Adjoint groups of p-nil rings and p-group automorphisms

Yassine Guerboussa* Bounabi Daoud

Abstract

We introduce a class of rings, namely the class of left or right p-nil rings, for which the adjoint groups behave regularly. Every p-ring is close to being left or right p-nil in the sense that it contains a large ideal belonging to this class. Also their adjoint groups occur naturally as groups of automorphisms of p-groups. These facts and some of their applications are investigated in this paper.

1 Introduction

The study of groups modulo other algebraic structures has proved to be very useful from the early days of group theory, namely in the context of Lie groups with their associated Lie algebras, or in the context of representation theory which provides a means of studying groups via linear algebra or more generally module theory. One should mention other interesting tools such as the Mal'cev and Lazard correspondences, and the Lie rings associated to the lower central series (or their variants) of groups, we refer the reader to [10] for more information and references. It is worth to note that some recent breakthroughs such as Zelmanov's solution of the restricted Burnside problem, or Shalev's proof of the coclass conjecture A, are done by reducing the original problems to questions about Lie algebras. Recall that the coclass of a p-group G of order p^n and class c is equal to $n - c$, and the coclass conjecture A (now a theorem) states that there is an integer

*Corresponding author
Received by the editors in September 2013 - In revised form in October 2013.
Communicated by F. Point.
2010 *Mathematics Subject Classification :* Primary: 20D45; Secondary: 16N20.
Key words and phrases : nilpotent rings, adjoint groups, finite p-groups, automorphisms.

$f(p,r)$ depending on p and r such that any finite p-group G of coclass r has a normal subgroup N of class at most 2 and index at most $f(p,r)$. The interested reader is referred to [13] for more details about the coclass theory.

On another side, ring theory arises naturally in studying the automorphisms of abelian groups. Indeed, the automorphism group of an abelian group G is the group of units of the ring of endomorphisms of G. This fact was used by Shoda [17] in investigating the structure of such automorphism groups. While the preceding fact is no longer true if G is not abelian, H. Laue (see [12]) observed that there is a general analogue which works for some subgroups of $\mathrm{Aut}(G)$.

If N is a subgroup of G, then we denote by $\mathrm{End}_N(G)$ the set of all endomorphisms u of G such that $x^{-1}\,\mathrm{u}(x) \in N$, for all $x \in G$; in other words $\mathrm{End}_N(G)$ is the set of all endomorphisms of G that leave N invariant and send each coset of N to itself. We denote by $\mathrm{Aut}_N(G)$ the set of automorphisms of G that lie in $\mathrm{End}_N(G)$. Clearly $\mathrm{End}_N(G)$ is a monoid under the usual composition of maps.
If N is normal and abelian, then it can be viewed as a G-module via conjugation $n^x = x^{-1}nx$, $x \in G$ and $n \in N$. A derivation of G into N is a mapping $\delta : G \to N$ such that $\delta(xy) = \delta(x)^y\delta(y)$. The set $\mathrm{Der}(G,N)$ of these derivations is a ring under the addition $(\delta_1 + \delta_2)(x) = \delta_1(x)\delta_2(x)$, and the composition of maps as a multiplication, that is $(\delta_1\delta_2)(x) = \delta_2(\delta_1(x))$, with $\delta_1, \delta_2 \in \mathrm{Der}(G,N)$ and $x \in G$. Now, every endomorphism $\mathrm{u} \in \mathrm{End}_N(G)$ defines a derivation $\delta_{\mathrm{u}}(x) = x^{-1}\,\mathrm{u}(x)$ of G into N. And conversely, to each derivation $\delta \in \mathrm{Der}(G,N)$ we can associate an endomorphism $\mathrm{u} \in \mathrm{End}_N(G)$, with $\mathrm{u}(x) = x\delta(x)$.

On the other hand, for any (associative) ring R, one can define the circle operation $x \circ y = x + y + xy$. The set of all elements of R forms a monoid with identity element $0 \in R$ under this operation. This monoid is called the adjoint monoid of the ring R, and the adjoint group R° of R is the group of invertible elements in this monoid.

Proposition 1.1. *(see [12, Lemma 3.1]) Under the above notation, the mapping $u \mapsto \delta_u$ is an isomorphism between the monoid $\mathrm{End}_N(G)$ and the adjoint monoid of the ring $\mathrm{Der}(G,N)$. In particular it induces an isomorphism between the corresponding groups of invertible elements.*

This relation was applied by H. Laue in [12] to proving some analogues of Shoda's results. In [3], F. Catino and M. Miccoli showed that the main results about IA-automorphisms of 2-generated metabelian groups can be derived in a natural way from Laue's relation, with a considerable gain of clarity. Note also that it was used implicitly by A. Caranti and S. Mattarei (see [2]), to prove results about the automorphisms of p-groups of maximal class. Excepting these papers, and in spite of its interest and the considerable work devoted to the group automorphisms, it seems that Laue's relation was ignored completely in the existing litterature.
The results of this paper may be seen as the fruit of further investigations of the interplay between Rings and Group Automorphisms, summarized in Proposition 1.1.

