Journal of Mathematical Sciences, Vol. 102, No. 3, 2000

ON THE ADJOINT GROUP OF A FINITE NILPOTENT p-ALGEBRA

B. Amberg and L. S. Kazarin UDC 512.554.31

The structure of the adjoint group R° of a finite nilpotent p-algebra R is considered under suitable additional conditions. For instance, the cases where R contains a large power subalgebra or has dimension at most 5, or when R° has small Prüfer rank, are studied.

1. Introduction

An associative algebra over the Galois field $GF(p)$ for some prime p is called a *p-algebra*. Nilpotent p-algebras have been studied in several papers (see, for example, [15, 20]). A nilpotent algebra R forms a group under the "circle" operation $x \circ y = xy + x + y$ for every two elements x and y in R. This group is called the *adjoint* or *circle group* of R and is denoted by R°. It is well known that the adjoint group of a nilpotent p-algebra is a p-group (see, for example, [3]). This raises the question of which finite p-groups occur as the adjoint group of some (finite) nilpotent p-algebra.

It is clear that every elementary abelian p-group is the adjoint group of the corresponding null algebra. On the other hand, for example, the group $\mathbb{Z}_{p^2}$ can only be the adjoint group of some nilpotent p-algebra if $p = 2$. In general, there will be many nilpotent p-algebras with isomorphic (nilpotent) adjoint groups. For example, it is observed in [15, Chapter V] that there are at least 100,000 nilpotent rings and more than 35,000 nilpotent 2-algebras of order 2^6, but only 267 groups of order 2^6.

In the following, we classify certain finite nilpotent p-algebras under additional restrictions. In Sec. 2, nilpotent p-algebras with large power subalgebras are studied. The latter correspond to cyclic subgroups in groups and algebras with large nilpotency class.

In Sec. 3, we study nilpotent p-algebras whose adjoint groups have small Prüfer rank. It is, for instance, shown that a Miller–Moreno p-group occurs as the adjoint group of some nilpotent p-algebra only when the order of this group is extremely small. Also, it is proved that the adjoint group of a nilpotent p-algebra with $p > 2$ has at least 3 generators provided the dimension of the corresponding algebra is at least 4 (see Theorem 3.4).

In Sec. 4, the adjoint group of a nilpotent p-algebra with dimension at most 5 is investigated. In [21], the adjoint groups of nilpotent p-rings for a prime number $p > 2$ were determined by relatively complicated methods.

Finally, in Sec. 5, we discuss some constructions that are useful to prove that some particular groups occur as the adjoint group of some p-algebra.

The notation is standard (see [3, 15]). With few exceptions all groups and algebras are finite.

Acknowledgment. The second author would like to thank the Deutsche Forschungsgemeinschaft (DFG) and the RFFI for financial support, and the Department of Mathematics of the University of Mainz for its excellent hospitality during the preparation of this paper.

2. Nilpotent p-Algebras with Large Power Subalgebras

An algebra $R = \langle\langle a\rangle\rangle$ over the field F is said to be a *power algebra* if there exists an element $a \in R$ such that every element of R can be expressed as $f(a)$ for some polynomial $f \in F[x]$. The least positive integer m such that $a^{m-1} \neq 0 = a^m$ is called the nillity (index) $\nu(a) = m$. Here $\nu(a) = \dim(R) + 1 = n(R) + 1$, where $n(R)$ is the nilpotency class of R. The nillity $\nu(R)$ of R is the maximum of all $\nu(a)$, where a runs through the elements of R. Obviously, $\nu(R) \leq n(R) + 1 \leq \dim(R) + 1$. The subalgebra of R generated by the elements $x_1, x_2, \dots, x_s$ will be denoted by $\langle\langle x_1, x_2, \dots, x_s\rangle\rangle$, whereas the subspace of R generated by these elements is $\langle x_1, x_2, \dots, x_s\rangle$. Multiplication in the algebra R will be denoted by $\cdot$, while multiplication in its

Translated from Itogi Nauki i Tekhniki, Seriya Sovremennaya Matematika i Ee Prilozheniya. Tematicheskie Obzory. Vol. 63, Algebra–13, 1999.

1072–3374/00/1023–3979 \$ 25.00 © 2000 Kluwer Academic/Plenum Publishers

adjoint group R° by $\circ$. The kth power of an element $x \in R^\circ$ is $x^{(k)}$, and the kth power of x in R is x^k. Note that if $k = p^m$ for some positive integer m, where p is the characteristic of the ground field F, then we have $x^k = x^{(k)}$. The annihilator of the subset S of R is $\mathrm{Ann}(S) = \{r \in R | rs = sr = 0 \text{ for any } s \in S\}$.

The structure of the adjoint group of the nilpotent power p-algebra $R = \langle\langle a \rangle\rangle$ can easily be described. Assume that $\dim(R) = n$, i.e., $a^{n+1} = 0 \neq a^n$. Then $\nu(a) = n + 1$ and the rank of the adjoint group of R is $r(R^\circ) = r = n - [n/p]$ (see [2]). For a power p-algebra R, define a matrix $M(R) = (\alpha_{ij})$ of size $l \times r$, where $l = 1 + [\log_p n]$ and r is as above. The elements $\alpha_{11}, \alpha_{12}, \dots, \alpha_{1l}$ of the first row are integers between n and $n - [n/p] + 1$, namely $\alpha_{11} = n$ and $\alpha_{1i+1} = \alpha_{1i} - 1$ for $i = 1, 2, \dots, l - 1$. The elements in each column are as follows: if α_{1j} is the first element in the jth column, then we put $\alpha_{2j} = \alpha_{1j}/p$ if p divides α_{1j} and $\alpha_{2j} = 0$ otherwise. The elements α_{kj} are defined inductively by $\alpha_{k+1j} = \alpha_{kj}/p$ if p divides α_{kj} and $\alpha_{k+1j} = 0$ otherwise for each $k = 1, 2, \dots, l$.

By way of illustration, consider the following example: $R = \langle\langle a \rangle\rangle$, $n = \dim R = 28$, $p = 3$. Then $r = 28 - [28/3] = 19$ and $l = [\log_3 28] + 1 = 4$. Hence

$$M(R) = \begin{pmatrix} 28 & 27 & 26 & 25 & 24 & 23 & 22 & 21 & 20 & 19 & 18 & 17 & 16 & 15 & 14 & 13 & 12 & 11 & 10 \\ 0 & 9 & 0 & 0 & 8 & 0 & 0 & 7 & 0 & 0 & 6 & 0 & 0 & 5 & 0 & 0 & 4 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

The matrix $M(R)$ is of type $(m_1, m_2, \dots, m_l)$ if it has m_1 columns with exactly 1 nonzero element, m_2 columns with 2 nonzero elements, ..., m_l columns with l nonzero elements. Note that $\sum_{i=1}^{l} i m_i = n$. Thus, in above example $M(R)$ is of type (13,4,1,1) and $1 \cdot 13 + 2 \cdot 4 + 3 \cdot 1 + 4 \cdot 1 = 28$.

Theorem 2.1. *Let $R = \langle\langle a \rangle\rangle$ be a nilpotent power p-algebra of dimension n whose matrix $M(R)$ is of type $(m_1, m_2, \dots, m_l)$. Then the adjoint group of R is isomorphic to a group*

$$G = \mathbb{Z}_p{}^{m_1} \times \mathbb{Z}_{p^2}{}^{m_2} \times \ldots \times \mathbb{Z}_{p^l}{}^{m_l}.$$

Proof. It follows from the description of $M(R)$ that $1 \cdot m_1 + 2 \cdot m_2 + \ldots + l \cdot m_l = n$. Indeed, we may define an equivalence relation on the set of elements $\{1, 2, \dots, n\}$ as follows: $x \sim y$ if $y = xp^t$ or $x = yp^t$ for some nonnegative integer t. Since $n \leq p^l$, there are at most l elements in each equivalence class. Moreover, these classes have at most one representative in the set $\{n, n-1, \dots, n-r+1\}$. Associate with each column j a generator $y_j = a^{k_j}$ of a cyclic subgroup C_j in R°, where k_j is the only element in the jth column of the matrix $M(R)$ that is coprime to p. For instance, in the above example $y_1 = a^{28}$, $y_2 = a$, $y_3 = a^{26}$, ..., $y_{11} = a^2, \dots$, and so on. The subgroup $C_j = \langle a^{k_j} \rangle$ of R° contains the elements $v = a^{k_j}, v^p, \dots, v^{p^s}$, where $\alpha_{1j} = p^s k_j$ ($s = s(j)$) is the first element in this column. By construction, $\alpha_{1j} p > n$ for each $1 \leq j \leq r$. Let $u_1 = a^n$, $u_2 = a^{n-1}$, ..., $u_r = a^{n-r+1}$. The elements $u_1, u_2, \dots, u_r$ are linearly independent in R and if $w \in R$ satisfies $w^p = 0$, then $w = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_r u_r$ (where $\lambda_i \in GF(p)$, $i \leq r$) is a linear combination of these elements. Hence the subalgebra $U = \langle\langle u_1, u_2, \dots, u_r \rangle\rangle$ has an elementary abelian p-group of rank r as its adjoint group, and is obviously an ideal of R. Let $U_1 = \langle\langle u_1 \rangle\rangle$, $U_i = \langle\langle U_{i-1}, u_i \rangle\rangle$ for each $i = 2, 3, \dots, r$. Then $U_1 < U_2 < \ldots < U_r = U$ is a chain of subalgebras of U. Clearly, U_i is also an ideal of R for each $i \leq r$. Define inductively the subgroups H_j of $G = R^\circ$ as follows: $H_1 = C_1$, $H_j = \langle C_i | i \leq j \rangle$. The multiplication law in R° and the relation $x^{(n)} = \sum_{i=1}^{t} \binom{t}{i} x^i$ show that $\Omega_1(H_j) = U_j$ and $H_{j-1} \cap C_j = U_{j-1} \cap \langle u_j \rangle = 1$. Hence $H_j = H_{j-1} \times C_j$. An easy induction completes the proof, and so $H_r = G$ since $|G| = p^n = p^{m_1 + 2m_2 + \ldots + lm_l} = |C_1| \times |C_2| \times \ldots \times |C_r|$. $\square$

The following theorem classifies finite nilpotent p-algebras with large power algebras.

Theorem 2.2. *Let R be a nilpotent p-algebra of dimension n that contains a power subalgebra $L = \langle\langle a \rangle\rangle$ of dimension $n - 1$. Then $R = \langle\langle a, b \rangle\rangle$ with $a^n = 0 = ab$ and $b^3 = 0$. Let the integer $k \geq 0$ satisfy the conditions $p^k | n - 1$, $p^{k+1} \not| n - 1$. The adjoint group L° of L contains subgroups H and C such that $C \simeq \mathbb{Z}_{p^{k+1}}$, $L^\circ \simeq H \times C$, and either*

(i) *R is commutative, $b^2 = \lambda a^{n-1}$, $\lambda \in GF(p)$, $R^\circ \simeq L^\circ \times \mathbb{Z}_p$, or $p = 2$, $n \equiv 0 \pmod 2$ and $R^\circ \simeq H \times \mathbb{Z}_4$, or*

(ii) *R is noncommutative, $ba = \mu a^{n-1}$, $b^2 = \lambda a^{n-1}$, $\lambda \in GF(p)$, $\mu \in GF(p)^*$, and one of the following holds:*
   (a) *$R^\circ \simeq (H \times C) \rtimes \langle b \rangle$ with $(a, b) = z \in C \cap Z(R^\circ), |z| = |b| = p$;*
   (b) *$p = 2$, $R^\circ \simeq \langle b \rangle \rtimes H$, where $\langle b \rangle \simeq \mathbb{Z}_4$, $n \equiv 0 \pmod 2$ and $(a, b) = b^2$;*
   (c) *$p = 2$, $n = 3$, and $R^\circ \simeq Q_8$.*

This implies the following result of Gorlov (see [12]).

Corollary 2.1. *If R is a finite nilpotent p-algebra whose adjoint group is metacyclic, then R° is either an elementary abelian p-group of order at most p^2, or $p = 3$ and $R^\circ \simeq \mathbb{Z}_9 \times \mathbb{Z}_3$, or $p = 2$ and R° is one of the following groups: $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_8$, $\mathbb{Z}_4 \rtimes \mathbb{Z}_4$, D_8, Q_8.*

The following lemma considers a more general situation.

