ON CENTRAL AUTOMORPHISMS OF GROUPS AND NILPOTENT RINGS

YASSINE GUERBOUSSA AND BOUNABI DAOUD

Abstract. Let $G$ be a group. The central automorphism group $\text{Aut}_c(G)$ of $G$ is the centralizer of $\text{Inn}(G)$ the subgroup of $\text{Aut}(G)$ of inner automorphisms. There is a one to one map $\sigma \mapsto h_\sigma$ from the set $\text{Aut}_c(G)$ onto the set $\text{Hom}(G, Z(G))$ of homomorphisms from $G$ onto its center, with $h_\sigma(x) = x^{-1}\sigma(x)$. This map can be used to obtain informations about the size of $\text{Aut}_c(G)$, and also about its structure in some special cases. In this paper we see how to use it to obtain informations about the structure of $\text{Aut}_c(G)$ in the general case. The notion of the adjoint group of a ring is the main tool in our approach.

1. Introduction

It is very difficult to prove general theorems about the automorphisms of finite $p$-groups, and very little is known about them. An automorphism of a group $G$ is termed central if it commutes with every inner automorphism, clearly the central automorphisms of $G$ form a normal subgroup $\text{Aut}_c(G)$ of $\text{Aut}(G)$. If $G$ is a finite $p$-group, then $\text{Aut}_c(G)$ has a great importance in investigating $\text{Aut}(G)$, and it has been studied by several authors, see for instance ([2]-[5], and also [9], [10]).

It is easy to see that the map, or the Adney-Yen map for convenience, $\sigma \mapsto h_\sigma$ determines a one to one map from the set $\text{Aut}_c(G)$ onto the set $\text{Hom}(G, Z(G))$, where $h_\sigma(x) = x^{-1}\sigma(x)$. What are the informations that can be deduced about $\text{Aut}_c(G)$ from this relation? this is the main task of this paper.

Let $R$ be a (associative) ring. Under the circle composition $x \odot y = x + y + xy$, the set of all elements of $R$ forms a monoid with identity element $0 \in R$, this monoid is called the adjoint monoid or semigroup of the ring $R$. The adjoint group $R^\circ$ of $R$ is the group of invertible elements in this monoid.

Let consider the set $\text{Hom}(G, Z(G))$ as a ring, the addition is defined in the usual way and we take the composition of maps as a multiplication. Our main observation is that the Adney-Yen map defines an isomorphism between $\text{Aut}_c(G)$ and the adjoint group of the ring $\text{Hom}(G, Z(G))$.

When the ring $R$ has an identity $1$, the mapping $x \mapsto 1 + x$ determines a group isomorphism from $R^\circ$ to the multiplicative group of the ring $R$. This agrees with the usual case when $G$ is abelian : the central automorphism group coincides with $\text{Aut}(G)$ which is the multiplicative group of the ring $\text{End}(G)$.

Assume that $G$ is finite. It was proved in [2] that the Adney-Yen map is a bijection if $G$ does not have a non-trivial abelian direct factor. In the light of our observation, this is equivalent to saying that $\text{Hom}(G, Z(G))$ is a radical ring. Following Jacobson, a ring $R$ is termed radical if its adjoint semigroup is a group, or equivalently $R^\circ = R$. Adjoint groups of radical rings are interesting objects.
to study and we may find a considerable number of papers in the subject (see [6] for some references).

The above results and some of its consequences are discussed in Section 2 in a more general context. And since we are mainly interested to finite p-groups, the remaining sections are devoted to their central automorphisms, in Section 3 we introduce the notion of a p-nil ring in order to studying the structure of $\text{Aut}_c(G)$ when $G$ is a finite p-group with $Z(G) \leq \Phi(G)$. The results of this section are applied in Section 4 to the longstanding problem of whether every non-abelian finite p-group has a non-inner automorphism of order $p$ (see [1]), we give a necessary and a sufficient condition for a finite p-groups to have a non-inner central automorphism of order $p > 2$.

