ON THE ORDER OF THE UNITARY
SUBGROUP OF MODULAR GROUP ALGEBRA

VICTOR BOVDI
Lajos Kossuth University, H-410 Debrecen, P.O. Box 12, Hungary
vbovdi@math.klte.hu

A. L. ROSA
Universidade Federal de Ouro Preto, 35400-000 Ouro Preto-M.G., Brasil
alrosa@iceb.ufop.br

Abstract. Let $K^G$ be a group algebra of a finite $p$-group $G$ over a finite
field $K$ of characteristic $p$. We compute 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 or $G$ has an abelian
subgroup $A$ of index 2 and an element $b$ such that $b$ inverts each element
of $A$.

1. Introduction. Let $K^G$ be the group algebra of a locally-finite $p$-group
$G$ over a commutative ring $K$ (with 1) and $V(K^G)$ be the group of nor-
malized units (that is, of the units with augmentation 1) in $K^G$. The anti-
automorphism $g \mapsto g^{-1}$ extends linearly to an anti-automorphism $a \mapsto a^*$
of $K^G$; this extension leaves $V(K^G)$ setwise invariant and its restriction
to $V(K^G)$ followed by $v \mapsto v^{-1}$ gives an automorphism of $V(K^G)$. The
elements of $V(K^G)$ fixed by this automorphism are the unitary normalized
units of $K^G$; they form a subgroup, which we denote by $V_*(K^G)$. Interest
in unitary units arose in algebraic topology and a more general definition,
involving an ‘orientation homomorphism’, is also current; the special case we use here arises when the orientation homomorphism is trivial.

In [3-4] A. Bovdi and A. Szakács solved the problem, posed by S. P. Novikov of the structure of the group $V_*(KG)$ of the group algebra of a finite abelian $p$-group over a finite field of $p^m$ elements. We also know a few facts on $V_*(KG)$ when $G$ is nonabelian (see survey [1]). Note that A. Bovdi and L. Erdei [2] have described the unitary subgroup $V_*(KG)$ for all groups of order 8 and 16. We shall study here the order of the group $V_*(KG)$ for some nonabelian groups $G$.

2. Basic facts. For an arbitrary element $x = \sum_{g \in G} \alpha_g g \in KG$ we put $\chi(x) = \sum_{g \in G} \alpha_g \in K$, for $a, b \in G$ we denote $a^b = b^{-1}ab$ and let $|a|$ denote the order of element $a$.

First, let us recall some facts about the order of $V_*(KG)$ for $\text{char}(K) > 2$, which are known from the theory of algebras with involution.

We use the following notation:

$$I_K(G) = \{ \sum_{g \in G} \alpha_g g \in KG \mid \sum_{g \in G} \alpha_g = 0 \}$$

for the augmentation ideal of $KG$. Let

$$S(I) = \{ x \in I_K(G) \mid x^* = x \}, \quad SK(I) = \{ x \in I_K(G) \mid x^* = -x \}$$

be the set of symmetric and the set of skew symmetric elements of $I_K(G)$, respectively.

Clearly, $I_K(G) = S(I) + SK(I)$ and $S(I) \cap SK(I) = 0$. Indeed, for any $y \in I_K(G)$ we have $y = \frac{y+y^*}{2} + \frac{y-y^*}{2}$. Moreover, if $x \in S(I)$, then $x = \sum_{g \in G} \alpha_g (g + g^{-1} - 2)$ and $|S(I)| = |K|^{[G]-1}$, whence

$$|SK(I)| = |K|^{[G]-1} : |K|^{[G]-1} = |K|^{[G]-1}.$$  

Recall that, if $k \in SK(I)$, then the element $1+k$ is a unit and the element $u = (1-k)(1+k)^{-1}$ is a unitary unit [6], which is called a Cayley unitary unit.

It is easy to observe that any element in $V_*(KG)$ is a Cayley unitary unit for $\text{char}(K) > 2$. Indeed, if $u \in V_*(KG)$ then $1+u$ is a unit because $\chi(1+u) = 2 \neq 0$ and $k = (1-u)(1+u)^{-1}$ is skew symmetric. Indeed,

$$k^* = (1+u^*)^{-1}(1-u)^* = (u^{-1}(1+u))^{-1}(u^{-1}(u-1)) = -k.$$
Therefore, \(1 + k = ((1 + u) + (1 - u))(1 + u)^{-1} = 2(1 + u)^{-1}\) is a unit and \(u = (1 - k)(1 + k)^{-1}\) is a Cayley unitary unit. We conclude that \(u = -1 + 2(1 + k)^{-1}\) and the number of the unitary units equals the number of skew symmetric elements and

\[
|V_*(KG)| = |SK(I)| = |K|^{|G|-1}/2.
\]

Now let us state some basic properties of group algebras of the 2-groups. To determine the order of the unitary subgroup \(V_*(KG)\), we need the following results from [5].

