24, 26, 27\] and \[28\]. For an overview we recommend the survey paper \[8\].

A modular group algebra has a large group of units and the isomorphism problem can be generalized. Such strong form of the isomorphism problem is said to be the isomorphism problem of normalized units \[7\], is due to Berman. Let \( F \) be a finite field of characteristic \( p \), \( G \) and \( H \) finite \( p \)-groups such that \( V(FG) \) and \( V(FH) \) are isomorphic. Can we state that \( G \) and \( H \) are isomorphic?

Berman \[7\] gave a positive answer for his question for finite abelian \( p \)-groups. Sandling \[25\] generalized the previous result, proving that if \( G \) is a finite abelian \( p \)-group, then a subgroup of \( V(FG) \), independent as a subset of the vector space \( FG \), is isomorphic to a subgroup of \( G \). For finite non-abelian \( p \)-groups \((p > 2)\) with cyclic Frattini subgroup as well as for the class of maximal 2-groups the Berman’s question has also a positive solution \[4, 5\].

An element \( u \in V(FG) \) is called unitary if \( u^{-1} = u^* \), with respect to the classical involution of \( G \) (which sends each element of \( G \) into its inverse). Obviously, the set \( V_*(FG) \) of all unitary elements of \( V(FG) \) forms a subgroup. The structure of the unitary subgroup \( V_*(FG) \) has been actively investigated in \[11, 13, 14, 15, 16\] and \[19\].

The unitary group \( V_*(FG) \) of a group algebra \( FG \) is a small subgroup in \( V(FG) \) so it is interesting to ask whether this smaller subgroup determine the basic group \( G \) or not. This problem is called the \( * \)-unitary isomorphism problem (\( * \)-UIP) of group algebras.

2000 Mathematics Subject Classification. 16S34, 16U60.
Key words and phrases. group ring, isomorphism problem, unitary subgroup.
A positive solution of (\textasteriskcentered-UIP) for the classes of finite abelian \( p \)-groups is given here.

**Theorem 1.** Let \( FG \) be the group algebra of a finite abelian \( p \)-group \( G \) over a finite field \( F \) of characteristic \( p \). Let \( V_\ast(FG) \) be the unitary subgroup of the group of normalized units of \( FG \) with the classical involution \( \ast \). If \( H \) is an abelian \( p \)-group, then \( V_\ast(FG) \cong V_\ast(FH) \) if and only if \( G \cong H \).

For non-abelian 2-groups we provide the following two results:

**Theorem 2.** Let \( F \) be the field of 2 elements, and let \( G \) and \( H \) be finite 2-groups of maximal class. Then \( V_\ast(FG) \cong V_\ast(FH) \) if and only if \( G \cong H \).

**Theorem 3.** Let \( FG \) be the group algebra of a finite 2-group \( G \) of order at most 16 over the field \( F \) of 2 elements. Then \( V_\ast(FG) \cong V_\ast(FH) \) if and only if \( G \cong H \).

### 2. Isomorphism Problem of Unitary Units

Let \( G \) be a finite abelian \( p \)-group. If \( \text{char}(F) = p \), then (see in [8] Chapters 2-3, p. 194-196])

\[
V(FG) = \left\{ x = \sum_{g \in G} \alpha_g g \in FG \mid \chi(x) = \sum_{g \in G} \alpha_g = 1 \right\},
\]

where \( \chi(x) \) is the augmentation of the element \( x \in FG \).

We denote by \( G[p^i] \) the subgroup of the group \( G \) generated by elements of order \( p^i \), by \( \exp(G) \) the exponent of \( G \) and set \( G[p^i] = \langle g^{p^i} \mid g \in G \rangle \). Let us denote by \( f_i(G) \) the number of subgroups of order \( p^i \) in the decomposition of the abelian \( p \)-group \( G \) into a direct product of cyclic groups.

We use the following.

**Lemma 1.** ([11] Theorem 2) Let \( G \) be a finite abelian 2-group and \( |F| = 2^m \geq 2 \). Then \( V_\ast(FG) \) is a direct product of cyclic 2-groups, such that

(i) the 2-rank of \( V_\ast(FG) \) is equal to \( \frac{m}{2}(|G| + |G[2]| + |G[2]| - |G^2|) - m \);

(ii) \( V_\ast(FG) = G \times M \) and

\[
f_i(M) = t_0 - 2t_1 + t_2 - f_1(G) - f_2(G) + m(|G[2]| - 1),
\]

\[
f_i(M) = t_{i-1} - 2t_i + t_{i+1} - f_{i+1}(G),
\]

where \( t_i = \frac{m}{2}(|G[2]| - |G^2[2]|) \) and \( (i \geq 2) \);

(iii) \( |V_\ast(FG)| = |G[2]| \cdot 2^{\frac{m}{2}(|G| + |G[2]|) - m} \).

Now we are able to consider the following.

