Publ. Math. Debrecen
65/3-4 (2004), 261–268

Group algebras with unit group of class p

By ZSOLT BALOGH (Nyíregyháza) and ADALBERT BOVDI (Debrecen)

Dedicated to the memory of Béla Brindza

Abstract. Let $V(\mathbb{F}_pG)$ be the group of normalized units of the group algebra $\mathbb{F}_pG$ of a finite nonabelian p-group G over the field $\mathbb{F}_p$ of p elements. Our goal is to investigate the power structure of $V(\mathbb{F}_pG)$, when it has nilpotency class p. As a consequence, we have proved that if G and H are p-groups with cyclic Frattini subgroups and $p > 2$, then $V(\mathbb{F}_pG)$ is isomorphic to $V(\mathbb{F}_pH)$ if and only if G and H are isomorphic.

1. Introduction

Let G be a finite p-group and $\mathbb{F}_pG$ its group algebra over the field $\mathbb{F}_p$ of p elements. The subgroup

$$V(\mathbb{F}_pG) = \left\{ \sum_{g\in G} \alpha_g g \in \mathbb{F}_pG \;\Big|\; \sum_{g\in G} \alpha_g = 1 \right\}$$

is called *the group of normalized units*. Evidently $V(\mathbb{F}_pG)$ is a finite p-group and its order is $p^{|G|-1}$.

It is well-known that if G is a finite nonabelian p-group then the nilpotency class of $V(\mathbb{F}_pG)$ is at least p. Mann and Shalev [10] have recently

Mathematics Subject Classification: Primary: 16A46, 16A26, 20C05; Secondary: 19A22.
Key words and phrases: group algebra, group of units, isomorphism problem.
Supported by OTKA grants No. T037202 and No. T043034.

shown that the nilpotency class of $V(\mathbb{F}_pG)$ is p if and only if the commutator subgroup G' is of order p. Our goal here is to study the power structure of $V(\mathbb{F}_pG)$ with nilpotency class p and to apply these results to the isomorphism problem of the group of units.

Since the modular isomorphism problem for finite p-groups has been positively resolved for some classes of finite p-groups, it is natural to investigate the question, originally raised by S. D. Berman, whether for a field $\mathbb{F}_p$ of characteristic p and finite p-groups G and H the isomorphism of groups $V(\mathbb{F}_pG)$ and $V(\mathbb{F}_pH)$ implies the isomorphism of G and H.

Note that Deskins [6] gave a positive answer to the isomorphism problem for finite abelian groups and the Berman's conjecture is true for these groups.

Further, the authors in [2] solved this problem for the group algebras of 2-groups of maximal class over the field of two elements, which is an extension of Baginski's result [1].

Note that, in general, for nonabelian p-groups the Berman's question is still open. In the present paper we give a positive answer to Berman's conjecture for p-groups of odd order with cyclic Frattini subgroup.

We introduce some additional notation. Let $\zeta(G)$ be the center and $\Phi(G)$ the Frattini subgroup of G, respectively; $G^p = \langle g^p \mid g \in G\rangle$, and let the commutator subgroup of G be denoted by G'. For each subset D of G, let $\widehat{D}$ denote the element $\sum_{g\in D} g$ of $\mathbb{F}_pG$.

2. Results

We begin with the description of the center $\zeta\big(V(\mathbb{F}_pG)\big)$ of $V(\mathbb{F}_pG)$, where G is a finite p-group with commutator subgroup G' of order p and $p > 2$. Let $C_{g_1}, \dots, C_{g_t}$ be all the different conjugacy classes of G which contain at least two elements. It is easy to check that $t = \frac{|G|-|\zeta(G)|}{p}$,

$$\widehat{C_{g_i}} = g_i\widehat{G'}, \qquad \widehat{C_{g_i}}\,\widehat{C_{g_j}} = 0 \qquad (1 \le i, j \le t)$$

and $\widehat{G'}$ is a central element with square 0.

Clearly, the set of all elements of the form $\sum_{i=1}^{t} \alpha_i\widehat{C_{g_i}}$ is an ideal of the center $\zeta(\mathbb{F}_pG)$. It follows that every central unit $x \in \zeta\big(V(\mathbb{F}_pG)\big)$ can

be written as

$$x = z + \sum_{i=1}^{t} \alpha_i \widehat{C_{g_i}} = z\Big(1 + \sum_{i=1}^{t} \beta_i \widehat{C_{g_i}}\Big) = z \prod_{i=1}^{t} \big(1 + g_i \widehat{G'}\big)^{\beta_i}, \qquad (1)$$

where $z \in V\big(\mathbb{F}_p\zeta(G)\big)$ and $\alpha_i, \beta_i \in \mathbb{F}_p$.

