Bull. Aust. Math. Soc. **92** (2015), 390–396
doi:10.1017/S0004972715000489

ON THE CENTRE OF THE AUTOMORPHISM GROUP OF A GROUP

M. FARROKHI D. G.✉ and MOHAMMAD REZA R. MOGHADDAM

(Received 27 February 2015; accepted 7 March 2015; first published online 16 June 2015)

Abstract

If the centre of a group G is trivial, then so is the centre of its automorphism group. We study the structure of the centre of the automorphism group of a group G when the centre of G is a cyclic group. In particular, it is shown that the exponent of $Z(\mathrm{Aut}(G))$ is less than or equal to the exponent of $Z(G)$ in this case.

2010 *Mathematics subject classification*: primary 20F28; secondary 11A07.

Keywords and phrases: automorphism group, centre, p-group, primitive root.

1. Introduction

Let G be a group and $\mathrm{Aut}(G)$ be the group of automorphisms of G. A routine exercise in group theory states that $Z(\mathrm{Aut}(G))$ is trivial whenever $Z(G)$ is trivial. This result, correlating the centre of G and $\mathrm{Aut}(G)$, was recently extended to a wider class of invariants by Deaconescu and Walls [2]. Indeed, they showed that if X is any group invariant satisfying the two properties:

(i) $Z(G) \leq X(G)$; and
(ii) $X(G) \cap H \leq X(H)$ for all subgroups H of G,

then $X(G) = 1$ implies that $X(\mathrm{Aut}(G)) = 1$. However, not much is known about the structure of $Z(\mathrm{Aut}(G))$ when $Z(G)$ is not trivial. The only result we are aware of is that of Formanek [3], which shows that $Z(\mathrm{Aut}(G))$ is nontrivial for a free nilpotent group G of rank r and class $c \geq 2$ if and only if $c \equiv 1 \pmod{2r}$.

The aim of this paper is to obtain the structure of $Z(\mathrm{Aut}(G))$ when the centre of G is a cyclic group. As a result, in Lemma 2.3, it is shown that the exponent of $Z(\mathrm{Aut}(G))$ is bounded above by the exponent of $Z(G)$ provided that $Z(G)$ is a cyclic group. We note that the order of $Z(\mathrm{Aut}(G))$ may be greater than the order of $Z(G)$ when $Z(G)$ is a cyclic group. Our main theorems are as follows.

THEOREM 1.1. *Let G be a group with cyclic centre of finite order $n = p_1^{a_1} \cdots p_m^{a_m}$, where $p_1, \ldots, p_m$ are distinct primes. Then $Z(\mathrm{Aut}(G)) \cong A_1 \times \cdots \times A_m$, where, for $i = 1, 2, \ldots, m$, the subgroup A_i is isomorphic with one of the following:*

(a) *the trivial group;*

(b) *an abelian p_i-group whose exponent divides $p_i^{a_i}$; or*

(c) *a cyclic group of order $p_i^{a_i-1}(p_i-1)$.*

THEOREM 1.2. *Let G be a group with infinite cyclic centre. Then $Z(\mathrm{Aut}(G))$ is isomorphic with one of the following:*

(a) *the trivial group;*

(b) *a cyclic group of order two; or*

(c) *a nontrivial torsion-free abelian group.*

2. Preliminaries

Let G be an arbitrary group and let $\theta \in Z(\mathrm{Aut}(G))$. Then $g^{-1}\theta(g) \in Z(G)$ for all $g \in G$ and the map $\overline{\theta} : G \longrightarrow Z(G)$ given by $\overline{\theta}(g) = g^{-1}\theta(g)$ is a homomorphism (see [1]).

Now assume that $Z(G) = \langle z \rangle$ is a cyclic group of order n. Then $\overline{\theta}(z) = z^{\alpha}$ for some integer α. For all $g \in G$,

$$\overline{\theta}^2(g) = \overline{\theta}(z^k) = z^{k\alpha} = \overline{\theta}(g)^{\alpha}, \tag{2.1}$$

where $\overline{\theta}(g) = z^k$. Using (2.1) and an induction argument,

$$\overline{\theta}^i(g) = \overline{\theta}(g)^{\alpha^{i-1}} \tag{2.2}$$

for all $i \geq 1$. Also, since $\theta(g) = g\overline{\theta}(g)$, we obtain the following equality:

$$\theta^k(g) = g^{\binom{k}{0}}\overline{\theta}(g)^{\binom{k}{1}} \cdots \overline{\theta}^k(g)^{\binom{k}{k}}, \tag{2.3}$$

by using induction on k for all $k \geq 1$.