**Lemma 2.** Let \( G \) be a finite abelian \( p \)-group and \( |F| = p^m \geq p \) where \( p \) is odd. Then \( V_\ast(FG) \cong V_\ast(FH) \) if and only if \( G \cong H \).

**Proof.** If \( \exp(V_\ast(FG)) = p^e \) for some \( e \), then \( \exp(G) = p^e \) and by Theorem 1 in [11] we have

\[
f_i(V_\ast(FG)) = \frac{m}{2}(|G^{p^{i-1}} - 2|G^{p^i}| + |G^{p^i+1}|).
\]

Since \( V_\ast(FG) \cong V_\ast(FH) \), so \( f_i(V_\ast(FG)) = f_i(V_\ast(FH)) \) for all \( i > 1 \) and \( \exp(H) = p^e \). Moreover, it is easy to check
The unitary subgroup. A similar statement seems to be true for non-abelian group algebras.

Lemma 5. According to Lemma 2, the theorem is true for odd $p$. Assume that $V_*(FG) \cong V_*(FH)$ for two finite 2-groups $G$ and $H$, where $F$ is a finite field of characteristic 2. Then $|G| = |H|$ by Lemma 2.

The theorem follows immediately from Lemma 1 (iii) and Lemma 3 for groups of order 4.

\[ |G| - 2|G^p| + |G^{p^2}| = |H| - 2|H^p| + |H^{p^2}| \]

\[ \vdots \]

\[ |G^{p^i-1}| - 2|G^{p^i}| + |G^{p^{i+1}}| = |H^{p^i-1}| - 2|H^{p^i}| + |H^{p^{i+1}}| \]

\[ \vdots \]

\[ |G^{p^{s-1}}| - 2|G^{p^s}| + |G^{p^{s+1}}| = |H^{p^{s-1}}| - 2|H^{p^s}| + |H^{p^{s+1}}| \]

\[ |G^{p^{s-2}}| - 2|G^{p^{s-1}}| + |G^{p^s}| = |H^{p^{s-2}}| - 2|H^{p^{s-1}}| + |H^p| \]

\[ |G^{p^{s-1}}| = |H^{p^{s-1}}|. \]

A straightforward calculation gives $|G^p| = |H^p|$, so \( f_i(G) = f_i(H) \) for all $i$. \qed

The following lemma is a simple consequence of Theorem 1 in [12].

**Lemma 3.** Let $G$ be a finite abelian 2-group and $F$ is a finite field of characteristic 2, and $V_*(FG) = V(FG)$. Then one of the following conditions holds:

(i) $G$ is an elementary abelian 2-group;

(ii) $G$ is a cyclic group of order 4, and $|F| = 2$.

**Lemma 4.** Let $G$ be a finite abelian 2-group and $|F| = 2^m \geq 2$. If $V_*(FG) \cong V_*(FH)$, then $|G| = |H|$.

**Proof.** Suppose that $|G| = 2^n$. According to Lemma 1 (iii) we have

\[ |V_*(FG)| = |G^2[2]| \cdot |F|^{\frac{|G| + |G^2[2]|}{2} - 1}. \]

Therefore, the lemma is true for $n = 1, 2$. Assume that $|G[2]| = 2^e \geq 2$. Since

\[ |F|^{\frac{|G|}{2^e}} \leq |G^2[2]| \cdot |F|^{2e - 1 - 1} \cdot |F|^{\frac{|G|}{2^e}} = |G^2[2]| \cdot |F|^{\frac{|G| + |G^2[2]|}{2} - 1} = |V_*(FG)|, \]

we have $|F|^{\frac{|G|}{2^e}} \leq |V_*(FG)|$.

Now, the following inequalities prove our lemma

\[ |F|^{\frac{|G|}{2^e} - 1} < |F|^{\frac{|G|}{2^e}} \leq |V_*(FG)| \leq |F|^{\frac{|G|}{2} - 1} = |V(FG)|. \]

Clearly, $|V_*(FG)| = |V(FG)| = |F|^{\frac{|G|}{2} - 1}$ only in the case if $V_*(FG) = V(FG)$, so $\exp(G) = 2$ or $G$ is cyclic of order 4 and $|F| = 2$ by Lemma 3.

The previous lemma states that the order of $G$ is determined by the isomorphism class of the unitary subgroup. A similar statement seems to be true for non-abelian group algebras.

We use the following well-known lemma.

**Lemma 5.** If $G$ is a finite abelian 2-group of $\exp(G) = 2^e$, then $G^{2e - 1} \cong G^{2e - 1}[2]$. 

Now we are ready to prove our first result.

**Proof of Theorem 1.** According to Lemma 2 the theorem is true for odd $p$.

Assume that $V_*(FG) \cong V_*(FH)$ for two finite 2-groups $G$ and $H$, where $F$ is a finite field of characteristic 2. Then $|G| = |H|$ by Lemma 2.

The theorem follows immediately from Lemma 1 (iii) and Lemma 3 for groups of order 4.
First, suppose that the exponent of $V_s(FG)$ is equal to 2. The exponent of $G$ and $H$ are also equal to 2 which confirms the theorem.

