

Class-preserving automorphisms of some finite p -groups

DEEPAK GUMBER^{1,*} and MAHAK SHARMA²

¹School of Mathematics and Computer Applications, Thapar University,
Patiala 147 004, India

²Department of Applied Sciences and Humanities, Baddi University of Emerging
Sciences and Technology, Baddi 173 205, India

*Corresponding author. E-mail: dkgumber@yahoo.com

MS received 5 December 2013

Abstract. Let G be a finite p -group of order p^5 , where p is a prime. We give necessary and sufficient conditions on G such that G has a non-inner class-preserving automorphism. As a consequence, we give short and alternate proofs of results of Yadav (§5 of *Proc. Indian Acad. Sci. (Math. Sci.)* **118** (2008) 1–11) and Kalra and Gumber (Theorem 4.2 of *Indian J. Pure Appl. Math.* **44** (2013) 711–725).

Keywords. Class-preserving automorphism; p -group; central automorphism.

2010 Mathematics Subject Classification. 20D45, 20D15.

1. Introduction

Let G be a finite group. An automorphism α of G is called a class-preserving automorphism if for each element $x \in G$, there exists an element $g_x \in G$ such that $\alpha(x) = g_x^{-1}xg_x$; and is called an inner automorphism if for all $x \in G$, there exists a fix element $g \in G$ such that $\alpha(x) = g^{-1}xg$. The group $\text{Inn}(G)$ of all inner automorphisms of G is a normal subgroup of the group $\text{Aut}_c(G)$ of all class-preserving automorphisms of G . We denote the group $\text{Aut}_c(G)/\text{Inn}(G)$ of all class-preserving outer automorphisms by $\text{Out}_c(G)$. The interest in class-preserving automorphisms took place when Burnside (p. 463 of [2]) asked the question: Does there exist any finite group G such that G has a non-inner class-preserving automorphism? Burnside [3] himself gave an affirmative answer to his question by constructing a group G of order p^6 for which $\text{Out}_c(G)$ was non-trivial. For more details about this problem, one can see the survey article by Yadav [13].

Here, we are especially interested in class-preserving automorphisms of p -groups of order up to p^5 . Using the known classifications and presentations of finite extra-special p -groups and of groups of order p^4 , Kumar and Vermani [8, 9] proved that if G is an extra-special p -group (in particular, if $|G| = p^3$) or if $|G| = p^4$, then $\text{Out}_c(G) = 1$. It follows from [6] that all finite p -groups of order p^5 , where p is an odd prime, are partitioned into ten isoclinism families; and from [4] that all finite 2-groups of order 2^5 are partitioned into eight isoclinism families. Yadav [12] proved that if G and H are two finite non-abelian isoclinic groups, then $\text{Aut}_c(G) \simeq \text{Aut}_c(H)$. He then showed, by picking up one group from each isoclinism family, that $\text{Out}_c(G) \neq 1$ for the groups $\Phi_7(1^5)$ and $\Phi_{10}(1^5)$ from seventh and tenth family in [6], and hence concluded that if G is a finite p -group of

order p^5 , where p is an odd prime, then $\text{Out}_c(G) \neq 1$ if and only if G is isoclinic to a group either in the seventh or in the tenth family. Recently, Kalra and Gumber (Theorem 4.2 of [7]), using the classifications, isoclinism families and presentations given by Hall and Senior [4] and Sag and Wamsley [10], have shown that if G is a finite 2-group of order 2^5 , then $\text{Out}_c(G) = 1$ except for the forty fourth and forty fifth groups from the sixth family in [4].

