

## ON THE RADICAL OF THE GROUP ALGEBRA OF A $p$ -GROUP OVER A MODULAR FIELD

GAIL L. CARNS AND CHONG-YUN CHAO<sup>1</sup>

**ABSTRACT.** Let  $G$  be a finite  $p$ -group,  $K$  be the field of integers modulo  $p$ ,  $KG$  be the group algebra of  $G$  over  $K$  and  $N$  be the radical of  $KG$ . By using the fact that the annihilator,  $A(N)$ , of  $N$  is one dimensional, we characterize the elements of  $A(N^2)$ . We also present relationships among the cardinality of  $A(N^2)$ , the number of maximal subgroups in  $G$  and the number of conjugate classes in  $G$ . Theorems concerning the Frattini subalgebra of  $N$  and the existence of an outer automorphism of  $N$  are also proved.

**1. Introduction.** Throughout this note, we let  $p$  be a prime,  $G$  be a finite  $p$ -group,  $K$  be the field of integers modulo  $p$  and  $KG$  be the group algebra of  $G$  over  $K$ . It is well known that  $KG$  is not semisimple; the fundamental ideal  $N = \{\sum_{g \in G} \alpha_g g \in KG; \sum_{g \in G} \alpha_g = 0\}$  of  $KG$  is its radical ([3], [6]). Let  $e$  be the identity of  $G$ , then the elements  $g - e$  for all  $g \neq e$  in  $G$  constitute a basis for  $N$ . Hence, the dimension,  $\dim N$ , of  $N$  is equal to  $|G| - 1$  where  $|G|$  is the order of  $G$ . Also,  $KG$  is the semidirect sum of the ideal  $N$  and the subalgebra  $\langle e \rangle$ . The nilpotent associative algebra  $N$  is said to be of exponent  $t$  if  $N^t \neq 0$  and  $N^{t+1} = 0$ , i.e.,

$$N = N^1 \supset N^2 \supset \cdots \supset N^t \supset N^{t+1} = 0.$$

Recently, Hill in [2] showed that the annihilator (two sided) of  $N^i$ ,  $A(N^i)$ , is  $N^{t+1-i}$ ,  $1 \leq i \leq t$ . In this note we shall present some properties of  $N$  by centering around the fact that  $A(N)$  is isomorphic to  $K$ , i.e., the dimension of  $A(N)$  is one. In §2, we present a characterization of elements in  $A(N^2)$  and relationships among the cardinality,  $|A(N^2)|$ , of  $A(N^2)$ , the number of maximal subgroups of  $G$  and the number of conjugate classes in  $G$ . In particular,  $\dim A(N^2)$  is equal to the least number of generators of  $G$  plus one. In §3, we show that the Frattini subalgebra of any associative nilpotent algebra  $U$  over a field is  $U^2$ . We also use Stitzinger's results in [7]

---

Received by the editors September 2, 1971.

AMS 1970 subject classifications. Primary 16A26; Secondary 16A22.

**Key words and phrases.** Modular group algebra, radical, annihilator, center, dimension, maximal subgroups, conjugate classes, Frattini subalgebra, nonimbedding, outer automorphism.

<sup>1</sup> The authors wish to thank the referee for his helpful suggestions.

to state the nonimbedding properties of  $N$ . In §4, analogous to Gaschütz' result in [1] on the existence of an outer  $p$ -automorphism of a finite nonabelian  $p$ -group, we show that  $N$  has an automorphism of order  $p$  which is not inner if  $|G| > 2$ .

**2. A characterization of elements in  $A(N^2)$ .** For each element  $\alpha = \sum_{g \in G} \alpha_g g \in KG$ , we may associate a map  $\alpha$  from  $G$  to  $K$  defined by  $\alpha(g) = \alpha_g$ . Clearly, this correspondence between  $\alpha$  and  $\alpha$  is one-to-one. Also, the addition of two such maps is defined as pointwise, i.e.,  $(\alpha + \beta)(g) = \alpha(g) + \beta(g)$ . Let  $N$  be the fundamental ideal of exponent  $t$  in  $KG$ . Then, by Hill's result in [2], we know  $A(N) = N^t$ . Also, one can easily verify that  $k \in A(N) = N^t$  if and only if  $k$  is a constant map, i.e.,  $k(g) = k$  for every  $g \in G$  and  $N^t = \langle (\sum_{g \in G} g) \rangle$ .