Throughout, the unexplained notation is standard in the literature. We denote by $\text{Hom}(G, N)$ the group of homomorphisms from $G$ to an abelian group $N$. We denote by $d(G)$ the minimal number of generators of $G$, and the rank $r(G)$ of $G$ is defined to be $\sup\{d(H), H \leq G\}$. The exponent of $G$ is denoted by $\exp(G)$ and $\mathbb{Z}_n$ denotes the ring of integers modulo $n$.

**Lemma 1.1.** If $M$ and $N$ are finite abelian p-groups, then the rank and the exponent of the abelian group $\text{Hom}(M, N)$ are equal respectively to $r(M).r(N)$ and $\min\{\exp(M), \exp(N)\}$.

**Proof.** This follows immediately from the properties

$$\text{Hom}(\prod_i M_i, \prod_j N_j) \cong \prod_{i,j} \text{Hom}(M_i, N_j)$$

where $M_i$ and $N_j$ are abelian groups, and

$$\text{Hom}(\mathbb{Z}_{p^n}, \mathbb{Z}_{p^n}) \cong \mathbb{Z}_{p^{\min\{n,m\}}}.$$

\[\square\]

Given an associative ring $R$, we denote by $R^+$ the additive group of $R$. The $n$th power $R^n$ of $R$ is the additive group generated by all the products of $n$ elements of $R$. We say that $R$ is nilpotent if $R^{n+1} = 0$ for some non-negative integer $n$, the least integer $n$ satisfying $R^{n+1} = 0$ is called the class of nilpotency of the ring $R$. Note that every nilpotent ring $R$ is radical since for every $x \in R$ we have

$$x \circ \sum_i (-1)^i x^i = (\sum_i (-1)^i x^i) \circ x = 0.$$

The Jacobson radical of the ring $R$ is the largest ideal of $R$ contained in the adjoint group $R^\circ$. This implies that $R$ is radical if and only if it coincides with its Jacobson radical. By a classical result the Jacobson radical of an artinian ring is nilpotent, so every artinian (in particular finite) radical ring is nilpotent.

The following lemma is standard in the literature (see [8], Section I.6).

**Lemma 1.2.** The adjoint group of a nilpotent ring $R$ is nilpotent of class at most equals to the nilpotency class of $R$.

**Proof.** The series of ideals

$$R \supset R^2 \supset ... \supset R^{n+1} = 0$$

induces a central series in the adjoint group of the ring $R$. \[\square\]
The following lemma is a variant of theorem B in [6], it gives a bound for the rank of the adjoint group of a finite (periodic in general) radical ring \( R \) in term of the rank of its additive group.

**Lemma 1.3.** Let \( R \) be a finite radical ring. Then \( r(R^0) \leq 3r(R^+) \), and if the order of \( R \) is odd then \( r(R^0) \leq 2r(R^+) \).

2. Central automorphisms and radical rings

We begin with the following general remark. Every abelian normal subgroup \( A \) of a group \( G \) can be viewed as a \( G \)-module via conjugation \( a^x = x^{-1}ax \), with \( x \in G \) and \( a \in A \). A derivation of \( G \) into \( A \) is a mapping \( \delta : G \to A \) such that \( \delta(xy) = \delta(x)\delta(y) \). The set \( \text{Der}(G,A) \) of these derivations is a ring under the addition \( \delta_1 + \delta_2(x) = \delta_1(x)\delta_2(x) \) and the multiplication \( \delta_1\delta_2(x) = \delta_2(\delta_1(x)) \), with \( \delta_1, \delta_2 \in \text{Der}(G,A) \) and \( x \in G \). Let denote by \( \text{End}_A(G) \) the set of endomorphisms \( u \) of \( G \) having the property \( x^{-1}u(x) \in A \), for all \( x \in G \). We check easily that \( \text{End}_A(G) \) is a submonoid of \( \text{End}(G) \) and every endomorphism \( u \in \text{End}_A(G) \) defines a derivation \( \delta_u(x) = x^{-1}u(x) \) of \( G \) into \( A \). Note also that to each derivation \( \delta \in \text{Der}(G,A) \) we can associate an endomorphism \( u \in \text{End}_A(G) \) with \( u(x) = x\delta(x) \).