Hertweck (Proposition 14.4 of [5]) proved that if G is a finite group having an abelian normal subgroup A with cyclic quotient G/A , then class-preserving automorphisms of G are inner automorphisms. Yadav (Corollary 3.6 of [12]) proved that if G is a finite p -group of nilpotence class 2 such that G' is cyclic, then $\text{Out}_c(G) = 1$. We shall use these results quite frequently in our proofs. Observe that if G is an extra-special p -group, then G' is cyclic; and if $|G| = p^4$, then G has a maximal abelian subgroup. It follows that for these groups G , $\text{Out}_c(G) = 1$. This paper is the result of an effort to find necessary and sufficient conditions, without using the available classifications and presentations, on a finite p -group G for which $\text{Out}_c(G)$ is non-trivial. In §2, we prove our main theorem, Theorem 2.3, which gives the necessary and sufficient conditions on a finite p -group G of order p^5 for which $\text{Out}_c(G) \neq 1$. As a consequence, we obtain short and alternate proofs of the results of Yadav (§5 of [12]) and Kalra and Gumber (Theorem 4.2 of [7]).

An automorphism α of a group G is called a central automorphism if it induces the identity automorphism on $G/Z(G)$; or equivalently, $x^{-1}\alpha(x) \in Z(G)$ for all $x \in G$. By $\text{Aut}_c(G)$, we denote the group of all central automorphisms of G . For $x \in G$, x^G denotes the conjugacy class of x in G . By G' and $\Phi(G)$, we respectively denote the commutator and the Frattini subgroup of G . A cyclic group of order m is denoted as C_m and $\gamma_3(G)$ denotes the third term of the lower central series of G . The symbol $\text{cl}(G)$ denotes the nilpotence class of G and by $d(G)$ we denote the smallest cardinality of a generating set of G . If H is a non-trivial proper normal subgroup of G , then (G, H) is called a Camina pair if and only if $H \subseteq [x, G]$ for all $x \in G - H$, where $[x, G] = \{[x, g] | g \in G\}$.

2. Proof of theorem

We start with the following crucial technical lemma. The lemma can be of independent interest also.

Lemma 2.1. Let G be any group such that $\text{Out}_c(G/Z(G))$ is trivial. Then $\text{Aut}_c(G) = (\text{Aut}_c(G) \cap \text{Aut}_z(G))\text{Inn}(G)$. In addition, if G is finite, then

$$|\text{Aut}_c(G)| = \frac{|\text{Aut}_c(G) \cap \text{Aut}_z(G)| |\text{Inn}(G)|}{|Z(\text{Inn}(G))|}.$$

Proof. If $\alpha \in \text{Aut}_c(G)$, then it induces a class-preserving automorphism, say $\bar{\alpha}$ on $G/Z(G)$ given by $\bar{\alpha}(xZ(G)) = \alpha(x)Z(G)$ for all $x \in G$. Since $\text{Out}_c(G/Z(G)) = 1$, $\alpha(x)Z(G) = a^{-1}xaZ(G)$ for a fix $a \in G$. Therefore, for each $x \in G$, there exists an element $z_x \in Z(G)$ such that $\alpha(x) = a^{-1}xaz_x = a^{-1}(xz_x)a$. Define a map $\beta : G \rightarrow G$ by $\beta(x) = a\alpha(x)a^{-1}$ for all $x \in G$. It is easy to see that $\beta \in \text{Aut}_c(G) \cap \text{Aut}_z(G)$ and $\alpha = i_a\beta$, where i_a denotes the inner automorphism of G given by conjugation with a . It thus follows that $\text{Aut}_c(G) = (\text{Aut}_c(G) \cap \text{Aut}_z(G))\text{Inn}(G)$. \square

PROPOSITION 2.2

Let G be a finite non-abelian p -group of order p^5 such that $|Z(G)| \geq p^2$. Then $\text{Out}_c(G) = 1$.

