Chin. Ann. Math. Ser. B
41(2), 2020, 241–266
DOI: 10.1007/s11401-020-0197-6

Chinese Annals of Mathematics, Series B

The Subgroups of Finite Metacyclic Groups*

Xu YANG[1]

Abstract In this paper, the author characterizes the subgroups of a finite metacyclic group K by building a one to one correspondence between certain 3-tuples $(k, l, \beta) \in \mathbb{N}^3$ and all the subgroups of K. The results are applied to compute some subgroups of K as well as to study the structure and the number of p-subgroups of K, where p is a fixed prime number. In addition, the author gets a factorization of K, and then studies the metacyclic p-groups, gives a different classification, and describes the characteristic subgroups of a given metacyclic p-group when $p \geq 3$. A "reciprocity" relation on enumeration of subgroups of a metacyclic group is also given.

Keywords Metacyclic groups, Subgroups, Metacyclic p-groups, Characteristic subgroups
2000 MR Subject Classification 20D15, 20D25, 20D30

1 Introduction

For a fixed finite group K, K is metacyclic if and only if $\exists A \lhd K$, such that both A and K/A are cyclic. Hölder started studying the metacyclic groups rather early (around 1890s). He showed that a finite metacyclic group can be represented by two generators and three relations (Hölder theorem, see [9, 19]). Basmaji [2] gave a necessary and sufficient condition to determine whether two fixed metacyclic groups are isomorphic (see [11]). His work is based on the Hölder theorem. Afterwards, there are several classifications of the metacyclic p-groups (see [3, 7, 9, 11–15, 17–18]). Sim [16] classified the metacyclic groups of odd order, and Hempel [9] classified all the metacyclic groups. In both [9] and [16], the metacyclic group K was characterized by a certain kind of 8-tuples of odd positive integers $(\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \theta, \kappa)$.

Similar to [2], our discussion is based on the Hölder theorem. This makes it easier to compute as well as enables us to use the arithmetic method (mainly congruence in $\mathbb{Z}$) to study the given group.

Now let K be a finite metacyclic group. By Hölder theorem, we can assume that

$$K = \langle \tau, \eta \mid \tau^n = 1, \eta^m = \tau^g, \eta\tau\eta^{-1} = \tau^h \rangle,$$

where $(m, n, g, h) \in \mathbb{N}^4$, $g < n$, $h < n$, $n \mid g(h-1)$, $n \mid (h^m - 1)$. Let $T = \{A \mid A \leq K\}$.

Manuscript received May 25, 2016. Revised September 2, 2017.
[1]School of Mathematical Sciences, Fudan University, Shanghai 200433, China.
E-mail:12110180008@fudan.edu.cn
*This work was supported by the National Natural Science Foundation of China (No. 11331006).

Consider the subset Γ of $\mathbb{N}^3$ and the map Ψ, where

$$\Gamma = \Big\{(k,l,\beta) \mid l \mid n, l \mid k, k \mid ml, \beta < \frac{n}{l}, \beta\Big(\sum_{j=0}^{\frac{k}{l}-1} h^{\frac{mlj}{k}}\Big) \equiv -g \, \Big(\mathrm{mod}\, \frac{n}{l}\Big)\Big\},$$

$$\Psi: \ \Gamma \to T \ (\forall (k,l,\beta) \in \Gamma: \ \Psi(k,l,\beta) = \langle \tau^\beta \eta^{\frac{ml}{k}}, \tau^{\frac{n}{l}} \rangle).$$

We show in Theorem 3.2 that Ψ is a one to one correspondence from Γ to T. Using Ψ, we study the construction of the subgroups. In Theorem 3.3, for any $A \le K$, we give a necessary and sufficient condition to determine whether $A \lhd K$, and when $A \lhd K$, we give the structure of K/A. We then compute several subgroups of K, including the upper and lower central series of K, the Carter subgroup C, the Fitting subgroup $F(K)$ and the Frattini subgroup $\Phi(K)$. We show that K is the semidirect product of K_∞ and its Carter subgroup C, i.e.,

$$K = K_\infty C, \quad K_\infty \cap C = \{1_K\}, \tag{1.1}$$

where K_∞ is the intersection of every term in the lower central series. Conversely, for any $B \le K$, if B is nilpotent and $BK_\infty = K$, then B is a Carter subgroup of K. The p-subgroups of K (where p is a prime number) are also studied, and results on counting the number of the p-subgroups and the structure of the Sylow p-group of K are given.

Two fundamental theorems of this note are proved in Section 3 (Theorems 3.2 and 3.3), and subgroups of K are studied in Section 4.

In Section 5, we study the metacyclic p-groups. By setting an isomorphism invariant for any metacyclic group K (Definition 5.1), we give a different classification for metacyclic p-groups. Section 6 and Section 7 are applications of the results we obtain. In Section 6, we consider the problem that for a given metacyclic group K, when for any $k \in \mathbb{N}, k \mid |K|$, the number of subgroups of order k and the number of subgroups of index k are the same. Finally, in Section 7, we find all the characteristic subgroups of a given metacyclic p-group G, where p is an odd prime number.

2 Some Notations

In this section, we give some notations we need.

First, we provide the notation of "Hölder-tuple", which we use throughout the paper, and it also leads to the idea of Theorem 3.2.

Definition 2.1 *Consider the tuple* $((m,n,g,h),K,T,\Gamma,\Psi)$. *We say* $((m,n,g,h),K,T,\Gamma,\Psi)$ *is a Hölder-tuple if and only if the next four conditions hold.*

(1) $(m,n,g,h) \in \mathbb{N}^4$, $m \ge 1, n \ge 1, g < n, h < n, n \mid g(h-1), n \mid (h^m - 1)$.

(2) $K = \langle \tau, \eta \mid \tau^n = 1, \eta^m = \tau^g, \eta\tau\eta^{-1} = \tau^h \rangle$.

(3) $T = \{A \mid A \le K\}$, *and* Γ *is the following subset of* $\mathbb{N}^3$,

$$\Gamma = \Big\{(k,l,\beta) \mid l \mid n, l \mid k, k \mid ml, \beta < \frac{n}{l}, \beta\Big(\sum_{j=0}^{\frac{k}{l}-1} h^{\frac{mlj}{k}}\Big) \equiv -g \, \Big(\mathrm{mod}\, \frac{n}{l}\Big)\Big\}.$$

(4) Ψ *is the map from* Γ *to* T *defined as follows,*

$$\Psi: \ \Gamma \to T \ (\forall (k,l,\beta) \in \Gamma: \ \Psi(k,l,\beta) = \langle \tau^\beta \eta^{\frac{ml}{k}}, \tau^{\frac{n}{l}} \rangle).$$

Throughout the paper, we denote Ω as the following subset of $\mathbb{N}^4$:

$$\Omega = \{(m,n,g,h) \mid m \geq 1, n \geq 1, g < n, h < n, n \mid g(h-1), n \mid (h^m - 1)\}.$$

For any $(m,n,g,h) \in \Omega$ and any group K, we say $K \cong (m,n,g,h)$ if and only if $K \cong \langle \tau, \eta \mid \tau^n = 1, \eta^m = \tau^g, \eta\tau\eta^{-1} = \tau^h \rangle$. And for any two 4-tuples (m,n,g,h) and $(\widetilde{m}, \widetilde{n}, \widetilde{g}, \widetilde{h})$ in Ω, we write $(m,n,g,h) \cong (\widetilde{m}, \widetilde{n}, \widetilde{g}, \widetilde{h})$ if and only if the following isomorphism relation between groups holds:

$$\langle \tau, \eta \mid \tau^n = 1, \eta^m = \tau^g, \eta\tau\eta^{-1} = \tau^h \rangle \cong \langle u, v \mid u^{\widetilde{n}} = 1, v^{\widetilde{m}} = u^{\widetilde{g}}, vuv^{-1} = u^{\widetilde{h}} \rangle.$$

For any prime number p and $a \in \mathbb{Z},\ a \neq 0$, denote $O(p,a)$ as the largest nonnegative integer γ satisfying $p^\gamma \mid a$. Let $O(p,0) = +\infty$ for convenience. For $(b,c) \in \mathbb{Z} \times \mathbb{Z},\ \gcd(b,c) = 1$, we write $\mathrm{ord}(c,b)$ as the smallest positive integer $\alpha \geq 1$ where $b^\alpha \equiv 1 \pmod{c}$. For $(b,c) \in \mathbb{Z} \times \mathbb{Z},\ c \neq 0$, let the notation $\lfloor \frac{b}{c} \rfloor$ denote the largest integer β satisfying $\beta \leq \frac{b}{c}$, and let $b\%c$ denote the only integer $\lambda \in \{0, 1, \cdots, |c|-1\}$ where $b \equiv \lambda \pmod{c}$. For fixed $n \in \mathbb{N},\ n \geq 2$, let $U_{(n)}$ denote the set $\{a \mid a \in \mathbb{N},\ a \leq n,\ \gcd(a,n) = 1\}$, and let $\odot_{(n)}$ denote the operation on $\mathbb{Z}$ defined as follows:

$$\forall (b,c) \in \mathbb{Z} \times \mathbb{Z}: \ b \odot_{(n)} c = (bc)\%n.$$

Therefore $(U_{(n)}, \odot_{(n)})$ is an Abelian group with unit 1. $\forall a \in U_{(n)}$, denote $\langle a \rangle_{(n)}$ as the subgroup of $(U_{(n)}, \odot_{(n)})$ generated by $\{a\}$.

Fix $a \in \mathbb{Z}$, let $X(a)$ denote the set of all the prime factors of a.

Let K be a group, $\forall (a,b) \in K \times K$, denote the commutator of (a,b): $[a,b] = aba^{-1}b^{-1}$. And for any $k \in \mathbb{N}, k \geq 3$, $\forall (x_1, \cdots, x_k) \in K^k$, define the commutator of $(x_1, \cdots, x_k)$ by induction: $[x_1, \cdots, x_k] = [x_1, [x_2, \cdots, x_k]]$. We write $K_\infty = \bigcap_{s \in \mathbb{N}, s \geq 2} [\underbrace{K, \cdots, K}_{s}]$, $Z_\infty(K) = \bigcup_{i \in \mathbb{N}} Z_i(K)$, where $\{1_K\} = Z_0(K)$, and $\forall i \in \mathbb{N}$, $Z_{i+1}(K)/Z_i(K) = Z(K/Z_i(K))$. Following the notations in [8] and [10], the Fitting subgroup of K is denoted as $F(K)$ and the Frattini subgroup of K is denoted as $\Phi(K)$. If K is finite, we write $\exp(K) = \mathrm{lcm}(o(a) \mid a \in K)$.

Finally, we mention that for a finite metacyclic group K, K is said to be split if and only if $\exists (m,n,0,h) \in \Omega$, such that $K \cong (m,n,0,h)$.

3 Characterization of the Subgroups

In this section, we state and prove our fundamental theorem (Theorems 3.2–3.3).

First, we state the following Hölder theorem (see [9, 19]), which is used throughout the paper. We state it in a relatively specific way, in order to tell more details.

Theorem 3.1 (Hölder) (1) *Let G be a finite metacyclic group, $A \leq G$, where $A \lhd G$, both A and G/A are cyclic, then $\exists (m_1, n_1, g_1, h_1) \in \Omega$, such that $n_1 = |A|$, $m_1 = |G/A|$, $G \cong (m_1, n_1, g_1, h_1)$.*

(2) *Fix $(m,n,g,h) \in \Omega$, let $K = \langle \tau, \eta \mid \tau^n = 1, \eta^m = \tau^g, \eta\tau\eta^{-1} = \tau^h \rangle$, then the following statements hold.*

(2.1) *$o(\tau) = n$, $\langle \tau \rangle \lhd K$, $\forall j \in \{1, \cdots, m-1\}: \ \eta^j \notin \langle \tau \rangle$.*

(2.2) *$K/\langle \tau \rangle = \langle\ \eta\langle \tau \rangle\ \rangle$, $|K/\langle \tau \rangle| = m$, K is metacyclic and $|K| = mn$.*

(2.3) $\forall (a,b),\ (c,d)\in\{0,1,\cdots,n-1\}\times\{0,1,\cdots,m-1\}$, *we have*:

$$\tau^a\eta^b=\tau^c\eta^d\ \Rightarrow\ (a,b)=(c,d).$$

Hence $K=\{\tau^i\eta^j\mid (i,j)\in\mathbb{N}\times\mathbb{N}, i<n, j<m\}$.

The following two lemmas are basic and used throughout the paper.

Lemma 3.1 *Fix* $(m,n,g,h)\in\mathbb{Z}^4,\ m\ge 1,\ n\ge 1$. *Let* G *be a group, and fix* $(\tau,\eta)\in G\times G$, *such that* $o(\tau)=n,\ \eta^m=\tau^g,\ \eta\tau\eta^{-1}=\tau^h$, *then*

(1) $g(h-1)\equiv 0\ (\mathrm{mod}\, n),\ h^m\equiv 1\ \big(\mathrm{mod}\, n\big),\ (m,n,g\%n,h\%n)\in\Omega$.

(2) *Fix* $(a,b)\in\mathbb{Z}\times\mathbb{N},\ (e,f)\in\mathbb{Z}\times\mathbb{N},\ k\in\mathbb{N},\ k\ge 1$.

(2.1) $(\tau^a\eta^b)(\tau^e\eta^f)=\tau^{a+eh^b}\eta^{b+f},\ (\tau^a\eta^b)^k=\tau^{a\left(\sum\limits_{i=0}^{k-1}h^{bi}\right)}\eta^{bk}$.

(2.2) $(\tau^a\eta^b)(\tau^e\eta^f)=(\tau^e\eta^f)(\tau^a\eta^b)\Leftrightarrow e(h^b-1)\equiv a(h^f-1)\ (\mathrm{mod}\, n)$.

(2.3) $[\underbrace{\tau^a\eta^b,\cdots,\tau^a\eta^b}_{k},\tau^e\eta^f]=\tau^{e(h^b-1)^k-a(h^f-1)(h^b-1)^{k-1}}$.

Lemma 3.2 *Let* $((m,n,g,h),K,T,\Gamma,\Psi)$ *be a Hölder-tuple.*

(1) *Fix* $(k,l,\beta)\in\Gamma$, *then* $\Psi(k,l,\beta)\cong\Big(\frac{k}{l},l,\dfrac{\big(\beta\big(\sum\limits_{j=0}^{\frac{k}{l}-1}h^{\frac{mlj}{k}}\big)+g\big)\%n}{\frac{n}{l}},h^{\frac{ml}{k}}\%l\Big)\in\Omega$. *Moreover*, $|\Psi(k,l,\beta)|=k,\ |\Psi(k,l,\beta)\cap\langle\tau\rangle|=l,\ \Psi(k,l,\beta)\cap\langle\tau\rangle=\langle\tau^{\frac{n}{l}}\rangle$.