**Lemma 2.1.** Under the above notation, the mapping \( u \mapsto \delta_u \) is an isomorphism between the monoid \( \text{End}_A(G) \) and the adjoint monoid of the ring \( \text{Der}(G,A) \). In particular it induces an isomorphism between the corresponding groups of invertible elements.

**Proof.** Straightforward verification. \( \square \)

Since the center \( Z(G) \) is a trivial \( G \)-module, we have \( \text{Der}(G,Z(G)) = \text{Hom}(G,Z(G)) \). So for \( A = Z(G) \) the mapping defined above reduces to the Adney-Yen map. It follows that

**Proposition 2.2.** The Adney-Yen map determines an isomorphism between the central automorphism group \( \text{Aut}_c(G) \) and the adjoint group of the ring \( \text{Hom}(G,Z(G)) \).

Assume that \( G \) is finite. In [2] Adney and Yen have proved that every endomorphism in \( \text{End}_Z(G)(G) \) is an automorphism if and only if \( G \) is purely non-abelian, that is \( G \) does not have a non-trivial abelian direct factor. The above observation allows us to set this result under the form

**Theorem 2.3.** (Adney-Yen) Let \( G \) be a finite group. Then the ring \( \text{Hom}(G,Z(G)) \) is radical if and only if \( G \) is purely non-abelian.

The above theorem can be generalized to arbitrary finite rings as follows.

**Theorem 2.4.** Let \( R \) be a finite ring. Then \( R \) is radical if and only if \( 0 \) is the only idempotent in \( R \).

Let be \( R = \text{Hom}(G,Z(G)) \). We have \( R \) is non-radical if and only if there exists a non-zero idempotent homomorphism \( e : G \to Z(G) \), and clearly this is equivalent to the existence of a non-trivial abelian direct factor of \( G \).

The proof of Theorem 2.4 is based on the following result.

**Lemma 2.5.** Let \( x \) be an element of a semigroup \( S \) such that \( x^n = x^m \) for some positive integers \( n \neq m \). Then the set \( \{x^k \in S, k > 0\} \) contains an idempotent.
Proof. For every $n > 0$, let $[n] = \{ k > 0, x^k = x^n \}$.
Assume that $n < \min[2n]$, for all $n > 0$. There exist by assumption $n < m$ such that $x^n = x^m$, so the class $[n]$ is unbounded since $n + k(m - n) \in [n]$, for all $k > 0$. On the other hand if $l \in [n]$, then $2n \in [2l]$, and so $l < 2n$, a contradiction.
Hence, there exists $n$ such that $n_0 = \min[2n] \leq n$. If $n_0 = n$, then $x^n$ is an idempotent element of $S$. And if $n_0 < n$, then $x^{2n-n_0}$ is an idempotent, since
$$(x^{2n-n_0})^2 = x^{4n-2n_0} = x^{2n}x^{2n-2n_0} = x^{n_0}x^{2n-2n_0} = x^{2n-n_0}.$$
The result follows. \qed

Proof of Theorem 2.4. Suppose that $R$ is not radical. Since $R^o$ contains every nilpotent element, then $R$ contains a non-nilpotent element $x$. And since $R$ is finite, the set of all the powers of $x$ can not be infinite. Hence there exist $n \neq m$ such that $x^n = x^m$. The existence of a non-zero idempotent element follows now from Lemma 2.5.
Conversely, if $x \neq 0$ is an idempotent of $R$, then $-x \notin R^o$. Otherwise there exists an element $y \in R$ such that $-x + y - xy = 0$, if we multiply this equation by $x$ on the left we obtain $-x = 0$, which is not the case. Hence $R^o \neq R$, and so $R$ is not radical. The result follows. \qed

As an immediate consequence of Theorem 2.3, we have

Corollary 2.6. If $G$ is a purely non-abelian finite group, then the ring $\text{Hom}(G, Z(G))$ is nilpotent. In particular, every homomorphism $h : G \to Z(G)$ is nilpotent.

The following corollary is well-known in the literature (see [9]).