First, let us fix some notation. The letter p denotes a prime number. Having a group G, $\gamma_i = \mathrm{fl}_i(G)$ and $Z_i = \mathrm{Z}_i(G)$ denote respectively the terms of the lower and the upper central series of G. We denote by $\Omega_{\{n\}}(G)$ the set of all elements $x \in G$ such that $x^{p^n} = 1$, and $\Omega_n(G)$ denotes the subgroup generated by $\Omega_{\{n\}}(G)$. By $\mathrm{d}(G)$ we denote the minimal number of generators of G, the (Prüfer) rank of G is defined to be

$$\mathrm{rk}(G) = \sup\{\mathrm{d}(H), H \text{ a finitely generated subgroup of } G\},$$

and the exponent of G is denoted by $\exp(G)$.
As a special notation, $\mathrm{P}(G)$ will denote $\gamma_2(G)G^4$ if $p = 2$, and $\gamma_2(G)G^p$ if $p > 2$, $\mathrm{S}(G)$ denotes $\mathrm{Z}(G) \cap \mathrm{P}(G)$. If G is a finite p-group then we denote by r and s the integers defined by $\exp(G/G') = p^r$ and $\exp(\mathrm{Z}(G)) = p^s$.

Let R be a ring. We say that R is left p-nil if every element x of order p (4 if $p = 2$) in R^+ is a left annihilator of R, that is $px = 0$ ($4x = 0$ if $p = 2$) implies $xy = 0$, for all $y \in R$. We say that R is right p-nil if its opposite ring is left p-nil. The ring R is said to be p-nil if it is left and right p-nil.

The first result shows that the p-power structure of the adjoint group of such a ring R is very close to that of R^+.

Theorem A. *Let R be a p-ring. If R is left or right p-nil, then $\Omega_{\{n\}}(R^\circ) = \Omega_n(R^+)$, for every $n \geq 1$. In particular we have $\Omega_n(R^\circ) = \Omega_{\{n\}}(R^\circ)$.*

It follows immediately that

Corollary A. *Let R be a p-ring. If R is p-nil, then $\Omega_1(R^\circ) \leq \mathrm{Z}(R^\circ)$ ($\Omega_2(R^\circ) \leq \mathrm{Z}(R^\circ)$, for $p = 2$), in other words, R° is p-central.*

Moreover if we assume that R is a finite p-ring and R^+ can be generated by d elements, then every subgroup of R° can be generated by d elements.

Theorem B. *Let R be a finite p-ring. If R is left or right p-nil, then* $\mathrm{rk}(R^\circ) = \mathrm{d}(R^+)$. *In particular,* $\mathrm{rk}(R^\circ) = \mathrm{d}(\Omega_1(R^\circ))$.

It is conjectured in ([4], see Remark (b) in the last paragraph) that $\mathrm{rk}(R^\circ) \leq \alpha.\,\mathrm{rk}(R^+)$, for any nilpotent finite p-ring R, with $\alpha = 2$ if $p = 2$, and $\alpha = 1$ if $p > 2$ (actually this conjecture is formulated for the class of nil rings and the class of radical periodic rings, whose additive groups have a finite rank, but from that paper one can reduce it to the class of finite nilpotent p-rings). Thus Theorem B confirmes this conjecture in the class of p-nil rings.
Note that particularly O. Dickenschied proved the above inequality for finite nilpotent p-rings, with $\alpha = 3$ if $p = 2$, and $\alpha = 2$ if $p > 2$, using powerful p-groups (see [4, Lemma 2.4]). The following corollary generalizes this to the class of all finite p-rings, though with an alternative (self contained) proof.

Corollary B. *Let be R a finite p-ring and P a p-sylow of R°. Then* $\mathrm{rk}(P) \leq \alpha.\,\mathrm{d}(R^+)$, *with $\alpha = 3$ if $p = 2$, and $\alpha = 2$ if $p > 2$.*

Let N be an abelian normal subgroup of a p-group G. It is straightforward to see that the set of derivations in $\mathrm{Der}(G,N)$ that are trivial on $\Omega_1(N)$ or $\Omega_2(N)$ if $p = 2$ (which in fact can be identified to the ring $\mathrm{Der}(G/\Omega_1(N),N)$ or $\mathrm{Der}(G/\Omega_2(N),N)$ for $p = 2$) forms a left p-nil ring, it follows that the above theorems apply to the group of automorphisms acting trivially on G/N and $\Omega_1(N)$ ($\Omega_2(N)$ if $p = 2$). However, we would be more interested to the case of the ring $\mathrm{Hom}(G,\mathrm{S}(G))$ which is right p-nil. Essentially, this fact can be used to prove the following.

