UDC 512.5

M. Hashemi (Univ. Guilan, Iran)

ON THE AUTOMORPHISM OF SOME CLASSES OF GROUPS

ПРО АВТОМОРФІЗМ ДЕЯКИХ КЛАСІВ ГРУП

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

Досліджено два класи 2-породжених нільпотентних груп класу нільпотентності 2 та обчислено порядок їх груп автоморфізмів.

1. Introduction. Many authors, have studied automorphism groups, of course most of these are devoted to p-groups. In [1] Jamali presents some non-abelian 2-groups with abelian automorphism groups. Bidwell and Curran [2] studied the automorphism group of a split metacyclic p-group. By a program in [3], one can calculate the order of small p-groups. Our purpose in the present paper is to calculate the order of the automorphism groups of two classes of groups. Let G be a group. $Z(G)$ denotes the center of G; G' the commutator subgroup of G; $\mathrm{Aut}(G)$ the automorphism of G and $\varphi(m)$ 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 hold 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 $\langle X | R \rangle$ for a group G, and a map $\theta : X \to G$. Then θ extends to an endomorphism of G if and only if for all $x \in X$ and all $r \in R$ the result of substituting $(x)\theta$ for x in r yield the identity of G. Furthermore if, in addition $(X)\theta$ generates G then θ extends to an epimorphism of G.*

We consider the finitely presented groups,

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

and

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

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

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

2. The order of $\mathrm{Aut}(K(n, l))$. In this section, we consider the metacyclic Fox groups $K(n, l)$ defined by $K(n, l) = \langle a, b \,|\, ab^n = b^l a,\ ba^n = a^l b \rangle$, where $(n, l) = 1$.

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

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

Note. 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 $\mathrm{Aut}(K_l)$.

Before we present 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 presented 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, $[a, b] = b^{l-1} \in Z(K_l)$.

Proof. Since $a^{l-1} = b^{1-l}$ then $a^{l-1} \in Z(K_l)$. By the relations of K_l we have

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

as desired.

The lemma is proved.

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

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

Proof. Let $f \in \mathrm{Aut}(K_l)$ and $f(a) = a^{\beta_1} b^{\gamma_1} a^{(l-1)\delta_1}$, $f(b) = a^{\beta_2} b^{\gamma_2} a^{(l-1)\delta_2}$, 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

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

After some routine calculations and Lemma 3 we see,

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

Also $ab = b^l a$ then we have

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

By the relations (2) and (3), we have

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

Since $|a| = |f(a)| = (l-1)^2$, consequently $(a^{\beta_1} b^{\gamma_1} a^{(l-1)\delta_1})^{(l-1)^2} = 1$. Thus $a^{(l-1)^2\left(\beta_1 - \gamma_1 + \gamma_1\beta_1 \frac{(l^2-2l)(l-1)}{2}\right)} = 1$. This further implies

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

For $|b| = |f(b)| = (l-1)^2$, by a similar argument we see that

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

Thus the assertions hold.

The proposition is proved.

The following proposition is the main result of this section.

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

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

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

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

By the second congruence in (4), we get $\gamma_2 \equiv \beta_1 + \beta_2 - \gamma_1 (\operatorname{mod} l-1)$. Substituting γ_2 in the first congruence gives $\beta_1^2 + \beta_1\beta_2 - \beta_1\gamma_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 (\operatorname{mod} l-1)$, or

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

Now $(\beta_1 - \gamma_1, l-1) = 1$ implies that $\beta_1 + \beta_2 \equiv 1 (\operatorname{mod} l-1)$. A consequence of the last congruence and $1 \leq \beta_1 + \beta_2 - 1 \leq 2l-3$ is that $\beta_2 = l - \beta_1$. This and the second congruence in (4) follows that $\gamma_2 = l - \gamma_1$. Now let $(t, l-1) = 1$. Then for every

$\beta_1 \in \{1, 2, \ldots, l-1\}$ there exist unique integer $\gamma_1 \in \{1, 2, \ldots, l-1\}$ such that $\beta_1 - \gamma_1 = t$ (for selection $\gamma_1 = t + \beta_1$). Combining all these facts, we see that for every $f \in \operatorname{Aut}(K_l)$ there are $\beta_1, \gamma_1, \delta_1, \delta_2$ 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 $1 \le \beta_1, \delta_1, \delta_2 \le l-1$, $(t, l-1) = 1$. Now if we denote f by $f_{\beta_1, t, \delta_1, \delta_2}$, then the assertion yields.