Lemma 2.1. *Let R be a nilpotent algebra over an arbitrary field F, containing a power subalgebra L of codimension 1. Then $R = \langle\langle a, b \rangle\rangle$ for some $b \in R \setminus L$ and $L = \langle\langle a \rangle\rangle$ such that the following holds: $ab = 0, ba = \lambda a^{\nu-1}, b^2 = \mu a^{\nu-1}$, where $\lambda, \mu \in F$ and $\nu = \nu(a) = \nu(R), n(R) = \dim L = \nu(R) - 1$.*

Proof. Let $\nu = \nu(a)$ for $L = \langle\langle a \rangle\rangle, b \in R \setminus L$. Then $R = \langle\langle a, b \rangle\rangle$ and $ab \in L$ since L is an ideal. Hence $ab = \sum_{i=1}^{\nu-1} \lambda_i a^i$ where $\lambda_i \in F$, $i = 1, 2, \ldots, \nu - 1$. Then $a(b - \sum_{i=1}^{\nu-1} \lambda_i a^{\nu-1}) = 0$. Assume that $\lambda_1 \neq 0$. It follows that $z = b - \sum_{i=1}^{\nu-1} a^{i-1} = -\lambda_1 + b - \sum_{i=2}^{\nu-1} \lambda_i a^{i-1} \in R + 1.F$ and is invertible. Therefore $az = 0$ implies $a = 0$, which is not the case. Now $\lambda_1 = 0$, $z = \sum_{i=2}^{\nu-1} \lambda_i a^{i-1}$ satisfies $az = 0$. Hence we may assume that $ab = 0$. Since L is an ideal, also $b^2 = \sum_{j=1}^{\nu-1} \beta_j a^j$ for some $\beta_1, \ldots, \beta_{n-1} \in F$. But $b^2 a = ab^2 = 0$ and so $\sum_{j=1}^{\nu-1} \beta_j a^{j+1} = 0$, which implies $\beta_1 = \beta_2 = \ldots = \beta_{\nu-2} = 0$. Hence $b^2 = \mu a^{\nu-1}$ for some $\mu \in F$. Since $ab = 0$ and $ba \in L$, we have $ba = \sum_{j=1}^{\nu-1} \gamma_j a^j$ and $aba = 0$. This forces $\sum_{j=1}^{\nu-1} \gamma_j a^{j+1} = 0$ and $\gamma_1 = \gamma_2 = \ldots = \gamma_{n-2} = 0$, so that $ba = \lambda a^{\nu-1}$ for some $\lambda \in F$. It is clear that $n(R) \geq n(L) = \nu(L) - 1 = \dim L$. The element $a^{\nu-1}$ generates an ideal J of R and $R/J = \langle\langle a + J, b + J \rangle\rangle$ is a commutative algebra, which is a direct sum of L/J and a subalgebra $\langle\langle b + J \rangle\rangle$ of dimension 1. Hence the product of any $\nu - 1$ elements in R/J is 0 and $n(R) = \nu(L) - 1 = \nu(R) - 1$. The lemma is proved. □

Proof of Theorem 2.2. Let R be a nilpotent p-algebra of dimension n that contains a power subalgebra $L = \langle\langle a \rangle\rangle$ of dimension $n - 1$. Let $b \in R \setminus L$ as in Lemma 2.1. Then $ab = 0$, $ba = \lambda a^{n-1}$, and $b^2 = \mu a^{n-1}$. Since $ab = 0$, we have $b^3 = bb^2 = 0$. Thus, if $p \geq 3$ there exists an element $b \in R^\circ \setminus L^\circ$ such that $b^p = 0$ in R°. In this case, R° is a semidirect product of a normal subgroup L° and a subgroup isomorphic to $\mathbb{Z}_p$. If R is commutative, then R° is even a direct product of these groups.

Let $p = 2$ and assume that R is commutative. Then if $n \equiv 1 \pmod 2$, we may take $u = \mu a^{(n-1)/2}$ and $v = u + b$. It is easy to see that $v^2 = u^2 + ub + bu + b^2 = u^2 + b^2 = 0$. Since $\nu \notin L$, there is an involution in $R^\circ - L^\circ$ and $R^\circ \simeq L^\circ \times \mathbb{Z}_2$ as above. Hence we may assume that $n \equiv 0 \pmod 2$. It was proved in Theorem 2.1 that $L^\circ \simeq H \times C$ with $C = \langle a^{n-1} \rangle$ (recall that $n - 1$ is odd), and we may have that $R^\circ \simeq H \times \mathbb{Z}_4$. We show that this case really occurs. Let $N = L \oplus S$, where S is an algebra with generator s such that $s^2 \neq 0 = s^3$. In this case $S^\circ \simeq \mathbb{Z}_4$. The multiplication in N is determined by the rule $sl = ls = 0$ for each $l \in L$ and multiplications inside the subalgebras L and S. The subalgebra J of N of the form $\langle\langle s^2 + a^{n-1} \rangle\rangle$ is an ideal of dimension 1 of N since $J \subseteq \mathrm{Ann}(N)$. Then the adjoint group of the quotient algebra N/J is isomorphic to $H \times \mathbb{Z}_4$.

Now let R be noncommutative. Since $ab = 0$ and $ba \in L$, we have $a(ba) = 0$ and hence $ba = \lambda a^{n-1} \in \mathrm{Ann}(R)$ with $\lambda \in GF(p)^*$. It follows that $[a, b] = ab - ba = -\lambda a^{n-1}$. This implies the required relations for $p > 2$.

Let $p = 2$. If there is an involution in $R^\circ \setminus L^\circ$, then we are in a case discussed above. Hence we may assume that there are no involutions in $R^\circ \setminus L^\circ$. Then $b^2 = a^{n-1}$ and $ba = a^{n-1}$. If $n - 1 \equiv 0 \pmod 2$ and $n > 3$, then there is an element $u = a^{(n-1)/2}$ such that

$$(u + b)^2 = ub + bu + u^2 + b^2 = a^{(n-1)/2} + b^{(n-1)/2}.$$

Since $aba = 0$ in each case, it follows that $(u + b)^2 = 0$ and $u + b \in R \setminus L$. Thus, either $n \equiv 0 \pmod 2$ or $n = 3$. The last case leads to a quaternion group $Q_8 \simeq R^\circ$. Now we will show that there exists an algebra R of dimension $n > 3$ such that $R^\circ \simeq \langle b \rangle \rtimes H$, where $H \times \mathbb{Z}_2 = L^\circ = \langle\langle a \rangle\rangle^\circ$.

Note first that an algebra of the form (ii)(a) really exists for each prime p. This can be seen by direct calculations, using a faithful representation of this algebra by $(n + 1) \times (n + 1)$-matrices over $GF(p)$). The adjoint group of this algebra T for $p = 2$ can be expressed in the form $T = (H \times \langle z \rangle) \rtimes \langle x \rangle$, where $\langle\langle a \rangle\rangle^\circ = H \times \langle z \rangle$, $z = a^{n-1}$, $x^2 = 1$, and $(a, x) = z$ ($x^2 = 0$ in T). Consider an algebra $S = \langle\langle s \rangle\rangle$ with $s^2 \neq 0 = s^3$ whose adjoint group is isomorphic to $\mathbb{Z}_4$ and $N = T \oplus S$, a direct sum of two algebras T and S. Then $ts = st = 0$ for each $t \in T$. Let $M = \langle\langle a, x + s \rangle\rangle$. It is obvious that $M^\circ = (H \times \langle z \rangle) \rtimes \langle\langle s + x \rangle\rangle^\circ$ with relations $[a, s + x] = z, a^2(s + x) = (s + x)a^2 = 0$. Clearly $J = \langle\langle (s + x)^2 + a^{n-1} \rangle\rangle$ is an ideal of M, and we obtain an n-dimensional algebra $R = M/J$ with a power subalgebra $(L + J)/J$ of dimension $n - 1$. The relation $(x + s)^2 = s^2$ implies that $(x + s)^2 + J = s^2 + J = a^{n-1} + J$. Hence the required algebra exists. Thus, Theorem 2.2 is proved.

Corollary 2.2. *Let R be a nilpotent p-algebra of dimension $n \geq p$ that contains a power subalgebra L of codimension 1. Then $r(R^\circ) \geq (p - 1)/p \dim R$ and $n(R) = n - 1$.*

Proof. The second assertion is clear. For every commutative algebra A, the subset $T(A) = \{x \in A | x^p = 0\}$ is a subalgebra of A. Since $\dim L \leq p/(p - 1) \dim T(L)$ for a power algebra L (see Theorem 2.1), we are done if we are able to prove that $T(R)$ is a commutative subalgebra of R and $\dim T(R) > \dim T(L)$. By the previous theorem, $\langle\langle a^2, a^3, \ldots, a^{n-1}, b \rangle\rangle$ is a commutative subalgebra of R for each $b \in R - L$. Hence if $a \notin T(R)$, then $T(R)$ is a subalgebra. By the previous theorem, there exists an element in $T(R) - T(L)$ provided that $p > 2$. If $a^p \neq 0$, then the corollary is proved.

If $p > 2$ and $a^p = 0$, then $\dim T(R) \geq \dim L = p - 1$ and $n = p = \dim R$. Assume that $p = 2$. If $a \in T(R)$, then $a^2 = 0$ and $\dim R = 2$. In this case, $2 \dim T(R) \geq \dim R$. If $n = 3$, the corollary is also true. Hence we may assume that $\dim R = n > 3$. If $n \equiv 0 \pmod 2$, then $R^\circ - L^\circ$ contains an involution by Theorem 2.2. If $n \equiv 1 \pmod 2$, then $\dim T(L) = (n - 1)/2 + 1$ and $2r(R^\circ) \geq 2 \dim T(L) \geq n + 1 \geq \dim R$. This concludes the proof of the corollary. □

The assertion $r(R^\circ) \geq (p-1)/p \dim R$, which is equivalent to a well-known conjecture of Eggert (see [10]) in the commutative case, need not be true in general by [2]. Consider an algebra R whose adjoint group is isomorphic to a nonabelian group of order p^3 and of exponent p. Then $r(R^\circ) = 2$, but the inequality $2p/(p - 1) \geq 3$ holds only if $p < 5$.

Corollary 2.3. *Let R be a commutative nilpotent p-algebra whose adjoint group has rank at most p. If $p = 2$, then $\dim R \leq 4$. If $p > 2$, then $\dim R \leq p + 1$. Equality holds if there exists an element of nillity $p + 1$ or $p + 2$. If $p = 3$ and $r(R^\circ) = 2$, then $\dim R = 3$. In all other cases with $r = r(R^\circ) < p$ we have $\dim R = r$.*

Proof. Let $p = 2$. Then the adjoint group of R is metacyclic and the statement is true by Corollary 2.2. Hence $p \geq 3$. If $\nu(R) \leq p$, then R° is elementary abelian and $\dim R = r(R^\circ) \leq p$. Hence we may assume that there exists an element $a \in R$ such that $\nu(a) = \nu \geq p+1$. If $\nu \geq p+3$, then $r(R^\circ) \geq (p-1)/p(p+2) = p+1-2/p$ and $r(R^\circ) \geq p + 1$. Assume that $R \neq \langle\langle a \rangle\rangle$ and $\dim R > p + 1$. Then there exists a subalgebra $L \geq \langle\langle a \rangle\rangle$ with $\dim L = \dim\langle\langle a \rangle\rangle + 1 \geq p + 2$. By Theorem 2.2 we have $r(R^\circ) \geq p + 1$. Therefore we may assume further that $\nu = p + 1$. If $\dim R \geq p + 2$, then there exist subalgebras L and S such that $\langle\langle a \rangle\rangle \subset L \subset S$ with $\dim L = \dim \langle\langle a \rangle\rangle + 1$ and $\dim S = \dim L + 1$. By Theorem 2.2 it follows that $r(R^\circ) \geq p$. If there exists an element $b \in S - L$ such that $b^p = 0$, then $r(R^\circ) \geq p + 1$. Hence for each $b \in S - L$ we have $b^p \neq 0$. If a^p and b^p are linearly independent, then $p + 2 = \dim S \geq 2p$ by Eggert's theorem [10]. This implies that $p \leq 2$, which is impossible. Hence $b^p = \lambda a^p$ for some $\lambda \in GF(p)$. It is clear that $b - \lambda a \in S - L$ and $(b - \lambda a)^p = 0$, a contradiction. □

Theorem 2.3. *Let R be a nilpotent algebra of dimension at least 4 over an arbitrary field F. If the nilpotency class is $n(R) \geq \dim R - 1$, then $\nu(R) \geq n(R) + 1$. Hence R contains a power subalgebra of codimension ≤ 1.*

Proof. If $n(R) = \dim R$, then R is a power algebra by [15, Lemma 2.3.1]. Hence assume that $n(R) = \dim R - 1$. Let $\dim R = 4$. Then by [15, Theorem 6.2.1], $n(R) = 3$ implies $\nu(R) = 4$. Thus for algebras R with $\dim R = 4$ Theorem 2.3 is true. Proceeding by induction, we may assume that this theorem is also true for any algebra S with $3 < \dim S < \dim R$, satisfying the hypotheses of the theorem. Let J be an ideal of R with dimension 1. If $n(R/J) = n(R)$, then $n(R/J) = \dim R/J$, so that R/J is a power algebra by the above considerations. In this case, R has a power subalgebra of codimension 1 and we are done. Therefore, we may assume that $n(R/J) = n(R) - 1$. Since $\dim R/J = \dim R - 1$, we have $\dim R/J - n(R/J) = 1$ and by induction R/J has a power subalgebra L/J of codimension 1. The full preimage L in R of L/J is either a power algebra or is a direct sum $L = S \oplus J$ of a power algebra S and an ideal J. Since $\dim S \geq 2$, $0 \neq L^2 \leq S$ contains an ideal I of R with dimension 1. Note that L is not a power subalgebra of R because otherwise we are done. Therefore, $0 \neq I$ is an ideal of R with trivial intersection with J and $I + J \subset \mathrm{Ann}(R)$. The algebra R/I also has nilpotency class at most $n(R) - 1$ and since $R \leq R/J \times R/I$, $n(R) \leq n(R) - 1$. This contradiction proves the theorem. □

The analogs of Theorem 2.3 for commutative matrix algebras over the field of complex numbers can be found in [20]. In general, there is no bound for $\nu(R)$ in terms of $n(R)$. It is possible to construct examples of a family of algebras R_i, $i \in \mathbb{N}$, where $\nu(R_i)$ is a constant and $n(R_i) > i$ for any $i \in \mathbb{N}$.

