Commun. Korean Math. Soc. **28** (2013), No. 4, pp. 643–647
http://dx.doi.org/10.4134/CKMS.2013.28.4.643

COMMUTING AUTOMORPHISM OF p-GROUPS WITH CYCLIC MAXIMAL SUBGROUPS

Fatemeh Vosooghpour, Zeinab Kargarian, and Mehri Akhavan-Malayeri

Abstract. Let G be a group and let p be a prime number. If the set $\mathcal{A}(G)$ of all commuting automorphisms of G forms a subgroup of $\mathrm{Aut}(G)$, then G is called $\mathcal{A}(G)$-group. In this paper we show that any p-group with cyclic maximal subgroup is an $\mathcal{A}(G)$-group. We also find the structure of the group $\mathcal{A}(G)$ and we show that $\mathcal{A}(G) = \mathrm{Aut}_c(G)$. Moreover, we prove that for any prime p and all integers $n \geq 3$, there exists a non-abelian $\mathcal{A}(G)$-group of order p^n in which $\mathcal{A}(G) = \mathrm{Aut}_c(G)$. If $p > 2$, then $\mathcal{A}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}}$ and if $p = 2$, then $\mathcal{A}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-3}}$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

1. Introduction

Let G be a group. An automorphism α of G is called a *commuting automorphism* if $g\alpha(g) = \alpha(g)g$ for all $g \in G$. The set of all commuting automorphism of the group G is denoted by $\mathcal{A}(G)$.

It is well known that $\mathcal{A}(G)$ does not necessarily form a subgroup of the $\mathrm{Aut}(G)$, but it has a number of interesting properties (see [1]). Also, if G satisfies some special conditions, then $\mathcal{A}(G)$ is a group. It is clear that $\mathcal{A}(G)$ contains the group $\mathrm{Aut}_c(G)$ of central automorphisms of G. The converse inclusion does not hold in general. A group G is called $\mathcal{A}(G)$-group if the set $\mathcal{A}(G)$ forms a subgroup of $\mathrm{Aut}(G)$. For example, $\mathcal{A}(G) = 1$ whenever G has no nontrivial abelian normal subgroups (see [4]) or $G = G'$ (see [1]).

Also, Deaconescu, Silberberg and Walls [1, Theorem 1.1] proved the following results:

Theorem 1.1. *Let G be a group satisfying maximal condition on subgroups. If $\alpha \in \mathcal{A}(G)$, then $[G,\alpha] \subseteq Z_\infty(G)$. In particular for such a group, $\mathcal{A}(G) = 1$ if and only if $\mathrm{Aut}_c(G) = 1$.*

As a direct consequence of Theorem 1.1 one obtains:

Corollary 1.2. *If G satisfies maximal condition on subgroups and $Z_2(G) = Z(G)$, then $\mathcal{A}(G) = \mathrm{Aut}_c(G)$.*

Received February 23, 2010; Revised March 12, 2013.
2010 *Mathematics Subject Classification.* Primary 20F28; Secondary 20E36, 20E28.
Key words and phrases. commuting automorphism, cyclic maximal subgroup.

Let $R_2(G)$ denote the set of all 2-Engel elements of G. The next result gives another condition which implies the equality $\mathcal{A}(G) = \mathrm{Aut}_c(G)$.

Lemma 1.3 ([2, Lemma 2.2(i)]). *If $R_2(G) = Z(G)$, then $\mathcal{A}(G) = \mathrm{Aut}_c(G)$.*

We will see later, the converse of Corollary 1.2 and Lemma 1.3 is false.
In [5] Deaconescu, Silberberg and Walls asked the following questions about the set $\mathcal{A}(G)$:

(1) Is it true that the set $\mathcal{A}(G)$ is always a subgroup of $\mathrm{Aut}(G)$?
(2) What conditions on G imply the equality $\mathcal{A}(G) = \mathrm{Aut}_c(G)$?

Regarding to these questions, in this paper we will compute the commuting automorphism of finite p-groups of order p^n which have a cyclic maximal subgroup. We show that any p-group with cyclic maximal subgroup is an $\mathcal{A}(G)$-group. We also find the structure of the group $\mathcal{A}(G)$ and we show that $\mathcal{A}(G) = \mathrm{Aut}_c(G)$.

