International Electronic Journal of Algebra
Volume 29 (2021) 187-198
DOI: 10.24330/ieja.852199

ON UNITARY SUBGROUPS OF GROUP ALGEBRAS

Zsolt Adam Balogh

Received: 10 April 2020; Revised: 7 June 2020; Accepted: 9 June 2020
Communicated by Burcu Üngör

Abstract. Let FG be the group algebra of a finite p-group G over a finite field F of characteristic p and let $*$ be the classical involution of FG. The $*$-unitary subgroup of FG, denoted by $V_*(FG)$, is defined to be the set of all normalized units u satisfying the property $u^* = u^{-1}$. In this paper we give a recursive method how to compute the order of the $*$-unitary subgroup for certain non-commutative group algebras. A variant of the modular isomorphism question of group algebras is also considered.

Mathematics Subject Classification (2020): 16S34, 16U60
Keywords: Group ring, group of units, unitary subgroup

1. Introduction and results

Let FG be the group algebra of a finite p-group G over a finite field F of positive characteristic p. Let $V(FG)$ denotes the group of normalized units in FG. The description of the structure of $V(FG)$ is a central problem in the theory of group algebras and it has been investigated by several authors. For an excellent survey on this topic we refer the reader to [8].

An element $u \in V(FG)$ is called *unitary* if $u^* = u^{-1}$, with respect to the classical $*$-involution of FG (the linear extension of the involution on G which sends each element of G to its inverse). The set of all unitary elements of $V(FG)$ forms a subgroup of $V(FG)$ which is denoted by $V_*(FG)$ and is called $*$-unitary subgroup. The group $V_*(FG)$ plays an important role of studying the structure of the group of units of group algebras and has been investigated in several papers (see [4], [5], [9], [10], [11], [12], [15], [16], [18] and [19]). Let L be a finite Galois extension of F with Galois group G, where F is a finite field of characteristic two. Serre [21] has showed that there is a relation between the self-dual normal basis of L over F and the unitary subgroup of FG. This application gives a hard reason to continue studying of the unitary subgroups.

The research was supported by UAEU Research *Start-up Grant No. G00002968.*

The order of $*$-unitary subgroup when G is a p-group and p is an odd prime is given in [13] and [14]. To compute the order of $V_*(FG)$ when G is a 2-group and $p=2$ is an open and is a particularly challenging problem. It is to be expected that the order is divisible by $|F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$, where $G\{2\}$ is the set of elements of order two in G with the unit element. In [14] this conjecture was confirmed when G is an abelian 2-group and F is a finite field of characteristic 2. For dihedral and generalized quaternion 2-groups G, where F is a finite field of characteristic 2 it was confirmed in [13]. In our paper we present a recursive method how to compute the order of $V_*(FG)$ and confirm the conjecture above.

The modular isomorphism problem is an old and unanswered problem in the theory of group representation. A stronger variant of the problem is said to be the *isomorphism problem of normalized units* (UIP) is due to Berman [7]. Let F be a finite field of characteristic p, let G and H be finite p-groups such that $V(FG)$ and $V(FH)$ are isomorphic. One may ask whether G and H are isomorphic groups? The studies in [1] and [2] resulted in proving the conjecture for some group classes. The $*$-unitary group of a group algebra is a small subgroup in $V(FG)$ so it is interesting to ask whether this smaller subgroup determines the basic group G or not. This problem is called the *$*$-unitary isomorphism problem* (*-UIP). Recently, the $*$-unitary isomorphism problem was solved for some classes of non-abelian groups in [3].

Define the following 2-groups: the dihedral $D_{2^{n+1}}$, the generalized quaternion $Q_{2^{n+1}}$, the semidihedral group $D^-_{2^{n+1}}$ the modular group $M_{2^{n+1}}$ and H_{2^n}, respectively:

$$\begin{aligned}
D_{2^{n+1}} &= \langle\ a,b \mid a^{2^n}=1, b^2=1, (a,b)=a^{-2}\ \rangle; && (n\geq 2)\\
Q_{2^{n+1}} &= \langle\ a,b \mid a^{2^n}=1, b^2=a^{2^{n-1}}, (a,b)=a^{-2}\ \rangle; && (n\geq 2)\\
D^-_{2^{n+1}} &= \langle\ a,b \mid a^{2^n}=1, b^2=1, (a,b)=a^{-2+2^{n-1}}\ \rangle; && (n\geq 3)\\
M_{2^{n+1}} &= \langle\ a,b \mid a^{2^n}=1, b^2=1, (a,b)=a^{2+2^{n-1}}\ \rangle; && (n\geq 3)\\
H_{2^n} &= \langle\ a,b,c \mid a^{2^{n-2}}=b^2=c^2=1, (a,b)=c,\\
&\qquad (a,c)=(b,c)=1\ \rangle, && (n\geq 4)
\end{aligned} \tag{1}$$

where $(a,b):=a^{-1}b^{-1}ab$.

