Publ. Math. Debrecen
69/3 (2006), 291–296

Units of commutative group algebra with involution

By A. BOVDI (Debrecen) and A. SZAKÁCS (Békéscsaba)

Dedicated to the memory of Dr. Edit Szabó

Abstract. Let p be an odd prime, F the field of p elements and G a finite abelian p-group with an arbitrary involutory automorphism. Extend this automorphism to the group algebra FG and consider the unitary and the symmetric normalized units of FG. This paper provides bases and determines the invariants of the two subgroups formed by these units.

1. Introduction

Let p be an odd prime, F the field of p, G a finite abelian p-group with an arbitrary automorphism η of order 2 and $G_\eta = \{g \in G \mid \eta(g) = g\}$. Extending the automorphism η to the group algebra FG we obtain the involution

$$x = \sum_{g\in G} \alpha_g g \mapsto x^{\circledast} = \sum_{g\in G} \alpha_g \eta(g)$$

of FG which we will call as η-canonical involution. In particular, if $\eta(g) = g^{-1}$ or $\eta(g) = g$ for all $g \in G$ then the involution is called involutory; if $\eta(g) = g^{-1}$ for all $g \in G$ then it is called canonical and denote by $*$.

Mathematics Subject Classification: Primary: 16S34, 16U60; Secondary: 20C05.
Key words and phrases: group algebra, group of units, unitary unit, symmetric unit.
Supported by OTKA No. T037202 and by FAPESP Brasil (proc. 06/56203-3).

Let $V(FG) = \{\sum_{g\in G} \alpha_g g \mid \sum_{g\in G} \alpha_g = 1\}$ be the group of normalized units of the group algebra FG and consider the subgroups of symmetric and unitary units

$$S_{\circledast}(FG) = \{x \in V(FG) \mid x^{\circledast} = x\},$$
$$V_{\circledast}(FG) = \{x \in V(FG) \mid x^{\circledast} = x^{-1}\}$$

respectively.

Our goal is to study the unitary subgroup $V_{\circledast}(FG)$ and the group of symmetric units $S_{\circledast}(FG)$. The problem of determining the invariants and the basis of $V_{*}(FG)$ had been raised by S. P. Novikov. Its solution for the canonical involution was given in [1]; here this result extended to arbitrary involutory involution.

2. Invariants

We start with some remarks about the invariants of unitary and symmetric subgroups to give a bases.

Since $V(FG)$ has an odd order and every $u \in V(FG)$ can be written as $u = (v^{\circledast})^2$, so $u = (v^{\circledast}v^{-1})(vv^{\circledast})$, where $v^{\circledast}v^{-1}$ is unitary and $vv^{\circledast}$ is a symmetric unit. But every $x \in S_{\circledast}(FG) \cap V_{\circledast}(FG)$ is such that $x = x^{\circledast} = x^{-1}$; since x is odd order it follows $x = 1$ and we have

$$V(FG) = S_{\circledast}(FG) \times V_{\circledast}(FG). \tag{1}$$

Define the mappings

$$\psi_1 : V(FG) \to V_{\circledast}(FG), \quad \psi_2 : V(FG) \to S_{\circledast}(FG)$$

given by $\psi_1(x) = x^{\circledast}x^{-1}$ and $\psi_2(x) = x^{\circledast}x$ respectively for $x \in V(FG)$. They are epimorphisms and as corollary conclude that

$$\begin{aligned} V_{\circledast}(FG) &= \{x^{\circledast}x^{-1} \mid x \in V(FG)\}, \\ S_{\circledast}(FG) &= \{x^{\circledast}x \mid x \in V(FG)\} \end{aligned} \tag{2}$$

and

$$S_{\circledast}(FG)^{p^i} = S_{\circledast}(FG^{p^i}), \quad V_{\circledast}(FG)^{p^i} = V_{\circledast}(FG^{p^i}), \tag{3}$$

which use for the description of the invariants of these groups. The subsets $\{g, \eta(g)\}$ with $g \in G \setminus G_\eta$ form a partition of the set $G \setminus G_\eta$ and let E be the system of representatives of these subsets. Clearly, $x \in S_\circledast(FG)$ can be uniquely written as

$$x = \sum_{g \in E} \alpha_g(g + \eta(g)) + \sum_{g \in G_\eta} \beta_g g$$

with $\alpha_g, \beta_g \in F$ and $\sum_{g\in E} 2\alpha_g + \sum_{g\in G_\eta} \beta_g = 1$, so the order of the group of symmetric units $S_\circledast(FG)$ equals $p^{\frac{1}{2}(|G|+|G_\eta|-2)}$. By (3) $S_\circledast(FG)^p = S_\circledast(FG^p)$, so as before, the order of $S_\circledast(FG)^p$ is $p^{\frac{1}{2}(|G^p|+|G_\eta^p|-2)}$. It follows that the p-rank of the group $S_\circledast(FG)$, that is the number of components in the decomposition of $S_\circledast(FG)$ into a direct product of cyclic groups, equals $\frac{1}{2}(|G| - |G^p| + |G_\eta| - |G_\eta^p|)$. Similarly, the p-rank of the group $S_\circledast(FG)^{p^{i-1}}$ equals $\frac{1}{2}(|G^{p^{i-1}}| - |G^{p^i}| + |G_\eta^{p^{i-1}}| - |G_\eta^{p^i}|)$.