Corollary 2.7. The central automorphism group of a purely non-abelian finite group is nilpotent.

We can also bound the rank of $\text{Aut}_c(G)$ using Lemma 1.3.

Corollary 2.8. Let $G$ be a purely non-Abelian finite group. Then $r(\text{Aut}_c(G)) \leq 3r(R^+)$, where $R$ denotes the ring $\text{Hom}(G, Z(G))$. The bound 3 can be replaced by 2 if the order of $Z(G)$ is odd. In particular if $G$ is a $p$-group then, $r(\text{Aut}_c(G)) \leq 2d(G)d(Z(G))$ for $p > 2$, and $r(\text{Aut}_c(G)) \leq 3d(G)d(Z(G))$ for $p = 2$.

Proof. The first part follows from Lemma 1.3. For the second observe that every homomorphism $h : G \to Z(G)$ can be factorized on $Gt$, this induces an isomorphism between the two groups $\text{Hom}(G, Z(G))$ and $\text{Hom}(G/Gt, Z(G))$. The result follows now from Lemma 1.1. \qed

3. Adjoint groups of $p$-nil rings

In this section we investigate more closely the structure of $\text{Aut}_c(G)$ when $G$ is a finite $p$-group with $Z(G) \leq \Phi(G)$. This situation motivates the introduction of the following notions.

Definition 3.1. Let $p$ be a prime number and $R$ be a ring. We say that $R$ is left (right, resp) $p$-nil if every element $x$ of order $p$ in $R^+$ is a left (right, resp) annihilator of $R$, that is $px = 0$ implies $xy = 0$ ($yx = 0$, resp), for all $y \in R$. The ring $R$ is said to be $p$-nil if it is left and right $p$-nil.
For instance, the subring $S = pR$ of any ring $R$ is $p$-nil. Also we check easily that the left and the right annihilators of $\Omega_1(R^+)$ are respectively right and left $p$-nil.

The following theorems shed some lights on the structure of the adjoint groups of these rings.

**Theorem 3.2.** Let $R$ be a ring with an additive group of finite exponent $p^n$. If $R$ is left or right $p$-nil, then $R$ is nilpotent of class at most $m$. In particular the adjoint group $R^\circ$ is nilpotent of class at most $m$.

*Proof.* Assume that $R$ is left $p$-nil. We proceed by induction on $n$ to prove that $p^{n-1}x = 0$. This is obvious for $n = 1$. Now if $x \in R^n$, then by induction $p^{n-1}x = 0$. It follows that $p^n - x$ has order 1 or $p$, therefore $(p^n - x)y = p^n - (xy) = 0$, for all $y \in R$. This shows that $p^n - R^{n+1} = 0$. Now, for $n = m + 1$ we have $R^{m+1} = 0$, this prove 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 Lemma 1.2.

**Lemma 3.3.** 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 $n \geq 1$, where $\Omega_n(R)$ denotes the ideal $\{x \in R, p^n x = 0\}$.

*Proof.* Assume that $R$ is left $p$-nil, and let be $\overline{x} \in R/\Omega_n(R)$ such that $p\overline{x} = \overline{0}$. Then $px \in \Omega_n(R)$, so $p^n x \in \Omega_1(R)$, and by assumption $(p^n x)y = p^n(xy) = 0$, for all $y \in R$. This shows that $xy \in \Omega_n(R)$, for all $y \in R$, that is $\overline{x}$ is a left annihilator of $R/\Omega_n(R)$. The result follows for $R$ right $p$-nil by a similar argument.

**Theorem 3.4.** Let $R$ be a $p$-ring, $p$ odd. 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 $\Omega_n(R^\circ) = \Omega_n(R)$. 

*Proof.* We denote by $x^{(k)}$ the $k$th power of $x$ in the adjoint group of $R$.

For $n = 1$ we have, if $px = 0$ then $x^i = 0$ 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 additive order of $x$. If $m \geq 2$, then $p^{m-1}x$ has order $p$, hence $p^{m-1}x^2 = 0$, and similarly we obtain $p^{m-2}x^i = 0$, 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 $x \in \Omega_1(R)$.