Now, assume that the exponent of $V_s(FG)$ is equal to 4. Then the exponent of $G$ and $H$ are also equal to 4. According to Lemma 5 and the first part of Lemma 1 we have $|G|^2 + |G[2]| = |H|^2 + |H[2]|$. Using the third part of Lemma 1 we get $G^2[2] \cong H^2[2]$, so $G^2 \cong G^2[2] \cong H^2[2] \cong H^2$ by Lemma 5. It follows that $G \cong H$.

Assume that the exponent of $V_s(FG)$ is equal to $2e$, where $e$ is greater than 2. Then $t_e = \frac{m}{2}(|G^{2e}| - |G^{2e}[2]|) = 0$ and

$$t_{e+1} = \frac{m}{2}(|G^{2e+1}| - |G^{2e+1}[2]|) = 0.$$  

Furthermore, $t_{e-1} = \frac{m}{2}(|G^{2e-1}| - |G^{2e-1}[2]|) = 0$ by Lemma 5 and so

$$f_e(M) = t_{e-1} - 2t_e + t_{e+1} - f_{e+1}(G) = 0.$$  

Consequently, $\exp(M) < \exp(G)$ and $f_s(V_s(FG)) = f_s(G)$.

Using Lemma 1(ii), we obtain that

$$f_1(V_s(FG)) = t_0 - 2t_1 + t_2 - f_2(G) + m(|G[2]| - 1),$$
$$f_2(V_s(FG)) = t_1 - 2t_2 + t_3 - f_3(G) + f_2(G),$$
$$\vdots$$
$$f_i(V_s(FG)) = t_{i-1} - 2t_i + t_{i+1} - f_{i+1}(G) + f_i(G),$$
$$\vdots$$
$$f_{e-2}(V_s(FG)) = t_{e-3} - 2t_{e-2} - f_{e-1}(G) + f_{e-2}(G),$$
$$f_{e-1}(V_s(FG)) = t_{e-2} - 2t_{e-1} + t_e = t_{e-2} - f_e(G) + f_{e-1}(G),$$
$$f_e(V_s(FG)) = f_e(G).$$

It is easy to check that $\sum_{i=1}^{e-2} f_i(V_s(FG))$ is equal to

$$t_0 - t_1 + m(|G[2]| - 1) - t_{e-2} - f_{e-1}(G)$$
$$= \frac{m}{2}(|G| - |G[2]|) - \frac{m}{2}(|G^2| - |G^2[2]|)$$
$$+ m(|G[2]| - 1) - t_{e-2} - f_{e-1}(G)$$
$$= \frac{m}{2}(|G| + |G[2]| - |G^2| + |G^2[2]|) - m - t_{e-2} - f_{e-1}(G).$$

Since $f_i(V_s(FG)) = f_i(V_s(FH))$ for all $i \geq 1$, from Lemma 1(i) we obtain that

$$t_{e-2} + f_{e-1}(G) = t'_{e-2} + f_{e-1}(H),$$
where $t'_{e-2} = \frac{m}{2}(|H^{2e-2}| - |H^{2e-2}[2]|)$. Using the facts that $f_e(G) = f_e(H)$ and

$$t_{e-2} = \frac{m}{2} \left(2f_{e-1}(G)(2f_e(G) - 1)2^{f_e(G)} \right)$$
we conclude that $f_{e-1}(G) = f_{e-1}(H)$ and $t_{e-2} = t'_{e-2}$.

Similarly, for every $1 \leq s \leq e - 3$ we get that $\sum_{i=1}^{s} f_i(V_s(FG))$ is equal to

$$t_0 - t_1 + m(|G[2]| - 1) - t_s + t_{s+1} - f_{s+1}(G)$$
$$= \frac{m}{2}(|G| + |G[2]| - |G^2| + |G^2[2]|) - m - t_s + t_{s+1} - f_{s+1}(G).$$

Thus $f_s(G) = f_s(H)$ for all $1 \leq s \leq e$, which proves the theorem.□
3. Group algebras of 2-groups of maximal class

Let $G$ be a 2-group of maximal class. It is well-known that $G$ is one of the following groups: the dihedral $D_{2^{n+1}}$, the generalized quaternion $Q_{2^{n+1}}$, or the semidihedral group $D_{2^{n+1}}^\text{+}$, respectively. Set

$$D_{2^{n+1}} = \langle a, b_1 \mid a^{2^n} = 1, b_1^2 = 1, (a, b_1) = a^{-2}, n \geq 2 \rangle;$$
$$Q_{2^{n+1}} = \langle a, b_2 \mid a^{2^n} = 1, b_2^2 = a^{2^{n-1}}, (a, b_2) = a^{-2}, n \geq 2 \rangle;$$
$$D_{2^{n+1}}^\text{+} = \langle a, b_3 \mid a^{2^n} = 1, b_3^2 = 1, (a, b_3) = a^{-2+2^{n-1}}, n \geq 3 \rangle. \tag{2}$$

In the sequel of this paragraph we fix the cyclic subgroup $C = \langle a \mid a^{2^n} = 1 \rangle \cong C_{2^n}$ of $G$ from the list $[2]$ and fix the following automorphism of $FC$:

$$x (\in FC) \mapsto \tilde{x} = x_1 + x_2 a = x_1 + x_2 a^{1+2^{n-1}} \in FC,$$

in which $F$ is the field of two elements and $x_1, x_2 \in V(FC^2)$.