Let G be a finite 2-group. We denote by $G[2^i]$ the subgroup of G generated by elements of order 2^i. We use the notation G^{2^i} for the subgroup $\langle\ g^{2^i} \mid g\in G\ \rangle$. Set $\Omega\{G\}=\{g^2 \mid g\in G\}$. Let $\zeta(G)$ and G' be the center and the commutator subgroup of G, respectively.

Let Θ denote the class of all groups with the property that $g^h := h^{-1}gh = g^{\pm 1}$ for all $g \in G \setminus G\{2\}$ and $h \in G$, which does not commute with g. It is clear that each abelian group, the dihedral $D_{2^{n+1}}$ and generalized quaternion $Q_{2^{n+1}}$ groups belong to the class Θ.

Theorem 1.1. *Let F be a field with $|F| = 2^m \geq 2$ and let G be a finite 2-group. If $C = \langle\, c \mid c \in \zeta(G)[2] \setminus \Omega\{G\}\,\rangle$ such that $G/C \in \Theta$, then*

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot |V_*(F[G/C])|.$$

Corollary 1.2. *Let F be a field with $|F| = 2^m \geq 2$ and let $G = H \times E$ be a finite 2-group, in which E is a finite elementary abelian 2-group and $H \in \Theta$. If*

$$|V_*(FH)| = n \cdot |F|^{\frac{1}{2}(|H|+|H\{2\}|)-1}$$

for some $n \in \mathbb{N}$, then $|V_*(FG)| = n \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$. Moreover, if $H \in \{D_{2^s}, Q_{2^s} \mid s > 2\}$ then $n = \begin{cases} 1 & if \quad H = D_{2^s}; \\ 4 & if \quad H = Q_{2^s}. \end{cases}$

Corollary 1.3. *Let $G = H_{2^n}$ with $n \geq 4$. If $|F| = 2^m \geq 2$, then*

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

Let us denote by $D_8 \curlyvee C_4$ the central product of the dihedral group D_8 and the cyclic group C_4.

Theorem 1.4. *Let G be a finite non-abelian 2-group of order $|G| = 2^4$. If F is a field with $|F| = 2^m \geq 2$, then $|V_*(FG)| = n \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$, where*

(i) $n = 1$ *if* $G \in \{D_8 \curlyvee C_4, D_{16}, D_8 \times C_2\}$;

(ii) $n = 2$ *if* $G \in \{M_{16}, D_{16}^{-}, H_{16}\}$;

(iii) $n = 4$ *if* $G \in \{Q_{16}, C_4 \ltimes C_4, Q_8 \times C_2\}$.

Theorem 1.5. *Let G and H be non-abelian 2-groups of order at most 2^4. If F is a finite field of characteristic two, then the isomorphism $V_*(FG) \cong V_*(FH)$ implies the following isomorphism $G \cong H$.*

2. Notations and preliminaries

Let G be a finite p-group. If $char(F) = p$, then (see [8, Chapters 2-3, p. 194-196])

$$V(FG) = \Big\{\ x = \sum_{g \in G} \alpha_g g \in FG \ \mid\ \chi(x) = \sum_{g \in G} \alpha_g = 1\ \Big\},$$

where $\chi(x)$ is the augmentation of the element $x \in FG$. Let supp(x) denote the support of $x \in FG$ and $x^g = g^{-1}xg$, where $g \in G$. We define $\widehat{C} := \sum_{g \in C} g$, where

C is a subset of G. Throughout this paper $|S|$ denotes the cardinality of a finite set S and $|g|$ the order of $g \in G$.

The following two lemmas will be useful.

Lemma 2.1. ([17, Theorem 2]) *Let $|F| = 2^m \geq 2$. If G is a finite abelian 2-group, then*

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

Lemma 2.2. ([13, Corollary 2]) *If $|F| = 2^m \geq 2$, then*

(i) $|V_*(FG)| = |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$ *if G is a dihedral 2-group;*

(ii) $|V_*(FG)| = 4 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$ *if G is a generalized quaternion 2-group.*

Let H be a normal subgroup of G and $I(H) := \langle\, 1+h \ \mid\ h \in H\,\rangle_{FG}$ be the ideal of FG generated by the set $\{1+h \mid h \in H\}$. Moreover, for the natural homomorphism $\Psi : FG \to F[G/H]$ we have that $FG/I(H) \cong F[G/H]$ and $\ker(\Psi) = I(H)$. Let us denote by $V_*(F\overline{G})$ the unitary subgroup of the factor algebra $FG/I(H)$, where $\overline{G} = G/H$. It is easy to check that the set

$$N^*_\Psi = \{x \in V(FG) \mid \Psi(x) \in V_*(F\overline{G})\}$$

forms a subgroup in $V(FG)$. Furthermore, the set $I(H)^+ = \{1 + x \,|\, x \in I(H)\}$ forms a normal subgroup in $V(FG)$. It is obvious that $S_H := \langle\, xx^* \mid x \in N^*_\Psi\,\rangle$ is a subgroup of $I(H)^+$, because $xx^* \in 1 + \ker(\Psi) = I(H)^+$ for $x \in N^*_\Psi$.

