AUTOMORPHISMS OF METACYCLIC GROUPS OF PRIME POWER ORDER

HYO-SEOB SIM

1. Introduction

There are a number of determinations of the isomorphism types of finite metacyclic p-groups in the literature (see, for example, Beyl [1], King [2], Newman and Xu [3], and Sim [6]). When \( p \) is odd, the results in the literature typically take this form: given an odd prime \( p \), each finite metacyclic \( p \)-group has precisely one presentation

\[
\langle x, y \mid x^{p^\alpha} = y^{p^\beta}, \ y^{p^\gamma} = 1, \ y^x = y^{1+p^\delta} \rangle
\]

with the parameters \( \alpha, \beta, \gamma, \delta \) subject to certain restrictions. (The choice of the restrictions varies from paper to paper, to fit the approach adopted.)

Our main result presents a determination of the automorphism group of a finite nonabelian metacyclic \( p \)-group in terms of the parameters which are invariants of the isomorphism type, by using the presentations of the above form.

Let \( G \) be a metacyclic group and let \( K \) be a cyclic normal subgroup of \( G \) such that \( G/K \) is cyclic. Then the automorphism group of \( G \) acts on the set of all such cyclic normal subgroups. Our strategy to determine the automorphisms of a metacyclic \( p \)-group \( G \) may be stated as follows: we first investigate the orbit containing \( K \) under the action of the automorphism group of \( G \), and then we try to determine all automorphisms of \( G \) that fix \( K \) setwise. This enables us to have the main results as follow.
Theorem 1.1. Let $P$ be a finite nonabelian split metacyclic $p$-group for an odd prime $p$.

(i) $P$ has the presentation of the form

$$P = \langle a, b \mid a^{\alpha} = 1, b^{p^\beta} = 1, a^b = a^{1+p^\gamma} \rangle,$$

where $0 < \gamma < \beta \leq \alpha + \gamma$, different values of parameters $\alpha, \beta, \gamma$ giving nonisomorphic such groups.

(ii) $\text{Aut}P$ is a soluble group of order $(p-1)p^{\min(\alpha,\beta)+\min(\alpha,\gamma)+\alpha+\gamma-1}$ and each Hall $p'$-subgroup of $\text{Aut}P$ is isomorphic to $\mathbb{Z}_{p-1}$.

Theorem 1.2. Let $P$ be a finite nonsplit metacyclic $p$-group for an odd prime $p$.

(i) $P$ has the presentation of the form

$$P = \langle a, b \mid a^{p^\alpha} = b^{p^\delta}, b^{p^\beta+1} = 1, a^b = b^{1+p^\gamma} \rangle$$

where $0 < \delta \leq \gamma < \beta < \alpha$, different values of parameters $\alpha, \beta, \gamma, \delta$ giving nonisomorphic such groups.

(ii) $\text{Aut}P$ is a $p$-group of order $p^{\alpha+\beta+\gamma+\delta}$.

2. Background results

We first setup some notation and terminology.

Let $m$ and $n$ be positive integers. Define

$$|m \mod n| := \min\{i \in \mathbb{Z} : i > 0, m^i \equiv 1 \mod n\},$$

the multiplicative order of $m$ modulo $n$; it is not defined unless $\gcd(m, n) = 1$.

We denote the commutator subgroup of a group $G$ by $G'$, the centre by $Z(G)$ and the Frattini subgroup by $\Phi(G)$. The automorphism group of a group $G$ is denoted by $\text{Aut}(G)$. If $G$ is a finite $p$-group, then $\Omega_1(G)$ denotes the subgroup generated by all elements of order $p$. For two subgroups $H$ and $K$ of a group $G$, let $C_H(K)$ denote the centralizer of $K$ in $H$ and let $N_H(K)$ denote the normalizer of $K$ in $H$.

We now collect some basic properties of metacyclic groups, which will be used later. The proofs of the results presented here can be found
in [6] if the relevant references were not given. In this note we only deal with \textit{finite} metacyclic groups, so for simplicity, by a metacyclic group we shall mean a finite metacyclic group.