**Lemma 1.** Let \(K\) be a field of prime characteristic \(p\) and let \(G\) be a non-abelian locally finite \(p\)-group. The subgroup \(V_*(KG)\) is normal in \(V(KG)\) if and only if \(p = 2\) and \(G\) is the direct product of an elementary abelian group with a group \(H\) for which one of the following holds:

(i) \(H\) has no direct factor of order 2, but it is a semidirect product of a group \(\langle h \rangle\) of order 2 and an abelian 2-group \(A\) with \(a^h = a^{-1}\) for all \(a\) in \(A\);

(ii) \(H\) is an extraspecial 2-group or the central product of such a group with a cyclic group of order 4.

Recall that a \(p\)-group is extraspecial if its centre, commutator subgroup and Frattini subgroup coincide and have order \(p\).

**Lemma 2.** Let \(K\) be a commutative ring and \(G\) be any group. For \(x \in V(KG)\) and \(y \in V_*(KG)\), we have \(x^{-1}yx \in V_*(KG)\) if and only if \(xx^*\) commutes with \(y\).

**Proof.** Clearly, \((x^{-1}yx)^* = (x^{-1}yx)^{-1}\) means that \(x^*y^*(x^*)^{-1} = x^{-1}y^{-1}x\) which in turn is equivalent to \(xx^*y^* = y^{-1}xx^*\). Since we are given \(y^* = y^{-1}\), this proves the lemma.

Since \(G \leq V_*(KG)\), any element, which commutes with every element of \(V_*(KG)\), is central in \(KG\). Thus Lemma 2 gives the following:

**Corollary 1.** The subgroup \(V_*(KG)\) is normal in \(V(KG)\) if and only if all elements of the form \(xx^*\) with \(x \in V(KG)\) are central in \(KG\).

**Lemma 3.** Let \(K\) be a field of characteristic 2 and let \(G\) be a nonabelian locally finite 2-group for which one of the following holds:
(i) $G$ is a semidirect product of a group $\langle b \rangle$ of order 2 and an abelian 2-group $A$, with $a^b = a^{-1}$ for all $a$ in $A$;
(ii) $G$ is an extraspecial 2-group or the central product of such a group with a cyclic group of order 4.

Then the map $x \rightarrow xx^*$ is a homomorphism of the group $V(KG)$ into the subgroup $S_K(G) = \{xx^* \mid x \in V(KG)\}$ of the symmetric units and if $V(KG)$ is finite, then the order of the unitary subgroup $V_*(KG)$ coincides with the index of the subgroup $S_K(G)$ in $V(KG)$.

Proof. From Corollary 1 we have that $xx^*$ is central in $V(KG)$. Setting $\phi(x) = xx^*$, we have

$$\phi(xy) = (xy)(xy)^* = xyy^*x^* = (xx^*)(yy^*) = \phi(x)\phi(y)$$

for all $x, y \in V(KG)$. Therefore $\phi$ is an epimorphism and the kernel of $\phi$ is the unitary subgroup $V_*(KG)$. From this follows the rest of Lemma 3.

\[\square\]

3. The order of the unitary subgroup. For a finite 2-group $G$ with the commutator subgroup $G' = \langle c \mid c^2 = 1 \rangle$ of order 2 we define $L_G$ as the subset of the elements of order 4 such that $L_G \cap L_Gc$ is empty and $L_G \cup L_Gc$ coincide with all elements of order 4 of $G$.

Lemma 4. Let $G$ be an extraspecial 2-group of order $|G| = 2^{2n+1}$ with $n \geq 2$. Then

$$|L_G| = 2^{n-1}(2^n - (-1)^n).$$

Proof. If $G$ is an extraspecial 2-group of order $|G| = 2^{2n+1}$ with $n \geq 2$, then by Theorem 5.3.8 in [7] we have $G = G_1 \cdots G_n$, where $G_i$ is a quaternion group of order 8. Then $\zeta(G) = G' = \langle c \mid c^2 = 1 \rangle$ and $G_i \cap G_j = \langle c \rangle$ for any $i \neq j$. Evidently every element of order 4 of $G$ can be written as

$$x = z_{i_1}z_{i_2} \cdots z_{i_s},$$

where $z_{i_k} \in G_{i_k}$ has order 4 and $i_1 < i_2 < \cdots < i_s$. Then the number $s$ is called the length of $x$. Clearly, $z_{i_k}^2 = c$ and the length of the element of order 4 is odd.