**THEOREM 1.** *Let  $N$  be the fundamental ideal of exponent  $t > 1$  in  $KG$  and  $\text{Hom}(G, K^+)$  be the set of group homomorphisms of  $G$  into the additive group  $K^+$  of the integers modulo  $p$ . Then  $\alpha \in A(N^2)$  if and only if  $\alpha = \alpha^* + k$  for some  $\alpha^* \in \text{Hom}(G, K^+)$  and some constant map  $k$ . Further,  $\alpha^*$  and  $k$  are unique for  $\alpha$ .*

**PROOF.** If  $\alpha = \alpha^* + k$  for some  $\alpha^* \in \text{Hom}(G, K^+)$  and some constant map  $k$ , then for every  $g \in G$ , we have

$$(1) \quad \alpha^*(g) = \alpha(g) - k(g) = \alpha_g - k.$$

Also, by using (1) and  $\alpha^*(gh) = \alpha^*(g) + \alpha^*(h)$ , we have

$$(2) \quad \alpha_{gh} = \alpha_g + \alpha_h - k$$

for all  $g, h \in G$ . Now by using (2), for all  $h, u \in G$ , we have

$$\begin{aligned} (h - e)(u - e)\alpha &= (hu - h - u + e) \left( \sum_{g \in G} \alpha_g g \right) \\ &= \sum_{g \in G} (\alpha_g hug - \alpha_g hg - \alpha_g ug + \alpha_g g) \\ &= \sum_{g \in G} (\alpha_{u^{-1}h^{-1}g} - \alpha_{h^{-1}g} - \alpha_{u^{-1}g} + \alpha_g)g \\ &= \sum_{g \in G} [(\alpha_{u^{-1}} + \alpha_{h^{-1}g} - k) - \alpha_{h^{-1}g} - (\alpha_{u^{-1}} + \alpha_g - k) + \alpha_g]g \\ &= 0 \end{aligned}$$

Similarly,  $\alpha(h - e)(u - e) = 0$ . It follows that  $\alpha \in A(N^2)$ .

Conversely, if  $\alpha \in A(N^2)$ , then for all  $h, u \in G$ ,

$$0 = (h^{-1} - e)(u^{-1} - e) \left( \sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} (\alpha_{uhg} - \alpha_{hg} - \alpha_{ug} + \alpha_g)g.$$

In particular, the coefficient of  $e$  is zero, i.e.,

$$\alpha_{uh} = \alpha_u + \alpha_h - \alpha_e,$$

or

$$(3) \quad \alpha(uh) = \alpha(u) + \alpha(h) - \alpha_e.$$

Let  $k = \alpha_e$  and  $\alpha^* = \alpha - k$ , then (3) can be written as

$$\alpha^*(uh) = \alpha^*(u) + \alpha^*(h),$$

i.e.,  $\alpha^* \in \text{Hom}(G, K^+)$ .

The uniqueness follows from the fact that  $\alpha^*(e) = 0$  yields  $\alpha(e) = k(e)$ .

REMARK. By Hill's result in [2], in Theorem 2,  $A(N^2)$  can be replaced by  $N^{t-1}$ .

COROLLARY 1.1. Let  $r = \dim A(N^2) = \dim N^{t-1}$ ,  $m =$  the number of maximal subgroups of  $G$ ,  $d =$  the least number of elements which generate  $G$ ,  $c =$  the number of conjugate classes in  $G$  and  $\phi(G) =$  the Frattini subgroup of  $G$ . Then,

- (i)  $|A(N^2)| = p \cdot |(G/\phi(G))|$ ,
- (ii)  $m = \sum_{i=0}^{r-2} p^i$ ,
- (iii)  $r = d + 1$ ,
- (iv)  $G$  is cyclic if and only if  $r = 2$ ,
- (v)  $G$  is elementary abelian if and only if  $r = n + 1$  where  $|G| = p^n$ ,
- (vi)  $m = \sum_{i=0}^{d-1} p^i$ ,
- (vii)  $A(N^2) = N^{t-1} \subseteq Z(N)$  where  $Z(N)$  is the center of  $N$ ,
- (viii)  $m \leq \sum_{i=0}^{c-4} p^i$  if  $|G| > 4$ .

