Czechoslovak Mathematical Journal, 68 (143) (2018), 803–815

AUTOMORPHISMS OF METACYCLIC GROUPS

Haimiao Chen, Beijing, Yueshan Xiong, Wuhan,
Zhongjian Zhu, Wenzhou

Received December 31, 2016. Published online December 7, 2017.

Abstract. A metacyclic group H can be presented as $\langle\alpha,\beta\colon \alpha^n=1,\ \beta^m=\alpha^t,\ \beta\alpha\beta^{-1}=\alpha^r\rangle$ for some n, m, t, r. Each endomorphism σ of H is determined by $\sigma(\alpha)=\alpha^{x_1}\beta^{y_1}$, $\sigma(\beta)=\alpha^{x_2}\beta^{y_2}$ for some integers x_1, x_2, y_1, y_2. We give sufficient and necessary conditions on x_1, x_2, y_1, y_2 for σ to be an automorphism.

Keywords: automorphism; metacyclic group; linear congruence equation

MSC 2010: 20D45

1. Introduction

A finite group G is *metacyclic* if it contains a cyclic normal subgroup N such that G/N is also cyclic. In some sense, metacyclic groups can be regarded as the simplest ones other than abelian groups.

As a natural object, the automorphism group of a metacyclic group has been widely studied. In 1970, Davitt in [5] showed that if G is a metacyclic p-group with $p\neq 2$, then the order of G divides that of $\mathrm{Aut}(G)$. In 2006, Bidwell and Curran in [1] found the order and the structure of $\mathrm{Aut}(G)$ when G is a split metacyclic p-group with $p\neq 2$, and in 2007, Curran in [3] obtained similar results for split metacyclic 2-groups. In 2008, Curran in [4] determined $\mathrm{Aut}(G)$ when G is a nonsplit metacyclic p-group with $p\neq 2$. In 2009, Golasiński and Gonçalves in [6] determined $\mathrm{Aut}(G)$ for any split metacyclic group G. The case of nonsplit metacyclic 2-groups remains unsolved.

In this paper we aim at writing down all of the automorphisms for a general metacyclic group. One of our main motivations stems from the study of regular Cayley maps on metacyclic groups (see [2]), which requires an explicit formula for a general automorphism.

DOI: 10.21136/CMJ.2017.0656-16

It is well-known (see Section 3.7 of [8]) that each metacyclic group can be presented as

$$\langle \alpha, \beta \colon\ \alpha^n = 1,\ \beta^m = \alpha^t,\ \beta\alpha\beta^{-1} = \alpha^r \rangle \tag{1.1}$$

for some positive integers n, m, r, t satisfying

$$r^m - 1 \equiv t(r-1) \equiv 0 \pmod{n}. \tag{1.2}$$

Denote this group by $H = H(n, m; t, r)$. There is an extension

$$1 \to \mathbb{Z}/n\mathbb{Z} \to H \to \mathbb{Z}/m\mathbb{Z} \to 1,$$

where $\mathbb{Z}/n\mathbb{Z} \cong \langle \alpha \rangle \lhd H$ and $\mathbb{Z}/m\mathbb{Z} \cong H/\langle \alpha \rangle$. It may happen that two groups given by different values of n, m, t, r are isomorphic. A complete classification (up to isomorphism) for finite metacyclic groups was obtained by Hempel in [7] in 2000.

In the presentation (1.1), we may assume $t \mid n$ which we do from now on. To see this, choose u, v such that $un + vt = (n, t)$, then $(v, n/(n, t)) = 1$. Let w be the product of all prime factors of m that do not divide v and let $v' = v + wn/(n, t)$, then $(v', m) = 1$. Replacing β by $\check{\beta} = \beta^{v'}$, we get another presentation: $H = \langle \alpha, \check{\beta} \colon\ \alpha^n = 1,\ \check{\beta}^m = \alpha^{(n,t)},\ \check{\beta}\alpha\check{\beta}^{-1} = \alpha^{r^{v'}} \rangle$.

Obviously each element can be written as $\alpha^u\beta^v$; note that $\alpha^u\beta^v = 1$ if and only if $m \mid v$ and $n \mid u + tv/m$. Each endomorphism σ of H is determined by $\sigma(\alpha) = \alpha^{x_1}\beta^{y_1}$, $\sigma(\beta) = \alpha^{x_2}\beta^{y_2}$ for some integers x_1, x_2, y_1, y_2. The main result of this paper gives sufficient and necessary conditions on x_1, x_2, y_1, y_2 for σ to be an automorphism. They consist of two parts, ensuring σ to be invertible and well-defined, respectively. Skillfully using elementary number theoretic techniques, we manage to reduce the second part to linear congruence equations. It turns out that the situation concerning the prime 2 is quite subtle, and this reflects the difficulty in determining the automorphism groups of nonsplit metacyclic 2-groups.

Notation and convention.

- ▷ For an integer $N > 0$, denote $\mathbb{Z}/N\mathbb{Z}$ by $\mathbb{Z}_N$ and regard it as a quotient ring of $\mathbb{Z}$. For $u \in \mathbb{Z}$, denote its image under the quotient $\mathbb{Z} \twoheadrightarrow \mathbb{Z}_N$ also by u.
- ▷ Given integers u, s with $u > 0$, set $[u]_s = 1 + s + \ldots + s^{u-1}$, so that $(s-1)[u]_s = s^u - 1$; for a prime number p, let $\deg_p(u)$ denote the largest integer s with $p^s \mid u$.
- ▷ Denote α^u by $\exp_\alpha(u)$ when the expression for u is too long.
- ▷ To avoid subtleties, we assume x_1, x_2, y_1, y_2 to be positive, and usually write an element of H as $\alpha^u\beta^v$ with $u, v > 0$.