Lastly, let l be odd. Since $\frac{l(l-1)}{2} \equiv \frac{l-1}{2} (\operatorname{mod} l-1)$, the system (1) simplifies to the following system:

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

Now suppose that $\frac{l-1}{2}$ is even. By the third condition in (5), one of β_1 and γ_1 is even and the other is odd. Also, it is true about β_2 and γ_2. Combining of all these and (5), we have

$$\begin{aligned}
&\gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 (\operatorname{mod} l-1),\\
&\gamma_1 + \gamma_2 \equiv \beta_1 + \beta_2 (\operatorname{mod} l-1),\\
&(\beta_1 - \gamma_1, l-1) = 1,\\
&(\beta_2 - \gamma_2, l-1) = 1.
\end{aligned}$$

The result follows in a similar way as for the first case.

To complete the proof, let $\frac{l-1}{2}$ be odd. Then by (5) we get

$$\begin{aligned}
&\gamma_2\beta_1 - \beta_2\gamma_1 \equiv \beta_1 - \gamma_1 \left(\operatorname{mod} \frac{l-1}{2}\right),\\
&\gamma_1 + \gamma_2 \equiv \beta_1 + \beta_2 \left(\operatorname{mod} \frac{l-1}{2}\right),\\
&\left(\beta_1 - \gamma_1, \frac{l-1}{2}\right) = 1,\\
&\left(\beta_2 - \gamma_2, \frac{l-1}{2}\right) = 1.
\end{aligned}$$

In a similar way as for the first case, we get $\beta_1 + \beta_2 \equiv 1\left(\bmod \frac{l-1}{2}\right)$. Since $1 \le \le \beta_1 + \beta_2 - 1 \le 2l - 3$, 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 β_2 and γ_2 in the first and second congruences of (5), we have

$$s\beta_1 - t\gamma_1 \equiv \beta_1\gamma_1 (\bmod 2),$$

$$s - t - \left(\frac{l-1}{2}\right)^2 st - \left(\left(\frac{l-1}{2}\right)s + 1\right)\beta_1 +$$

$$+ \left(\frac{l-1}{2}\right)(s+t) - \left(\left(\frac{l-1}{2}\right)t + 1\right)\gamma_1 + 1 \equiv 0 (\bmod 2).$$

Moreover, since one of β_1 and γ_1 is even and the other is odd then

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

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

1. Let s and t be odd. Utilizing the first congruence of (6), we have $\beta_1 - \gamma_1 \equiv \equiv 0 (\bmod 2)$ and which is a contradiction (for, one of β_1 and γ_1 is even and the other is odd).

2. Let s and t be even, then

$$0 \equiv 0 (\bmod 2),$$

$$\beta_1 + \gamma_1 \equiv 1 (\bmod 2).$$

So that $\beta_2 = l - \beta_1$ and $\gamma_2 = l - \gamma_1$ are solutions of (1), where $1 \le \beta_1, \gamma_1 \le l - 1$ and $\left(\beta_1 - \gamma_1, \frac{l-1}{2}\right) = 1$. Hence the number solutions of (6) (in this case) is $(l - - 1)\varphi(l-1)$.

3. Suppose one of s and t is even and other is odd. First let s be even, then

$$\gamma_1 \equiv 0 (\bmod 2),$$

$$\beta_1 \equiv 1 (\bmod 2).$$

Now let s be odd, then

$$\beta_1 \equiv 0 (\bmod 2),$$

$$\gamma_1 \equiv 1 (\bmod 2).$$

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

The proposition is proved.

3. The order of $\mathrm{Aut}(G_n)$. The goal of this section is to calculate the $|\mathrm{Aut}(G_n)|$, where

$$G_n = \langle a, b \,|\, a^n = b^n = 1,\ [a,b]^a = [a,b],\ [a,b]^b = [a,b] \rangle, \qquad n \ge 1.$$

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

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

We now show that every element in the G_n, where $n \in N$, has 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 $0 \le i, s, k \le n-1$.*

Proof. Since $[a,b]^a = [a,b]$, $[a,b]^b = [a,b]$, then $[a,b] \in Z(G)$ 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 may easily prove that every element of G is in the form $a^i b^j g$, where $0 \le i < m-1$, $0 \le j \le n-1$ and $g \in G'$ (by induction method on the length of the word x). Suppose $x = a^i b^j g = e$ then $a^i b^j \in Z(G)$ and $[a, b^j] = [a,b]^j = 1$, thus $n \,|\, j$. Similarly $n \,|\, i$, that is $i = j = 0$ and $g = e$. The result is now immediate.