3. Nilpotent p-Algebras with Adjoint Groups of Small Ranks

Recall that a group G has *finite Prüfer rank* $r = r(G)$ if every finitely generated subgroup of G can be generated by r elements and r is minimal with this property. In this section, we investigate the case where the abelian subgroups of a group G that is the adjoint group of some nilpotent p-algebra have small rank. If G is a group of rank 1 or a metacyclic group, the corresponding results were obtained by Ault and Watters in [4] and by Gorlov [12]. The following theorem generalizes results mentioned above.

Theorem 3.1. *Let R be a nilpotent noncommutative finite 2-algebra whose adjoint group G has no elementary abelian subgroups of rank 3. If G is not metacyclic, then one of the following holds:*

(i) *$G \simeq Q_8 \times Q_8$, where $G' \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ or $G \simeq Q_8 * Q_8$, a central product, or G is isomorphic to a subgroup of these groups;*

(ii) *$G \simeq \langle a, b, c\rangle$ with the relations $a^4 = b^4 = c^4 = 1$; $a^2 = c^2$, $(a, c) = b^2$, $(b, c) = c^2$, $(a, b) = 1$;*

(iii) *G is isomorphic to a Sylow 2-subgroup of a group of type $U_3(4)$: $G = \langle a, b, c, d\rangle$ with relations $a^4 = b^4 = c^4 = d^4 = 1$, $d^2 = a^2 \circ b^2$, $c^2 = b^2$, $(a, c) = a^2$, $(a, d) = (b, c) = a^2 \circ b^2$, $(b, d) = b^2$, $(a, b) = (c, d) = 1$.*

Proof. Let A be a maximal abelian subgroup of the group $G = R^{\circ}$. Then A is also a subalgebra of R. By Corollary 2.1 it follows that $A \simeq \mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, or $\mathbb{Z}_2$. Since G is not metacyclic, the last 3 possibilities do not occur. If $A \simeq \mathbb{Z}_8 \times \mathbb{Z}_2$, then A is a power subalgebra of R and so is a power subalgebra of some subalgebra of R with dimension 5 since R is not commutative. By Theorem 2.2, G has an abelian subgroup of rank 3. Hence we may assume that G has no elements of order 8. Assume that A is a maximal normal abelian subgroup of G with rank 2. By the above discussion, $A \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $G/A \simeq \mathrm{Aut}_G(A)$. Consider the centralizer H in G of a subgroup $E = \Omega_1(A)$. It is easy to see that $|G : H| \leq 2$. Note that H has exactly 3 involutions. Assume that $g \in G \setminus A$. Then g^2 is an involution in H and hence $g^2 \in E$. Now it is easy to see that G/E is an elementary abelian group.

Consider first the case $A \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$. There are only four elements of order 4 in A and G permutes them. If $a \in A \setminus E$ and $a^x = a$ for some $x \in H \setminus A$, then also $x \in C_G(A)$. In this case $\langle x, A\rangle$ is a maximal abelian normal subgroup of G, contradicting the choice of A. We may assume further that H/A acts fixed-point-freely on the elements in $A \setminus E$ and hence is a group of order at most 4. Assume that H contains a subgroup $K = \langle a\rangle \rtimes \langle b\rangle$ with $|a| = |b| = 4$ and $(a, b) = a^2$. The subgroup K is normal in G, since it contains $E \geq G'$. By [22, Theorem B], we have $G \neq H$. Let $g \in G \setminus H$. Then g permutes the involutions in K and has at least one orbit of size 2 on $E^{\#}$. However, this is not the case because there are no square roots of the element $a^2 \circ b^2$ in K and g fixes a^2, which is the only nontrivial commutator in K. This is a contradiction.

If $h \in H \setminus A$, then $\langle a, h\rangle$ is a subgroup of G of order at most 16, which is nonabelian and not of the form $\langle x\rangle \rtimes \langle t\rangle$ with $x^4 = t^4 = 1$. It follows that in this case $\langle a, h\rangle \simeq Q_8$. If $y \in H \setminus A$ and $\langle a, y\rangle \simeq Q_8$, then $(h \circ y, a) = 1$, which gives the unique possibility $|H : A| = 2$ (recall that H acts fixed-point-freely on $A \setminus E$). Let $H = \langle a, b\rangle \times \langle c\rangle$, where $\langle a, b\rangle \simeq Q_8$, $|c| = 2$ (see the above discussion). If $G = H$, the theorem is proved. Assume that $G \neq H$ and $d \in G \setminus H$. Since d permutes the involutions in H nontrivially and $a^{2d} = a^2$, we have $c^d = a^2 \circ c$. Since $A = \langle a\rangle \times \langle c\rangle$ is normal in G, $a^d = a \circ z$ for some $z \in E$. Since $d^2 \in A$, we have $a = a^{d^2} = a^d \circ z^d = a \circ z \circ z^d$ and $z = z^d$. It follows that either $a^d = a$ or $a^d = a^{(-1)}$. For the same reason $b^d = b$ or $b^{(-1)}$. This implies that $G' \subseteq \langle a, b\rangle$, so that $|G'| = 2$ and $d^2 \in \langle a^2\rangle$. Therefore G/G' is elementary abelian. It follows from [13, Satz II.13.7] that G is a central product $D_8 * Q_8$ or $D_8 * D_8$. The second case cannot occur since this group contains an elementary abelian subgroup of order 8 (see [13, Satz III,13.8]). This implies that $G \simeq Q_8 * D_8 \simeq Q_8 * Q_8$, and so the theorem is proved in the case $|A| = 8$.

Now we will consider the case $A \simeq \mathbb{Z}_4 \times \mathbb{Z}_4 = \langle a\rangle \times \langle b\rangle$. Prove that $H = C_G(E) = G$. If $g \in G \setminus H$, then g induces an automorphism of order 2 of A and acts nontrivially on E. Without loss of generality, we may assume that $g^{(-1)} \circ a^2 \circ g = b^2$ and $g^{(-1)} \circ b^2 \circ g = a^2$. Then $g^{(-1)} \circ a \circ g = b \circ e$ with $e \in E$. Hence

$$(g \circ a)^2 = g \circ a \circ g \circ a = g^2 \circ g^{(-1)} \circ a \circ g \circ a = g^2 \circ e \circ a^2 \circ b.$$

Since $g^2 \in E$, this implies $(g \circ a)^4 = b^2 \neq 1$ and $g \circ a$ has order 8, a contradiction. Now we may apply a result of Ustyuzhaninov [22, Theorem B] (see also [16]), and the theorem is proved. □

It will be proved in Sec. 4 that all groups in Theorem 3.1 occur as adjoint groups of some nilpotent 2-algebras.

Corollary 3.1. *Let R be a nilpotent p-algebra with $\dim R > 3$ for $p > 2$ and $\dim R > 6$ for $p = 2$. Then the adjoint group R° contains an abelian subgroup of rank at least 3.*

Theorem 3.2. *Let R be a nilpotent p-algebra with $p > 2$ whose dimension is at least $p(p+1)/2$. Then R° contains an elementary abelian p-subgroup of rank p.*

Proof. Assume that there exists a nilpotent p-algebra of dimension at least $p(p+1)/2$ whose adjoint group has no elementary abelian p-subgroups of rank p. If $\nu(R) \geq p+1$, then R contains a power subalgebra L with $\dim L \geq p$. If there exists in R a power subalgebra of dimension n, then by [2, Lemma 5.1] it has a subalgebra with elementary abelian adjoint group of rank $r \geq n(p-1)/p$. Hence if $r < p$, then we have $n < p + 1 + 1/(p-1)$. It follows that every power subalgebra of dimension $p+1$ contains a subalgebra with an abelian adjoint group of rank p. Hence $\dim L = p$. Since $\dim R \geq p(p+1)/2 \geq p+1$, there exists a subalgebra S of R which has dimension $\dim L + 1$ and $L \subset S$. Since in the case $p = 3$ the theorem is obviously true, we may assume that $p > 3$, $\dim R \geq 6$, and by Theorem 2.2, S° contains an abelian subgroup of rank $\dim L$. Thus, we obtain a contradiction. Hence we may assume that $\nu(R) \leq p$ and so G is a group of exponent p. Assume that A is a maximal abelian normal subgroup of G. Let $k = \log_p |A|$. Since $C_G(A) = A$, it follows that $G/A \subseteq GL_k(p) \simeq \mathrm{Aut}(A)$. Thus, the order of G/A is at most $p^{k(k-1)/2}$. Now we have $(k^2 + k)/2 = k(k-1)/2 + k \geq \dim R \geq p(p+1)/2$ and $k \geq p$. This contradiction proves the theorem. □

It is easy to construct for $p > 2$ a p-algebra of dimension $2n+1$ that has no subalgebras of dimension $n+2$ with an elementary abelian adjoint group. To see this consider an extraspecial p-group of order p^{2n+1} of exponent p and use a theorem of Kaloujnine [15].

A Miller–Moreno p-group is a nonabelian p-group all of whose proper subgroups are abelian (see [13]). The structure of such groups is well known and can be summarized as follows (see [13, II.7]).

Lemma 3.1. (i) *Let G be a finite p-group. If G is a Miller–Moreno group, then G is isomorphic to one of the following groups:*
(a) *$G = \langle a\rangle \rtimes \langle b\rangle$ with $|a| = p^m$, $|b| = p^n = 1$, and $(a, b) = a^{p^{m-1}}$, $m > 1$, $n \geq 1$;*
(b) *$G = (\langle a\rangle \times \langle c\rangle) \rtimes \langle b\rangle$ with $|a| = p^m$, $|b| = p^n$, $|c| = p$, $m, n \geq 1$, and $(a, b) = c$, $(a, c) = (b, c) = 1$;*
(c) *$G \simeq Q_8$, a quaternion group of order 8;*
(ii) *G is a Miller–Moreno p-group if and only if $d(G) = 2$ and $|G'| = p$;*
(iii) *G is a Miller–Moreno p-group if and only if $\Phi(G) = Z(G)$ and $|G : Z(G)| = p^2$.*

The following theorem describes the Miller–Moreno groups that occur as adjoint groups of some nilpotent p-algebras.

Theorem 3.3. *Let G be a Miller–Moreno p-group that is the adjoint group of some finite nilpotent p-algebra. Then one of the following assertions holds:*

(i) *G is a metacyclic 2-group of order at most 16;*

(ii) *G is isomorphic to a group of type* (b) *in Lemma* 3.1 *with $m \leq 2$, $n \leq 2$, i.e., $|G| \leq 2^5$ and $\exp(G) \leq 4$;*

(iii) *G is a nonabelian p-group of order p^3 and of exponent p.*

Proof. First let $p > 2$. Then it follows from Lemma 3.1 and Corollary 2.1 that there are no nonabelian metacyclic p-groups that are adjoint groups of some nilpotent p-algebra. Hence we may assume that G is a group of type (b) of Lemma 3.1. This group has no elementary abelian subgroups of rank 4. Hence if $p > 3$, then each maximal subalgebra of R (with $R^\circ = G$) has dimension at most $p+1$ (see Corollary 2.3). However, $r(R^\circ) > 3$ for each $p > 3$ if $\nu(R) > p$ and by Corollary 2.3 we have $\nu(R) \leq p$, i.e., G has exponent p. Hence G is a group of type (iii). If $p = 3$ and G is not a group of exponent 3, then the maximal commutative subalgebra of R has dimension at most 4 and so $4 \leq \dim R \leq 5$. If $\nu(R) = 4$ and $\dim R = 4$ or $\nu(R) = 5$ and $\dim(R) = 5$, then Theorem 2.2 gives a contradiction. Hence $\nu(R) = 4$, $\dim R = 5$. In this case, $R^\circ = G \simeq (\mathbb{Z}_9 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_9$. If J is an ideal of R of dimension 1, then R/J has either a metacyclic adjoint group or a Miller–Moreno group of order 81. By Corollary 2.1 and the above discussion we obtain a contradiction. Hence $p = 2$ and $G = (\langle a\rangle \times \langle c\rangle) \rtimes \langle b\rangle$ with $|a| = 2^m$, $|b| = 2^n$, $|c| = 2$, and $(a, b) = c \in Z(G)$. By [2, Lemma 5.1], we have $(\nu(R) - 1) \leq 2r(R^\circ) \leq 6$. Hence $\nu(R) \leq 7$ and $m, n \leq 3$ in each case.