2.1. Preparation.

Lemma 2.1. *If* $s > 1$ *with* $\deg_p(s-1) = l \geqslant 1$ *and* $x > 0$ *with* $\deg_p(x) = u \geqslant 0$, *then*

(I) $[x]_s \equiv \begin{cases} x, & p \neq 2 \ \text{ or } \ u = 0 \\ (1+2^{l-1})x, & p = 2 \ \text{ and } \ u > 0 \end{cases} \pmod{p^{l+u}};$

(II) $s^x - 1 \equiv \begin{cases} (s-1)x, & p \neq 2 \ \text{ or } \ u = 0 \\ (s-1+2^{2l-1})x, & p = 2 \ \text{ and } \ u > 0 \end{cases} \pmod{p^{2l+u}}.$

Proof. We only prove (I), then (II) follows from the identity $(s-1)[x]_s = s^x - 1$.
If $u = 0$, then $s \equiv 1 \pmod{p^{l+u}}$, so $[x]_s \equiv x \pmod{p^{l+u}}$.
Let us assume $u > 0$. Write $s = 1 + p^l h$ with $p \nmid h$. Note that

$$\begin{aligned}\deg_p\left(\binom{p^u}{j}\right) &= \deg_p\left(\frac{(p^u)!}{j!(p^u-j)!}\right) = \sum_{i=0}^{j-1}\deg_p(p^u-i) - \sum_{i=1}^{j}\deg_p(i) \\ &= u - \deg_p(j) + \sum_{i=1}^{j-1}(\deg_p(p^u-i) - \deg_p(i)) \\ &= u - \deg_p(j).\end{aligned}$$

If $p \neq 2$, then

$$[p^u]_s = \sum_{i=0}^{p^u-1}(1+p^l h)^i = \sum_{i=0}^{p^u-1}\sum_{j=0}^{i}\binom{i}{j}(p^l h)^j = \sum_{j=1}^{p^u}\binom{p^u}{j}(p^l h)^{j-1} \equiv p^u \pmod{p^{l+u}},$$

using that for all $j \geqslant 2$,

$$\deg_p\left(\binom{p^u}{j}\right) = u - \deg_p(j) \geqslant u - (j-2)l = (l+u) - (j-1)l.$$

Hence $s^{p^u} = (s-1)[p^u]_s + 1 \equiv 1 \pmod{p^{l+u}}$. Writing $x = p^u x'$ with $p \nmid x'$, we have

$$[x]_s = [p^u]_s \sum_{j=0}^{x'-1}(s^{p^u})^j \equiv x'[p^u]_s \equiv x \pmod{p^{l+u}}.$$

If $p = 2$, then using that for all $j \geqslant 3$,

$$\deg_2\left(\binom{2^u}{j}\right) = u - \deg_2(j) \geqslant u - (j-2)l = (l+u) - (j-1)l,$$

we obtain

$$[2^u]_s = \sum_{j=1}^{2^u} \binom{2^u}{j} (2^l h)^{j-1} \equiv 2^u + \binom{2^u}{2} 2^l h \equiv 2^u(1 + 2^{l-1}) \pmod{2^{l+u}}.$$

Hence $s^{2^u} = (s-1)[2^u]_s + 1 \equiv 1 \pmod{2^{l+u}}$. Writing $x = 2^u x'$ with $2 \nmid x'$, we have

$$[x]_s = [2^u]_s \sum_{j=0}^{x'-1} (s^{2^u})^j \equiv x'[2^u]_s \equiv (1 + 2^{l-1})x \pmod{2^{l+u}}.$$

□

2.2. The method. It follows from (1.1) that for $k, u, v, u', v' > 0$,

$$\beta^v \alpha^u = \alpha^{ur^v} \beta^v, \tag{2.1}$$

$$(\alpha^u \beta^v)(\alpha^{u'} \beta^{v'}) = \alpha^{u+u'r^v} \beta^{v+v'}, \tag{2.2}$$

$$(\alpha^u \beta^v)^k = \alpha^{u[k]_{r^v}} \beta^{vk}, \tag{2.3}$$

$$[\alpha^u \beta^v, \alpha^{u'} \beta^{v'}] = \exp_\alpha(u'(r^v - 1) - u(r^{v'} - 1)), \tag{2.4}$$

where the notation $[\theta, \eta] = \theta\eta\theta^{-1}\eta^{-1}$ for the commutator is adopted.

In view of (2.4), the commutator subgroup $[H, H]$ is generated by α^{r-1}. The abelianization $H^{\mathrm{ab}} := H/[H, H]$ has a presentation

$$\langle \overline{\alpha}, \overline{\beta}\colon\ q\overline{\alpha} = 0,\ m\overline{\beta} = t\overline{\alpha} \rangle \quad \text{with } q = (r-1, n), \tag{2.5}$$

where additive notation is used and $\overline{\alpha} + \overline{\beta} = \overline{\beta} + \overline{\alpha}$ is implicitly assumed.