Lemma 2.3. *Let H be a normal subgroup of order two in a finite 2-group G and let $|F| = 2^m \geq 2$. If S_H is central in N^*_Ψ, then*

$$|V_*(FG)| = |F|^{\frac{1}{2}|G|} \cdot \tfrac{|V_*(F\overline{G})|}{|S_H|}. \tag{2}$$

Proof. Let $\Phi(x) = xx^*$ for each $x \in V(FG)$. The map $\Phi : V(FG) \to V(FG)$ is not necessary a group homomorphism on $V(FG)$. However, S_H being central in N^*_Ψ implies that the restriction $\Phi|_{N^*_\Psi}$ is a homomorphism. Since $N^*_\Psi / \ker(\Phi|_{N^*_\Psi}) \cong S_H$,

$$|\ker(\Phi|_{N^*_\Psi})| = |V_*(FG)| = \tfrac{|N^*_\Psi|}{|S_H|} = \tfrac{|I(H)^+|\cdot|V_*(F\overline{G})|}{|S_H|}.$$

Evidently, $I(H)$ can be considered as a vector space over F with the following basis $\{u(1+h) \mid u \in T(G/H),\ h \in H\}$, where $T(G/H)$ is a complete set of left coset representatives of H in G. Thus we have that $|I(H)^+| = |F|^{\frac{1}{2}|G|}$ and (2) holds. □

Let $|F| = 2^m \geq 2$. Let C be a central subgroup of a 2-group G. We denote by $V_{g_1,\dots,g_n}$ the vector space in FG over F spanned by elements $\alpha_1 g_1 \widehat{C}, \dots, \alpha_n g_n \widehat{C}$, where $g_1, \dots, g_n \in G$ and $\alpha_1, \dots, \alpha_n \in F$. Set the following subgroup of G:

$$G_{g_1,\dots,g_n} := \langle\, 1 + \alpha_1 g_1 \widehat{C}, \dots, 1 + \alpha_n g_n \widehat{C} \mid \alpha_i \in F\,\rangle.$$

Lemma 2.4. *The set* $1+V_{g_1,\dots,g_n}$ *coincides with* $G_{g_1,\dots,g_n}$.

Proof. If $x_1, x_2 \in FG$, then the proof follows from the fact that

$$1+(x_1+x_2)\widehat{C} = 1+x_1\widehat{C}+x_2\widehat{C} = (1+x_1\widehat{C})(1+x_2\widehat{C}). \qquad \square$$

Lemma 2.5. *Let* $|F| = 2^m \geq 2$. *If* G *is a finite* 2*-group, then*

$$\operatorname{supp}(xx^*)\cap G\{2\} = \{1\} \qquad\qquad (x \in V(FG)).$$

Proof. If $x = \sum_{i=1}^{|G|} \alpha_i g_i \in V(FG)$, then

$$xx^* = 1 + \sum_{1\leq i<j\leq |G|} \alpha_i\alpha_j\big(g_ig_j^{-1} + (g_ig_j^{-1})^{-1}\big).$$

Obviously, $g_ig_j^{-1} + (g_ig_j^{-1})^{-1} = 0$ for $g_ig_j^{-1} \in G\{2\}$. $\square$

Lemma 2.6. *Let* $|F| = 2^m \geq 2$. *Let* $H = \langle\ c \mid c^2 = 1\ \rangle$ *be a central subgroup of a finite* 2*-group* G. *If* $1+g\widehat{H} \in S_H$ *for some* $g \in G$*, then* $g^2 = c$.

Proof. Assume that $1+g\widehat{H} \in S_H$ for some $g \in G$. Since S_H contains only $*$-symmetric elements, $1+g\widehat{H} = 1+g^{-1}\widehat{H}$, so

$$(g+g^{-1})\widehat{H} = g+gc+g^{-1}+g^{-1}c = 0.$$

The case $|g| = 2$ is impossible by Lemma 2.5. Thus, $g = g^{-1}c$ and $g^2 = c$. $\square$

Lemma 2.7. *Let* $|F| = 2^m \geq 2$ *and let* G *be a finite* 2*-group. For each subgroup* $H = \langle\ c \in \zeta(G) \mid c^2 = 1\ \rangle$ *of* G *we define the set* $H_c := \{g \in G \mid g^2 = c\}$. *Then*

$$S_H = \langle\ 1+\alpha_g g\widehat{H}, \quad 1+\beta_h(h+h^{-1})\widehat{H} \quad \mid \quad g \in H_c, h \notin H_c, \quad \alpha_g, \beta_h \in F\ \rangle.$$