Assume that R is a minimal counterexample to Theorem 3.3. If J is an ideal of dimension 1 of R, then the adjoint group of R/J is R°/J° (see, for example, [21]). If $J^\circ = \langle c\rangle$ is a commutator subgroup of G, then $G/\langle c\rangle$ is a metacyclic group and by Corollary 2.1 we have $|G/\langle c\rangle| \leq 16$. If, also, $G/\langle c\rangle$ is a group of exponent 8, then R/J is a power algebra, hence R is commutative, which is not the case. Therefore, if J° is a commutator subgroup of G, then the theorem is true. Thus we may assume that J° does not contain the commutator subgroup of G. On the other hand, the adjoint group of R/J is also a Miller–Moreno group. Hence we may assume that $\dim R \leq 6$. Since $\nu(R) \leq \dim R$ with the equality only for algebras having a power subalgebra of codimension 1, by Theorem 2.2 we may assume that $\nu(R) \leq \dim R - 1$. Hence $\nu(R) \leq 5$.

Consider the case $m = 3$ and $n = 1$. Then $\dim R = 5$ and since $\nu(R) \geq 4$, we obtain a contradiction. Hence we may consider the case $m = 3$, $n = 2$, and since G has an element of order 8 it can be assumed that $\nu(R) = 5$. Here $G = (\langle a\rangle \times \langle c\rangle) \rtimes \langle b\rangle \simeq (\mathbb{Z}_8 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_4$ with $a^8 = b^4 = c^2 = 1$, $(a, b) = c \in Z(G)$, and $a^4 \neq 0$ in R, $b^4 = 0$ in R. There are just two possibilities for the Jordan decomposition of R into cyclic subspaces corresponding to the action of a as an operator on R:

$$R = \langle\langle a\rangle\rangle \oplus \langle d\rangle \oplus \langle b\rangle, \quad ba = da = 0 \tag{$*$}$$

with $\dim\langle b\rangle = \dim\langle d\rangle = 1$ and

$$R = \langle\langle a\rangle\rangle \oplus \langle ba, b\rangle, \quad ba^2 = 0 \tag{$**$}$$

with $\dim\langle b, ba\rangle = 2$.

Consider first the case $(*)$. Since every subalgebra of R is commutative and $R = \langle\langle a, b\rangle\rangle$, we may assume that $d \in S$, where S is a maximal subalgebra containing a. Hence $da = ad = 0$ and $ba = 0 \neq ab$. Since S is an ideal of R, we have

$$b^2 = \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3 + \lambda_4 a^4 + \lambda_0 d,$$

where $\lambda_i \in GF(2)$, $0 \leq i \leq 4$. From $b^2 a = ab^2 = 0$ it follows that $\lambda_1 = \lambda_2 = \lambda_3 = 0$. Hence $b^2 = \lambda_4 a^4 + \lambda_0 d$. Since $ab, a \in S$, which is commutative, we have $a^2 b = aba = 0$ with $ab = \beta_1 a + \beta_2 a^2 + \beta_3 a^3 + \beta_4 a^4 + \beta_0 d$, where $\beta_i \in GF(2), 0 \leq i \leq 4$. It follows that $\beta_1 = \beta_2 = \beta_3 = 0$. Hence $ab = \beta a^4 + \beta_0 d$, $b^2 = \lambda a^4 + \lambda_0 d$ ($\lambda = \lambda_4$, $\beta = \beta_4$). Assume that $\beta_0 = 0$. Then $ab = \beta a^4 \in \operatorname{Ann}(R)$ and $\langle\langle a^4\rangle\rangle = J$ is an ideal of R. Modulo J the algebra R is commutative, contradicting the structure of its adjoint group. Hence $\beta_0 = 1$. If $\lambda_0 = 0$, then $b^2 \in \langle a, a^2, a^4\rangle$ and $b^2 = \lambda a^4$ implies $(b - \lambda a^2)^2 = 0$, which is not the case. Hence $ab = \beta a^4 + d$ and $b^2 = \lambda a^4 + d$. It follows that $d = ab + \beta a^4$ and $b^2 = (\lambda + \beta)a^4 + ab$, which implies $b^3 = 0$ and $bd = 0$. Hence

$$(\beta a^4 + d)b = (\beta a^4 + d)a = 0, \quad z = [a, b] \in \operatorname{Ann}(R).$$

Now $R/\langle\langle z\rangle\rangle$ has a metacyclic adjoint group $\mathbb{Z}_8 \times \mathbb{Z}_4$, which is impossible by Corollary 2.1. Therefore, we may now consider the second case:

$$R = \langle\langle a\rangle\rangle \oplus \langle b, ba\rangle, \qquad a^5 = ba^2 = 0, \quad a^4 \neq 0, \quad b^4 = 0. \tag{**}$$

Since $ba \in \mathrm{Ann}\langle\langle a\rangle\rangle$ and $\mathrm{Ann}\langle\langle a\rangle\rangle + \langle\langle a\rangle\rangle \neq R$, we have $ba \in S$, which is maximal in R. Now S has a basis $\{a, a^2, a^3, a^4, ba\}$. Since $b^2 \in S$, we have

$$b^2 = \lambda_1 a + \lambda_2 a^2 + \lambda_3 a^3 + \lambda_4 a^4 + \lambda_0 ba, \quad \lambda_i \in GF(2), \quad 0 \le i \le 4.$$

Since $b^2a^2 = b(ba^2) = 0$, we have $\lambda_1 = \lambda_2 = 0$ and $b^2 = \lambda_3 a^3 + \lambda_4 a^4 + \lambda_0 ba$. Since $b^4 = 0$ and $b^2 a = \lambda_3 a^4$, it follows that $ba^2 = 0 = a^2 b$, $b^2 = \alpha a^3 + \beta a^4 + \gamma ba$ $(\alpha = \lambda_3, \beta = \lambda_4, \gamma = \lambda_0)$ and $b^2 a = \alpha a^4$. Since $ab \in S$, we have

$$ab = \mu_1 a + \mu_2 a^2 + \mu_3 a^3 + \mu_4 a^4 + \mu_0 ba, \quad \mu_i \in GF(2), \quad 0 \le i \le 4.$$

Using the relation $aba = ba^2 = 0$, we obtain $\mu_1 = \mu_2 = \mu_3 = 0$ and $ab = \mu a^4 + \mu_0 ba$, where $\mu = \mu_4$. If $\mu_0 \neq 0$, then $[a, b] = ab - ba = \mu a^4 \in \mathrm{Ann}(R)$ and $R/\langle\langle a^4\rangle\rangle$ is a commutative algebra, which is impossible. Hence $\mu_0 = 0$, $ab = \mu a^4$, and $b^2 = \alpha a^3 + \beta a^4 + \gamma ba$. Since $ab^2 = b^2 a$, $(ab)b = \mu a^4 b = 0$. However, $b^2 a = \alpha a^4$. Therefore, $\alpha = 0$. We have $ab = \mu a^4$, $b^2 a = 0$, and $b^2 = \beta + \gamma ba$. Since $b^2 a = 0$, $b^3 = 0$ and $ab - ba = \mu a^4 + ba$. It is easy to see that $ba \in \mathrm{Ann}(R)$ and $a^4 \in \mathrm{Ann}(R)$. Hence $z = [a, b] \in \mathrm{Ann}(R)$. As before, this leads to a contradiction. Thus this case is also impossible, and the theorem is proved. □

It is easy to show that if a noncommutative nilpotent p-algebra R of finite dimension has two maximal commutative subalgebras, then $R^\circ \simeq (\langle a\rangle \times \langle c\rangle) \rtimes \langle b\rangle \times A$, where $a^{p^m} = b^{p^n} = c^{p^k} = 1$, $(a, b) = c^{p^{k-1}}$, and A is an abelian group or $R^\circ \simeq M \times A$, where M is a Miller–Moreno group and A is an abelian group. Hence Theorem 3.3 shows that the case $A \neq 1$ occurs very rarely. Below we construct an algebra R that has two commutative maximal subalgebras and its adjoint group has prescribed Miller–Moreno factor M.

The next theorem is perhaps surprising.

Theorem 3.4. *Let R be a finite nilpotent p-algebra $(p > 2)$ whose adjoint group has only two generators. Then either R° is a metacyclic group or R° is a nonabelian p-group of order p^3 and of exponent p. In each case,* $\dim R \le 3$.

Proof. Consider the chain $R \supset R^2 \supset R^3 \ldots \supset R^k = 0$, where $k - 1$ is the nilpotency class of R. Since R has two generators, $|R/R^2| = p^2$. Since R^2/R^3 is contained in the center of R/R^3, the algebra R/R^3 is either commutative or the adjoint group $(R/R^3)^\circ$ is nilpotent of class 2. Consider a factor algebra R/R^{i+1} such that the algebra R/R^i is commutative and R/R^{i+1} is noncommutative. Without loss of generality, we may assume that $R^{i+1} = 0$. Then R has two generators a, b that are also generators of R°. Since $G = R^\circ$ is a group with two generators a, b and $(a, b) \in Z(G)$, we have $G' = \langle(a, b)\rangle$ and the group G/G' is metacyclic. It follows that the rank of G is at most 3. Consider first the case $p > 3$. By Corollary 2.3, $\dim A \le 3$ for each maximal commutative subalgebra A of R. Hence the order of any maximal abelian subgroup of G is bounded by p^3 and each nontrivial element of G is of order p. Since $d(G) = 2$ and $G' \subset Z(G)$ is elementary abelian, G is a Miller–Moreno group and by Theorem 3.3 $\dim R = 3$. Assume that $p = 3$ and $(R/R^i)^\circ$ is not elementary abelian. This case can occur only when R/R^i is a power algebra by [12], but then R is a commutative algebra. Hence $(R/R^i)^\circ$ is an elementary abelian p-group in each case and G is a Miller–Moreno group. By Theorem 3.3, $\dim R = 3$ and $i = 2$. Now we may assume that $R^3 \neq 0 = R^4$. Since $\dim R/R^3 = 3$ by the previous discussion, we have $\dim R^2/R^3 = 1$. By [15, Lemma 1.6.1], it follows that $R^2 \subset Z(R)$. Then $R^3 = 0$, a contradiction. The theorem is proved. □

4. Nilpotent p-Algebras of Small Dimension

Nilpotent p-algebras of small dimension have been studied for a long time. A list of those of dimension 4 was given by Allen [1] with corrections by Ghent [11]. The description of these algebras can be found in Kruse and Price ([15]) (see also Scorza [19]).

It seems that so far no attempts have been made to determine the structure of the adjoint groups of these algebras. One of the difficulties is that similarly defined algebras can lead to adjoint groups with different structure (depending on the characteristic of the field). For instance, the adjoint group of a p-algebra determined by the laws $x^3 = 0$ and $ab = ba$ for all $x, a, b \in R$ can be isomorphic to $\mathbb{Z}_4$ (if $p = 2$) or to $\mathbb{Z}_p \times \mathbb{Z}_p$ (if $p > 2$). A list of all p-algebras of dimension 5 is contained in the dissertation of Boyce [8], and a bibliography can be found in [15]. We will describe here all nonisomorphic finite p-groups that can occur as the adjoint group of some nilpotent p-algebra of dimension less than or equal to 5. In Theorem 4.3 we give a complete description of the groups of class 3 that can occur as an adjoint group of some nilpotent p-algebra, indicating only for $p = 3$ the general properties of groups of class 2 that occur as an adjoint group, because the complete description would long. It is interesting to compare this list with the list of groups of class 3 of order p^5 that can occur as an adjoint group of some nilpotent p-ring obtained by Tahara and Hirosi [21] for $p > 2$. Note that for $p = 2$ we have been able to find all 2-groups of order 2^5 that occur as adjoint groups of some 2-algebras.