Using presentation $[2]$ we compute the number $\Theta_G(2)$ of involutions in $V_*(FG)$ for groups $D_{2^{n+1}}$ and $Q_{2^{n+1}}$.

Let $x = x_1 + x_2 b_1 \in V(FD_{2^{n+1}})$, where $x_1, x_2 \in FC$. It is easy to check that $x \in V_*(FC)[2]$ if and only if $x^* = x \in V(FC)[2]$. Therefore $x \in V_*(FD_{2^{n+1}})[2]$ if and only if $(x_1 + x_2 b_1)^2 = 1$ and $x_1 + x_2 b_1 = (x_1 + x_2 b_1)^* = x_1^* + x_2 b_1$, hence

$$\begin{cases}
  x_1^2 = x_2 x_2^* + 1; \\
  x_1 = x_1^*.
\end{cases} \tag{3}$$

Let $x = x_1 + x_2 b_2 \in V(FQ_{2^{n+1}})$, where $x_1, x_2 \in FC$. Then $x \in V_*(FQ_{2^{n+1}})[2]$ if and only if $(x_1 + x_2 b_2)^2 = 1$ and $x_1 + x_2 b_2 = (x_1 + x_2 b_2)^* = x_1^* + x_2 a^{2^{n-1}} b_2$, hence

$$\begin{cases}
  x_1^2 = x_2 x_2^* + 1; \\
  x_1 = x_1^*; \\
  x_2 = x_2 a^{2^{n-1}}.
\end{cases} \tag{4}$$

According to Lemma $[1]$ we have

$$|V_*(FC)| = |C^{2}[2]| \cdot 2^{\frac{1}{2}(|C|+|C[2]|)} = 2^{2^{n-1}+1}.$$

For each $0 \leq i < 2^n$ we define the set

$$H_i = \{ h \in V(FC) \mid hh^*(1 + a)^{i}(1 + a^{-1})^i \in FC^2 \}.$$

**Lemma 6.** [5] **Lemma 8**] The set $H_i$ has the following properties:

(i) If $i \geq 2^{n-1}$, then $H_i = V(FC)$.
(ii) If $i < 2^{n-1}$ is odd, then $H_i$ is empty.
(iii) If $l < 2^{n-2}$, then $H_2l \leq V(FC)$ and $|H_2l| = 2^{2^{n-2}+l}$.

The set of the $*$-symmetric elements in $V(FC)$ we denote by $S_*(FC)$.

**Lemma 7.** The group $S_*(FC)[2] = S_*(FC) \cap V(FC)[2]$ has order $2^{2^{n-2}+1}$.

**Proof.** If $x = \sum_{i=0}^{2^{n-1}-1} a_i a^i \in FC$, then $x^2 = \sum_{i=0}^{2^{n-1}-1} (a_i + a_{i+2^{n-1}}) a^{2i}$ and $x^* = a_0 + a_{2^{n-1}} a^{2^{n-1}} + \sum_{i=1}^{2^{n-1}-2} (a_i + a_{-i} \mod 2^n) a^i$. 

\[\sum_{i=0}^{2^{n-1}-1} a_i a^i \in FC, x^2 = \sum_{i=0}^{2^{n-1}-1} \]
It follows that each \( x \in S_*(FC)[2] \) can be written in the following form
\[
x = \alpha_0 + \alpha_{2^n-1}(2^{2n-2} + a^{2n-2}) + \alpha_{2^n-1}a^{2n-1} + \sum_{i=1}^{2^n-2} \alpha_i(a^i + a^{2i} + a^{-2i} + a^{-i}),
\]
so the number of all units in \( S_*(FC)[2] \) is equal to \( 2^{2n-2}+1 \). \( \square \)

**Lemma 8.** The number \( \Theta_{D_{2n+1}}(2) \) is equal to \( 2^{2n+2} - 2^{3 \cdot 2n-2}+1 \).

**Proof.** Let \( x_1 + x_2b_1 \in V_*(FD_{2n+1}) \) be an involution, where \( x_1, x_2 \in FC \), such that \( \chi(x_1) = 1 \) and \( \chi(x_2) = 0 \). Since \( x_2 \) is not a unit,
\[
x_2 \in \{ 0, \gamma(1+a)^i \mid \gamma \in V(FC), \ 0 < i < 2^{n-1} \}.
\]
For \( x_2 = 0 \), the number of different \( x_1 \) coincides with \( |S_*(FC)[2]| \) by (3). If \( x_2 = \gamma(1+a)^i \) for \( 0 < i < 2^{n-1} \), then the number of such different \( x_2 \) is \( |H_i|/|A_i| \), where \( A_i = \{ u \in V(FC) \mid u(1+a)^i \} \) by Lemma 3. It is easy to see that \( A_i = 1 + Ann((1+a)^i) \), where \( Ann((1+a)^i) \) is the annihilator of \( (1+a)^i \), so \( |A_i| = 2^i \) by (2).