Lemma 2.2. *There exists a homomorphism $\sigma\colon H \to H$ with $\sigma(\alpha) = \alpha^{x_1}\beta^{y_1}$, $\sigma(\beta) = \alpha^{x_2}\beta^{y_2}$ if and only if*

$$(r-1, t)y_1 \equiv 0 \pmod{m}, \tag{2.6}$$

$$x_2[m]_{r^{y_2}} + ty_2 - x_1[t]_{r^{y_1}} - \frac{ty_1}{m} t \equiv 0 \pmod{n}, \tag{2.7}$$

$$x_2(r^{y_1} - 1) + x_1([r]_{r^{y_1}} - r^{y_2}) + \frac{(r-1)y_1}{m} t \equiv 0 \pmod{n}. \tag{2.8}$$

P r o o f. Sufficient and necessary conditions for σ to be well-defined are

$$\begin{aligned} \alpha^{x_1[n]_{r^{y_1}}} \beta^{y_1 n} &= \sigma(\alpha)^n = 1, \\ \alpha^{x_2[m]_{r^{y_2}}} \beta^{y_2 m} &= \sigma(\beta)^m = \sigma(\alpha)^t = \alpha^{x_1[t]_{r^{y_1}}} \beta^{y_1 t}, \\ \alpha^{x_2}\beta^{y_2}\alpha^{x_1}\beta^{y_1}\beta^{-y_2}\alpha^{-x_2} &= \sigma(\beta)\sigma(\alpha)\sigma(\beta)^{-1} = \sigma(\alpha)^r = \alpha^{x_1[r]_{r^{y_1}}} \beta^{y_1 r}; \end{aligned}$$

equivalently,

$$(2.9)\qquad ny_1 \equiv 0 \pmod{m}, \qquad x_1[n]_{r^{y_1}} + \frac{ny_1}{m}t \equiv 0 \pmod{n},$$

$$(2.10)\qquad ty_1 \equiv 0 \pmod{m}, \qquad x_2[m]_{r^{y_2}} + y_2 t \equiv x_1[t]_{r^{y_1}} + \frac{ty_1}{m}t \pmod{n},$$

$$(2.11)\quad (r-1)y_1 \equiv 0 \pmod{m}, \quad x_2(1-r^{y_1}) + x_1 r^{y_2} \equiv x_1[r]_{r^{y_1}} + \frac{(r-1)y_1}{m}t \pmod{n}.$$

Due to $t \mid n$, the first parts of (2.9), (2.10), (2.11) are equivalent to the single condition (2.6). Then the second part of (2.9) can be omitted: for each prime divisor p of n, if $p \mid r^{y_1}-1$, then by Lemma 2.1 (I), $\deg_p([n]_{r^{y_1}}) \geqslant \deg_p(n)$; if $p \nmid r^{y_1}-1$, then since $r^{ny_1}-1$ is a multiple of r^m-1, we also have $\deg_p([n]_{r^{y_1}}) = \deg_p(r^{ny_1}-1) \geqslant \deg_p(r^m-1) \geqslant \deg_p(n)$. □

Let Λ denote the set of prime divisors of nm, and for each $p \in \Lambda$, denote

$$(2.12)\qquad a_p = \deg_p(n), \qquad b_p = \deg_p(m), \qquad c_p = \deg_p(t), \qquad d_p = \deg_p(q).$$

Subdivide Λ as $\Lambda = \Lambda_1 \sqcup \Lambda_2 \sqcup \Lambda'$, with

$$(2.13)\quad \Lambda_1 = \{p\colon\ d_p > 0\}, \quad \Lambda_2 = \{p\colon\ a_p > 0,\ d_p = 0\}, \quad \Lambda' = \{p\colon\ b_p > 0,\ a_p = 0\}.$$

Denote

$$(2.14)\qquad e = \deg_2(r+1).$$

It follows from $t \mid n$ and $t(r-1) \equiv 0 \pmod{n}$ that

$$(2.15)\qquad \begin{cases} a_p - d_p \leqslant c_p \leqslant a_p, & p \in \Lambda_1, \\ c_p = a_p, & p \in \Lambda_2, \end{cases}$$

and it follows from $r^m - 1 \equiv 0 \pmod{n}$ and Lemma 2.1 (II) that

$$(2.16)\quad d_p + b_p \geqslant a_p \quad \text{for all } p \in \Lambda_1 \text{ with } (p, d_p) \neq (2,1) \text{ or } (p, d_p, b_p) = (2,1,0);$$

finally, when $d_2 = 1$ and $b_2 > 0$, Lemma 2.1 (II) applied to $r^m - 1 = (r^2)^{m/2} - 1$ implies

$$(2.17)\qquad e + b_2 \geqslant a_2.$$

The condition (2.6) is equivalent to

$$(2.18)\qquad \min\{d_p, c_p\} + \deg_p(y_1) \geqslant b_p \quad \text{for all } p \in \Lambda.$$

Suppose that x_1, x_2, y_1, y_2 satisfy the conditions (2.6), (2.7) and (2.8) and let σ be the endomorphism of H given in Lemma 2.2. Since H is finite, σ is invertible if and only if it is injective, which is equivalent to the condition that both the induced homomorphism $\overline{\sigma}\colon H^{\mathrm{ab}} \to H^{\mathrm{ab}}$ and the restriction $\sigma_0 := \sigma|_{[H,H]}$ are injective.