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 3.3 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 $R^\circ$ and $\Omega_n(R^\circ)$ is generated by $\Omega_{\{n\}}(R^\circ)$. 

\qed
Corollary 3.5. Let $R$ be a $p$-ring, $p$ odd. If $R$ is $p$-nil, then $\Omega_1(R^c) \leq Z(R^c)$, in other word $R^c$ is $p$-central.

Proof. Every element $x$ of $\Omega_1(R^c)$ lies $\Omega_1(R)$ by the above theorem. Hence $x$ is an annihilator of $R$, and so it lies in the center of $R^c$. \qed

Note that this can be used to prove Lemma 1.3 among the same lines of Dickenschied proof ([6]), only we use the fact that the group $(pR)^c$ is $p$-central instead of being powerful (a finite $p$-group $G$ is powerful if $G/G^p (G/G^4$, for $p = 2$) is abelian), and the fact that the rank of a $p$-central finite $p$-group $G$ is bounded by $d(Z(G))$ by a result of Thompson (see [7, III, Hilfssatz 12.2]). It seems that this alternative proof is simpler, since it is easier to prove that $(pR)^c$ is $p$-central than proving that is powerful, but unfortunately this proof does not deal with the prime $p = 2$.

In connection with central automorphisms we have

Proposition 3.6. If $G$ is a finite $p$-group such that $Z(G) \leq \Phi(G)$, then the ring $\text{Hom}(G, Z(G))$ is right $p$-nil.

Proof. Let be $k, h \in \text{Hom}(G, Z(G))$ such that $ph = 0$. Then $h : G \to \Omega_1(Z(G))$. Since the image of $h$ is an elementary abelian $p$-group, its kernel contains the frattini subgroup, and since $Z(G) \leq \Phi(G)$ we have $kh(x) = h(k(x)) = 1$, for all $x \in G$. It follows that $h$ is a right annihilator of the ring $\text{Hom}(G, Z(G))$. \qed

The above proposition leads to a new proof of Theorem 4.8 in [9].

Corollary 3.7. If $G$ is a finite $p$-group such that $Z(G) \leq \Phi(G)$, then $\text{Aut}_c(G)$ is nilpotent of class at most $\min\{r, s\}$, where $\exp(G/G^r) = p^r$ and $\exp(Z(G)) = p^s$.

Proof. By Theorem 3.2 the nilpotency class of $\text{Aut}_c(G)$ does not exceed $m$, where $p^m$ is the exponent of $\text{Hom}(G, Z(G)) \cong \text{Hom}(G/G^r, Z(G))$ which is equal to $p^{\min\{r,s\}}$ by Lemma 1.1. \qed

Theorem 3.8. If $G$ is a finite $p$-group with $p$ odd, such that $Z(G) \leq \Phi(G)$, then

$$\Omega_n(\text{Aut}_c(G)) = \Omega_{\{n\}}(\text{Aut}_c(G)) = \text{Aut}_{Z_n}(G)$$

where $Z_n$ denotes the subgroup $\Omega_n(Z(G))$.

Proof. This is an immediate consequence of Theorem 3.4 and Proposition 3.6. \qed

4. Non-inner central automorphisms of order $p$.

A longstanding conjecture asserts that every non-abelian finite $p$-group has a non-inner automorphism of order $p$. More informations about this conjecture can be found for instance in [1].

First, note that we can reduce it to indecomposable $p$-groups.

Proposition 4.1. Let $G$ be a non-abelian finite $p$-group. If $G$ is decomposable then $G$ has a non-inner central automorphism of order $p$. 
Proof. Assume that $G$ is a direct product of $G_1$ and $G_2$, where $G_1$, $G_2$ are non-trivial normal subgroups of $G$. Let $M$ be a maximal subgroup of $G_1$ and $g \in G_1 - M$, clearly every element of $G$ can be written in the form $xg^i$, where $x \in MG_2$. If $z$ is a central element of order $p$ in $G_2$, then the mapping $xg^i \mapsto xg^iz^i$ is a central automorphism of $G$ of order $p$ which is not inner since it maps $g \in G_1$ to $gz \notin G_1$. □

For $p$ odd, the results of the previous section allows us to characterize the $p$-groups in which every central automorphism of order $p$ is inner. Let denote $d = d(G)$, $d_1 = d(Z(G))$ and $d_2 = d(Z(I\!n(G)))$.