Proof. If $|Z(G)| \geq p^3$, then G has a maximal abelian subgroup and hence $\text{Out}_c(G) = 1$. We therefore suppose that $|Z(G)| = p^2$. Then $\text{cl}(G)$ is either 2 or 3. First suppose that $\text{cl}(G) = 2$. Then $G' \leq Z(G)$. If G' is cyclic, then $\text{Out}_c(G) = 1$. Therefore suppose that $G' = Z(G) \simeq C_p \times C_p$. Then $\exp(G/Z(G)) = \exp(G') = p$. It follows that $Z(G) = G' = \Phi(G)$ and hence $d(G) = 3$. If $G = \langle a, b, c \rangle$, then $G' = \langle [a, b], [a, c], [b, c] \rangle$. We can assume that $[b, c] = [a, b]^m [a, c]^n$ for some $m, n, 0 \leq m, n \leq p-1$. Set $u := ba^{-n}$ and $v := ca^m$. Then

$$[u, v] = [ba^{-n}, ca^m] = [b, c][b, a]^m [a, c]^{-n} = 1.$$

It follows that $\langle u, v, G' \rangle$ is a maximal abelian subgroup of G and hence $\text{Out}_c(G) = 1$.

Now suppose that $\text{cl}(G) = 3$. Then G' is abelian of order p^2 or p^3 . First assume that $|G'| = p^2$. Since $G/C_G(G')$ is isomorphic to a subgroup of $\text{Aut}(G')$, $[G : C_G(G')] \leq p$ and hence $|C_G(G')| = p^4$. The subgroup $G'Z(G)$ is of order p^3 and is contained in $C_G(G')$. It follows that $C_G(G') = \langle a, G'Z(G) \rangle$, where $a \in C_G(G') - G'Z(G)$, is a maximal abelian subgroup of G and hence $\text{Out}_c(G) = 1$. Next assume that $|G'| = p^3$. Then $G' = \Phi(G)$ and $d(G) = 2$. Let $G = \langle a, b \rangle$ and let $w := [a, b]$, $u := [a, w]$ and $v := [b, w]$. Then $G' = \langle w, \gamma_3(G) \rangle$ and $\gamma_3(G) = \langle u, v \rangle$. Since $[a, b]^p \equiv [a, b^p] \equiv 1 \pmod{\gamma_3(G)}$, $|G'/\gamma_3(G)| = p$ and hence $|\gamma_3(G)| = p^2$. If $|h^G| = p$ for some $h \in G - G'$, then $C_G(h) = \langle h, G' \rangle$ is a maximal abelian subgroup of G and thus $\text{Out}_c(G) = 1$; and if $|h^G| = p^3$ for some $h \in G - G'$, then $|C_G(h)| = p^2$ and hence $h \in Z(G)$, which is absurd. We therefore suppose that $|x^G| = p^2$ for all $x \in G - G'$. Then $|\text{Aut}_c(G)| \leq p^4$. Let $|\text{Aut}_c(G)| = p^4$. Then, for any $x, y \in G$, there exists an $\alpha \in \text{Aut}_c(G)$ such that $\alpha(a) = x^{-1}ax$ and $\alpha(b) = y^{-1}by$. In particular, there exists an $\alpha \in \text{Aut}_c(G)$ such that $\alpha(a) = b^{-1}ab$ and $\alpha(b) = a^{-1}ba$. Now $(ab)^{-1}\alpha(ab) \in [ab, G]$. But $(ab)^{-1}\alpha(ab) = b^{-1}a^{-1}\alpha(a)\alpha(b) = b^{-1}wbw^{-1} = [w, b] = v^{-1}$. Thus $v^{-1} \in [ab, G]$. Let $v^{-1} = [ab, h]$, where $h \in G$. Observe that $uv = [a, w][b, w] = [ab, w]$ and therefore $u = (uv)v^{-1} = [ab, w][ab, h] = [ab, wh] \in [ab, G]$. Thus $\gamma_3(G) \leq [ab, G]$. But since $[ab, G] = |(ab)^G| = p^2$, $\gamma_3(G) = [ab, G]$. Thus $w^{-1} = [b, a] = \in [ab, G] = \gamma_3(G)$. This is a contradiction and hence $\text{Out}_c(G) = 1$. This completes the proof. \square

Theorem 2.3. Let G be a finite non-abelian p -group of order p^5 . Then $\text{Out}_c(G) \neq 1$ if and only if $|Z(G)| = p$, $Z(G) < G'$ and either (i) $\text{cl}(G) = 3$ and $d(G) = 3$ or (ii) $\text{cl}(G) = 4$ and $Z(G) \subseteq [x, G]$ for all $x \in G - G'$.