In the remainder of this subsection, let

$$w = \frac{ty_1}{m}. \tag{2.19}$$

Lemma 2.3. *The homomorphism $\overline{\sigma}$ is injective if and only if*

$$\begin{cases} p \nmid y_2, & p \in \Lambda', \\ p \nmid x_1 + w, & p \in \Lambda_1 \text{ with } b_p c_p = 0, \\ p \nmid x_1 y_2 - x_2 y_1, & p \in \Lambda_1 \text{ with } b_p, c_p > 0. \end{cases} \tag{2.20}$$

Proof. For each $p \in \Lambda' \sqcup \Lambda_1$, let

$$H_p^{\mathrm{ab}} = \langle \overline{\alpha}_p, \overline{\beta}_p \rangle, \quad \text{with } \overline{\alpha}_p = \frac{tq}{p^{c_p+d_p}}\overline{\alpha},\ \overline{\beta}_p = \frac{mq}{p^{b_p+d_p}}\overline{\beta};$$

it is the Sylow p-subgroup of H^{ab}. Then $\overline{\sigma}$ is injective if and only if $\overline{\sigma}_p := \overline{\sigma}|_{H_p^{\mathrm{ab}}}$ is injective for all p. Take an integer z_p with $(t/p^{c_p})z_p \equiv 1 \pmod{p^{d_p}}$. We have

$$\overline{\sigma}_p(\overline{\alpha}_p) = \frac{tq}{p^{c_p+d_p}}(x_1\overline{\alpha} + y_1\overline{\beta}) = x_1\overline{\alpha}_p + \frac{p^{b_p}ty_1}{p^{c_p}m}\overline{\beta}_p, \tag{2.21}$$

$$\overline{\sigma}_p(\overline{\beta}_p) = \frac{mq}{p^{b_p+d_p}}(x_2\overline{\alpha} + y_2\overline{\beta}) = \frac{m}{p^{b_p}}z_p x_2\overline{\alpha}_p + y_2\overline{\beta}_p. \tag{2.22}$$

Let $\check{H}_p = H_p^{\mathrm{ab}}/pH_p^{\mathrm{ab}}$, let $\check{\alpha}_p$, $\check{\beta}_p$ denote the images of $\overline{\alpha}_p$, $\overline{\beta}_p$ under the quotient homomorphism $H_p^{\mathrm{ab}} \to \check{H}_p$, and let $\check{\sigma}_p$ denote the endomorphism of $\check{H}_p$ induced from $\overline{\sigma}_p$. Then $\overline{\sigma}_p$ is injective if and only if $\check{\sigma}_p$ is injective. It follows from (2.21), (2.22) that

$$\check{\sigma}_p(\check{\alpha}_p) = x_1\check{\alpha}_p + \frac{p^{b_p}ty_1}{p^{c_p}m}\check{\beta}_p, \tag{2.23}$$

$$\check{\sigma}_p(\check{\beta}_p) = \frac{m}{p^{b_p}}z_p x_2\check{\alpha}_p + y_2\check{\beta}_p. \tag{2.24}$$

- ▷ If $b_p > d_p = 0$, then $\check{\alpha}_p = 0$, $\check{H}_p = \langle \check{\beta}_p \rangle \cong \mathbb{Z}_p$, and by (2.24), $\check{\sigma}_p$ is injective if and only if $p \nmid y_2$.
- ▷ If $d_p > b_p = 0$, then $\check{\beta}_p = p^{c_p}\check{\alpha}_p$, $\check{H}_p = \langle \check{\alpha}_p \rangle \cong \mathbb{Z}_p$, and by (2.23), $\check{\sigma}_p$ is injective if and only if $p \nmid x_1 + w$.

▷ If $d_p > c_p = 0$, then $\check{\alpha}_p = p^{b_p}\check{\beta}_p$, $\check{H}_p = \langle\check{\beta}_p\rangle$, and by (2.24), $\check{\sigma}_p$ is injective if and only if $p \nmid mz_px_2 + y_2$, which, by (2.7), is equivalent to $p \nmid x_1 + w$.

▷ If $b_p, c_p, d_p > 0$, then $\check{H}_p = \langle\check{\alpha}_p, \check{\beta}_p\rangle \cong \mathbb{Z}_p^2$, and by (2.23), (2.24), $\overline{\sigma}_p$ is invertible if and only if

$$0 \not\equiv x_1y_2 - \frac{p^{b_p}ty_1}{p^{c_p}m}\frac{m}{p^{b_p}}z_px_2 \equiv x_1y_2 - x_2y_1 \pmod p.$$

□

Lemma 2.4. *Suppose $p \nmid x_1y_2 - x_2y_1$ for all $p \in \Lambda_1$ with $d_p < a_p$. Then the homomorphism σ_0 is injective if and only if*

$$r^{y_1} \equiv 1 \pmod{p^{a_p}} \quad \text{and} \quad p \nmid x_1 + w \quad \text{for all } p \in \Lambda_2. \tag{2.25}$$

