*Ukrainian Mathematical Journal, Vol. 61, No. 12, 2009*

# ON THE AUTOMORPHISM OF SOME CLASSES OF GROUPS

**M. Hashemi**

UDC 512.5

We study two classes of 2-generated nilpotent groups of nilpotency class 2 and compute the order of their automorphism groups.

## 1. Introduction

Many authors have studied automorphism groups, and, of course, most of these works are devoted to $p$-groups. In [1], Jamali presents some nonabelian 2-groups with abelian automorphism groups. Bidwell and Curran [2] studied the automorphism group of a split metacyclic $p$-group. By using the program presented in [3], one can calculate the order of small $p$-groups. Our purpose in the present paper is to calculate the order of automorphism groups of two classes of groups. Let $G$ be a group, let $Z(G)$ denote the center of $G$, let $G'$ be the commutator subgroup of $G$, let $\mathrm{Aut}(G)$ denote the automorphism of $G$, and let $\varphi(m)$ denote the Euler function.

First, we state a lemma without proof that establishes some properties of groups of nilpotency class 2.

**Lemma 1.** *If $G$ is a group and $G' \subseteq Z(G)$, then the following assertions are true for every integer $k$ and $u, v, w \in G$:*

*(i)* $[uv, w] = [u, w][v, w]$ *and* $[u, vw] = [u, v][u, w]$;

*(ii)* $[u^k, v] = [u, v^k] = [u, v]^k$;

*(iii)* $(uv)^k = u^k v^k [v, u]^{k(k-1)/2}$.

**Theorem 1** ([4, p. 44], Proposition 3)**.** *Suppose that we are given a presentation $\langle X \mid R \rangle$ for a group $G$ and a map $\theta : X \to G$. Then $\theta$ extends to an endomorphism of $G$ if and only if, for all $x \in X$ and $r \in R$, the result of substituting $(x)\theta$ for $x$ in $r$ yields the identity of $G$. Furthermore, if, in addition, $(X)\theta$ generates $G$, then $\theta$ extends to an epimorphism of $G$.*

We consider the finitely presented groups

$$K(n, l) = \langle a, b \mid ab^n = b^l a,\ ba^n = a^l b \rangle, \quad \text{where} \quad (n, l) = 1,$$

and

Guilan University, Rasht, Iran.

Published in Ukrains'kyi Matematychnyi Zhurnal, Vol. 61, No. 12, pp. 1704–1712, December, 2009. Original article submitted June 5, 2009.

$$G_n = \langle a, b \mid a^n = b^n = 1,\ [a, b]^a = [a, b],\ [a, b]^b = [a, b] \rangle, \quad n \geq 1.$$

In Sec. 2, we investigate the automorphism group of $K(n, l)$ and compute the order of its automorphism group. In Sec. 3, we solve a system and, by using it, find an explicit formula for $|\mathrm{Aut}(G_n)|$.

Most of theorems of this paper were suggested by data from a computer program written in the GAP computational algebra system [3].

## 2. Order of $\mathrm{Aut}(K(n, l))$

In this section, we consider the metacyclic Fox groups $K(n, l)$ defined by

$$K(n, l) = \langle a, b \mid a b^n = b^l a,\ b a^n = a^l b \rangle, \quad \text{where} \quad (n, l) = 1.$$

We state some known results concerning $K(n, l)$, the proofs of which can be found in [5, 6].

**Theorem 2.** *The groups $K(n, l)$ defined by the above presentation have the following properties:*

*(i)* $|K(n, l)| = |l - n|^3$ *if* $(l, n) = 1$ *and is infinite otherwise;*

*(ii) if* $(l, n) = 1$, *then* $|a| = |b| = (l - n)^2$;

*(iii) if* $(l, n) = 1$, *then* $a^{l-n} = b^{n-l}$.

**Lemma 2.** *The following assertions are true:*

*(i)* $K(n, l) \cong K(1, 2 - l)$ *for every* $l \geq 3$;

*(ii)* $K(n, n + i) \cong K(1, i + 1)$ *for every* $i \geq 2$ *and* $(n, i) = 1$.