Let $G$ be a metacyclic group and let $K$ be a cyclic normal subgroup of $G$ such that $G/K$ is cyclic. Then there exists a cyclic subgroup $S$ such that $G = SK$. Such a factorization is called a metacyclic factorization. In particular, if $G$ has a split metacyclic factorization, namely $G = SK$ such that $SCK = 1$, then $G$ is called \textit{split metacyclic}.

**Lemma 2.1.** Let $G$ be a group with a metacyclic factorization $G = SK$. Let $S = \langle a \rangle$ and $K = \langle b \rangle$. Let $r$ be an integer such that $a^{-1}ba = b^r$. Set $s := |r \text{ mod } |K||$ and $t := |K|/\gcd(|K|, r - 1)$. Then $G' = \langle a^{r-1} \rangle \cong \mathbb{Z}_t$, $Z(G) = \langle a^s, b^t \rangle$ and $S/C_S(K) \cong \mathbb{Z}_s$.

**Lemma 2.2.** Let $P$ be a metacyclic $p$-group for an odd prime $p$ and let $P = SK$ be a metacyclic factorization. Then $S/C_S(K) \cong P'$.

**Lemma 2.3.** [7, Theorem 4.3.14] Let $P$ be a metacyclic $p$-group for an odd prime $p$. Then $P$ is regular, and so $(ab^{-1})^{p^m} = 1 \iff a^{p^m} = b^{p^m}$, for every $a, b$ in $P$ and every nonnegative integer $m$. If $|P'|$ divides $n$, then $(a^nb^l)^n = a^{nm}b^{ln}$.

**Lemma 2.4.** If $P$ is a noncyclic metacyclic $p$-group for an odd prime $p$,

(i) $P/\Phi(P) \cong \mathbb{Z}_p \times \mathbb{Z}_p$;

(ii) $\Omega_1(P) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

**Lemma 2.5.** Let $P$ be a noncyclic metacyclic $p$-group for an odd prime $p$ and $K$ a subgroup. Then

(i) $K$ is cyclic if and only if $K$ does not contain $\Omega_1(P)$;

(ii) $K$ is normal and $P/K$ is cyclic if and only if $K$ contains $P'$ and $K$ is not contained in $\Phi(P)$.

**Lemma 2.6.** Let $P$ be a metacyclic $p$-group for an odd prime $p$. If $K$ and $P/K$ are cyclic, then there exists a cyclic subgroup $S$ of $P$ such that $P = SK$ and $|S| = \exp P$.

We will also need the following lemma; a stronger version of it can be found in Rose [5, p. 193].
Lemma 2.7. If $C$ is a cyclic subgroup of a finite abelian group $A$ such that $|C| = \exp A$, then $C$ is a direct factor of $A$.

3. Presentations of metacyclic $p$-groups

In this section, we consider canonical presentations for metacyclic $p$-groups for an odd $p$.

Let $p$ be an odd prime and let $P$ be a noncyclic metacyclic $p$-group. Let $P = SK$ be a metacyclic factorization of $P$. Define $\alpha, \beta, \gamma, \delta$ by

$$p^\alpha = |S : S \cap K|, \quad p^\beta = |K : S \cap K|, \quad p^\gamma = |K : P'|, \quad p^\delta = |S \cap K|.$$ 

Then it is easy to show that $P$ has the presentation

$$\langle a, b \mid a^{p^\alpha} = b^{p^\beta}, \quad b^{p^\beta + \delta} = 1, \quad b^\alpha = b^{1+p^\gamma} \rangle$$

and $0 \leq \delta \leq \gamma \leq \beta + \delta \leq \alpha + \gamma$, $1 \leq \gamma$. The presentation is obtained by choosing relevant generators $a$ of $S$ and $b$ of $K$ from the metacyclic factorization $P = SK$; we call this presentation a metacyclic presentation of $P$, and we denote it by $\varphi(\alpha, \beta, \gamma, \delta)$. Note that the parameters of the presentation are not invariants of the isomorphism type of $P$ in general, but determined by the choice of a metacyclic factorization of $P$.

If $\delta = 0$, then $P$ is a split metacyclic; in this case, we denote the corresponding metacyclic presentation simply by $\varphi(\alpha, \beta, \gamma)$ and call it a split metacyclic presentation of $P$. A metacyclic $p$-group is split if and only if it has a split metacyclic presentation.

