Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
25 (2009), 29–37
www.emis.de/journals
ISSN 1786-0091

ON THE AUTOMORPHISM OF A CLASS OF GROUPS

M. HASHEMI

ABSTRACT. We exhibit a presentation for automorphism group of a class of 2-generator metabelian groups.

1. Introduction

Many authors have studied the automorphism groups, of course most of these are devoted to p-groups. In [3], Jamali presents some non-abelian 2-groups with abelian automorphism groups. Bidwell and Curran [2] studied the automorphism group of a split metacyclic p-groups. By a program in [1], one can calculate the order of small p-groups. In this paper G will denote a group. G', $Z(G)$ and $\mathrm{Aut}(G)$ will denote the derived subgroup, center and automorphism group of G.

Let $m \geq 2$ be an integer. Consider the group $U(m) = \{n | 1 \leq n \leq m,\ (n,m) = 1\}$, clearly $U(m)$ is abelian and $|U(m)| = \phi(m)$. Furthermore, there exist $c_1, c_2, \ldots, c_t \in U(m^2)$ such that $U_{m^2} = \langle s_1 \rangle \times \langle s_2 \rangle \times \cdots \times \langle s_t \rangle$.

We consider the finitely presented group,

$$H_m = \langle x, y | x^{m^2} = y^m = 1, y^{-1}xy = x^{1+m} \rangle, \qquad m \geq 2.$$

In Section 2, we study the groups H_m and show that H_m is an extra-special group ($G' \simeq Z(G)$). Section 3 is devoted to the characterization of the automorphism group of H_m.

2. Some properties of H_m

First, we state a lemma without proof that establishes some properties of H_m.

Lemma 2.1. *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) $[u^k, v] = [u, v^k] = [u, v]^k$.

2000 *Mathematics Subject Classification.* 20D15, 20E36.
Key words and phrases. Groups, automorphism groups, group presentation.

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

Proposition 2.2. *Let* $G = H_m$. *Then* $Z(G) = G' \simeq \langle z | z^m = 1\rangle$.

Proof. We first prove that $G' \subseteq Z(G)$. By the relations of G, we get $[x,y] = x^{-1}x^y = x^{-1}x^{1+m} = x^m$. Then

$$\begin{aligned}[[x,y],y] &= y^{-1}x^{-1}yxy^{-1}x^{-1}y^{-1}xy^2 = (x^{-1})^y x (x^{-1})^y x^{y^2} \\ &= x^{-m}x^{-1-m}x^{(1+m)^2} = x^{-2m-1}x^{1+2m+m^2} \\ &= x^{m^2} = 1.\end{aligned}$$

Also we have $[[x,y],x] = 1$ so that $G' \subseteq Z(G)$ and $[x,y]^m = 1$.

It is sufficient to show that $Z(G) \subseteq G'$. For every $U = u_1^{s_1}u_2^{s_2}\dots u_k^{s_k}$ in G, where $u_i \in \{x,y\}$ and $s_1, s_2, \dots, s_k$ are integers, using the relation $y^{-1}xy = x^{1+m}$, we may easily prove that U is in the form $y^r x^s$, where $0 \le r < m$ and $0 \le s \le m^2$. Suppose $y^r x^s \in Z(G)$. Then $y^r x = xy^r$ and $yx^s = x^s y$. Hence

$$1 = [x, y^r] = x^{-1}x^{(1+m)^r} = x^{-1}x^{(1+rm)} = x^{rm},$$
$$1 = [x^s, y] = x^{-s}(x^s)^y = x^{-s}x^{(1+m)s} = x^{ms}.$$

These show that $m|r$ and $m|s$, and then $y^r x^s = (x^m)^t = [x,y]^t \in G'$. Therefore $Z(G) = G'$. □

By the above calculations, we get:

Corollary 2.3. *Every element of* $G = H_m$ *can be written uniquely in the form* $y^r x^s$, *where* $0 \le r \le m-1$ *and* $0 \le s \le m^2 - 1$. *Also* $|G| = m^3$.

