On commuting automorphisms of finite p-groups

By Pradeep Kumar Rai

School of Mathematics, Harish-Chandra Research Institute,
Chhatnag Road, Jhunsi, Allahabad 211019, India

(Communicated by Shigefumi Mori, M.J.A., April 13, 2015)

Abstract: Let G be a group. An automorphism α of G is called a commuting automorphism if $[\alpha(x), x] = 1$ for all $x \in G$. Let $A(G)$ be the set of all commuting automorphisms of G. A group G is said to be an $A(G)$-group if $A(G)$ forms a subgroup of $Aut(G)$. We give some sufficient conditions on a finite p-group G such that G is an $A(G)$-group. As an application we prove that a finite p-group G of coclass 2 for an odd prime p is an $A(G)$-group. Also we classify non-$A(G)$ groups G of order p^5.

Key words: Commuting automorphism; coclass 2 group.

1. Introduction. For a group G, let $A(G) = \{\alpha \in Aut(G) \mid x\alpha(x) = \alpha(x)x \ \forall\ x \in G\}$. Automorphisms from the set $A(G)$ are called commuting automorphisms. These automorphisms were first studied for various classes of rings [1,3,9]. The following problem was proposed by I. N. Herstein to the American Mathematical Monthly: If G is a simple non-abelian group, then $A(G) = 1$ [6]. Giving answer to Herstiens's problem, Laffey proved that $A(G) = 1$ provided G has no non-trivial abelian normal subgroups [8]. Also, Pettet gave a more general statement proving that $A(G) = 1$ if $Z(G) = 1$ and the commutator subgroup $\gamma_2(G) = G$ (See [8]). In 2002, Deaconescu, Silberberg and Walls proved a number of interesting properties of commuting automorphisms [2], and raised the following natural question about $A(G)$: Is it true that the set $A(G)$ is always a subgroup of $Aut(G)$, the automorphism group of G? They themselves answered the question in negative by constructing an extra-special group of order 2^5.

Following Vosooghpour and Akhavan-Malayeri we say that, a group G is an $A(G)$-group if $A(G)$ forms a subgroup of $Aut(G)$. Vosooghpour and Akhavan-Malayeri [10] showed that, for a given prime p, minimum order of a non-$A(G)$ p-group G is p^5. They also proved that there exists a non-$A(G)$ p-group G of order p^n for all $n \geq 5$. Fouladi and Orfi have shown that, if G is either a finite AC-group or a p-group of maximal class or a metacyclic p-group, then G is an $A(G)$-group [4].

We prove the following theorem for p-groups of coclass 2. By the coclass of a p-group G of order p^n we mean the number $n - c$, where c is the nilpotency class of G.

Theorem A. *Let G be a finite p-group of coclass 2 for an odd prime p. Then G is an $A(G)$-group.*

Vosooghpour and Akhavan-Malayeri proved that if G is a non-$A(G)$ p-group of order p^5 and nilpotency class 2 then $d(G) = 4$. Improving their result we prove the following theorem.

Theorem B. *Let G be a group of order p^5 for a prime p. Then G is a non-$A(G)$ group if and only if G is an extra-special p-group for an odd prime p or G is an extra-special 2-group of plus type, i.e., the central product of two dihedral groups of order 8.*

Remark 1.1. We would like to remark here that our claim, that the only non-$A(G)$ group G of order 32 is the extra-special group of plus type, does not agree with the claim of Vosooghpour and Akhavan-Malayeri in [10], where it is shown that, both the extra-special groups G of order 32 are non-$A(G)$ groups. One can notice in their proof of Theorem 1.2, that the definition of α, for the extra-special group of order 2^n with relation $x_2^2 = z$ is invalid because it maps x_4 to $x_4x_2z^{c_4}$ and therefore does not preserve the relation $x_4^2 = 1$.

We use the following notations. For a multiplicatively written group G, let $x, y \in G$. Then $[x, y]$ denotes the commutator $x^{-1}y^{-1}xy$. By $Z(G)$ and $Z_2(G)$ we denote the center and second center of G respectively. The centralizer of H in G, where H is a subgroup of G, is denoted by $C_G(H)$. We write

2010 Mathematics Subject Classification. Primary 20F28.

doi: 10.3792/pjaa.91.57

$\gamma_k(G)$ for the k'th term in the lower central series of G. For $\alpha \in Aut(G)$ and $H \leq G$, $[H, \alpha]$ denotes the set $\{h^{-1}\alpha(h) \mid h \in H\}$ and $C_H(\alpha)$ denotes the subgroup $\{h \in H \mid \alpha(h) = h\}$. Let $H \leq G$ and $T \leq Aut(G)$, then $[H, T]$ denotes the set $\{h^{-1}\alpha(h) \mid h \in H,\ \alpha \in T\}$. By $d(G)$ we mean the minimum no. of generators of G.