In [7] we proved that the minimum order of a non-$\mathcal{A}(G)$ p-group is p^5. We also found the smallest group order of a non-$\mathcal{A}(G)$ p-group. Furthermore we proved that for any prime p and for all integers $n \geq 5$, there exists a non-$\mathcal{A}(G)$ p-group of order p^n.

In this paper we prove that for any prime p and all integers $n \geq 3$, there exists a non-abelian $\mathcal{A}(G)$-group of order p^n in which $\mathcal{A}(G) = \mathrm{Aut}_c(G)$. If $p > 2$, then $\mathcal{A}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}}$ and if $p = 2$, then $\mathcal{A}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-3}}$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

We will use the following classification theorem to obtain information about the commuting automorphisms of these groups (see [6, 5.3.4]).

Theorem 1.4. *A group of order p^n has a cyclic maximal subgroup if and only if it is of one of the following types*:

(i) *a cyclic group of order p^n*;
(ii) *the direct product of a cyclic group of order p^{n-1} and one of order p*;
(iii) $\langle x, a \mid x^p = 1 = a^{p^{n-1}}, a^x = a^{1+p^{n-2}} \rangle$, $n \geq 3$;
(iv) *the dihedral group D_{2^n}, $n \geq 3$*;
(v) *the generalized quaternion group Q_{2^n}, $n \geq 3$*;
(vi) *the semidihedral group $\langle x, a \mid x^2 = 1 = a^{2^{n-1}}, a^x = a^{2^{n-2}-1} \rangle$, $n \geq 3$.*

The main results of this paper are as follows:

Theorem 1.5. *Let G be a p-group of order p^n which has a cyclic maximal subgroup. Then G is an $\mathcal{A}(G)$-group. In particular, $\mathcal{A}(G) = \mathrm{Aut}_c(G)$.*

Next we obtain the structure of commuting automorphisms of non-abelian p-groups with cyclic maximal subgroup.

Theorem 1.6. *Let G be a non-abelian p-group of order p^n with cyclic maximal subgroup. If p is an odd prime, then $\mathcal{A}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}}$. If $p = 2$, then $\mathcal{A}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-3}}$ or $\mathcal{A}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

In particular, we have the following consequences of the above theorems.

Corollary 1.7. *For a given prime p and all integers $n \geq 3$, there exists a non-abelian $\mathcal{A}(G)$-group of order p^n in which $\mathcal{A}(G) = \mathrm{Aut}_c(G)$ is an abelian p-group.*

Corollary 1.8. *For a given prime p, the minimum order of a non-abelian $\mathcal{A}(G)$ p-group is p^3.*

Corollary 1.9. *Let G be a group of order p^n. If G has a unique subgroup of order p, then G is an $\mathcal{A}(G)$-group and $\mathcal{A}(G) = \mathrm{Aut}_c(G)$.*

2. Proofs of the main results

In this paper all unexplained notation is standard and follows that of [6]. First we establish the following easy but basic result, required in the proof of the main results.

Lemma 2.1. *Let $G = \langle x, a\rangle$ be a non-abelian group and $\langle a\rangle$ be a normal cyclic maximal subgroup of G. Then $C_G(a) = \langle a\rangle$, $C_G(x) = \langle x\rangle Z(G)$ and $C_G(xa) = \langle xa\rangle Z(G)$.*

Proof. Since $\langle a\rangle$ is a normal maximal subgroup of G, we have $G = \langle a\rangle\langle x\rangle$. Thus every element of G can be expressed in the form $a^i x^j$ for some integers i, j. Let $g = a^i x^j \in C_G(a)$, then $[x^j, a] = 1$. It follows that $x^j \in Z(G)$. Since G is non-abelian and $\langle a\rangle$ is a maximal subgroup of G, we have $Z(G) < \langle a\rangle$. Hence $C_G(a) = \langle a\rangle$. Similarly, $C_G(x) = \langle x\rangle Z(G)$.

To complete the proof it is enough to observe that $G = \langle a\rangle\langle xa\rangle$. That is, every element of G can be expressed in the form $a^i(xa)^j$ for some integers i, j. Now, for any $g = a^i(xa)^j \in C_G(xa)$, we have $[a^i, x] = 1$ and hence $a^i \in Z(G)$. This completes the proof. □

The relationship between the commuting automorphisms and central automorphisms for a p-group with a cyclic maximal subgroup is given in Theorem 1.5. Now we prove this result.