Theorem C. *Let G be a finite p-group of class c. Then the exponent of $\mathrm{Aut}_{\mathrm{P}(G)}(G)$ does not exceed p^{t^2c-t}, where $t = \min\{r,s\}$. Moreover if G is generated by d elements then $\exp(P) \leq p^{t^2c-t+d-1}$ if $p > 2$ and $\exp(P) \leq p^{t^2c-t+2d-1}$ if $p = 2$, for any p-subgroup P of $\mathrm{Aut}(G)$.*

As show the automorphism groups of elementary abelian p-groups, the p-exponent of $\mathrm{Aut}(G)$ cannot in general be independent from the number of generators of G.

A slightly modified version of the following proposition was first proved (as noted in [14, p. 111]) by Kargapolov (see [9]). Another different proof was given by R. Baer and H. Heineken in [1]. In this paper we give another proof based on a property of the right p-nil rings. It seems that this proof is more transparent, however it gives just a slight improvement of the known bounds.

Proposition D. *Let G be an abelian p-group of rank d and let d' denote the rank of $\mathrm{P}(G)$. Then every p-subgroup P of $\mathrm{Aut}(G)$ can be generated by $dd' + \frac{d^2}{4}$ elements if $p > 2$, and by $dd' + \frac{3d^2-d}{2}$ elements if $p = 2$. In particular for every such a P we have $\mathrm{d}(P) \leq \frac{5d^2}{4}$ if $p > 2$, and $\mathrm{d}(P) \leq \frac{5d^2-d}{2}$ if $p = 2$.*

D. Segal and A. Shalev generalized Proposition D to all the finite p-groups in [18, Lemma 2.1] (we don't know if such a generalization was established earlier). This generalization was proved directly, without using the abelian case. By combining the idea of the proof of [18, Lemma 2.1] and Proposition D, we obtain a shorter proof which provides better bounds.

Corollary D. *Let G be a finite p-group of rank k. Then every p-subgroup P of $\mathrm{Aut}(G)$ can be generated by $\frac{9k^2}{4}$ elements if $p > 2$, and by $\frac{7k^2-k}{2}$ elements if $p = 2$.*

The remaining part of this paper is divided into two sections, Section 2 is devoted to studying the above class of rings and their adjoint groups. In Section 3 we shows how these rings can be used to investigate the automorphisms of p-groups.

2 Adjoint groups of p-nil rings

Let us recall the definition.

Definition 2.1. *Let R be a ring. We say that R is left p-nil if every element x of order p (4 if $p = 2$) in R^+ is a left annihilator of R, that is $px = 0$ ($4x = 0$ if $p = 2$) implies $xy = 0$, for all $y \in R$. We say that R is right p-nil if its opposite ring is left p-nil. The ring R is said to be p-nil if it is left and right p-nil.*

For instance, for any ring R, the subring $S = pR$ ($S = 4R$ if $p = 2$) is p-nil. Also, it follows easily that the left and the right annihilators of $\Omega_1(R^+)$ ($\Omega_2(R^+)$ if $p = 2$) are respectively right and left p-nil.
A ring R is said to be nilpotent of class n, if $R^{n+1} = 0$ and n is the least non-negative integer satisfying this. Here R^{n+1} denotes the additive subgroup generated by all the products of $n + 1$ elements of R.

Theorem 2.2. *Let R be a ring with an additive group of finite exponent p^m. If R is left or right p-nil, then R is nilpotent of class at most m. In particular the adjoint group R° is nilpotent of class at most m.*

Proof. Assume that R is left p-nil. We claim that $p^{m-n+1}R^n = 0$, for all $n \leq m + 1$. This is obvious for $n = 1$. Now if $x \in R^n$, then by induction $p^{m-n+1}x = 0$. It follows that $p^{m-n}x$ has order 1 or p, therefore $(p^{m-n}x)y = p^{m-n}(xy) = 0$, for all $y \in R$. This shows that $p^{m-n}R^{n+1} = 0$. Now, for $n = m + 1$ we have $R^{m+1} = 0$, which proves that R is nilpotent of class at most m. The result follows for R right p-nil by a similar argument. The second assertion follows from ([11, Theorem 1.6.4]). ∎

Remark. *Note that the bound on the nilpotency class can be improved to $m/2 + 1$ for the even prime. And the above theorem holds for $p = 2$, under the assumption that every element $x \in R$ satisfying $2x = 0$ is a left or right annihilator of R.*

Since it is obvious that a subring of a left (right) p-nil ring is left (right) p-nil, it is not clear that this would be true for all the factor rings. The following lemma shows that this holds for some factors.