If \( i \) is odd, then \( H_i \) is empty by Lemma 3 so there are no involutions. Furthermore, for \( i = 2k \), the number of different \( x_2 \) by Lemma 6 is equal to
\[
\frac{|H_{2k}|}{|A_{2k}|} = 2^{3 \cdot 2n-2}+k = 2^{3 \cdot 2n-2}-k.
\]

Suppose that \( x_1' + x_2b_1 \) is also an involution, such that \( \chi(x_1) = 1 \) and \( \chi(x_2) = 0 \). Then \( (x_1^{-1}x_1') = x_1^{-2}(x_1')^2 = 1 \) and \( x_1' = (x_1')^* \), so \( x_1' \in x_1S_*(FC)[2] \). Thus, for even \( 0 \leq i = 2k < 2^{n-1} \) the number of different units which satisfy (3) is
\[
\left( 1 + \sum_{k=1}^{2^{n-1}-1} \frac{|H_{2k}|}{|A_{2k}|} \right) \cdot |S_*(FC)[2]|
= 2^{2n-2}+1 + (2^{3 \cdot 2n-2}) (2^{2n-2} + 2^{2n-2-1} + \cdots + 2^2).
= 2^{2n-2}+1 + 2^2 (2^{3 \cdot 2n-2}) (2^{2n-2-1} - 1)
\]

Now, let \( 2^{n-1} \leq i < 2^n \). Clearly \( H_i = V(FC) \) and the number of different units of the form \( x_1 + x_2b_1 \) such that \( \chi(x_1) = 1 \) and \( \chi(x_2) = 0 \) is
\[
\sum_{i=2^{n-1}}^{2^n-1} \frac{|H_{2i}|}{|A_{2i}|} \cdot |S_*(FC)[2]| = \sum_{i=2^{n-1}}^{2^n-1} \frac{2^{n-1}}{2^i} \cdot (2^{2n-2}+1)
= \sum_{i=0}^{2^{n-1}-1} 2^i \cdot (2^{2n-2}+1) = (2^{2n-1} - 1) \cdot (2^{2n-2}+1).
\]

Consequently, the number of units of the form \( x_1 + x_2b_1 \) in \( V_*(FD_{2n+1}) \), such that \( \chi(x_1) = 0 \) and \( \chi(x_2) = 1 \) is equal to
\[
(2^{2n-1} - 1) \cdot (2^{2n-2}+1) + 2^{2n-2}+1 + 2^2 \cdot (2^{3 \cdot 2n-2} (2^{2n-2-1} - 1))
= (2^{2n-2}+1) \cdot (2^{2n-1}) + 2^2 \cdot (2^{3 \cdot 2n-2} (2^{2n-2-1} - 1))
= 2^{3 \cdot 2n-2} \cdot (2^{2n-2}+1 - 2).
\]

Now, consider the number of units of the form \( x_1 + x_2b_1 \in V_*(FD_{2n+1}) \), where \( x_1, x_2 \in FC \) such that \( \chi(x_1) = 0 \) and \( \chi(x_2) = 1 \). Clearly, \( x_2 \) is a unit and \( x_2x_2^* = (1 + x_1)^2 \) by (3), where \( 1 + x_1 \)
is a $*$-symmetric unit and $x_2x_3^* \in V(FC^2)$. For a fixed unit $x_2$ it is easy to proved that the set

$$L_{x_2} = \{1 + x_1 \in S_\ast(FC) \mid (1 + x_1)^2 = x_2x_2^\ast\}$$

is a coset of $S_\ast(FC)$ by $S_\ast(FC)[2]$. Therefore the number of different $x_1$ is $|S_\ast(FC)[2]|$.

Since the number of different $x_2$ coincides with $|H_0|$, the number of units in $V(FD_{2^n+1})$, such that $\chi(x_1) = 0$ and $\chi(x_2) = 1$ is equal to

$$|H_0| \cdot |S_\ast(FC)[2]| = 2^{3 \cdot 2^{n-2} + 2^n - 2} = 2^{2^n+1}.$$ 

Hence $\Theta_{D_{2^n+1}}(2) = 2^{2^n+2} - 2^{3 \cdot 2^{n-2}+1}$. \hfill \Box

**Lemma 9.** The number $\Theta_{Q_{2^n+1}}(2)$ is equal to $2^{3 \cdot 2^{n-2}+1}$.

**Proof.** Let $x_1 + x_2b_2 \in V_\ast(FQ_{2^n+1})$ be an involution, where $x_1, x_2 \in FC$ such that $\chi(x_1) = 0$ and $\chi(x_2) = 1$. According to equations (3) we have $x_2(1 + a^{2^{n-1}}) = 0$. Since $x_2$ is a unit we conclude that $(1 + a^{2^{n-1}}) = 0$ which is impossible, so we have no unit satisfying the given conditions.