Also it is easy to check that

$$\begin{aligned} \big|V\big(\mathbb{F}_p\zeta(G)\big)\big| &= p^{|\zeta(G)|-1}, \\ \big|\zeta\big(V(\mathbb{F}_pG)\big)\big| &= p^{\frac{|G|+(p-1)|\zeta(G)|-p}{p}}, \end{aligned} \qquad (2)$$

and according to (1) we get

$$\zeta\big(V(\mathbb{F}_pG)\big) = V\big(\mathbb{F}_p\zeta(G)\big) \times N, \qquad (3)$$

where $N = \prod_{i=1}^{t} \langle 1 + \widehat{C_{g_i}} \rangle$ is an elementary abelian subgroup of $V(\mathbb{F}_pG)$.

Further, the commutator subgroup $V(\mathbb{F}_pG)'$ has exponent p because it is a subgroup of $1 + \mathfrak{I}(G')$ and $\mathfrak{I}(G')^p = 0$, where $\mathfrak{I}(G')$ is the ideal generated by the elements of the form $h - 1$ with $h \in G'$.

Denote by $[\mathbb{F}_pG, \mathbb{F}_pG]$ the span of all ring commutators $xy - yx$ with $x, y \in \mathbb{F}_pG$, which is called *the commutator subspace* of $\mathbb{F}_pG$.

Lemma 1 (Brauer, [5])**.** *An element $\sum_{g\in G} \alpha_g g$ belongs to the commutator subspace $[\mathbb{F}_pG, \mathbb{F}_pG]$ if and only if $\sum_{g\in C_h} \alpha_g = 0$ for every conjugacy class C_h of G. Moreover*

$$(x + y)^p \equiv x^p + y^p \pmod{[\mathbb{F}_pG, \mathbb{F}_pG]}$$

for any $x, y \in \mathbb{F}_pG$.

We start by investigating the p-th powers of the elements of $V(\mathbb{F}_pG)$.

Lemma 2. *Let G be a finite p-group with commutator subgroup G' of order $p > 2$. Then $V(\mathbb{F}_pG)^p$ is a subgroup of the center $\zeta\big(V(\mathbb{F}_pG)\big)$.*

Proof. Let H be the subgroup of $V(\mathbb{F}_pG)$ generated by x and y, where $x \in V(\mathbb{F}_pG)$, $g \in G$, and $y = g^{-1}xg$. Evidently,

$$(x, y) = x^{-1}(g, x)x(x, g) = \big(x, (x, g)\big) \in \gamma_3\big(V(\mathbb{F}_pG)\big),$$

so the subgroup $H\gamma_3\big(V(\mathbb{F}_pG)\big)/\gamma_3\big(V(\mathbb{F}_pG)\big)$ is abelian. Thus H' is contained in $\gamma_3\big(V(\mathbb{F}_pG)\big)$ and the nilpotency class of H is less than p. Then H is a regular p-group and so, according to Theorem 12.4.2 in [7], we have

$$x^{-p}y^p = (x^{-1}y)^p d^p = (x,g)^p d^p$$

for some element d of the commutator subgroup of $V(\mathbb{F}_pG)$. But $V(\mathbb{F}_pG)'$ has exponent p, so $x^{-p}y^p = 1$ and $x^p = g^{-1}x^p g$ for all $g \in G$. Thus x^p is central, as asserted. □

Lemma 3. *Let H be a group generated by two elements a, b, and suppose that its commutator subgroup H' is central of prime order p. In any group ring of H,*

$$(a+b)^p = a^p + b^p + \sum_{r=1}^{p-1} \frac{1}{p}\binom{p}{r} a^r b^{p-r} \widehat{H'}. \tag{4}$$