Proof. Obviously, $gh+(gh)^{-1} = gh(1+(gh)^{-2})$, so $S_H \subseteq I(H)^+$ and S_H contains only $*$-symmetric elements. Thus each $x \in S_H$ can be expressed (see Lemma 2.5 and Lemma 2.6) in the following form

$$x = 1+\sum_{g\in H_c}\alpha_g g\widehat{H} + \sum_{h\notin H_c}\beta_h(h+h^{-1})\widehat{H}.$$

Since $(1+x_1\widehat{H})(1+x_2\widehat{H}) = 1+(x_1+x_2)\widehat{H}$ for each $x_1, x_2 \in FG$, the proof is done. $\square$

Lemma 2.8. *Let* $|F| = 2^m \geq 2$ *and let* G *be a finite* 2*-group. If* $H \leq \zeta(G)$ *has order 2, then* $1+\alpha(g+g^{-1})\widehat{H} \in S_H$ *for all* $g \in G$ *such that* $g^2 \notin H$.

Proof. Let $g \in G$ such that $g^2 \notin H$. Since $g \neq g^{-1}$ and $1+\alpha g\widehat{H} \in \ker(\Psi)$,

$$(1+\alpha g\widehat{H})(1+\alpha g\widehat{H})^* = 1+\alpha(g+g^{-1})\widehat{H}, \qquad (\alpha \in F)$$

which proves the lemma. $\square$

3. Proofs of Theorems

Proof of Theorem 1.1. If $c \in \zeta(G)[2] \setminus \Omega\{G\}$, then (see Lemmas 2.4, 2.5 and 2.8)

$$S_C = \langle\, 1 + \alpha(g + g^{-1})\widehat{C} \mid \alpha \in F,\ g \in G \setminus G\{2\} \,\rangle.$$

Furthermore, $h^{-1}(g + g^{-1})\widehat{C}h = (g + g^{-1})\widehat{C}$ for all $h \in G$, because $\overline{G} \in \Theta$. Now using Lemma 2.3 we have that

$$|V_*(FG)| = |F|^{\frac{1}{2}|G|} \cdot \frac{|V_*(F\overline{G})|}{|F|^{\frac{1}{4}(|G|-|G\{2\}|)}} = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot |V_*(F\overline{G})|. \qquad \square$$

Proof of Corollary 1.2. Let $G = H \times E$, where $H \in \Theta$, E is an elementary abelian 2-group and $|E| = 2^m \geq 1$. Now, we proceed by induction on the order of E.

For the base case ($m = 0$) we have that $|V_*(FH)| = n \cdot |F|^{\frac{1}{2}(|H|+|H\{2\}|)-1}$ for some n.

Let $m \geq 1$. If $C = \langle\, c \mid 1 \neq c \in E \,\rangle$, then $N := G/C \cong H \times E_1$ in which $|E_1| = 2^{m-1}$. Obviously, $N \in \Theta$ and using Theorem 1.1 we conclude that

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)}|V_*(FN)|,$$

where $|V_*(FN)| = n \cdot |F|^{\frac{1}{2}(|N|+|N\{2\}|)-1}$. Since $|G| + |G\{2\}| = 2(|N| + |N\{2\}|)$,

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot n \cdot |F|^{\frac{1}{2}(|N|+|N[2]|)-1} = n \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}.$$

The second sentence follows immediately from the fact that D_{2^s} and Q_{2^s} belong to Θ for every $s > 2$. $\square$

Proof of Corollary 1.3. Let $G' = \langle\, c \,\rangle$ (see (1)). Clearly,

$$c \in \zeta(G)[2] \setminus \Omega(G) \quad \text{and} \quad \overline{G} = G/G' \cong C_{2^{n-2}} \times C_2 \in \Theta.$$

Therefore $|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)}\big|V_*(F\overline{G})\big|$ by Theorem 1.1 and

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot 2 \cdot |F|^{\frac{1}{4}(|G|+|G\{2\}|)} = 2 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$$

by Lemma 2.1 and the fact that $|G\{2\}| = 2|\overline{G}[2]|$. $\square$

Lemma 3.1. *Let $G = (C_4 \rtimes C_4) \times E$, where E is a finite elementary abelian 2-group. If $|F| = 2^m \geq 2$, then $|V_*(FG)| = 4 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$.*

Proof. Let $G = \langle\, a, b \,\rangle \cong C_4 \rtimes C_4$. If $C = \langle\, a^2b^2 \,\rangle$, then $a^2b^2 \in \zeta(G)[2] \setminus \Omega\{G\}$ and $\overline{G} = G/C \cong Q_8 \in \Theta$. Now using Theorem 1.1, we obtain that

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)}|V_*(FQ_8)|.$$

According to Lemma 2.2 (ii) and the fact that $|G\{2\}| = 4$, we have that

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot 4 \cdot |F|^{\frac{1}{4}(|G|+|G\{2\}|)-1} = 4 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}.$$

Since $(C_4 \rtimes C_4) \in \Theta$, the proof follows from Corollary 1.2. □

Lemma 3.2. *If $|F| = 2^m \geq 2$, then the map $\tau : F \to F$, such that $\tau(x) = x^2 + x$ is a homomorphism on the additive group of F, in which* $\ker(\tau) = \{0, 1\}$.