Consider the set

$$\{ K : K \trianglelefteq P, \ K \text{ and } P/K \text{ cyclic } \}.$$ 

The subgroups of minimal order in this set will be called minimal kernels. A metacyclic factorization $P = SK$ is called standard if $|S| = \exp P$ and $K$ is a minimal kernel. Lemma 2.6 guarantees that $P$ has a standard metacyclic factorization. The corresponding metacyclic presentation to a standard metacyclic factorization $P = SK$ is called a standard metacyclic presentation of $P$. 


Automorphisms of metacyclic $p$-groups

As a special case of the general observation for the metacyclic groups of odd order in [6], we see that a metacyclic presentation $\varphi(\alpha, \beta, \gamma, \delta)$ of a noncyclic metacyclic $p$-group $P$ is standard if and only if the parameters

$$0 \leq \delta \leq \gamma \leq \beta \leq \alpha, \ 1 \leq \gamma,$$

and so the parameters are invariants of the isomorphism type of $P$.

We now consider split noncyclic metacyclic $p$-groups. Let $\varphi(\alpha, \beta, \gamma, \delta)$ be a standard metacyclic presentation of $P$. If $\delta = 0$, then $P$ is obviously split; if $\alpha = \beta$, then $P = \langle ab \rangle$ is split; if $\beta = \gamma$, then $P = \langle ab^{\alpha-\beta} \rangle$ is split. Suppose now that $P$ is split. Then $P$ has a split metacyclic presentation $\varphi(\alpha', \beta', \gamma')$, where $\alpha = \max\{\alpha', \gamma'\}$, $\beta = \min\{\alpha', \beta'\}$, $\gamma = \min\{\alpha', \gamma'\}$, $\delta = \max\{\alpha', \beta'\} - \min\{\alpha', \gamma'\}$. Therefore either $\alpha = \beta$, or $\beta = \gamma$, or $\delta = 0$. Consequently, $P$ is split if and only if either $\alpha = \beta$, or $\beta = \gamma$, or $\delta = 0$. We also observe that $\varphi(\alpha', \beta', \gamma')$ is the unique split metacyclic presentation of $P$ if $P$ is nonabelian. This means the parameters for the split metacyclic presentation of $P$ are invariants of the isomorphism type, provided $P$ is not abelian.

By summarizing the above observation, we have

**Theorem 3.1.** Let $p$ be an odd prime.

(i) Every finite nonabelian split metacyclic $p$-group $P$ has a presentation of the form

$$P = \langle a, b \mid a^{\alpha} = 1, b^{\beta} = 1, b^{\alpha} = b^{1+p^\gamma} \rangle$$

where $\alpha, \beta, \gamma$ are positive integers such that $1 \leq \gamma < \beta \leq \alpha + \gamma$. Conversely, each such presentation defines a nonabelian split metacyclic $p$-group of order $p^{\alpha+\beta}$, different values of the parameters $\alpha, \beta, \gamma$ (with the above condition) giving nonisomorphic such groups.

(ii) Every finite nonsplit metacyclic $p$-group $P$ has a presentation of the form

$$P = \langle a, b \mid a^{\alpha} = b^{\beta}, b^{\beta+\delta} = 1, b^{\alpha} = b^{1+p^\gamma} \rangle$$

where $\alpha, \beta, \gamma, \delta$ are nonnegative integers such that $1 < \delta \leq \gamma < \beta < \alpha$. Conversely, each such presentation defines such a metacyclic $p$-group of order $p^{\alpha+\beta+\delta}$, different values of the parameters $\alpha, \beta, \gamma, \delta$ (with the above condition) giving nonisomorphic groups.
4. Automorphisms of metacyclic $p$-groups

In this section, we determine the automorphism groups of non-abelian metacyclic $p$-groups for an odd prime $p$. With Theorem 3.1, this will complete the proofs of the main results.

We first observe the following lemma.

**Lemma 4.1.** For an odd prime $p$, let $P$ be a finite nonabelian metacyclic $p$-group with a metacyclic factorization $P = SK$ such that $P'$ properly contains $S \cap K$. There exists a one-to-one correspondence between the set $\{K\theta : \theta \in \text{Aut}P\}$ and $\text{Hom}(S/P'/P', K/P')$, the set of all homomorphisms from $S/P'/P'$ to $K/P'$.