Proof. As a first step, observe that $\zeta(H) = \langle a^p, b^p\rangle H'$ has index p^2, and that the centralizer of any non-central element h is $\langle h\rangle\zeta(H)$. For $k, r \in \{1, 2, \dots, p-1\}$ and $c_1, \dots, c_p \in \{a, b\}$ with $c_1 \cdots c_p \in a^r b^{p-r} H'$, it follows that no element of the coset $a^r b^{p-r} H'$ can commute with the product $c_1 \cdots c_k$ and so

$$c_{k+1} \cdots c_p c_1 \cdots c_k = (c_1 \cdots c_k)^{-1}(c_1 \cdots c_p)(c_1 \cdots c_k) \neq c_1 \cdots c_p.$$

Next, consider the set of all words $z_1 z_2 \cdots z_p$ of length p in the alphabet $\{x, y\}$, as elements of the free semigroup S freely generated by $\{x, y\}$. The group of order p acts on this set by cyclically permuting the letters of a word. It is easy to see that there are only two words fixed under this action, x^p and y^p. Since p is prime, the length of each non-singleton orbit is p. There are precisely $\binom{p}{r}$ words in which x occurs r times and y occurs $p - r$ times, and we conclude that these are permuted in $\frac{1}{p}\binom{p}{r}$ orbits.

Let $\sigma : S \to H$ be the homomorphism defined by $x \mapsto a$, $y \mapsto b$. The images of the orbits we counted all lie in the coset $a^r b^{p-r} H'$. The point of the first step of our argument was to show that the restriction of σ to each of these orbits is one-to-one. Since each orbit has length p and this is also the number of elements in the coset, it follows that each element of $a^r b^{p-r} H'$ is the image of precisely $\frac{1}{p}\binom{p}{r}$ of the words under consideration.

The rest of the proof may now be left to the reader. □

Let $x = \sum_{g\in G} \alpha_g g \in V(\mathbb{F}_p G)$. From Lemma 1, we know that $x^p = y + u$, where $y = \sum_{g\in G} \alpha_g g^p$ and $u \in [\mathbb{F}_p G, \mathbb{F}_p G]$. Lemma 2 tells us that x^p and the g^p are central in $\mathbb{F}_p G$; therefore so is y, and then also u. By Lemma 1 again, the support of u cannot contain any element of $\zeta(G)$, so u must be a linear combination of the $\widehat{C_{g_i}}$. Thus $u^2 = 0$, and then

$$x^{p^2} = (y+u)^p = y^p = \left(\sum_{g\in G} \alpha_g g^p\right)^p = \sum_{g\in G} \alpha_g g^{p^2} \tag{5}$$

(because each g^p is central). We have proved that $V(\mathbb{F}_p G)^{p^2} = V(\mathbb{F}_p G^{p^2})$. When $\exp G > p$, this shows that the exponents of the groups $V(\mathbb{F}_p G)$ and G coincide. Consider next the case $\exp(G) = p$. Choose $a, b \in G$ with $(a,b) \neq 1$. Then $a + b - 1 \in V(\mathbb{F}_p G)$ and by (4) we have $(a+b-1)^p = (a+b)^p - 1 \neq 1$. It follows that

$$\exp\big(V(\mathbb{F}_p G)\big) = \begin{cases} \exp(G) & \text{if} \quad \exp(G) > p; \\ p^2 & \text{if} \quad \exp(G) = p. \end{cases} \tag{6}$$

Lemma 4 (Lemma III.9.6 in HUPPERT [8])**.** *Let $U(\mathbb{F}_p)$ be the group of units of $\mathbb{F}_p$ with odd prime p. Then*

$$\sum_{\gamma\in U(\mathbb{F}_p)} \gamma^r = \begin{cases} 0 & \text{for} \quad 1 \le r \le p-2; \\ p-1 & \text{for} \quad r = p-1. \end{cases}$$

Lemma 5. *Let G be a finite nonabelian p-group with $|\Phi(G)| = p$. Then $V(\mathbb{F}_p G)^p = V\big(\mathbb{F}_p G^p\big) \times N$, where $N = \prod_{i=1}^t \langle 1 + \widehat{C_{g_i}}\rangle$.*

PROOF. First we shall prove that $N \subseteq V(\mathbb{F}_p G)^p$. Let $\gamma \in U(\mathbb{F}_p)$, $g \in G \setminus \zeta(G)$ and $h \in G$ such that $(g,h) \neq 1$. The commutator subgroup of $\langle h, g^{-1}h\rangle$ coincides with G' and

$$\widehat{G'} h^{-p} = \widehat{G'}, \qquad \big((g^{-1}h)^p - 1\big)\widehat{G'} = 0, \tag{7}$$

because h^p, $(g^{-1}h)^p \in G'$.

