Jurnal Teknologi

Full paper

Verification of an Old Conjecture on Nonabelian 2-generated Groups of Order p^3

Yasamin Barakat[a,b], Nor Haniza Sarmin[c*]

[a]Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Malaysia
[b]Islamic Azad University, Ahvaz Branch, Ahvaz, Iran
[c]Department of Mathematical Sciences, Faculty of Science and Ibnu Sina Institute for Fundamental Science Studies, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Malaysia

*Corresponding author: nhs@utm.my

Article history

Received :30 May 2012
Received in revised form :28 July 2012
Accepted :13 August 2012

Abstract

A longstanding conjecture in group theory states: "Every finite non-abelian p-group possesses at least a non-inner automorphism of order p", where p is a prime number. Recently, an updated classification of 2-generated p-groups of nilpotency class two has been published. Using this classification, we prove the verification of this conjecture for 2-generated groups of order p^3.

Keywords: Automorphism; non-inner; 2-generated; p-group; nilpotency class two

1.0 INTRODUCTION

Let H and K be two arbitrary subgroups of a group G. Then $[H,K]=\langle\{h^{-1}k^{-1}hk : h\in H, k\in K\}\rangle$ is a subgroup of G, and $G'=[G,G]$ is called the *commutator subgroup* of G. A group G is *nilpotent of class two* if and only if $[G',G]=\{1\}$ or $G'\leq Z(G)$. Furthermore, a group G is called a *p-group* if the order of every element of G is a power of p. If G is a finite p-group, then $|G|=p^n$. The group of isomorphisms on G to itself is called *automorphism group* of G, and denoted by $Aut(G)$. Let $g\in G$, then the map $i_g(x)=g^{-1}xg$ for all $x\in G$ is an automorphism on G. For all g in G, the set of i_g's forms a normal subgroup of $Aut(G)$, called *inner group*, and denoted as $Inn(G)$.

Throughout this paper we set p to be a prime number. In 1965, Liebeck showed that if G is a finite p-group of nilpotency class two, then G has non-inner p-automorphisms [1]. A year later, Gaschütz found a similar result for all finite non-abelian p-groups [2]. By a p-automorphism, it is meant an automorphism of order p^m for some positive integer m. Eventually, a conjecture appeared, which concerned with the existence of non-inner automorphisms of order exactly p for finite non-abelian p-groups as given in the following:

Conjecture 1.1 [3]
Every finite non-abelian p-group possesses at least a noninner automorphism of order exactly p.

Since the year of appearance of the conjecture, many researchers tried to show the verification of the conjecture considering a particular subcategory of finite non-abelian p-groups. For instance, refer to [4, 5, 6, 7]. In this study, we consider to show the conjecture verification for 2-generated groups of order p^3.

2.0 PRELIMINARY RESULTS

Some useful theorems and lemmas are provided through this section. For undefined terms and notations, kindly refer to [8].

Lemma 2.1 [8]
Let G be a group of nilpotency class two. For any $x,y,z\in G$ and $n\in\mathbb{Z}$, the following equations hold in G:

i. $[x,yz]=[x,y][x,z]$,
ii. $[xy,z]=[x,z][y,z]$,
iii. $[x^n,y]=[x,y]^n$,
iv. $(xy)^n=x^ny^n[y,x]^{\frac{n(n-1)}{2}}$.

Since Lemma 2.1 is used in each sequence of operations several times, we use it without referring.

Lemma 2.2 [9]
Let $G=\langle a,b\rangle$ be a non-abelian 2-generated group of nilpotency class two, then $G'=\langle[a,b]\rangle$. If G' is a finite group of order m, then $\langle a\rangle\cap Z(G)=\langle a^m\rangle$ and $\langle b\rangle\cap Z(G)=\langle b^m\rangle$.

The following theorem classifies all finite 2-generated p-groups of nilpotency class two. We use this classification to study their automorphism groups.

Theorem 2.3 [10, 11]
Let p be a prime and $n > 2$ a positive integer. Every 2-generated p-group of class exactly two of order p^n, corresponds to an ordered 5-tuple of integers $(\alpha, \beta, \gamma; \rho, \sigma)$, such that:

i. $\alpha \geq \beta \geq \gamma \geq 1$,
ii. $\alpha + \beta + \gamma = n$,
iii. $0 \leq \rho \leq \gamma$ and $0 \leq \sigma \leq \gamma$;

where $(\alpha, \beta, \gamma; \rho, \sigma)$ corresponds to the group presented by
$G = \langle a, b \colon [a,b]^{p^\gamma} = [a,b,a] = [a,b,b] = 1,\ a^{p^\alpha} = [a,b]^{p^\rho},$
bpβ=a,bpσ.
Moreover,
(1) If $\alpha > \beta$, then G is isomorphic to:

a) $(\alpha, \beta, \gamma; \rho, \gamma)$ when $\rho \leq \sigma$,
b) $(\alpha, \beta, \gamma; \gamma, \sigma)$ when $0 \leq \sigma < \sigma + \alpha - \beta \leq \rho$ *or* $\sigma < \rho = \gamma$,
c) $(\alpha, \beta, \gamma; \rho, \sigma)$ when $0 \leq \sigma < \rho < min\,(\gamma, \sigma + \alpha - \beta)$.