Proof. Note that $\sigma_0(\alpha^{r-1}) = \alpha^u$, with

$$u = x_1[r-1]_{r^{y_1}} + (r-1)w. \tag{2.26}$$

For each $p \in \Lambda_1$ with $d_p < a_p$, by (2.8) we have

$$\begin{aligned} u &\equiv (1 - r^{y_1})x_1[r-1]_{r^{y_1}} + x_1(r^{y_2} - 1) - x_2(r^{y_1} - 1) \pmod{p^{a_p}} \\ &\equiv (r-1)(x_1y_2 - x_2y_1) \pmod{p^{d_p+1}}, \end{aligned}$$

the second line following from $r^{y_j} - 1 \equiv (r-1)y_j \pmod{p^{2d_p}}$, $j = 1, 2$. Hence

$$\deg_p(u) = d_p. \tag{2.27}$$

Thus σ_0 is injective if and only if $p \nmid u$ for all $p \in \Lambda_2$. For $p \in \Lambda_2$, by (2.15), (2.18),

$$\deg_p(w) = c_p + \deg_p(y_1) - b_p \geqslant c_p = a_p.$$

Hence, if $p \nmid u$ then $p \nmid x_1[r-1]_{r^{y_1}}$ and this implies that $r^{y_1} \equiv 1 \pmod{p^{a_p}}$ (by the argument given). On the other hand, if $r^{y_1} \equiv 1 \pmod p$ then $[r-1]_{r^{y_1}} \equiv r - 1 \not\equiv 0 \pmod{p^{a_p}}$ and hence $p \mid u$ if and only if $p \mid x_1$. Therefore, σ_0 is injective if and only if $p \nmid u$ if and only if $r^{y_1} \equiv 1 \pmod{p^{a_p}}$ and $p \nmid x_1$; the condition $p \nmid x_1$ is equivalent to $p \nmid x_1 + w$. □

Remark 2.5. In order to obtain neat conditions, we prefer $p \nmid x_1 + w$ to $p \nmid x_1$.

Summarizing, sufficient and necessary conditions for σ to be an automorphism are (2.6), (2.7), (2.8), (2.20) and (2.25). Let $(2.7)_p$ denote the condition (2.7) with mod n replaced by mod p^{a_p}. Then (2.7) is equivalent to $(2.7)_p$ for all $p \in \Lambda_1 \sqcup \Lambda_2$ simultaneously. The same holds when $(2.7)_p$ is repleiced by $(2.8)_p$.

Remark 2.6. If $p \in \Lambda_2$, then $p \neq 2$: otherwise $2 \mid n$ but $2 \nmid r-1$, contradicting $n \mid r^m - 1$. Due to (2.15), (2.25), the conditions $(2.7)_p$, $(2.8)_p$ are equivalent to $r^{y_2-1} \equiv 1 \pmod{p^{a_p}}$.

If $p \in \Lambda_1$ with $d_p = a_p$, then $r \equiv 1 \pmod{p^{a_p}}$, hence $(2.8)_p$ is trivial, and $(2.7)_p$ becomes $t(x_1 + w - y_2) \equiv mx_2 \pmod{p^{a_p}}$.

Suppose $p \in \Lambda_1$ with $d_p < a_p$. Note that by (2.16), $b_p > 0$. We will simplify $(2.7)_p$ and $(2.8)_p$, with (2.6) and (2.20) assumed.

By Lemma 2.1 (I), $[r-1]_{r^{y_1}} \equiv r - 1 \pmod{p^{2d_p}}$ when $p \neq 2$ or $p = 2$, $\deg_2(r^{y_1} - 1) > 1$. Hence by (2.27),

$$p \nmid x_1 + w \qquad \text{if } p \neq 2 \text{ or } p = 2,\ d_2 + \deg_2(y_1) > 1. \tag{2.28}$$

By (2.15), (2.16), (2.18),

$$\deg_p(y_1) \geqslant b_p - d_p \geqslant a_p - 2d_p \quad \text{if } (p, d_p) \neq (2,1), \tag{2.29}$$

$$\deg_p(w) = \deg_p(y_1) + c_p - b_p \geqslant c_p - d_p \geqslant a_p - 2d_p \quad \text{if } (p, d_p) \neq (2,1). \tag{2.30}$$

We will use (2.28), (2.29), (2.30) repeatedly.

Lemma 2.7. *If $2 \neq p \in \Lambda_1$, then the conditions $(2.7)_p$ and $(2.8)_p$ hold if and only if*

$$mx_2 \equiv t(x_1 + w - y_2) \pmod{p^{a_p}}, \tag{2.31}$$

$$y_2 \equiv 1 + w \pmod{p^{a_p - d_p}}. \tag{2.32}$$

P r o o f. Abbreviate a_p, b_p, c_p, d_p, $\deg_p(x)$ to a, b, c, d, $\deg(x)$, respectively.

Applying Lemma 2.1, with (2.15), (2.16), (2.29) recalled, we obtain

$$r^{y_1} \equiv 1 + (r-1)y_1, \quad [t]_{r^{y_1}} \equiv t, \quad [m]_{r^{y_2}} \equiv m \pmod{p^a},$$
$$[r]_{r^{y_1}} = (r^{y_1})^{r-1} + [r-1]_{r^{y_1}} \equiv 1 + (r-1) = r \pmod{p^a}.$$

Hence $(2.7)_p$ can be simplified as (2.31) and $(2.8)_p$ can be rewritten as

$$(r-1)y_1x_2 + (r-1)w \equiv (r^{y_2} - r)x_1 \pmod{p^a}. \tag{2.33}$$

By (2.29) and (2.30), $\deg((r-1)y_1x_2 + (r-1)w) \geqslant a - d$, hence

$$\deg(y_2 - 1) + \deg(x_1) = \deg((r^{y_2} - r)x_1) - d \geqslant a - 2d. \tag{2.34}$$

By Lemma 2.1 (II), $r^{y_2-1}-1\equiv(r-1)(y_2-1) \pmod{p^{a-\deg(x_1)}}$, and then

$$(r^{y_2}-r)x_1=(r-1)^2(y_2-1)x_1+(r-1)(y_2-1)x_1\equiv(r-1)(y_2-1)x_1 \pmod{p^a}.$$

