GLASNIK MATEMATIČKI
Vol. 51(71)(2016), 117 – 123

A NOTE ON AUTOMORPHISMS OF FINITE p-GROUPS

Gustavo A. Fernández-Alcober and Anitha Thillaisundaram

University of the Basque Country, Spain and Heinrich-Heine Universität, Germany

Abstract. Let G be a finite non-cyclic p-group of order at least p^3. If G has an abelian maximal subgroup, or if G has an elementary abelian centre with $C_G(Z(\Phi(G))) \neq \Phi(G)$, then $|G|$ divides $|\mathrm{Aut}(G)|$.

1. Introduction

From the 1970s, the question "Does every finite non-cyclic p-group G of order $|G| \geq p^3$ have $|G|$ dividing $|\mathrm{Aut}(G)|$?" began to take form. Observe that, if $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ denotes the group of outer automorphisms of G, this is equivalent to asking whether $|\mathrm{Out}(G)|$ divides $|Z(G)|$. Over the past forty years, this question was partially answered in the affirmative for specific families of p-groups, for instance p-abelian p-groups, p-groups of class 2, p-groups of maximal class, etc (see [12] for a fairly up-to-date list). This led many to believe that the complete answer might be yes, which is why the question was reformulated as a conjecture: "If G is a finite non-cyclic p-group with $|G| \geq p^3$, then $|G|$ divides $|\mathrm{Aut}(G)|$".

What is more, Eick ([4]) proved that all but finitely many 2-groups of a fixed coclass satisfy the conjecture. Couson ([2]) generalized this to p-groups for odd primes, but only to infinitely many p-groups of a fixed coclass. The coclass theory shed new light on the conjecture, and provided more evidence as to why it could be true. Looking at past efforts, it could also be said that

2010 *Mathematics Subject Classification.* 20D15, 20D45.

Key words and phrases. Finite p-groups, automorphisms.

The first author is supported by by the Spanish Government, grants MTM2011-28229-C02-02 and MTM2014-53810-C2-2-P, and by the Basque Government, grant IT753-13. The second author, who is funded by the Alexander von Humboldt Foundation, would like to thank the University of the Basque Country for its hospitality.

an underlying theme was cohomology, which hinted that the full conjecture might be settled using such means.

However, it came as a surprise that the conjecture is false. Very recently, González-Sánchez and Jaikin-Zapirain [7] disproved the conjecture using Lie methods, where the question was first translated into one for Lie algebras. The main idea was to use the examples of Lie algebras with derivation algebra of smaller dimension, from which they constructed a family of examples of p-groups with small automorphism group. We remark that these counter-examples are powerful and p-central, which means that $G' \leq G^p$ and $\Omega_1(G) \leq Z(G)$ respectively, if p is odd, and that $G' \leq G^4$ and $\Omega_2(G) \leq Z(G)$ respectively, if $p = 2$.

Now a new question may be formulated: which other finite non-cyclic p-groups G with $|G| \geq p^3$ have $|G|$ dividing $|\mathrm{Aut}(G)|$? In this short note, we prove that for G a finite non-cyclic p-group with $|G| \geq p^3$, if G has an abelian maximal subgroup, or if G has elementary abelian centre and $C_G(Z(\Phi(G))) \neq \Phi(G)$, then $|G|$ divides $|\mathrm{Aut}(G)|$. The latter is a partial generalization of Gaschütz' result [6] that $|G|$ divides $|\mathrm{Aut}(G)|$ when the centre has order p.

Notation. We use standard notation in group theory. All groups are assumed to be finite and p always stands for a prime number. For M, N normal subgroups in G, we set $\mathrm{Aut}_N^M(G)$ to be the subgroup of automorphisms of G that centralize G/M and N, and let $\mathrm{Out}_N^M(G)$ be its corresponding image in $\mathrm{Out}(G)$. When M or N is $Z(G)$, we write just Z for conciseness. On the other hand, if G is a finite p-group then $\Omega_1(G)$ denotes the subgroup generated by all elements of G of order p.

2. An abelian maximal subgroup

Let G be a finite p-group with an abelian maximal subgroup A. We collect here a few well-known results (see [9, Lemma 4.6 and its proof]).

Theorem 2.1. *Let G be a group having an abelian normal subgroup A such that the quotient $G/A = \langle gA \rangle$, with $g \in G$, is cyclic.*

Then (i) $G' = \{[a, g] \mid a \in A\}$ and (ii) $|G'| = |A : A \cap Z(G)|$.