(2) *Fix* $(\rho,\delta,\varsigma)\in\Gamma$, *and* $(e,f)\in\mathbb{N}\times\{0,1,\cdots,m\}$, *then*

$$\tau^e\eta^f\in\Psi(\rho,\delta,\varsigma)\Leftrightarrow m\delta\mid f\rho,\ e\equiv\varsigma\Big(\sum_{j=0}^{\frac{\rho f}{m\delta}-1}h^{\frac{m\delta j}{\rho}}\Big)\ \Big(\mathrm{mod}\,\frac{n}{\delta}\Big).$$

(3) *Fix* $(c,d)\in\mathbb{N}^2,\ c\mid n,\ c\mid g,\ d\mid m$, *then* $\big(\frac{mn}{cd},\ \frac{n}{c},0\big)\in\Gamma,\ \Psi\big(\frac{mn}{cd},\ \frac{n}{c},0\big)=\langle\tau^c,\eta^d\rangle$. *Moreover*, $\forall(a,b)\in\mathbb{N}^2:(\tau^a\eta^b)\in\langle\tau^c,\eta^d\rangle\Leftrightarrow\ c\mid a,\ d\mid b$.

Proof (1) Write

$$\vartheta=\frac{\Big(\beta\Big(\sum\limits_{j=0}^{\frac{k}{l}-1}h^{\frac{mlj}{k}}\Big)+g\Big)\%n}{\dfrac{n}{l}}.$$

Since $(k,l,\beta)\in\Gamma$, hence $\vartheta\in\mathbb{Z}$. By (2.1) of Theorem 3.1, $\forall w\in\mathbb{N},\ 1\le w<\frac{k}{l}:(\tau^\beta\eta^{\frac{ml}{k}})^w\notin\langle\tau\rangle$. Consider $(\tau^{\frac{n}{l}},\tau^\beta\eta^{\frac{ml}{k}})$ and $(\frac{k}{l},l,\vartheta,h^{\frac{ml}{k}}\%l)\in\mathbb{N}^4$. By Lemma 3.1 (2), we have:

$$o\big(\tau^{\frac{n}{l}}\big)=l,\quad \big(\tau^\beta\eta^{\frac{ml}{k}}\big)^{\frac{k}{l}}=\big(\tau^{\frac{n}{l}}\big)^\vartheta,\quad \big(\tau^\beta\eta^{\frac{ml}{k}}\big)\tau^{\frac{n}{l}}\big(\tau^\beta\eta^{\frac{ml}{k}}\big)^{-1}=\big(\tau^{\frac{n}{l}}\big)^{(h^{\frac{ml}{k}}\%l)}.$$

Hence $|\Psi(k,l,\beta)|=k$, and by Lemma 3.1, the rest follows.

(2) $\Leftarrow$ Write $\mu=\frac{f\rho}{m\delta}$. Let $\lambda\in\mathbb{Z}$, where

$$\frac{n\lambda}{\delta}=e-\varsigma\Big(\sum_{j=0}^{\frac{\rho f}{m\delta}-1}h^{\frac{m\delta j}{\rho}}\Big).$$

By Lemma 3.1 (2), we have $\tau^e\eta^f = \tau^{\frac{n\lambda}{\delta}}(\tau^\varsigma\eta^{\frac{m\delta}{\rho}})^\mu \in \Psi(\rho,\delta,\varsigma)$.

$\Rightarrow$ By (1), $\exists(\lambda_1,\mu_1) \in \mathbb{Z}\times\{1,\cdots,\frac{\rho}{\delta}\}$, such that $\tau^e\eta^f = \tau^{\frac{n\lambda_1}{\delta}}(\tau^\varsigma\eta^{\frac{m\delta}{\rho}})^{\mu_1}$. If $f=0$, then $\tau^e \in \Psi(\rho,\delta,\varsigma)\cap\langle\tau\rangle = \langle\tau^{\frac{n}{\delta}}\rangle$, and $\frac{n}{\delta} \mid e$. If $f\neq 0$, by Lemma 3.1 (2), $f \equiv \frac{m\delta\mu_1}{\rho} \pmod m$, $1\le f\le m, 1\le \frac{m\delta\mu_1}{\rho}\le m$, thus $f=\frac{m\delta\mu_1}{\rho}$, $\mu_1 = \frac{\rho f}{m\delta}$. Since $o(\tau)=n$, we deduce that

$$e \equiv \varsigma\Big(\sum_{j=0}^{\frac{\rho f}{m\delta}-1} h^{\frac{m\delta j}{\rho}}\Big)\Big(\mathrm{mod}\,\frac{n}{\delta}\Big).$$

(3) This follows from (2) and the fact $\tau^a\eta^b = \tau^{a+\lfloor\frac{b}{m}\rfloor g}\eta^{b\% m}$.

Now we state and prove our two fundamental theorems.

Theorem 3.2 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple.*

(1) *Fix $(b,a,\alpha)\in\Gamma$, $(f,e,\gamma)\in\Gamma$, then*

$$\Psi(b,a,\alpha)\subseteq\Psi(f,e,\gamma)\Leftrightarrow a\mid e,\quad be\mid af,\quad \alpha\equiv\gamma\Big(\sum_{j=0}^{\frac{af}{be}-1} h^{\frac{mej}{f}}\Big)\Big(\mathrm{mod}\,\frac{n}{e}\Big).$$

(2) *Ψ is a one to one correspondence from Γ to T.*

Proof (1) This follows immediately from Lemma 3.2 (2).

(2) (1) already implies that Ψ is injective, and it remains to show $\Psi[\Gamma]=T$. To show $\Psi[\Gamma]=T$, we fix $H\le K$. Let $\rho=|H|$, $\delta=|H\cap\langle\tau\rangle|$. Hence we get

$$\delta\mid\rho,\quad \delta\mid n,\quad H\cap\langle\tau\rangle=\langle\tau^{\frac{n}{\delta}}\rangle,\quad |H/H\cap\langle\tau\rangle| = |H\langle\tau\rangle/\langle\tau\rangle| = \frac{\rho}{\delta},\quad \frac{\rho}{\delta}\mid m.$$

Since $K/\langle\tau\rangle$ is cyclic and $|K/\langle\tau\rangle|=m$, we have $(\langle\tau\rangle\eta^{\frac{m\delta}{\rho}})\in H\langle\tau\rangle/\langle\tau\rangle$. Hence $\exists v\in H$, $\langle\tau\rangle v = \langle\tau\rangle\eta^{\frac{m\delta}{\rho}}$. Thus $\exists\pi\in\mathbb{N}$, where $v=\tau^\pi\eta^{\frac{m\delta}{\rho}}$. Since $\langle\tau^{\frac{n}{\delta}}\rangle = H\cap\langle\tau\rangle\lhd H$, $v\in H$, we have $v^{\frac{\rho}{\delta}}\in\langle\tau^{\frac{n}{\delta}}\rangle$. Write $\chi=\sum_{j=0}^{\frac{\rho}{\delta}-1} h^{\frac{m\delta j}{\rho}}$. By Lemma 3.1 (2), o$\big(v^{\frac{\rho}{\delta}} = \tau^{\pi\chi+g}$. Hence we get

$$\frac{n}{\delta}\mid(\pi\chi+g),\quad \Big(\rho,\delta,\pi\%\frac{n}{\delta}\Big)\in\Gamma.$$

Notice that $\Psi\big(\rho,\delta,\pi\%\frac{n}{\delta}\big)\subseteq H$, and by Lemma 3.2 (1), $|\Psi(\rho,\delta,\pi\%\frac{n}{\delta})| = \rho = |H|$, hence $H=\Psi\big(\rho,\delta,\pi\%\frac{n}{\delta}\big)$.

Theorem 3.3 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple, fix $(\rho,\delta,\varsigma)\in\Gamma$.*

(1) $\forall(c,d)\in\mathbb{Z}\times\mathbb{N}:(\tau^c\eta^d)\in N_K(\Psi(\rho,\delta,\varsigma))\Leftrightarrow c\big(h^{\frac{m\delta}{\rho}}-1\big)\equiv\varsigma(h^d-1)\ \big(\mathrm{mod}\,\frac{n}{\delta}\big)$.

(2) $\Psi(\rho,\delta,\varsigma)\lhd K\Leftrightarrow\varsigma(h-1)\equiv 0\ \big(\mathrm{mod}\,\frac{n}{\delta}\big), h^{\frac{m\delta}{\rho}}\equiv 1\ \big(\mathrm{mod}\,\frac{n}{\delta}\big)$.

(3) *If $\Psi(\rho,\delta,\varsigma)\lhd K$, then $K/\Psi(\rho,\delta,\varsigma)\cong\big(\frac{m\delta}{\rho},\frac{n}{\delta},(-\varsigma)\%\frac{n}{\delta},h\%\frac{n}{\delta}\big)\in\Omega$.*

Proof (1) Since Ψ is injective, using Lemma 3.1 (2), (1) follows from the following fact

$$\Big(\rho,\delta,(c(1-h^{\frac{m\delta}{\rho}})+\varsigma h^d)\%\frac{n}{\delta}\Big)\in\Gamma,$$

together with the equation:

$$(\tau^c\eta^d)\Psi(\rho,\delta,\varsigma)(\tau^c\eta^d)^{-1} = \Psi\Big(\rho,\delta,(c(1-h^{\frac{m\delta}{\rho}})+\varsigma h^d v)\%\frac{n}{\delta}\Big).$$

(2) Take $(c,d)=(1,0)$ and $(c,d)=(0,1)$ in (1), and (2) follows.

(3) Write $B=\Psi(\rho,\delta,\varsigma)$, (3) follows from Lemma 3.1 and the following relations:

$$\tau^{\frac{n}{\delta}}B=B,\quad \eta^{\frac{m\delta}{\rho}}B=\tau^{(-\varsigma)\%\frac{n}{\delta}}B,\quad (\eta B)(\tau B)(\eta^{-1}B)=\tau^{h\%\frac{n}{\delta}}B,\quad |K/B|=\frac{mn}{\rho}.$$

Using Theorem 3.2, we get the following Proposition 3.1 which gives a way to count the number of subgroups of a given order.

Proposition 3.1 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple.*

(1) *Fix $(\rho,\delta)\in\mathbb{N}^2$, such that $\delta\mid\rho,\ \delta\mid n,\ \rho\mid m\delta$, let Υ denote the set*

$$\{B\mid B\le K,|B|=\rho,|B\cap\langle\tau\rangle|=\delta\},$$

then we have

$$\Upsilon\ne\varnothing\ \Leftrightarrow\ \gcd\Big(\frac{n}{\delta},\sum_{j=0}^{\frac{\rho}{\delta}-1}h^{\frac{m\delta j}{\rho}}\Big)\Big|g.$$

Moreover, once $\Upsilon\ne\varnothing$, then $|\Upsilon|=\gcd\big(\frac{n}{\delta},\sum\limits_{j=0}^{\frac{\rho}{\delta}-1}h^{\frac{m\delta j}{\rho}}\big)$.

(2) *Fix $k\in\mathbb{N},\ k\mid mn$. Then we have*

$$|\{C\mid C\le K,|C|=k\}|=\sum_{l\in\Theta}\gcd\Big(\frac{n}{l},\sum_{j=0}^{\frac{k}{l}-1}h^{\frac{mlj}{k}}\Big),$$

where

$$\Theta=\Big\{l\mid l\in\mathbb{N},l\mid n,l\mid k,k\mid ml,\gcd\Big(\frac{n}{l},\sum_{j=0}^{\frac{k}{l}-1}h^{\frac{mlj}{k}}\Big)\Big|g\Big\}.$$

Proposition 3.2 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple, denote $\vartheta=\sum\limits_{i=0}^{m-1}h^i$. Let Y be the following set*

$$\{a\mid a\in\{0,1,\cdots,n-1\},\vartheta a\equiv -g\pmod n\},$$

and let $W=\{E\mid E\le K,E\cap\langle\tau\rangle=\{1_K\},\langle\tau\rangle E=K\}$. Then

(1) *$W\ne\varnothing\Leftrightarrow\gcd(n,\vartheta)\mid g$. Moreover, once $W\ne\varnothing$, then we have*

$$|W|=|Y|=\gcd(n,\vartheta).$$

(2) *Assume that $\gcd(n,\vartheta)\mid g$. Fix $D\in W$. Then $(m,n,g,h)\cong(m,n,0,h)$, and we have*

$$N_K(D)=C_K(D),\ |\{uDu^{-1}\mid u\in K\}|=\frac{n}{\gcd(n,h-1)}.$$

Moreover, any two complements of $\langle\tau\rangle$ in K are conjugate in K if and only if the following equation holds:

$$n=\gcd(n,h-1)\gcd(n,\vartheta).$$

Proof (1) Since for any $a \in \{0, 1, \cdots, n-1\} : (m, 1, a) \in \Gamma \Leftrightarrow a \in Y$. By Theorem 3.2, we get $W = \{\Psi(m, 1, a)(= \langle \tau^a \eta \rangle) \mid a \in Y\}$, and (1) follows.

(2) By (1), $Y \neq \varnothing$. Fix $a \in Y$, consider $(\tau, \tau^a \eta) \in K \times K$, we get

$$K = \langle \tau, \tau^a \eta \rangle, \quad o(\tau) = n, \quad o(\tau^a \eta) = m, \quad (\tau^a \eta)\tau(\tau^a \eta)^{-1} = \tau^h, \quad \langle \tau^a \eta \rangle \cap \langle \tau \rangle = \{1_K\}.$$

Hence $(m, n, g, h) \cong K \cong (m, n, 0, h)$. Now fix $D \in W$, by (1), $\exists!\ a \in Y,\ D = \Psi(m, 1, a)$. For any $(\alpha, \beta) \in \mathbb{N}^2$, by Lemma 3.1 (2) and Theorem 3.3 (1), we have

$$(\tau^\alpha \eta^\beta) \in N_K(D) \Leftrightarrow \alpha(h-1) \equiv a(h^\beta - 1) \pmod n \Leftrightarrow (\tau^\alpha \eta^\beta) \in C_K(D).$$

This implies $C_K(D) = N_K(D)$. Now we compute $|C_K(D)|$. By the previous discussion and Theorem 3.1 (2), we deduce that

$$|C_K(D)| = |\{(\alpha, \beta) \in \mathbb{N}^2 |\ 0 \le \alpha < n,\ 0 \le \beta < m,\ \alpha(h-1) \equiv a(h^\beta - 1) \pmod n\}|.$$

Since for any $\beta \in \{0, 1, \cdots, m-1\}$, we have $\gcd(n, h-1) \mid a(h^\beta - 1)$, and

$$|\{\alpha |\ \alpha \in \{0, 1, \cdots, n-1\},\ \alpha(h-1) \equiv a(h^\beta - 1) \pmod n\}| = \gcd(n, h-1),$$

it follows that $|C_K(D)| = m \cdot \gcd(n, h-1)$. Since $C_K(D) = N_K(D)$, we get $N_K(D) = m \cdot \gcd(n, h-1)$, and $|\{uDu^{-1} \mid u \in K\}| = \frac{n}{\gcd(n,h-1)}$. Now the last part follows from the fact $|W| = \gcd(n, \vartheta)$.