It is easy to see that $|\theta| = \exp(\mathrm{Im}\,\overline{\theta})$ when $\alpha = 0$. Now assume that $\alpha \neq 0$. Then, by using (2.2) and (2.3),

$$\theta^k(g) = g\overline{\theta}(g)^{(1/\alpha)((1+\alpha)^k-1)} \tag{2.4}$$

for all $g \in G$ and $k \geq 1$. Note that in (2.4), the number α depends on the automorphism θ, and so in what follows we indicate this dependence by denoting it by α_θ. Now, by using the definition of α_θ, we prove the following lemmas, which play an important role in determining the structure of $Z(\mathrm{Aut}(G))$. In what follows, $U(\mathbb{Z}_n)$ denotes the multiplicative group of units of $\mathbb{Z}_n$, the ring of integers modulo n.

LEMMA 2.1. *Let G be a group with cyclic centre of finite order n. Then, for all $\varphi, \psi \in Z(\mathrm{Aut}(G))$:*

(a) $\alpha_{\varphi\psi} + 1 \equiv (\alpha_\varphi + 1)(\alpha_\psi + 1) \pmod n$*; and*

(b) *the map $\alpha^* : Z(\mathrm{Aut}(G)) \longrightarrow \mathrm{Aut}(Z(G)) \cong U(\mathbb{Z}_n)$ given by $\alpha^*(\varphi) = \alpha_\varphi + 1$ is a homomorphism, where $\alpha_\varphi + 1$ is identified with the automorphism which sends z to $z^{\alpha_\varphi+1}$.*

https://doi.org/10.1017/S0004972715000489 Published online by Cambridge University Press

Proof. For any $\varphi, \psi \in Z(\mathrm{Aut}(G))$ and $g \in G$,

$$\varphi\psi(g) = \varphi(\psi(g)) = \varphi(g\overline{\psi}(g)) = \varphi(g)\varphi(\overline{\psi}(g)) = g\overline{\varphi}(g)\overline{\psi}(g)\overline{\varphi}\overline{\psi}(g).$$

Thus, $\overline{\varphi\psi} = \overline{\varphi} \cdot \overline{\psi} \cdot \overline{\varphi}\overline{\psi}$, which implies that

$$\overline{\varphi\psi}(z) = \overline{\varphi}(z)\overline{\psi}(z)\overline{\varphi}\overline{\psi}(z) = z^{\alpha_\varphi} z^{\alpha_\psi} \overline{\varphi}(z^{\alpha_\psi}) = z^{\alpha_\varphi} z^{\alpha_\psi} z^{\alpha_\varphi \alpha_\psi} = z^{\alpha_\varphi + \alpha_\psi + \alpha_\varphi \alpha_\psi}.$$

Hence, $\alpha_{\varphi\psi} \equiv \alpha_\varphi + \alpha_\psi + \alpha_\varphi\alpha_\psi \pmod n$ or $\alpha_{\varphi\psi} + 1 \equiv (\alpha_\varphi + 1)(\alpha_\psi + 1) \pmod n$, which proves part (a).

To prove part (b), it is enough to show that $(\alpha_\varphi + 1, n) = 1$, that is, $\alpha_\varphi + 1 \in U(\mathbb{Z}_n)$ for all $\varphi \in Z(\mathrm{Aut}(G))$. Assume the contrary. Then there exists $\varphi \in Z(\mathrm{Aut}(G))$ such that $(\alpha_\varphi + 1, n) \neq 1$ and hence

$$|z| = |\varphi(z)| = |z\overline{\varphi}(z)| = |z^{\alpha_\varphi + 1}| < |z|,$$

which is a contradiction. □

The result for groups with infinite cyclic centre is proved by similar means, so we omit the proof.