(2) If $\alpha = \beta > \gamma$, or $\alpha = \beta = \gamma$ and $p > 2$, then G is isomorphic to $(\alpha, \beta, \gamma; min\,(\rho, \sigma), \gamma)$.
(3) If $\alpha = \beta = \gamma$ and $p = 2$, then G is isomorphic to:

a) $(\alpha, \beta, \gamma; min\,(\rho, \sigma), \gamma)$ when $0 \leq min(\rho, \sigma) < \gamma - 1$,
b) $(\alpha, \beta, \gamma; \gamma - 1, \gamma - 1)$ when $\rho = \sigma = \gamma - 1$,
c) $(\alpha, \beta, \gamma; \gamma, \gamma)$ when $min(\rho, \sigma) \geq \gamma - 1$ and $max(\rho, \sigma) = \gamma$.

The groups listed in (1)(a) – (3)(c) are pairwise non-isomorphic.

Lemma 2.4 [8]
Let G be a non-abelian group of order p^3. Then $G' = Z(G)$.

Lemma 2.4 shows that every non-abelian group of order p^3 is a nilpotent group of class two. Thus, in this study we have $n = 3$. Applying Theorem 2.3[(i)-(iii)] we found that $\alpha = \beta = \gamma = 1$ and $0 \leq \rho, \sigma \leq 1$.

Proposition 2.5 Let $G = \langle a, b \rangle$ be a 2-generated group of class exactly two. If G' is a finite subgroup of order m, then
$Inn(G) = \{\varphi : G \to G \mid \varphi(a) = a[a,b]^i, \varphi(b) = b[a,b]^j, 0 \leq i, j < m\}$.

Proof. Suppose that the right hand side in the given equivalency is denoted as A. Consider $\varphi \in A$, we have to show that φ can be written of the form i_g for some $g \in G$. Let $g = a^{-j} b^i$. Then, since $G' \leq Z(G)$,

$$i_g(a) = g^{-1} a g = b^{-i} a^j a a^{-j} b^i = b^{-i} a b^i = a[a,b]^i = \varphi(a)$$

and

$$i_g(b) = b^{-i} a^j b a^{-j} b^i = b^{-i}\left(a^j b a^{-j} b^{-1}\right) b^{i+1} = b[a^{-j}, b^{-1}] = b[a,b]^j = \varphi(b).$$

However, a and b are the generators of G, thus we have $\varphi = i_g \in Inn(G)$.
Also, for every i_g we have $i_g(a) = g^{-1} a g = a[a,g]$ and $i_g(b) = g^{-1} b g = b[b,g]$. By Lemma 2.2, $[a,g], [b,g] \in G' = \langle [a,b] \rangle$. Thus $[a,g] = [a,b]^i$ and $[b,g] = [a,b]^j$ for some $0 \leq i, j < m$. This shows that $i_g \in A$.

The following theorem will help us to show that a particular map is an automorphism.

Theorem 2.6 (Von Dyck's Theorem) [12]
Let G be a group with presentation $\langle X \mid R \rangle$. Suppose that H is a group generated by a subset Y and there is a bijection map $f \colon X \to Y$ such that if $r(x_1, \ldots, x_n) \in R$, then $(f(x_1), \ldots, f(x_n)) = 1 \in H$. Then there exists a group epimorphism $\bar{f} \colon G \to H$ such that $\bar{f}(x) = f(x)$, for any $x \in X$.

Remark 2.7 Let G be one of those groups listed in Theorem 2.3. According to Von Dyck's Theorem, every map $\varphi : \{a, b\} \to G$ which satisfies the following conditions, extends to an automorphism on G.

1) $G = \langle \varphi(a), \varphi(b) \rangle$.
2) $[\varphi(a), \varphi(b)]^{p^\gamma} = [\varphi(a), \varphi(b), \varphi(a)] = [\varphi(a), \varphi(b), \varphi(b)] = 1$.
3) $[\varphi(a)]^{p^\alpha} = [\varphi(a), \varphi(b)]^{p^\rho}$.
4) $[\varphi(b)]^{p^\beta} = [\varphi(a), \varphi(b)]^{p^\sigma}$.