For further discussion, we now state some lemmas and basic constructions of metacyclic groups.

Lemma 3.3 (see [2]) *Let p be a prime number, $r \in \mathbb{Z}$, $p \mid (r-1)$, $m \in \mathbb{N}$, $m \ge 1$.*

(1) *If $p \ge 3$ or $p = 2$, $4 \mid (r-1)$, then $O(p, r^m - 1) = O(p, r-1) + O(p, m)$.*

(2) *If $p = 2$, $4 \mid (r-3)$, $2 \mid m$, then $O(2, r^m - 1) = O(2, r+1) + O(2, m)$.*

Lemma 3.4 *Fix $(k, n, r) \in \mathbb{Z}^3$, $n \ge 1$, $k \mid n$, $k \mid (r^n - 1)$, then $k \big| \big(\sum\limits_{j=0}^{n-1} r^j\big)$.*

Proof Write $\mu = \sum\limits_{j=0}^{n-1} r^j$. We have $r^n - 1 = (r-1)\mu$. Fix $p \in X(k)$, we now show that $O(p, k) \le O(p, \mu)$. Notice that $k \mid n$, $k \mid (r^n - 1)$, hence $O(p, k) \le O(p, n)$, $O(p, k) \le O(p, r^n - 1)$. Next, we consider the following three cases.

(i) If $p \nmid (r-1)$, then $O(p, \mu) = O(p, r^n - 1)$, it follows that $O(p, k) \le O(p, \mu)$.

(ii) If $(p \mid (r-1), p \ge 3)$ or $(p = 2,\ 4 \mid (r-1))$, by Lemma 3.3 (1), we deduce that

$$O(p, r^n - 1) = O(p, r-1) + O(p, n) = O(p, r-1) + O(p, \mu).$$

It follows that $O(p, \mu) = O(p, n)$, and $O(p, k) \le O(p, \mu)$.

(iii) If $p = 2$, $4 \mid (r-3)$, then $O(p, r-1) = 1$, $O(p, r+1) \ge 2$. Notice that $p \mid k$, we have $p \mid n$. By Lemma 3.3 (2), we deduce that

$$O(p, n) \le O(p, r^n - 1) - 2,\ O(p, \mu) = O(p, r^n - 1) - 1.$$

It follows that $O(p, k) \le O(p, n) < O(p, \mu)$.

By case (i)–case (iii). We deduce that $O(p,k) \le O(p,\mu)$. Finally, since $p \in X(k)$ is arbitrary, we have $k \mid \mu$.

The next two lemmas provide the numerical results we need in the discussion, and they may be regarded as corollaries of Lemma 3.3.

Lemma 3.5 *Let p be a prime number, $p \ge 3$, $(a,b,c) \in \mathbb{Z}^3$, where*

$$a \neq \pm 1, \quad p \nmid a, \quad b \neq 1, \quad b \equiv 1 \pmod 4, \quad c \neq -1, \quad c \equiv 3 \pmod 4,$$

and fix $k \in \mathbb{N}$.

(1) *If $k \ge O(2, b-1)$, then* $\operatorname{ord}(2^k, b) = 2^{k-O(2,b-1)}$.

(2) *If $k \ge O(2, c+1)+1$, then* $\operatorname{ord}(2^k, c) = 2^{k-O(2,c+1)}$.

(3) *If $k \ge O(p, a^{\operatorname{ord}(p,a)}-1)$, then* $\frac{\operatorname{ord}(p^k,a)}{\operatorname{ord}(p,a)} = p^{k-O(p,a^{\operatorname{ord}(p,a)}-1)}$.

Lemma 3.6 (see [2]) (1) *Let p be a prime number, $p \ge 3$, fix $k \in \mathbb{N}$, $k \ge 1$, then $(U_{(p^k)}, \odot_{(p^k)})$ is cyclic, and $\forall b \in U_{(p^k)}$, if $b \ge 2, p \mid (b-1)$, then $\langle b \rangle_{(p^k)} = \langle 1 + p^{O(p,b-1)} \rangle_{(p^k)}$.*

(2) *Fix $m \in \mathbb{N}$, $m \ge 4$, $\pi \in U_{(2^m)}$.*

(2.1) *If $\pi \equiv 1 \pmod 4$, $\pi \neq 1$, then $\langle \pi \rangle_{(2^m)} = \langle 1 + 2^{O(2,\pi-1)} \rangle_{(2^m)}$.*

(2.2) *If $\pi \equiv 3 \pmod 4$, then $\langle \pi \rangle_{(2^m)} = \langle 2^{O(2,\pi+1)} - 1 \rangle_{(2^m)}$.*

Proposition 3.3 *Let $((m,n,g,h), K, T, \Gamma, \Psi)$ be a Hölder-tuple. Then the following statements hold.*

(1) $\exp(K) = \frac{mn}{\gcd(g,m,n)}$.

(2) *Assume that $n \ge 2$, then K is Abelian if and only if $h = 1$, and K is cyclic if and only if $h = 1$, $\gcd(g,m,n) = 1$.*

(3) *Fix $(a,b) \in \mathbb{Z} \times \mathbb{N}$, then*

$$o(\tau^a \eta^b) = \frac{mn}{\gcd(b,m)\gcd\Big(n,\ a\Big(\sum_{i=0}^{\frac{m}{\gcd(b,m)}-1} h^{bi}\Big) + \frac{gb}{\gcd(m,b)}\Big)}.$$

Proof Write $\lambda = \frac{mn}{\gcd(g,m,n)}$. Since

$$\operatorname{lcm}(o(\tau), o(\eta)) = \operatorname{lcm}\Big(n, \frac{mn}{\gcd(g,n)}\Big) = \lambda,$$

hence $\lambda \mid \exp(K)$. Now fix $(\alpha,\beta) \in \mathbb{N}^2$, by Lemma 3.1 (2), $(\tau^\alpha \eta^\beta)^\lambda = \tau^{\alpha\left(\sum_{i=0}^{\lambda-1} h^{\beta i}\right)} \eta^{\beta\lambda}$. Since $n \mid (h^{\beta\lambda} - 1)$, $n \mid \lambda$, by Lemma 3.4, $n \Big| \sum_{i=0}^{\lambda-1} h^{\beta i}$. Thus $(\tau^\alpha \eta^\beta)^\lambda = 1_K$. This implies $\exp(K) \mid \lambda$. Thus $\exp(K) = \lambda$. The rest (2)–(3) is proved by using Theorem 3.1, Lemma 3.1 and (1), we omit the details.

Using Theorems 3.2–3.3 and Proposition 3.3, we get the following proposition, in which more details are given.

Proposition 3.4 *Let $((m,n,g,h), K, T, \Gamma, \Psi)$ be a Hölder-tuple.*

(1) *Fix $(\rho, \delta, \varsigma) \in \Gamma$, denote*

$$\gcd\Big(\frac{\rho}{\delta}, \delta, \frac{\delta\Big(\varsigma\Big(\sum_{j=0}^{\frac{\rho}{\delta}-1} h^{\frac{m\delta j}{\rho}}\Big) + g\Big)}{n}\Big) = \theta.$$

(1.1) $\exp(\Psi(\rho,\delta,\varsigma)) = \frac{\rho}{\theta}$.

(1.2) $\Psi(\rho,\delta,\varsigma)$ *is Abelian* $\Leftrightarrow h^{\frac{m\delta}{\rho}} \equiv 1 \pmod{\delta}$.

(1.3) $\Psi(\rho,\delta,\varsigma)$ *is cyclic* $\Leftrightarrow h^{\frac{m\delta}{\rho}} \equiv 1 \pmod{\delta},\ \theta = 1$.

(2) *Fix* $(\rho,\delta,\varsigma)\in\Gamma$, *assume that* $\Psi(\rho,\delta,\varsigma) \lhd K$.

(2.1) $\exp(K/\Psi(\rho,\delta,\varsigma)) = \frac{mn}{\rho\gcd(\frac{m\delta}{\rho},\frac{n}{\delta},\varsigma)}$.

(2.2) $K/\Psi(\rho,\delta,\varsigma)$ *is cyclic* $\Leftrightarrow h\equiv 1 \left(\operatorname{mod}\frac{n}{\delta}\right),\ \gcd\left(\frac{m\delta}{\rho},\frac{n}{\delta},\varsigma\right)=1$.

(3) $[K,K] = \langle \tau^{h-1}\rangle = \langle \tau^{\gcd(n,h-1)}\rangle$, $\exp(K/[K,K]) = \frac{m\gcd(n,h-1)}{\gcd(g,m,n,h-1)}$.

Lemma 3.7 (see [2]) *Fix* $(m,n,t,r)\in\Omega$, $(c,d)\in\mathbb{N}\times\mathbb{N}$, *such that* $(m,n,c,d)\in\Omega$, $\langle r\rangle_{(n)} = \langle d\rangle_{(n)}$, $\gcd(t,n)=\gcd(c,n)$, *then* $(m,n,t,r)\cong(m,n,c,d)$.

Using Proposition 3.2 (2) Lemmas 3.3 and 3.5–3.7, we have the following lemma on the metacyclic p-groups.

Lemma 3.8 *Let p be a prime number, fix* $(l,k)\in\mathbb{N}^2$, $l\ge 1$, $k\ge 1$, *let* $b=\min(l,k)$, *fix* $(t,r)\in\mathbb{N}^2$, *such that* $(p^l,p^k,t,r)\in\Omega$. *Then*

(1) *Assume* $p\ge 3$ *or* $p=2$, $r\equiv 1 \pmod 4$. *Then* $O(p,r-1)+l\ge k$, *and*

(1.1) *if* $r=1$, $p^b\mid t$, *then* $(p^l,p^k,t,r)\cong(p^l,p^k,0,1)$;

(1.2) *if* $r\ne 1$, $p^b\mid t$, *then* $(p^l,p^k,t,r)\cong(p^l,p^k,0,1+p^{O(p,r-1)})$;

(1.3) *if* $r=1$, $p^b\nmid t$, *then* $(p^l,p^k,t,r)\cong(p^l,p^k,p^{O(p,t)},1)$;

(1.4) *if* $r\ne 1$, $p^b\nmid t$, *then* $(p^l,p^k,t,r)\cong(p^l,p^k,p^{O(p,t)},1+p^{O(p,r-1)})$.

(2) *Assume* $p=2$, $r\equiv 3 \pmod 4$, *then* $O(2,r+1)+l\ge k$, $t\in\{0,2^{k-1}\}$. *Moreover,* $(2^l,2^k,t,r)\cong(2^l,2^k,t,2^{O(2,r+1)}-1)$.

Now we can apply Theorems 3.2–3.3 on split metacyclic p-groups. Here a simpler form of this kind of groups is given.

Proposition 3.5 *Let p be a prime number,* $(l,k,s)\in\mathbb{N}^3$, *where*

$$l\ge 1,\quad k\ge 2,\quad 1\le s<k,\quad s+l\ge k.$$

Let $((p^l,p^k,0,1+p^s),K,T,\Gamma,\Psi)$ *be a Hölder-tuple, and let* Γ^* *denote the following set*

$$\{(a,b,c)\mid (a,b,c)\in\mathbb{N}^3, b\le a, b\le k, a\le b+l, 0\le c<p^{\min(a,k)-b}\}.$$

If $p=2$, *then assume* $k\ge 3$, $s\ge 2$. *Define the map* $\Psi^*:\ \Gamma^*\to T$, *where*

$$\forall (a,b,c)\in\Gamma^*:\ \Psi^*(a,b,c) = \langle \tau^{c\times p^{k-\min(a,k)}}\eta^{p^{l+b-a}}, \tau^{p^{k-b}}\rangle.$$

Then

(1) Ψ^* *is a one to one correspondence from* Γ^* *to* T.

(2) *Fix* $(f,e,d)\in\Gamma^*$, *then we have*

$$\Psi^*(f,e,d)\lhd K \Leftrightarrow f-2e\le l+s-k,\quad \min(f,k)-e-O(p,d)\le s.$$

Proof Define the map $\varphi:\ \Gamma^*\to\mathbb{Z}^3$, where

$$\forall (a,b,c)\in\Gamma^*:\ \varphi(a,b,c) = (p^a,p^b,c\cdot p^{k-\min(a,k)}).$$

Using Lemma 3.3, we get $\varphi[\Gamma^*]=\Gamma$, φ is injective, and $\Psi^*=\Psi\circ\varphi$. Now (1) follows from Theorem 3.2, and (2) follows from Theorem 3.3 (2) and Lemma 3.3.

4 The Upper and Lower Central Series, $\Phi(K)$, $F(K)$, the Carter Subgroup C and the p-Subgroups

In this section, we compute and characterize some subgroups of a finite metacyclic group K.

First, we write the upper and lower central series for K. Using induction when necessary, the next lemma follows from Lemma 3.1 and Theorem 3.2.

Lemma 4.1 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple. Fix $(k,l,\beta)\in\Gamma,\ (\rho,\delta,\varsigma)\in\Gamma$, then*

(1) $[\Psi(k,l,\beta),K]=\langle\tau^{\gcd\left(h^{\frac{ml}{k}}-1,\ \beta(h-1),\ \frac{n(h-1)}{l}\right)}\rangle$.

(2) $[\Psi(k,l,\beta),K]\subseteq\Psi(\rho,\delta,\varsigma)\Leftrightarrow\frac{n}{\delta}\mid\gcd\left(h^{\frac{ml}{k}}-1,\ \beta(h-1),\ \frac{n(h-1)}{l}\right)$.