Lemma 2.2. *Let G be a group with infinite cyclic centre. Then, for all $\varphi, \psi \in Z(\mathrm{Aut}(G))$:*

(a) $\alpha_{\varphi\psi} + 1 \equiv (\alpha_\varphi + 1)(\alpha_\psi + 1) \pmod 2$*; and*

(b) *the map $\alpha^* : Z(\mathrm{Aut}(G)) \longrightarrow \mathrm{Aut}(Z(G)) \cong C_2$ given by $\alpha^*(\varphi) = \alpha_\varphi + 1$ is a homomorphism, where $\alpha_\varphi + 1$ is identified with the automorphism which sends z to $z^{\alpha_\varphi + 1}$. (C_2 in this context is the multiplicative group with elements 1 and -1.)*

Lemma 2.3. *Let G be a group with cyclic centre of order $n = p_1^{a_1} \cdots p_m^{a_m}$ and let $\varphi \in Z(\mathrm{Aut}(G))$. Then*

$$|\varphi| \,\big|\, \mathrm{lcm}(d_1, \ldots, d_m),$$

where $d_i = p_i^{a_i}$ when $p_i \mid \alpha_\varphi$ and $d_i = p_i^{a_i - 1}(p_i - 1)$ when $p_i \nmid \alpha_\varphi$. In particular, $\exp(Z(\mathrm{Aut}(G)) \leq \exp(Z(G))$.

Proof. Let $\varphi \in Z(\mathrm{Aut}(G))$ and $g \in G$. If $\alpha_\varphi = 0$, then $|\varphi| = \exp(\mathrm{Im}\,\overline{\varphi})$ and the result holds. Now suppose that $\alpha_\varphi \neq 0$. Then, by (2.4),

$$\varphi^k(g) = g\overline{\varphi}(g)^{(1/\alpha_\varphi)((1+\alpha_\varphi)^k - 1)}$$

for all $k = 1, \ldots, m$. Two cases occur, namely either $p_i \mid \alpha_\varphi$ or $p_i \nmid \alpha_\varphi$. In the first case, $\alpha_\varphi = p_i^b t$ for some $1 \leq b \leq a_i$ such that $p_i \nmid t$. Now, using an induction argument, one obtains that $(1 + p^u w)^{p^v} \equiv 1 \pmod{p^{u+v}}$ for all $u > 0$, $v \geq 0$ and $w \in \mathbb{Z}$. Thus, $(1 + \alpha_\varphi)^{p_i^{a_i}} \equiv 1 \pmod{p^{b+a_i}}$ and hence $(1/\alpha_\varphi)((1 + \alpha_\varphi)^{p_i^{a_i}} - 1) \equiv 0 \pmod{p_i^{a_i}}$. On the other hand, if $p_i \nmid \alpha_\varphi$, then, using $(1 + \alpha_\varphi)^{p_i^{a_i - 1}(p_i - 1)} \equiv 1 \pmod{p_i^{a_i}}$, we obtain $(1/\alpha_\varphi)((1 + \alpha_\varphi)^{p_i^{a_i-1}(p_i-1)} - 1) \equiv 0 \pmod{p_i^{a_i}}$. Therefore,

$$\frac{1}{\alpha_\varphi}((1 + \alpha_\varphi)^{d_i} - 1) \equiv 0 \pmod{p_i^{a_i}}$$

in either case and consequently

$$\varphi^{\mathrm{lcm}(d_1, \ldots, d_m)}(g) = g,$$

which proves the assertion. □

https://doi.org/10.1017/S0004972715000489 Published online by Cambridge University Press

3. Proofs of main theorems

Using the results obtained in the previous section, we are able to determine the structure of $Z(\mathrm{Aut}(G))$ when the centre of G is a finite cyclic group.

Proof of Theorem 1.1. Let $\varphi \in Z(\mathrm{Aut}(G))$ and let $g \in G$. Then $\varphi(g) = g\overline{\varphi}(g)$, where $\overline{\varphi}$ is defined in Section 2. Since $\overline{\varphi}(g)$ lies in the centre of G, it has a unique expression as $\overline{\varphi}(g) = \overline{\varphi_1}(g) \cdots \overline{\varphi_m}(g)$, where $\overline{\varphi_i}(g) \in P_i$, the Sylow p_i-subgroup of $Z(G)$. For $i = 1, \ldots, m$, consider the map $\varphi_i : G \longrightarrow G$ defined by $\varphi_i(g) = g\overline{\varphi_i}(g)$. Then φ_i is a homomorphism. Also, when $i \neq j$ and for $g \in G$, we have $\overline{\varphi_i}(\overline{\varphi_j}(g)) = 1$ (the identity element of G), which implies that $\varphi = \varphi_1 \cdots \varphi_m$. Thus, since φ is a bijection, each φ_i is also a bijection and hence it is an automorphism. On the other hand, if $\theta \in \mathrm{Aut}(G)$, then $\varphi\theta = \theta\varphi$. Hence, for all $g \in G$,