2. Prerequisites. An automorphism α of a group G is called central automorphism if $x^{-1}\alpha(x) \in Z(G)$ for all $x \in G$. These automorphisms form a normal subgroup of $Aut(G)$, which we denote by $\mathrm{Autcent}(G)$.

Now we collect some results on commuting automorphisms which we will use in section 3.

Theorem 2.1 ([2, Theorem 1.3]). *Let G be a group such that $Z(G')$ contains no involutions. Then $A(G)$ is a subgroup of $Aut(G)$ if and only if commutators of elements in $A(G)$ are central automorphisms.*

Theorem 2.2 ([2, Theorem 1.4]). *If G is a group and if $\alpha \in A(G)$, then $[G^2, \alpha] \leq Z_2(G)$.*

Lemma 2.3 ([8]). *If $\alpha \in A(G)$ and $x, y \in G$, then $[\alpha(x), y] = [x, \alpha(y)]$.*

Lemma 2.4 ([2, Lemma 2.4 (ii, vi, viii), Lemma 2.6 (iii)]). *Let G be a group and $\alpha, \beta \in A(G)$, then*

(i) *$A(G)$ is closed under powers.*
(ii) *$\alpha\beta \in A(G)$ if and only if $[\alpha(x), \beta(x)] = 1$ for all $x \in G$.*
(iii) *$\alpha^2 \in \mathrm{Autcent}(G)$ if and only if $\gamma_2(G) \leq C_G(\alpha)$.*
(iv) *$\gamma_3(G) \leq C_G(\alpha)$.*

Lemma 2.5 ([10, Lemma 2.2]). *Let G be a group of nilpotency class 2. If $d(G/Z(G)) = 2$, then G is an $A(G)$-group.*

Theorem 2.6 ([10, Theorem 1.5]). *For a given prime p, the minimal number of generators of a non-$A(G)$ p-group of order p^5 and of nilpotency class 2 is equal to 4.*

3. Proofs of the Theorems A and B. We first prove the following theorem.

Theorem 3.1. *Let G be a finite p-group for an odd prime p. If $[Z_2(G), A(G)] \leq Z(G)$, then G is an $A(G)$-group.*

Proof. Since G is an odd order group, by Theorem 2.2 we have, for all $\delta \in A(G)$ and for all $x \in G$, $x^{-1}\delta(x) \in Z_2(G)$. Let $\alpha, \beta \in A(G)$, $x \in G$ and $\alpha(x) = xz_1$, $\beta(x) = xz_2$ for some $z_1, z_2 \in Z_2(G)$. Note that $\alpha^{-1}(x) = x\alpha^{-1}(z_1^{-1})$ and $\beta^{-1}(x) = x\beta^{-1}(z_2^{-1})$. Now we have

$$\begin{aligned}
&[\alpha, \beta](x)\\
&= \alpha^{-1}\beta^{-1}\alpha\beta(x)\\
&= \alpha^{-1}\beta^{-1}\alpha(xz_2)\\
&= \alpha^{-1}\beta^{-1}(xz_1\alpha(z_2))\\
&= \alpha^{-1}(\beta^{-1}(x)\beta^{-1}(z_1)\beta^{-1}\alpha(z_2))\\
&= \alpha^{-1}(x\beta^{-1}(z_2^{-1})\beta^{-1}(z_1)\beta^{-1}\alpha(z_2))\\
&= x\alpha^{-1}(z_1^{-1})\alpha^{-1}\beta^{-1}(z_2^{-1})\alpha^{-1}\beta^{-1}(z_1)\alpha^{-1}\beta^{-1}\alpha(z_2)\\
&= x\alpha^{-1}\beta^{-1}(\beta(z_1^{-1})z_2^{-1}z_1\alpha(z_2))\\
&= x\alpha^{-1}\beta^{-1}(\beta(z_1^{-1})z_1[z_1, z_2]z_2^{-1}\alpha(z_2)).
\end{aligned}$$

So that $x^{-1}[\alpha, \beta](x) = \alpha^{-1}\beta^{-1}(\beta(z_1^{-1})z_1[z_1, z_2]z_2^{-1}\alpha(z_2))$. Since $[Z_2(G), A(G)] \leq Z(G)$, we have $\beta(z_1^{-1})z_1, z_2^{-1}\alpha(z_2) \in Z(G)$. Obviously, $[z_1, z_2] \in Z(G)$. It follows that $\alpha^{-1}\beta^{-1}(\beta(z_1^{-1})z_1[z_1, z_2]z_2^{-1}\alpha(z_2)) \in Z(G)$. We have proved that for all α, $\beta \in A(G)$ and for all $x \in G$, $x^{-1}[\alpha, \beta](x) \in Z(G)$. This shows that $[\alpha, \beta] \in \mathrm{Autcent}(G)$ for all α, $\beta \in A(G)$. Now from Theorem 2.1, it follows that G is an $A(G)$-group. □