Let $H_k = H(i_1, i_2, \ldots, i_k) = G_{i_1} \cdots Y G_{i_2} \cdots Y G_{i_k}$, where $k$ is odd and $i_1 < i_2 < \cdots < i_k$. We shall prove that there are precisely $3^k$ elements of length $k$ in $L_{H_k}$. Of course, every $L_{G_i}$ contains 3 different elements and every element of length $k$ of the form (1) has order 4. We conclude that the number of elements of $L_{H_k}$ is $3^k$. Since the number of different subgroups
Let $G$ be a central product of an extraspecial $2$-group $H$ of order $|H| = 2^{2n+1}$ with a cyclic group $\langle d \rangle$ of order $4$. Then $|L_G| = 2^{2n}$. 

**Proof.** It is obvious that any element of order $4$ in $G$ either lies in $H$ or may be written as $ud$, where $u \in H$ and $|u| \neq 4$. The number of elements $u$ is exactly $|H| - 2|L_H|$. We conclude that 

$$|L_G| = |L_H| + \frac{|H| - 2|L_H|}{2} = \frac{|H|}{2} = 2^{2n}. \quad \square$$

**Theorem 1.** Let $K$ be a finite field of characteristic $2$.

(i) If $G$ is an extraspecial $2$-group of order $|G| = 2^{2n+1}$ with $n \geq 2$, then

$$|V^*(KG)| = |K|^{2^{n-1}(2^{n+2} - 2^n + (-1)^n) - 1}. $$

(ii) If $G$ is a central product of an extraspecial $2$-group $H$ of order $|H| = 2^{2n+1}$ with a cyclic group $\langle d \rangle$ of order $4$, then

$$|V^*(KG)| = |K|^{3 \cdot 2^{2n} - 1}. $$
Proof. Recall that, if \( x = \sum_{i=1}^{t} \alpha_i a_i \in V(KG) \), then

\[
x x^* = 1 + \sum_{i<j} \alpha_i \alpha_j (a_i a_j^{-1} + a_j a_i^{-1}).
\]

If \( a_i a_j^{-1} \) has order 2, then \( a_i a_j^{-1} = a_j a_i^{-1} \) and therefore the support of \( xx^* \) contain no elements of order 2. Thus we obtain

\[
xx^* = 1 + \sum_{b \in L_G} \alpha_b (1 + c) = \prod_{b \in L_G} (1 + \alpha_b (1 + c)),
\]

where \( \alpha_b \in K \). Of course, the number of elements of the form \( xx^* \) with \( x \in V(KG) \) is at most \( |K|^{|L_G|} \). We shall prove that the subgroup \( S_K(G) = \{ xx^* \mid x \in V(KG) \} \) has order \( |K|^{|L_G|} \).

(i) Now let \( G \) be an extraspecial 2-group of order \( |G| = 2^{2n+1} \) with \( n \geq 2 \). Take \( b \in L_G \) and \( \alpha_b \in K \). Then there exists an element \( w_b \in G \) of order 2, such that \( (w_b, b) \neq 1 \). Indeed, the length of \( b = z_{i_1} z_{i_2} \cdots z_{i_{2k+1}} \) is odd. Then we choose another \( u_1 \in G_{i_1} \) of order 4 such that \( (u_1, z_{i_1}) \neq 1 \) and an arbitrary element \( u_2 \) either from the set \( \{ z_{i_2} \cdots z_{i_{2k+1}} \} \) or, if \( k = 0 \), from \( G_t \) with \( t \neq i_1 \) and \( |u_2| = 4 \). Then \( w_b = u_1 u_2 \) is an element of order 2 and does not commute with \( b \).

Since \( (1 + \alpha_b (b + w_b))(1 + \alpha_b (b + w_b))^* = 1 + \alpha_b (1 + c) \), this shows us that any factors of \( \prod_{b \in L_G} (1 + \alpha_b (1 + c)) \) belong to the subgroup \( S_K(G) \).