**Theorem 4.2.** Let $G$ be a finite non-abelian $p$-group, $p$ odd. In order for $G$ to have a non-inner central automorphism of order $p$ it is necessary and sufficient that $d_2 \neq d \cdot d_1$.

For instance, the $p$-groups of maximal class satisfy this condition, as well as the class of non-abelian finite $p$-central $p$-groups, this follows easily from [7, III, Hilfssatz 12.2]. We need the following two lemmas to prove Theorem 4.2.

**Lemma 4.3.** If $G$ is a purely non-abelian finite $p$-group, then $\Omega_1(Z(G)) \leq \Phi(G)$. In particular if $exp(Z(G)) = p$ then $Z(G) \leq \Phi(G)$.

**Proof.** Let $z \in \Omega_1(Z(G))$. If there exists a maximal subgroup $M$ such that $z \notin M$, then $G \cong z \times M$. Thus $G$ is not purely non-abelian. This is another proof based on the nilpotency of the ring $Hom(G,Z(G))$. Let be $z \in \Omega_1(Z(G))$. To each homomorphism $r : G \to \mathbb{Z}_p$ we can associate an endomorphism $h \in Hom(G,Z(G))$ by setting $h(x) = r(x)z$, for all $x \in G$. This implies that $h^n(z) = r(z)^n z$. By corollary 2.6, $h$ is nilpotent, so there exists an integer $n$ such that $r(z)^n = 0$. Therefore $r(z) = 0$, since $\mathbb{Z}_p$ is a field. This shows that $z$ lies in the intersection of the set of all kernels of homomorphisms from $G$ to $\mathbb{Z}_p$. Since every maximal subgroup of $G$ occurs as a kernel of some homomorphism $r : G \to \mathbb{Z}_p$. It follows that $z \in \Phi(G)$. □

**Lemma 4.4.** Let $G$ be a finite $p$-group. Then every inner automorphism which is central of order $p$ is induced by some non-trivial homomorphism $h : G \to \Omega_1(Z(G))$. Moreover, if $G$ is purely non-abelian then for every non-trivial homomorphism $h : G \to \Omega_1(Z(G))$, the order of the central automorphism $\sigma = 1_G + h$ induced by $h$ is equal to $p$.

**Proof.** Let be $\tau$ an inner central automorphism of order $p$. We can write $\tau = 1_G + h$, for some $h \in Hom(G,Z(G))$, and $1_G$ denotes the identity map of $G$. We have $h = h\tau = h + h^2$, and so $h^2 = 0$. This implies that $1_G = \tau^p = 1_G + ph$, and so $ph = 0$. Therefore $h : G \to \Omega_1(Z(G))$.

Assume that $G$ is purely non-abelian. Since the kernel of every homomorphism $h : G \to \Omega_1(Z(G))$ contains $\Phi(G)$, Lemma 4.3 implies that $h^2 = 0$. Therefore, if $\sigma = 1_G + h$ then $\sigma^p = 1_G + \sum_{i=1}^{p} (\binom{p}{i})h^i = 1_G + ph = 1_G$. The result follows. □