Proof. Let $y^r x^s = 1$ then $1 = [x, y^r] = [x,y]^r = x^{rm}$. Therefore $m|r$, $m^2|s$ and uniqueness of the presentation follows. This yields that $|G| = m^3$. □

Remark 2.4. For an integer $n \ge 1$ and $u = y^{r_1}x^{s_1},\ v = y^{r_2}x^{s_2} \in H_m$, when we are trying to find the automorphism of H_m we need to concentrate on the terms uv, $u^n$and $(uv)^n$. By the Lemma 2.1 and Proposition 2.2, we get

$$\begin{aligned}uv &= y^{r_1}x^{s_1}y^{r_2}x^{s_2} = y^{r_1+r_2}x^{s_1+s_2}[x,y]^{s_1r_2} = y^{r_1+r_2}x^{s_1+s_2+ms_1r_2} \\ u^n &= y^{nr_1}x^{ns_1}[x^{s_1}, y^{r_1}]^{n(n-1)/2} = y^{nr_1}x^{ns_1+mr_1s_1n(n-1)/2} \\ u^n v^n &= y^{n(r_1+r_2)}x^{n(s_1+s_2)+m(r_1s_1+r_2s_2)n(n-1)/2}[x,\ y]^{nr_2(ns_1+mr_1s_1n(n-1)/2} \\ &= y^{n(r_1+r_2)}x^{n(s_1+s_2)+mn^2s_1r_2+m(r_1s_1+r_2s_2)n(n-1)/2} \\ (uv)^n &= (y^{r_1+r_2}x^{s_1+s_2+ms_1r_2})^n \\ &= y^{n(r_1+r_2)}x^{n(s_1+s_2+ms_1r_2)}[x,y]^{n(r_1+r_2)(s_1+s_2+ms_1r_2)(n-1)/2} \\ &= y^{n(r_1+r_2)}x^{n(s_1+s_2+ms_1r_2)+(r_1+s_1)(r_2+s_2)mn(n-1)/2}.\end{aligned}$$

3. A presentation for automorphisms group of H_m

The following proposition is the main result of this section.

Proposition 3.1. *Let* $m \ge 2$ *be an integer.*

(i) If m is odd then

$$\mathrm{Aut}(H_m) = \big\{f_{r,s,i} | (x)f_{r,s,i} = y^r x^s,\ (y)f_{r,\ s,\ i} = yx^{mi},\ \text{where } 0 \le r < m,\ 0 \le i < m \text{ and } 1 \le s < m^2,\ \text{when } (m,s) = 1\big\}.$$

(ii) If $\frac{m}{2}$ is even then

$$\mathrm{Aut}(H_m) = \big\{f_{r,s,i} | (x)f_{r,s,i} = y^r x^s,\ (y)f_{r,s,i} = y^{r_3} x^{mi},\ \text{where } 0 \le r < m,\ 0 \le i < m,\ r_3 = 1 \text{ if } r \text{ is even and } r_3 = 1 + \frac{m}{2} \text{ if } r \text{ is odd also } 1 \le s < m^2,\ \text{when } (m,s) = 1\big\}.$$

(iii) If $\frac{m}{2}$ is odd then

$$\mathrm{Aut}(H_m) = \big\{f_{2r,s,i} | (x)f_{2r,s,i} = y^{2r} x^s,\ (y)f_{2r,s,i} = yx^{\frac{m}{2}i},\ \text{where } 0 \le r < \frac{m}{2},\ 0 \le i < 2m \text{ and } 1 \le s < m^2,\ \text{when } (m,s) = 1\big\}.$$

Proof. Let $f \in \mathrm{Aut}(H_m)$ and $(x)f = y^{r_1}x^{s_1}$, $(y)f = y^{r_2}x^{s_2}$. Then for every $u = y^k x^n \in H_m$, we get

$$\begin{aligned}(u)f &= ((y)f)^k((x)f)^n = (y^{r_2}x^{s_2})^k(y^{r_1}x^{s_1})^n \\ &= y^{kr_2+nr_1}x^{ks_2+ns_1+mkns_2r_1+m(r_2s_2k(k-1)/2+s_1r_1n(n-1)/2)}.\end{aligned}$$

Since $(x^m)f = x^{ms_1+ms_1r_1m(m-1)/2}$ and $|(x^m)f| = |x^m| = m$, we have

$$(m, s_1(1 + r_1m(m-1)/2) = 1,$$

namely,

(1) $$(m, s_1) = 1 \text{ and } (m, 1 + r_1m(m-1)/2) = 1.$$

Also $|(y)f| = m$, thus $x^{m(s_2+\frac{m(m-1)}{2}r_2s_2)} = 1$ that is

(2) $$s_2 + \frac{m(m-1)}{2}r_2s_2 \equiv 0 \pmod{m}.$$

For $(m, 1 + \frac{m(m-1)}{2}) = 1$ or 2 so that $m|s_2$ or $\frac{m}{2}|s_2$.