PROOF. (i) By Theorem 1,  $|A(N^2)| = p \cdot |\text{Hom}(G, K^+)|$ . Since  $K^+$  is a simple group, the kernel of any nonzero map  $\eta$  in  $\text{Hom}(G, K^+)$  is a maximal subgroup in  $G$ . Since the kernel of  $\eta$  contains the kernel of the natural map from  $G$  onto  $G/\phi(G)$ , any homomorphism of  $G$  into  $K^+$  can be factored through  $G/\phi(G)$ . Thus,  $|\text{Hom}(G, K^+)| = |\text{Hom}(G/\phi(G), K^+)|$ . Also,  $G/\phi(G)$  is elementary abelian and every finite abelian group is isomorphic to its dual group [5, p. 50], therefore we have

$$|\text{Hom}(G/\phi(G), K^+)| = |G/\phi(G)|.$$

Consequently,

$$|A(N^2)| = p \cdot |\text{Hom}(G, K^+)| = p \cdot |G/\phi(G)|.$$

(ii) Let  $\sigma$  be a nonzero homomorphism of  $G$  onto  $K^+$ . Then the kernel of  $\sigma$  is a maximal subgroup of  $G$ . Two nonzero homomorphisms in  $\text{Hom}(G, K^+)$  have the same kernel if and only if they differ by an automorphism of  $K^+$ . Thus,  $|\text{Hom}(G, K^+)| = 1 + (p-1)m$  and  $p^r = |A(N^2)| = p \cdot |\text{Hom}(G, K^+)| = p(1 + (p-1)m)$ , i.e.,  $m = \sum_{i=0}^{r-2} p^i$ .

(iii) By (i),  $r = \dim(A(N^2)) = \dim_K(G/\phi(G)) + 1$  and, by the Burnside basis theorem,  $\dim_K(G/\phi(G)) = d$ .

(iv), (v) and (vi) follow from (i), (ii) and (iii).

REMARK. By using Corollary 14 in [2] we can state: If  $r=2$ ,  $KG$  has exactly one ideal of each dimension.

(vii) It is well known that the conjugate sums  $C^1=e$ ,  $C^2, \dots, C^c$  constitute a basis for the center,  $Z(KG)$ , of  $KG$  where each  $C^i$  is the sum of elements in a conjugate class in  $G$ . Let  $\alpha = \sum_{g \in G} \alpha_g g$  be an arbitrary element in  $A(N^2)$ . If  $u$  and  $h$  are conjugates in  $G$ , i.e.,  $h = vuv^{-1}$  for some  $v \in G$ , then, by using Theorem 1, we have

$$\alpha_h = \alpha^*(h) + k = \alpha^*(vuv^{-1}) + k = \alpha^*(u) + k = \alpha_u.$$

Hence,  $\alpha$  is a linear combination of conjugate sums, i.e.,  $\alpha \in Z(KG)$ . Since  $Z(N) = Z(KG) \cap N$ ,  $A(N^2) \subseteq Z(N)$ .

(viii) Since  $Z(N) = Z(KG) \cap N$  and  $e \in Z(KG)$  and  $e \notin N$ ,  $\dim Z(N) < \dim Z(KG) = c$ . Let  $a_i$ ,  $2 \leq i \leq c$ , be the cardinality of the conjugate class from which the sum  $C^i$  is taken. We note that since  $G$  is a  $p$ -group,  $a_i$  is equal to a power of  $p$  greater than one if the conjugate class consists of more than one element. Since  $C^1, C^2, \dots, C^c$  constitute a basis for  $KG$ ,  $C^2 - a_2 e, C^3 - a_3 e, \dots, C^c - a_c e$  are in  $Z(N)$  and are linearly independent. Hence,  $\dim Z(N) = c - 1$ .

Since  $G$  is a  $p$ -group, there is a nonidentity  $h$  in  $Z(G)$  such that  $h - e \notin N^{t-1}$ . The reason is that if  $h - e$  belonged to  $N^{t-1}$ , then  $(u - e)(h - e) = \sum_{g \in G} g$  for some  $u \in G$ . This is impossible since  $|G| > 4$ . Consequently,  $A(N^2) \neq Z(N)$  and  $p(1 + (p-1)m) = |A(N^2)| < p^{c-1}$ , i.e.,  $p(1 + m(p-1)) \leq p^{c-2}$ , and  $m \leq (p^{c-3} - 1)/(p-1) = \sum_{i=0}^{c-4} p^i$ .