**Proof.** Let $\theta$ be an automorphism of $P$. Since the cyclic $p$-group $K\theta$ contains $P'$, and $S \cap K < P'$, we have $S \cap K\theta = S \cap K < P'$. Thus $P = S(K\theta)$ is a metacyclic factorization of $P$. It follows that $K\theta/P'$ is a direct complement of $S/P'/P'$ in $P/P'$.

On the other hand, let $Y/P'$ be a direct complement of $S/P'/P'$ in $P/P'$. Then $SY = P$ and $S/P' \cap Y = P'$. Since $S/P'$ contains $\Omega_1(P)$ and $S/P' \cap Y = P'$ is cyclic, the subgroup $Y$ does not contain $\Omega_1(P)$; so $Y$ is cyclic by Lemma 2.5. Since $P' \leq Y$, we see that $Y$ is also normal in $P$. Consequently, $P = SY$ is a metacyclic factorization such that $|K| = |Y|$ and $S \cap Y = S \cap K$. Therefore we see that the metacyclic factorizations $P = SK$ and $P = SY$ yield the same metacyclic presentation of $P$. This gives an automorphism $\theta$ of $P$ such that $K\theta = Y$.

Consequently, we now have showed that there exists a one-to-one correspondence between $\{K\theta : \theta \in \text{Aut}P\}$ and the set of all complements of $S/P'/P$ in $P/P'$. Since $P/P'$ is the direct product of $S/P'/P'$ and $K/P'$, the lemma is now clear from (11.1.2) in [4].

Let $p$ be an odd prime and let $P$ be a nonabelian metacyclic $p$-group. $P$ has a presentation of the form

$$\langle a, b \mid a^{p^\alpha} = b^{p^\beta}, \quad b^{p^{\beta+\delta}} = 1, \quad b^a = b^{1+p^\gamma} \rangle,$$

where $1 \leq \gamma$, $0 \leq \delta \leq \gamma \leq \beta + \delta \leq \alpha + \gamma$. Let $S = \langle a \rangle$ and let $K = \langle b \rangle$. By Lemma 2.1 and Lemma 2.2, $P' = \langle b^{p^\gamma} \rangle$ and $C_p(K) = \langle a^{p^{\beta+\delta-\gamma}}, b \rangle$; so $|P'| = p^{\beta+\delta-\gamma}$. Since $P$ is regular (see Lemma 2.3), $(a^i b^j)^{p^n} = a^{ip^n} b^{jp^n}$ for all integers $i, j, n$ with $n \geq \beta + \delta - \gamma$. 

Let $$A(K) := \{x \in P : y^x = y^{1+p^r}, y \in K\}$$. Then $$A(K) = aC_P(K)$$. Let $$N$$ be the set of all automorphisms $$\theta$$ of $$P$$ such that $$K\theta = K$$. Then $$N$$ is a subgroup of $$\text{Aut}P$$. The map $$a \mapsto x, \ b \mapsto y$$ defines an automorphism in $$N$$ if and only if $$x \in A(K), \langle y \rangle = K$$ and $$x^{p^s} = y^{p^\alpha}$$. Define $$\mathcal{K} := \{K\theta : \theta \in \text{Aut}P\}$$.

Then since $$\text{Aut}(P)$$ acts transitively on $$\mathcal{K}$$, we have

$$|\text{Aut}P| = |N||\mathcal{K}|.$$

Let $$r, s, t$$ be integers such that

$$0 \leq r < p^{\alpha-\beta+\gamma-\delta}, \ 0 \leq s < p^{\beta+\delta}, \ 0 \leq t < p^{\beta+\delta}.$$

The map

$$a \mapsto a^{1+rp^{\beta+\delta-\gamma}}t^{\gamma-1}, \ b \mapsto b^t$$

defines an automorphism in $$N$$ if and only if

$$\gcd(p, t) = 1, \ tp^\beta \equiv p^\beta(1 + rp^{\beta+\delta-\gamma}) + sp^\alpha \mod p^{\beta+\delta}.$$