***Remark 1.*** If $(m, n) = 1$, then $K(n, m) \cong K(1, m - n + 1)$, which we may write as $K_{m-n+1}$. Hence, we only calculate $\mathrm{Aut}(K_l)$.

Prior to presenting the main result of this section, we need to develop some results concerning $K_l$.

**Lemma 3.** *Every element of $K_l$ may be uniquely represented by $x = a^{\beta} b^{\gamma} a^{(l-1)\delta}$, where $1 \leq \beta, \gamma, \delta \leq l - 1$.*

***Proof.*** By parts (ii) and (iii) of Theorem 2, every element of $K_l$ can be written in this form. Since $|K_l| = |l - 1|^3$, that expression is unique.

The lemma is proved.

**Lemma 4.** *In* $K_l$, *one has* $[a, b] = b^{l-1} \in Z(K_l)$.

***Proof.*** Since $a^{l-1} = b^{1-l}$, we have $a^{l-1} \in Z(K_l)$. According to the relations of $K_l$, we get

$$[a, b] = a^{-1}b^{-1}ab = a^{-1}b^{-1}b^l a = a^{-1}b^{l-1}a = b^{l-1} \in Z(K_l),$$

as desired.

The lemma is proved.

**Proposition 1.** *Let* $l \geq 3$ *be an integer and let* $f \in \mathrm{Aut}(K_l)$. *Then there exist* $1 \leq \beta_i, \gamma_i, \delta_i \leq l-1$ *for* $1 \leq i \leq 2$ *such that* $f(a) = a^{\beta_1}b^{\gamma_1}a^{(l-1)\delta_1}$ *and* $f(b) = a^{\beta_2}b^{\gamma_2}a^{(l-1)\delta_2}$, *where* $\beta_i$ *and* $\gamma_i$ *are solutions of the following system:*

$$\begin{gathered}
\gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 + \gamma_1\beta_1 \frac{l(l-1)}{2} \pmod{l-1},\\
\gamma_1 + \gamma_2 - \gamma_2\beta_2 \frac{l(l-1)}{2} \equiv \beta_1 + \beta_2 + \gamma_1\beta_1 \frac{l(l-1)}{2} \pmod{l-1},\\
\left(\beta_1 - \gamma_1 + \beta_1\gamma_1 \frac{(l-1)(l^2-2l)}{2}, l-1\right) = 1,\\
\left(\beta_2 - \gamma_2 + \beta_2\gamma_2 \frac{(l-1)(l^2-2l)}{2}, l-1\right) = 1.
\end{gathered} \tag{1}$$

***Proof.*** Let $f \in \mathrm{Aut}(K_l)$, $f(a) = a^{\beta_1}b^{\gamma_1}a^{(l-1)\delta_1}$, and $f(b) = a^{\beta_2}b^{\gamma_2}a^{(l-1)\delta_2}$, where $1 \leq \beta_i, \gamma_i, \delta_i \leq l-1$ and $1 \leq i \leq 2$. Since $ba = a^l b$, we have $f(b)f(a) = f(a)^l f(b)$. By setting the values $f(a)$ and $f(b)$ in the recent relation, we get

$$a^{\beta_2}b^{\gamma_2}a^{(l-1)\delta_2}a^{\beta_1}b^{\gamma_1}a^{(l-1)\delta_1} = (a^{\beta_1}b^{\gamma_1}a^{(l-1)\delta_1})^l (a^{\beta_2}b^{\gamma_2}a^{(l-1)\delta_2}).$$

Performing some routine calculations and using Lemma 3, we obtain

$$\gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 + \gamma_1\beta_1 \frac{l(l-1)}{2} \pmod{l-1}. \tag{2}$$

We also have $ab = b^l a$, whence

$$\gamma_1\beta_2 - \beta_1\gamma_2 \equiv \beta_2 - \gamma_2 + \gamma_2\beta_2 \frac{l(l-1)}{2} \pmod{l-1}. \tag{3}$$