REMARK. If  $G$  is the dihedral group of order 8 and if  $K$  is the field of integers modulo 2, then  $m=3$ ,  $c=5$  and the equality in (viii) holds.

**3. Nonimbedding.** Let  $S$  be an associative algebra (not necessarily finite dimensional) over a field. The Frattini subalgebra,  $\phi(S)$ , of  $S$  is defined as the intersection of all maximal subalgebras of  $S'$  if maximal subalgebras of  $S'$  exist and as  $S$  otherwise. Stitzinger showed in [7, p. 531] that if  $B$  is a nontrivial finite dimensional nilpotent associative algebra over a field such that the right annihilator of  $B$  is one dimensional, then  $B$  cannot be imbedded as an ideal in any associative algebra  $S$  contained in  $\phi(S)$ .

**THEOREM 2.** *Let  $U$  be a nilpotent associative algebra over a field  $F$ . Then  $\phi(U) = U^2$ .*

In order to prove Theorem 2, we need the following: We define the normalizer,  $n_V(W)$ , of a subalgebra  $W$  in an associative algebra  $V$  over a field  $F$  to be  $\{v \in V : vW \subseteq W \text{ and } Wv \subseteq W\}$ . We say that a subalgebra  $W$  is self-normalizing if  $n_V(W) = W$ .

LEMMA 1. Let  $V$  be a nilpotent associative algebra of exponent  $t > 1$  over a field  $F$ . If  $W$  is a proper subalgebra of  $V$  then  $W$  is not self-normalizing.

PROOF.  $W$  contains  $V^{t+1} = 0$ . Assume that  $W$  contains  $V^j$  and does not contain  $V^{j-1}$ . Then  $W + V^j \subseteq W$  and  $W + V^{j-1} \not\subseteq W$ . Also,

$$(W + V^{j-1})W \subseteq W + V^j \subseteq W \quad \text{and} \quad W(W + V^{j-1}) \subseteq W + V^j \subseteq W.$$

Hence,  $n_V(W) \not\subseteq W$ .

The proof of Theorem 2 goes as follows: We claim that  $U^2 \supseteq \phi(U)$ . Since  $U/U^2$  has zero multiplication, every maximal subspace  $\bar{M}_\alpha$  of the vector space  $U/U^2$  is a maximal subalgebra. Hence  $M_\alpha + U^2$  is a maximal subalgebra in  $U$  and  $U^2 \supseteq \phi(U)$ .

Now we show that  $\phi(U) \supseteq U^2$ . Let  $M$  be any maximal subalgebra of  $U$ . By Lemma 1,  $M$  is an ideal in  $U$ . Hence,  $\bar{U} = U/M \neq \bar{0}$ . Since  $M$  is maximal and  $U$  is nilpotent,  $\bar{U}$  is a nilpotent algebra with no proper subalgebras. Since  $\bar{U}^2$  is a subalgebra of  $\bar{U}$  and  $\bar{U}$  is nilpotent,  $\bar{U}^2 = \bar{0}$ , i.e.,  $U^2 \subseteq M$  for any arbitrary maximal subalgebra  $M$  of  $U$ . It follows that  $U^2 \subseteq \phi(U)$ .

COROLLARY 2.1. Let  $N$  be the fundamental ideal of  $KG$  where  $|G| > 2$ . Then  $N$  cannot be imbedded as an ideal in any finite nilpotent associative algebra  $B$  over  $K$  such that  $B^2 \supseteq N$ .

PROOF. It follows from  $\dim A(N) = 1$ , Stitzinger's result in [7] and our Theorem 2.