Since $xy = yx^{1+m}$, then

$$\begin{aligned}(xy)f &= (yx^{m+1})f = y^{r_1+r_2}x^{s_2+(m+1)s_1+m(m+1)s_2r_1+\frac{ms_1r_1m(m+1)}{2}} \\ &= (x)f(y)f = y^{r_1+r_2}x^{s_2+s_1+ms_1r_2}.\end{aligned}$$

Therefore, by the Corollary 2.3, we get

(3) $$s_1 + s_2r_1 + s_1r_1\frac{m(m+1)}{2} \equiv s_1r_2 \pmod{m}.$$

To prove (i), since m is odd then by (2), we get $m|s_2$. This together with (1) and (3) gives $r_2 = 1$. As above, we consider

$$(x)f = y^{r_1}x^{s_1}, \quad (y)f = y^{r_2}x^{mi}$$

where $0 \le r_1 \le m-1$, $r_2 = 1$, $0 \le i \le m-1$ and $0 \le s_1 \le m^2-1$ when $(m, s_1) = 1$.

It is sufficient to prove that f, with the above conditions, is an isomorphism. Let

$$(y^k x^n)f = y^{r_2 k + r_1 n} x^{mki + ns_1 + ms_1 r_1 n(n-1)/2} = e.$$

Since $r_2 = 1$, Corollary 2.3 implies that

$$k + nr_1 \equiv 0 \pmod{m} \tag{4}$$

$$mki + ns_1 + ms_1 r_1 \frac{n(n-1)}{2} \equiv 0 \pmod{m^2}. \tag{5}$$

Using the relations (1) and (5), we obtain $m|n$. It follows that $m|k$. This together with (5) yields $m^2|n + \frac{mr_1 n(n-1)}{2}$. Since m is odd, $m^2|n$ (for $(m,2) = 1$, $m|n$) and $u = y^k x^n = e$.

Now, let m be even and $\frac{m}{2} = 2t$. Then by (2), $m|s_2$. This together with (3) gives $r_2 = 1$ if r_1 is even and $r_2 = 1 + \frac{m}{2}$ if r_1 is odd. Consider $(x)f = y^{r_1} x^{s_1}$, $(y)f = y^{r_2} x^{mi}$, where $0 \le r_1 \le m-1$, $r_2 = 1$(when r_1 is even) and $r_2 = 1 + \frac{m}{2}$(when, r_1 is odd), $0 \le i \le m-1$ and $0 \le s_1 \le m^2 - 1$ while $(m, s_1) = 1$.

In a similar way as for the Case (i), we get

$$r_2 k + nr_1 \equiv 0 \pmod{m} \tag{6}$$

$$mki + ns_1 + ms_1 r_1 \frac{n(n-1)}{2} \equiv 0 \pmod{m^2}. \tag{7}$$

Since $(m, s_1) = 1$, the congruence (7) yields that $m|n$. Also $(m, r_2) = 1$ then by (6) we have $m|k$. Combining all these facts, we see that $n + mr_1 \frac{n(n-1)}{2} \equiv 0 (mod\ m^2)$ and hence $m^2|n$ or $n = \frac{m^2}{2}$. If $n = \frac{m^2}{2}$ then we have

$$\frac{m^2}{2} + \frac{mr_1 m^2 (\frac{m^2}{2} - 1)}{4} \equiv 0 \pmod{m^2}.$$

This yields that $1 + \frac{mr_1(\frac{m^2}{2}-1)}{2} \equiv 0 \pmod{2}$, which is a contradiction (for, $\frac{m}{2} = 2t$). Then $m^2|n$ and $u = y^k x^n = e$. This completes the proof of (ii).