By using relations (2) and (3), we get

$$\gamma_1 + \gamma_2 - \gamma_2\beta_2 \frac{l(l-1)}{2} \equiv \beta_1 + \beta_2 + \gamma_1\beta_1 \frac{l(l-1)}{2} (\mathrm{mod}\, l-1).$$

Since $|a| = |f(a)| = (l-1)^2$, we have $(a^{\beta_1} b^{\gamma_1} a^{(l-1)\delta_1})^{(l-1)^2} = 1$. Thus,

$$a^{(l-1)^2\left(\beta_1 - \gamma_1 + \gamma_1\beta_1 \frac{(l^2-2l)(l-1)}{2}\right)} = 1.$$

This yields

$$\left(\beta_1 - \gamma_1 + \beta_1\gamma_1 \frac{(l-1)(l^2-2l)}{2}, l-1\right) = 1.$$

For $|b| = |f(b)| = (l-1)^2$, by analogy, we obtain

$$\left(\beta_2 - \gamma_2 + \beta_2\gamma_2 \frac{(l-1)(l^2-2l)}{2}, l-1\right) = 1.$$

Thus, the required assertions are true.

The proposition is proved.

The statement below is the main result of this section.

**Proposition 2.** *Let $l \geq 3$ be an integer. Then*

$$|\mathrm{Aut}(K_l)| = \begin{cases} (l-1)^3\varphi(l-1) & \text{if } l \text{ or } \dfrac{l-1}{2} \text{ is even,} \\ 3(l-1)^3\varphi(l-1) & \text{if } \dfrac{l-1}{2} \text{ is odd.} \end{cases}$$

***Proof.*** First, let $l$ be even. Then system (1) reduces to the following equivalent system:

$$\begin{gathered} \gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 (\mathrm{mod}\, l-1), \\ \gamma_1 + \gamma_2 \equiv \beta_1 + \beta_2 (\mathrm{mod}\, l-1), \\ (\beta_1 - \gamma_1, l-1) = 1, \\ (\beta_2 - \gamma_2, l-1) = 1. \end{gathered} \tag{4}$$

By the second congruence in (4), we get

$$\gamma_2 \equiv \beta_1 + \beta_2 - \gamma_1 \pmod{l-1}.$$

Substituting $\gamma_2$ in the first congruence, we obtain

$$\beta_1^2 + \beta_1\beta_2 - \beta_1\gamma_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 \pmod{l-1},$$

or

$$\beta_1(\beta_1 - \gamma_1) + \beta_2(\beta_1 - \gamma_1) \equiv \beta_1 - \gamma_1 \pmod{l-1}.$$

It now follows from the relation $(\beta_1 - \gamma_1, l-1) = 1$ that $\beta_1 + \beta_2 \equiv 1 \pmod{l-1}$. A consequence of the last congruence and the relation $1 \le \beta_1 + \beta_2 - 1 \le 2l-3$ is that $\beta_2 = l - \beta_1$. This and the second congruence in (4) imply that $\gamma_2 = l - \gamma_1$. Now let $(t, l-1) = 1$. Then, for every $\beta_1 \in \{1, 2, \dots, l-1\}$, there exists a unique integer $\gamma_1 \in \{1, 2, \dots, l-1\}$ such that $\beta_1 - \gamma_1 = t$ (for the selection $\gamma_1 = t + \beta_1$). Combining all these facts, we see that, for every $f \in \mathrm{Aut}(K_l)$, there are $\beta_1$, $\gamma_1$, $\delta_1$, and $\delta_2$ such that

$$f(a) = a^{\beta_1} b^{t+\beta_1} a^{(l-1)\delta_1},$$

$$f(b) = a^{l-\beta_1} b^{l-(t+\beta_1)} a^{(l-1)\delta_2},$$

where $1 \le \beta_1, \delta_1, \delta_2 \le l-1$ and $(t, l-1) = 1$. If we now denote $f$ by $f_{\beta_1, t, \delta_1, \delta_2}$, then we obtain the required assertion.