Corollary 2.2. *Let G be a finite non-abelian p-group having an abelian maximal subgroup. Then $|G : Z(G)| = p|G'|$.*

In [13], Webb uses the following approach to find non-inner automorphisms of p-power order, which we will use in the forthcoming theorem. For a maximal subgroup M of G, we first define two homomorphisms on $Z(M)$. Let $g \in G$ be such that $G/M = \langle gM \rangle$, then

$$\begin{aligned} \tau : m &\mapsto g^{-p}(gm)^p = m^{g^{p-1}+\ldots+g+1}, \\ \gamma : m &\mapsto [m, g] = m^{g-1}, \end{aligned}$$

for all $m \in Z(M)$.

We have $\operatorname{im}\gamma \subseteq \ker\tau$ and $\operatorname{im}\tau \subseteq \ker\gamma = Z(G) \cap M$.

COROLLARY 2.3 ([13]). *Let G be a finite non-abelian p-group and M a maximal subgroup of G containing $Z(G)$. Then G has a non-inner automorphism of p-power order inducing the identity on G/M and M if and only if* $\operatorname{im}\tau \neq \ker\gamma$.

We remark that the proof of the above also tells us that if $\operatorname{im}\tau \neq \ker\gamma$, then $|\mathrm{Out}_M^M(G)| = |\ker\gamma|/|\operatorname{im}\tau|$.

THEOREM 2.4. *Let G be a finite non-cyclic p-group with $|G| \geq p^3$ and with an abelian maximal subgroup A. Then $|G|$ divides $|\mathrm{Aut}(G)|$.*

PROOF. We work with the subgroup $\mathrm{Aut}^Z(G)$ of central automorphisms in $\mathrm{Aut}(G)$. Now

$$|\mathrm{Aut}^Z(G)\mathrm{Inn}(G)| = \frac{|\mathrm{Aut}^Z(G)| \cdot |\mathrm{Inn}(G)|}{|\mathrm{Aut}^Z(G) \cap \mathrm{Inn}(G)|} = \frac{|\mathrm{Aut}^Z(G)| \cdot |G/Z(G)|}{|Z_2(G)/Z(G)|}$$

and hence it suffices to show that $|\mathrm{Aut}^Z(G)| \geq |Z_2(G)|$.

According to Otto [11], when G is the direct product of an abelian p-group H and a p-group K having no abelian direct factor, then one has $|H| \cdot |\mathrm{Aut}(K)|_p$ divides $|\mathrm{Aut}(G)|$. Hence, we may assume that G has no abelian direct factor. It then follows by Adney and Yen [1] that $|\mathrm{Aut}^Z(G)| = |\mathrm{Hom}(G/G', Z(G))|$.

By Corollary 2.2, we have $|G : Z(G)| = p|G'|$ and equally,

$$|G : G'| = p|Z(G)|. \tag{2.1}$$

Let $H = G/Z(G)$. Then $A/Z(G)$ is an abelian maximal subgroup of H. Applying Corollary 2.2 to H yields

$$|H : H'| = p|Z(H)|,$$

so

$$|G : G'Z(G)| = p|Z_2(G) : Z(G)|.$$

Hence

$$|Z_2(G)| = \frac{1}{p} \cdot |G' \cap Z(G)| \cdot |G : G'|. \tag{2.2}$$

Combining this with (2.1) gives

$$|Z_2(G)| = |G' \cap Z(G)| \cdot |Z(G)|. \tag{2.3}$$

Next we have $G' = \{[a, g] \mid a \in A\}$ by Theorem 2.1. By Webb's construction, we know that $\operatorname{im}\gamma \subseteq \ker\tau$ and here $\operatorname{im}\gamma = [A, g] = G'$. Now for $a \in A$ and g as in Theorem 2.1, we have

$$[a, g]^{g^{p-1}+\ldots+g+1} = 1.$$

We claim that $\exp(G' \cap Z(G)) = p$. For, if $[a, g] \in Z(G)$, then $[a, g]^g = [a, g]$. Consequently,

$$1 = [a, g]^{g^{p-1}+\ldots+g+1} = [a, g]^p$$

and thus $o([a, g]) \leq p$.

Clearly the minimal number $d := d(G)$ of generators of G is at least 2. In order to proceed, we divide into the following two cases: (A) $\exp(G/G') \geq \exp Z(G)$, and (B) $\exp(G/G') \leq \exp Z(G)$.

Case (A): Suppose $\exp(G/G') \geq \exp Z(G)$. We express G/G' as

$$G/G' = \langle g_1 G' \rangle \times \langle g_2 G' \rangle \times \ldots \times \langle g_d G' \rangle,$$

where $o(g_1 G') = \exp(G/G')$ and by assumption $d \geq 2$.

We consider homomorphisms from G/G' to $Z(G)$. The element $g_1 G'$ may be mapped to any element of $Z(G)$, and $g_2 G'$ may be mapped to any element of $G' \cap Z(G)$, which is of exponent p.