Clearly, for each $\gamma \in U(\mathbb{F}_p)$ the element $u_\gamma = h + \gamma(g^{-1}h - 1)$ is a unit in $\mathbb{F}_p G$. By (4) and (7)

$$\begin{aligned} u_\gamma^p &= \big((h + \gamma g^{-1}h) - \gamma\big)^p = (h + \gamma g^{-1}h)^p - \gamma^p \\ &= h^p + \gamma\big((g^{-1}h)^p - 1\big) + \sum_{r=1}^{p-1} \tfrac{1}{p}\tbinom{p}{r} h^r (\gamma g^{-1}h)^{p-r} \widehat{G'}. \end{aligned}$$

It follows that, with γ ranging over $U(\mathbb{F}_p)$,

$$\prod_{\gamma\in U(\mathbb{F}_p)}(u_\gamma^p h^{-p}) = 1 + \Big(\sum_{\gamma\in U(\mathbb{F}_p)}\gamma\Big)\big((g^{-1}h)^p - 1\big)h^{-p} + \sum_{r=1}^{p-1}\tfrac{1}{p}\tbinom{p}{r}\Big(\textstyle\sum_{\gamma\in U(\mathbb{F}_p)}\gamma^{p-r}\Big)h^r(g^{-1}h)^{p-r}\widehat{G'}$$

and here, by Lemma 4, all summands with $r > 1$ vanish, leaving

$$\prod_{\gamma\in U(\mathbb{F}_p)}(u_\gamma^p h^{-p}) = 1 - h(g^{-1}h)^{p-1}\widehat{G'}.$$

Since $(g^{-1}h)^p\widehat{G'} = \widehat{G'}$ by (7), we have $h(g^{-1}h)^{-1}(g^{-1}h)^p\widehat{G'} = g\widehat{G'}$ and

$$\prod_{\gamma\in U(\mathbb{F}_p)}(u_\gamma^p h^{-p}) = 1 - g\widehat{G'} = (1 + g\widehat{G'})^{-1}.$$

Thus $1 + g\widehat{G'} = \big(\prod_{\gamma\in U(\mathbb{F}_p)}(u_\gamma^p h^{-p})\big)^{-1} \in V(\mathbb{F}_pG)^p$. Since the elements of the form $1 + g\widehat{G'}$ constitute a generator system of N, we have proved that $N \subseteq V(\mathbb{F}_pG)^p$, as required.

Let G^p be a nontrivial subgroup of G. Since $\Phi(G)$ is cyclic, then $G^p = \langle g^p\rangle$ for some $g \in G$ and

$$V(\mathbb{F}_p\langle g^p\rangle) \subseteq V(\mathbb{F}_p\langle g\rangle)^p \subseteq V(\mathbb{F}_pG)^p.$$

Thus we have proved that $V\big(\mathbb{F}_pG^p\big) \times N \subseteq V(\mathbb{F}_pG)^p$.

Finally, the relation $V(\mathbb{F}_pG)^p \subseteq V\big(\mathbb{F}_pG^p\big) \times N$ follows from (5) and the prove is complete. □

The question: for which p-group G is it true that $G \cap V(\mathbb{F}_pG)^p = G^p$, is due to Johnson [9]. The previous lemma can be applied to conclude the following

Corollary. *Let G be a finite p-group such that $|\Phi(G)| = p > 2$. Then*

$$G \cap V(\mathbb{F}_pG)^p = G^p.$$

Proof. By Lemma 5 we get $V(\mathbb{F}_pG)^p = V\big(\mathbb{F}_pG^p\big) \times N$, and so

$$G \cap V(\mathbb{F}_pG)^p = G \cap V\big(\mathbb{F}_pG^p\big) = G^p.$$ □

Theorem. *Let G and H be finite nonabelian p-groups with cyclic Frattini subgroup and $p > 2$. Then $V(\mathbb{F}_pG)$ is isomorphic to $V(\mathbb{F}_pH)$ if and only if G and H are isomorphic.*

Proof. We say that G is a central product $G_1 \curlyvee G_2$ of its subgroups G_1 and G_2 if the elements of G_1 and G_2 commute and together generate G, and $G_1 \cap G_2$ is the center of one of the factors G_1, G_2.