Now, let $x_1 + x_2b_2 \in V_\ast(FQ_{2^n+1})$ be an involution, where $x_1, x_2 \in FC$ such that $\chi(x_1) = 1$ and $\chi(x_2) = 0$. Since $x_2$ is not a unit,

$$x_2 \in \{0, \gamma(1 + a)^i \mid \gamma \in V(FC), i > 0\}.$$ 

According to (3), we have $x_2(1 + a^{2^{n-1}}) = 0$ which holds if and only if either $x_2 = 0$ or $2^{n-1} \leq i$. If $2^{n-1} \leq i$, then (3) and (4) are equivalent. Therefore the number $\Theta_{Q_{2^n+1}}(2)$ of involutions in $V_\ast(FQ_{2^n+1})$ is equal to

$$\left(1 + \sum_{i=2^{n-1}} \frac{|H_i|}{|X_i|}\right) \cdot |S_\ast(FC)[2]| = (2^{2^{n-1}}) \cdot (2^{2^{n-2}+1}) = 2^{3 \cdot 2^{n-2}+1}. \hfill \Box$$

Let $x = x_1 + x_2b_3 \in V(FD_{2^n+1})$, where $x_1, x_2 \in FC$. Then $x \in V_\ast(FD_{2^n+1})[2]$ if and only if $(x_1 + x_2b_3)^2 = 1$ and $x_1 + x_2b_3 = (x_1 + x_2b_3)^* = x_1^* + \tilde{x}_2b_3$, hence

$$\begin{aligned}
  x_1^2 &= x_2x_2^* + 1; \\
  x_1 &= x_1^*; \\
  x_2 &= \tilde{x}_2. 
\end{aligned} \tag{5}$$

**Proof of Theorem 4.** Let us prove that

$$\Theta_{Q_{2^n+1}}(2) < \Theta_{D_{2^n-1}}(2) < \Theta_{D_{2^n+1}}(2), \tag{6}$$

where $\Theta_G(2)$ is the number of involutions in $V_\ast(FC)$.

First, let us prove the left inequality in (4). Let $x_1 + x_2b_3 \in V_\ast(FD_{2^n+1})$ be an involution, where $x_1, x_2 \in FC$ such that $\chi(x_1) = 1$ and $\chi(x_2) = 0$. If

$$x_2 \in \{0, \gamma(1 + a)^{2^{n-1}} \mid \gamma \in V(FC)\},$$

then (4) and (5) are equivalent, so $\Theta_{Q_{2^n+1}}(2) \leq \Theta_{D_{2^n-1}}(2)$.

Let $x_1 + x_2b_3 \in V_\ast(FD_{2^n-1})$ be an involution, where $x_1, x_2 \in FC$ such that $\chi(x_1) = 0$ and $\chi(x_2) = 1$. It turned out that there is no unit in $V_\ast(FQ_{2^n+1})$ that satisfies this conditions. However, the unit $b_3$ satisfies this conditions and $b_3$ is a unitary unit. Thus the left inequality of (4) holds.

Now, let us prove the right inequality in (4). If $x_2 = \tilde{x}_2$, then (4) and (5) are equivalent.
Let $x_1 + x_2 b_3 \in V_4(FD_2^3)$ be an involution, where $x_1, x_2 \in FC$ and $\chi(x_1) = 1$, $\chi(x_2) = 0$. It is easy to see that for $x_1 = 1 + a + a^{-1}$ and $x_2 = a + a^{-1}$ the element $x_1 + x_2 b_1 \in V_4(FD_2^3)$ but $x_1 + x_2 b_3 \not\in V_4(FD_2^3)$.

Now, let $x_1 + x_2 b_3 \in V_4(FD_2^3)$ be an involution, where $x_1, x_2 \in FC$ such that $\chi(x_1) = 0$ and $\chi(x_2) = 1$. Set $x_1 = 1 + a^{2n-1}$ and $x_2 = a$. Clearly, $x_1 + x_2 b_1 \in V_4(FD_2^3)$ but $x_1 + x_2 b_3 \not\in V_4(FD_2^3)$, so $\Theta_{D_2^{2n+1}}(2) < \Theta_{D_2^{2n+1}}(2)$.

4. UNITARY SUBGROUPS OF NON-COMMUTATIVE GROUP ALGEBRAS

Proof of Theorem 3. If $G \cong \{Q_8, D_8\}$, then $V_4(FG) \cong G \times C_2^3$ by [16, 10, 15].

Corollary 10 in [6] alleges that $V_4(FG)$ is Hamiltonian if and only if $G$ is Hamiltonian and the theorem holds.