Finally, let $l$ be odd. Since

$$\frac{l(l-1)}{2} \equiv \frac{l-1}{2} \pmod{l-1},$$

system (1) reduces to the following system:

$$\begin{gathered}
\gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 + \gamma_1\beta_1 \frac{l-1}{2} \pmod{l-1}, \\
\gamma_1 + \gamma_2 - \gamma_2\beta_2 \frac{l-1}{2} \equiv \beta_1 + \beta_2 + \gamma_1\beta_1 \frac{l-1}{2} \pmod{l-1}, \\
\left(\beta_1 - \gamma_1 + \beta_1\gamma_1 \frac{l-1}{2}, l-1\right) = 1, \\
\left(\beta_2 - \gamma_2 + \beta_2\gamma_2 \frac{l-1}{2}, l-1\right) = 1.
\end{gathered} \tag{5}$$

Now assume that $(l-1)/2$ is even. By the third condition in (5), one of $\beta_1$ and $\gamma_1$ is even and the other is odd. The same is true for $\beta_2$ and $\gamma_2$. Combining all these results and relation (5), we get

$$\gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 (\mathrm{mod}\, l-1),$$

$$\gamma_1 + \gamma_2 \equiv \beta_1 + \beta_2 (\mathrm{mod}\, l-1),$$

$$(\beta_1 - \gamma_1, l-1) = 1,$$

$$(\beta_2 - \gamma_2, l-1) = 1.$$

The required result follows similarly to the first case.

To complete the proof, we assume that $(l-1)/2$ is odd. Then, by using (5), we get

$$\gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 \left( \mathrm{mod}\, \frac{l-1}{2} \right),$$

$$\gamma_1 + \gamma_2 \equiv \beta_1 + \beta_2 \left( \mathrm{mod}\, \frac{l-1}{2} \right),$$

$$\left( \beta_1 - \gamma_1, \frac{l-1}{2} \right) = 1,$$

$$\left( \beta_2 - \gamma_2, \frac{l-1}{2} \right) = 1.$$

By analogy with the first case, we get

$$\beta_1 + \beta_2 \equiv 1 \left( \mathrm{mod}\, \frac{l-1}{2} \right).$$

Since $1 \leq \beta_1 + \beta_2 - 1 \leq 2l-3$, we have

$$\beta_2 = \left( \frac{l-1}{2} \right) t + 1 - \beta_1,$$

where $t \in \{1, 2, 3\}$. Similarly,

$$\gamma_2 = \left( \frac{l-1}{2} \right) s + 1 - \gamma_1,$$

where $s \in \{1, 2, 3\}$. By setting the values $\beta_2$ and $\gamma_2$ in the first and second congruences of (5), we get

$$s\beta_1 - t\gamma_1 \equiv \beta_1\gamma_1 (\mathrm{mod}\, 2),$$

$$s - t - \left(\frac{l-1}{2}\right)^2 st - \left(\left(\frac{l-1}{2}\right)s + 1\right)\beta_1 + \left(\frac{l-1}{2}\right)(s+t) - \left(\left(\frac{l-1}{2}\right)t + 1\right)\gamma_1 + 1 \equiv 0 (\mathrm{mod}\, 2).$$

Moreover, since one of $\beta_1$ and $\gamma_1$ is even and the other is odd, we have

$$\begin{aligned} &s\beta_1 - t\gamma_1 \equiv 0 (\mathrm{mod}\, 2), \\ &s - t - \left(\frac{l-1}{2}\right)^2 st - \left(\left(\frac{l-1}{2}\right)s + 1\right)\beta_1 + \left(\frac{l-1}{2}\right)(s+t) - \left(\left(\frac{l-1}{2}\right)t + 1\right)\gamma_1 + 1 \equiv 0 (\mathrm{mod}\, 2). \end{aligned} \tag{6}$$

We now count the solutions of (6). To do this, we must consider the following three cases:

1. Let $s$ and $t$ be odd. Using the first congruence of (6), we get $\beta_1 - \gamma_1 \equiv 0 (\mathrm{mod}\, 2)$, a contradiction (because one of $\beta_1$ and $\gamma_1$ is even and the other is odd).