Theorem 4.1. *Let G be the adjoint group of some nilpotent p-algebra R. If $\dim R = 3$, then exactly one of the following holds:*

(i) $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$;
(ii) *G is a nonabelian p-group of exponent p and order p^3;*
(iii) $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p$ $(p \leq 3)$;
(iv) *$G \cong D_8$ or Q_8 (a dihedral or a quaternion group).*

Proof. This is an easy consequence of the description of these algebras in [15, Theorem 2.3.6]. □

Theorem 4.2. *Let G be the adjoint group of some nilpotent p-algebra R. If $\dim R = 4$, then exactly one of the following holds:*

(i) *$p > 2$, $G \cong X \times \mathbb{Z}_p$ with a group X isomorphic to the adjoint group of some nilpotent p-algebra of dimension 3;*
(ii) *$p = 3$, $G \cong X \times \mathbb{Z}_3$, where X is a metacyclic Miller–Moreno group of order 27;*
(iii) *$p = 2$, G is a group of class at most 2 and of exponent at most 4;*
(iv) *$p = 2$, $G \cong \mathbb{Z}_8 \times \mathbb{Z}_2$.*

Proof. By Corollary 2.1, we may assume that G is not metacyclic. It follows from Theorem 2.2 that $\nu(R) \leq 4$. If $\nu(R) \leq p$, then G is either an elementary abelian p-group or a nonabelian group of exponent p. It follows from Theorem 3.4 that the algebra R can have an adjoint group G with two generators ($p > 2$) if and only if $\dim R \leq 3$. Hence we may assume that $d(G) \geq 3$ and by Burnside's basic theorem $|G/\Phi(G)| \geq p^3$. This implies $|G'| = p$ in the noncommutative case. It follows from the description of the groups with Frattini subgroup of order p (see [13, Satz III.13.7]) that $G \cong X \times \mathbb{Z}_p$, where X is a nonabelian p-group of order p^3 or is a central product of a nonabelian group of order p^3 and a cyclic subgroup of order p^2. Since $\nu(R) \leq 4$, this case can occur only for $p \leq 3$. Assume that $p = 3$ and G is not an abelian 3-group (if G is abelian and $|\Phi(G)| = 3$, then $G \cong \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$). If the exponent of G is not 3, then $\nu(R) = 4$ and R contains a power subalgebra L of codimension 1. From Theorem 2.2 we obtain that this is case (ii) of Theorem 4.2. Assume now that $p = 2$ and G is not an elementary abelian 2-group. By a theorem of Tausski (see [13, Satz III.11.9]), if $|G : G'| = 4$, then G is a metacyclic 2-group. By Corollary 2.1, this leads to a contradiction. Hence $|G/G'| \geq 8$. If $d(G) = 2$ and G is a nonabelian group, then it is a Miller–Moreno group by Lemma 3.1(ii), and so by Lemma 3.1(i) and Theorem 3.3 we have the required conclusion. Therefore $d(G) \geq 3$ and $G' = \Phi(G)$ has order 2. In this case, G is a group of class 2 and of exponent 4. The abelian case gives no difficulties. The theorem is proved. □

Theorem 4.3. *Let G be a nonabelian adjoint group of some nilpotent p-algebra R of dimension 5. Then one of the following holds:*

(i) *G is p-group of class 2 and of exponent p;*
(ii) *G is one of the following groups of class 3:*
 (a) *$G \simeq X \times \mathbb{Z}_p$ $(p \geq 3)$, where X is a p-group of maximal class of order p^4 with $exp(X) = p$ for $p > 3$;*
 (b) *$G = \langle a, b, c, d, e\rangle$ $(p \geq 3)$ with relations $b^p = c^p = d^p = e^p = 1$, $\langle d\rangle = Z(G)$, $(a, b) = e$, $(e, a) = d$, $(b, c) = d$, $(a, c) = 1$, $a^p = d^n$ ($n = 0$ if $p > 3$ and $n \in \{0, 1\}$ if $p = 3$);*

(c) $G = \langle a, b, e, c\rangle$ $(p = 3)$, *where* $b^3 = a^9 = c^3 = e^3 = 1$, $(a, c) = 1 = (e, c) = (e, b)$, $(a, b) = c^{(\mu)}$ $(\mu \in \{1, -1\})$, $(c, b) = a^3 = (a, e)$;

(d) $G = \langle a, b, c\rangle$ $(p = 2)$, $a^4 = b^4 = c^2 = 1$, $(a, c) = 1$, $(a, b) = c$, $(b, c) = a^2$;

(iii) *G is a p-group $(p \leq 3)$ of class at most 2 and of exponent $\leq p^2$ such that G' is group of order $\leq p^2$ and $\Phi(G) \leq Z(G)$ is an elementary abelian p-group.*

Proof. Assume that $\nu(R) > p$. Since $\nu(R) \leq \dim R + 1$ and $\nu(R) = \dim R + 1$ only for power algebras, we may assume that $\nu(R) \leq \dim R$. The case where equality holds is described in Theorem 2.2. Hence we may assume that $\nu(R) \leq \dim R - 1 = 4$ in each case.

Consider first the case $p = 2$. Since $\nu(R) \leq 4$, G is a group of exponent 4. By a theorem of Tausski (see [13, Satz III.11.9]) and Corollary 2.1, we have $|G : G'| \geq 2^3$ and $|G'| \leq 4$. If $|G'| = 2$ and $d(G) = 2$, then by Lemma 3.1 G is a Miller–Moreno group and Theorem 3.3 gives the required assertion.

If $|G'| = 2$ and $d(G) \geq 3$, then $\Phi(G) \leq Z(G)$, which also gives condition (iii) of the theorem. The same is true if $\Phi(G) \leq Z(G)$ is an elementary abelian group and $|G'| = 4$. Hence we may assume that either $\Phi(G) \not\leq Z(G)$ or $\Phi(G)$ is not an elementary abelian 2-group.

We shall prove that G' is an elementary abelian 2-group. Assume that G' is a cyclic group of order 4. If G/G' is elementary abelian, then $\langle a, G'\rangle$ is a group of order 8 that has a cyclic subgroup G' of index 2. Since G has no elements of order 8, we have $a^2 \in \Omega_1(G')$. This implies that $G/\Omega_1(G')$ is an elementary abelian 2-group and $G' \leq \Omega_1(G')$, which is a contradiction.

Therefore, the group G/G' is not elementary abelian, and so $G/G' \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. It is clear that G has two generators a, b such that at least one of them, say b, is in the centralizer of G'. If $\langle G', b\rangle$ is a group of order 8, then we may take b of order 2. This implies

$$1 = (a, b^2) = (a, b) \circ (a, b)^b = (a, b)^2,$$

and G' is of order 2, which is impossible. Finally, if $\langle G', b\rangle$ is a group of order 16, then $a^{(-1)} \circ b \circ a = b \circ (b, a)$ and $(a \circ b)^4 = ((a \circ b)^2)^2 = a^4 \circ b^4 \circ (b, a)^2 = (b, a)^2 \neq 1$. This is a contradiction.

Hence G' is an elementary abelian 2-group. If $G' \leq Z(G)$ and $d(G) = 2$, then $G = \langle a, b\rangle$ with $(a, b)^2 = 1$, $(a, b) \in Z(G)$, and by Lemma 3.1 G is a Miller–Moreno group.

Therefore, if $G' \leq Z(G)$, then $d(G) \geq 3$ and $|G/\Phi(G)| \geq 8$ by Burnside's basic theorem. It follows that $G' = \Phi(G) \leq Z(G)$, and we are done.

Consider now the case $G' \not\leq Z(G)$. Since $|G'| = 4$, $H = C_G(G')$ has index 2 in G. If an element $a \in G \setminus H$ induces an automorphism of H of order 2, then for each $h \in H$ we have $(h, a) = h^{(-1)} \circ h^a$ and $(h, a)^a = (h^a)^{(-1)} \circ h^{a^2} = (h^{(-1)} \circ h^a)^{(-1)} = (h, a)^{(-1)}$.

Since each element in G' has order at most 2, we have $(H, a) \leq Z(G)$. On the other hand, $H' \leq Z(H)$ and since $|H| = 16$, it is clear that also $H' \leq Z(G)$ (if H is nonabelian, then it is either a Miller–Moreno group or $|\Phi(H)| = 2$).

Hence there are no involutions in $G \setminus H$, H is nonabelian, and $a^2 \in H \setminus Z(H)$ for each $a \in G \setminus H$. Moreover, $Z(H) \geq G'$ is noncyclic. Since $H = C_G(A)$ is a subalgebra of R with $\dim H = 4$, we may use Theorem 4.2. Let x, y be noncommuting elements in H. If $\langle x, y\rangle \geq Z(H)$, then $\langle x, y\rangle = H$ is a Miller–Moreno group of order 2^4, satisfying the restrictions on H. It is easy to see that this is a group of the form $(\langle x\rangle \times \langle z\rangle) \rtimes \langle y\rangle$ with $x^4 = z^2 = y^2 = 1$ and $(x, y) = z \in Z(H)$. Since $G' = \langle x^2\rangle \times \langle z\rangle$, it follows that the subgroups $\langle x\rangle \times \langle z\rangle$ and $\langle x^2\rangle$ are normal in G. Hence $(x^2, a) = 1$ for each $a \in G$. On the other hand, $\langle z\rangle = H'$ is normal in G and $(z, a) = 1$ for each $a \in G$. In this case $G' \leq Z(G)$. We may assume now that $\langle x, y\rangle$ does not contain the center of H. Since $\langle x, y\rangle$ is a nonabelian group, it has order 8 and $H = \langle x, y\rangle \times \langle z\rangle$ for some element z of order 2 in $G' \leq Z(H)$. If $\langle x, y\rangle$ is a quaternion group, then all involutions in H lie in its center. This is impossible by the above. Hence $H \cong D_8 \times \mathbb{Z}_2$. Without loss of generality, we may assume that $a^2 = x \in H \setminus Z(H)$ and y is an element of order 4 in H, $z \in G' \setminus (\langle x, y\rangle \cap G')$. Then $(\langle y\rangle \times \langle z\rangle) \rtimes \langle a\rangle = G$ and $a^2 \circ y \circ a^2 = y^{(-1)}$. Since $(y^2, a) = 1$, a permutes the involutions z and $y^2 z$, i.e., $a^{(-1)} \circ z \circ a = z \circ y^2$. It is clear that $a^{(-1)} \circ y \circ a \notin \langle y\rangle$. Therefore $a^{(-1)} \circ y \circ a = y \circ z$ or $y \circ z \circ y^2$. We may denote the element (y, a) by z and then G is a group of type (ii) of the theorem. We show now that the algebra R with the adjoint group of this form really exists. Let R be a matrix algebra consisting of all matrices over $GF(2)$ of the form

$$\begin{pmatrix} 0 & \alpha & \beta & \gamma & \delta & \lambda \\ 0 & 0 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & \alpha & \beta+\gamma \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Then $R^\circ = G$ has the required structure.

Let $p \geq 3$. By Corollary 2.1 and Theorem 2.3, if $R^4 \neq 0$, then G is one of the groups of Theorem 4.3. Hence $R^4 = 0$. On the other hand, $d(G) \geq 3$ by Theorem 3.4, so in each case $|G'| \leq p^2$ by Burnside's basic theorem. There are two possibilities: $G' \not\leq Z(G)$ and $G' \leq Z(G)$. The latter gives us conclusion (i) or (iii) of Theorem 4.3. Hence $G' \not\leq Z(G)$ and $|G'| = p^2$. By [15, Lemma 1.6.10], if $|R^2 : R^3| = p$, then $R^2 \leq Z(R)$ and $G' \leq Z(G)$, which is not the case. Hence $|R^2 : R^3| = p^2$ and $\dim R^3 = 1$. Thus there is a basis a, b, c, d, e of the algebra R, such that $d \in R^3$, $\{c, e, d\}$ is a basis for R^2, and $a, b \in R \setminus R^2$. Since $|G'| = p^2$, $H = C_G(G')$ is a subgroup of G of index p and a is a subalgebra in R of codimension 1. We may assume that $b \in H$. Note that $d \in \operatorname{Ann} R$ and R^2 is generated by elements ab, ba, a^2, b^2, and d. Since $R^4 = 0$, R^2 is a null algebra and in particular $e^2 = c^2 = d^2 = 0$. Since $xc, xe \in R^3$ for each $x \in R$, $\langle\langle u, d\rangle\rangle$ is an ideal in R for each $u \in R^2$. If H is a commutative subalgebra, then $|Z(G)| \geq p^2$, since by Theorem 3.4 $d(G) \geq 3$ and $Z(G) \neq G'$ since G is assumed to be of class 3. Now it is easy to obtain the required relations for G (provided the exponent of H is p):

$$G = \langle x, y, z_1, z_2, a\rangle \quad \text{with relations} \quad (x,a) = y, \quad (y,a) = z_1, \quad (z_2, a) = (z_1, a) = 1, \quad a^p = 1,$$

and $\langle x, y, z_1, z_2\rangle$ is an elementary abelian p-group. We need to show that there exists a nilpotent p-algebra R with required adjoint group G. This group is a direct product of a p-group $G_1 = \langle x, y\rangle$ and $\langle z\rangle$. Consider the set of 6×6 matrices with coefficients in $GF(p)$ and of the form

$$\begin{pmatrix} 0 & \alpha & \beta & \gamma & \lambda & \delta \\ 0 & 0 & 0 & -\alpha & -\beta & \lambda \\ 0 & 0 & 0 & 0 & \alpha & \alpha+\gamma \\ 0 & 0 & 0 & 0 & 0 & \beta \\ 0 & 0 & 0 & 0 & 0 & -\alpha \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Obviously the set of these matrices is an algebra of dimension 5 containing a basis $\{a, b, c, d, e\}$ that satisfies the relations $ab = -e$, $ba = e + d$, $ae = d$, $ea = -d$, $eb = be = 0$, $ac = ca = 0$, $bc = d = cb$, $a^2 = -c$, and $b^2 = 0$. It is easy to see that the adjoint group of this algebra is G.