Let $G$ be a non-abelian group of order 16. A generator set of unitary subgroups $V_4(FG)$ for groups $G$ of order $|G| = 16$ can be found in [9]. Based on these results we can describe the structure of the unitary subgroups of these group algebras.

Let $G = Q_8 \times C_2$ be the Hamiltonian group of order 16. The group $V_4(FG)$ is Hamiltonian [6, Corollary 10] if and only if $G$ is Hamiltonian. Moreover, $V_4(FG) \cong G \times C_2^2 \cong Q_8 \times C_2^3$ by [9].

Let $MD_{16}$ denotes the modular group $\langle a, b | a^8 = b^2 = 1, (a, b) = a^4 \rangle$. If $G \in \{MD_{16}, Q_{16}\}$, then $|V_4(FG)| = 2^{10}$ and $V_4(FMD_{16}) \not\cong V_4(FQ_{16})$ by [9, Example 3, 10].

For $G = MD_{16}$ we have

$$V_4(FG) \cong (G \times C_2^3) \times C_2^2 = (\langle a, b \rangle \ltimes \langle c_1, c_2, c_3 \rangle) \times C_2^2,$$

in which $(c_1, a) = (c_3, a) = (c_3, a) = c_3 c_4$, $(c_1, b) = c_2 c_3$ and $(c_2, b) = (c_3, b) = 1$. It yields that $V_4(FMD_{16}) \cong G' \times C_2 \times C_2 \cong C_2^3$.

If $G = Q_{16}$, then we have

$$V_4(FG) \cong (G \times C_2^3) \times C_2^2 = (\langle a, b \rangle \ltimes \langle c_1, \ldots, c_4 \rangle) \times C_2^2,$$

in which $(c_1, a) = (c_2, a) = c_1 c_2$, $(c_3, a) = c_4 c_3$, $(c_1, b) = c_2 b$ and $(c_3, b) = c_3 c_4$. This yields that $V_4(FQ_{16}) \cong C_4 \times C_2^2$, so $V_4(FMD_{16})$ is not isomorphic to $V_4(FQ_{16})$.

Let $G \in \{C_4 \ltimes C_4, D_{16}^-, D_8 \ltimes C_4\}$. Then $|V_4(FG)| = 2^{11}$ (see [9, 19]). Using the relations in [9] we prove that these unitary subgroups are not isomorphic groups. If $G = C_4 \ltimes C_4$, then by [9, Example 9] we get

$$V_4(FG) \cong (G \times C_2^3) \times C_2^3 = (\langle a, b \rangle \ltimes \langle c_1, \ldots, c_4 \rangle \times C_2^3,$$

in which $(c_1, a) = (c_1, b) = (c_4, a) = (c_4, b) = 1$, $(c_2, a) = (c_3, a) = c_1 c_2 c_3$, $(c_4, a) = c_1$, $(c_2, b) = (c_3, b) = c_2 c_3$ and $(c_4, a) = 1$. This yields that $V_4(FG) \cong G' \times C_2^3 \cong C_2^4$.

If $G = D_{16}^-$, then by [10, Theorem 4] we have

$$V_4(FG) \cong G \times C_2^3 = \langle a, b \rangle \ltimes \langle c_1, \ldots, c_7 \rangle,$$

in which $(c_1, a) = c_2 c_4 c_5 c_7$, $(c_2, a) = (c_3, a) = 1$, $(c_4, a) = (c_6, a) = c_5 c_6$, $(c_5, a) = (c_7, a) = c_5 c_7$, $(c_1, b) = c_2 c_3 c_5 c_6 c_7$, $(c_2, b) = (c_3, b) = (c_4, b) = (c_6, b) = 1$ and $(c_3, b) = (c_7, b) = c_5 c_7$. Moreover, $V_4(FG) \cong C_4 \times C_2^3$.

If $G = D_8 \ltimes C_4$, then $V_4(FG) \cong G \times C_2^3$ and $V_4(FG) \cong C_2$ by [9, Example 5].

Since each pairwise of $V_4(FG)$ of the groups $\{C_4 \ltimes C_4, D_{16}^-, D_8 \ltimes C_4\}$ are not isomorphic groups, the proof is done.
Let $G \in \{D_{16}, G(4, 4)\}$, where $G(4, 4) = \langle a, b, c | a^4 = b^2 = c^2 = 1, (a, b) = 1, (a, c) = b, (b, c) = 1 \rangle$. Then $|V_u(FG)| = 2^{12}$ by [10] [9] [19]. Using the relations in [10] and [9] Example 9 we prove that these unitary subgroups are not isomorphic groups.