**Proof of Theorem 4.2.** Suppose that $G$ has a non-inner central automorphism $\sigma = 1_G + h_\sigma$ of order $p$. Let $I$ be the image of $\Omega_1(Z(i\!n(G)))$ by the Adney-Yen map. By Lemma 4.4 $I$ is a subspace of the $\mathbb{Z}_p$-vector space $Hom(G,\Omega_1(Z(G)))$ of dimension $d_2$. If $d_2 = d \cdot d_1$, then $I = Hom(G,\Omega_1(Z(G)))$. If $Z(G) \notin \Phi(G)$ then we can find an element $g \in Z(G) - M$ for some maximal subgroup $M$ of $G$. Consider a non-trivial element $z \in \Omega_1(Z(G)) \cap M$ and let $h(x) = z^{r(x)}$, where $r : G \to \mathbb{Z}_p$ is the
homomorphism defined by \( r(mg^i) = i \mod p, m \in M \). Clearly, \( h \in I \) and \( 1_G + h \) is not inner, since it maps \( g \) to \( gz \), a contradiction. It follows that \( Z(G) \leq \Phi(G) \). Theorem 3.8 implies that \( ph_\sigma = 0 \), that is \( h_\sigma \in I \). It follows that \( \sigma = 1_G + h_\sigma \) is inner, a contradiction. Therefore \( Z(G) \leq \Phi(G) \). Theorem 3.8 implies that \( ph_\sigma = 0 \), that is \( h_\sigma \in I \). It follows that \( \sigma = 1_G + h_\sigma \) is inner, a contradiction. Therefore \( d_2 \neq d \cdot d_1 \).

Conversely, by Proposition 4.1 we may suppose that \( G \) is purely non-abelian. If \( d_2 \neq d \cdot d_1 \), then \( I \) is a proper subspace of \( \text{Hom}(G, \Omega_1(Z(G))) \). Hence there exists \( h : G \to \Omega_1(Z(G)) \) such that the automorphism \( \sigma = 1_G + h \) is not inner. It follows from Lemma 4.4 that \( \sigma \) has order \( p \). □

Let \( G \) be a finite non-abelian \( p \)-group of order \( p^n \) and class \( c \). Under the above notation, does the equality \( d_2 = d \cdot d_1 \) imply that \( G \) has a cyclic center?.

Assume that \( G \) is a counter example to this question, by a formula of Abdollahi [1, Theorem 2.5] we have \( d_1 \cdot (d + 1) \leq r + 1 \), where \( r = n - c \) is the coclass of \( G \). The class of \( G \) must be \( \geq 3 \), otherwise we would have \( d_2 = d(G/Z(G)) \leq d_1 \) which is not the case. On the other hand \( d \geq 2 \), hence \( 3d_1 \leq r + 1 \), so we must have \( r + 1 \geq 6 \), thus \( n \geq 5 + c \geq 8 \).

This shows that if a counter example to the above question exists then it has at least coclass 5 and order \( p^8 \). It is well-known that in a powerful \( p \)-group \( G \), every subgroup can be generated by \( d(G) \) elements, so a counter example to our question can not be a powerful \( p \)-group.

Acknowledgment. The first author is grateful to Miloud Reguiat for his encouragement, and his comments about early drafts of this paper.

References

[1] A. Abdollahi, Powerful \( p \)-groups have non-inner automorphisms of order \( p \) and some cohomology, J. Algebra. 323 (2010), 779-789.

[2] A. Abdollahi, Powerful \( p \)-groups have non-inner automorphisms of order \( p \) and some cohomology, J. Algebra. 323 (2010), 779-789.

[3] J.E. Adney and T. Yen, Automorphisms of a \( p \)-group, Illinois J. Math. 9 (1965), 137-143.

[4] M.S. Attar, Finite \( p \)-groups in which each central automorphism fixes centre elementwise, Comm. Algebra. 40 (2012), 1096-1102.

[5] M.J. Curran, Finite groups with central automorphism group of minimal order, Math. Proc. Royal Irish Acad. 104 A(2) (2004), 223-229.

[6] M.J. Curran and D.J. McCaughan, Central automorphisms that are almost inner, Comm. Algebra. 29 (5) (2001), 2081-2087.

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

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

[9] R.L. Kruse and D.T. Price, Nilpotent rings, Gordon and Breach, New York (2010).

[10] 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.

[11] M.K. Yadav, On central automorphisms fixing the center element-wise, Comm. Algebra. 37 (2009), 4325-4331.

Yassine Guerboussa
Department of Mathematics, University Kasdi Merbah Ouargla, Ouargla, Algeria

Email: yassine_guer@hotmail.fr
Bounabi Daoud
Department of Mathematics, University of Setif, Setif, Algeria
Email: boun_daoud@yahoo.com