If H is commutative but not elementary abelian, then $p = 3$ and there exists an element $b \in H$ such that $b^3 \neq 0$. By Theorem 2.2, we may choose a basis in H of the form $\{b, b^2, b^3, c\}$ with $cb = bc = 0$. By the above discussion, $\langle\langle b^3\rangle\rangle = R^3$ is an annihilator of R and $\{b^2, b^3, c\}$ is a basis for R^2. Let $a \in R \setminus H$. Since $a^2 = \beta_1 b^2 + \beta_2 b^3 + \beta_3 c$, $ab = \alpha_1 b^2 + \alpha_2 b^3 + \alpha_3 c$, $ba = \gamma_1 b^2 + \gamma_2 b^3 + \gamma_3 c$ $(\alpha_i, \beta_j, \gamma k \in GF(3))$ and $ab, ba \in H$, we have $b^2 a = b(ba) = (ba)b = b(ab) = ab^2 = (ab)b$. This implies that $b^2 a = \gamma_1 b^3 = ab^2 = \alpha_1 b^3$ and $\alpha_1 = \gamma_1$. Now it is clear that $G' = \langle\langle b^3, c\rangle\rangle$ and $\langle\langle b^2, b^3\rangle\rangle = Z(G)$ (recall that $G' \not\leq Z(G)$). It is possible to describe the structure of the adjoint group G of this algebra. The group G has generators a, b, c, and d such that $b^9 = c^3 = d^3 = 1$, $a^3 = b^{(3\delta)}$, $\langle b^3, c\rangle = G'$ and $(b, a) = c$, $(c, a) = d$, $(a, d) = (b, d) = 1$, or $(b, a) = c$, $(c, a) = b^3$, $(a, d) = 1$. But $\langle b, b \circ c, d\rangle = H$ in the first case and then $G = \langle a, b\rangle$, which is impossible. Hence there is only one possibility (up to the choice of notation): $G = \langle a, b, c, d\rangle$ with $(b, a) = c$, $(c, a) = b^{(3\mu)}$, $\mu \in \{1, -1\}$, $(d, a) = 1$ and $G \cong (\langle b\rangle \times \langle c\rangle) \times \langle a\rangle \times \langle d\rangle$; $b^9 = c^3 = d^3 = 1$, $a^3 = b^{(3\delta)}$, $\delta \in GF(3)^*$. This case really occurs since there exists an algebra R of 6×6-matrices with coefficients in $GF(3)$ whose adjoint group is isomorphic to G. These matrices have the form

$$\begin{pmatrix} 0 & \alpha & \beta & \delta & \gamma & \lambda \\ 0 & 0 & 0 & \alpha & -\beta & -\gamma \\ 0 & 0 & 0 & \beta & \alpha & \delta \\ 0 & 0 & 0 & 0 & 0 & \beta \\ 0 & 0 & 0 & 0 & 0 & \alpha \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

It remains to consider the case $H = C_G(G')$, where H is a nonabelian group. We have the following two possibilities:

(a) there exists an element $b \in H$ such that $b^3 \neq 0$;

(b) $x^3 = 0$ for each $x \in H$.

In case (a) there exists a basis $\{b, b^2, b^3, c\}$ of the subalgebra H such that $cb = 0$, $bc = b^3$, and $c^2 = \delta b^3$, $\delta \in GF(p)$ (see Theorem 2.2). Since $R^4 = (R^2)^2 = 0$, it is clear that $c^2 = 0$. Therefore $cb = 0 = c^2$, $bc = b^3$, and $Z(H) = \langle\langle b^2, b^3\rangle\rangle = G'$ is an ideal in R. This forces that R/G' is a commutative algebra and $[a, b] = -ba + ab \in G'$, so that we can write

$$ab = \alpha_1 c + \alpha_2 b^2 + \alpha_3 b^3, \quad ba = \alpha_1 c + \beta_2 b^2 + \beta_3 b^3 \quad (\alpha_i, \beta_j \in GF(p)).$$

On the other hand, $\langle\langle c, b^3\rangle\rangle$ is also an ideal of R. Hence $R/\langle\langle c, b^3\rangle\rangle$ is a noncommutative 3-dimensional algebra. By [15, Theorem 2.3.6], we may assume that $b^2 \equiv ba \pmod{\langle\langle c, b^3\rangle\rangle}$ and $ab \equiv 0 \pmod{\langle\langle c, b^3\rangle\rangle}$. Thus $ab = \alpha_1 c + \alpha_3 b^3$, $ba = \alpha_1 c + b^2 + \beta_3 b^3$, $bc = b^3$, $cb = 0$, $ac = \lambda b^3$, and $ca = \mu b^3$ for some $\lambda, \mu \in GF(p)$. Using these relations, we obtain $ab^2 = (ab)b = 0$, $b^2 a = b(ba) = \alpha_1 bc + b^3 = (\alpha_1 + 1)b^3$, and $(ba)b = bab = \alpha_1 cb + b^3 = b(ab) = \alpha_1 bc = \alpha_1 b^3$. Hence $\alpha_1 = 1$ and we can rewrite our relations in the following form: $ab = c + \alpha b^3$, $ba = c + b^2 + \beta b^3$, $bc = b^3$, $cb = 0$, $ac = \lambda b^3$, $ca = \mu b^3$, $ab^2 = 0$, and $b^2 a = 2b^3$, where $\alpha = \alpha_3$, $\beta = \beta_3$, and $bab = b^3$. It is easy to see that $a^2 b = ac = \lambda b^3$ and $ba^2 = ca + b^2 a = (\mu + 2)b^3$. Obviously $a^2 = \gamma_1 c + \gamma_2 b^2 + \gamma_3 b^3$, where $\gamma_1, \gamma_2, \gamma_3 \in GF(p)$. Since $a^2 b = \lambda b^3 = a^2 b = \gamma_1 cb + \gamma_2 b^3 = \gamma_2 b^3$, $\gamma_2 = \lambda$. On the other hand, $ba^2 = ca + b^2 a = (\mu + 2)b^3 = b \cdot a^2 = \gamma_1 bc + \gamma_2 b^3 = (\gamma_1 + \gamma_2)b^3$. It follows that $a^2 = (\mu - \lambda + 2)c + \lambda b^2 + \gamma b^3$ with $\gamma = \gamma_3$. Since $aba = ab \cdot a = a \cdot ba$, $aba = ca = ac + ab^2 = ac = \lambda b^3 = \mu b^3$ and $\lambda = \mu$. Thus $a^2 = 2c + \lambda b^2 + \gamma b^3$ and the equality $a \cdot a^2 = a^2 \cdot a = a^3$ implies $a^3 = 2ac + \lambda ab^2 = 2ca + \lambda b^2 a$, so $\lambda ab^2 = \lambda b^2 a = 0 = 2\lambda b^3$. This forces $\lambda = 0$. Finally $ab = c + \alpha b^3$, $ba = c + b^2 + \beta b^3$, $bc = b^3$, $cb = 0$, $ac = ca = 0$, $ab^2 = 0$, $b^2 a = 2b^3$, and $a^2 = 2c + \gamma b^3$. If $p > 3$, then the adjoint group of this algebra has generators a, b, c, d, e with the relations $a^p = b^p = c^p = d^p = e^p = 1$, $d \in Z(G)$, $(b, a) = e$, $(e, a) = d$, and $(b, c) = d$. One example of an algebra of this kind is given by all 6×6-matrices with coefficients in $GF(p)$ of the form

$$\begin{pmatrix} 0 & \alpha & \beta & \gamma & \delta & \lambda \\ 0 & 0 & 0 & 2\alpha + \beta & 0 & 0 \\ 0 & 0 & 0 & \alpha & \alpha + \beta & \gamma + \delta \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2\alpha + \beta \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

If $p = 3$, then the adjoint group of this algebra has generators a, b, c, e with relations $b^9 = c^3 = e^3 = 1$, $(b, a) = e$, $(e, a) = b^{(3\lambda)}$, $(b, c) = b^3$, $\lambda \in GF(3)^*$, $b^3 \in Z(G)$, and $a^3 \in \langle b^3 \rangle$.

Consider now case (b). There are no additional cases if $p > 3$ or if $\exp(G) = p$ since the structure of a group G having a subgroup H of order p^4 and of exponent p is completely determined if we know that $G' = Z(H)$ (see [5], this is a group of type 40 in this list). But we have already shown the existence of such a group as the adjoint group of an appropriate algebra. Hence we will assume that $p = 3$ and G is not a group of exponent 3. In this case, also $x^3 = 0$ for each $x \in H$ and there exists an element $a \in R \setminus H$ such that $a^3 \neq 0 = a^4$. Obviously, there exists a maximal noncommutative subalgebra L of R containing a. By Theorem 2.2, L has a basis $\{a, a^2, a^3, c\}$ such that $ac = 0$, $ca = a^3$ and $c^2 = \delta a^3$ for some $\delta \in GF(3)$. An element $b \in H \setminus L$ satisfies $b^3 = 0$. As above, $R^2 = \{a^2, a^3, c\}$ and R^2 is a null algebra, so that $\delta = 0$. Since $G' \not\leq Z(L)$, $e = \lambda a^2 + c \in G'$ for appropriate $\lambda \in GF(3)$ and $G' = \langle\langle e, a^3\rangle\rangle \subseteq C_R(b)$ for $b \in H \setminus L$. Since $b^2 \in R^2$ and R^2 is a commutative subalgebra of L, $\langle\langle b, C_L(b)\rangle\rangle$ is also a commutative subalgebra. Moreover, it has dimension at most 3 since there are no commutative subalgebras of codimension 1 in R. It follows that $C_L(b) = G'$ and $b^2 \in G'$. Since G' is an ideal in our case, R/G' is a commutative algebra of dimension 3, having power subalgebra $\langle\langle a + G'\rangle\rangle$ of codimension 1. By [15, Theorem 2.3.6], we have $ab \equiv ba \equiv 0 \pmod{G'}$ and $b^2 \equiv 0 \pmod{G'}$. Hence $ab = \alpha_1 e + \alpha_2 a^3$, $b^2 = \gamma_1 e + \gamma_2 a^3$, and $ba = \beta_1 e + \beta_2 a^3$ for some α_i, b_j, $\gamma_k \in GF(3)$, $1 \leq i, j, k \leq 2$.

Note that $ae = \lambda a^3$ and $ea = (\lambda + 1)a^3$. If $\gamma_1 \neq 0$, then $b^3 = 0$ implies $eb = be = 0$. Since $ab^2 = (ab)b = (\alpha, e + \alpha_2 a^3)b = \alpha_1 eb + \alpha_2 a^3 b = 0$ in this case, $ab^2 = \gamma_1 ae = \gamma_1 \lambda a^3 = 0$ and $\lambda = 0$. For the same reason, $b^2 a = 0$ and $b^2 \cdot a = \gamma_1 ea = \gamma_1(\lambda + 1)a^3$, which implies $\lambda + 1 = 0$. This is a contradiction, and $\gamma_1 = 0$, $b^2 = \gamma a^3$, where $\gamma = \gamma_2$. In this case, also $be = eb = \sigma a^3$ for some $\sigma \in GF(3)$. Therefore $b^2 \cdot a = a \cdot b^2 = 0$. On the other hand, $ab^2 = \alpha_1 eb = \beta_1 be = \alpha_1 \sigma a^3 = \beta_1 \sigma a^3$. If $\sigma \neq 0$, then $\alpha_1 = \beta_1 = 0$ and $ab - ba \in Z(R)$, which is not the case. Thus $be = eb = 0$ and $ab^2 = b^2 a = 0$.

Since $ab \cdot a = a \cdot ba$, $\alpha_1 ea = \beta_1 ae = \alpha_1(\lambda + 1)a^3 = \beta_1 \lambda a^3$. This forces that $\alpha_1(\lambda + 1) = \beta_1 \lambda$ and $(\alpha_1 - \beta_1)\lambda \neq \alpha_1 = 0$. Note that $\alpha_1 \neq \beta_1$, since $ab - ba = [a, b] \notin Z(R)$. Consider possible types of groups with this structure. By Theorem 4.2, the subgroup L° has the following structure: $L^\circ = (\langle a\rangle \rtimes \langle e\rangle) \times \langle c\rangle$, where $\langle e\rangle \times \langle a^3\rangle = G'$, $a^9 = e^3 = c^3 = 1$. An element $b \in G \setminus L^\circ$ has order 3 and b centralizes $\langle a^3\rangle \times \langle e\rangle = G'$. Since $\langle a\rangle \rtimes \langle e\rangle = K$ is normal in G, $(a, b) = e_1$ for some $e_1 \in K$ of order p. Without loss of generality, we may assume that $e_1 = e$. Hence it remains to describe the action of b on c. Since $Z(L^\circ) = \langle a^3\rangle \times \langle c\rangle$ is normal in G, so $(c, b) = a^{(3\sigma)}$ for some $\sigma \in GF(3)^*$. This forces $(c^2, b) = a^{(3\cdot 2\sigma)}$, and we may assume that $(c, b) = a^3$ for some element $c \in Z(L)$. Thus $(a, b) = e$, $(e, b) = 1$, $(c, b) = a^3$, $b^3 = a^9 = c^3 = e^3 = 1$, and $(a, c) = 1 = (e, c)$. Thus, the structure of G is completely determined. On the other hand, the 3-algebra R of 6×6-matrices over $GF(3)$ of the following form has the required adjoint group of class 3:

$$\begin{pmatrix} 0 & \alpha & \beta & \gamma & \delta & \lambda \\ 0 & 0 & 0 & \alpha & \beta & \gamma - \delta \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \alpha - \beta \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

In [21], the p-groups of order p^5 and of class 3 that are the adjoint group of some nilpotent p-ring R are determined. These are the groups of types 4, 5, 19, 20_1, 21, 40, 41, and 54 in [5]. It follows from the above theorem that the only groups of types 4, 19, 20_1, 40, and 41 are the adjoint group of some nilpotent p-algebra and the types 19, 20_1, and 41 occur only for $p = 3$. □

5. Some Special Nilpotent p-Algebras

In this section, we will present some examples and constructions for nilpotent p-algebras.