Lastly, let $\frac{m}{2}$ be odd. Then by (2), we get $\frac{m}{2}|s_2$. Also $(m, 1 + r_1 \frac{m(m-1)}{2}) = 1$. Therefore r_1 is even and we have $r_2 = 1$ by using relation (3). Consider $(x)f = y^{r_1} x^{s_1}$ and $(y)f = yx^{\frac{m}{2} i}$, where r_1 is even , $0 \le i \le 2m-1$ and $0 \le s_1 \le m^2 - 1$ when $(m, s_1) = 1$.

Now, we show that f is an automorphism. Similar to Case (i), we have

$$k + nr_1 \equiv 0 \pmod{m} \tag{8}$$

$$\frac{m}{2} ki + ns_1 + ms_1 r_1 \frac{n(n-1)}{2} \equiv 0 \pmod{m^2}. \tag{9}$$

By (9), we get $\frac{m}{2}|n$. Since r_1 is even, by (8) we have $m|k$. So $k = 0$. This together with (9) and (1) yields $m^2|n$ so that (iii) is established. □

As a result of this proposition and using $\phi(m^2) = m\phi(m)$ (for every positive integer m) we get:

Corollary 3.2. *For every $m \geq 2$, $|\operatorname{Aut}(H_m)| = m^3\phi(m)$ then the order of H_m divides $|\operatorname{Aut}(H_m)|$.*

Before we give the presentation for $\operatorname{Aut}(H_m)$ and its proof, we need the following lemma.

Lemma 3.3. *Let $m \geq 2$ be an integer. By using the notations of the Proposition 3.1,*

(i) if m is odd then $Z(\operatorname{Aut}(H_m)) = \{f_{0,\ mt+1,\ 0} |\ 0 \leq t < m\}$

(ii) if $\frac{m}{2}$ is odd then $Z(\operatorname{Aut}(H_m)) = \{f_{0,\ 2mt+1,\ 0},\ f_{0,\ 2mt+1,\ m} |\ 0 \leq t < m\}$

(iii) if $\frac{m}{2}$ is even then $Z(\operatorname{Aut}(H_m)) = \{f_{0,\ 2mt+1,\ 0},\ f_{0,\ 2mt+m,\ \frac{m}{2}} |\ 0 \leq t < m\}$

Proof. (i) Consider $T = \{f_{0,\ mt+1,\ 0} |\ 0 \leq t < m\}$. One can easily check that $T \subseteq Z(\operatorname{Aut}(H_m))$. Let $f_{r,\ s,\ i} \in Z(\operatorname{Aut}(H_m))$. Then for every $f_{r_1,\ s_1,\ i_1} \in \operatorname{Aut}(H_m)$, we have

$$(x)f_{r_1,\ s_1,\ i_1}f_{r,\ s,\ i} = (x)f_{r,\ s,\ i}f_{r_1,\ s_1,\ i_1}$$
$$(y)f_{r_1,\ s_1,\ i_1}f_{r,\ s,\ i} = (y)f_{r,\ s,\ i}f_{r_1,\ s_1,\ i_1}.$$

These yield

(10) $$i_1(1-s) \equiv i(1-s_1) \pmod{m}$$

(11) $$r_1 + s_1 r \equiv r + sr_1 \pmod{m}$$

(12) $$mr_1 i + \frac{mrss_1(s_1-1)}{2} + \frac{mrss_1(s_1-1)}{2} \equiv mi_1 + \frac{ms_1r_1s(s-1)}{2} \pmod{m}.$$

Substituting, $i_1 = 1$ and $s_1 = 1$ in the congruence (10) gives $s = mt+1,\ 0 \leq t \leq m$. Similarly, we get $r = 0$ by selecting $r_1 = 0$ and $s_1 = 2$. With using the above values in (12), we have $i = 0$. Then $f_{r,\ s,\ i} = f_{0,\ mt+1,\ 0} \in T$.