The lemma is proved.

The following proposition is the main result of this section.

Proposition 3. *Let $n \ge 2$ be an integer. Then $f \in \mathrm{Aut}(G_n)$ if and only if there exist $0 \le s_i, t_i, k_i \le n-1$ for $1 \le i \le 2$ 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, t_2 are solutions of the following system*:

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

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

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

Proof. Let $f \in \mathrm{Aut}(G_n)$ and $f(a) = a^{t_1} b^{s_1} [a,b]^{k_1}$, $f(b) = a^{t_2} b^{s_2} [a,b]^{k_2}$, 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 $n \,\Big|\, s_1 t_1 \dfrac{n(n-1)}{2}$. Also $|b| = |(b)f| = n$ so that $n \,\Big|\, s_2 t_2 \dfrac{n(n-1)}{2}$. Finally, $|[a,b]| = n$ hence $[a,b]^{n(t_1 s_2 - s_1 t_2)} = e$. This yields that $(t_1 s_2 - s_1 t_2, n) = 1$.

Now it is sufficient to prove that f, with the above conditions, is an isomorphism. Let $u = a^s b^t [a, b]^k$ and $(u)f = e$, then by the Lemma 6, we have

$$\begin{aligned} &t_1 t + t_2 s \equiv 0 (\operatorname{mod} n), \\ &s_1 t + s_2 s \equiv 0 (\operatorname{mod} n), \\ &k_1 t + k_2 s + (t_1 s_2 - s_1 t_2)k - s_1 t_2 t s - \frac{s_1 t_1 t(t-1)}{2} - \frac{s_2 t_2 s(s-1)}{2} \equiv 0 (\operatorname{mod} n). \end{aligned} \tag{8}$$

By adding s_1 times the first congruence of (8) to $(-t_1)$ times the second congruence, we get $s_1 t_2 s - t_1 s_2 s \equiv 0 (\operatorname{mod} n)$ or $(s_1 t_2 - t_1 s_2)s \equiv 0 (\operatorname{mod} n)$. Since $(t_1 s_2 - s_1 t_2, n) = 1$, we have $n \mid s$. An identical argument shows that $n \mid t$. Using these in the third congruence of (8), yield that $(t_1 s_2 - s_1 t_2)k \equiv 0 (\operatorname{mod} n)$. Hence $n \mid k$. That is $u = e$ and f is an isomorphism.

The proposition is proved.

In order to give an expression for the $|\operatorname{Aut}(G_n)|$, we need the following key lemma.

Lemma 7. *Let* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, *where* p_i *is 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 $k = 2$. We know that, the number of $\{ m \mid 0 \leq m \leq n-1 \text{ and } p_1 \mid m \}$ is $p_1^{\alpha_1 - 1} p_2^{\alpha_2}$. Also, 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) when s_1 and s_2 are multiple of p_1 or p_2 not being allowed, we may choose (s_1, s_2) in t ways, where

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

Now, we 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

$$s_1 y - s_2 x \equiv 0 (\operatorname{mod} p_1) \quad \text{or} \quad s_1 y - s_2 x \equiv 0 (\operatorname{mod} p_2).$$

Let $s_1 y - s_2 x \equiv 0 (\operatorname{mod} p_1)$, then for every $0 \leq x \leq n-1$ there is a unique $0 \leq y_0 \leq$ $\leq p_1 - 1$ such that $s_1 y_0 \equiv s_2 x (\operatorname{mod} p_1)$ (for $y_0 \equiv 0$ or $s_1^* s_2 x (\operatorname{mod} p_1)$, where s_1^* is the arithmetic inverse of s_1 respect to p_1). Hence for every $0 \leq x \leq n-1$ the number solutions of $s_1 y - s_2 x \equiv 0 (\operatorname{mod} p_1)$ in Z_n is $p_1^{\alpha_1 - 1} p_2^{\alpha_2}$ (for $y_i = y_0 + p_1 k$, $0 \leq k \leq$