3.0 MAIN RESULTS

In this study we consider to find at least one non-inner automorphism of order p on 2-generated groups of order p^3, to show that Conjecture 1.1 verifies for these kind of groups. As it is discussed earlier, for 2-generated non-abelian groups of order p^3 we have $\alpha = \beta = \gamma = 1$. If $p > 2$, then based on Theorem 2.3-(2), these groups are classified as follows:

1) $(\alpha, \beta, \gamma; \rho, \gamma) = (1, 1, 1;\ 0, 1)$ if $min(\rho, \sigma) = 0$.
2) $(\alpha, \beta, \gamma; \rho, \gamma) = (1, 1, 1; 1, 1)$ if $min(\rho, \sigma) = 1$.

If $p = 2$, then these groups are isomorphic to either dihedral group, D_4; or Quaternion, Q [8]. It can be shown that in this case $[p = 2, n = 3]$, groups listed in Theorem 2.3-(3b) are of the form $(1, 1, 1;\ 0, 0)$ and are isomorphic to Q. Also, groups listed in Theorem 2.3-[(3a),(3c)] are of forms $(1, 1, 1;\ 0, 1)$ and $(1, 1, 1;\ 1, 1)$, which are both isomorphic to D_4 [13].

We separate our main theorem in two parts, namely for $p > 2$ and $p = 2$.

Theorem 3.1 Let G be a nonabelian 2-generated group of order p^3. Then G has at least one non-inner automorphism of order p, where p is an odd prime number.

Proof. According to Theorem 2.3-(2) and our earlier discussion, these groups are isomorphic to either
$\langle a, b : a^p = [a,b], b^p = [a,b]^p = [a,b,a] = [a,b,b] = 1 \rangle$,
or
$\langle a, b : a^p = b^p = [a,b]^p = [a,b,a] = [a,b,b] = 1 \rangle$.

Anyway, in both cases we have $b^p = [a,b]^p = 1$. Hence, $\langle b \rangle \cap Z(G) = \langle b \rangle \cap G' = \{1\}$. Now, we are ready to define our desired automorphism. Consider

$$\begin{cases} \varphi \colon \{a, b\} \to G \\ \varphi(a) = ab^{p-1} \\ \varphi(b) = b. \end{cases}$$

We use Remark 2.7 to show that φ extends to an automorphism on G, which is exactly of order p. Since G is generated by $\{a, b\}$ it is enough to show that $\{\varphi(a), \varphi(b)\}$ produces $\{a, b\}$. However, $\varphi(b) = b$ and $\varphi(a)\varphi(b) = ab^{p-1} b = a$. Also, $[\varphi(a), \varphi(b)] = [ab^{p-1}, b] = [a,b] \in Z(G)$. Thus $[\varphi(a), \varphi(b)]^p = [\varphi(a), \varphi(b), \varphi(a)] = [\varphi(a), \varphi(b), \varphi(b)] = 1$. In addition,

$$[\varphi(a)]^p = (ab^{p-1})^p = a^p b^{p(p-1)} [b,a]^{p(p-1)\left(\frac{p-1}{2}\right)} = a^p = [a,b]^{p^\rho} = [\varphi(a), \varphi(b)]^{p^\rho}.$$

Since $\varphi(b) = b$, Remark 2.7-(4) obviously holds. Therefore, φ is extendable to an automorphism on G, which is non-inner by Proposition 2.5, for $b^{p-1} \notin G'$. It remains to show that φ is of

order p. Since, $\varphi(b) = b$, it is enough to study $\varphi(a)$. We use induction on m to show that $\varphi^m(a) = ab^{m(p-1)}$. If $m = 1$, then obviously it holds. Let it be true for m. To show it is true for $m+1$, we have $\varphi^{m+1}(a) = \varphi(ab^{m(p-1)}) = ab^{p-1}b^{m(p-1)} = ab^{[(m+1)(p-1)]}$.
However, the order of b is p, this implies that $\varphi^p(a) = a$ and $\varphi^m(a) \neq 1$, if $m < p$; or $|\varphi| = p$. □

Theorem 3.2 Both the Quaternion and Dihedral groups of order eight have at least one non-inner automorphism of order two.