Proof of Theorem 1.5. If G is abelian, then $\mathcal{A}(G) = \mathrm{Aut}_c(G) = \mathrm{Aut}(G)$. Let G be a non-abelian p-group. First suppose G is of type (iii) in Theorem 1.4, that is,

$$G = \langle x, a \mid x^p = 1 = a^{p^{n-1}}, a^x = a^{1+p^{n-2}}\rangle, \quad n \geq 3.$$

Since $\langle a\rangle$ is a normal maximal subgroup of G, by Lemma 2.1, we have $C_G(a) = \langle a\rangle$ and $C_G(x) = \langle x\rangle Z(G)$. Now consider $\alpha \in \mathcal{A}(G)$. There exist integers i, j and s such that $\alpha(x) = x^i z^s$ and $\alpha(a) = a^j$ where $z = a^p$ is a generator of $Z(G)$, $1 \leq i < p$, $0 \leq s < p^{n-2}$ and $1 \leq j < p^{n-1}$. Since α is an automorphism, we get $(j, p) = 1$ and $p^{n-3} \mid s$. Now it follows from the relation $[a, x] = a^{p^{n-2}}$ that $[\alpha(a), \alpha(x)] = \alpha(a)^{p^{n-2}}$ and so $i = 1$. Also, the equality $[\alpha(xa), xa] = 1$ shows that $p \mid j - 1$. Therefore, $\alpha(a) = az^k$ and $\alpha(x) = xz^s$ for some integers $0 \leq s < p^{n-2}$ and $0 \leq k < p^{n-2}$ where $p^{n-3} \mid s$. This shows that $\alpha \in \mathrm{Aut}_c(G)$.

In the cases (iv)-(vi) we have $G = \langle x, a\rangle$ where $Z(G) = \langle a^{2^{n-2}}\rangle$ and $x^2, (xa)^2 \in Z(G)$. For $\alpha \in \mathcal{A}(G)$, by Lemma 2.1, we have $\alpha(xa) = xaz^k$ and $\alpha(x) = xz^s$ for some integers $0 \le k, s < 2$, where $z = a^{2^{n-2}}$. So $\alpha(a) = az^l$ and $\alpha(x) = xz^s$ where $0 \le l, s < 2$. This shows that $\alpha \in \mathrm{Aut}_c(G)$ and it has order 2. □

Proof of Theorem 1.6. First, let

$$G = \langle x, a \mid x^p = 1 = a^{p^{n-1}}, a^x = a^{1+p^{n-2}}\rangle, \quad n \ge 3.$$

Then, as we have shown in Theorem 1.5, for fixed $\alpha \in \mathcal{A}(G)$, we have $\alpha(a) = az^r$ and $\alpha(x) = xz^s$ for some integers $0 \le r, s < p^{n-2}$ where $p^{n-3} \mid s$. Clearly, $\mathcal{A}(G)$ is abelian and by considering the possible choices for r and s, we get $|\mathcal{A}(G)| = p^{n-1}$. Since $z = a^p$ and $\alpha(a) = az^r$, we obtain $\alpha(z) = z^{rp+1}$. Hence,

$$\alpha^m(a) = az^{r\sum_{k=0}^{m-1}(rp+1)^k} \quad \text{and} \quad \alpha^m(x) = xz^{s\sum_{k=0}^{m-1}(rp+1)^k},$$

by a simple induction on m. Thus,

$$\alpha^m(a) = az^{r\frac{1-(rp+1)^m}{-rp}} \quad \text{and} \quad \alpha^m(x) = xz^{s\frac{1-(rp+1)^m}{-rp}}.$$

Now assume p is an odd prime and put $r = 1$. We may apply Binomial Theorem to produce the following congruence relations:

$$\begin{aligned}(p+1)^{p^{k-1}} &\equiv 1 \mod p^k,\\ (p+1)^{p^{k-2}} &\equiv 1 + p^{k-1} \mod p^k\end{aligned}$$

for $k > 1$. This shows that $\mathcal{A}(G)$ has an element of order p^{n-2}. So $\mathcal{A}(G)$ is a cyclic group of order p^{n-1} or the direct product of a cyclic group of order p^{n-2} and one of order p, according to Theorem 1.4. Note that G is nilpotent of class 2 and so $\mathrm{Inn}(G) \le \mathrm{Aut}_c(G) = \mathcal{A}(G)$. Therefore, $\mathcal{A}(G)$ has a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Hence $\mathcal{A}(G) \cong \mathbb{Z}_p \times \mathbb{Z}_{p^{n-2}}$.