$$\theta(g)\overline{\varphi_1}(\theta(g)) \cdots \overline{\varphi_m}(\theta(g)) = \theta(g)\theta(\overline{\varphi_1}(g)) \cdots \theta(\overline{\varphi_m}(g)),$$

so that

$$\begin{aligned}\overline{\varphi_i}(\theta(g))\theta(\overline{\varphi_i}(g))^{-1} = \theta(\overline{\varphi_1}(g))\overline{\varphi_1}(\theta(g))^{-1} \cdots \theta(\overline{\varphi_{i-1}}(g))\overline{\varphi_{i-1}}(\theta(g))^{-1}\\ \cdot \theta(\overline{\varphi_{i+1}}(g))\overline{\varphi_{i+1}}(\theta(g))^{-1} \cdots \theta(\overline{\varphi_m}(g))\overline{\varphi_m}(\theta(g))^{-1}.\end{aligned}$$

Note that the left-hand side of the above equality is in P_i and the right-hand side belongs to $P_1 \cdots P_{i-1}P_{i+1} \cdots P_m$. Hence, $\overline{\varphi_i}(\theta(g)) = \theta(\overline{\varphi_i}(g))$, which implies that $\varphi_i\theta = \theta\varphi_i$ and hence $\varphi_i \in Z(\mathrm{Aut}(G))$. Now put

$$A_i = \{\varphi \in Z(\mathrm{Aut}(G)) : \overline{\varphi}(g) \in P_i \text{ for all } g \in G\}$$

for all $i = 1, \ldots, m$. Then $Z(\mathrm{Aut}(G)) = A_1 \cdots A_m \cong A_1 \times \cdots \times A_m$.

Let α^* be the same homomorphism as in Lemma 2.1(b). Since the elements of $\mathrm{Im}(\alpha^*)$ are integers coprime to $|Z(G)|$, they are also coprime to $|P_i|$. Hence, $\alpha_i^* = \alpha^*|_{A_i}$ may be considered as a homomorphism from A_i into $U(P_i)$, the group of units of the cyclic group P_i. If $\varphi \in \mathrm{Ker}\,\alpha_i^*$, then $\varphi(z_i) = z_i$, from which it follows that $\varphi^k(g) = g\overline{\varphi}(g)^k$ for all $g \in G$ and integers k. By definition, $\overline{\varphi}(g) \in P_i$ for all $g \in G$, which implies that φ is a p_i-automorphism. Hence, $\mathrm{Ker}\,\alpha_i^*$ is a p_i-group and $\mathrm{Im}\,\alpha_i^*$ is a subgroup of $U(P_i)$ which is a cyclic group of order $p_i^{a_i-1}(p_i - 1)$. Note that in Lemma 2.3, if $\mathrm{Im}\,\overline{\varphi} \subseteq H \leq Z(G)$, then we may use H instead of $Z(G)$. Thus, if $\varphi \in A_i$, then the order of φ divides either $p_i^{a_i}$ or $p_i^{a_i-1}(p_i - 1)$.

If $p_i = 2$, then A_i is an abelian group with exponent dividing $p_i^{a_i}$ and we are done. Hence, we may assume that $p_i \neq 2$. Then, since the exponent of A_i divides $p_i^{a_i}(p_i - 1)$, either A_i has exponent dividing $p_i^{a_i}$, which is one of the types mentioned in parts (a) and (b) of the conclusion of the theorem, or it contains a nontrivial element φ whose order divides $p_i - 1$. Suppose that the latter case holds. Put $\alpha = \alpha_\varphi$, $n_i = p_1^{a_1} \cdots p_{i-1}^{a_{i-1}}p_{i+1}^{a_{i+1}} \cdots p_m^{a_m}$ and $z_i = z^{n_i}$, where z is a generator of $Z(G)$. Then $P_i = \langle z_i\rangle$. Also, n_i divides α and, since $\varphi \neq I$ (the identity automorphism of G) has order dividing $p_i - 1$, we get $\alpha \neq 0$ and so $p_i \nmid \alpha$ by the proof of Lemma 2.3. Hence, we can choose $0 < \beta < p_i^{a_i}$ in such a way that $1 + \alpha\beta$ is a primitive root modulo $p_i^{a_i}$. Define the maps

https://doi.org/10.1017/S0004972715000489 Published online by Cambridge University Press