2. Let $s$ and $t$ be even. Then

$$0 \equiv 0 (\mathrm{mod}\, 2),$$

$$\beta_1 + \gamma_1 \equiv 1 (\mathrm{mod}\, 2).$$

Thus, $\beta_2 = l - \beta_1$ and $\gamma_2 = l - \gamma_1$ are solutions of (1), where

$$1 \le \beta_1, \gamma_1 \le l - 1 \quad \text{and} \quad \left(\beta_1 - \gamma_1, \frac{l-1}{2}\right) = 1.$$

Hence, the number of solutions of (6) (in this case) is $(l-1)\varphi(l-1)$.

3. Suppose that one of $s$ and $t$ is even and the other is odd. First, let $s$ be even. Then

$$\gamma_1 \equiv 0 (\mathrm{mod}\, 2),$$

$$\beta_1 \equiv 1 (\mathrm{mod}\, 2).$$

Now let $s$ be odd. Then

$$\beta_1 \equiv 0 (\mathrm{mod}\, 2),$$

$$\gamma_1 \equiv 1 (\mathrm{mod}\, 2).$$

Thus, the number of solutions of (6) (in this case) is $2(l-1)\varphi(l-1)$. Therefore, by the above reasoning, the required assertion is established.

The proposition is proved.

## 3. Order of $\mathrm{Aut}(G_n)$

The goal of this section is to calculate $\left|\mathrm{Aut}(G_n)\right|$, where

$$G_n = \left\langle a, b \,\middle|\, a^n = b^n = 1,\ [a,b]^a = [a,b],\ [a,b]^b = [a,b] \right\rangle, \qquad n \geq 1.$$

First, we recall the following lemma from [7]:

**Lemma 5.** *Let* $G = G_n$. *Then* $\left|G_n\right| = n^3$, $\left|Z(G)\right| = n$, *and* $Z(G) = G' = \langle x \,|\, x^n = 1 \rangle$.

We now show that every element in $G_n$, $n \in N$, has the standard form.

**Lemma 6.** *Every element of the group* $G = G_n$ *can be written uniquely in the form* $a^i b^j [b,a]^k$, *where* $0 \leq i, s, k \leq n-1$.

***Proof.*** Since $[a,b]^a = [a,b]$ and $[a,b]^b = [a,b]$, we have $[a,b] \in Z(G)$ and

$$[a, b^{-1}] = \left([a,b]^{b^{-1}}\right)^{-1} \in Z(G),$$

$$[a^{-1}, b] = \left([a,b]^{a^{-1}}\right)^{-1} = [a,b]^{-1} \in Z(G).$$

Moreover, for every $x = x_1^{s_1} x_2^{s_2} \ldots x_k^{s_k}$ in $G_n$, where $x_i \in \{a, b\}$ and $s_1, s_2, \ldots, s_k$ are integers, using the relations $b^j a^i = a^i b^j [b^j, a^i]$, we can easily prove that every element of $G$ is of the form $a^i b^j g$, where $0 \leq i < m-1$, $0 \leq j \leq n-1$, and $g \in G'$ (by induction on the length of the word $x$). Assume that $x = a^i b^j g = e$. Then $a^i b^j \in Z(G)$ and $[a, b^j] = [a,b]^j = 1$, whence $n \,|\, j$. Similarly, we get $n \,|\, i$, i.e., $i = j = 0$ and $g = e$. The required result now follows immediately.

The lemma is proved.

The proposition below is the main result of this section.