(3) $\forall(s,b)\in\mathbb{N}\times\mathbb{Z},\ w\in\mathbb{N}$,

$$w\geq 2:[\underbrace{\langle\tau^b,\eta^s\rangle,\cdots,\langle\tau^b,\eta^s\rangle}_{w}]=\langle\tau^{b(h^s-1)^{w-1}}\rangle.$$

Theorem 4.1 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple. Denote*

$$\mu=\prod_{p\in X(n)\cap X(h-1)}p^{O(p,n)},$$

and let $\nu=\frac{n}{\mu}$. Fix $s\in\mathbb{N}$, such that $\forall p\in X(n)\cap X(h-1):(s-1)O(p,h-1)\geq O(p,n)$. Then the lower central series of K are

$$K\supseteq\langle\tau^{h-1}\rangle\supseteq\cdots\supseteq\langle\tau^{(h-1)^\lambda}\rangle\supseteq\cdots\supseteq[\underbrace{K,\cdots,K}_{s}]=\langle\tau^\mu\rangle,$$

and the upper central series of K are

$$\{1_K\}\subseteq\cdots\subseteq\langle\tau^{\frac{n}{\gcd(n,(h-1)^\lambda)}},\eta^{\mathrm{ord}\left(\frac{n}{\gcd(n,(h-1)^{\lambda-1})},\ h\right)}\rangle\subseteq\cdots\subseteq Z_s(K)=\langle\tau^\nu,\eta^{\mathrm{ord}(\nu,h)}\rangle.$$

Moreover, K is nilpotent $\Leftrightarrow X(n)\subseteq X(h-1)$.

Proof First, $\forall w\in\mathbb{N},\ w\geq 1$, by Lemma 4.1 (3) $[\underbrace{K,\cdots,K}_{w+1}]=\langle\tau^{(h-1)^w}\rangle=\langle\tau^{\gcd(n,(h-1)^w)}\rangle$. Now we prove the following Claim 1 by induction.

Claim 1 $\forall w\in\mathbb{N},\ w\geq 1$

$$Z_w(K)=\langle\tau^{\frac{n}{\gcd(n,(h-1)^w)}},\eta^{\mathrm{ord}\left(\frac{n}{\gcd(n,(h-1)^{w-1})},\ h\right)}\rangle.$$

Proof of Claim 1 By (2.2) of Lemma 3.1,

$$Z(K)=\langle\tau^{\frac{n}{\gcd(n,h-1)}},\eta^{\mathrm{ord}(n,h)}\rangle.$$

Now fix $\lambda\in\mathbb{Z}^+$, assume Claim 1 holds for λ. Write

$$f=\gcd(n,(h-1)^{\lambda-1}),\quad\pi=\gcd(n,(h-1)^\lambda),\quad\theta=\gcd(n,(h-1)^{\lambda+1}).$$

Using Lemma 3.2, we have

$$Z_\lambda(K)=\Psi\Big(\frac{m\pi}{\mathrm{ord}\Big(\dfrac{n}{f},h\Big)},\pi,0\Big).$$

By Lemma 4.1 (2), $\forall(k,l,\beta)\in\Gamma$, we have

$$\Psi(k,l,\beta)\subseteq Z_{\lambda+1}(K)\Leftrightarrow l\Big|\theta,\ \frac{n}{\theta}\Big||\beta,\ k|\frac{ml}{\mathrm{ord}\Big(\dfrac{n}{\pi},h\Big)}.$$

By Theorem 3.2,

$$|Z_{\lambda+1}(K)|\le\frac{m\theta}{\mathrm{ord}\Big(\dfrac{n}{\pi},h\Big)}.$$

Again by Lemma 3.2 and the previous discussion, we get

$$\Big(\frac{m\theta}{\mathrm{ord}\Big(\dfrac{n}{\pi},h\Big)},\theta,0\Big)\in\Gamma,\quad \Psi\Big(\frac{m\theta}{\mathrm{ord}\Big(\dfrac{n}{\pi},h\Big)},\theta,0\Big)\subseteq Z_{\lambda+1}(K).$$

This implies

$$Z_{\lambda+1}(K)=\Psi\Big(\frac{m\theta}{\mathrm{ord}\Big(\dfrac{n}{\pi},h\Big)},\theta,0\Big).$$

The induction is completed. And the theorem follows immediately.

Now we turn to the Carter subgroup of a finite metacyclic group K. Recall that for any group G and $A\le G$, by [5], we say A is a Carter subgroup of G, if and only if A is nilpotent and $N_G(A)=A$. It is well known that any finite solvable group G contains a Carter subgroup C, and any two Carter subgroups of G are conjugate in G. Furthermore, the identity $G=CG_\infty$ always holds (see [5]).

For a finite metacyclic group K, we can say more about its Carter subgroup, and the following is our main result on the Carter subgroup of K.

Theorem 4.2 *Let K be a finite metacyclic group, fix $C\le K$, then*
(1) *if C is a Carter subgroup of K, then $C\cap K_\infty=\{1_K\},\ K=CK_\infty$;*
(2) *C is a Carter subgroup of $K\Leftrightarrow K=CK_\infty$ and C is nilpotent.*

Using Theorem 3.2, Theorem 4.2 follows from the next proposition.

Proposition 4.1 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple. Denote*

$$\mu=\prod_{p\in X(n)\cap X(h-1)}p^{O(p,n)}$$

and let $\nu=\frac{n}{\mu}$. Fix $(k,l,\beta)\in\Gamma,\ \gamma\in\mathbb{N},\ \gamma<\nu$.
(1) *If $\Psi(k,l,\beta)K_\infty=K$, $\Psi(k,l,\beta)$ is nilpotent, then $l=\mu,\ k=m\mu$.*
(2) *$(m\mu,\mu,\gamma)\in\Gamma,\ \Psi(m\mu,\mu,\gamma)$ is a Carter subgroup of K. Moreover, we have*

$$\Psi(m\mu,\mu,\gamma)\cap K_\infty=\{1_K\},\quad \Psi(m\mu,\mu,\gamma)K_\infty=K.$$

Proof (1) By Lemma 3.2 (1), we have

$$\Psi(k,l,\beta)\cap K_\infty=\langle\tau^{\frac{n}{l}}\rangle\cap\langle\tau^{\mu}\rangle=\langle\tau^{\frac{n}{\gcd(l,\nu)}}\rangle,$$

and it follows that

$$mn=|\Psi(k,l,\beta)K_\infty|=\frac{k\nu}{\gcd(l,\nu)}=\frac{k\mathrm{lcm}(l,\nu)}{l}.$$

Since $\frac{k}{l}\mid m,\ \mathrm{lcm}(l,\nu)\mid n$, we have $\frac{k}{l}=m,\ \mathrm{lcm}(l,\nu)=n,\ \mu\mid l$. Next, by Lemma 3.2, $\exists\theta_1\in\mathbb{N}$, where $\Psi(k,l,\beta)\cong(m,l,\theta_1,h\%l)$, by Theorem 4.1, $X(l)\subseteq X((h\%l)-1)$. Thus $X(l)\subseteq X(h-1),\ l\mid n$, and this implies $l\mid\mu$. Hence $\mu=l,\ k=ml=m\mu$.

(2) First, we have $(m\mu,\mu,\gamma)\in\Gamma,\ \Psi(m\mu,\mu,\gamma)=\langle\tau^{\gamma}\eta,\tau^{\nu}\rangle$. Write $B=\Psi(m\mu,\mu,\gamma)$. By Lemma 3.2, $\exists\theta_2\in\mathbb{N}$, such that $B\cong(m,\mu,\theta_2,h\%\mu)$. Since $X(\mu)\subseteq X((h\%\mu)-1)$, by Theorem 4.1, B is nilpotent. Next, fix $(e,f)\in\mathbb{N}^2$, where $(\tau^e\eta^f)\in N_K(B)$. By Theorem 3.3, we have

$$\gamma(h^{f}-1)\equiv e(h-1)\ (\mathrm{mod}\,\nu).$$

Notice that $\gcd(h-1,\nu)=1$, together with Lemma 3.2, we have

$$\gamma\Big(\sum_{j=0}^{f-1}h^{j}\Big)\equiv e\ (\mathrm{mod}\,\nu),\quad(\tau^e\eta^f)\in B.$$

This implies $B=N_K(B)$. Finally, we deduce that

$$B\cap K_\infty=\langle\tau^{\nu}\rangle\cap\langle\tau^{\mu}\rangle=\langle\tau^{\nu\mu}\rangle=\langle\tau^{n}\rangle=\{1_K\},$$

and $|BK_\infty|=m\mu\nu=|K|$, $BK_\infty=K$.

Now we describe the Frattini subgroup $\Phi(K)$. The next lemma follows from Theorem 3.2 and the fact that every metacyclic group is supersolvable.

Lemma 4.2 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple, then*

(1) $\forall C\le K$: C is a proper maximal subgroup of K and $\langle\tau\rangle\subseteq C$ if and only if $\exists s\in X(m)$, such that $C=\langle\tau,\eta^s\rangle$.

(2) $\forall B\le K$: B is a proper maximal subgroup of K and $\langle\tau\rangle\nsubseteq B$ if and only if $\exists q\in X(n)$, $\exists\beta\in\mathbb{N}$, such that $\big(\frac{mn}{q},\frac{n}{q},\beta\big)\in\Gamma$, $B=\Psi\big(\frac{mn}{q},\frac{n}{q},\beta\big)$.

Theorem 4.3 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple, and let (V_1,V_2,V_3,V_4,V_5) denote the following 5-tuple:*

$$\begin{aligned}&((X(n)-X(g))\cap X(m),\quad X(n)-X(gm),\quad (X(n)\cap X(g))-X(h-1),\\&(X(n)\cap X(g)\cap X(h-1))-X(m),\quad X(n)\cap X(g)\cap X(h-1)\cap X(m)).\end{aligned}$$

Denote

$$v_1=\prod_{p\in X(n)\cap X(g)}p,\quad\forall i\in\{2,3,4,5\}:\ v_i=\prod_{p\in V_i}p,$$

and denote

$$v_6=\prod_{p\in X(m)}p,\quad\varphi=\mathrm{lcm}(\mathrm{ord}(v_3,h),v_6).$$

Then $\exists!\ (\theta,\lambda)\in\mathbb{N}^2$, *where* $(\theta,\lambda)\in\{0,1,\cdots,v_2-1\}\times\{0,1,\cdots,v_1v_2-1\}$, *and*

$$\theta\Big(\sum_{j=0}^{m-1}h^{^j}\Big)\equiv -g\ (\mathrm{mod}\,v_2),\quad \lambda\equiv\theta\Big(\sum_{i=0}^{\varphi-1}h^{^i}\Big)\ (\mathrm{mod}\,v_2),\quad \lambda\equiv 0\ (\mathrm{mod}\,v_1).$$

Moreover, $\big(\frac{mn}{\varphi v_1v_2},\frac{n}{v_1v_2},\lambda\big)\in\Gamma$, $\Phi(K)=\Psi\big(\frac{mn}{\varphi v_1v_2},\frac{n}{v_1v_2},\lambda\big)=\langle\tau^\lambda\eta^\varphi,\tau^{v_1v_2}\rangle$.

Proof The existence and uniqueness of (θ,λ) follow from $\gcd\big(\sum\limits_{j=0}^{m-1}h^{^j},v_2\big)=1$ and the Chinese remainder theorem. Also notice that $\big(\frac{mn}{\varphi v_1v_2},\frac{n}{v_1v_2},\lambda\big)\in\Gamma$, $\big(\frac{mn}{v_2},\frac{n}{v_2},\theta\big)\in\Gamma$, (V_1,V_2,V_3,V_4,V_5) is a partition of $X(n)$. We compute $\Phi(K)$ by presenting a series of facts, all of which follow from Lemma 3.2.

(1) $\forall p\in V_1,\ \forall\beta\in\mathbb{N}:\ \big(\frac{mn}{p},\frac{n}{p},\beta\big)\notin\Gamma$.

(2) Fix $p\in V_2$, then $\forall\beta\in\mathbb{N},\ \beta<p:\ \big(\frac{mn}{p},\frac{n}{p},\beta\big)\in\Gamma\Leftrightarrow\beta=\theta\%p$.

(3) $\bigcap\limits_{p\in V_2}\Psi\big(\frac{mn}{p},\frac{n}{p},\theta\%p\big)=\langle\tau^\theta\eta,\tau^{v(2)}\rangle,\ \langle\tau^\theta\eta,\tau^{v_2}\rangle\lhd K$.

(4) Fix $p\in V_4,\ \beta\in\mathbb{N},\ 0\le\beta<p$, then: $\big(\frac{mn}{p},\frac{n}{p},\beta\big)\in\Gamma\Leftrightarrow\beta=0$.

(5) Using Lemma 3.2, we get $\bigcap\limits_{p\in V_4}\Psi\big(\frac{mn}{p},\frac{n}{p},0\big)=\langle\tau^{v_4},\eta\rangle$.

(6) Fix $s\in V_5$, then $\forall\gamma\in\{0,1,\cdots,s-1\}:\big(\frac{mn}{s},\frac{n}{s},\gamma\big)\in\Gamma$. And we have

$$\bigcap_{\gamma=0}^{s-1}\Psi\Big(\frac{mn}{s},\frac{n}{s},\gamma\Big)=\langle\tau^s,\eta^s\rangle.$$

(7) Using Lemma 3.2, we get $\bigcap\limits_{s\in V_5}\langle\tau^s,\eta^s\rangle=\langle\tau^{v_5},\eta^{v_5}\rangle$.

(8) Fix $q\in V_3$, then $\forall\gamma\in\{0,1,\cdots,q-1\}:\big(\frac{mn}{q},\frac{n}{q},\gamma\big)\in\Gamma$. And we have

$$\bigcap_{\gamma=0}^{q-1}\Psi\Big(\frac{mn}{q},\frac{n}{q},\gamma\Big)=\langle\tau^q,\eta^{\mathrm{ord}(q,h)}\rangle.$$

(9) Using Lemma 3.2, we get $\bigcap\limits_{q\in V_3}\langle\tau^q,\eta^{\mathrm{ord}(q,h)}\rangle=\langle\tau^{v_3},\eta^{\mathrm{ord}(v_3,h)}\rangle$.

(10) By lemma 4.2 (1), and (1)–(9), we get

$$\Phi(K)=\langle\tau,\eta^{v_6}\rangle\cap\langle\tau^{v_4},\eta\rangle\cap\langle\tau^{v_5},\eta^{v_5}\rangle\cap\langle\tau^{v_3},\eta^{\mathrm{ord}(v_3,h)}\rangle\cap\langle\tau^\theta\eta,\tau^{v_2}\rangle.$$

And by Lemma 3.2, $\Phi(K)=\langle\tau^{v_1},\eta^\varphi\rangle\cap\langle\tau^\theta\eta,\tau^{v_2}\rangle=\langle\tau^\lambda\eta^\varphi,\tau^{v_1v_2}\rangle$.

Now we compute $F(K)$ for a finite metacyclic group K.

Proposition 4.2 *Let* $((m,n,g,h),K,T,\Gamma,\Psi)$ *be a Hölder-tuple. Denote* $\omega=\prod\limits_{p\in X(n)}p$. *Then* $F(K)=\langle\tau,\eta^{\mathrm{ord}(\omega,h)}\rangle$, *and moreover,* $\forall y\in K$,

(1) $y\in F(K)\Leftrightarrow\exists l\in\mathbb{N},\ l\ge1$, *such that* $\forall x\in K:\ [\underbrace{y,\cdots,y}_{l},x]=1_K$.