In this case, the automorphism so defined is denoted by $$\theta_{r,s,t}$$. On the other hand, let $$\theta$$ be an automorphism in $$N$$. Then $$a\theta \in aC_P(K)$$. Since $$C_P(K) = \langle a^{p^{\beta+\delta-\gamma}}, b \rangle$$, we have $$a\theta = a^{1+rp^{\beta+\delta-\gamma}}b^t$$ for some integers $$r, s$$ such that $$0 \leq r < p^{\alpha-\beta+\gamma-\delta}$$ and $$0 \leq s < p^{\beta+\delta}$$. Obviously $$b\theta = b^t$$ for some integer $$t$$ with $$0 \leq t < p^{\beta+\delta}$$. Therefore, $$N$$ consists of the automorphisms $$\theta_{r,s,t}$$ with the above conditions.

We now consider a nonabelian split metacyclic $$p$$-group $$P$$. By Theorem 3.1, $$P$$ has the presentation as the above for some integers $$\alpha, \beta, \gamma$$ such that $$1 \leq \gamma < \beta \leq \alpha + \gamma$$. By the above observation, we have

$$\theta_{r,s,t} \in N \iff \gcd(p, t) = 1, \ sp^\alpha \equiv 0 \mod p^\beta.$$. 
Thus \(|N| = (p - 1)p^{\alpha + \gamma - 1 + \min(\alpha, \beta)}\). On the other hand, observing that 
\(|SP'/P'| = p^\alpha\) and \(|K/P'| = p^\gamma\) we have, from Lemma 4.1, that 
\(|K| = p^{\min(\alpha, \gamma)}\) and so 
\(|\text{Aut}P| = (p - 1)p^{\min(\alpha, \beta) + \min(\alpha, \gamma) + \alpha + \gamma - 1}\). Moreover, 
each Hall \(p'\)-subgroup of \(\text{Aut}P\) is isomorphic to the cyclic group of 
order \(p - 1\), and so \(\text{Aut}P\) is soluble.

We finally consider a nonsplit metacyclic \(p\)-group \(P\). By Theorem 3.1 again, we can choose the parameters in the above presentation 
for \(P\) so that \(1 < \delta < \gamma < \beta < \alpha\). We note that \(P'\) contains \(S \cap K\) 
properly. By applying Lemma 4.1, we get \(|\text{Aut}P| = p^{\min(\alpha, \gamma)} = p^\gamma\) in this 
case. We also have

\[\theta_{r,s,t} \in N \iff \gcd(p, t) = 1, \ sp^{\alpha - \beta} \equiv t - 1 \mod p^\delta\]

from the above observation. There exist precisely \(p^{2\beta + \delta}\) different pairs 
of integers \(s\) and \(t\) satisfying the condition. So we have 
\(|\text{Aut}P| = p^{\alpha + \beta + \gamma + \delta}\).

We summarize the observation as follow:

**Theorem 4.2.** For an odd prime \(p\), let \(P\) be a finite nonabelian 
metacyclic \(p\)-group. 

(i) If \(P\) is presented by

\[P = \langle a, b \mid a^{p^\alpha} = 1, b^{p^\gamma} = 1, a^b = a^{1+p^\gamma} \rangle,\]

where \(0 < \gamma < \beta \leq \alpha + \gamma\), then

\(|\text{Aut}P| = (p - 1)p^{\min(\alpha, \beta) + \min(\alpha, \gamma) + \alpha + \gamma - 1}\).

Moreover, each Hall \(p'\)-subgroup of \(\text{Aut}P\) is isomorphic to \(\mathbb{Z}_{p-1}\), and 
so \(\text{Aut}P\) is soluble.

(ii) If \(P\) is presented by

\[P = \langle a, b \mid a^{p^\alpha} = b^{p^\beta}, b^{p^\beta s} = 1, b^a = b^{1+p^\gamma} \rangle\]

where \(\alpha, \beta, \gamma, \delta\) are nonnegative integers such that \(1 < \delta \leq \gamma < \beta < \alpha\),
then \(\text{Aut}P\) is a \(p\)-group of order \(p^{\alpha + \beta + \gamma + \delta}\).
References


Division of Mathematical Sciences
Pukyong National University
Pusan 608-737, Korea