$\overline{\varphi_\beta} : G \longrightarrow P_i$ and $\varphi_\beta : G \longrightarrow G$ by $\overline{\varphi_\beta}(g) = \overline{\varphi}(g)^\beta$ and $\varphi_\beta(g) = g\overline{\varphi_\beta}(g)$, respectively. Then both $\overline{\varphi_\beta}$ and φ_β are homomorphisms. Moreover, φ_β is one-to-one, for, if $\varphi_\beta(g) = 1$, then $g\overline{\varphi}(g)^\beta = 1$ and hence $g = \overline{\varphi}(g)^{-\beta} \in P_i$. If $g \neq 1$, then, for some $0 < u < p_i^{a_i}$, we have $g = z_i^u$ and therefore $z_i^{u(1+\alpha\beta)} = 1$, which is impossible by the choice of β. Therefore, φ_β is one-to-one. Moreover, $P_i \cap \operatorname{Ker}\overline{\varphi} = \{1\}$ and $G = P_i \operatorname{Ker}\overline{\varphi}$. Now, for $g \in G$, there exists an integer u with $0 \leq u < p_i^{a_i}$ and $k \in \operatorname{Ker}\overline{\varphi}$ such that $g = z_i^u k$. Let $0 \leq v < p_i^{a_i}$ be such that $v(1 + \alpha\beta) \equiv u \pmod{p_i^{a_i}}$. Then

$$\varphi_\beta(z_i^v k) = \varphi_\beta(z_i^v)\varphi_\beta(k) = (z_i\overline{\varphi_\beta}(z_i))^v k\overline{\varphi_\beta}(k) = z_i^{v(1+\alpha\beta)}k = z_i^u k = g,$$

which implies that φ_β is onto and hence it is an automorphism. It is easy to see that $\psi \in Z(\operatorname{Aut}(G))$ if and only if $\overline{\psi}$ commutes with every automorphism of G. Since $\varphi \in Z(\operatorname{Aut}(G))$, we see that $\overline{\varphi}$ and hence $\overline{\varphi_\beta}$ commutes with every automorphism of G. Thus, $\varphi_\beta \in Z(\operatorname{Aut}(G))$ and so it is in A_i. Now we have $\overline{\varphi_\beta}(z) = z^{\alpha\beta}$ and so $\alpha_{\varphi_\beta} \equiv \alpha\beta \pmod{n}$. Thus, by using (2.4),

$$\begin{aligned}\varphi_\beta^k(z_i) &= z_i\overline{\varphi_\beta}(z_i)^{(1/\alpha\beta)((1+\alpha\beta)^k-1)}\\ &= z_i z_i^{(1+\alpha\beta)^k-1}\end{aligned}$$

for all $k \geq 1$.

If $k = |\varphi_\beta|$ is the order of φ_β, then $\varphi_\beta^k(z_i) = z_i$ and hence $z_i^{(1+\alpha\beta)^k-1} = 1$. This implies that $(1+\alpha\beta)^k \equiv 1 \pmod{p_i^{a_i}}$, so that $p_i^{a_i-1}(p_i-1)$ divides k. Therefore, $|\varphi_\beta| = p_i^{a_i-1}(p_i-1)$.