**Proposition 3.** *Let* $n \geq 2$ *be an integer. In this case, one has* $f \in \mathrm{Aut}(G_n)$ *if and only if there exist* $0 \leq s_i, t_i, k_i \leq n-1$ *for* $1 \leq i \leq 2$ *such that* $f(a) = a^{t_1} b^{s_1} [a,b]^{k_1}$, $f(b) = a^{t_2} b^{s_2} [a,b]^{k_2}$, *and* $s_1$, $s_2$, $t_1$, *and* $t_2$ *are solutions of the following system:*

$$s_1 t_1 \frac{n(n-1)}{2} \equiv 0 (\mathrm{mod}\, n),$$

$$s_2 t_2 \frac{n(n-1)}{2} \equiv 0 (\mathrm{mod}\, n), \tag{7}$$

$$(s_1 t_2 - s_2 t_1, n) = 1.$$

***Proof.*** Let $f \in \mathrm{Aut}(G_n)$, $f(a) = a^{t_1} b^{s_1} [a,b]^{k_1}$, and $f(b) = a^{t_2} b^{s_2} [a,b]^{k_2}$, where $1 \le s_i, t_i, k_i \le n$, $1 \le i \le 2$. Since $|a| = |(a)f| = n$ and

$$(a)f^n = a^{nt_1} b^{ns_1} [a,b]^{nk_1 - s_1 t_1 \frac{n(n-1)}{2}} = [a,b]^{s_1 t_1 \frac{n(n-1)}{2}},$$

we get

$$n \mid s_1 t_1 \frac{n(n-1)}{2}.$$

We also have $|b| = |(b)f| = n$, whence

$$n \mid s_2 t_2 \frac{n(n-1)}{2}.$$

Finally, $|[a,b]| = n$ and, hence, $[a,b]^{n(t_1 s_2 - s_1 t_2)} = e$. This yields $(t_1 s_2 - s_1 t_2, n) = 1$.

It now suffices to prove that, under the above conditions, $f$ is an isomorphism. Let $u = a^s b^t [a,b]^k$ and $(u)f = e$. Then, by virtue of Lemma 6, we have

$$t_1 t + t_2 s \equiv 0 (\mathrm{mod}\, n),$$

$$s_1 t + s_2 s \equiv 0 (\mathrm{mod}\, n), \tag{8}$$

$$k_1 t + k_2 s + (t_1 s_2 - s_1 t_2) k - s_1 t_2 ts - \frac{s_1 t_1 t(t-1)}{2} - \frac{s_2 t_2 s(s-1)}{2} \equiv 0 (\mathrm{mod}\, n).$$

Adding the first congruence of (8) $s_1$ times to $(-t_1)$ times the second congruence, we get

$$s_1 t_2 s - t_1 s_2 s \equiv 0 (\mathrm{mod}\, n), \quad \text{or} \quad (s_1 t_2 - t_1 s_2) s \equiv 0 (\mathrm{mod}\, n).$$

Since $(t_1 s_2 - s_1 t_2, n) = 1$, we have $n \mid s$. The identical argument shows that $n \mid t$. Using these in the third congruence of (8), we get $(t_1 s_2 - s_1 t_2) k \equiv 0 (\mathrm{mod}\, n)$. Hence, $n \mid k$. In other words, $u = e$ and $f$ is an isomorphism.

The proposition is proved.

In order to give an expression for $\left|\mathrm{Aut}\,(G_n)\right|$, we need the following key lemma:

**Lemma 7.** *Let*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

*where* $p_i$ *is a prime number and* $\alpha_i \geq 1$. *Then the number of solutions of the system*

$$1 \leq s_1, s_2, t_1, t_2 \leq n-1,$$

$$(s_1 t_2 - s_2 t_1, n) = 1$$

*is*

$$n\varphi(n)^2 \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i + 1).$$

***Proof.*** Without loss of generality, we assume that $k = 2$. We know that the number of $\{m \,|\, 0 \leq m \leq n-1$ and $p_1 \,|\, m\}$ is $p_1^{\alpha_1 - 1} p_2^{\alpha_2}$. For $p_2$ and $p_1 p_2$, it is $p_1^{\alpha_1} p_2^{\alpha_2 - 1}$ and $p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1}$, respectively. Since $(s_1, s_2)$ is not allowed if $s_1$ and $s_2$ are multiples of $p_1$ or $p_2$, we may choose $(s_1, s_2)$ in $t$ ways, where

$$t = \begin{cases} p_1^{2\alpha_1} p_2^{2\alpha_2} - (p_1^{2\alpha_1 - 2} p_2^{2\alpha_2} - p_1^{2\alpha_1} p_2^{2\alpha_2 - 2} + p_1^{2\alpha_1 - 2} p_2^{2\alpha_2 - 2}) = p_1^{2\alpha_1 - 2} p_2^{2\alpha_2 - 2}(p_1^2 p_2^2 - p_1^2 - p_2^2 + 1), \\ p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) p_1^{\alpha_1 - 1}(p_1 + 1) p_2^{\alpha_2 - 1}(p_2 + 1) = \varphi(n) p_1^{\alpha_1 - 1}(p_1 + 1) p_2^{\alpha_2 - 1}(p_2 + 1). \end{cases}$$