Lemma 3.2. *Let p be an odd prime and G be a finite p-group such that $Z_2(G)$ is abelian. Then G is an $A(G)$-group.*

Proof. Let $\alpha, \beta \in A(G)$ and $x \in G$. By Theorem 2.2, $\alpha(x) = xz_1$, $\beta(x) = xz_2$ for some z_1, $z_2 \in Z_2(G)$. Since $Z_2(G)$ is abelian, and z_1, $z_2 \in C_G(x)$, we have $[\alpha(x), \beta(x)] = [xz_1, xz_2] = 1$. By Lemma 2.4 (ii) we get that $\alpha\beta \in A(G)$. Since $A(G)$ is closed under powers and G is finite we also have $\alpha^{-1} \in A(G)$. This proves that $A(G)$ is a subgroup. □

Theorem 3.3. *Let p be an odd prime and G be a finite p-group such that $|Z_2(G)/Z(G)| = p^2$ and $Z(G) = \gamma_k(G)$ for some $k \geq 2$. Then G is an $A(G)$-group.*

Proof. For $k = 2$, the result follows from Lemma 2.5. So let us assume $k \geq 3$. Now in view of Lemma 3.2, we can assume that $Z_2(G)$ is non-abelian. It follows that $Z_2(G)/Z(G)$ is elementary abelian, for if $Z_2(G)/Z(G)$ is cyclic, then $Z_2(G)$ is abelian, which is a contradiction. Let $Z_2(G) = \langle a, b, Z(G)\rangle$. Clearly $[a, b] \neq 1$, because $Z_2(G)$ is non-abelian. Also we have $[a, b] \in Z(G)$. Let $\alpha \in A(G)$. Note that any element of $Z_2(G)$ can be written as $a^r b^s z$ for some $r, s \in \mathbf{Z}$ and $z \in Z(G)$. Now since $[\alpha(a), a] = 1$, $[\alpha(b), b] = 1$ and $[a, b] \neq 1$ we get that $\alpha(a) = a^{r_1}z_1$ and $\alpha(b) = b^{s_1}z_2$ for some $r_1, s_1 \in \mathbf{Z}$ and $z_1, z_2 \in Z(G)$. Since $Z_2(G)/\ Z(G)$ is elementary abelian we can assume that $r_1 \not\equiv 0 \pmod p$ and $s_1 \not\equiv 0 \pmod p$. Now since $k \geq 3$, by Lemma

2.4 (iv), we have that $Z(G) \leq C_G(\alpha)$. Therefore $\alpha([a,b]) = [a,b]$ which gives the equality that $[a,b]^{r_1 s_1} = [a,b]$. It follows that

$$r_1 s_1 - 1 \equiv 0 \pmod{p}. \tag{3.1}$$

Again consider $[a,b] = \alpha([a,b]) = [\alpha(a), \alpha(b)]$, which by Lemma 2.3 equals $[a, \alpha^2(b)]$ which, after putting the value of $\alpha^2(b)$, turns out to be $[a,b]^{s_1^2}$. It follows that

$$s_1^2 - 1 \equiv 0 \pmod{p}. \tag{3.2}$$

Subtracting equation (3.2) from equation (3.1) we get that $s_1(r_1 - s_1) \equiv 0 \pmod{p}$. But $s_1 \not\equiv 0 \pmod{p}$. Therefore $r_1 \equiv s_1 \pmod{p}$. Since $Z_2(G)/Z(G)$ is elementary abelian, without loss of generality we can assume that $\alpha(b) = b^{r_1} z_3$ for some $z_3 \in Z(G)$. As $r_1^2 - 1 \equiv 0 \pmod{p}$, we get that either $r_1 - 1 \equiv 0 \pmod{p}$ or $r_1 + 1 \equiv 0 \pmod{p}$. If $r_1 \equiv 1 \pmod{p}$, then clearly $a^{-1}\alpha(a), b^{-1}\alpha(b) \in Z(G)$. It easily follows that for all $y \in Z_2(G)$, $y^{-1}\alpha(y) \in Z(G)$. Since α was chosen arbitrarily, by Theorem 3.1 G is an $A(G)$-group. Suppose $r_1 - 1 \not\equiv 0 \pmod{p}$, then $r_1 \equiv -1 \pmod{p}$. Therefore we have $\alpha(a) = a^{-1}u_1$ and $\alpha(b) = b^{-1}u_2$ for some $u_1, u_2 \in Z(G)$. It easily follows that for all $y \in Z_2(G)$, $\alpha(y) = y^{-1}u$ for some $u \in Z(G)$. Let $x \in G$. By Theorem 2.2 $\alpha(x) = xy$ for some $y \in Z_2(G)$. But then $\alpha^2(x) = \alpha(x)\alpha(y) = xyy^{-1}u = xu$ for some $u \in Z(G)$. Since x was chosen arbitrarily, this shows that $\alpha^2 \in \mathrm{Autcent}(G)$. By Lemma 2.4 (iii), we get that $\gamma_2(G) \leq C_G(\alpha)$. Hence $Z_2(G) \cap \gamma_2(G) \leq C_G(\alpha)$. Now observe that $\gamma_{k-1}(G) \leq Z_2(G)$ because $Z(G) = \gamma_k(G)$. Therefore, $|Z_2(G) \cap \gamma_2(G)| > |Z(G)|$. It follows that α fixes some $y \in Z_2(G) - Z(G)$. Let $a^r b^s z \in C_G(\alpha) - Z(G)$ for some $r, s \in \mathbf{Z}$ and $z \in Z(G)$. Therefore $a^r b^s \in C_G(\alpha) - Z(G)$. But then $a^r b^s = a^{-r} b^{-s} u_1^r u_2^s$. It follows that $a^{2r} b^{2s} = (a^r b^s)^2 [a,b]^{rs} \in Z(G)$. Hence $a^r b^s \in Z(G)$ which is a contradiction. This completes the proof. □