(2) $y\in Z_\infty(K)\Leftrightarrow\exists l\in\mathbb{N},\ l\ge1$, *such that* $\forall x\in K:\ [\underbrace{x,\cdots,x}_{l},y]=1_K$.

Remark 4.1 Actually, by [1], (1) and (2) hold for every finite group G.

Proof First, denote $\mu = \prod_{p\in X(n)\cap X(h-1)} p^{O(p,n)}$, $\nu = \frac{n}{\mu}$, and $\forall(\alpha,\beta) \in K^2$, $\forall k \in \mathbb{Z}^+$, denote $\varepsilon(\alpha,k,\beta) = [\underbrace{\alpha,\cdots,\alpha}_{k},\beta]$. Let $A = \langle\tau,\eta^{\mathrm{ord}(\omega,h)}\rangle$. Hence $A \lhd K$. Fix $t \in \mathbb{N}$, where $n \mid (h^{\mathrm{ord}(\omega,h)}-1)^t$. By Lemma 4.1 (3), $[\underbrace{A,\cdots,A}_{t+1}] = \{1_K\}$. Thus $A \subseteq F(K)$. Using (2.3) of Lemma 3.1 and straightforward computation, we have the following claim.

Claim Fix $(e,f) \in \mathbb{N}^2$, then

$$(\exists l \in \mathbb{N},\ l \geq 1,\quad \text{such that } \forall x \in K : \varepsilon(x,l,\tau^e\eta^f) = 1_K) \ \Leftrightarrow\ \nu \mid e, \mathrm{ord}(\nu,h) \mid f.$$
$$(\exists r \in \mathbb{N},\ r \geq 1,\quad \text{such that } \forall x \in K : \varepsilon(\tau^e\eta^f,r,x) = 1_K) \ \Leftrightarrow\ \mathrm{ord}(\omega,h) \mid f.$$

By Theorem 4.1, $Z_\infty(K) = \langle\tau^\nu,\eta^{\mathrm{ord}(\nu,h)}\rangle$. Notice that the "$\Rightarrow$" part of (1) and (2) are trivial. by the above two claims, Proposition 4.2 is proved.

Now we begin to study the p-subgroups of a metacyclic group K, where p is a prime number. We mainly consider three problems: counting the number of the subgroups of order p^a, where $a \in \mathbb{N}$; giving a way to judge whether the Sylow p-group of K is normal; finding a relatively simple 4-tuple in Ω which is isomorphism to the Sylow p-group of K.

Theorem 4.4 *Let $((m,n,g,h),K,T,\Gamma,\Psi)$ be a Hölder-tuple, and p a prime number where $p \mid mn$. Fix $P \leq K$, $|P| = p^{O(p,mn)}$, $\mu \in \mathbb{N}$, $1 \leq \mu \leq O(p,mn)$. Let Δ denote the following set*

$$\{V \mid V \leq K, |V| = p^\mu\}.$$

$\forall\pi \in \mathbb{N}$, $\pi \leq \min(\mu,O(p,n))$, denote $\psi(\pi)$ as the following integer:

$$\psi(\pi) = p^{\min(\mu,O(p,n))-\pi}\Big(\prod_{q\in X(n),\ q\neq p,\ O(p,\mathrm{ord}(q,h))\geq O(p,m)+\pi+1-\mu} q^{O(q,n)}\Big).$$

(1) *If $p \nmid m$, then $P = \langle\tau^{\frac{n}{p^{O(p,n)}}}\rangle$, $|\Delta| = 1$. If $p \nmid \gcd(m,n)$, then P is cyclic.*
(2) *$P \lhd K \Leftrightarrow \forall q \in X(n)\ (p \nmid \mathrm{ord}(q,h))$.*
(3) *Denote $f_0 = \max(0,\mu - O(p,m),\min(\mu,O(p,n)) - O(p,g))$. Assume that $p \geq 3$, $p \mid m$ or $p = 2$, $p \mid m$, $h \equiv 1 \pmod 4$. Then*

$$|\Delta| = \sum_{\pi=f_0}^{\min(\mu,O(p,n))} \psi(\pi).$$

(4) *Assume $p = 2$, $2 \nmid n$, $2 \mid m$. Then*

$$|\Delta| = \prod_{q\in X(n),\ O(2,\mathrm{ord}(q,h))\geq O(2,m)-\mu+1} q^{O(q,n)}.$$

(5) *Assume $p = 2$, $2 \mid m$, $2 \mid n$, $4 \nmid n$. Then $2 \mid g \Rightarrow P \cong (2^{O(2,m)},2,0,1)$, and $2 \nmid g \Rightarrow P$ is cyclic.*
(6) *Assume $p \geq 3$, $p \mid m$, $p \mid n$ or $p = 2$, $2 \mid m$, $4 \mid n$, $h \equiv 1 \pmod 4$.*
(6.1) *If $h^{\mathrm{ord}(p,h)} \equiv 1 \pmod{p^{O(p,n)}}$, $O(p,g) \geq \min(O(p,m),O(p,n))$, then*

$$P \cong (p^{O(p,m)},p^{O(p,n)},0,1).$$

(6.2) *If* $h^{\mathrm{ord}(p,h)} \equiv 1 \pmod{p^{O(p,n)}}$, $O(p,g) < \min(O(p,m), O(p,n))$, *then*

$$P \cong (p^{O(p,m)}, p^{O(p,n)}, p^{O(p,g)}, 1).$$

(6.3) *If* $h^{\mathrm{ord}(p,h)} \not\equiv 1 \pmod{p^{O(p,n)}}$, $O(p,g) \geq \min(O(p,m), O(p,n))$, *then*

$$P \cong (p^{O(p,m)}, p^{O(p,n)}, 0, 1 + p^{O(p,\ h^{\mathrm{ord}(p,h)}-1)}).$$

(6.4) *If* $h^{\mathrm{ord}(p,h)} \not\equiv 1 \pmod{p^{O(p,n)}}$, $O(p,g) < \min(O(p,m), O(p,n))$, *then*

$$P \cong (p^{O(p,m)}, p^{O(p,n)}, p^{O(p,g)}, 1 + p^{O(p,\ h^{\mathrm{ord}(p,h)}-1)}).$$

Proof By Theorem 3.2, $\exists!\ \beta \in \mathbb{N}$, $\beta < \frac{n}{p^{O(p,n)}}$, and $(p^{O(p,mn)}, p^{O(p,n)}, \beta) \in \Gamma$,

$$P = \Psi(p^{O(p,mn)}, p^{O(p,n)}, \beta).$$

Denote

$$\vartheta = \frac{\Big(\beta\Big(\sum_{j=0}^{p^{O(p,m)}-1} h^{\frac{mj}{p^{O(p,m)}}}\Big) + g\Big)\%n}{\frac{n}{p^{O(p,n)}}}.$$

By Theorem 3.2, $P \cong (p^{O(p,m)}, p^{O(p,n)}, \vartheta, h^{\frac{m}{p^{O(p,m)}}} \% p^{O(p,n)})$.

(1) Using Theorem 3.1 and the Sylow theorem, we omit the details.

(2) Using Theorem 3.3 (2), we only prove the "$\Leftarrow$" part.

$\Leftarrow$ We deduce from Lemma 3.5.(3) that

$$h^{\frac{m}{p^{O(p,m)}}} \equiv 1 \Big(\mathrm{mod}\, \frac{n}{p^{O(p,n)}}\Big).$$

Since $(p^{O(p,mn)}, p^{O(p,n)}, \beta) \in \Gamma$, thus

$$\beta p^{O(p,m)} \equiv -g \Big(\mathrm{mod}\, \frac{n}{p^{O(p,n)}}\Big).$$

Hence $\beta(h-1) \equiv 0 \ \big(\mathrm{mod}\, \frac{n}{p^{O(p,n)}}\big)$. By Theorem 3.3 (2), we get $P \lhd K$.

(3) Consider the set

$$E = \Big\{ l \mid\ l \mid n, l \mid p^{\mu}, p^{\mu} \mid ml, \gcd\Big(\frac{n}{l}, \sum_{j=0}^{\frac{p^{\mu}}{l}-1} h^{\frac{mlj}{p^{\mu}}}\Big) \mid g \Big\}.$$

First, fix $\delta \in \mathbb{N}$, $\max(0, \mu - O(p,m)) \leq \delta \leq \min(\mu, O(p,n))$. Write

$$\chi = \sum_{j=0}^{p^{\mu-\delta}-1} h^{\frac{mj}{p^{\mu-\delta}}}.$$

Using lemma 3.3, we get $\gcd\big(\frac{n}{p^{\delta}}, \chi\big) = \psi(\delta)$, and

$$p^{\delta} \in E \Leftrightarrow p^{\min(O(p,n),\mu)-\delta} \mid g \Leftrightarrow f_0 \leq \delta \leq \min(\mu, O(p,n)).$$

Now by Proposition 3.1, (3) follows from the fact

$$|\Delta| = \sum_{l\in E} \gcd\Big(\frac{n}{l}, \sum_{j=0}^{\frac{p^\mu}{l}-1} h^{\frac{mlj}{p^\mu}}\Big).$$

(4) The proof is similar to the proof in (3), we omit the details.

(5) Notice that $2 \mid g$ implies $\vartheta = 0$, and $2 \nmid g$ implies $\vartheta = 1$, the rest follows.

(6) By Lemma 3.3 and Lemma 3.8, this follows by straightforward computation, and we omit the details.

Theorem 4.4 enables us to focus on the 2-subgroups of a metacyclic group K. First we state a lemma, which follows from Proposition 3.3 (2) and Lemma 3.3, and is also necessary when we classify the metacyclic 2-groups.

Lemma 4.3 *Fix* $(l, k) \in \mathbb{N}^2$, $l \geq 1$, $k \geq l+2$, *then* $(2^l, 2^k, 0, 2^{k-l}-1) \in \Omega$, $(2^l, 2^k, 2^{k-1}, 2^{k-l}-1) \in \Omega$, *and* $(2^l, 2^k, 0, 2^{k-l}-1) \cong (2^l, 2^k, 2^{k-1}, 2^{k-l}-1)$.

Theorem 4.5 *Let* $((m, n, g, h), K, T, \Gamma, \Psi)$ *be a Hölder-tuple, where* $2 \mid m$, $2 \mid n$, $h \equiv 3 \pmod 4$. *Fix* $Q \leq K$, $|Q| = 2^{O(2,mn)}$, *fix* $\nu \in \mathbb{N}$, *such that* $1 \leq \nu \leq O(2, mn)$. *Denote* $S = \{U \mid U \leq K, |U| = 2^\nu\}$. $\forall \pi \in \mathbb{N}$, $\pi \leq \min(\nu, O(2, n))$, *denote* $\varpi(\pi)$ *as the integer*

$$\varpi(\pi) = 2^{\min(\nu,O(2,n))-\pi}\Big(\prod_{q\in X(n),\ O(2,\mathrm{ord}(q,h))\geq O(2,m)+\pi+1-\nu} q^{O(q,n)}\Big).$$

(1) *If* $O(2, h+1) + O(2, m) = O(2, n)$, *then* $Q \cong (2^{O(2,m)}, 2^{O(2,n)}, 0, 2^{O(2,h+1)} - 1)$.

(2) *Assume* $O(2, h+1) + O(2, m) \geq O(2, n) + 1$, $O(2, h+1) \leq O(2, n) - 1$.

(2.1) *If* $O(2, g) \geq O(2, n)$, *then* $Q \cong (2^{O(2,m)}, 2^{O(2,n)}, 0, 2^{O(2,h+1)} - 1)$.

(2.2) *If* $O(2, g) = O(2, n) - 1$, *then* $Q \cong (2^{O(2,m)}, 2^{O(2,n)}, 2^{O(2,n)-1}, 2^{O(2,h+1)} - 1)$.

(3) *Assume* $O(2, h+1) \geq O(2, n)$.

(3.1) *If* $O(2, g) \geq O(2, n)$, *then* $Q \cong (2^{O(2,m)}, 2^{O(2,n)}, 0, 2^{O(2,n)} - 1)$.

(3.2) *If* $O(2, g) = O(2, n) - 1$, *then* $Q \cong (2^{O(2,m)}, 2^{O(2,n)}, 2^{O(2,n)-1}, 2^{O(2,n)} - 1)$.

(4) *Assume* $\nu \geq O(2, m) + 1$, *then*

$$|S| = \Big(\sum_{\pi=\nu-O(2,m)+1}^{\min(\nu,O(2,n))} \varpi(\pi)\Big) + 2^{O(2,mn)-\nu}\Big(\prod_{q\in X(n),\ 2\mid\mathrm{ord}(q,h)} q^{O(q,n)}\Big).$$

(5) *Assume* $\nu = O(2, m)$.

(5.1) *If* $\min(O(2, n), O(2, h^m - 1) - 1) > O(2, g)$, *then* $|S| = \sum_{\pi=1}^{\min(\nu,O(2,n))} \varpi(\pi)$.

(5.2) *If* $\min(O(2, n), O(2, h^m - 1) - 1) \leq O(2, g)$, *then*

$$|S| = \Big(\sum_{\pi=1}^{\min(\nu,O(2,n))} \varpi(\pi)\Big) + 2^{\min(O(2,n),O(2,h+1)+O(2,m)-1)}\Big(\prod_{q\in X(n),\ 2\mid\mathrm{ord}(q,h)} q^{O(q,n)}\Big).$$

(6) *If* $\nu \leq O(2, m) - 1$, *then* $\exists!\ \sigma \in \{0, 1\}$, *where*

$$|S| = \sum_{\pi=\sigma}^{\min(\nu,O(2,n))} \varpi(\pi).$$

Moreover, we have

$$\sigma = 0 \ \Leftrightarrow \ \min(\nu, O(2,n)) \leq O(2,g).$$

Proof Write

$$E = \Big\{ l \mid \ l \mid n, l \mid 2^{\nu}, 2^{\nu} \mid ml, \gcd\Big(\frac{n}{l}, \sum_{j=0}^{\frac{2^{\nu}}{l}-1} h^{\frac{mlj}{2^{\nu}}}\Big)\Big| g \Big\}.$$

We omit the details of the proof of (1)–(3) since it is straightforward by using Lemmas 3.3 and 3.8. Now we give a claim, which follows from Lemma 3.3.

Claim 3 Fix $\delta \in \mathbb{N}$, where $\max(0, \nu - O(2,m)) \leq \delta \leq \min(\nu, O(2,n))$.