We now select $(t_1, t_2)$ such that $(s_1 t_2 - s_2 t_1, n) = 1$. To do this, we find the number of $(x, y)$ such that $(s_1 y - s_2 x, n) \neq 1$. In other words, we find the number of $(x, y)$ such that

$$s_1 y - s_2 x \equiv 0 (\mathrm{mod}\ p_1)$$

or

$$s_1 y - s_2 x \equiv 0 (\mathrm{mod}\ p_2).$$

Let $s_1 y - s_2 x \equiv 0 (\mathrm{mod}\ p_1)$. Then, for every $0 \leq x \leq n-1$, there is a unique $0 \leq y_0 \leq p_1 - 1$ such that $s_1 y_0 \equiv s_2 x (\mathrm{mod}\ p_1)$ (because $y_0 \equiv 0$ or $s_1^* s_2 x (\mathrm{mod}\ p_1)$, where $s_1^*$ is the arithmetic inverse of $s_1$ with respect to $p_1$). Hence, for every $0 \leq x \leq n-1$, the number of solutions of $s_1 y - s_2 x \equiv 0 (\mathrm{mod}\ p_1)$ in $Z_n$ is $p_1^{\alpha_1 - 1} p_2^{\alpha_2}$ (because $y_i = y_0 + p_1 k$, $0 \leq k \leq p_1^{\alpha_1 - 1} p_2^{\alpha_2}$, are solutions). By analogy, for every $0 \leq x \leq n-1$, the number of solutions of $s_1 y - s_2 x \equiv 0 (\mathrm{mod}\ p_2)$ in $Z_n$ is $p_1^{\alpha_1} p_2^{\alpha_2 - 1}$. We also know that $p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1}$ solutions are common in two sets of solutions. Consequently, for selected $(s_1, s_2)$, we may choose $(t_1, t_2)$ in $l$ ways, where

$$l = \begin{cases} p_1^{2\alpha_1} p_2^{2\alpha_2} - p_1^{\alpha_1} p_2^{\alpha_2} (p_1^{\alpha_1 - 1} p_2^{\alpha_2} + p_1^{\alpha_1} p_2^{\alpha_2 - 1} - p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1}) = p_1^{2\alpha_1 - 1} p_2^{2\alpha_2 - 1} (p_1 p_2 - p_1 - p_2 + 1), \\ n p_1^{\alpha_1 - 1} (p_1 - 1) p_2^{\alpha_2 - 1} (p_2 - 1) = n\varphi(n). \end{cases}$$

Multiplying the number $t$ by the number $l$, we obtain the required assertion.

The lemma is proved.

In the previous notation, we prove the following important result:

**Proposition 4.** *Let*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

*be an integer. Then*

$$\left| \operatorname{Aut}(G_n) \right| = \begin{cases} n^3 \varphi(n)^2 \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i + 1) & \text{if } n \text{ is odd}, \\ \dfrac{n^3}{3} \varphi(n)^2 \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i + 1) & \text{if } n \text{ is even}. \end{cases}$$

***Proof.*** First, let $n$ be odd. Then system (7) reduces to the equivalent system

$$0 \le s_1, s_2, t_1, t_2 \le n - 1,$$

$$(s_1 t_2 - s_2 t_1, n) = 1.$$

Since the number of solutions of this system is

$$n\varphi(n)^2 \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p_i + 1)$$

and $k_1, k_2 \le n - 1$, the required assertion follows from Proposition 3.