(ii) Let $T = \{f_{0,\ mt+1,\ 0},\ f_{0,\ mt+1,\ m} |\ 0 \leq t \leq \frac{m}{2}\}$. Then one can easily prove that $T \subseteq Z(\operatorname{Aut}(H_m))$. We now suppose that $f_{2r,\ s,\ i} \in Z(\operatorname{Aut}(H_m))$. Then for every $f_{2r_1,\ s_1,\ i_1} \in \operatorname{Aut}(H_m)$, we get

$$(x)f_{2r_1,\ s_1,\ i_1}f_{2r,\ s,\ i} = (x)f_{2r,\ s,\ i}f_{2r_1,\ s_1,\ i_1}$$
$$(y)f_{2r_1,\ s_1,\ i_1}f_{2r,\ s,\ i} = (y)f_{2r,\ s,\ i}f_{2r_1,\ s_1,\ i_1}.$$

Hence

(13) $$2r + 2sr_1 \equiv 2r_1 + 2s_1 r \pmod{m}$$

(14) $$rmi_1 + \frac{m^2}{2}i_1(r(2r-1) + mr_1s_1s(s-1)$$
$$\equiv r_1mi + \frac{m^2}{2}ir_1(2r_1-1) + mrss_1(s_1-1) \pmod{m^2}$$

$$\begin{aligned}(15)\quad &\frac{m}{2}i+\frac{m}{2}i_1s+\frac{m^2}{2}rsi_1(\frac{m}{2}i_1-1)\\ &\equiv \frac{m}{2}i_1+\frac{m}{2}is_1+\frac{m^2}{2}s_1r_1i(\frac{m}{2}i-1) \pmod{m^2}.\end{aligned}$$

We consider the congruence (13) and take $r_1=s_1=1$, so $2s\equiv 2 \pmod m$, that is $s=1+\frac{m}{2}t_1$. For, $(s,m)=1$, t_1 is even, so that $s=1+mt$. Again in (4), replacing s_1 by $m-1$ and s by $1+mt$, we get $4r\equiv 0(mod\ m)$, so $2r\equiv 0 \pmod m$.

Now, by (15) with $i_1=r_1=0$ and $s_1=-1$, we have $mi\equiv 0 \pmod{m^2}$ so that $i=0$ or $i=m$. Finally, by (15) when $s=mt+1$, $r=0$, $i_1=1$ and $i=0$ or $i=m$, we get $s=2mk+1$. Consequently, $f_{2r,s,i}=f_{0,2mk+1,0}$ or $f_{0,2mk+1,m}$. Similarly, if $\frac{m}{2}$ is even the result follows in a similar way as for the case (ii). □

The following corollary is now a consequence of Lemma 3.3.

Corollary 3.4. *For every $m\geq 2$, $|Z(\mathrm{Aut}(H_m))|=m$.*

Let $m\geq 2$ be an integer and let $U_{m^2}=\langle s_1\rangle\times\langle s_2\rangle\times\cdots\times\langle s_t\rangle$. Since $m+1\in U_{m^2}$, there exist unique integers m_1, m_2,…,m_t such that $m+1=s_1^{m_1}s_2^{m_2}\dots s_t^{m_t}$. Finally, let k_i denote the order of s_i modulo m^2. In other words, k_i is the smallest positive integer such that $s_i^{k_i}\equiv 1 \pmod{m^2}$.

Consider

$$\begin{aligned}A=\langle a_1,a_2,\dots,a_t,a,b|&a^m=b^m=a_i^{k_i}=1,\\ &[[a,b],a]=[[a,b],b]=[[a,b],a_i]=[a_i,a_j]=1,[a,a_i]=a^{s_i-1},\\ &[b,a_i]=b^{\alpha_i}[b,a]^{\beta_i},\ [a,b]=a_1^{m_1}a_2^{m_2}\dots a_t^{m_t},\quad 1\leq i,\ j\leq t\ \rangle;\end{aligned}$$

$$\begin{aligned}B=\langle a_1,a_2,\dots,a_t,a,b|\ &a^{2m}=b^{\frac{m}{2}}=a_i^{k_i}=1,\\ &[[a,b],a]=[[a,b],b]=[[a,b],a_i]=[a_i,a_j]=1,\ [a,a_i]=a^{s_i-1},\\ &[b,a_i]=b^{\alpha_i}[b,a]^{\alpha_i},\ [a,b]=(a_1^{m_1}a_2^{m_2}\dots a_t^{m_t})^{\frac{m}{2}-1},\quad 1\leq i,\ j\leq t\rangle;\end{aligned}$$