Proof. Obviously,

$$\tau(x + y) = (x + y)^2 + (x + y) = x^2 + y^2 + x + y = \tau(x) + \tau(y) \qquad (x, y \in F)$$

and $x^2 + x = x(x + 1) = 0$ if and only if $x \in \{0, 1\}$. □

Consider the following system of equations over F with variables w_1, w_2, w_3, w_4:

$$\begin{cases} w_1 + w_2 + w_3 + w_4 = 1; \\ w_1w_4 + w_2w_3 = A; \\ w_1w_2 + w_3w_4 = 0, \qquad\qquad (A \in F). \end{cases} \tag{3}$$

Lemma 3.3. *Let $|F| = 2^m \geq 2$. If $\mathbb{S}$ is a subset of F consisting of all such $A \in F$ for which* (3) *has a solution in F, then $|\mathbb{S}| = \frac{1}{2}|F|$.*

Proof. First, we prove that $\mathbb{S} \subseteq \mathrm{im}(\tau)$ (see Lemma 3.2). Suppose that $A \in \mathbb{S}$ and $w_1, w_2, w_3, w_4 \in F$ satisfy the system (3). Then

$$\begin{aligned} \tau(w_1 + w_3) &= (w_1 + w_3)^2 + (w_1 + w_3) \\ &= (w_1 + w_3)(1 + w_1 + w_3) = (w_1 + w_3)(w_2 + w_4) = A. \end{aligned}$$

Thus for $w = w_1 + w_3$ we have $\tau(w) = A$ so $\mathbb{S} \subseteq \mathrm{im}(\tau)$.

Assume that $\tau(w) = A$ for some $w \in F$. If $w = 0$, then $\tau(w) = A = 0$ and $w_1 = 0, w_2 = 1, w_3 = 0, w_4 = 0$ is a solution of the equation system 3. Let $w_1 + w_3 = w \neq 0$ for some $w_1, w_3 \in F$. Set $w_2 = (A + w_1 + ww_1)w^{-1}$ and $w_4 = w_2 + w + 1$. It is clear that $w_1 + w_3 + w_2 + w_4 = w + w + 1 = 1$. Furthermore,

$$w_1w_2 + w_3w_4 = w_1w_2 + (w_1 + w)(w_2 + w + 1) = w_1(1 + w) + A + ww_2,$$

because $\tau(w) = w^2 + w = A$. Since $w_2 = (A + w_1 + ww_1)w^{-1}$ we can compute that $w_1(w + 1) + ww_2 + A = w_1(1 + w) + (A + w_1 + ww_1) + A = 0$. Thus we have proved that $w_1w_2 + w_3w_4 = 0$. Finally,

$$\begin{aligned} A = w(w + 1) &= (w_1 + w_3)(w_2 + w_4) \\ &= w_1w_2 + w_1w_4 + w_2w_3 + w_3w_4 = w_1w_4 + w_2w_3, \end{aligned}$$

which shows that $\mathrm{im}(\tau) = \mathbb{S}$. The proof is complete. □

Lemma 3.4. *Let* $G = \langle\, a, b \,\rangle \cong D_{16}^{-}$ *(see* (1)*). If* $|F| = 2^m \geq 2$*, then*

$$|V_*(FD_{16}^{-})| = 2 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}.$$

Proof. Clearly, $\zeta(G) = \langle\, a^4 \,\rangle$ and $N = \langle\, a^2 \,\rangle$ is normal in G. Furthermore, each $x \in FG$ can be written as $x = x_1 + x_2 a + x_3 b + x_4 ab$ with $x_i \in FN$ and

$$xx^* = \big(x_1x_1^* + x_2x_2^* + x_3x_3^* + x_4x_4^*\big) + (x_2x_1^* + x_4x_3^*)a \\ + (x_1x_2^* + x_3x_4^*)a^7 + (x_1x_4^* + x_2x_3^*)(a + a^5)b.$$

Set $w_i = \chi(x_i)$. If $xx^* \in S_{\zeta(G)}$, then $w_1+w_2+w_3+w_4 = 1$ and $w_1w_2+w_3w_4 = 0$ by the previous formula. Therefore if $xx^* \in S_{\zeta(G)}$, then there exist $w_1, w_2, w_3, w_4 \in F$ satisfying the system (3), for some $A \in \mathbb{S}$.