Since \( uu^* \) is central for arbitrary \( u \in V(KG) \), we have

\[
\prod_{b \in L_G} (1 + \alpha_b (b + w_b))(1 + \alpha_b (b + w_b))^* = (1 + \alpha_b (b_1 + w_{b_1})) \times 
\]

\[
x (\prod_{b \in L_G \setminus \{b_1\}} (1 + \alpha_b (b + w_b))(1 + \alpha_b (b + w_b))^*)(1 + \alpha_b (b_1 + w_{b_1}))^* = 
\]

\[
= \prod_{b \in L_G} (1 + \alpha_b (b + w_b))(\prod_{b \in L_G} (1 + \alpha_b (b + w_b)))^*.
\]

Thus \( |S_K(G)| = |K|^{|L_G|} \) and by Lemmas 3 and 4 we get the result.

(ii) Now let \( G = H \ast \langle d \rangle \), where \( H = G_1 \ast \cdots \ast G_n \) is an extraspecial 2-group of order \( |H| = 2^{2n+1} \). If \( |H| > 8 \) and \( b \in L_H \), then, as before, we can prove that \( 1 + \alpha_b (1 + c) \in S_K(G) \). Thus it remains to consider the case, when the element \( b \) of order 4 commutes with any element of order 2 in \( G \).

In this case there exists \( G_i = \langle a_i, b_i \rangle \) such that \( \langle G_i, b \rangle = \langle G_i \rangle \ast \langle b \rangle \). Evidently \( x = 1 + a_i + b \) and \( y = 1 + a_i + b_i b \) are units, \( xx^* = 1 + (a_i + b)(1 + c) \) and
$yy^* = 1 + a_i(1 + c)$. Recall that $xx^*$ and $yy^*$ are central units by Lemma 1. Furthermore, it follows that

$$1 + b(1 + c) = xx^*yy^* = (xy)(xy)^* \in S_K(G).$$

Thus, we conclude that $|S_K(G)| = |K|^{|L_G|}$ and by Lemmas 3 and 5 we prove (ii) of the theorem. □

Let $A$ be an abelian group and we define $A[2] = \{a \in A \mid a^2 = 1\}$.

**Theorem 2.** Let $K$ be a finite field of characteristic 2 and $G$ has an abelian subgroup $A$ of index 2 and an element $b$ which inverts every element of $A$.

(i) If $b$ has order 2, then

$$|V_+(KG)| = |K|^{3|A| + |A[2]| - 2}.$$

(ii) If $b$ has order 4, then

$$|V_+(KG)| = 2 \cdot |A^2[2]| \cdot |K|^{|A| + \frac{1}{2}|A[2]| - 1}.$$

**Proof.** (i) Any element of $V(KG)$ can be written as $x = x_0 + x_1b$, where $x_i \in KA$ and $\chi(x_0) + \chi(x_1) = 1$. Evidently, $x_i^b = x_i^*$ ($i = 1, 2$) and

$$xx^* = (x_0 + x_1b)(x_0^* + x_1b) = x_0x_0^* + x_1x_1^*.$$

Before observed that for any $y = \alpha_1a_1 + \alpha_2a_2 + \cdots + \alpha_s a_s \in KA$ with $a_i \in A$ we have

$$yy^* = (\alpha_1^2 + \alpha_2^2 + \cdots + \alpha_s^2) + \sum_{i < j} \alpha_i \alpha_j(a_i a_j^{-1} + a_j a_i^{-1}).$$

If $a_i a_j^{-1}$ is an element of order two, then $a_i a_j^{-1} = a_j a_i^{-1}$ and, therefore, the support of the element $yy^*$ does not contain the element of order 2. As a consequence, $xx^* \in S_K(G)$ has a unique expression in the form

(3) $$1 + \sum_{a \in L} \alpha_a (a + a^{-1}),$$

where $L$ is a full system of representatives of the subset $\{a^{-1}, a\}$ with $a \in A \setminus A[2]$. Obviously, the number of elements of $L$ is $l = \frac{|A| - |A[2]|}{2}$. Hence the order of the subgroup $S_K(G)$ is at most $|K|^l$. To prove that it is
the order of $S_K(G)$, it remains to note that for any $z$ of the form (3) there
exists $x \in V(KG)$ such that $xx^* = z$. Indeed, if
\[ z = 1 + \alpha_1(a_1 + a_1^{-1}) + \alpha_2(a_2 + a_2^{-1}) + \cdots + \alpha_s(a_s + a_s^{-1}) \]
we put $x_0 = \alpha_1a_1 + \alpha_2a_2 + \cdots + \alpha_sa_s$ and $x_1 = 1 + x_0$. Then
\[ \chi(x_0) + \chi(x_1) = 1 + 2(\alpha_1 + \alpha_2 + \cdots + \alpha_s) = 1 \]
and $x = x_0 + x_1b$ is a unit with $xx^* = 1 + x_0 + x_0^* = z$. Thus the order of
the subgroup $S_K(G)$ equals $|K|$. Using this result, it is easy to find the
order of the unitary subgroup, using Lemma 3.