$$C=\langle a_1,a_2,\dots,a_t,a,b,c|R\rangle,$$

where

$$\begin{aligned}R=\{&a^m,\ b^{\frac{m}{2}},\ a_i^{k_i},\ c^{-2}b^{1+\frac{m}{4}},\\ &[a_i,a_j],\ [b,c],\ [[b,a],a],\ [[b,a],b],\ [[b,a],a_i],[a_i,a]a^{s_i-1},\ [a,b][c,a]^2,\\ &[a_i,b](b[b,a])^{\alpha_i},\ [a^{-1},c^{-1}]([c,a])^{1+\frac{m}{2}},\ ca_ic^{-1}[a,c]^{(\frac{m}{2}-1)\frac{s_i-1}{2}}a_i^{-1}b^{\frac{s_i-1}{2}},\\ &c^{-1}a_i^{-1}cb^{\frac{s_i-1}{2}}a_i[c,a]^{(\frac{m}{2}-1)\frac{s_i-1}{2}},\ [a,c]a_1^{m_1}a_2^{m_2}\dots a_t^{m_t},1\leq i,\ j\leq t\},\end{aligned}$$

$\alpha_i=s_i^{k_i-1}-1$ and $\beta_i=\frac{s_i^{k_i}\alpha_i}{2}$.

With these notations, we state the main result of this paper.

Proposition 3.5. *Let $m\geq 2$ be an integer. With the notations of Proposition 3.1,*

(i) if m is odd then $\mathrm{Aut}(H_m) \simeq A$,
(ii) if $\frac{m}{2}$ is odd then $\mathrm{Aut}(H_m) \simeq B$,
(iii) if $\frac{m}{2}$ is even then $\mathrm{Aut}(H_m) \simeq C$.

Proof. (i) For simplicity, we write $f_{011} = f_{0,\ 1,\ 1}$, $f_{110} = f_{1,\ 1,\ 0}$ and $f_{s_i} = f_{0,\ s_i,\ 0}$, $(1 \leq i \leq t)$. Then for every $k \geq 0$,

$$(x)f_{011}^k = x,\ (y)f_{011}^k = yx^{km}$$
$$(x)f_{110}^k = y^k x,\ (y)f_{110}^k = y$$
$$(x)f_{s_i}^k = x^{{s_i}^k},\ (y)f_{s_i}^k = y.$$

Consequently $|f_{011}| = |f_{110}| = m$, $|f_{s_i}| = k_i$ and $\prod_{i=1}^t |f_{s_i}| = m\phi(m)$. Also we can show that,

$$[f_{011},\ f_{s_i}] = f_{011}^{s_i-1},\ [f_{110},\ f_{s_i}] = f_{110}^{\alpha_i} f_{m+1}^{\beta_i},\ [f_{s_i},\ f_{s_j}] = 1,\ [f_{110},\ f_{011}] = f_{m+1}$$

and

$$f_{m+1} = f_{s_1}^{m_1} f_{s_2}^{m_2} \dots f_{s_t}^{m_t},$$

where $\alpha_i = s_i^{k_i-1} - 1$ and $\beta_i = \frac{s_i^{k_i}\alpha_i}{2}$.

Consider, $T = \{(\prod_{i=1}^t f_{s_i}^{l_i}) f_{110}^{i_1} f_{011}^{i_2} | 0 \leq i_1, i_2 < m,\ 0 \leq l_i < k_i\}$, so that $|T| = m^3\phi(m)$. Since $T \subseteq \mathrm{Aut}(H_m)$,

$$\mathrm{Aut}(H_m) = \langle f_{s_1},\ f_{s_2}, \dots, f_{s_t}, f_{110},\ f_{011}\rangle.$$