Let $C := \zeta(G)$ and $M = \{g \in G \mid g^2 = a^4\} = \{a^2, a^6, ab, a^3b, a^5b, a^7b\}$. Each $*$-symmetric element of $I(C)^+$ (see Lemma 2.7) can be written as

$$1 + \alpha_1(a + a^{-1})\widehat{C} + \alpha_2 a^2\widehat{C} + \alpha_3 ab\widehat{C} \\ + \alpha_4 a^3 b\widehat{C} + \alpha_5 b + \alpha_6 a^2 b + \alpha_7 a^4 b + \alpha_8 a^6 b, \qquad (\alpha_i \in F).$$

According to Lemma 2.8, $1 + \alpha(a + a^{-1})\widehat{C} \in S_C$ for any $\alpha \in F$. It follows that $1 + \alpha g \notin S_C$ if $g \in G\{2\}$ by Lemma 2.5.

Since $\delta + \delta a^2 + a \in V(FG)$ for every $\delta \in F$, an easy computation shows that

$$\big(\delta + \delta a^2 + a\big)\big(\delta + \delta a^2 + a\big)^* = 1 + \delta^2(a^2 + a^{-2}) = 1 + \delta^2 a^2\widehat{C},$$

which confirm that $\delta + \delta a^2 + a \in N_\Psi^*$. Obviously, $\eta(\alpha) = \alpha^2$ is an automorphism of $U(F)$, so we can pick δ such that $\alpha_2 = \delta^2$. Therefore $1 + \alpha_2 a^2\widehat{C} \in S_C$ for every $\alpha_2 \in F$.

A straightforward computation shows that

$$\big(\alpha(a + a^7) + b\big)\big(\alpha(a + a^7) + b\big)^* = 1 + \alpha^2 a^2\widehat{C} + \alpha(ab + a^3b)\widehat{C}$$

for every $\alpha \in F$ so $\alpha(a + a^7) + b \in N_\Psi^*$. Using Lemma 2.4 and the fact that $1 + \alpha_2 a^2\widehat{C} \in S_C$, we have that $1 + \alpha(ab + a^3b)\widehat{C} \in S_C$ for every $\alpha \in F$.

We have proved that the group N_1 generated by the set

$$\{1 + \alpha_1(a + a^{-1})\widehat{C}\} \cup \{1 + \alpha_2 a^2\widehat{C}\} \cup \{1 + \alpha_3(ab + a^3b)\widehat{C}\}, \qquad (\alpha_i \in F)$$

is a subgroup of S_C by Lemma 2.4 and $|N_1| = |F|^3$.

Let $u = w_1 + w_2 a + w_3 b + w_4 ab \in FD_{16}^{-}$, such that $w_1, w_2, w_3, w_4 \in F$ satisfy the system (3). It is easy to check that

$$uu^* = 1 + (w_1w_4 + w_2w_3)ab\widehat{C}$$

and $N_2 = \langle\ 1 + \alpha ab\widehat{C} \mid \alpha \in \mathbb{S}\ \rangle$ is a subgroup of S_C with order $|N_2| = \frac{1}{2}|F|$ by Lemma 3.3. Using a similar argument, $1 + \alpha a^3 b\widehat{C} \in S_C$ if $\alpha \in \mathbb{S}$. It follows that $S_C = N_1 \times N_2$ and $|S_C| = \frac{1}{2}|F|^4$.

Since $\overline{G} = G/\zeta(G) \cong D_8$, the order $|V_*(F\overline{G})| = |F|^{\frac{3}{8}|G|}$ by Lemma 2.2 (i). It is clear that $\frac{3}{8}|G| - 3 = \frac{1}{2}|G\{2\}|$. According to Lemma 2.3

$$|V_*(FG)| = 2 \cdot |F|^{\frac{1}{2}|G|}|F|^{(\frac{3}{8}|G|-3)-1} = 2 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}. \qquad \square$$

Lemma 3.5. *Let $G = \langle\ a, b\ \rangle \cong M_{16}$ (see (1)). If $|F| = 2^m \geq 2$, then*

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

Proof. If $y \in S_{G'}$, then

$$y = 1 + \beta_1(a + a^3)\widehat{G'} + \beta_2 a^2\widehat{G'} + \beta_3\widehat{G'} + \beta_4 b\widehat{G'} + \beta_5(a + a^3)b\widehat{G'} + \beta_6 a^2 b\widehat{G'},$$

in which $\beta_1, \dots, \beta_6 \in F$. Moreover,

$$1 + \beta_3\widehat{G'}, \quad 1 + \beta_4 b\widehat{G'} \notin S_{G'} \quad \text{and} \quad \beta_1(a + a^3)\widehat{G'}, \beta_5(a + a^3)b\widehat{G'} \in S_{G'}$$

by Lemma 2.5 and Lemma 2.8, respectively. Since $\eta(\alpha) = \alpha^2$ is an automorphism of $U(F)$ we can pick α such that $\beta_2 = \alpha^2$. Then $u = \alpha^2 + a + \alpha^2 a^2 \in V(FG)$ and

$$uu^* = 1 + \beta_2 a^2\widehat{G'},$$

which proves that $u \in N_\Psi^*$ and $1 + \beta_2 a^2\widehat{G'} \in S_{G'}$ for every $\beta_2 \in F$. The identity