Thus, with the aid of (2.3),

$$|\mathrm{Hom}(G/G', Z(G))| \geq |Z(G)| \cdot |G' \cap Z(G)| = |Z_2(G)|.$$

Case (B): Suppose $\exp(G/G') \leq \exp Z(G)$. Similarly we express $Z(G)$ as

$$Z(G) = \langle z_1 \rangle \times \langle z_2 \rangle \times \ldots \times \langle z_r \rangle$$

where $r = d(Z(G))$ and $o(z_1) = \exp Z(G)$.

We consider two families of homomorphisms from G/G' to $Z(G)$. First,

$$\begin{aligned} G/G' &\to Z(G) \\ g_i G' &\mapsto z_1^{b_i} \end{aligned}$$

for $1 \leq i \leq d$, where b_i is such that $o(z_1^{b_i})$ divides $o(g_i G')$. This gives rise to $|G/G'|$ homomorphisms.

Next, we consider all homomorphisms from G/G' to $Z(G)$ where each element $g_i G'$ is mapped to any element of order p in $\langle z_2 \rangle \times \ldots \times \langle z_r \rangle$. This gives

$$(p^{r-1})^d \geq p^{r-1} = \frac{|\Omega_1(Z(G))|}{p} \geq \frac{|G' \cap Z(G)|}{p}$$

different homomorphisms.

Multiplying both together and then using (2.2), we obtain

$$|\mathrm{Hom}(G/G', Z(G))| \geq \frac{|G/G'| \cdot |G' \cap Z(G)|}{p} = |Z_2(G)|.$$

□

3. Elementary abelian centre

Let G be a finite p-group with elementary abelian centre. In order to prove that $|G|$ divides $|\mathrm{Aut}(G)|$, we may assume, upon consultation of [5] and the final remarks in [8], that $Z(G) < \Phi(G)$. One of the following three cases exclusively occurs.

Case 1. $Z(M) = Z(G)$ for some maximal subgroup M of G.

Case 2. $Z(M) \supset Z(G)$ for all maximal subgroups M of G. Then either

(A) $C_G(Z(\Phi(G))) \neq \Phi(G)$; or
(B) $C_G(Z(\Phi(G))) = \Phi(G)$.

The main result of this section is to show that if G is a finite p-group with elementary abelian centre and not in Case 2B, then $|G|$ divides $|\mathrm{Aut}(G)|$.

With regard to Case 2B, we would also like to mention another long-standing conjecture for finite p-groups: does there always exist a non-inner automorphism of order p? The case 2B is the only remaining case for this conjecture (see [3]).

First we deal with Case 1.

Lemma 3.1 ([10, Lemma 2.1(b)]). *Suppose M is a maximal subgroup of G. If $Z(M) \subseteq Z(G)$ then $\mathrm{Aut}_M^Z(G)$ is a non-trivial elementary abelian p-group such that $\mathrm{Aut}_M^Z(G) \cap \mathrm{Inn}(G) = 1$.*

We comment that the proof of this result in [10] tells us that

$$|\mathrm{Aut}_M^Z(G)| = |\mathrm{Hom}(G/M, Z(M))| = |\Omega_1(Z(M))|.$$

Lemma 3.2. *Let G be a finite p-group with elementary abelian centre. Suppose that $Z(M) = Z(G)$ for some maximal subgroup M of G. Then $|G|$ divides $|\mathrm{Aut}(G)|$.*

Proof. Using Lemma 3.1 and the above comment, it follows that

$$|\mathrm{Out}(G)|_p \geq |\mathrm{Aut}_M^Z(G)| = |Z(G)|.$$

Hence $|G|$ divides $|\mathrm{Aut}(G)|$ as required. □

Next, suppose G is as in Case 2(A). We will need the following.

Theorem 3.3 ([13]). *Let G be a finite non-abelian p-group. Then p divides the order of $\mathrm{Out}_Z(G)$.*

Now we present our result.

Proposition 3.4. *Let G be a finite p-group with elementary abelian centre, such that $C_G(Z(\Phi(G))) \neq \Phi(G)$ and $Z(M) \supset Z(G)$ for all maximal subgroups M of G. Then $|G|$ divides $|\mathrm{Aut}(G)|$.*

PROOF. By Müller [10, proof of Lemma 2.2], there exist maximal subgroups M and N such that $G = Z(M)N$ and $Z(G) = Z(M) \cap N$. Write $G/M = \langle gM \rangle$ for some $g \in G$, and consider the homomorphism

$$\begin{array}{rccc} \tau_M & : & Z(M) & \longrightarrow & Z(M) \\ & & m & \longmapsto & g^{-p}(gm)^p = m^{g^{p-1}+\cdots+g+1}. \end{array}$$

Since

$$\frac{Z(M)}{Z(G)} = \frac{Z(M)}{Z(M) \cap N} \cong \frac{Z(M)N}{N} = \frac{G}{N}$$

and $Z(G) \subseteq \ker \tau_M$, it follows that $|\mathrm{im}\ \tau_M| \leq p$. If $\mathrm{im}\ \tau_M = 1$, the remark after Corollary 2.3 implies that $|\mathrm{Out}_M^M(G)| = |Z(G)|$ and we are done. Hence we assume that $\mathrm{im}\ \tau_M \cong C_p$. If $Z(G) \cong C_p$, then $|G|$ divides $|\mathrm{Aut}(G)|$ by Gaschütz ([6]). So we may assume that $|Z(G)| > p$. Again by the same remark, we have $|\mathrm{Out}_M^M(G)| = |Z(G)|/p$.