Example 5.1. Let R be a commutative nilpotent matrix algebra over the field F, consisting of all matrices of the form

$$\begin{pmatrix} 0 & \alpha_{12} & \alpha_{13} & \cdots & \alpha_{1m} \\ 0 & 0 & \alpha_{23} & \cdots & \alpha_{2m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

If R contains a matrix of the form

$$a = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

then

$$R = \left\{ \begin{pmatrix} 0 & \alpha & \beta & \cdots & \delta \\ 0 & 0 & \alpha & \cdots & \gamma \\ \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & 0 & \cdots & \alpha \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \middle| \alpha, \beta, \gamma \ldots \in F \right\},$$

and R is called a triangularly striped matrix algebra [20]. It is clear that the set of all triangularly striped $(m+1) \times (m+1)$-matrices over F is a commutative nilpotent algebra over F of dimension m and of nilpotency class m. Since $a^{m+1} = 0 \neq a^m$, this is a power algebra over the field F.

Example 5.2. Let R be a set of all matrices of the form

$$\begin{pmatrix} 0 & a & b \\ 0 & 0 & \theta(a) \\ 0 & 0 & 0 \end{pmatrix}.$$

with elements a, b in an algebra L over the field F and an endomorphism θ of the additive group of L. Then R is a nilpotent algebra of class 2 over F that is commutative if $a\theta(c) = \theta(c)a$ for each pair $(a, c) \in L \times L$. For example, if $F = GF(2)$, $L = GF(2^m)$, and θ is an automorphism of the field L, then we have an algebra $R(L)$ whose adjoint group $A(m, \theta)$ is described in [14]. A particular case of this is a Sylow 2-subgroup of the Suzuki simple group ${}^2B_2(2^m)$. Since $G = R^\circ$ is a group that has an automorphism transitive on maximal subalgebras (of codimension 1 in R), there exists a 2-algebra all of whose maximal subalgebras are isomorphic. Moreover, each subgroup of the adjoint group of this algebra is a subalgebra (see, for example, [18]). These groups are noncommutative and have rank m, while the corresponding algebra has dimension $2m$. For $p > 2$ these algebras give examples of algebras for which $\dim R = 2(r(R^\circ)-)$, where $r(R^\circ)$ is the Prüfer rank of R°. We do not know whether such examples exist in the commutative case for $p > 2$.

The other series of examples occur if we take the field $L = GF(q^2)$ of characteristic p with an automorphism θ of order 2 of this field. The set of matrices of the form

$$\begin{pmatrix} 0 & a & b \\ 0 & 0 & -\theta(a) \\ 0 & 0 & 0 \end{pmatrix}$$

with coefficients $a, b \in L$ is a p-algebra $R(L)$ whose adjoint group contains a Sylow p-subgroup of a group ${}^2A_2(q) = U_3(q)$. It consists of matrices satisfying the relations $\mathrm{tr}(b) + N(a) = 0$ and $N(a) = a\theta(a)$. However, the property $\mathrm{tr}(b) + N(a) = 0$ is not inherited by the sum of matrices and it is possible to prove that the Sylow 2-subgroup S of $U_3(q)$ is the adjoint group of some nilpotent p-algebra finding an appropriate ideal J in this algebra over $GF(p)$ such that $(R(L)/J)^\circ$ is isomorphic to S. Below we will describe another construction that shows that every group of class 2 and of exponent 4 is the adjoint group of some nilpotent p-algebra.

Example 5.3 (see also [6]). We shall prove that every 2-group of class 2 and of exponent 4 is the adjoint group of some nilpotent 2-algebra. The following property is crucial (see [6]): If G is a nilpotent group of class 2 and of exponent 4, then $\Phi(G) \leq Z(G)$ and is of exponent 2. Let G be a 2-group for which the above property holds, $x_1, x_2, \ldots, x_d$ be a minimal set of generators of a group G, and $z_1, z_2, \ldots, z_k$ be a minimal set of generators of a group $\Phi(G)$. Attach to G the vector space $R = V \oplus W$ over $F = GF(2)$, where V and W are its subspaces of dimension d and k respectively. We consider a one-to-one map $\psi : G \to R$ given by the following rule: if

$$g = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_d^{\alpha_d} z_1^{\beta_1} z_2^{\beta_2} \ldots z_k^{\beta_k},$$

then $\psi(g) = \sum\limits_{i=1}^{d} \alpha_i v_i + \sum\limits_{j=1}^{k} \beta_j w_j$, where $v_1, v_2, \ldots, v_d$ is a basis of V and $w_1, w_2, \ldots, w_k$ is a basis of W and $\alpha_i, \beta_j \in F (i \leq d, j \leq k)$. The multiplication in G determines two functions on R, a commutator function $(x_i, x_j) \in \Phi(G)$ for each pair x_i, x_j in $\{x_1, x_2, \ldots, x_d\}$ and the square map $x_i \to x_i^2 \in \Phi(G)$ for each $x_i \in \{x_1, x_2, \ldots, x_d\}$. Define products of elements in R by the rule $v_i v_j = 0$ if $i < j$, $v_i v_j = \psi((x_i, x_j)) \in W$ if $i > j$, and $v_i v_i = \psi(x_i^2) \in W$ for each $x_i, x_j \in \{x_1, x_2, \ldots, x_d\}$. Since the commutator and squaring function satisfy the well-known identities $(a,b)=(b,a)$ (recall that G is a 2-group) and $(a\circ b,c)=(a,c)\circ(b,c)$, $(a\circ b)^2=a^2\circ b^2\circ(a,b)$ for any $a,b,c\in G$, we have $\psi((x\circ y)^2)=\psi(x^2)+\psi(y^2)+\psi((x,y))$ for each pair of elements $x,y\in G$. Moreover, $[v_i,v_j]=v_iv_j-v_jv_i=\psi((x_i,x_j))$. By linearity we obtain the multiplication on R. If

$$u=\sum_{i=1}^{d}\alpha_iv_i+\sum_{j=1}^{k}\beta_jw_j,\qquad r=\sum_{i=1}^{d}\gamma_iv_i+\sum_{j=1}^{k}\delta_jw_j,$$

then $uv=\sum\limits_{i=1}^{d}\sum\limits_{j=1}^{d}\alpha_i\gamma_j(v_iv_j)$ and $\psi^{-1}([u,v])=\psi^{-1}(uv-vu)=(\psi^{-1}(u),\psi^{-1}(v))$ for each pair of elements $u,v\in R$. It is easy to find a matrix representation of an algebra R. If $v_iv_j=\sum\limits_{i=1}^{k}\beta_{ij}^sw_s$ with $\beta_{ij}^s\in F$, then we have the matrices

$$\theta(x_i)=\begin{pmatrix}\theta_1(x_i)\\ \theta_2(x_i)\\ \cdots\cdots\\ \theta_d(x_i)\end{pmatrix}=\begin{pmatrix}\beta_{i1}^1 & \beta_{i1}^2 & \cdots & \beta_{i1}^k\\ \beta_{i2}^1 & \beta_{i2}^2 & \cdots & \beta_{i2}^k\\ \cdots & \cdots & \cdots & \cdots\\ \beta_{id}^1 & \beta_{id}^2 & \cdots & \beta_{id}^k\end{pmatrix},$$

where β_{ij}^s are as above, and the elements x_i are represented by matrices of the following form with 1 in position $1,i+1$:

$$\begin{pmatrix}0 & \cdots & 1 & 0 & \cdots & 0\\ 0 & \cdots & 0 & 0 & \cdots & \theta(x_i)\\ 0 & \cdots & 0 & 0 & \cdots & 0\end{pmatrix}.$$

Thus, to x_i^2 and x_ix_j correspond to the following matrices:

$$\begin{pmatrix}0 & \theta_i(x_i)\\ 0 & 0\end{pmatrix},\quad\begin{pmatrix}0 & \theta_i(x_j)\\ 0 & 0\end{pmatrix}$$

respectively. By linearity we have determined all elements of a matrix algebra of dimension $d+k$ (which is a subalgebra of a $(d+k+1)\times(d+k+1)$ matrix algebra), and they are of the form

$$\begin{pmatrix}0 & x & y\\ 0 & 0 & \theta(x)\\ 0 & 0 & 0\end{pmatrix},$$

where $x\in F^d\simeq V$ and $y\in F^k\simeq W$. If $x=\sum\limits_{i=1}^{d}\lambda_iv_i$, then $\theta(x)=\sum\limits_{i=1}^{d}\lambda_i\theta(x_i)$. The adjoint group of this algebra is isomorphic to G by construction. Note that these arguments are valid for infinite 2-groups of exponent 4 as well.

Example 5.4. The same construction can be used to show that any p-group of class 2 and of exponent p is the adjoint group of some nilpotent p-algebra provided $p>2$ (see also [17]). The details are omitted. Note only that it also leads to matrices of the form

$$\begin{pmatrix}0 & x & y\\ 0 & 0 & \theta(x)\\ 0 & 0 & 0\end{pmatrix},$$

where $\theta(x)$ is determined as in the preceding example. The last example is also interesting since it gives the matrix description of all p-algebras ($p>2$) each subgroup of whose adjoint group is a subalgebra [18].

Example 5.5. An interesting series of examples can be obtained by a generalization of Example 5.2. Let A be a commutative p-algebra and $\theta_1,\theta_2,\dots,\theta_{k-1}$ be endomorphisms of its additive group. Define $R_k(A)$ to be the set of all $(k+1) \times (k+1)$-matrices with elements in A of the following form:

$$\begin{pmatrix} 0 & a_1 & a_2 & \dots & a_k \\ 0 & 0 & \theta_1(a_1) & \cdots & \theta_1(a_{k-1}) \\ \hdotsfor{5} \\ 0 & 0 & 0 & \cdots & \theta_{k-1}(a_1) \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Under suitable restrictions on the operators θ_i these matrices form an algebra. For example, if $A = F = GF(p^m), \theta_i = \theta i$, where $\theta_1 = \theta$ is a Frobenius automorphism of F, then $R_k(A)$ is a p-algebra that contains a power subalgebra of dimension k over $GF(p)$. The dimension of $R_k(A)$ over $GF(p)$ is mk and its nilpotency class is k.

Example 5.6. The adjoint group of the direct sum $R = R_1 \oplus R_2$ of two nilpotent p-algebras R_1 and R_2 with adjoint groups $R_1^\circ = G_1$ and $R_2^\circ = G_2$ respectively, is $G = G_1 \times G_2$. If J_1, J_2 are subalgebras of $\mathrm{Ann}(R_1)$ and $\mathrm{Ann}(R_2)$ respectively and $\phi : J_1 \to J_2$ is an isomorphism from J_1 onto J_2, then the subalgebra $I = \{j - \phi(j) | j \in J_1\}$ of R is contained in the annihilator $\mathrm{Ann}(R)$ of an algebra R. The quotient algebra R/I is called the sum of subalgebras with joint subalgebra $I \simeq J_1 \simeq J_2$. It is clear that the adjoint group of this algebra is a central product $G_1 * G_2$ with common subgroup $I^\circ \simeq G_1 \cap G_2 \subseteq Z(G_1) \cap Z(G_2)$. This simple construction allows us to obtain new classes of algebras and their adjoint groups. For example, if $G = (\langle a \rangle \times \langle z \rangle) \rtimes \langle b \rangle$ is a Miller–Moreno group of order p^3 that is the adjoint group of a nilpotent p-algebra R defined by relations $a^2 = b^2 = z^2 = 0$, $ab = -ba = z$, then we obtain an algebra S whose adjoint group is of the form

$$((\langle x \rangle \times \langle t \rangle) \rtimes \langle y \rangle) \times A = H, \quad |x| = p^m, \quad |y| = p^k, \quad |t| = p^n, \quad [x, y] = t^{p^{n-1}}, \quad x^p, y^p, t \in Z(H)$$

and A is an abelian group.

Let U_1, U_2, and U_3 be the power algebras with $\dim U_1 = p^{m-1}$, $\dim U_2 = p^{k-1}$, and $\dim U_3 = p^{n-1}$. It follows from the above consideration that the element z of the algebra R is in the annihilator of R. We can form the algebra $R_1 = R \oplus U_1 \oplus U_2 \oplus U_3$, where $U_i = \langle\langle u_i \rangle\rangle$ $(i = 1, 2, 3)$. It follows from Theorem 2.1 that $U_i^\circ = C_i \times Y_i$ with $C_1 \simeq \mathbb{Z}_{p^m}$, $C_2 \simeq \mathbb{Z}_{p^k}$, and $C_3 \simeq \mathbb{Z}_{p^n}$. Moreover, C_i contains the annihilator of U_i for each $i \leq 3$. Identifying the images of u_1, u_2, u_3, a, b, z in R_1 with these elements, we have that $x = u_1 + a$ has nillity $p^{m-1} + 1$, $y = u_2 + b$ has nillity $p^{k_1} + 1$, and $[x, y] = [u_1 + a, u_2 + b] = [a, b] \in \mathrm{Ann}(R \oplus U_1 \oplus U_2)$. Next form an algebra $S = R_1/J$, which is a sum of subalgebras $R + U_1 + U_2$ and U_3 with joint subalgebra $\langle\langle z \rangle\rangle \simeq \langle\langle u_3^{p^{n-1}} \rangle\rangle$. It is clear that the subalgebra S generated by the elements x, y, and u_3 has an adjoint group of the required form.