(ii) Now let $A$ be a finite abelian 2-group. Then $V_s(KA) = A \times U$ by [3]
and the group $V_s(KA)$ has order
\[ |A^2[2]| \cdot |K|^{\frac{1}{2}(|A|+|A[2]|)} - 1. \]
Let us calculate the order of the unitary subgroup for the group $G$ using the
method of the paper [3].

Let $G$ has an abelian subgroup $A$ of index 2 and an element $b$ of order 4, such that $a^b = a^{-1}$ for all $a \in A$. Consider the subgroup
\[ R = \{ 1 + (1 + b^2)z \mid z \in KA \} = \prod_{u \in T} \langle 1 + \lambda u(1 + b^2)b \mid \lambda \in K \rangle, \]
where $T$ is a transversal to $\langle b^2 \rangle$ in $A$. Clearly, the elements of $R$ are unitary
units of order 2 and $|K|^{\frac{1}{2}(|A|)}$ is the order of $R$.

Let $x \in V_s(KG)$. Because $G \subseteq V_s(KG)$, either $x$ or $xb$ can be written
as $x = x_1(1 + x_2b)$, where $x_i \in KA$ and $\chi(x_1) = 1$. Then $x \in V_s(KG)$ if
and only if
\[ x_1x_1^*(1 + x_2x_2^*) = 1 \quad \text{and} \quad x_2(1 + b^2) = 0. \]

It follows that $x_2x_2^* = 0$ and the element $x_1$ is unitary and $1 + x_2b \in R$. Since
$w^{-1}(1 + \lambda z(1 + b^2)b)w = 1 + \lambda w^{-1}w^*z(1 + b^2)b \in R$, where $w \in V_s(KA)$
and $R \cap U = \langle 1 \rangle$, we have that $W = U \ltimes R$ is a subgroup of $V_s(KG)$. Finally,
$b^{-1}wb = w^* = w^{-1} \in V_s(KA)$ for every $w \in V_s(KA)$ and we conclude that $V_s(KG) = G \ltimes (R \ltimes U)$ and
\[ |V_s(KG)| = 2 \cdot |A^2[2]| \cdot |K|^{\frac{1}{2}(|A|+|A[2]|)} - 1 \cdot |K|^{\frac{|A|}{2}} = 2 \cdot |A^2[2]| \cdot |K|^{\frac{|A|}{2} + \frac{1}{2}|A[2]|} - 1. \]
\[ \square \]
Corollary 2. Let $K$ be a finite field of characteristic 2.

(i) If $D_{2n+1} = \langle a, b \mid a^{2^n} = b^2 = 1, a^b = a^{-1} \rangle$ is a dihedral group of order $2^{n+1}$, then

$$|V_*(KD_{2n+1})| = |K|^{3 \cdot 2^{n-1}}.$$  

(ii) If $Q_{2n+1} = \langle a, b \mid a^{2^n} = 1, a^{2^{n-1}} = b^2, a^b = a^{-1} \rangle$ is a quaternion group of order $2^{n+1}$, then

$$|V_*(KQ_{2n+1})| = 4 \cdot |K|^{2^n}.$$

\qed

References

1. Bovdi, A.A., *The group of units of a group algebra of characteristic p*, Publ. Math. Debrecen 52 (1–2) (1998), 193–244.
2. Bovdi, A.A., Erdei, L., *Unitary units in modular group algebras of groups of order 16*, Technical Report Universitas Debrecen, Dept. of Math., L. Kossuth Univ. 96/4 (1996), 1–16.
3. Bovdi, A.A., Szakács A., *Unitary subgroup of the group of units of a modular group algebra of a finite abelian p-group*, Mat. Zametki 45, No. 6 (1989), 23–29.
4. Bovdi, A.A., Szakács A., *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.
5. Bovdi, V., Kovács, L.G., *Unitary units in modular group algebras*, Manuscripta Math. 84 (1994), 57–72.
6. Chuang, C.L., Lee, P.H., *Unitary elements in simple artinian rings*, J. Algebra 176 (1995), 449–459.
7. Robinson, D.J.S., *A course in the theory of groups*, Springer-Verlag, Berlin-Heidelberg-New York, 1996, pp. 490.