Lemma 2.3. *If R is a left (right, resp) p-nil ring, then the factor ring $R/\Omega_n(R^+)$ is left (right, resp) p-nil for all $n \geq 1$.*

Proof. Assume that R is left p-nil.
Assume first that $p > 2$, and let be $x \in R$ such that $px \in \Omega_n(R^+)$. Then $p^n x \in \Omega_1(R^+)$, and by assumption $(p^n x)y = p^n(xy) = 0$, for all $y \in R$. Therefore $xy \in \Omega_n(R^+)$, for all $y \in R$.
For $p = 2$, if $x \in R$ such that $4x \in \Omega_n(R^+)$, then $2^n x \in \Omega_2(R^+)$, therefore $(2^n x)y = 2^n(xy) = 0$, and so $xy \in \Omega_n(R^+)$, for all $y \in R$.
The result follows similarly if R is right p-nil. ∎

Proof of Theorem A. We denote by $x^{(k)}$ the *kth* power of x in the adjoint group of R.
Assume first that $n = 1$. For $p > 2$, we have $px = 0$ implies $x^i = 0$ for $i \geq 2$. Hence

$$x^{(p)} = \sum_{i \geq 1} \binom{p}{i} x^i = px = 0,$$

and so $x \in \Omega_{\{1\}}(R^\circ)$. Conversely, if $x^{(p)} = 0$ then

$$px = -\sum_{i \geq 2} \binom{p}{i} x^i.$$

Let p^m be the order of x in R^+. If $m \geq 2$, then $p^{m-1}x$ has order p, hence $p^{m-1}x^2 = 0$, and similarly we have $p^{m-2}x^i = 0$, for $i \geq 3$. Now if we multiply the above equation by p^{m-2}, we obtain

$$p^{m-1}x = -\sum_{i \geq 2} \binom{p}{i} p^{m-2}x^i = 0$$

This contradicts the definition of the order of x. Therefore $m \leq 1$, and so $x \in \Omega_1(R^+)$.
For $p = 2$, $2x = 0$ implies $4x = 0$, thus $x^2 = 0$. It follows that $x^{(2)} = 2x + x^2 = 0$, so $x \in \Omega_{\{1\}}(R^\circ)$. Conversely, if $x^{(2)} = 0$ then $2x = -x^2$. Assume that x has order $2^n > 2$ in R^+, then $2^{n-2}x^2 = 0$, thus $2^{n-1}x = -2^{n-2}x^2 = 0$, a contradiction. It follows that $2x = 0$.
Now we proceed by induction on n. If $x \in \Omega_n(R^+)$, then $px \in \Omega_{n-1}(R^+)$. This implies that $x + \Omega_{n-1}(R^+) \in \Omega_1((R/\Omega_{n-1}(R^+))^+)$. Lemma 2.3 and the first step imply that $x + \Omega_{n-1}(R^+) \in \Omega_{\{1\}}((R/\Omega_{n-1}(R^+))^\circ)$. Hence $x^{(p)} \in \Omega_{n-1}(R^+)$, and by induction $x^{(p)} \in \Omega_{\{n-1\}}(R^\circ)$. Thus $x \in \Omega_{\{n\}}(R^\circ)$. It follows that $\Omega_n(R^+) \subset \Omega_{\{n\}}(R^\circ)$. The inverse inclusion follows similarly.
Finally, the equality $\Omega_n(R^\circ) = \Omega_{\{n\}}(R^\circ)$ follows from the fact that $(\Omega_n(R^+))^\circ$ is a subgroup of R° and $\Omega_n(R^\circ)$ is generated by $\Omega_{\{n\}}(R^\circ)$. ∎

Before proving Theorem B, we need the following lemma.