Proof. It is known that $Q = \{a, b\colon a^4 = 1, a^2 = b^2 = [a,b], b^{-1}ab = a^3\}$ [8]. We show that the following map is as desired.

$$\begin{cases} \varphi\colon \{a,b\} \longrightarrow Q \\ \varphi(a) = ab \\ \varphi(b) = b^{-1}. \end{cases}$$

We have $\varphi(a)\varphi(b) = a$, so then $\{\varphi(a), \varphi(b)\}$ generates G. Also, $b^{-1} = b^3$ implies that $[\varphi(a), \varphi(b)] = [a, b^3] = [a,b]^3 = [a,b]$, which makes φ satisfying Remark 2.7-(2). Additionally, $(\varphi(a))^2 = (ab)^2 = a^2\,b^2\,[b,a] = [a,b] = [\varphi(a), \varphi(b)]$. Note that in a group, every element is of the same order of its inverse. Thus, φ extends to a noninner automorphism, for $b \notin G'$. Finally, φ is of order two since
$\varphi^2(a) = \varphi(\varphi(a)) = \varphi(ab) = (ab)b^{-1} = a$; and
$\varphi^2(b) = \varphi(\varphi(b)) = \varphi(b^{-1}) = b$.

Now, consider $D_4 = \{a, b\colon a^4 = b^2 = 1, a^2 = [a,b], b^{-1}ab = a^3\}$ [8]. To show that Conjecture 1.1 is verified for dihedral group, we define θ as follows:

$$\begin{cases} \theta\colon \{a,b\} \longrightarrow D_4 \\ \theta(a) = a^{-1} \\ \theta(b) = ba. \end{cases}$$

By using similar arguments, we have $\theta(b)\theta(a) = b$ and $[\theta(a), \theta(b)] = [a^3, b] = [a,b]^3 = [a,b]$. Thus, our defined θ satisfies in Remark 2.7-(1),(2). For the last part, we have $(\theta(b))^2 = (ba)^2 = b^2a^2\,[a,b] = 1 = [\theta(a), \theta(b)]^2$. The fact that $a \notin G'$ implies that θ is a non-inner automorphism on G. The following equivalences show that θ is of order two :
$\theta^2(a) = \theta(\theta(a)) = \theta(a^{-1}) = a$;
$\theta^2(b) = \theta(\theta(b)) = \theta(ba) = (ba)a^{-1} = b$.
This ends our proof. □

4.0 RESULTS AND DISCUSSION

In this study, the verification of an old conjecture in group theory has been shown for every non-abelian 2-generated group of order p^3. In other words, it is proved that each one of these groups possesses at least one non-inner automorphism of order p, where p is a prime number.

Acknowledgement

The first author would like to thank Universiti Teknologi Malaysia for its financial support via allocating Institutional Doctoral Fellowship (IDF).

References

[1] Liebeck, H. 1965. Outer Automorphisms in Nilpotent p-Groups of Class 2. *J. London Math. Soc.* 40: 268–275.
[2] Gaschütz, W. 1966. Nichtabelsche p-Gruppen Besitzen Aussere p-automorphismen. *J. Algebra.* 4: 1–4.
[3] Mazurov, V. D. and E. I. Khukhro (Eds.). 2006. *Unsolved Problems in Group Theory*. Novosibirsk: The Kourovka Notebook, Russian Academy of Sciences, Siberian Division, Institute of Mathematics.
[4] Abdollahi, A. 2007. Finite p-Groups of Class 2 Have Noninner Automorphisms of Order p. *J. Algebra.* 312: 876–879.
[5] Curran, M. J., and D. J. McCaughan. 2001. Central Automorphisms that Are Almost Inner. *Comm. Algebra.* 29(5): 2081–2087.
[6] Deaconescu, M., and G. Silberberg. 2002. Noninner Automorphisms of Order p of Finite p −Groups. *J. Algebra.* 250: 283–287.
[7] Attar, M. S. 2007. On Central Automorphisms that Fix the Centre Elementwise. *Arch. Math.* 89: 296–297.
[8] Rotman, J. J. 1994. *The Theory of Groups: An Introduction.* Fourth Ed. New York: Springer-Verlag, Inc.
[9] Kappe, L. C., M. P. Visscher, and N. H. Sarmin. 1999. Two-generator Two-groups of Class Two and Their Nonabelian Tensor Squares. *Glasgow Math. J.* 41: 417–430.
[10] Ahmad, A., A. Magidin, and R. F. Morse. Two Generator p-Groups of Nilpotency Class 2 and Their Conjugacy Classes. Retrieved on February 20, 2011 from *http://www.ucs.louisiana.edu/avm1260/preprints/ãmmpaper.pdf.*
[11] Ahmad, A., A. Magidin, and R. F. Morse. Two Generator p-Groups of Nilpotency Class 2 and Their Conjugacy Classes. To be appear in *Publicationes Mathematicae Debrecen.*
[12] Robinson, J. S. 1993. *A Course in the Theory of Groups.* New York: Springer-Verlag, Inc.
[13] Barakat, Y. and N. H. Sarmin. 2011. *Noninner p-Automorphisms of Nonabelian 2-Generated Groups of order p^3.* Technical Report. Universiti Teknologi Malaysia. LT/M BIL.3.