Now suppose $p = 2$. We may assume $n \ge 4$ and define $\alpha, \beta, \gamma \in \mathcal{A}(G)$ as follows:

$$\alpha : \begin{cases} a & \mapsto az \\ x & \mapsto x \end{cases}, \quad \beta : \begin{cases} a & \mapsto az^{2^{n-3}-1} \\ x & \mapsto xz^{2^{n-3}} \end{cases}, \quad \gamma : \begin{cases} a & \mapsto az^{2^{n-2}-1} \\ x & \mapsto x \end{cases}$$

Clearly, β and γ are of order 2 and by the following congruence relations:

$$\begin{aligned}(2+1)^{2^{k-2}} &\equiv 1 \mod 2^k,\\ (2+1)^{2^{k-3}} &\equiv 1 + 2^{k-1} \mod 2^k\end{aligned}$$

for $k \ge 4$, we have $|\alpha| = 2^{n-3}$. An easy direct argument shows that $\mathcal{A}(G) = \langle\alpha\rangle \times \langle\beta\rangle \times \langle\gamma\rangle$ and hence $\mathcal{A}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-3}}$.

In the cases (iv)-(vi), as we see in the proof of Theorem 1.5, $\alpha(x) = xz^s$ and $\alpha(a) = az^l$ for some integers $0 \le s, l \le 1$. Thus $|\mathcal{A}(G)| = 2^2$ and $\mathcal{A}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Remark 2.2. In [5], we have computed $\mathcal{A}(G)$ for any non-abelian group of order p^3, where p is an odd prime. Now let G be a non-abelian group of order 2^3. It is well known that $G \cong D_8$ or $G \cong Q_8$. Theorem 1.5 implies

$\mathrm{Aut}_c(G) = \mathcal{A}(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Hence we identify the structure of $\mathcal{A}(G)$ for any group of order p^3, where p is prime.

From our results, Corollary 1.7 and Corollary 1.8 are obvious.

Proof of Corollary 1.9. By Theorem 5.3.6 of [6], any group G satisfying the hypotheses of Corollary 1.9 is cyclic or a generalized quaternion group. Hence G is an $\mathcal{A}(G)$-group and $\mathcal{A}(G) = \mathrm{Aut}_c(G)$ by Theorem 1.5. □

Finally, let

$$G = \langle x, a \mid x^p = 1 = a^{p^{n-1}}, a^x = a^{1+p^{n-2}} \rangle, \quad n \geq 3.$$

Then according to Theorem 1.5, $\mathcal{A}(G) = \mathrm{Aut}_c(G)$. But since G is a nilpotent group of class 2, $Z_2(G) \neq Z(G) \neq R_2(G)$. Therefore the converse of Corollary 1.2 and Lemma 1.3 do not hold in general.

Acknowledgment. The authors would like to thank the Managing Editor of the Communications of the Korean Mathematical Society and the referees for their valuable comments.

References

[1] M. Deaconescu, Gh. Silberberg, and G. L. Walls, *On commuting automorphisms of groups*, Arch. Math. (Basel) **79** (2002), no. 6, 423–429.

[2] M. Deaconescu and G. L. Walls, *Right* 2*-Engel elements and commuting automorphism of group*, J. Algebra **238** (2001), no. 2, 479–484.

[3] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice-Hall, Inc, 1991.

[4] I. N. Herstein, T. J. Laffey, *Problems and solutions*: *Solutions of elementary problems*: *E3039*, Amer. Math. Monthly **93** (1986), no. 10, 816–817.

[5] Z. Kargarian and M. Akhavan Malayeri, *On the commuting automrphisms of groups of order* p^3, Adv. Appl. Math. Sci. **9** (2011), no. 2, 115–120.

[6] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[7] F. Vosooghpour and M. Akhavan-Malayeri, *On commuting automorphisms of p-groups*, Comm. Algebra **41** (2013), no. 4, 1292–1299.

Fatemeh Vosooghpour
Department of Mathematics
Alzahra University
Vank, Tehran, 19834, Iran
E-mail address: vosooghpour@yahoo.com

Zeinab Kargarian
Department of Mathematics
Alzahra University
Vank, Tehran, 19834, Iran
E-mail address: zkargaryan@yahoo.com

Mehri Akhavan-Malayeri
Department of Mathematics
Alzahra University
Vank, Tehran, 19834, Iran
E-mail address: makhavanm@yahoo.com, mmalayer@alzahra.ac.ir