$$\big(\alpha a^2 + (1 + \alpha a^2)b\big)\big(\alpha a^2 + (1 + \alpha a^2)b\big)^* = 1 + \alpha a^2\widehat{G'} + \alpha a^2\widehat{G'}b$$

shows that $\alpha a^2 + (1 + \alpha a^2)b \in N_\Psi^*$. Therefore $1 + \alpha a^2\widehat{G'} + \alpha a^2 b\widehat{G'} \in S_{G'}$ for every $\alpha \in F$. From $1 + \alpha a^2\widehat{G'} \in S_{G'}$ we get $1 + \alpha a^2 b\widehat{G'} \in S_{G'}$ by Lemma 2.4.

We have proved that

$$S_{G'} = \langle 1 + \alpha_1(a + a^3)\widehat{G'}, \quad 1 + \alpha_2 a^2\widehat{G'}, \quad 1 + \alpha_3(a + a^3)b\widehat{G'}, \quad 1 + \alpha_4 a^2 b\widehat{G'} \mid \alpha_i \in F\rangle \subseteq \zeta(V(FG)).$$

Consequently, $|S_{G'}| = |F|^4$ and $|V_*(F\overline{G})| = 2 \cdot |F|^5$, by Lemma 2.1 and the fact that $\overline{G} = G/G' \cong C_4 \times C_2$.

Finally, using that $|G\{2\}| = 4$ Lemma 2.3 shows that

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

Lemma 3.6. *Let $G = \langle\ a, b\ \rangle \curlyvee \langle\ c\ \rangle \cong D_8 \curlyvee C_4$ (see (1)). If $|F| = 2^m \geq 2$, then*

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

Proof. Clearly, $G' = \langle a^2 \rangle$ and $\{g \in G \mid g^2 = a^2\} = \{a, a^3, c, a^2c, bc, abc, a^2bc, a^3bc\}$. Let us prove that $S_{G'} = \langle 1 + \alpha g\widehat{G'} \mid g \in G \setminus G\{2\}, \alpha \in F \rangle$. Indeed, each $x \in S_{G'}$ can be written as $x = 1 + \alpha_1 a\widehat{G'} + \alpha_2 bc\widehat{G'} + \alpha_3 c\widehat{G'} + \alpha_4 abc\widehat{G'}$ by Lemma 2.7 and 2.8. Using the following computation

$$(1 + \alpha b + \alpha a)(1 + \alpha b + \alpha a)^* = 1 + \alpha a\widehat{G'},$$

$$(1 + \alpha c + \alpha a)(1 + \alpha c + \alpha a)^* = 1 + \alpha c\widehat{G'} + \alpha a\widehat{G'},$$

$$(1 + \alpha c + \alpha b)(1 + \alpha a^2 c + \alpha b)^* = 1 + \alpha c\widehat{G'} + \alpha^2 bc\widehat{G'},$$

$$(a^2c + \alpha ab + \alpha ac)(a^2c + \alpha ab + \alpha ac)^* = 1 + (\alpha abc + \alpha a + \alpha^2 bc)\widehat{G'},$$

it is easy to check that $S_{G'} = \langle 1+\alpha_1 a\widehat{G'}, 1+\alpha_2 c\widehat{G'}, 1+\alpha_3 bc\widehat{G'}, 1+\alpha_4 abc\widehat{G'} \mid \alpha_i \in F \rangle$ by Lemma 2.4 so $|S_{G'}| = |F|^4$.

Since $\overline{G} = G/G' \cong C_2 \times C_2 \times C_2$, Lemma 2.1 shows that $|V_*(F\overline{G})| = |F|^7$. It is obvious that $|G\{2\}| = 4$, so $\frac{|V_*(F\overline{G})|}{|S_{G'}|} = |F|^{\frac{1}{2}|G\{2\}|-1}$. According to Lemma 2.3 we get

$$|V_*(FG)| = |F|^{\frac{1}{2}|G|}|F|^{\frac{1}{2}|G\{2\}|-1} = |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}. \qquad \square$$

Proof of Theorem 1.4. It follows immediately from Corollaries 1.2, 1.3 and Lemmas 3.1, 3.4 – 3.6. $\square$

Proof of Theorem 1.5. Our statement holds if G is a non-abelian group of order $|G| = 2^3$ by [18] and [19]. Moreover, it is also true if $|G| = 2^4$ and $|F| = 2$ by [3] and [9].