4. **Outer automorphisms.** Let  $R$  be a ring with an identity  $e$ , then, for a right quasi-regular element  $a$  in  $R$ ,  $\omega_a(x) = x + a'x + xa + a'xa = (e + a')x(e + a)$ , where  $a'$  is a right quasi-inverse of  $a$ , is an automorphism of  $R$  called an inner automorphism of  $R$ . As indicated on p. 55 in [4], the algebra which has a basis  $\{x, y, z\}$  over the field of integers modulo 2 with the multiplication defined by  $xy = z$  and all other products being zero has no outer (noninner) automorphism. Since every nilpotent element is right quasi-regular and since  $N$  is a nilpotent ideal in  $KG$ , for each  $q \in N$ ,  $\omega_q(x) = (e + q')x(e + q)$  is an inner automorphism of  $N$ . In fact, each automorphism  $\bar{\omega}$  of  $G$  induces an automorphism  $\omega$  on  $N$  defined linearly by  $\omega(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} \alpha_g (\bar{\omega}g)$ . If  $\bar{\sigma}_g(h) = g^{-1}hg$  is an inner automorphism of  $G$ , then one can easily verify that it induces an automorphism on  $N$  which is equal to the inner automorphism  $\omega_{g-e}$  on  $N$ . Although Gaschütz showed in [1] that every nonabelian  $p$ -group  $G$  possesses a noninner automorphism whose order is a power of  $p$ , it is not known whether this outer automorphism of  $G$  induces an outer automorphism on  $N$ . However, by using  $A(N) = \langle (\sum_{g \in G} g) \rangle$  we can prove the following

THEOREM 3. Let  $N$  be the fundamental ideal of  $KG$  where  $|G| > 2$ . Then  $N$  has an automorphism of order  $p$  which is not inner.

PROOF. Let  $h \in G$ ,  $(h-e) \in N$  and  $(h-e) \notin N^2$ . Since  $(h-e) \notin N^2$ , we may choose a complementary subspace  $M$  of  $\langle(h-e)\rangle$  in  $N$  such that  $M \supseteq N^2$ . Then  $N = M + \langle(h-e)\rangle$  where the sum is the direct sum of vector spaces. Since  $|G| > 2$ ,  $z = \sum_{g \in G} g \in N^2 \subseteq M$  and  $M \neq 0$ . Since every element  $x \in N$  can be uniquely written as  $x = y + k(h-e)$  where  $y \in M$  and  $k \in K$ , we can define a linear transformation  $T$  on  $N$  such that  $Ty = y$  and  $T(k(h-e)) = k(h-e) + kz$ . We claim that  $T$  is an automorphism. By using  $z \in A(N)$  and  $M$  being an ideal in  $N$  (since  $M \supseteq N^2$ ), it follows that  $T$  is an endomorphism. Also,  $T(y + k(h-e) - kz) = y + k(h-e)$  indicates that  $T$  is surjective. Hence,  $T$  is an automorphism.

We claim that  $T$  is not inner. Suppose the contrary, i.e., there existed a  $q \in N$  such that  $T = \omega_q$ , then, we would, in particular, have

$$(4) \quad (h-e) + z = T(h-e) = \omega_q(h-e) = (e+q')(h-e)(e+q).$$

Multiplying both sides of (4) by  $(e+q)$ , we obtain

$$(h-e) + z + q(h-e) = (h-e) + (h-e)q,$$

i.e.,  $z = hq - qh$ . Say  $q = \cdots + \alpha_{h-1}h^{-1} + \cdots$ , then  $z = (\alpha_{h-1} - \alpha_{h-1})e + \cdots$ . But  $z = \sum_{g \in G} g$ . Hence, it is a contradiction, and  $T$  is not inner.

Since  $T^p(x) = T^p(y + k(h-e)) = y + k(h-e) + pkz = x$  for every  $x \in N$ ,  $T$  is of order  $p$ .

#### REFERENCES

1. W. Gaschütz, *Nichtabelsche  $p$ -Gruppen besitzen äussere  $p$ -Automorphismen*, J. Algebra. **4** (1966), 1-2. MR **33** #1365.
2. 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. MR **41** #6995.
3. 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. MR **3**, 34.
4. R. L. Kruse and D. T. Price, *Nilpotent rings*, Gordon and Breach, New York, 1969. MR **42** #1858.
5. Serge Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965. MR **33** #5416.
6. Gerald Losey, *On group algebras of  $p$ -groups*, Michigan Math. J. **7** (1960), 237-240. MR **23** #A212.
7. E. L. Stitzinger, *A nonimbedding theorem of associative algebras*, Pacific J. Math. **30** (1969), 529-531. MR **40** #7307.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PITTSBURGH, PITTSBURGH, PENNSYLVANIA 15213.