Lemma 2.4. *Let R be a left p-nil p-ring with an additive group of finite exponent. Let U be the intersection of $\Omega_1(R^+)$ with the right annihilator of R. Then U is a non-trivial ideal and the factor ring R/U is left p-nil.*

Proof. As R is nilpotent, let n denote the largest integer such that $R^n \neq 0$. Then $0 \neq \Omega_1(R^n)$ lies in U, so U is not trivial.
Let be $x, y \in R$ such that $px \in U$ ($4x \in U$, for $p = 2$). Then $z(px) = pzx = 0$ ($z(4x) = 4zx = 0$, for $p = 2$) for all $z \in R$. As R is left p-nil, it follows that $zxy = 0$, for all $z \in R$, hence xy is a right annihilator of R. Also we have $px \in \Omega_1(R^+)$ ($px \in \Omega_2(R^+)$, for $p = 2$), so $pxy = 0$, thus $xy \in U$. ∎

Proof of Theorem B. Since $U^+ = U^\circ$, we shall denote both of them by U. We claim that $\mathrm{d}(H) \leq \mathrm{d}(\Omega_1(H))$, for any $H \leq R^\circ$. Assume that R is left p-nil, and assume

the result is true for any such ring of order $< |R|$. Also, we assume that the result holds for any subgroup with order $< |H|$. We have $HU/U \cong H/H \cap U$ is a subgroup of $R^\circ/U = (R/U)^\circ$, from our assumption and Lemma 2.4 it follows that $\mathrm{d}(H/H \cap U) \leq \mathrm{d}(\Omega_1(H/H \cap U))$. Now if $H \cap U \not\leq \Phi(G)$, and since $U \leq \Omega_1(\mathrm{Z}(R^\circ))$, we can find a maximal subgroup $K \leq H$ and a subgroup P of order p in $H \cap U$ such that $H \cong K \times P$. By the minimality of H, we have $\mathrm{d}(H) = d(K) + 1 \leq \mathrm{d}(\Omega_1(K)) + 1 = \mathrm{d}(\Omega_1(H))$. Otherwise, we have $\mathrm{d}(H) = \mathrm{d}(H/H \cap U)$. Let A be the subgroup of H such that $A/H \cap U = \Omega_1(H/H \cap U)$. By induction, if $A < H$ then $\mathrm{d}(H) \leq \mathrm{d}(A/H \cap U) \leq \mathrm{d}(A) \leq \mathrm{d}(\Omega_1(A))$, and since $\Omega_1(H)$ is abelian, it follows that $\mathrm{d}(H) \leq \mathrm{d}(\Omega_1(A)) \leq \mathrm{d}(\Omega_1(H))$.
Now we have to assume that $H/H \cap U = \Omega_1(H/H \cap U)$ which is abelian. For $p = 2$, we have $H \leq \Omega_2(R^\circ)$, so H is abelian and we are done. For $p > 2$, we have $[H, H] \leq H \cap U$. Since $H \cap U$ is central, it follows that H is nilpotent of class ≤ 2, so H is regular (see [5, II.10]). We have $p^{\mathrm{d}(H)} \leq |H : H^p| = |\Omega_1(H)| = p^{\mathrm{d}(\Omega_1(H))}$. Finally, since $\Omega_1(R^\circ)$ is abelian, it follows that $\mathrm{d}(H) \leq \mathrm{d}(\Omega_1(H)) \leq \mathrm{d}(\Omega_1(R^\circ)) = \mathrm{d}(R^+)$. ∎

Proof of Corollary B. First note that the ideal $U = pR$ ($4R$ if $p = 2$) is a left p-nil p-ring, and $(R/U)^\circ \cong R^\circ/U^\circ$ (note that one can take U to be the left or the right annihilator of $\Omega_1(R^+)$, or $\Omega_2(R^+)$ if $p = 2$). Let H be a p-subgroup of R°. Then $\mathrm{d}(H) \leq \mathrm{d}(H/H \cap U^\circ) + \mathrm{d}(H \cap U^\circ)$. Theorem B implies that $\mathrm{d}(H \cap U^\circ) \leq \mathrm{d}(U^+) \leq \mathrm{d}(R^+)$. On the other hand, $H/H \cap U^\circ \cong HU^\circ/U^\circ$ is a subgroup of $R^\circ/U^\circ \cong (R/U)^\circ$, so $p^{\mathrm{d}(H/H \cap U^\circ)} \leq |(R/U)^\circ| \leq |R/U|$. Now, if $p > 2$ then $|R/U| = p^{\mathrm{d}(R^+)}$, and if $p = 2$ then $|R/U| = |R/2R||2R/4R| = p^{\mathrm{d}(R^+)} p^{\mathrm{d}((2R)^+)} \leq p^{2\,\mathrm{d}(R^+)}$, the result follows. ∎

3 Applications to p-group automorphisms

Note that we were motivated by the following result in introducing the class of p-nil rings.

Proposition 3.1. *Let G be a finite p-group, and let be $S = \mathrm{Z}(G) \cap \mathrm{P}(G)$. Then*
(a) the ring $\mathrm{Hom}(G, S)$ *is right p-nil;*
(b) $\Omega_n(\mathrm{Aut}_S(G)) = \Omega_{\{n\}}(\mathrm{Aut}_S(G)) = \mathrm{Aut}_{\Omega_n(S)}(G)$*;*
(c) the exponent of $\mathrm{Aut}_S(G)$ *is* $\leq p^{\min\{r,s\}}$*;*
(d) $\mathrm{Aut}_S(G)$ *is nilpotent of class at most* $\min\{r, s\}$*;*
(e) the rank of $\mathrm{Aut}_S(G)$ *is equal to* $\mathrm{d}(G)\,\mathrm{d}(S)$.