Now, by [4, Proposition 4.2], there is an epimorphism $\psi\colon A \to \mathrm{Aut}(H_m)$ such that $\psi(a) = f_{110}$, $\psi(b) = f_{011}$ and $\psi(a_i) = f_{s_i}$, $1 \leq i \leq t$. It remains to prove that ψ is one-to-one, and for this, consider the subset

$$L = \{(\prod_{i=1}^t a_i^{l_i}) a^{i_1} b^{i_2} | 0 \leq i_1, i_2 < m,\ 0 \leq l_i < k_i\},$$

of A. By using the relations of A, for every $w \in A$, we get $Lw \subseteq L$ then $A = L$. Suppose that $\psi((\prod_{i=1}^t a_i^{l_i}) a^{i_1} b^{i_2}) = e$ then $(\prod_{i=1}^t f_{s_i}^{l_i}) f_{110}^{i_1} f_{011}^{i_2} = 1$ that is

$$(x)(\prod_{i=1}^t f_{s_i}^{l_i}) f_{110}^{i_1} f_{011}^{i_2} = x \tag{16}$$

$$(y)(\prod_{i=1}^t f_{s_i}^{l_i}) f_{110}^{i_1} f_{011}^{i_2} = y. \tag{17}$$

By (2), $yx^{mi_2} = y$. So that Corollary 2.3, yields $m|i_2$ i.e. $i_2 = 0$. Again, with using (1) and Corollary 2.3 we get

$$i_1 s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} \equiv 0 \pmod{m} \tag{18}$$

$$s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} + m i_1 s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} (\frac{s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} - 1}{2}) \equiv 1 \pmod{m^2}. \tag{19}$$

Since $(s_i, m) = 1$, by (18), we conclude that $m|i_1$. This together with (19) gives

$$s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} \equiv 1 \pmod{m^2}.$$

Also $\langle s_j \rangle \bigcap \prod_{i \neq j} \langle s_i \rangle = \{1\}$ then for every i where $1 \leq i \leq t$, we have $s_i^{l_i} \equiv 1$ $(mod\ m^2)$ that is $k_i|\ l_i$. Combining all these facts, we see that $(\prod_{i=1}^{t} a_i^{l_i}) a^{i_1} b^{i_2} = e$.

(ii) Let $\frac{m}{2}$ be odd. To calculate the $Aut(H_m)$, take $f_{011} = f_{0,\ 1,\ 1}$, $f_{210} = f_{2,\ 1,\ 0}$ and $f_{s_i} = f_{0,\ s_i,\ 0}$, $(1 \leq i \leq t)$ then for every $k \geq 0$, by using induction method on k, we get

$$(x) f_{011}^k = x,\ (y) f_{011}^k = y x^{km/2}$$
$$(x) f_{210}^k = y^{2k} x,\ (y) f_{210}^k = y$$
$$(x) f_{s_i}^k = x^{s_i{}^k},\ (y) f_{s_i}^k = y.$$

Therefore, $|f_{011}| = 2m,\ |f_{210}| = \frac{m}{2}$, $|f_{s_i}| = k_i$ and $\prod_{i=1}^{t} |f_{s_i}| = m\phi(m)$. Also we have,

$$[f_{011},\ f_{s_i}] = f_{011}^{s_i - 1},\ [f_{210},\ f_{s_i}] = f_{210}^{\alpha_i} f_{m+1}^{\alpha_i},\ [f_{s_i},\ f_{s_j}] = 1,\ [f_{011},\ f_{210}] = f_{m+1}^{\frac{m}{2} - 1}$$

and

$$f_{m+1} = f_{s_1}^{m_1} f_{s_2}^{m_2} \dots f_{s_t}^{m_t},$$

where $\alpha_i = s_i^{k_i - 1} - 1$.

Consider the subset

$$T = \{ (\prod_{i=1}^{t} f_{s_i}^{l_i}) f_{110}^{i_1} f_{210}^{i_2} |\ 1 \leq i_1 < 2m,\ 0 \leq i_2 < \frac{m}{2},\ 0 \leq l_i < k_i \},$$

so that $|T| = m^3 \phi(m)$ and

$$\mathrm{Aut}(H_m) = \langle f_{s_1},\ f_{s_2}, \dots, f_{s_t}, f_{110},\ f_{210} \rangle.$$

Now, let $(\prod_{i=1}^{t} f_{s_i}^{l_i}) f_{011}^{i_1} f_{210}^{i_2} = 1$ then by Corollary 2.3 we get

$$2 i_2 s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} \equiv 0 \pmod{m}$$
$$s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} + 2 m i_2 s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} \left(\frac{2 i_2 s_1^{l_1} s_2^{l_2} \dots s_t^{l_t} - 1}{2} \right) \equiv 1 \mod m^2$$
$$\frac{m i_1}{2} \equiv 0 \mod m^2.$$

So that $2m|i_1,\ \frac{m}{2}|i_2,\ k_i|\ l_i$ and the result follows in a similar way as for the case (i).