It is easy to see that an automorphism $\psi \in A_i$ has order two if and only if $\alpha_\psi \equiv -2 \pmod{n}$. From the preceding paragraph, it follows that A_i has an element ψ of order two and hence $\alpha_\psi \equiv -2 \pmod{n}$. Now, for $\theta \in \operatorname{Ker}\alpha^*$, we have $\alpha_{\psi\theta} \equiv -2 \pmod{n}$, from which it follows that $|\psi\theta| = 2$. Since $\operatorname{Ker}\alpha^*$ is a p-group, the orders of ψ and θ are coprime and we have $|\psi\theta| = |\psi|\,|\theta|$. Hence, $\theta = I$. Thus, $\operatorname{Ker}\alpha^* = \langle I\rangle$ and A_i is a cyclic group of order $p_i^{a_i-1}(p_i - 1)$. The proof is complete. □

Corollary 3.1. *Let G be a finite nilpotent group with cyclic centre of order $n = p_1^{a_1} \cdots p_m^{a_m}$. Then either the Sylow p_i-subgroup of G is cyclic or the subgroup A_i defined in Theorem 1.1 is isomorphic to:*

(a) *the trivial group; or*

(b) *an abelian p_i-group whose exponent divides $p_i^{a_i}$.*

Proof. As in the proof of Theorem 1.1, if A_i is not isomorphic to the groups in parts (a) or (b), then $G = P_i \operatorname{Ker}\overline{\varphi}$ for some φ in A_i. Now let Q_i be the Sylow p_i-subgroup of $\operatorname{Ker}\overline{\varphi}$. Then $R_i = P_iQ_i \cong P_i \times Q_i$ is a Sylow p_i-subgroup of G and hence $P_i = Z(R_i) \cong P_i \times Z(Q_i)$, which implies that $Q_i = \langle 1\rangle$. Therefore, $R_i = P_i$ is a cyclic group. □

Using a similar method, we obtain the structure of $Z(\operatorname{Aut}(G))$ when $Z(G)$ is an infinite cyclic group.

https://doi.org/10.1017/S0004972715000489 Published online by Cambridge University Press

Proof of Theorem 1.2. Let φ be in $Z(\mathrm{Aut}(G))$ and let α^* be the homomorphism in Lemma 2.2(b). By Lemma 2.2(a),

$$1 = \alpha_I + 1 = (\alpha_\varphi + 1)(\alpha_{\varphi^{-1}} + 1).$$

Hence, $\alpha_\varphi = \alpha_{\varphi^{-1}} = 0$ or $\alpha_\varphi = \alpha_{\varphi^{-1}} = -2$.

If $\varphi \in \mathrm{Ker}\,\alpha^* \neq \langle I \rangle$, then $\alpha_\varphi = 0$, which implies that $\overline{\varphi}^2(g) = 1$ for all $g \in G$. Hence, $\varphi^k(g) = g\overline{\varphi}(g)^k$ for all $k \in \mathbb{N}$, and so φ is of infinite order, that is, $\mathrm{Ker}\,\alpha^*$ is a torsion-free abelian group. Suppose that $Z(\mathrm{Aut}(G))$ is none of the groups in parts (a), (b) or (c). Then $Z(\mathrm{Aut}(G))/\mathrm{Ker}\,\alpha^*$ is isomorphic to C_2 with $\mathrm{Ker}\,\alpha^*$ nontrivial. Hence, $Z(\mathrm{Aut}(G))$ contains two elements φ and ψ, say, with $\alpha_\varphi = -2$ and $\alpha_\psi = 0$. It is easy to see that $\alpha_\theta = -2$ if and only if $|\theta| = 2$ for each $\theta \in Z(\mathrm{Aut}(G))$. Now, since $\alpha_{\varphi\psi} = -2$, it follows that $|\varphi\psi| = 2$, which is impossible, for $\varphi\psi$ is of infinite order. □

The following examples, together with the finite cyclic p-groups, show that all parts (a), (b) and (c) in Theorem 1.1 may occur and so the results in Theorem 1.1 cannot be further improved.

Example 3.2. Let p be an odd prime number and $G = \langle a, b \mid a^p = b^p = [a, b]^p = 1, [a, b]^a = [a, b]^b = [a, b]\rangle$ be a p-group of order p^3 and exponent p. It can be easily verified that for all $0 \leq u, v, w, u', v', w' < p$, the map given by $a \mapsto a^u b^v [a, b]^w$ and $b \mapsto a^{u'} b^{v'} [a, b]^{w'}$ defines a homomorphism of G. This homomorphism is an automorphism if and only if

$$\begin{vmatrix} u & u' \\ v & v' \end{vmatrix} \not\equiv 0 \pmod{p},$$

which implies that $|\mathrm{Aut}(G)| = p^3(p^2 - 1)(p - 1)$. Let $\varphi \in Z(\mathrm{Aut}(G))$; then $\varphi(a) = az^s$ and $\varphi(b) = bz^t$ for some s, t. If ψ is the automorphism which sends a to $a^2 b$ and b to ab, then, from the equalities $\varphi(\psi(a)) = \psi(\varphi(a))$ and $\varphi(\psi(b)) = \psi(\varphi(b))$, it follows that $s = t = 0$. Hence, $Z(\mathrm{Aut}(G)) = \langle I \rangle$.