If $G = (a, c) \times \langle b \rangle \cong D_8 \times C_2$, then

$$V_u(FG) \cong (G \rtimes C_2^6) \times C_2^2 = \langle a, b, c \rangle \rtimes \langle d_1, \ldots, d_6 \rangle \times C_2^2$$

in which $(d_1, a) = (d_2, a) = 1$, $(d_3, a) = (d_4, a) = d_5d_4$, $(d_5, a) = (d_6, a) = d_5d_6$, $(d_1, c) = (d_2, c) = d_1d_2$, $(d_3, c) = (d_4, c) = 1$ and $(d_5, c) = (d_6, c) = d_5d_6$. Since $b$ is a central element, $G' \cong G \rtimes C_2^6 \times C_2^3 \cong C_4^3 \times C_2^3$. Therefore the corresponding unitary subgroups are not isomorphic groups.

If $G = D_8 \times C_2$, then $V_u(FG) \cong G \rtimes C_2^6 \times C_2^3$ by [11] Example 8, so $|V_u(FG)| = 2^{13}$. □

References

[1] C. Bańk-śki. The isomorphism question for modular group algebras of metacyclic $p$-groups. Proc. Amer. Math. Soc., 104(1):39–42, 1988.

[2] C. Bańk-śki. Modular group algebras of 2-groups of maximal class. Comm. Algebra, 20(5):1229–1241, 1992.

[3] C. Bańk-śki and A. Caranti. The modular group algebras of $p$-groups of maximal class. Canad. J. Math., 40(6):1422–1435, 1988.

[4] Z. Balogh and A. Bovdi. Group algebras with unit group of class $p$. Publ. Math. Debrecen, 65(3-4):261–268, 2004.

[5] Z. Balogh and A. Bovdi. On units of group algebras of 2-groups of maximal class. Comm. Algebra, 32(8):3227–3245, 2004.

[6] Z. Balogh, L. Creedon, and J. Gildea. Involutions and unitary subgroups in group algebras. Acta Sci. Math. (Szeged), 79(3-4):391–400, 2013.

[7] S. D. Berman. Group algebras of countable abelian $p$-groups. Publ. Math. Debrecen, 14:365–405, 1967.

[8] A. Bovdi. The group of units of a group algebra of characteristic $p$. Publ. Math. Debrecen, 52(1-2):193–244, 1998.

[9] A. Bovdi and L. Erdei. Unitary units in modular group algebras of groups of order 16. Technical Reports, Universitas Debrecen, Dept. of Math., L. Kossuth Univ., 4(157):1–16, 1996.

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

[11] A. Bovdi and A. Szakács. Units of commutative group algebra with involution. Publ. Math. Debrecen, 69(3):291–296, 2006.

[12] A. A. Bovdi. Unitarity of the multiplicative group of an integral group ring. Mat. Sb. (N.S.), 119(161)(3):387–400, 448, 1982.

[13] V. Bovdi and L. G. Kovács. Unitary units in modular group algebras. Manuscripta Math., 84(1):57–72, 1994.

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

[15] L. Creedon and J. Gildea. Unitary units of the group algebra $\mathbb{F}_{2^k}Q_8$. Internat. J. Algebra Comput., 19(2):283–286, 2009.

[16] L. Creedon and J. Gildea. The structure of the unit group of the group algebra $\mathbb{F}_{2^k}D_8$. Canad. Math. Bull., 54(2):237–243, 2011.

[17] W. E. Deskins. Finite Abelian groups with isomorphic group algebras. Duke Math. J., 23:35–40, 1956.
[18] V. Drensky. The isomorphism problem for modular group algebras of groups with large centres. In Representation theory, group rings, and coding theory, volume 93 of Contemp. Math., pages 145–153. Amer. Math. Soc., Providence, RI, 1989.

[19] J. Gildea. Units of group algebras of non-abelian groups of order 16 and exponent 4 over $\mathbb{F}_{2^k}$. Results Math., 61(3-4):245–254, 2012.

[20] E. T. Hill. The annihilator of radical powers in the modular group ring of a $p$-group. Proc. Amer. Math. Soc., 25:811–815, 1970.

[21] W. May. The isomorphism problem for modular abelian $p$-group algebras. J. Algebra Appl., 13(4):1350125, 14, 2014.

[22] M. A. Salim and R. Sandling. The unit group of the modular small group algebra. Math. J. Okayama Univ., 37:15–25 (1996), 1995.

[23] M. A. Salim and R. Sandling. The modular group algebra problem for groups of order $p^5$. J. Austral. Math. Soc. Ser. A, 61(2):229–237, 1996.

[24] M. A. Salim and R. Sandling. The modular group algebra problem for small $p$-groups of maximal class. Canad. J. Math., 48(5):1064–1078, 1996.

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

[26] R. Sandling. The modular group algebra of a central-elementary-by-abelian $p$-group. Arch. Math. (Basel), 52(1):22–27, 1989.

[27] R. Sandling. The modular group algebra problem for metacyclic $p$-groups. Proc. Amer. Math. Soc., 124(5):1347–1350, 1996.

[28] M. Wursthorn. Isomorphisms of modular group algebras: an algorithm and its application to groups of order $2^6$. J. Symbolic Comput., 15(2):211–227, 1993.

Department of Mathematical Sciences, UAEU, United Arab Emirates

E-mail address: {baloghzsa,vbovdi}@gmail.com