Proof. First suppose that $\text{Out}_c(G) \neq 1$. Then $|Z(G)| = p$ by Proposition 2.2 and hence $Z(G) < G'$. It follows that G is purely non-abelian and $\text{cl}(G)$ is either 3 or 4. Suppose that $\text{cl}(G) = 3$. Since $|G'| = p^2$ or p^3 , $|\text{Aut}_z(G)| = |\text{Hom}(G/G', Z(G))| \leq p^3$ by Theorem 1 of [1]. Also, since $G/Z(G)$ is a class 2 group of order p^4 , $|Z(\text{Inn}(G))| = p^2$. It now follows by Lemma 2.1 that

$$|\text{Aut}_c(G)| = p^2 |\text{Aut}_c(G) \cap \text{Aut}_z(G)| \leq p^5.$$

Since $|\text{Aut}_c(G)| > |\text{Inn}(G)| = p^4$, $|\text{Aut}_z(G)| = p^3$ and hence $d(G) = 3$. Next suppose that $\text{cl}(G) = 4$. Then G is of maximal class and hence $|G'| = p^3$, $|Z(\text{Inn}(G))| = p$, $d(G) = 2$ and $|\text{Aut}_z(G)| = |\text{Hom}(C_p \times C_p, C_p)| = p^2$. Thus

$$|\text{Aut}_c(G)| = p^3 |\text{Aut}_c(G) \cap \text{Aut}_z(G)| \leq p^5,$$

by Lemma 2.1. It follows that $|\text{Aut}_c(G) \cap \text{Aut}_z(G)| = p^2$ and hence $\text{Aut}_z(G) \leq \text{Aut}_c(G)$. Let $a \in G - G'$ and let $G = \langle a, b \rangle$. Suppose that all central automorphisms of G fix a . Then each $1 \neq \alpha \in \text{Aut}_z(G)$ would have to move b . Since $|\text{Aut}_z(G)| = p^2$, this would require that $|Z(G)| = p^2$, which is not so. Thus, there exists a central automorphism α such that $\alpha(a) = az$ for some $1 \neq z \in Z(G)$. On the other hand, since α is class-preserving, $\alpha(a) = g^{-1}ag$ for some $g \in G$. It follows that $z = [a, g]$ and, since $z^n = [a, g^n]$ for all $n \geq 1$, $Z(G) \subseteq [x, G]$ for all $x \in G - G'$.

To prove the converse, we first suppose that $|Z(G)| = p$, $Z(G) < G'$, $\text{cl}(G) = 4$ and $Z(G) \subseteq [x, G]$ for all $x \in G - G'$. Since G is of maximal class, $|Z(\text{Inn}(G))| = p$, $|G'| = p^3$, $d(G) = 2$ and hence $|\text{Aut}_z(G)| = |\text{Hom}(C_p \times C_p, C_p)| = p^2$. Also, since $Z(G) \subseteq [x, G]$ for all $x \in G - G'$, $\text{Aut}_z(G) \leq \text{Aut}_c(G)$. It follows by Lemma 2.1 that $|\text{Aut}_c(G)| = p^5 > |\text{Inn}(G)|$. Next suppose that $|Z(G)| = p$, $Z(G) < G'$ and $\text{cl}(G) = d(G) = 3$. Then $|G'| = |\Phi(G)| = p^2$ and hence $|\text{Aut}_z(G)| = |\text{Hom}(G/G', Z(G))| = p^3$. It follows from Theorems 4.7 and 5.1 of [11] that $(G, Z(G))$ is a Camina pair. Thus $Z(G) \subseteq [x, G]$ for all $x \in G - Z(G)$ and hence $\text{Aut}_z(G) \leq \text{Aut}_c(G)$. Since $|G/Z(G)| = p^4$ and $\text{cl}(G/Z(G)) = 2$, $|Z(\text{Inn}(G))| = p^2$ and thus $|\text{Aut}_c(G)| = p^5 > |\text{Inn}(G)|$ by Lemma 2.1. This proves the theorem. \square