Proof. (a) Let be $k, h \in \mathrm{Hom}(G, S)$ such that $ph = 0$ ($4h = 0$ if $p = 2$). Hence $\mathrm{Im}(h)$ is an abelian group of exponent p (4 if $p = 2$), so its kernel contains $\mathrm{P}(G)$, and since $S \leq \mathrm{P}(G)$ we have $\mathrm{Im}(k) \subset \ker(h)$. It follows that h is a right annihilator of the ring $\mathrm{Hom}(G, S)$.
Observe that the additive group $\mathrm{Hom}(G, S) = \mathrm{Hom}(G/G', S)$ has exponent $\leq p^{\min\{r,s\}}$ and rank $\mathrm{d}(G)\,\mathrm{d}(S)$, now (b) and (c) follow from Theorem A, (d) follows from Theorem 2.2, and (e) follows from Theorem B. ∎

A slight modification of the proof of Proposition 3.1 (d) together with the remark that follows Theorem 2.2, yield a new proof of Theorem 4.8 in [8] which asserts the following.

Corollary 3.2. *If G is a finite p-group such that $\mathrm{Z}(G) \leq \Phi(G)$, then $\mathrm{Aut}_{\mathrm{Z}(G)}(G)$ is nilpotent of class at most $\min\{r,s\}$, where $\exp(G/G\prime) = p^r$ and $\exp(\mathrm{Z}(G)) = p^s$.*

It is interesting that Proposition 3.1 has a strong implication on the structure of $\mathrm{Aut}(G)$, where G is an abelian p-group. For instance if $p > 2$, we are speaking about the ring $\mathrm{Hom}(G, G^p)$ and about the automorphism group $\mathrm{Aut}_{G^p}(G)$. The quotient $\mathrm{Aut}(G)/\mathrm{Aut}_{G^p}(G)$ can be embedded as a subgroup of $\mathrm{GL}(d,p)$, with $d = \mathrm{d}(G)$. Thus $\mathrm{Aut}_{G^p}(G)$ has index at most $p^{\binom{d}{2}}$ in a p-sylow of $\mathrm{Aut}(G)$, that is a p-sylow of $\mathrm{Aut}(G)$ contains a large normal subgroup having a very regular structure.

Proof of Proposition D. We have $K = \mathrm{Aut}_{\mathrm{P}(G)}(G)$ is the adjoint group of the ring $\mathrm{Hom}(G, \mathrm{P}(G)) = \mathrm{Hom}(G, \mathrm{S}(G))$. Let P be a p-subgroup of $\mathrm{Aut}(G)$. We have $\mathrm{d}(P) \leq \mathrm{d}(P/P \cap K) + \mathrm{d}(P \cap K)$, since $P \cap K$ is a subgroup of K it follows from Proposition 3.1 (e) that $\mathrm{d}(P \cap K) \leq dd'$.
For p odd, $P/P \cap K \cong PK/K$ is a p-subgroup of $\mathrm{GL}(d,p)$, and since every p-subgroup of $\mathrm{GL}(d,p)$ can be generated by $d^2/4$ (see [16]), it follows that $\mathrm{d}(P/P \cap K) \leq d^2/4$. Therefore $\mathrm{d}(P) \leq dd' + d^2/4$.
For $p = 2$, $P/P \cap K$ can be embedded as a 2-subgroup of $\mathrm{Aut}(G/G^4)$, so we have only to show that the 2-part of $|\mathrm{Aut}(A)|$ is at most $2^{\frac{3d^2-d}{2}}$, for any abelian group A of rank d and exponent 4. Indeed, $\mathrm{Aut}(A)/\mathrm{Aut}_{A^2}(A)$ is a subgroup of $\mathrm{GL}(2,d)$, so the order of one of its 2-sylow is at most $2^{\frac{d^2-d}{2}}$. On the other hand $\mathrm{Aut}_{A^2}(A)$ is isomorphic to the adjoint group of $\mathrm{Hom}(A, A^2)$, which has order 2^{d^2}, the result follows. ∎

Proof of Corollary D. Let be P a p-subgroup of $\mathrm{Aut}(G)$, A a maximal abelian P-invariant subgroup of G, and $C = \mathrm{C}_P(A)$. It follows from the three subgroup lemma applied in $G \rtimes P$, that $[C, G, A] = 1$, thus $[C, G] \leq \mathrm{C}_G(A)$. It follows easily from the maximality of A that $\mathrm{C}_G(A) = A$, thus C acts trivially on A and G/A, so by Laue's relation it can be embedded in the additive group $\mathrm{Der}(G/A, A)$, which embeds in a direct sum of k copies of A. Thus $\mathrm{rk}(C) \leq k^2$. Now, as P/C embeds as a p-subgroup of $\mathrm{Aut}(A)$, the result follows at once from Proposition D. ∎

The remainder of the paper is devoted to proving Theorem C.