Proof of Theorem A. In view of Lemma 3.2 we can assume that $Z_2(G)$ is non-abelian. Since G is a p-group of coclass 2, we have $|Z_2(G)| = p^3$, $|Z(G)| = p$. Clearly $Z(G) = \gamma_c(G)$, where c is the nilpotency class of G. Now the Theorem A follows from Theorem 3.3. □

Now we are ready to prove Theorem B. We will use the classification of groups of order p^5 by James [7] in the proof. We note that James has classified these groups in 10 isoclinism families. These families are denoted by Φ_k for $k = 1, \ldots, 10$.

Proof of Theorem B. For $p = 2$, it can be checked using small group library and programming in GAP [5] that the only non-$A(G)$ group G of order 32 is the extra-special group with the GAP id SmallGroup(32, 49), which is the extra-special 2-group of plus type. So now we assume that p is an odd prime. We proceed by cases according to the nilpotency class of G. If G is a group of nilpotency class 4 then it is a group of maximal class and therefore $Z_2(G)$ is abelian. So by Lemma 3.2, G is an $A(G)$-group. Next suppose that G is a group of nilpotency class 3. Then it is a group of coclass 2 and so by Theorem A it is an $A(G)$-group. Now suppose that G is a group of nilpotency class 2. There are 3 isoclinic families, Φ_2, Φ_4 and Φ_5, of groups of order p^5 and of nilpotency class 2. Let $G \in \Phi_4$. It can be observed from James list of these groups that G is a 3 generated group. Therefore by Theorem 2.6, G is an $A(G)$-group. Next suppose that $G \in \Phi_2$. Then from the James list we note that either $d(G/Z(G)) = 2$ or $d(G) \leq 3$. Hence by Lemma 2.5 and Theorem 2.6, G is an $A(G)$-group. The family Φ_5 consists of two extra-special p-groups. It has been proved in [10, Theorem 1.2] that extra-special p-groups of order p^5 are non $A(G)$-groups. Clearly the abelian groups G are $A(G)$-groups. This completes the proof of the Theorem B. □

Acknowledgement. I thank the referee for his/her very valuable comments and suggestions.

References

[1] H. E. Bell and W. S. Martindale, III, Centralizing mappings of semiprime rings, Canad. Math. Bull. **30** (1987), no. 1, 92–101.

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

[3] N. Divinsky, On commuting automorphisms of rings, Trans. Roy. Soc. Canada. Sect. III. (3) **49** (1955), 19–22.

[4] S. Fouladi and R. Orfi, Commuting automorphisms of some finite groups, Glas. Mat. Ser. III **48(68)** (2013), no. 1, 91–96.

[5] The GAP Group, GAP — Groups, Algorithms, and Programming (Version 4.4.12, 2008). `http://www.gap-system.org`

[6] I. N. Herstein, Problems and Solutions: Elementary Problems: E3039, Amer. Math. Monthly **91** (1984), no. 3, 203.

[7] R. James, The groups of order p^6 (p an odd prime), Math. Comp. **34** (1980), no. 150, 613–637.

[8] T. J. Laffey, Problems and Solutions: Solutions of

Elementary Problems: E3039, Amer. Math. Monthly **93** (1986), no. 10, 816–817.
[9] J. Luh, A note on commuting automorphisms of rings, Amer. Math. Monthly **77** (1970), 61–62.
[10] F. Vosooghpour and M. Akhavan-Malayeri, On commuting automorphisms of p-groups, Comm. Algebra **41** (2013), no. 4, 1292–1299.