Similar arguments show that for each Miller–Moreno p-group M there exists an abelian p-group A, such that $M \times A$ is the adjoint group of some nilpotent p-algebra R.

Example 5.7. It is possible to show that the direct product of the dihedral group D of order 16 (or another 2-group of maximal class and of order at least 16) with any abelian 2-group A cannot be the adjoint group of some nilpotent 2-algebra. On the other hand, for any p-group G of order p^4 with $p > 2$ and of exponent p there exists a nilpotent p-algebra R of dimension 5 such that $G \times \mathbb{Z}_p$ is the adjoint group of this algebra (see Sec. 4).

Example 5.8. The notion of a quasi-direct sum of rings was introduced in [9]. Let A and B be rings. A ring R, written as $A \uplus B$, is called a quasi-direct sum of A and B if the following conditions are satisfied:

(i) B is a subring of R;
(ii) A is an ideal of R;
(iii) R is a direct sum of A and B as additive groups.

Clearly, if $R = A \uplus B$ is a nilpotent or nil ring, then the adjoint group of this ring is a semidirect product $R^\circ = A^\circ \rtimes B^\circ$ of the adjoint group of A and the adjoint group of B. This definition could be generalized in order to determine external quasi-direct sums [9]. We present here a slightly weaker useful construction.

Assume that M is a ring that is also a right A-module. Define the ring $R = M^2 \uplus A$ in the following way: $R = (M^2, A) = \{(m_1, m_2, a) | m_1, m_2 \in M, a \in A\}$ with $(m_1, m_2, a) = (m_1', m_2', a')$ if and only if $m_1 = m_1'$,

$m_2 = m'_2$, and $a = a'$. The operations in R are defined by the laws

$$(m_1, m_2, a) + (m'_1, m'_2, a') = (m_1 + m'_1, m_2 + m'_2, a + a'),$$
$$(m_1, m_2, a)\,(m'_1, m'_2, a') = (m_1 m'_1, m_1 m'_2 + m_2 a, aa')$$

It is easy to see that all ring properties are satisfied. If M and A are nilpotent rings of nilpotency class $n(M), n(A)$ respectively, then R is a nilpotent ring of nilpotency class at most $n(M) + n(R) + 1$. This construction can be expressed symbolically in the following form:

$$R = \begin{pmatrix} M & M \\ 0 & A \end{pmatrix} = \begin{pmatrix} M & M \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & A \end{pmatrix},$$

and it is easy to see that the operations on R agree with this representation. Moreover, the elements $(0, 0, a)$ with $a \in A$ form a subring isomorphic to A and the elements $(m, 0, 0)$ with $m \in M$ form a subring isomorphic to M. Again the structure of R° could be expressed in matrix form:

$$R^\circ = \begin{pmatrix} M+I & M \\ 0 & A+I \end{pmatrix}, \quad A^\circ = \begin{pmatrix} I & M \\ 0 & A+I \end{pmatrix}, \quad (M+M)^\circ = \begin{pmatrix} M+I & M \\ 0 & I \end{pmatrix}.$$

Example 5.9. A slight simplification of the above construction leads to the following definitions. Let A be a ring and M be a right A-module. Define $R = (M, A) = \{(m, a) | m \in M,\ a \in A\}$ with the equality $(m, a) = (m', a')$ for $m, m' \in M$, $a, a' \in A$ if and only if $m = m'$, $a = a'$. The operations on R are as follows:

$$(m, a) + (m', a') = (m + m', a + a'), \quad (m, a)(m', a') = (ma', aa').$$

As before, R is a quasi-direct sum of M and A where M is a null ring, and R is a nilpotent or nil ring if A has this property. A similar construction was used in [3].

We will use the preceding construction in order to obtain the following.

Theorem 5.1. *Let H be a subgroup of the adjoint group of some nilpotent p-algebra R such that $H^\#$ is a linearly independent set in R. Let V be a right regular R-module, regarded as a null algebra. Then the quasi-direct sum $L = V \uplus R$ defined in Example 5.9 has an adjoint group that contains the wreath product $\mathbb{Z}_p \operatorname{wr} H$ of the groups $\mathbb{Z}_p$ and H.*

Before the proof of this theorem recall some definitions. If R is a nilpotent p-algebra, then the additive group of the algebra $A = R \oplus 1.F$ ($F = GF(p)$) is called a right regular R-module and the action of R on V is defined by the multiplications in R. If $\{1, a_1, a_2, \dots, a_n\}$ is a basis of A (and $\{a_1, a_2, \dots, a_n\}$ is a basis of R), then V has a basis of elements $v_1, v_{a_1}, v_{a_2}, \dots, v_{a_n}$ and if

$$a_i r = \sum_{j=1}^{n} \beta_{ij} a_j \quad (r \in R) \quad \text{then} \quad v_{a_i} r = \sum_{j=1}^{n} \beta_{ij} v_{a_j}.$$

This construction gives a natural representation of R as a subalgebra of $M_{n+1}(F)$ and is described in [20]. We say that the subgroup H of the adjoint group of p-algebra R is an active subgroup of R° if the regular representation of the algebra R induces a regular representation of H in the usual sense. In other words, $H^\#$ consists of linearly independent elements in R. Hence $A = R \oplus 1.F$ contains a group algebra of a subgroup H. It is clear that if H is an active subgroup of an algebra R, then $\dim R \geq |H|$. Thus, the theorem asserts that if H is an active subgroup of some nilpotent p-algebra R, then there exists a nilpotent p-algebra $L = V \uplus R$ whose adjoint group $L^\circ = V^\circ \rtimes R^\circ$ is a semidirect product of V° and R° and L° contains a wreath product $\mathbb{Z}_p \operatorname{wr} H$.

Proof of Theorem 5.1. Let $\{a_1, a_2, \dots, a_n\}$ is a basis of R, where $\{a_1, a_2, \dots, a_m\} = H^\#, m \leq n$. Let $\{v_1, v_{a_1}, v_{a_2}, \dots, v_{a_n}\}$ be a basis of V corresponding to an algebra $R + 1.F$ as described above. Then $v_1 a_i = v_{a_i}$ for each $i \leq n$. The action of a group R° on V° corresponds with the law $u^r = u(1 + r)$ for each $u \in V$ and $r \in R$. Let $U_1 = \langle v_1 \rangle$ be a subalgebra spanned by v_1 (this is also an additive cyclic subgroup of V). If $U_1^a = U_1$ for some $a \in R^\circ$, then $v_1^a = v_1(1 + a) = \lambda v_1$ for some $\lambda \in F$ and $v_1((\lambda - 1) - a) = 0$. It follows that

$\lambda - 1 = 0$ and $v_1 a = 0$, hence $a = 0$. Thus, only the identity element of R° fixes U_1. Let $\Omega = \{U_1^h | h \in H\}$. It is clear that for each $h \in H$ there corresponds a permutation

$$\phi(h) = \begin{pmatrix} U_1 & U_1^{a_1} & U_1^{a_2} & \cdots & U_1^{a_m} \\ U_1^h & U_1^{a_1 \circ h} & U_1^{a_2 \circ h} & \cdots & U_1^{a_m \circ h} \end{pmatrix},$$

where $\circ$ is the operation in R°. Since $\{h, a_1 \circ h, \dots a_m \circ h\} = H$, this map is well defined. It is obvious that $\phi(h \circ y) = \phi(h) \circ \phi(y)$ since $(1 + a_i)(1 + h) = (1 + a_i + h + a_i h) = 1 + a_i \circ h$, where $a_i \circ h \in R$ for each $i \leq m$. Assume that the elements $v_1, v_1(1 + a_1), \dots, v_1(1 + a_m)$ are not linearly independent. Then there exists $\lambda_0, \lambda_1, \dots, \lambda_m \in F$ such that $\sum_{i=0}^{m} \lambda_i = 1$ and $\sum_{i=0}^{m} \lambda_i v_1(1 + a_i) = v_1(\sum_{i=1}^{m} \lambda_i(1 + a_i)) = v_1(1 + \sum_{i=0}^{m} \lambda_i a_i) = 0$. Since $\sum_{i=0}^{m} \lambda_i a_i = a \in R$, $1 + a$ is an invertible element in $A = R + 1.F$ and the equality $v_1(1 + a) = 0$ forces $v_1 = 0$, which is not the case. Hence the subgroup $T = \langle U_1^h | h \in H\rangle$ is a direct sum of subgroups $U_1^h (h \in H)$ and is invariant under H and $T \rtimes H$ is isomorphic to the wreath product $\mathbb{Z}_p \operatorname{wr} H$. Hence the adjoint group $L^\circ = V^\circ \rtimes R^\circ$ contains $T \rtimes H \simeq \mathbb{Z}_p \operatorname{wr} H$. Theorem 5.1 is proved. $\square$

It is easy to see that any abelian group H can be embedded as an active subgroup into the adjoint group of some commutative nilpotent p-algebra. It is enough to consider the group algebra FH over $F = GF(p)$. By Theorem 5.1, for any p-group G with an elementary abelian commutator subgroup, there exists a p-algebra L such that $G \leq L^\circ$ and L° is a metabelian group. However, we cannot assume that G can be embedded in some modular group algebra of the same nilpotency class in general, since usually a metabelian group algebra is abelian [7]. Therefore, no metabelian group can be the active subgroup of some nilpotent p-algebra with metabelian adjoint group. It seems that the following problem is open: is every finite p-group G embedded into the adjoint group of some nilpotent p-algebra with the same derived length?

REFERENCES

1. B. R. Allen, "On hypercomplex number systems belonging to an arbitrary field," *Trans. Amer. Math. Soc.*, **9**, 203–218 (1908).
2. B. Amberg and L. S. Kazarin, "On the rank of the product of two finite p-groups and nilpotent p-algebras," *Commun. Algebra*, to appear.
3. B. Amberg and Ya. P. Sysak, "Radical rings and products of groups," In: *Proc. "Groups'97 Bath/St. Andrews,"* to appear (1999).
4. J. C. Ault and J. F. Watters, "Circle groups of multiplicative rings," *Amer. Math. Monthly*, **80**, 48–52 (1973).
5. H. A. Bender, "A determination of the groups of order p^5," *Ann. Math. (2)*, **29**, 61–72 (1972).
6. A. A. Bovdi, "On circle groups of nilpotent rings of characteristic 2," *Periodica Math. Hungarica*, **32** (1–2), 31–34 (1996).
7. A. A. Bovdi, "The group of units of a group algebra of characteristic p," *Publ. Math. Debrecen*, **52** (1–2), 193–244 (1998).
8. F. W. Boyce, *Certain types of nilpotent algebras*, Ph.D. dissertation, University of Chicago (1938).
9. Y. Q. Chen and K. P. Shum, "Quasi-direct sums of rings and their radicals," *Commun. Algebra*, **25** (9), 3043–3055 (1997).
10. N. H. Eggert, "Quasi-regular groups of finite commutative nilpotent algebras," *Pacif. J. Math.*, **36**, 631–634 (1971).
11. K. S. Ghent, "A note on nilpotent algebras in four units," *Bull. Amer. Math. Soc.*, **40**, 331–338 (1934).
12. B. O. Gorlov, "Finite nilpotent algebras with metacyclic adjoint group," *Ukr. Math. Zh.*, **47**, 1426–1431 (1995).
13. B. Huppert, *Endliche Gruppen*, I, Springer, Berlin (1967).
14. B. Huppert and N. Blackburn, *Finite Groups*, II, Springer, Berlin–Heidelberg–New York (1982).
15. R. L. Kruse and D. T. Price, *Nilpotent Rings*, Gordon and Breach, New York (1967).
16. M. W. Konvisser, "2-Groups which contain exactly three involutions," *Math. Z.*, **130**, 19–30 (1973).

17. L. E. Moran and R. N. Tench, "Normal complements in mod p envelopes," *Israel J. Math.*, **27**, 331–338 (1977).
18. S. V. Popovich and Ya. P. Sysak, "Radical algebras in which every subgroup of the adjoint group is a subalgebra," *Ukr. Math. Zh.*, **49**, 1646–1653 (1997).
19. G. Scorza, "Lie algebre del 4° ordine," *Mem. Real Acad. Sci. Fis. Mat. Napoli (2)*, **20**, No. 14, (1935); *Giorg. Mat. Battaglini (3)*, **73**, 129–212 (1935).
20. D. A. Suprunenko and R. I. Tyshkevich, *Commutative Matrices*, Academic Press, New York–London (1968).
21. K.-I. Tahara and H. Hirosi, "On the circle group of finite nilpotent rings," In: *Proc. "Groups-Korea,"* 161–179 (1983).
22. A. D. Ustyuzhaninov, "Finite 2-groups with three involutions," *Sib. Mat. Zh.*, **13**, 198–211 (1972).