Example 3.3. Let $G = \langle a, b \mid a^{p^2} = b^p = 1, ba = a^{p+1}b\rangle$ be a p-group of order p^3 for any prime number p. An easy manipulation shows that for all $0 \leq u, u' < p^2$ and $0 \leq v, v' < p$, the map given by $a \mapsto a^u b^v$ and $b \mapsto a^{u'} b^{v'}$ is a homomorphism if and only if $p \mid u'$ and $p \mid u(v' - 1)$, and it is an automorphism if and only if $p \mid u'$, $p \nmid u$ and $v' = 1$. From these facts, it follows that $|\mathrm{Aut}(G)| = p^3(p - 1)$. Also, $\varphi \in Z(\mathrm{Aut}(G))$ if and only if $\overline{\varphi}(a) = a^{kp}$ and $\overline{\varphi}(b) = 1$, where $0 \leq k < p$. Hence, $Z(\mathrm{Aut}(G)) \cong C_p$.

The following example, together with the infinite cyclic group, shows that both parts (a) and (b) in Theorem 1.2 may occur. We have no example yet of a group with infinite cyclic centre such that the centre of its automorphism group is a nontrivial torsion-free abelian group.

Example 3.4. Let $G = \langle a, b, c \mid [a, c] = [b, c] = 1\rangle$ be a group with infinite cyclic centre. Assume that $\varphi \in Z(\mathrm{Aut}(G))$ and take ψ_1 and ψ_2 to be automorphisms given by $\psi_1 : a \mapsto ab, b \mapsto b, c \mapsto c$ and $\psi_2 : a \mapsto a, b \mapsto ab, c \mapsto c$. Now, since $\overline{\varphi}(a), \overline{\varphi}(b) \in Z(G) = \langle c \rangle$ and $\overline{\varphi}$ commutes with both ψ_1 and ψ_2, it can be easily seen that $\overline{\varphi}(a) = \overline{\varphi}(b) = 1$ and so $\varphi = I$. Therefore, $Z(\mathrm{Aut}(G)) = \langle I \rangle$.

https://doi.org/10.1017/S0004972715000489 Published online by Cambridge University Press

We conclude this paper by posing two problems.

QUESTION 3.5. Is there a group G with infinite cyclic centre such that $Z(\mathrm{Aut}(G))$ is a nontrivial torsion-free abelian group?

As we have shown in Lemma 2.3, $\exp(Z(\mathrm{Aut}(G)) \leq \exp(Z(G))$ for groups with a cyclic centre. Thus, we may ask the following question.

QUESTION 3.6. Is it true that $\exp(Z(\mathrm{Aut}(G)) \leq \exp(Z(G))$ for any group G?

References

[1] J. E. Adney and T. Yen, 'Automorphisms of a p-group', *Illinois J. Math.* **9** (1965), 137–143.
[2] M. Deaconescu and G. L. Walls, 'On the group of automorphisms of a group', *Amer. Math. Monthly* **118**(5) (2011), 452–455.
[3] E. Formanek, 'Fixed points and centers of automorphism groups of free nilpotent groups', *Comm. Algebra* **30**(2) (2002), 1033–1038.

M. FARROKHI D. G., Mathematical Science Research Unit,
College of Liberal Arts, Muroran Institute of Technology,
27-1, Mizumoto, Muroran 050-8585, Hokkaido, Japan
e-mail: m.farrokhi.d.g@gmail.com

MOHAMMAD REZA R. MOGHADDAM,
Department of Pure Mathematics and the Centre of Excellence
in Analysis on Algebraic Structures, Ferdowsi University of Mashhad,
Mashhad, Iran
and
Department of Mathematics, Khayyam University,
Mashhad, Iran
e-mail: rezam@ferdowsi.um.ac.ir