Let $|F| > 2$ and $|G| = 2^4$. Theorem 1.4 yields that $|V_*(FG)| = |V_*(FH)|$ if and only if $G \in \{C_4 \ltimes C_4, Q_8 \times C_2\}$. Without loss of generality we can assume that $G \cong Q_8 \times C_2 = \langle a, b \rangle \times \langle c \rangle$ and $H \cong C_4 \ltimes C_4$. If $M = \langle a, c \rangle < G$, then each $x \in V(FG)$ can be written as $x = x_1 + x_2 b$, where $x_1, x_2 \in FM$. Obviously, $xx^* = x_1x_1^* + x_2x_2^* + (x_1x_2 + x_1x_2a^2)b$ and

$$x^2 = x_1^2 + x_2x_2^*a^2 + (x_1x_2 + x_1^*x_2)b. \tag{4}$$

Furthermore, $x \in V_*(FG)$ if and only if $x_1x_1^* = x_2x_2^* + 1$ and $x_1x_2 = x_1x_2a^2$. Since x is a unit, $\chi(x_1) + \chi(x_2) = 1$, so consider the following cases.

Case 1. Let $\chi(x_1) = 1$ and $\chi(x_2) = 0$. From the equality $x_1x_2 = x_1x_2a^2$ we conclude that $x_2(1 + a^2) = 0$ and (see [20, Theorem 11]) we can write

$$x_2 = \alpha_0(1 + a^2) + \alpha_1(1 + a^2)a + \alpha_2(1 + a^2)c + \alpha_3(1 + a^2)ac, \qquad (\alpha_i \in F).$$

By (4) and the fact that

$$x_1 + x_1^* = \beta_0(1 + a^2) + \beta_1(1 + a^2)a + \beta_2(1 + a^2)c + \beta_3(1 + a^2)ac, \qquad (\beta_i \in F)$$

we conclude that $x^2 = x_1^2$ and $x_1^{-1} = x_1^*$. According to [14, Theorem 2(ii)] $V_*(FM) \cong M \times N$ in which N is an elementary abelian group. Consequently, $x^2 \in \{1, a^2\}$.
Case 2. Let $\chi(x_1) = 0$ and $\chi(x_2) = 1$. From the equation $x_1x_2 = x_1x_2a^2$ we conclude that $x_1(1+a^2) = 0$, so (see [20, Theorem 11])

$$x_1 = \alpha_0(1+a^2) + \alpha_1(1+a^2)a + \alpha_2(1+a^2)c + \alpha_3(1+a^2)ac, \qquad (\alpha_i \in F).$$

Equations (4), $x_2x_2^* = x_1x_1^* + 1 = 1$ and $x_1 + x_1^* = 0$ imply that $x^2 = x_1^2 + 1 = 1$.

Consequently, if $x \in V_*(FG)$, then $x^2 \in \{1, a^2\}$, so $|V_*^2(FG)| = |\langle\, a^2 \,\rangle| = 2$.

Let $H \cong C_4 \ltimes C_4$. Clearly, $|V_*(FH)| > 2$ because $H^2 \subseteq V_*^2(FH)$. This proofs that $V_*(FG)$ and $V_*(FH)$ are not isomorphic groups. □

Note that Theorem 1.4 was verified by GAP package RAMEGA [6].

Acknowledgement. The author would like to thank the anonymous reviewers for their careful reading of the manuscript and their many insightful comments and suggestions.

References

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

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

[3] Z. Balogh and V. Bovdi, *The isomorphism problem of unitary subgroups of modular group algebras*, Publ. Math. Debrecen, 97(1-2) (2020), 27-39, see also arXiv:1908.03877v2 [math.RA].

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

[5] Z. Balogh and V. Laver, *Isomorphism problem of unitary subgroups of group algebras*, Ukrainian Math. J., 72(6) (2020), 871-879.

[6] Z. Balogh and V. Laver, *RAMEGA - RAndom MEthods in Group Algebras, Version 1.0.0*, (2020).

[7] S. D. Berman, *Group algebras of countable abelian p-groups*, Publ. Math. Debrecen, 14 (1967), 365-405.

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

[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) (1996), 1-16.

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

[11] V. A. Bovdi and A. N. Grishkov, *Unitary and symmetric units of a commutative group algebra*, Proc. Edinb. Math. Soc. (2), 62(3) (2019), 641-654.

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

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

[14] A. A. Bovdi and A. A. Sakach, *Unitary subgroup of the multiplicative group of a modular group algebra of a finite abelian p-group*, Mat. Zametki, 45(6) (1989), 23-29.

[15] V. Bovdi and M. Salim, *On the unit group of a commutative group ring*, Acta Sci. Math. (Szeged), 80(3-4) (2014), 433-445.

[16] A. A. Bovdi and A. Szakács, *A basis for the unitary subgroup of the group of units in a finite commutative group algebra*, Publ. Math. Debrecen, 46(1-2) (1995), 97-120.

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

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

[19] 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) (2011), 237-243.

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

[21] J.-P. Serre, *Bases normales autoduales et groupes unitaires en caractéristique 2*, Transform. Groups, 19(2) (2014), 643-698.

Zsolt Adam Balogh
Department of Mathematical Sciences
United Arab Emirates University (UAEU)
United Arab Emirates
e-mail: baloghzsa@gmail.com