Thus (2.33) can be converted into $(y_2-1)x_1\equiv y_1x_2+w \pmod{p^{a-d}}$. Since by (2.31),

$$\begin{aligned}(2.35)\qquad y_1x_2&\equiv\frac{ty_1}{m}(x_1+w-y_2)=w(x_1+w-y_2) \pmod{p^{a+\deg(y_1)-b}}\\&\equiv w(x_1+w-y_2) \pmod{p^{a-d}},\end{aligned}$$

we are led to $(y_2-1)x_1\equiv w(x_1+w-y_2+1) \pmod{p^{a-d}}$, i.e.,

$$(2.36)\qquad (y_2-1-w)(x_1+w)\equiv 0 \pmod{p^{a-d}};$$

due to (2.28), this is equivalent to (2.32). □

Set

(2.37)

$$f(y_1)=\begin{cases}2^{a_2-d_2-1} & \text{if } c_2\neq b_2,\ \min\{b_2,c_2\}=a_2-d_2 \text{ and } \deg_2(y_1)=b_2-d_2,\\ 0 & \text{otherwise.}\end{cases}$$

Lemma 2.8. *If $2\in\Lambda_1$, then the conditions $(2.7)_2$ and $(2.8)_2$ hold if and only if*

(i) *if $b_2=c_2=d_2=1$ (so that $a_2=2$), then no additional condition is required;*

(ii) *if $d_2=1$ and $\max\{b_2,c_2\}>1$, then $2\mid y_1$, $\deg_2(x_2)\geqslant a_2-b_2-e+1$ and*

$$(2.38)\qquad w\equiv 2^{e-1}(y_1-y_2+1) \pmod{2^{a_2-1}};$$

(iii) *if $d_2>1$, then*

$$(2.39)\qquad mx_2\equiv t(x_1+w-y_2) \pmod{2^{a_2}},$$

$$(2.40)\qquad y_2\equiv (1+w+f(y_1)) \pmod{2^{a_2-d_2}}.$$

Proof. Abbreviate a_2, b_2, c_2, d_2, $\deg_2(x)$ to a, b, c, d, $\deg(x)$, respectively.

(i) For any $x,u>0$, we have $r^x\equiv 1+2x \pmod 4$, and

$$[u]_{r^x}=\sum_{i=0}^{u-1}r^{ix}\equiv\sum_{i=0}^{u-1}(1+2ix)\equiv u+u(u-1)x \pmod 4.$$

In particular, $[m]_{r^{y_2}} \equiv 2+2y_2$, $[t]_{r^{y_1}} \equiv 2+2y_1$, $[r]_{r^{y_1}} \equiv 3+2y_1 \pmod 4$. The conditions $(2.7)_2$, $(2.8)_2$ can be converted into, respectively,

$$(2.41) \qquad (x_2+1)(y_2+1)-(x_1+1)(y_1+1) \equiv 0 \pmod 2,$$

$$(2.42) \qquad x_2y_1 + x_1(1+y_1-y_2) + y_1 \equiv 0 \pmod 2.$$

Due to (2.20), $x_2y_1 \equiv x_1y_2 + 1 \pmod 2$, hence (2.42) is equivalent to $(x_1+1)\times(y_1+1) \equiv 0 \pmod 2$, which is true since by (2.20), at least one of x_1, y_1 is odd. Then similarly, (2.41) also holds.

(ii) We first show $2 \mid y_1$. Assume on the contrary that $2 \nmid y_1$. By (2.18), $b=1$, so that $c>1$. By $(2.7)_2$, $x_2[m]_{r^{y_2}} \equiv 0 \pmod 4$, which forces $2 \nmid y_2$: if $2 \mid y_2$, then $r^{y_2} \equiv 1 \pmod 4$ so that $4 \nmid [m]_{r^{y_2}}$, and we would get $2 \mid x_2$, contradicting (2.20). Then $r^{y_j} \equiv -1 \pmod 4$, $j=1,2$, and $[r]_{r^{y_1}} \equiv 1 \pmod 4$, so $(2.8)_2$ implies $2(x_1-x_2) \equiv 0 \pmod 4$. But this contradicts (2.20).

Thus $2 \mid y_1$. By (2.20), $2 \nmid x_1y_2$; by (2.28), $2 \mid w$. Hence

$$(2.43) \qquad t(x_1+w-y_2) \equiv 0 \pmod{2^a}.$$

By (2.17), (2.18), $1+\deg(y_1)+e \geqslant b+e \geqslant a$, hence

$$(2.44) \qquad \deg(r^{y_1}-1) = \deg((r^2)^{y_1/2}-1) = e+\deg(y_1) \geqslant a-1.$$

When $c>1$, applying Lemma 2.1 we obtain

$$\begin{aligned}
[t]_{r^{y_1}} &\equiv (1+2^{e+\deg(y_1)-1})t \pmod{2^{e+\deg(y_1)+c}} \equiv t \pmod{2^a},\\
[r]_{r^{y_1}} &= (r^{y_1})^{r-1} + [r-1]_{r^{y_1}} \equiv 1+(1+2^{e+\deg(y_1)-1})(r-1) \pmod{2^{e+\deg(y_1)+1}}\\
&\equiv r+2^ey_1 \pmod{2^a};
\end{aligned}$$

when $c=1$ so that $a=2$, these congruence relations obviously hold.