Finally, let $n$ be even. In this case, $s_1$, $s_2$, $t_1$, and $t_2$ are solutions of system (7) if and only if, for every $1 \le i \le k - 1$, they are solutions of the following system:

$$s_1 t_1 \frac{n(n-1)}{2} \equiv 0 (\operatorname{mod} p_i^{\alpha_i}),$$

$$s_2 t_2 \frac{n(n-1)}{2} \equiv 0 (\operatorname{mod} p_i^{\alpha_i}),$$

$$(s_1 t_2 - s_2 t_1, p_i^{\alpha_i}) = 1.$$

If $p_i$ is an odd number, then this system reduces to the system

$$0 \le s_1, s_2, t_1, t_2 \le p_i^{\alpha_i} - 1,$$

$$(s_1t_2 - s_2t_1, p_i^{\alpha_i}) = 1,$$

which was investigated in Lemma 7.

It now suffices to compute the solutions of the system

$$s_1t_1 \frac{n(n-1)}{2} \equiv 0(\mathrm{mod}\, 2^{\alpha}),$$

$$s_2t_2 \frac{n(n-1)}{2} \equiv 0(\mathrm{mod}\, 2^{\alpha}),$$

$$(s_1t_2 - s_2t_1, 2^{\alpha}) = 1,$$

which is equivalent to

$$\begin{aligned} s_1t_1 &\equiv 0(\mathrm{mod}\, 2), \\ s_2t_2 &\equiv 0(\mathrm{mod}\, 2), \\ (s_1t_2 - s_2t_1, 2) &= 1. \end{aligned} \tag{9}$$

It follows from the first and third conditions of (9) that exactly one of $s_1$ and $t_1$ should be odd. Then we may choose $(s_1, t_1)$ in $2^{2\alpha-1}$ ways. We now select $(s_2, t_2)$ such that $(s_1t_2 - s_2t_1, 2) = 1$. If $t_1$ is even, then $t_2$ and $s_1$ are odd. This, together with $2 \mid s_2t_2$, implies that $s_2$ is even. Therefore, the number of solutions of system (9) in this case is $2^{4\alpha-4}$. Similarly, this is true if $t_1$ is odd. By the above argument, the number of solutions of (9) is

$$2^{4\alpha-3} = \frac{2^{\alpha}}{3}(\varphi(2^{\alpha}))^2 2^{\alpha-1}(2+1).$$

This completes the proof.

***Corollary 1.*** *Let $G$ be a nonabelian group of order $p^3$, where $p$ is an odd prime number. Then $|\mathrm{Aut}(G)| = p^3(p-1)$ or $p^3(p-1)^2(p+1)$.*

***Proof.*** According to [8], $G$ is isomorphic to one of $K_{p+1}$ or $G_p$. Then the required result follows from Propositions 2 and 4.

## REFERENCES


1. Jamali, "Some new non-abelian 2-groups with abelian automorphism groups," *J. Group Theory,* **5**, No. 1, 53–57 (2002).
2. J. N. S. Bidwell and M. J. Curran, "The automorphism group of a split metacyclic $p$-group," *Arch. Math.,* **87**, No. 6, 488–497 (2006).
3. *GAP–Groups, Algorithms, Programming, Version 4.4, AutPGroup and Small Groups Packages,* http://www.gap-system.org.
4. D. L. Johnson, *Presentations of Groups,* Cambridge University Press, Cambridge (1977).
5. C. M. Campbell, P. P.Campel, H. Doostie, and E. F. Robertson, "Fibonacci length for metacyclic groups," *Algebra Colloq.,* 215–222 (2004).
6. C. M. Campbell and E. F. Robertson, "On a group presentation due to Fox," *Can. Math. Bull.,* **19**, 247–248 (1976).
7. H. Doostie and M. Hashemi, "Fibonacci lengths involving the Wall number $\mathbf{k}(\mathbf{n})$," *J. Appl. Math. Comput.,* **20**, No. 1–2, 171–180 (2006).
8. D. J. S. Robinson, *A Course in the Theory of Groups,* Springer, New York (1982).