Lemma 3.3. *Let G be a finite p-group. Then $\mathrm{Z}(\mathrm{Aut}_{\mathrm{P}(G)}(G))$ has exponent at most $p^{min\{r,s\}}$.*

Proof. Let be $\mathrm{u} \in \mathrm{Z}(\mathrm{Aut}_{\mathrm{P}(G)}(G))$. Since $\mathrm{Aut}_{\mathrm{P}(G)}(G)$ contains $\mathrm{Inn}(G)$, we have u commutes with $\mathrm{Inn}(G)$, thus $x^{-1}\,\mathrm{u}(x) \in \mathrm{Z}(G)$ and so $x^{-1}\,\mathrm{u}(x) \in \mathrm{Z}(G) \cap \mathrm{P}(G)$, for all $x \in G$. It follows from Proposition 3.1 (c) that the order of u is at most $p^{min\{r,s\}}$. ∎

Note that one can replace $Z(\mathrm{Aut}_{P(G)}(G))$ in the above lemma by $Z(P)$, where P is p-sylow of $\mathrm{Aut}(G)$, for (at least) $p > 2$. Indeed, we claim that if $u \in Z(P)$ then $x^{-1}\,u(x) \in \Phi(G)$, for all $x \in G$. We have u is a p-automorphism that acts on the p-group $\Omega_1(Z(G) \cap \Phi(G))$, so it fixes at least a non-trivial element z in this group. Let M be a maximal subgroup of G, and let $r : G \to \mathbb{Z}_p$ be a homomorphism with kernel M. Consider the endomorphism $h(x) = z^{r(x)}$, for $x \in G$. Then $1 + h : x \mapsto x\,h(x)$ is an automorphism of G lying in $\mathrm{Aut}_{\Phi(G)}(G)$, so it lies in P. It follows that u commutes with h, thus $z^{r(x)} = z^{r(u(x))}$, so $x^{-1}\,u(x) \in M$, for all $x \in G$. This is true for any maximal subgroup M, and the claim follows.

In [15], H. Liebeck proved that the nilpotence class of $\mathrm{Aut}_{\Phi(G)}(G)$, where G is a finite p-group, can be bounded in terms of the class of G and $r_1(G)$ (as defined bellow). The following Lemma extends Liebeck's result. For a finite p-group G, $e(G)$ denotes the integer satisfying $p^{e(G)} = \exp(G)$.

Lemma 3.4. *Let G be a finite p-group of class c, let be $r_1 = r_1(G) = \sum_{i=1}^{c} e(\gamma_i/\gamma_{i+1})$ and $s_1 = s_1(G) = \sum_{i=1}^{c} e(Z_i/Z_{i-1})$. Then $\mathrm{Aut}_{\Phi(G)}(G)$ is nilpotent of class at most $\min\{r_1, s_1\} - 1$. In particular its class does not exceed $tc - 1$.*

Recall first that the lower p-central series of a group G is defined by $P_1(G) = G$ and by induction $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$, $i \geq 1$. And note that $P_2(G) = \Phi(G)$. The least integer n such that $P_{n+1}(G) = 1$ is the p-lower length of G, and any central series of G having factors of exponent p, has length at least n.

Proof. By ([6, Theorem VIII.1.7]), if an automorphism u of G acts trivially on $G/P_2(G)$, then it acts trivially on each section $P_{i+1}(G)/P_i(G)$. Thus $\mathrm{Aut}_{\Phi(G)}(G)$ is a stability group of the lower p-series. It follows from a well known result of Kaloujnine (see [5, Satz III.2.9]), that $\mathrm{Aut}_{\Phi(G)}(G)$ is nilpotent of class at most $n - 1$.
Now we have to connect the upper and the lower central series of G to the above series. Define the p-series of an abelian p-group A of exponent p^m by