Due to (2.43), the condition $(2.7)_2$ becomes $x_2[m]_{r^{y_2}} \equiv 0 \pmod{2^a}$. Since $\deg(r^{y_2}+1) = \deg(r+1) = e$ and $[m]_{r^{y_2}} = (r^{y_2}+1)[m/2]_{r^{2y_2}}$, we have $\deg([m]_{r^{y_2}}) = e+b-1$. Hence

$$\deg(x_2) \geqslant a-b-e+1.$$

This together with (2.18) implies

$$\deg((r^{y_1}-1)x_2) = \deg(y_1)+e+\deg(x_2) \geqslant b-1+e+\deg(x_2) \geqslant a.$$

Then $(2.8)_2$ becomes

$$(2.45) \qquad x_1(r^{y_2}-r-2^ey_1) \equiv (r-1)w \pmod{2^a}.$$

Since $\deg(r^{y_2-1}-1)=\deg((r^2)^{(y_2-1)/2}-1)=e+\deg(y_2-1)$, we have $r^{y_2-1}-1=2^e(y_2-1)z$ for some odd z. Using $2^{e+1}y_1\equiv 2(r-1)w\equiv 0 \pmod{2^a}$, we can convert (2.45) into (2.38).

(iii) Applying Lemma 2.1 (with (2.29) recalled), we obtain

$$\begin{aligned} r^{y_1} &\equiv \begin{cases} 1+(r-1)y_1, & 2\nmid y_1 \\ 1+(r-1+2^{2d-1})y_1, & 2\mid y_1 \end{cases} \pmod{2^a}, \\ [r]_{r^{y_1}} &\equiv (r+2^{2d-1}y_1) \pmod{2^a}, \\ [t]_{r^{y_1}} &\equiv (1+2^{d-1}y_1)t \pmod{2^a}, \\ [m]_{r^{y_2}} &\equiv (1+2^{d-1}y_2)m \pmod{2^a}. \end{aligned}$$

We deal with the cases $2\mid y_1$ and $2\nmid y_1$ separately.

(iii 1) If $2\mid y_1$, then by (2.20), $2\nmid x_1y_2$, and by (2.28), $2\mid w$. The condition $(2.7)_2$ becomes

$$(1+2^{d-1}y_2)mx_2\equiv t(x_1+w-y_2) \pmod{2^a}, \tag{2.46}$$

which can be converted into (2.39) via multiplying by $1-2^{d-1}y_2$. Moreover, (2.46) implies $b+\deg(x_2)\geqslant\min\{c+1,a\}$, hence

$$\begin{aligned} 2d-1+\deg(x_2)+\deg(y_1) &\geqslant 2d-1+(\min\{c+1,a\}-b)+(b-d) \\ &= d-1+\min\{c+1,a\}\geqslant a. \end{aligned}$$

As a result, $x_2(r^{y_1}-1)\equiv(r-1)x_2y_1 \pmod{2^a}$. Using this and $2^{2d-1}(x_1-1)y_1\equiv 0 \pmod{2^a}$, we may convert $(2.8)_2$ into

$$(r-1)x_2y_1+2^{2d-1}y_1+(r-r^{y_2})x_1+(r-1)w\equiv 0 \pmod{2^a}. \tag{2.47}$$

By an argument similar to that used for deducing (2.34) in the proof of Lemma 2.7, we obtain $\deg(y_2-1)\geqslant a-2d$, and then by Lemma 2.1 (II),

$$r^{y_2-1}-1\equiv(1+2^{d-1})(r-1)(y_2-1) \pmod{2^a}.$$

Using $(r-1)(r^{y_2-1}-1)\equiv 0 \pmod{2^a}$, we can convert (2.47) further into

$$(y_2-1)x_1\equiv y_1x_2+w+2^{d-1}(y_1-y_2+1) \pmod{2^{a-d}}. \tag{2.48}$$

Similarly to (2.35), it follows from (2.39) that $y_1x_2\equiv w(x_1+w-y_2) \pmod{2^{a-d}}$, and then (2.48) becomes

$$(y_2-1-w)(x_1+w+2^{d-1})\equiv 2^{d-1}(y_1-w) \pmod{2^{a-d}}. \tag{2.49}$$

From (2.29) and (2.30) we see that $\deg(y_1 - w) \geqslant a - 2d$, and the equality holds if and only if one of the following cases occurs:

▷ $\deg(w) > \deg(y_1) = a-2d$, which is equivalent to $\deg(y_1) = b-d$ and $c > b = a-d$;

▷ $\deg(y_1) > \deg(w) = a-2d$, which is equivalent to $\deg(y_1) = b-d$ and $b > c = a-d$.

Thus (2.49) becomes

$$(y_2 - 1 - w)(x_1 + w + 2^{d-1}) \equiv f(y_1) \equiv f(y_1)(x_1 + w + 2^{d-1}) \pmod{2^{a-d}},$$

which is equivalent to (2.40).

(iii 2) If $2 \nmid y_1$, then $d, c \geqslant b$, and $2d \geqslant a$. By Lemma 2.1 (II), $r^{y_2} \equiv 1 + (r-1)y_2 \pmod{2^a}$, hence $(2.7)_2$, $(2.8)_2$ become, respectively,

$$(1 + 2^{d-1}y_2)mx_2 + ty_2 \equiv (1 + 2^{d-1})tx_1 + tw \pmod{2^a}, \tag{2.50}$$

$$(y_2 - 1)x_1 \equiv y_1x_2 + w + 2^{d-1}x_1 \pmod{2^{a-d}}. \tag{2.51}$$

If $c = b$, then by (2.28), $2 \mid x_1$, and by (2.20), $2 \nmid x_2$. By (2.50), $2 \mid y_2$, and then (2.50) becomes (2.39). We can reduce (2.51) to $y_2 - 1 \equiv w \pmod{2^{a-d}}$ similarly to the proof of Lemma 2.7.