As a consequence of Theorem 2.3, we can now obtain the following results of Yadav (§5 of [12]) and Kalra and Gumber (Theorem 4.2 of [7]). In [6], the groups of order p^5 , where p is an odd prime, are divided into ten isoclinism families; and in [4], the groups of order 32 are divided into eight isoclinism families. The isoclinism families appearing in Corollaries 2.4 and 2.5 are respectively from [6] and [4]. The i -th family is denoted as Φ_i . We would like to remark here that the derived groups of all the groups in the tenth family of [6] are elementary abelian for $p \geq 5$, but, for $p = 3$, the derived groups are not elementary abelian because $|\alpha_2| = 9$. It follows that, for $p = 3$, the groups $H_1 = \Phi_{10}(2111)a_0$, $H_2 = \Phi_{10}(2111)a_1$ and $H = \Phi_{10}(1^5)$ are not in the tenth family.

COROLLARY 2.4

Let G be a finite p -group of order p^5 , where p is an odd prime. Then $\text{Out}_c(G) \neq 1$ if and only if G is isomorphic to one of the groups in Φ_7 or one of the groups in Φ_{10} for $p \geq 5$ or to H , H_1 or H_2 .

Proof. If G is any group from the first six families, then either $\text{cl}(G) < 3$ or $|Z(G)| > p$. There are two isoclinism families Φ_7 and Φ_8 consisting of groups of class 3; and there are two isoclinism families Φ_9 and Φ_{10} consisting of groups of class 4. The only group in the eighth family is $\Phi_8(32)$ with $d(\Phi_8(32)) = 2$. Any group G in the seventh family is generated by α, α_1, β , and it is easy to see that the p -th power of any of these generators is either 1 or is in G' . It thus follows that $|\Phi(G)| = |G'| = p^2$ and consequently $d(G) = 3$. Any group G in the ninth family is minimally generated by α and α_1 with abelian commutator subgroup $G' = \langle [\alpha_1, \alpha], \gamma_3(G) \rangle = \langle \alpha_2, \gamma_3(G) \rangle$ and $\gamma_3(G) = \langle [\alpha_1, \alpha_2], [\alpha, \alpha_2], Z(G) \rangle = \langle \alpha_3^{-1}, Z(G) \rangle$. Thus α_1 commutes with G' and hence $|\alpha_1^G| = p$. It is easy to see that any element g of G is of the form $g' \alpha_1^k \alpha^j$, where $0 \leq j, k \leq p-1$ and $g' \in G'$, and hence $[\alpha_1, g] = [\alpha_1, g' \alpha_1^k \alpha^j] = [\alpha_1, \alpha^j] \in G' - \gamma_3(G)$. It follows that $Z(G)$ is not contained in $[x, G]$ for all $x \in G - G'$. Let G be any group in the tenth family. Any element $g \in G - G'$ is of the form $g = g' \alpha_1^l \alpha^m$, where

$0 \leq l, m \leq p - 1$ and $g' \in G'$. If $m \neq 0$, then $[g, \alpha_3] = [\alpha^m, \alpha_3] \in Z(G)$. Let $m = 0$ and $l \neq 0$. It is easy to see, by induction, that $[\alpha_1^l, \alpha_2] = [\alpha_1, \alpha_2]^l z_1 z_2 \dots z_{l-1}$, where $z_1, z_2, \dots, z_{l-1} \in Z(G)$. Then $[g, \alpha_2] = [g' \alpha_1^l, \alpha_2] = [\alpha_1^l, \alpha_2] = [\alpha_1, \alpha_2]^l \in Z(G)$, because $[\alpha_1, \alpha_2] \in Z(G)$. It follows that $Z(G) \subseteq [x, G]$ for all $x \in G - G'$. \square