(i) If $O(2,m) + \delta - \nu \geq 1$, then

$$\gcd\Big(\frac{n}{2^{\delta}}, \sum_{j=0}^{2^{\nu-\delta}-1} h^{\frac{mj}{2^{\nu-\delta}}}\Big) = \varpi(\delta).$$

Moreover, we have

$$2^{\delta} \in E \Leftrightarrow \min(\nu, O(2,n)) - O(2,g) \leq \delta.$$

(ii) If $O(2,m) + \delta - \nu = 0$, then

$$\gcd\Big(\frac{n}{2^{\delta}}, \sum_{j=0}^{2^{\nu-\delta}-1} h^{\frac{mj}{2^{\nu-\delta}}}\Big) = 2^{\min(O(2,n)-\delta,\ O(2,h+1)+O(2,m)-1)}\Big(\prod_{q\in X(n),\ 2|\mathrm{ord}(q,h)} q^{O(q,n)}\Big).$$

$$2^{\delta} \in E \Leftrightarrow \min(O(2,n) - \delta,\ O(2,h+1) + O(2,m) - 1) \leq O(2,g).$$

Now (4)–(6) follows from the fact

$$|S| = \sum_{l\in E} \gcd\Big(\frac{n}{l}, \sum_{j=0}^{\frac{2^{\nu}}{l}-1} h^{\frac{mlj}{2^{\nu}}}\Big)$$

(see Proposition 3.1).

5 Nonabelian Metacyclic p-Groups

In this section, we give a different classification of nonabelian metacyclic p-groups by using the results we obtain in the previous sections.

First, we set an isomorphism invariant for all finite metacyclic groups.

Definition 5.1 *Let* $((m,n,g,h), K, T, \Gamma, \Psi)$ *be a Hölder-tuple, we denote* $\Lambda(m,n,g,h) = \max(|A| \mid A \leq K, A \lhd K, A \text{ is cyclic}, K/A \text{ is cyclic})$.

Lemma 5.1 *Fix* $(m,n,g,h) \in \Omega$, $(\widetilde{m}, \widetilde{n}, \widetilde{g}, \widetilde{h}) \in \Omega$, *then* $n \leq \Lambda(m,n,g,h)$. *Assume that* $(m,n,g,h) \cong (\widetilde{m}, \widetilde{n}, \widetilde{g}, \widetilde{h})$, *then* $\Lambda(m,n,g,h) = \Lambda(\widetilde{m}, \widetilde{n}, \widetilde{g}, \widetilde{h})$, $mn = \widetilde{m}\widetilde{n}$, $m\gcd(n, h-1) = \widetilde{m}\gcd(\widetilde{n}, \widetilde{h}-1)$, $\gcd(g,m,n) = \gcd(\widetilde{g}, \widetilde{m}, \widetilde{n})$, $\gcd(g,m,n,h-1) = \gcd(\widetilde{g}, \widetilde{m}, \widetilde{n}, \widetilde{h}-1)$. *Moreover, if* $n = \widetilde{n}$, *then* $m = \widetilde{m}$, $\mathrm{ord}(n,h) = \mathrm{ord}(n, \widetilde{h})$, $\gcd(n, h-1) = \gcd(n, \widetilde{h}-1)$.

Proof Using Proposition 3.3 and Proposition 3.4 (3), we omit the details.

Theorem 5.1 *Let p be a prime number, fix $(l,k)\in\mathbb{N}^2$, $(t,r)\in\mathbb{N}^2$, where*

$$l\geq 1,\quad k\geq 2,\quad (p^l,p^k,t,r)\in\Omega,\quad r\neq 1,\quad O(p,r-1)<O(p,t).$$

If $p=2$, $k\geq 3$, then $\Lambda(p^l,p^k,t,r)=p^k$.

Proof Let $((p^l,p^k,t,r),K,T,\Gamma,\Psi)$ be a Hölder-tuple. Fix $(\rho,\delta,\varsigma)\in\Gamma$, such that $\Psi(\rho,\delta,\varsigma)\lhd K$, $\Psi(\rho,\delta,\varsigma)$ is cyclic, $K/\Psi(\rho,\delta,\varsigma)$ is cyclic. It is enough to show $\rho\leq p^k$. Notice that $\exists!\ b\in\mathbb{N}$, $\delta=p^b$, $b\leq k$, $\exists!\ a\in\mathbb{N}$, $\rho=p^a$, $b\leq a$. Write $\chi=\sum\limits_{j=0}^{\frac{\rho}{\delta}-1} r^{\frac{p^l\delta j}{\rho}}$. By Proposition 3.4, we have

$$r\equiv 1\ (\operatorname{mod} p^{k-b}),\quad r^{\frac{p^l\delta}{\rho}}\equiv 1\ (\operatorname{mod}\delta),\quad \gcd\Big(\frac{\rho}{\delta},\delta,\frac{\delta(\varsigma\chi+t)}{p^k}\Big)=1,$$

thus $k-b\leq O(p,r-1)<k$, hence $b\geq 1$, and $p=2\wedge r\equiv 3\ (\operatorname{mod} 4)\Rightarrow b\geq 2$. Now assume $a\geq k+1$. Thus $a-b\geq 1$, $p\mid\frac{\rho}{\delta}$, this implies $p\nmid\frac{\delta(\varsigma\chi+t)}{p^k}$, hence $p^{k+1-b}\nmid(\varsigma\chi+t)$. Since $k-b\leq O(p,r-1)<O(p,t)$, thus $p^{k+1-b}\mid t$, hence $p^{k+1-b}\nmid\chi$. But by Lemma 3.3, we have:

$$O(p,\chi)=O\Big(p,\frac{\rho}{\delta}\Big)=a-b\geq k+1-b,$$

which is a contradiction. Therefore $a\leq k$, and the result follows.

Proposition 5.1 *Let p be a prime number, fix $(l,k)\in\mathbb{N}^2$, $(\xi,w)\in\mathbb{N}^2$, where*

$$l\geq 1,\quad k\geq 2,\quad \xi\leq l,\quad 1\leq\xi\leq w<k,\quad \xi+w\geq k.$$

If $p=2$, $l\geq 2$, $k\geq 3$, $w\geq 2$, then $(p^l,p^k,p^\xi,1+p^w)\cong(p^\xi,p^{l+k-\xi},0,1+p^{l+w-\xi})$.

Proof Let $K=\langle x,y\mid x^{p^k}=1,y^{p^l}=x^{p^\xi},yxy^{-1}=x^{1+p^w}\rangle$. Consider $(y,x)\in K\times K$. Since $\xi\leq w$, we get

$$o(y)=p^{l+k-\xi},\ x^{p^\xi}=y^{p^l},\ xyx^{-1}=y^{p^{l+k-\xi}-p^{l+w-\xi}+1},$$

hence $K\cong(p^\xi,p^{l+k-\xi},p^l,p^{l+k-\xi}-p^{l+w-\xi}+1)\in\Omega$. Notice that $\xi\leq l$, by Lemma 3.8 (1.2), we get $K\cong(p^\xi,p^{l+k-\xi},0,1+p^{l+w-\xi})$.

Now we are ready to give the classification of the nonabelian metacyclic p-groups when p is an odd prime number.

Theorem 5.2 *Let p be an odd prime number, consider the set* $\operatorname{Met}(p)$:

$$\begin{aligned}\operatorname{Met}(p)=&\{(p^a,p^b,0,1+p^c)\mid(a,b,c)\in\mathbb{N}^3,a\geq 1,b\geq 2,1\leq c<b,a+c\geq b\}\cup\\&\{(p^\alpha,p^\beta,p^\gamma,1+p^\theta)\mid(\alpha,\beta,\gamma,\theta)\in\mathbb{N}^4,\theta+\gamma\geq\beta,1\leq\theta<\gamma<\min(\alpha,\beta)\}.\end{aligned}$$

Then $\forall G$ is a nonabelian metacyclic p-group, $\exists!\ \overrightarrow{\omega}\in\operatorname{Met}(p)$, $G\cong\overrightarrow{\omega}$.

Proof First, by Lemma 3.3, we get $\operatorname{Met}(p)\subseteq\Omega$, we prove in two steps.

(1) Let G be a nonabelian metacyclic p-group, then $\exists\overrightarrow{\omega}\in\operatorname{Met}(p)$, $G\cong\overrightarrow{\omega}$.

Proof of (1) By Theorem 3.1, since G is nonabelian, $\exists(l,k)\in\mathbb{N}^2$, $\exists(t,r)\in\mathbb{N}^2$, where $l\geq 1$, $k\geq 2$, $r\neq 1$, $G\cong(p^l,p^k,t,r)\in\Omega$. We discuss in three cases.

Case 1 Assume $\min(l,k) \le O(p,t)$. Hence $p^{\min(l,k)} \mid t$, by Lemma 3.8, we get

$$G \cong (p^l, p^k, t, r) \cong (p^l, p^k, 0, 1 + p^{O(p,r-1)}) \in \mathrm{Met}(p).$$

Case 2 Assume $\min(l,k) > O(p,t) \ge O(p, r-1) + 1$. By Lemma 3.8, we get

$$G \cong (p^l, p^k, t, r) \cong (p^l, p^k, p^{O(p,t)}, 1 + p^{O(p,r-1)}) \in \mathrm{Met}(p).$$

Case 3 Assume $\min(l,k) > O(p,t),\ O(p, r-1) \ge O(p,t)$. By Lemma 3.8 and Proposition 5.1, we get

$$G \cong (p^l, p^k, p^{O(p,t)}, 1 + p^{O(p,r-1)}) \cong (p^{O(p,t)}, p^{l+k-O(p,t)}, 0, 1 + p^{l+O(p,r-1)-O(p,t)}) \in \mathrm{Met}(p).$$

And (1) is proved.

(2) Any two distinct 4-tuples in $\mathrm{Met}(p)$ are not isomorphism.

Proof of (2) Using Lemma 5.1 and Theorem 5.1, we omit the details.

Now we turn to the nonabelian metacyclic 2-groups, and the following lemma is well-known.

Lemma 5.2 (see [8, 10]) (1) $(2, 4, 0, 3) \ncong (2, 4, 2, 3)$.

(2) *Let A be a nonabelian group where $|A| = 8$, then $\exists e \in \{0, 2\}$, such that $A \cong (2, 4, e, 3)$.*

(3) *Fix $k \in \mathbb{N},\ k \ge 3$. Let Y denote the following set*

$$\{(2, 2^k, 0, 2^{k-1} \pm 1)\} \cup \{(2, 2^k, t, 2^k - 1) \mid t \in \{0, 2^{k-1}\}\}.$$

Then $\forall (t, r) \in \mathbb{N}^2$, where $(2, 2^k, t, r) \in \Omega,\ r \ne 1$, $\exists!\ \overrightarrow{\omega} \in Y$, such that $(2, 2^k, t, r) \cong \overrightarrow{\omega}$.

Proposition 5.2 *Fix $l \in \mathbb{N},\ l \ge 2$, then $(2^l, 4, 2, 3) \cong (2, 2^{l+1}, 0, 1 + 2^l)$, and $\Lambda(2^l, 4, 0, 3) = 4$.*

Proof Let $G = \langle x, y \mid x^4 = 1, y^{2^l} = x^2, yxy^{-1} = x^3\rangle$. Consider $(y, x) \in G \times G$, we get

$$o(y) = 2^{l+1}, \quad x^2 = y^{2^l}, \quad xyx^{-1} = y^{2^l+1}.$$

By Lemma 3.8 (1.2), we have

$$G \cong (2^l, 4, 2, 3) \cong (2, 2^{l+1}, 2^l, 2^l + 1) \cong (2, 2^{l+1}, 0, 2^l + 1).$$

And similar to the proof of Theorem 5.1, we get $\Lambda(2^l, 4, 0, 3) = 4$.

Proposition 5.3 *Consider the following set $\mathrm{Met}_{(1)}(2)$:*

$$\begin{aligned}\mathrm{Met}_{(1)}(2) = \{&(2^a, 2^b, 0, 1 + 2^c) \mid (a, b, c) \in \mathbb{N}^3, a \ge 1, b \ge 3, 2 \le c < b, a + c \ge b\} \cup \\ &\{(2^\alpha, 2^\beta, 2^\gamma, 1 + 2^\theta) \mid (\alpha, \beta, \gamma, \theta) \in \mathbb{N}^4, \theta + \gamma \ge \beta, 2 \le \theta < \gamma < \min(\alpha, \beta)\}.\end{aligned}$$

Then $\forall (l, k) \in \mathbb{N}^2,\ \forall (t, r) \in \mathbb{N}^2$, where

$$l \ge 1, \quad k \ge 3, \quad r \ne 1, \quad r \equiv 1 \pmod 4, \quad (2^l, 2^k, t, r) \in \Omega,$$

$\exists!\ \overrightarrow{\omega} \in \mathrm{Met}_{(1)}(2)$, such that $(2^l, 2^k, t, r) \cong \overrightarrow{\omega}$.

Proof This is similar to the proof of Theorem 5.2, we omit the details.

The following lemma follows from Lemma 5.1 and Theorem 5.1.

Lemma 5.3 *Fix* $(l,k)\in\mathbb{N}^2,\ (t,r)\in\mathbb{N}^2$, *where*

$$l\geq 1,\quad k\geq 3,\quad r\neq 1,\quad (2^l,2^k,t,r)\in\Omega.$$

Similarly, Fix $(a,b)\in\mathbb{N}^2,\ (c,d)\in\mathbb{N}^2$, *where*

$$a\geq 1,\quad b\geq 3,\quad d\equiv 3\ (\mathrm{mod}\,4),\quad (2^a,2^b,c,d)\in\Omega.$$

(1) *If* $r\equiv 3\ (\mathrm{mod}\,4),\ (2^l,2^k,t,r)\cong(2^a,2^b,c,d)$, *then* $a=l,\ b=k$, *and*
(1.1) *if* $O(2,r+1)\leq k-2$, *then* $O(2,r+1)=O(2,d+1)$;
(1.2) *if* $O(2,r+1)\geq k-1$, *then* $r\in\{2^{k-1}-1,2^k-1\},\ d\in\{2^{k-1}-1,2^k-1\}$.
(2) *If* $r\equiv 1\ (\mathrm{mod}\,4),\ O(2,r-1)<O(2,t)$, *then* $(2^l,2^k,t,r)\ncong(2^a,2^b,c,d)$.

Lemma 5.4 (see [9]) *Fix* $(l,k)\in\mathbb{N}^2,\ s\in\mathbb{N}$, *where*

$$l\geq 2,\quad k\geq 3,\quad 2\leq s\leq k,\quad s+l\geq k+1,$$

then $(2^l,2^k,0,2^s-1)\ncong(2^l,2^k,2^{k-1},2^s-1)$.