Now assume $c > b$ so that $2 \mid w$. By (2.28), $2 \nmid x_1$. Since $c + d - 1 \geqslant b + d \geqslant a$, we can reduce (2.50) to (2.39) via multiplying by $1 - 2^{d-1}y_2$. If $2d > a$, then still similarly to the proof of Lemma 2.7, we can reduce (2.51) to $y_2 - 1 \equiv w \pmod{2^{a-d}}$; if $2d = a$, then $b = a - d = d$, then similarly to (iii 1), we can reduce (2.51) to $y_2 - 1 \equiv w + 2^{a-d-1} \pmod{2^{a-d}}$.

Thus in any case, $(2.7)_2$, $(2.8)_2$ are equivalent to (2.39), (2.40). □

2.3. Main result.

Let m_0 be the smallest positive integer k such that $r^k \equiv 1 \pmod{p^{a_p}}$ for all $p \in \Lambda_2$. Combining Lemma 2.3, Lemma 2.4, Remark 2.6, Lemma 2.7 and Lemma 2.8, we establish

Theorem 2.9. *Each automorphism of $H(n, m; t, r)$ is given by*

$$\alpha^u\beta^v \mapsto \exp_\alpha(x_1[u]_{r^{y_1}} + r^{y_1u}x_2[v]_{r^{y_2}})\beta^{y_1u+y_2v}, \quad u, v > 0,$$

for a unique quadruple (x_1, x_2, y_1, y_2) with $0 < x_1, x_2 \leqslant n$, $0 < y_1, y_2 \leqslant m$ and such that

(i) *for all $p \in \Lambda$,*

$$\begin{cases} p \nmid y_2, & p \in \Lambda', \\ p \nmid x_1 + ty_1/m, & p \in \Lambda_2 \text{ or } p \in \Lambda_1 \text{ with } b_pc_p = 0, \\ p \nmid x_1y_2 - x_2y_1, & p \in \Lambda_1 \text{ with } b_p, c_p > 0; \end{cases}$$

(ii) $(r-1,t)y_1 \equiv 0 \pmod m$ *and* $y_1 \equiv y_2 - 1 \equiv 0 \pmod{m_0}$*;*

(iii) *for all* $p \in \Lambda_1$ *with* $p \neq 2$ *or* $p = 2$*,* $a_2 = d_2$*,*

$$mx_2 \equiv t(x_1 + ty_1/m - y_2) \pmod{p^{a_p}},$$
$$y_2 \equiv 1 + ty_1/m \pmod{p^{a_p - d_p}};$$

(iv) *if* $\max\{b_2, c_2\} > d_2 = 1$ *and* $a_2 > 1$*, then* $2 \mid y_1$*,* $\deg_2(x_2) \geqslant a_2 - b_2 - e + 1$ *and*

$$ty_1/m \equiv 2^{e-1}(y_1 - y_2 + 1) \pmod{2^{a_2 - 1}};$$

(v) *if* $d_2 > 1$*, then*

$$mx_2 \equiv t(x_1 + ty_1/m - y_2) \pmod{2^{a_2}},$$
$$y_2 \equiv 1 + ty_1/m + f(y_1) \pmod{2^{a_2 - d_2}}.$$

References

[1] *J. N. S. Bidwell, M. J. Curran*: The automorphism group of a split metacyclic p-group. Arch. Math. *87* (2006), 488–497. zbl MR doi

[2] *H.-M. Chen*: Reduction and regular t-balanced Cayley maps on split metacyclic 2-groups. Available at ArXiv:1702.08351 [math.CO] (2017), 14 pages.

[3] *M. J. Curran*: The automorphism group of a split metacyclic 2-group. Arch. Math. *89* (2007), 10–23. zbl MR doi

[4] *M. J. Curran*: The automorphism group of a nonsplit metacyclic p-group. Arch. Math. *90* (2008), 483–489. zbl MR doi

[5] *R. M. Davitt*: The automorphism group of a finite metacyclic p-group. Proc. Am. Math. Soc. *25* (1970), 876–879. zbl MR doi

[6] *M. Golasiński, D. L. Gonçalves*: On automorphisms of split metacyclic groups. Manuscripta Math. *128* (2009), 251–273. zbl MR doi

[7] *C. E. Hempel*: Metacyclic groups. Commun. Algebra *28* (2000), 3865–3897. zbl MR doi

[8] *H. J. Zassenhaus*: The Theory of Groups. Chelsea Publishing Company, New York, 1958. zbl MR

Authors' addresses: Haimiao Chen, Beijing Technology and Business University, Fucheng Road 11/33, Beijing 10048, Haidian, China, e-mail: `chenhm@pku.edu.cn`; Yueshan Xiong, Huazhong University of Science and Technology, Luoyu Road 1037, Wuhan 430074, Hogshan, Hubei, China, e-mail: `xiongyueshan@gmail.com`; Zhongjian Zhu, Wenzhou University, 276 Xueyuan Middle Rd, Lucheng, Wenzhou 325035, Zhejiang, China, e-mail: `zhuzhongjianzzj@126.com`.