By [10, Lemma 2.2], it follows that G is a central product of subgroups R and S, where $R/Z(R) \cong C_p \times C_p$ and $Z(R) = Z(G) = Z(S) = R \cap S$. Furthermore, $R = Z(M)Z(N)$ and $S = M \cap N = C_G(R)$.

By Theorem 3.3, there exists a non-inner automorphism $\beta \in \mathrm{Aut}_Z(S)$ of p-power order. As observed by Müller in [10, Section 3], the automorphism β extends uniquely to some non-inner $\gamma \in \mathrm{Aut}_Z(G)$ with trivial action on R.

Certainly γ does not act trivially on $M \cap N = S$, so $\gamma \notin \mathrm{Aut}_M(G)$. Let $\overline{\gamma}$ be the image of γ in $\mathrm{Out}(G)$. We now show that $\overline{\gamma} \notin \mathrm{Out}_M^M(G)$. On the contrary, suppose that $\gamma = \rho.\iota$ where $\rho \in \mathrm{Aut}_M^M(G)$ and $\iota \in \mathrm{Inn}(G)$. As $S \leq M$, we have $\beta(s) = \gamma(s) = \rho(s)^x = s^x$ for all $s \in S$ and a fixed $x \in G$. Writing $x = rs'$ for some $r \in R$, $s' \in S$ and recalling that $S = C_G(R)$, we have $\beta(s) = s^{s'}$. This implies that $\beta \in \mathrm{Inn}(S)$, a contradiction. Thus

$$|\mathrm{Out}(G)|_p \geq |\langle \overline{\gamma}, \mathrm{Out}_M^M(G) \rangle| \geq |Z(G)|.$$

It follows that $|G|$ divides $|\mathrm{Aut}(G)|$. □

ACKNOWLEDGEMENTS.

The authors are grateful to the various people who helped to read and improve this manuscript.

REFERENCES

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

[2] M. Couson, On the character degrees and automorphism groups of finite p-groups by coclass, PhD Thesis, Technische Universität Braunschweig, Germany, 2013.

[3] M. Deaconescu and G. Silberberg, *Noninner automorphisms of order p of finite p-groups*, J. Algebra **250** (2002), 283-287.

[4] B. Eick, *Automorphism groups of 2-groups*, J. Algebra **300** (2006), 91–101.

[5] R. Faudree, *A note on the automorphism group of a p-group*, Proc. Amer. Math. Soc. **19** (1968), 1379–1382.

[6] W. Gaschütz, *Nichtabelsche p-Gruppen besitzen äussere p-Automorphismen (German)*, J. Algebra **4** (1966), 1–2.
[7] J. González-Sánchez and A. Jaikin-Zaipirain, *Finite p-groups with small automorphism group*, Forum Math. Sigma **3** (2015), e7, 11 pp.
[8] K. G. Hummel, *The order of the automorphism group of a central product*, Proc. Amer. Math. Soc. **47** (1975), 37–40.
[9] I. M. Isaacs, Finite group theory, Amer. Math. Soc., Providence, 2008.
[10] O. Müller, *On p-automorphisms of finite p-groups*, Arch. Math. (Basel) **32** (1979), 533–538.
[11] A. D. Otto, *Central automorphisms of a finite p-group*, Trans. Amer. Math. Soc. **125** (1966), 280–287.
[12] A. Thillaisundaram, *The automorphism group for p-central p-groups*, Int. J. Group Theory **1** (2012), 59–71.
[13] U. H. M. Webb, *An elementary proof of Gaschütz' theorem*, Arch. Math. (Basel) **35** (1980), 23–26.
[14] M. K. Yadav, *On automorphisms of finite p-groups*, J. Group Theory **10** (6) (2007), 859–866.

G. A. Fernández-Alcober
Department of Mathematics
University of the Basque Country UPV/EHU
48080 Bilbao
Spain
E-mail: gustavo.fernandez@ehu.eus

A. Thillaisundaram
Mathematisches Institut
Heinrich-Heine Universität
40225 Düsseldorf
Germany
E-mail: anitha.t@cantab.net

Received: 26.10.2015.