To prove (iii), let $\frac{m}{4}$ be odd. We consider $f_{011},\ f_{110},\ f_{210}$ and f_{s_i} then for every $k \geq 0$

$$(x) f_{011}^k = x,\ (y) f_{011}^k = y x^{km}$$
$$(x) f_{110}^k = y^{k + [\frac{k}{2}] \frac{m}{2}} x,\ (y) f_{110}^k = y^{1 + \frac{km}{2}}$$
$$(x) f_{210}^k = y^{2k} x,\ (y) f_{210}^k = y.$$

Hence $|f_{011}| = m$, $|f_{110}| = |f_{210}| = \frac{m}{2}$, and $|f_{s_i}| = k_i$. Combining all these facts, we see that

$$[f_{011},\ f_{s_i}] = f_{011}^{s_i-1},\ [f_{210},\ f_{s_i}] = f_{210}^{\alpha_i} f_{m+1}^{\alpha_i},$$
$$[f_{s_i},\ f_{s_j}] = 1,\ [f_{210},\ f_{011}] = f_{2m+1},$$
$$[[f_{210},\ f_{011}], f_{011}] = [[f_{210},\ f_{011}], f_{210}] = [[f_{210},\ f_{011}], f_{s_i}] = 1$$

and $f_{m+1} = f_{s_1}^{m_1} f_{s_2}^{m_2} \dots f_{s_t}^{m_t}$, where $\alpha_i = s_i^{k_i-1} - 1$.

Take $N = \langle f_{s_1},\ f_{s_2}, \dots, f_{s_t}, f_{011},\ f_{210} | R_1 \rangle$, where

$$R_1 = \{f_{011}^{m},\ f_{210}^{\frac{m}{2}},\ f_{s_i}^{k_i},\ [f_{s_i},\ f_{011}] f_{011}^{s_i-1},\ [f_{s_i},\ f_{210}] f_{210}^{\alpha_i} f_{m+1}^{\alpha_i},\ [f_{s_i},\ f_{s_j}],$$
$$[f_{011},\ f_{210}] f_{2m+1},\ [[f_{210},\ f_{011}], f_{011}],\ [[f_{210},\ f_{011}], f_{210}],\ [[f_{210},\ f_{011}], f_{s_i}]\}.$$

Then by the above relations we get

$$N = \{(\prod_{i=1}^{t} f_{s_i}^{l_i}) f_{110}^{i_1} f_{210}^{i_2} | 1 \le i_1 < m,\ 0 \le i_2 < \frac{m}{2},\ 0 \le l_i < k_i\}.$$

Hence $|N| = \frac{m^3 \phi(m)}{2}$, therefore $(\mathrm{Aut}(H_m) : N) = 2$ and

$$\frac{\mathrm{Aut}(H_m)}{N} = \langle N f_{110} | (N f_{110})^2 = N \rangle.$$

Then the assertion may be obtained by [5, 2.2.4].

We note that, for this case, if $\frac{m}{4}$ is even then $|f_{110}| = m$. By the above consideration, the assertion is established. □

References

[1] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.12. http://www.gap-system.org.

[2] J. N. S. Bidwell and M. J. Curran. The automorphism group of a split metacyclic p-group. *Arch. Math. (Basel)*, 87(6):488–497, 2006.

[3] A.-R. Jamali. Some new non-abelian 2-groups with abelian automorphism groups. *J. Group Theory*, 5(1):53–57, 2002.

[4] D. L. Johnson. *Presentations of groups*, volume 15 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second edition, 1997.

[5] D. J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

Received August 3, 2008.

Department of Mathematics,
Faculty of Science,
University of Guilan,
P. O. Box 451 Rasht, Iran
E-mail address: m_hashemi@guilan.ac.ir