Proof Let

$$K=\langle\tau,\eta\mid\tau^{2^k}=1,\eta^{2^l}=1,\eta\tau\eta^{-1}=\tau^{2^s-1}\rangle,\quad L=\langle x,y\mid x^{2^k}=1,y^{2^l}=x^{2^{k-1}},yxy^{-1}=x^{2^s-1}\rangle.$$

Fix $(a,b)\in\mathbb{N}^2,\ 2\nmid b$. By Lemma 3.3 and Proposition 3.3 (3), we deduce that $o(\tau^a\eta^b)=2^l,\ o(x^ay^b)=2^{l+1}$. Hence

$$|\{\omega\mid\omega\in K,o(\omega)=2^l\}|\geq 2^{l+k-1},\quad |\{\sigma\mid\sigma\in L,o(\sigma)=2^{l+1}\}|\geq 2^{l+k-1}.$$

It follows that $K\ncong L$.

Lemma 5.5 *Fix* $(l,k)\in\mathbb{N}^2,\ l\geq 2,\ k\geq 3$, *then* $(2^l,2^k,0,2^{k-1}-1)\ncong(2^l,2^k,0,2^k-1)$, *and* $(2^l,2^k,2^{k-1},2^{k-1}-1)\cong(2^l,2^k,2^{k-1},2^k-1)$.

Proof First, let $K=\langle\tau,\eta\mid\tau^{2^k}=1,\eta^{2^l}=1,\eta\tau\eta^{-1}=\tau^{2^{k-1}-1}\rangle$. Now fix any $(\alpha,\beta,\gamma,\theta)\in\mathbb{N}^4$, such that $(\tau^\alpha\eta^\beta)(\tau^\gamma\eta^\theta)(\tau^\alpha\eta^\beta)^{-1}=(\tau^\gamma\eta^\theta)^{2^k-1}$. By (2.3) of Theorem 3.1 and (2.1) of Lemma 3.1, we get $2\mid\gamma$, and $2^{l-1}\mid\theta$. Using Proposition 3.3.(3), we get $o(\tau^\gamma\eta^\theta)\mid 2^{k-1}$. Hence $K\ncong(2^l,2^k,0,2^k-1)$.

Next, let $G=\langle x,y\mid x^{2^k}=1,y^{2^l}=x^{2^{k-1}},yxy^{-1}=x^{2^{k-1}-1}\rangle$. Consider $(xy^{2^{l-1}},y)\in G\times G$. Using Lemma 3.1 and Proposition 3.3.(3), we get

$$G=\langle xy^{2^{l-1}},\quad y\rangle,\quad \mathrm{o}(xy^{2^{l-1}})=2^k,\quad y^{2^l}=(xy^{2^{l-1}})^{2^{k-1}},\ y(xy^{2^{l-1}})y^{-1}=(xy^{2^{l-1}})^{2^k-1}.$$

It follows that

$$(2^l,2^k,2^{k-1},2^{k-1}-1)\cong G\cong(2^l,2^k,2^{k-1},2^k-1).$$

By Lemma 3.8 (2) and all the previous results in this section, we get the following classification for nonabelian metacyclic 2-groups with order greater than 8.

Theorem 5.3 *Consider the following set* Met(2) :

$$\begin{aligned}\mathrm{Met}(2) = &\{(2^a, 2^b, 0, 1+2^c) \mid (a,b,c) \in \mathbb{N}^3, a \geq 1, b \geq 3, 2 \leq c < b, a+c \geq b\}\\ &\cup \{(2^\alpha, 2^\beta, 2^\gamma, 1+2^\theta) \mid (\alpha,\beta,\gamma,\theta) \in \mathbb{N}^4, \theta+\gamma \geq \beta, 2 \leq \theta < \gamma < \min(\alpha,\beta)\}\\ &\cup \{(2^l, 2^k, 0, 2^s-1) \mid (l,k,s) \in \mathbb{N}^3, l \geq 2, k \geq 3, 2 \leq s \leq k, s+l \geq k\}\\ &\cup \{(2^{\widetilde{l}}, 2^{\widetilde{k}}, 2^{\widetilde{k}-1}, 2^{\widetilde{s}}-1) \mid (\widetilde{l},\widetilde{k},\widetilde{s}) \in \mathbb{N}^3, \widetilde{l} \geq 2, \widetilde{k} \geq 3, 2 \leq \widetilde{s} < \widetilde{k}, \widetilde{s}+\widetilde{l} > \widetilde{k}\}\\ &\cup \{(2, 2^k, 0, 2^{k-1}-1) \mid k \in \mathbb{N}, k \geq 3\} \cup \{(2, 2^k, 0, 2^k-1) \mid k \in \mathbb{N}, k \geq 3\}\\ &\cup \{(2, 2^k, 2^{k-1}, 2^k-1) \mid k \in \mathbb{N}, k \geq 3\} \cup \{(2^l, 4, 0, 3) \mid l \in \mathbb{N}, l \geq 2\}.\end{aligned}$$

Then $\forall G$ *is a nonabelian metacyclic* 2*-group,* $|G| \geq 16$, $\exists \overrightarrow{\omega} \in \mathrm{Met}(2)$*, such that* $G \cong \overrightarrow{\omega}$*. Moreover, any two distinct* 4*-tuples in* Met(2) *are not isomorphism.*

6 A " Reciprocity " Relation on Enumeration of Subgroups

Let G be a finite abelian group, in [4, Theorem 7.2], Birkhoff proved that for any $n \in \mathbb{N}$, $n \mid |G|$, the number of subgroups of order n in G is equal to the number of subgroups of index n $\big($i.e., of order $\frac{|G|}{n}\big)$ in G. In this section, we consider the analog for a finite metacyclic group K.

For convenience, in this section, for a finite group G, we say G has property P, if and only if for any $n \in \mathbb{N}$, $n \mid |G|$, the number of subgroups of order n in G is equal to the number of subgroups of order $\frac{|G|}{n}$ in G.

Also for convenience, in this section, let Θ denote the following set

$$\{(2^l, 2^k, t, 2^s-1) \mid (l,k,s) \in \mathbb{N}^3, t \in \{0, 2^{k-1}\}, 1 \leq l < k \leq s+l, 2 \leq s \leq k\}.$$

Now we state the main result in this section.

Theorem 6.1 *Let* K *be a finite metacyclic group. If* $2 \nmid |K|$*, regard* $\{1_K\}$ *as the Sylow* 2*-group of* K*. Then* K *has property* P *if and only if* K *is nilpotent, and the Sylow* 2*-group of* K *is not isomorphism to any 4-tuple in* Θ*.*

First, we provide some lemmas. The following two lemmas are deduced from Theorem 4.4 (3) and Theorem 4.5 (4)–(6).

Lemma 6.1 *Fix* $(l,k) \in \mathbb{N}^2$, $l \geq 1$, $k \geq 2$*. Let* p *be a prime number. Fix* $(t,r) \in \mathbb{N}^2$*, such that* $(p^l, p^k, t, r) \in \Omega$*. Assume* $p \geq 3$ *or* $p = 2$, $4 \mid (r-1)$*. Let* G *be a finite group, where* $G \cong (p^l, p^k, t, r)$*. Then* G *has property* P*. Actually, fix* $\mu \in \mathbb{N}$, $\mu \leq l+k$*, then*

$$|\{A \mid A \leq G, |A| = p^\mu\}| = \sum_{\theta=0}^{\min(k,l,\mu,k+l-\mu,O(p,t))} p^\theta.$$

Throughout the rest of this section, we fix the following notation: let $(l,k) \in \mathbb{N}^2$, $(t,r) \in \mathbb{N}^2$, where

$$l \geq 1, \quad k \geq 2, \quad r \equiv 3 \pmod 4, \quad (2^l, 2^k, t, r) \in \Omega.$$

Let G be a group, where $G \cong (2^l, 2^k, t, r)$. Write $a = O(2, r+1) + l - 1$.

Lemma 6.2 *Fix $\mu \in \mathbb{N},\ \mu \le l+k$, let $S = \{A \mid A \le G, |A| = p^{\mu}\}$.*
(1) *If $\mu > l$, then $|S| = 2^{\min(l,k+l-\mu)} + 2^{k+l-\mu} - 1$.*
(2) *If $\mu = l,\ \min(k,a) > O(2,t)$, then $|S| = 2^{\min(\mu,k)} - 1$.*
(3) *If $\mu = l,\ \min(k,a) \le O(2,t)$, then $|S| = 2^{\min(\mu,k)} + 2^{\min(k,a)} - 1$.*
(4) *If $\mu < l,\ \min(\mu,k) > O(2,t)$, then $|S| = 2^{\min(\mu,k)} - 1$.*
(5) *If $\mu < l,\ \min(\mu,k) \le O(2,t)$, then $|S| = 2^{\min(\mu,k)+1} - 1$.*

Corollary 6.1 *Assume $k > l$. Let $S_1 = \{A \mid A \le G, |A| = p^l\}$, and $S_2 = \{A \mid A \le G, |A| = p^k\}$. Then $|S_1| \ne |S_2|$, G does not have property* P.

Proof By Lemma 6.2, $\exists \sigma \in \{0,1\},\ |S_1| = 2^l + \sigma 2^{\min(k,a)} - 1$, and $|S_2| = 2^{l+1} - 1$. Since $k > l,\ O(2, r+1) \ge 2$, hence $\min(k,a) > l,\ |S_1| \ne |S_2|$.

Corollary 6.2 *Assume $l \ge k \ge 2$. If $t = 2^{k-1}$, then assume $a \ge k$. Then G has property* P. *Actually, fix $\mu \in \mathbb{N},\ \mu \le l+k$, let $S = \{A \mid A \le G, |A| = p^{\mu}\}$.*
(1) *If $\mu > l$, then $|S| = 2^{k+l-\mu+1} - 1$.*
(2) *If $k \le \mu \le l$, then $(t = 0,\ |S| = 2^{k+1} - 1)$ or $(t = 2^{k-1},\ |S| = 2^k - 1)$.*
(3) *If $\mu < k$, then $|S| = 2^{\mu+1} - 1$.*

The following lemma, which is proved by using the property of normal Hall subgroups, gives the relationship between property P and direct product which we need. We state it without detailed proof.

Lemma 6.3 *Fix $s \in \mathbb{Z}^+$, let $(m_1, \cdots, m_s)$ be an s-tuple of positive integers such that $\forall 1 \le i < j \le s : \gcd(m_i, m_j) = 1$. Let G be a group of order $m_1 m_2 \cdots m_s$. Assume that $\forall 1 \le \lambda \le s$, G contains a normal subgroup of order $m_\lambda \cdots m_s$, and the number of subgroups of order $m_\lambda \cdots m_s$ in G is equal to the number of subgroups of order $m_1 \cdots m_{\lambda-1}$ in G. Then $\forall 1 \le i \le s : \exists!\ B_i \lhd G$, where $|B_i| = m_i$. Moreover, G has property* P *if and only if $\forall 1 \le i \le s : B_i$ has property* P.

Now Fix $s \ge 1$, let $p_1, \cdots, p_s$ be prime numbers where $p_1 < p_2 < \cdots < p_s$, and let $\alpha_1, \cdots, \alpha_s$ be positive integers. Let K be a metacyclic group of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. Since K is supersolvable, therefore $\forall 1 \le \lambda \le s$, K contains a normal subgroup of order $p_\lambda^{\alpha_\lambda} \cdots p_s^{\alpha_s}$. Now Theorem 6.1 follows from Lemma 6.3 and the previous results in this section.

7 Characteristic Subgroups of a Metacyclic p-Group ($p \ge 3$)

Throughout this section, let p be a fixed prime number, $p \ge 3$. Using Theorem 3.2, we give a description of the characteristic subgroups of a finite metacyclic p-group G. Particularly, we show that if G is split, then any characteristic subgroup of G is actually closed under every element in $\mathrm{End}\,(G)$. For any $A \le G$, we write A char G, if and only if A is a characteristic subgroup of G.

The following lemma, which is similar to [16, Lemma 2.1], is needed in our discussion.

Lemma 7.1 *Fix $r \in \mathbb{Z},\ r \ne 1,\ p \mid (r-1)$, write $O(p, r-1) = u$, then $\forall m \in \mathbb{N}$: $r^m - 1 \equiv m(r-1) \pmod{p^{2u+O(p,m)}}$, $\sum\limits_{i=0}^{m-1} r^i \equiv m \pmod{p^{u+O(p,m)}}$.*

Proposition 7.1 *Fix* $(l,k) \in \mathbb{N}^2,\ r \in \mathbb{N},\ l \geq 1,\ k \geq 2,\ (p^l,p^k,0,r) \in \Omega$. *If* $r=1$, *then assume* $l \leq k$. *Let* $((p^l,p^k,0,r),K,T,\Gamma,\Psi)$ *be a Hölder-tuple. Fix* $A \leq K$, *then the following three statements are equivalent to each other.*

(1) A *char* K.

(2) $\exists (a,b) \in \mathbb{N}^2$, *where*

$$k-\max(l,k) \leq 2b-a \leq k-\min(l,O(p,r-1)), \quad b \leq a,\ b \leq k, \quad a \leq b+l,$$

and $A=\Psi(p^a,p^b,0)=\langle \tau^{p^{k-b}}, \eta^{p^{l+b-a}} \rangle$.

(3) $\forall \varphi \in \mathrm{End}\,(K): \varphi[A] \subseteq A$.