$\le p_1^{\alpha_1-1}p_2^{\alpha_2}$ are solutions). By a similar argument, for every $0 \le x \le n-1$ the number solutions of $s_1y - s_2x \equiv 0 (\mathrm{mod}\, p_2)$ in Z_n is $p_1^{\alpha_1}p_2^{\alpha_2-1}$. Also, we know that $p_1^{\alpha_1-1}p_2^{\alpha_2-1}$ solutions are common in two sets of solutions. Consequently, when (s_1, s_2) select, we may choose (t_1, t_2) in l ways where

$$l = \begin{cases} p_1^{2\alpha_1}p_2^{2\alpha_2} - p_1^{\alpha_1}p_2^{\alpha_2}(p_1^{\alpha_1-1}p_2^{\alpha_2} + p_1^{\alpha_1}p_2^{\alpha_2-1} - p_1^{\alpha_1-1}p_2^{\alpha_2-1}) = \\ \qquad = p_1^{2\alpha_1-1}p_2^{2\alpha_2-1}(p_1p_2 - p_1 - p_2 + 1), \\ np_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1) = n\varphi(n). \end{cases}$$

Multiplying the number t and l together we obtain the assertion.

The lemma is proved.

With the previous notations, we prove that the important result of this section.

Proposition 4. *Let* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ *be an integer. Then*

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

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

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

$$(s_1t_2 - s_2t_1, n) = 1.$$

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 assertion follows from the Proposition 3.

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

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

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

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

When p_i is odd number, then this system reduces to

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

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

which was investigated in the Lemma 7.

Now it is sufficient to compute the solutions of the system

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

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

$$(s_1 t_2 - s_2 t_1, 2^{\alpha}) = 1.$$

This is equivalent to:

$$\begin{aligned} s_1 t_1 &\equiv 0(\operatorname{mod} 2), \\ s_2 t_2 &\equiv 0(\operatorname{mod} 2), \\ (s_1 t_2 - s_2 t_1, 2) &= 1. \end{aligned} \tag{9}$$

From first and third conditions of (9), we note that exactly one of s_1 an t_1 should be odd. Then we may choose (s_1, t_1) in $2^{2\alpha-1}$ ways. Now, we select (s_2, t_2) such that $(s_1 t_2 - s_2 t_1, 2) = 1$. If t_1 is even then t_2 and s_1 are odd. This together with $2 \mid s_2 t_2$ yields that s_2 is even. Therefore, the number of solutions of system (9) for this case is $2^{4\alpha-4}$. Similarly, it is true if t_1 is odd. By the above argument, the number 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. *Let G be a non-abelian group of order p^3, where p is odd prime. Then $|\operatorname{Aut}(G)| = p^3(p-1)$ or $p^3(p-1)^2(p+1)$.*

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

1. *Jamali.* Some new non-abelian 2-groups with abelian automorphism groups // J. Group Theory. – 2002. – **5**, № 1. – P. 53 – 57.
2. *Bidwell J. N. S., Curran M. J.* The automorphism group of a split metacyclic p-group // Arch. Math. – 2006. – **87**, № 6. – S. 488 – 497.
3. *The GAP Group,* GAP Groups, Algorithms, and programming version 4.4 packages AutPGroup and Small Groups http. A. R.
4. *Johnson D. L.* Presentations of groups. – 2nd ed. // London Math. Soc. Stud. Texts 15. – Cambridge: Cambridge Univ. Press, 1977.
5. *Campbell C. M., Campel P. P., Doostie H., Robertson E. F.* Fibonacci length for metacyclic groups // Algebra Colloq. – 2004. – P. 215 – 222.
6. *Campbell C. M., Robertson E. F.* On a group presentation due to Fox // Can. Math. Bull. – 1976. – **19**. – P. 247 – 248.
7. *Doostie H., Hashemi M.* Fibonacci lenghts involving the Wall number $\mathbf{k}(\mathbf{n})$ // J. Appl. Math. Comput. – 2006. – **20**, № 1 – 2. – P. 171 – 180.
8. *Robinson D. J. S.* A course in the theory of groups. – New York: Springer-Verlag, 1982.

Received 05.06.09