We conclude that the number of components of order p^i in the decomposition of $S_\circledast(FG)$ into a direct product of cyclic groups equals

$$f_i(S_\circledast(FG)) = \frac{1}{2}(|G^{p^{i-1}}| - 2|G^{p^i}| + |G^{p^{i+1}}| + |G_\eta^{p^{i-1}}| - 2|G_\eta^{p^i}| + |G_\eta^{p^{i+1}}|). \quad (4)$$

We known from [3] that the equality $V(FG)^{p^i} = V(FG^{p^i})$ holds and the p-rank of $V(FG)^{p^{i-1}}$ equals $|G^{p^{i-1}}| - |G^{p^i}|$. Now (1) it yields that the p-rank of $V_\circledast(FG)^{p^{i-1}}$ equals $\frac{1}{2}(|G^{p^{i-1}}| - |G^{p^i}| - |G_\eta^{p^{i-1}}| + |G_\eta^{p^i}|)$. It immediately follows that the number of components of order p^i in the decomposition of the group $V_\circledast(FG)$ into a direct product of cyclic groups is equal to

$$f_i(V_\circledast(FG)) = \frac{1}{2}(|G^{p^{i-1}}| - 2|G^{p^i}| + |G^{p^{i+1}}| - |G_\eta^{p^{i-1}}| + 2|G_\eta^{p^i}| - |G_\eta^{p^{i+1}}|). \quad (5)$$

3. The bases

We will use the following well-known generators of $V(FG)$ (see [2]):

Lemma. *Let G be a finite abelian p-group, $I = I(FG)$ the augmentation ideal of FG and assume that $I^{s+1} = 0$. If*

$$v_{d1} + I^{d+1}, v_{d2} + I^{d+1}, \dots, v_{dr_d} + I^{d+1}$$

is a basis for I^d/I^{d+1}, then the units $1 + v_{dj}$ ($d = 1, 2, \dots, s$; $j = 1, 2, \dots, r_d$) generate $V(FG)$.

Let us return to the involutory automorphism η of G. Clearly, G has the decomposition

$$G = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_l\rangle \times \cdots \times \langle a_t\rangle$$

such that the elements $a_1, a_2, \dots, a_l$ inverted by η and if $t > l$ then η leaves fixed a_i for $i > l$.

Let q_i be the order of a_i and the set L consisting of those t-tuples $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_t)$ such that $\alpha_i \in \{0, 1, \dots, q_i - 1\}$ and at least one of α_j is not divisible by p ; the number of these elements $|G| - |G^p|$. Write L as the disjoint union $L = L_0 \cup L_1 \cup L_2$, where α belongs to L_0, L_1 or L_2 according to whether $\alpha_1 + \alpha_2 + \cdots + \alpha_\ell$ is 0, odd or even and positive. The cardinality of L_1 is $\frac{1}{2}(|G| - |G^p| - |G_\eta| + |G_\eta^p|)$, and it is the p-rank of $V_\circledast(FG)$ and the cardinality of $L_0 \cup L_2$ is $\frac{1}{2}(|G| - |G^p| + |G_\eta| - |G_\eta^p|)$, which is the p-rank of $S_\circledast(FG)$.

Put $u_\alpha := 1 + (a_1 - 1)^{\alpha_1}(a_2 - 1)^{\alpha_2} \cdots (a_t - 1)^{\alpha_t}$ for $\alpha \in L$.

Theorem. *Let G be a finite abelian p-group of odd order with an involutory automorphism η and F is field of p elements. Then*

1. *The invariants of the unitary subgroup $V_\circledast(FG)$ are indicated in* (5) *and the set $\{{u_\alpha}^\circledast {u_\alpha}^{-1} \mid \alpha \in L_1\}$ is basis for it, that is $V_\circledast(FG) = \prod_{\alpha\in L_1}\langle {u_\alpha}^\circledast {u_\alpha}^{-1}\rangle$.*
2. *The invariants of the group of symmetric units $S_\circledast(FG)$ are indicated in* (4) *and the set $\{u_\alpha^\circledast u_\alpha \mid \alpha \in L_2\} \cup \{u_\alpha \mid \alpha \in L_0\}$ is basis for it, that is*

$$S_\circledast(FG) = \prod_{\alpha\in L_2}\langle {u_\alpha}^\circledast u_\alpha\rangle \times \prod_{\alpha\in L_0}\langle u_\alpha\rangle.$$

Proof. Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_t)$ with $\alpha_i \in \{0, 1, \dots, q_i - 1\}$; define $d(\alpha) = \alpha_1 + \alpha_2 + \cdots + \alpha_t$ and put $z_\alpha := (a_1 - 1)^{\alpha_1}(a_2 - 1)^{\alpha_2} \cdots (a_t - 1)^{\alpha_t}$. It is known from [2] that all z_α form a vector space basis for the augmentation ideal I and the elements $z_\alpha + I^{d+1}$ with $d(\alpha) = d$ constitute a basis for I^d/I^{d+1} with the property required for the application of Lemma. Therefore the elements $u_\alpha = 1 + z_\alpha$ generate $V(FG)$ and from [3] follows that $\{u_\alpha | \alpha \in L\}$ is a basis of $V(FG)$.