$$1 < A^{p^{m-1}} < ... < A^p < A$$

This series has length m, and factors of exponent p. Using this definition one can refine each factor of the lower and the upper central series, by its p-series. We obtain two central series of G having factors of exponent p and their length are respectively equal to $r_1(G) = \sum_{i=1}^{c} e(\gamma_i/\gamma_{i+1})$ and $s_1(G) = \sum_{i=1}^{c} e(Z_i/Z_{i-1})$. As $n \leq \min\{r_1, s_1\}$, it follows that $\mathrm{Aut}_{\Phi(G)}(G)$ is nilpotent of class at most $\min\{r_1, s_1\} - 1$.
Finally, by a well known result $\exp(Z_i/Z_{i-1}) \leq \exp(Z(G))$ and $\exp(\gamma_i/\gamma_{i+1}) \leq \exp(G/\gamma_2)$, it follows that $r_1(G) \leq rc$ and $s_1(G) \leq sc$. Therefore $\mathrm{Aut}_{\Phi(G)}(G)$ is nilpotent of class at most $\min\{r, s\}c - 1 = tc - 1$. ∎

Proof of Theorem C. By Lemma 3.3, the exponent of the center of $\mathrm{Aut}_{P(G)}(G)$ is $\leq p^t$. It follows from Lemma 3.4 that the exponent of $\mathrm{Aut}_{P(G)}(G)$ is at most $(p^t)^{tc-1} = p^{t^2c-t}$.
Now let P be a p-sylow in $\mathrm{Aut}(G)$. As $P/\mathrm{Aut}_{P(G)}(G)$ embeds as p-subgroup of

$\mathrm{Aut}(G/\mathrm{P}(G))$, it follows from a result of Horosevskii (see [7, Corollary 3.3]) that the exponent of $P/\mathrm{Aut}_{\mathrm{P}(G)}(G)$ is bounded by p^{d-1} if $p > 2$ and by p^{2d-1} if $p = 2$. The result follows. ∎

Acknowledgments

We are very grateful to the referee for many useful comments and suggestions that improved the presentation of this paper.

References

[1] R. Baer and H. Heineken, Radical groups of finite abelian subgroup rank, *Illinois J. Math.* **16** (1972), 533-580.

[2] A. Caranti and S. Mattarei, Automorphisms of p-groups of maximal class, *Rend. Sem. Mat. Univ. Padova* **115** (2006), 189 -198.

[3] F. Catino and M. M. Miccoli, A note on IA-automorphisms of two-generated metabelian groups, *Rend. Sem. Mat. Univ. Padova* **96** (1996), 99 -104.

[4] O. Dickenschied, On the adjoint group of some radical rings, *Glasgow Math. J.* **39** (1997), 35-41.

[5] B. Huppert. Endliche Gruppen. I. *Die Grundlehren der Mathematischen Wissenschaften*, Band 134. Springer-Verlag, Berlin, 1967.

[6] B. Huppert and N. Blackburn, *Finite Groups II*, Springer-Verlag, Berlin, (1982).

[7] I. M. Isaacs, *Finite Group Theory*, Graduate studies in mathematics; v. **92**, (2008)

[8] M.H. Jafari and A.R. Jamali, On the nilpotency and solubility of the central automorphism group of finite group, *Algebra Coll.* **15**:3 (2006), 485-492.

[9] M. I. Kargapolov, On solvable groups of finite rank. (Russian). *Algebra i Logika*, **1**(5) (1962), 37-44.

[10] E.I. Khukhro, *p-Automorphisms of Finite p-Groups*, Cambridge University Press, (1998).

[11] R.L. Kruse and D.T. Price, *Nilpotent Rings*, Gordon and Breach, New York, (2010).

[12] H. Laue, On group automorphisms which centralize the factor group by an abelian normal subgroup, *J. Algebra.* **96** (1985), 532-547.

[13] C. R. Leedham-Green and S. McKay, The structure of groups of prime power order, London Math. Soc. Monogr., Oxford University Press, Oxford, 2002.

[14] J. C. Lennox and D. J. S. Robinson, *The Theory of Infinite Soluble Groups*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, Oxford, (2004).

[15] H. Liebeck, The automorphism group of finite p-groups, *J. Algebra.* **4** (1966), 426-432 (1966).

[16] A. R. Patterson, The minimal number of generators for p-subgroups of $GL(n, p)$, *J. Algebra* **32** (1974), 132140.

[17] K. Shoda, Über die Automorphismengruppe einer endlichen Abelschen Gruppe, *Math. Ann*. **100** (1928), 674-686.

[18] D. Segal and A. Shalev, Profinite groups with polynomial subgroup growth, *J. London Math*. Soc.(2) **55** (1997), 320-334.

Department of Mathematics,
Kasdi Merbah Ouargla University,
Ouargla, Algeria.
Email: yassine_guer@hotmail.fr

Department of Mathematics,
Setif University I, Algeria.
Email: boun_daoud@yahoo.com