It follows (for example) from Theorem 2 in [3] that, when $p > 2$, every finite nonabelian p-group G with cyclic Frattini subgroup may be written as

$$G = E \times (K \curlyvee L), \tag{8}$$

where E is elementary abelian, K is either of order p or an extraspecial group of exponent p, and L is either nontrivial cyclic or nonabelian with a cyclic maximal subgroup, that is, L is either $C_{p^n} = \langle a \mid a^{p^n} = 1\rangle$ with $n \geq 1$ or

$$M_{p^n} = \langle a, b \mid a^{p^{n-1}} = b^p = 1,\ (a,b) = a^{p^{n-2}}\rangle \quad \text{with } n \geq 3.$$

It is obvious that L is cyclic if and only if $\exp(G) = \exp\big(\zeta(G)\big)$; in this case, $|L| = \exp(G)$ and $|K| = p \cdot |G : \zeta(G)|$, and otherwise $|L| = p \cdot \exp(G)$ and $|L| = p^{-1} \cdot |G : \zeta(G)|$. Consequently, the isomorphism type of such a group is determined by the orders and exponents of the group and its center.

The nontrivial part of the proof of the theorem is the claim that these four invariants of G are recognizable from the isomorphism type of $V(\mathbb{F}_pG)$.

First, $|G|$ is recognizable from $|V(\mathbb{F}_pG)|$, and then $|\zeta(G)|$ can be computed from $\big|\zeta\big(V(\mathbb{F}_pG)\big)\big|$ and (2). Using (1), it is not hard to see that

$$\exp(\zeta(G)) = \exp\big(\zeta(V(\mathbb{F}_pG)\big).$$

It remains to show that the exponent of G is also recognizable. By (6) if $\exp\big(V(\mathbb{F}_pG)\big) > p^2$, then $\exp\big(V(\mathbb{F}_pG)\big) = \exp(G)$ and so we only have an issue when $\exp\big(V(\mathbb{F}_pG)\big) = p^2$.

In this outstanding case $\exp(G) \leq p^2$, so we obtain that $|\Phi(G)| = p$. Indeed, it is clearly for the group G with $\exp(G) = p$. If $\exp(G)$ is equal to p^2 then by (8) $\exp(G) = \exp(L) = p^2$. Clearly $\Phi(G) = \Phi(L)$ and from the fact that L is isomorphic to either C_{p^2} or M_{p^3} follows that the subgroup $\Phi(G)$ has order p.

Then by Lemma 5 $V(\mathbb{F}_pG)^p = V\left(\mathbb{F}_pG^p\right) \times N$, where $|N| = p^{\frac{|G|-|\zeta(G)|}{p}}$. Therefore we can determine whether $|G^p|$ is either 1 or p. We have proved that the exponent of G is also recognizable, as required. □

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

References

[1] C. Baginski, Modular group algebras of 2-groups of maximal class, *Comm. algebra* **20**(5) (1992), 1229–1241.

[2] Zs. Balogh and A. Bovdi, Units of order two of group algebras of 2-groups of maximal class, *Comm. Algebra* **32**, no. 8 (2004), 3227–3245.

[3] T. R. Berger, L. G. Kovács and M. F. Newman, Groups of prime power order with cyclic Frattini subgroup, *Nederl. Akad. Wetensch. Indag. Math.* **42**, no. 1 (1980), 13–18.

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

[5] R. Brauer, Zur Darstallungstheorie der Gruppen endlicher Ordnung, *Math. Z.* **63** (1956), 406–444.

[6] W. E. Deskins, Finite abelian groups with isomorphic group algebras, *Duke Math. J.* **23** (1956), 35–40.

[7] M. Hall, The theory of groups, *Macmillan, New York*, 1959.

[8] B. Huppert, Endlichen Gruppen I, *Springer-Verlag, Berlin*, 1967.

[9] D. L. Johnson, The modular group ring of a finite p-group, *Proc. Amer. Math. Soc.* **68**, no. 1 (1978), 19–22.

[10] A. Mann and A. Shalev, The nilpotency class of the unit group of a modular group algebra II, *Israel J. Math.* **70** (1990), 267–277.

zsolt balogh
institute of mathematics and informatics
college of nyíregyháza
sóstói út 31/b, h-4410 nyíregyháza
hungary

E-mail: baloghzs@nyf.hu

adalbert bovdi
institute of mathematics
university of debrecen
4010 debrecen, p.o. box 12
hungary

E-mail: bodibela@math.klte.hu

(Received May 5, 2004; revised October 6, 2004)