If $i \le l$ then $((a_i-1)+1)^{-1} = ((a_i-1)+1)^{\circledast} = (a_i-1)^{\circledast}+1$ and from

$$(1+(a_i-1))(1-(a_i-1)+(a_i-1)^2-\cdots+(a_i-1)^{q_i-1}) \\ = 1+(a_i-1)^{q_i} = 1$$

it follows that $(a_i-1)^{\circledast} = -(a_i-1)+(a_i-1)^2-\cdots+(a_i-1)^{q_i-1}$. Note that for $i > l$ the equality $(a_i-1)^{\circledast} = (a_i-1)$ holds.

Let $\alpha \in L_1 \cup L_2$, $d = \alpha_1+\alpha_2+\cdots+\alpha_t$ and $k = \alpha_1+\alpha_2+\cdots+\alpha_l$. The above argument ensures that $z_\alpha{}^{\circledast} = (-1)^k z_\alpha + y$ for a suitable $y \in I^{d+1}$. It follows that if k is odd then

$$(1+z_\alpha)^{-1}(1+z_\alpha)^{\circledast} = (1-z_\alpha+z_\alpha^2-\cdots)(1-z_\alpha+y) \\ \equiv 1-2z_\alpha \pmod{I^{d+1}}$$

and for the even k we have

$$(1+z_\alpha)(1+z_\alpha)^{\circledast} = (1+z_\alpha)(1+z_\alpha+y) \equiv 1+2z_\alpha \pmod{I^{d+1}}.$$

Recall that $u_\alpha = 1+z_\alpha$ and define

$$z'_\alpha = \begin{cases} u_\alpha^{-1}u_\alpha^{\circledast}-1, & \text{if } \alpha \in L_1; \\ u_\alpha u_\alpha^{\circledast}-1, & \text{if } \alpha \in L_2; \\ z_\alpha, & \text{if } \alpha \in L_0. \end{cases}$$

As a consequence of the foregoing argument, we obtain, modulo I^{d+1},

$$z'_\alpha \equiv \begin{cases} 2z_\alpha, & \text{if } \alpha \in L_1; \\ -2_\alpha, & \text{if } \alpha \in L_2; \\ z_\alpha, & \text{if } \alpha \in L_0. \end{cases}$$

Now Lemma applies to the z'_α, yielding that the $u'_\alpha = 1+z'_\alpha$ with $\alpha \in L$ also generate $V(FG)$. We claim that in fact they form a basis for $V(FG)$. To this end, it now suffices to show that the products of their orders is no larger than order $V(FG)$. Clearly that if $u'_\alpha \ne u_\alpha$ then such u'_α is the image of u_α either under the endomorphism $v \mapsto v^{\circledast}v^{-1}$ or under the endomorphism $v \mapsto v^{\circledast}v$ of $V(FG)$ according to whether α belongs to L_1 or L_2. It follows that $|u'_\alpha| \le |u_\alpha|$, where $|u_\alpha|$ is the order of u_α. But [3] asserts that $\prod_{\alpha\in L}|u_\alpha|$ is the order of $V(FG)$ and this gives that $\prod_{\alpha\in L}|u'_\alpha| \le |V(FG)|$, so $\{u'_\alpha \mid \alpha \in L\}$ is a basis. It follows from the definition of the u'_α with $\alpha \in L$ that each of them is either fixed or inverted by the involution $\circledast$. Accordingly, this basis is the disjoint union of bases for the subgroups of symmetric and unitary normalized units, and these are the bases in the theorem. □

Acknowledgement. The authors would like to thank the referee for their valuable comments and suggestions for clarifying the exposition.

References

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

[2] S. A. Jennings, The structure of the group ring of a p-group over a modular field, *Trans. Amer. Math. Soc.* **50** (1941), 175–185.

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

ADALBERT BOVDI
INSTITUTE OF MATHEMATICS
UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: bodibela@math.klte.hu

A. SZAKÁCS
DEPARTMENT OF BUSINESS MATHEMATICS
TESSEDIK SAMUEL COLLEGE
H-5600 BÉKÉSCSABA
BAJZA U. 33.
HUNGARY

E-mail: szakacs@zeus.kf.hu

(Received January 4, 2006; revised September 1, 2006)