There are, in all, fifty one groups of order 32. Sag and Wamsley [10] have given minimal presentations of these groups. As mentioned in [10], the groups are in the same order in [4] and [10]. We denote the i -th group as G_i .

COROLLARY 2.5

Let G be a finite group of order 32. Then $\text{Out}_c(G) \neq 1$ if and only if either G is isomorphic to G_{44} or isomorphic to G_{45} .

Proof. First forty three groups are divided into first five families. The families Φ_1, Φ_2, Φ_4 and Φ_5 contain groups of class ≤ 2 . The third family contains ten groups $G_{23} - G_{32}$ of class 3, and each of these groups has center of order 4. The sixth family contains groups G_{44} and G_{45} . Both of these groups are of class 3, rank 3, and with centers of order 2. The seventh family contains groups $G_{46} - G_{48}$ of class 3 and rank 2. The last family contains 2-generated groups $G_{49} - G_{51}$ of maximal class. It is clear from [10] that in each of these groups, one generator, say x , is of order 16 and hence $|x^G| = 2$. If y is another generator, then $y^{-1}xy$ is respectively x^{15}, x^7 and x^{15} in the group G_{49}, G_{50} and G_{51} . The center of each of these groups is $\{1, x^8\}$. For any element g in these groups, if $[x, g] = x^8$, then $g^{-1}xg = x^9$, which is not so.

Acknowledgement

The research of the second author was supported by UGC under the Research Award Scheme.

References

- [1] Adney J E and Yen T, Automorphisms of a p -group, *Illinois J. Math.* **9** (1965) 137–143
- [2] Burnside W, Theory of groups of finite order, 2nd ed. (1955) (Dover Publication, Inc.), Reprint of the 2nd edition (Cambridge, 1911)
- [3] Burnside W, On the outer automorphisms of a group, *Proc. London Math. Soc.* **11** (1913) 40–42
- [4] Hall M Jr and Senior J K, The groups of order 2^n ($n \leq 6$) (1964) (New York: Macmillan)
- [5] Hertweck M, Contributions to the integral representation theory of groups, Habilitationsschrift (University of Stuttgart) (2004), available at <http://elib.unistuttgart.de/opus/volltexte/2004/1638>
- [6] James R, The groups of order p^6 (p an odd prime), *Math. Comp.* **34** (1980) 613–637
- [7] Kalra H and Gumber D, On equality of central and class preserving automorphisms of finite p -groups, *Indian J. Pure Appl. Math.* **44** (2013) 711–725
- [8] Kumar M and Vermani L R, Hasse principle for extra-special p -groups, *Proc. Japan Acad.* **76** (2000) 123–125
- [9] Kumar M and Vermani L R, Hasse principle for groups of order p^4 , *Proc. Japan Acad.* **77** (2001) 95–98

- [10] Sag T W and Wamsley J W, Minimal presentations for groups of order 2^n , $n \leq 6$, *J. Aust. Math. Soc.* **15** (1973) 461–469
- [11] Tandra H and Moran W, Flatness conditions on finite p -groups, *Comm. Algebra* **32** (2004) 2215–2224
- [12] Yadav M K, On automorphisms of some finite p -groups, *Proc. Indian Acad. Sci. (Math. Sci.)* **118** (2008) 1–11
- [13] Yadav M K, Class preserving automorphisms of finite p -groups – A Survey, *Groups St. Andrews, LMS Lecture Note Series 388 vol. 2* (2011) pp. 569–579

COMMUNICATING EDITOR: B V Rajarama Bhat