Proof Fix $\alpha \in U_{(p^k)}$, where $U_{(p^k)}=\langle \alpha \rangle_{(p^k)}$. By Theorem 3.2, $\exists (a,b) \in \mathbb{N}^2,\ \exists \varsigma \in \mathbb{N}$, where

$$b \leq a,\ b \leq k,\ a \leq b+l,\ \varsigma < p^{k-b},\ (p^a,p^b,\varsigma) \in \Gamma,\ A=\Psi(p^a,p^b,\varsigma).$$

Write $w=\max(0,l-O(p,r-1)),\ v=\max(0,k-l)$. Consider $(\tau\eta^{p^w},\eta)$. By Lemma 3.1 and Lemma 7.1, it's straightforward to verify that

$$(\tau\eta^{p^w})^{p^k}=1_K, \quad \eta(\tau\eta^{p^w})\eta^{-1}=(\tau\eta^{p^w})^r.$$

Thus $\exists!\ \sigma_1 \in \mathrm{Aut}\,(K)$, where

$$\sigma_1(\tau)=\tau\eta^{p^w},\ \sigma_1(\eta)=\eta.$$

Similarly, $\exists!\ (\sigma_2,\sigma_3) \in \mathrm{Aut}\,(K)^2$, where

$$\sigma_2(\tau)=\tau,\ \sigma_2(\eta)=\tau^{p^v}\eta,\ \sigma_3(\tau)=\tau^\alpha,\ \sigma_3(\eta)=\eta.$$

(1)⇒(2) First, notice that

$$\sigma_3(\tau^\varsigma\eta^{p^{l+b-a}})(\tau^\varsigma\eta^{p^{l+b-a}})^{-1}=\tau^{\varsigma(\alpha-1)} \in A,$$

it follows that $p^{k-b} \mid \varsigma(\alpha-1)$. Since $p \nmid (\alpha-1),\ \varsigma < p^{k-b}$, hence $\varsigma=0$. Write $\mu = p^v(\sum_{i=0}^{p^{l+b-a}-1} r^i)$. By Lemma 3.1, $\exists \lambda \in \mathbb{N}$, where

$$\sigma_1(\tau^{p^{k-b}})=\tau^\lambda\eta^{p^{w+k-b}} \in A,\ \sigma_2(\eta^{p^{l+b-a}})=\tau^\mu\eta^{p^{l+b-a}} \in A.$$

By Lemma 3.3 and Lemma 3.2, we have $p^{l+b-a} \mid p^{w+k-b},\ p^{k-b} \mid \mu$, hence we get

$$k-\max(l,k) \leq 2b-a \leq k-\min(l,O(p,r-1)).$$

(2)⇒(3) Fix $\varphi \in \mathrm{End}\,(K)$, hence $\exists \left(\begin{smallmatrix} \alpha & \beta \\ \pi & \theta \end{smallmatrix}\right) \in \mathrm{Met}_2(\mathbb{N})$, where

$$\varphi(\tau)=\tau^\alpha\eta^\beta,\ \varphi(\eta)=\tau^\pi\eta^\theta.$$

Thus $(\tau^\pi\eta^\theta)^{p^l}=1_K,\ [\tau^\pi\eta^\theta,\tau^\alpha\eta^\beta]=(\tau^\alpha\eta^\beta)^{r-1}$. By Lemmas 3.1 and 3.3, we deduce that

$$p^k \mid \pi p^l, \quad p^l \mid \beta(r-1), \quad O(p,\pi) \geq v, \quad O(p,\beta) \geq u.$$

Consider $(\mu_1,\mu_2) \in \mathbb{N}^2$, where

$$\mu_1=\sum_{i=0}^{p^{k-b}-1} r^{\beta i}, \quad \mu_2=\sum_{i=0}^{p^{l+b-a}-1} r^{\theta i},$$

by Lemma 3.1, we have

$$\varphi(\tau^{p^{k-b}}) = \tau^{\alpha\mu_1}\eta^{\beta p^{k-b}}, \quad \varphi(\eta^{p^{l+b-a}}) = \tau^{\pi\mu_2}\eta^{\theta p^{l+b-a}}.$$

By Lemma 3.3, we have

$$O(p, \pi\mu_2) \geq k-b, \quad O(p, \beta p^{k-b}) \geq l+b-a,$$

and by Lemma 3.2, $\varphi(\eta^{p^{l+b-a}}) \in A,\ \varphi(\tau^{p^{k-b}}) \in A$. Hence $\varphi[A] \subseteq A$.

Since (3)$\Rightarrow$(1) is trivial, we've completed the proof.

Now we consider the nonsplit case. Throughout the rest of this section, we fix the following notation: let $(l, k, \varepsilon, s) \in \mathbb{N}^4$, where

$$1 \leq s < \varepsilon < \min(l, k), \quad s + \varepsilon \geq k.$$

Moreover, let $((p^l, p^k, p^\varepsilon, 1+p^s), K, T, \Gamma, \Psi)$ be a Hölder-tuple.

We need the following lemma, which is part of [6, Theorems 3.3 and 3.5]), and gives the generators of Aut (K).

Lemma 7.2 *$\exists!\ (\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \mathrm{Aut}\,(K)^4$, where*

$$\sigma_1(\tau) = \tau, \quad \sigma_1(\eta) = \eta^{1+p^{k-s}}, \quad \sigma_2(\tau) = \tau, \quad \sigma_2(\eta) = \tau^{p^{k-\min(l,k)}}\eta,$$

$$\sigma_4(\tau) = \tau\eta^{p^{l-s}}, \quad \sigma_4(\eta) = \eta^{1+p^{\varepsilon-s}}, \quad \sigma_3(\tau) = \tau^{1+p^{\min(l,k)-\varepsilon}}.$$

And if $k \leq l$, then $\sigma_3(\eta) = \eta$, if $k > l$, then $\sigma_3(\eta) = \tau\eta$. Moreover, we have

$$\mathrm{Aut}\,(K) = \langle\sigma_1\rangle\langle\sigma_2\rangle\langle\sigma_3\rangle\langle\sigma_4\rangle.$$

The following lemma is deduced from Theorem 3.2 and Lemma 7.1.

Lemma 7.3 *Fix $A \leq K$, then $\exists!\ (a, b, \varsigma) \in \mathbb{N}^3$, such that*

$$b \leq \min(a, k),\ a \leq l+b,\ \varsigma < p^{k-b},\ \varsigma p^a \equiv -p^{\varepsilon+b} \pmod{p^k},$$

where $(p^a, p^b, \varsigma) \in \Gamma$, and $A = \Psi(p^a, p^b, \varsigma)$.

The following proposition describes the characteristic subgroups of K.

Proposition 7.2 *Fix $(a, b, \varsigma) \in \mathbb{N}^3$, where*

$$b \leq \min(a, k),\ a \leq l+b,\ \varsigma < p^{k-b},\ \varsigma p^a \equiv -p^{\varepsilon+b} \pmod{p^k}.$$

Let $A = \Psi(p^a, p^b, \varsigma) = \langle\tau^\varsigma\eta^{p^{l+b-a}}, \tau^{p^{k-b}}\rangle$. Write $\lambda_0 = O(p, \varsigma)$.

(1) *Assume $\varsigma = 0$, then A char $K \Leftrightarrow k-l \leq 2b-a \leq k-s$.*

(2) *Assume $\varsigma \neq 0$, $\lambda_0 > \varepsilon+b-a$, then A char K if and only if the following two conditions hold.*

(2.1) *$(l < k,\ k-l \leq 2b-a \leq k-s)$ or $(k \leq l,\ k-l \leq 2b-a,\ \lambda_0 \geq \varepsilon-b)$.*

(2.2) *$(b+\varepsilon \geq a+s)$ or $(b+\varepsilon \leq a+s,\ \lambda_0 \geq k+s-\varepsilon-b)$.*

(3) *Assume $\lambda_0 = \varepsilon+b-a$, write $\lambda_1 = \mathrm{O}(p, \frac{\varsigma}{p^{\varepsilon+b-a}}+1)$. Then A char K if and only if one of the following conditions holds.*

(3.1) $l < k,\ 0 \le 2b - a \le k - s,\ \lambda_1 \ge k + a - l - 2b,\ \lambda_1 \ge k + a + s - 2b - 2\varepsilon.$

(3.2) $k \le l,\ 2b \ge a,\ \lambda_1 \ge k + a + s - 2b - 2\varepsilon.$

(4) *Assume* $\lambda_0 < \varepsilon + b - a$*, then* A char K *if and only if the following two conditions hold.*

(4.1) $2b - a \le k - s,\ \lambda_0 \ge b + s - a,\ 2\lambda_0 \ge k + s - a.$

(4.2) $(k \le l,\ \lambda_0 \ge \varepsilon - b)$ *or* $(l < k,\ 2b \ge a,\ \lambda_0 \ge k + \varepsilon - l - b).$

Proof Assume that $l < k$, and the proof for the case $k \le l$ is similar. Let $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \mathrm{Aut}\,(K)^4$, the same as in Lemma 7.2. By Lemma 7.2, we deduce that

$$A \text{ char } K \ \Leftrightarrow\ \forall j \in \{1,2,3,4\} : \sigma_j[A] \subseteq A.$$

Using Lemmas 3.1, 3.3 and 7.1, by straightforward computation, we deduce that

$$\sigma_1[A] \subseteq A \Leftrightarrow \eta^{p^{k+l+b-a-s}} \in A, \quad \sigma_2[A] \subseteq A \Leftrightarrow 2b \ge a.$$

Now assume that $2b \ge a$, then we have

$$\sigma_3[A] \subseteq A \Leftrightarrow \varsigma p^{l-\varepsilon} \equiv -p^{l+b-a} \pmod{p^{k-b}},$$

as well as

$$\sigma_4[A] \subseteq A \Leftrightarrow \eta^{p^{l+k-s-b}} \in A,\ \tau^{\varsigma + \frac{\varsigma(\varsigma-1)}{2}p^l} \eta^{\varsigma p^{l-s} + (1+p^{\varepsilon-s})p^{l+b-a}} \in A.$$

Now assume $2b \ge a,\ \varsigma p^{l-\varepsilon} \equiv -p^{l+b-a} \pmod{p^{k-b}}$, therefore $\lambda_0 \ge \varepsilon - b$, and $p^{k-b} \mid \frac{\varsigma(\varsigma-1)}{2}p^l$, $k + l + b - a - s \ge k + l - s - b$. We deduce that

$$\tau^{\varsigma + \frac{\varsigma(\varsigma-1)}{2}p^l} \eta^{\varsigma p^{l-s} + (1+p^{\varepsilon-s})p^{l+b-a}} \in A \Leftrightarrow \eta^{\varsigma p^{l-s} + p^{l+b+\varepsilon-a-s}} \in A.$$

Using Lemma 3.2, assume that $\eta^{\varsigma p^{l-s} + p^{l+b+\varepsilon-a-s}} \in A$, then we deduce that $\eta^{p^{l+k-s-b}} \in A \Leftrightarrow 2b - a \le k - s$. Therefore, A char K if and only if

$$0 \le 2b - a \le k - s, \quad \varsigma p^{l-\varepsilon} \equiv -p^{l+b-a} \pmod{p^{k-b}}, \quad \eta^{\varsigma p^{l-s} + p^{l+b+\varepsilon-a-s}} \in A.$$

(1) and (2) Assume $\lambda_0 > \varepsilon + b - a$. Since $\varsigma p^a \equiv -p^{\varepsilon+b} \pmod{p^k}$, therefore

$$\varepsilon + b \ge k,\ \eta^{\varsigma p^{l-s} + p^{l+b+\varepsilon-a-s}} \in A \Leftrightarrow \eta^{p^{l+b+\varepsilon-a-s}} \in A,$$

and

$$\varsigma p^{l-\varepsilon} \equiv -p^{l+b-a} \pmod{p^{k-b}} \Leftrightarrow l + b - a \ge k - b \Leftrightarrow k - l \le 2b - a.$$

And by Lemmas 3.2–3.3, we deduce that $\eta^{p^{l+b+\varepsilon-a-s}} \in A$ if and only if $(b + \varepsilon \ge a + s)$ or $(b + \varepsilon \le a + s,\ \lambda_0 \ge k + s - \varepsilon - b)$.

(3) Assume that $\lambda_0 = \varepsilon + b - a$, by Lemmas 3.2 (2) and 3.3, we deduce that

$$\eta^{\varsigma p^{l-s} + p^{l+b+\varepsilon-a-s}} \in A \Leftrightarrow \eta^{p^{l+b+\varepsilon-a-s+\lambda_1}} \in A \Leftrightarrow \lambda_1 \ge k + a + s - 2b - 2\varepsilon.$$

Since $\varsigma p^{l-\varepsilon} \equiv -p^{l+b-a} \pmod{p^{k-b}} \Leftrightarrow \lambda_1 \ge k + a - l - 2b$, (3) is proved.

(4) Assume $\lambda_0 < \varepsilon + b - a$. Thus we have

$$\varsigma p^{l-\varepsilon} \equiv -p^{l+b-a} \pmod{p^{k-b}} \Leftrightarrow \lambda_0 \ge k + \varepsilon - l - b.$$

By Lemmas 3.2 (2) and 3.3, we deduce that

$$\eta^{\varsigma p^{l-s}+p^{l+b+\varepsilon-a-s}} \in A \ \Leftrightarrow\ \eta^{p^{\lambda_0+l-s}} \in A \ \Leftrightarrow\ \lambda_0 \geq b+s-a,\ 2\lambda_0 \geq k+s-a,$$

and (4) is proved.

Acknowledgement The author is grateful to Professor Zhu Shenglin for his guidance during the work.

References

[1] Baer, R., Engelsche elemente nöetherscher gruppen, *Math. Ann.*, **133**, 1957, 256–270.

[2] Basmaji, B. G., On the isomorphisms of two metacyclic groups, *Proc. Amer. Math. Soc.*, **22**, 1969, 175–182.

[3] Beyl, F. R., The classification of metacyclic p-groups, and other applications of homological algebra to group theory, *Ph.D. thesis*, Cornell University, 1972.

[4] Birkhoff, G., Subgroups of abelian groups, *Proc. London Math. Soc.*, **38**, 1935, 385–401.

[5] Carter, R. W., Nilpotent self-normalizing subgroups of soluble groups, *Math. Zeit.*, **75**, 1961, 136–139.

[6] Curran, M. J., The automorphim group of a nonsplit metacyclic p-group, *Arch. Math.*, **90**, 2008, 483–489.

[7] Gerhards, L., Über die struktur bizyklischer gruppen, *J. reine angew. Math.*, **241**, 1970, 180–199.

[8] Hall, M., Theory of Groups, Macmillan, New York, 1959.

[9] Hempel, C. E., Metacyclic groups, *Comm. in Algebra*, **28**, 2000, 3865–3897.

[10] Huppert, B., Endliche Gruppen I, Springer-Verlag, Berlin, New York, 1967.

[11] King, B. W., Presentations of metacyclic groups, *Bull. Aus. Math. Soc.*, **8**, 1973, 101–131.

[12] Liedahl, S., Enumeration of metacyclic p-groups, *J. Algebra*, **186**, 1996, 436–446.

[13] Lindenberg, W., Struktur und klassifizierung bizyklischer p-gruppen, *Gesellsch. Math. Datenverarbeitung. Bonn. Ber.*, **40**, 1971, 1–36.

[14] Newman, M. F. and Xu, M. Y., Metacyclic groups of prime-power order, *Adv. in Math* (*China*), **17**, 1988, 106–107.

[15] Rédei, L., Endliche p-Gruppen, Akadémiai Kiadó, Budapest, 1989.

[16] Sim, H. S., Metacyclic groups of odd order, *Proc. London Math. Soc.*, **69**, 1994, 47–71.

[17] Xu, M. Y. and Qu, H. P., Finite p-groups, Beijing University Press, Beijing, 2010 (in Chinese).

[18] Xu, M. Y. and Zhang, Q. H., A classification of metacyclic 2-groups, *Alg. Colloq.*, **13**, 2006, 25–34.

[19] Zhang, Y. D., The Construction of Finite Groups, Science Press, Beijing, 1982 (in Chinese).