Thesis for the Degree of

Master of Education

A Classi¯cation of Metacyclic Groups of Odd Prime-Power Order

by

Sang-Won Lee

Graduate School of Education

Pukyong National University

August 2002

A Classification of Metacyclic Groups of Odd Prime-Power Order

홀수 소수의 거듭제곱 위수를 갖는 메터순환군의 분류

Advisor : Hyo-Seob Sim

by

Sang-Won Lee

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Education

Graduate School of Education
Pukyong National University

August 2002

A Classification of Metacyclic Groups of Odd Prime-Power Order

A Dissertation
by
Sang-Won Lee

Approved as to style and content by :

_____
Young-Gheel Baik, Ph. D.

_____ _____
Hyun-Jong Song, Ph. D. Hyo-Seob Sim, Ph. D.

June 22, 2002

Contents

홀수 소수의 거듭제곱 위수를 갖는 메터순환군의 분류

이 상 원

부경대학교 교육대학원 수학교육전공

요 약

G/K가 순환군(cyclic group)이 되는 정규순환부분군(cyclic normal subgroup) K가 존재할 때, 군(group) G를 메터순환군(metacyclic group)이라 한다. 메터순환군은 가해군(soluble group)의 특별한 경우로서 오랫동안 여러 학자들의 주목을 받아왔다.

본 논문의 주요 목적은, 지금까지 알려진 연구방법의 대안으로서, 홀수 소수 p에 대하여 유한메터순환 p-군(finite metacyclic groups for an odd prime p)의 부분군 (subgroups)의 구조와 대응하는 가환 p-군(abelian p-groups)의 부분군의 구조와의 관계를 이용하여 홀수 소수 거듭제곱의 위수를 갖는 메터순환군(metacyclic groups of odd prime-power order)을 그 동형사상형(isomorphism type)에 의하여 분류하는 것이다.

1 Introduction

A metacyclic group is a group G that has a cyclic normal subgroup K such that G/K is also cyclic. Given a metacyclic group G, if K is a cyclic normal subgroup of G, then there exists a cyclic subgroup S such that $G = SK$. Therefore each metacyclic group G has a factorization $G = SK$. Subgroups and quotient groups of metacyclic groups are also metacyclic. Some special classes of metacyclic groups can be found in [3] and Chapter 1 of Coxeter and Moser [5]. As a special subfamily of soluble groups, metacyclic groups have been received considerable attention by many authors.

Metacyclic groups are usually presented on two generators with three defining relations. In fact each metacyclic group has presentations of the form

$$\langle\, x, y \,|\, x^{\mathsf{m}} = y^{\mathsf{s}},\ y^{\mathsf{n}} = 1,\ x^{\mathsf{i}\,1} y x = y^{\mathsf{r}} \,\rangle$$

with the arithmetic conditions

$$0 < m, n,\ r^{\mathsf{m}} \equiv 1 \bmod n,\ s(r-1) \equiv 0 \bmod n.$$

Conversely, every group defined by such a presentation is a metacyclic group of order mn. Even if this characterization is well-known, it is unsatisfactory in that the parameters involved in this metacyclic presentation may not be invariants of the isomorphism types.

Most of the literature of metacyclic groups concerns the classification of metacyclic groups of prime power order, or more simply metacyclic p-groups.

Various classifications for metacyclic p-groups may be found in [9, 10], [3], [8] and [13]. The classifications are usually given by listing representatives of the isomorphism types of metacyclic p-groups in terms of various standard presentations for which the parameters involved consist of some invariants of the isomorphism types.

The main purpose of this thesis is to give an alternative approach to the classification of metacyclic p-groups for each odd prime p. Apart from the previous approaches, our approach relies on a understanding of the relationship between the subgroup lattices of finite metacyclic p-groups and corresponding abelian p-groups for each odd prime p.

A lattice isomorphism of the subgroup lattice of a group G onto that of a group H is called a projectivity from G onto H. Projectivity of groups were extensively studied by Baer [2, 1]. It is known in [2] that every finite metacyclic p-group for an odd prime p has a projectivity from some abelian p-group. We use this result to give a proof of the following classification of finite metacyclic p-groups for an odd prime p:

(1) Every noncyclic metacyclic p-group P for an odd prime p has a presentation of the form:

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

where $\alpha, \beta, \gamma, \delta$ are nonnegative integers such that $\alpha \geq \beta \geq \gamma \geq \delta,\ \gamma \geq 1$.

(2) Each such a presentation defines a metacyclic p-group of order $p^{\alpha+\beta+\gamma+\delta}$;

di®erent values of the parameters $\alpha, \beta, \gamma, \delta$ with the above condition give non-isomorphic metacyclic p-groups.

2 General conventions and some basic facts

We first set up some general conventions and notation, which will be used frequently in this thesis.

The cardinality of a set X is denoted by $|X|$.

Throughout this thesis actions of groups and most algebraic maps such as automorphisms, homomorphisms and isomorphisms are usually written as right operators. If g and h are elements of a group, the conjugate $h^{-1}gh$ is denoted by g^h.

The identity element of a multiplicative group is denoted by 1 and the same notation is also used for the trivial subgroup consisting of the identity element. Let G be a finite group. The center of G is denoted by $Z(G)$. For a subgroup H of G, the centralizer $\{x \in G \mid xh = hx \text{ for all } h \in H\}$ of H in G is denoted by $C_G(H)$, and the normalizer $\{x \in G \mid xH = Hx\}$ of H in G is denoted by $N_G(H)$. The commutator subgroup of G is denoted by G'. The exponent of G is the smallest positive integer n such that $x^n = 1$ for all $x \in G$; the exponent of G is denoted by $\exp(G)$. The Frattini subgroup of G is denoted by $\Phi(G)$. If G is a finite p-group, then $\Omega_1(G)$ denotes the subgroup generated by all elements of order p.

The kernel of a homomorphism φ of a group is denoted by $\ker(\varphi)$. The automorphism group of a group G is denoted by $\mathrm{Aut}(G)$.

The notation and terminology not defined in this thesis is standard and can be found in almost all standard books on related areas.

We here have some investigation about the automorphism groups of finite cyclic group.

Let Z_n denote the additive group of integers modulo n for a positive integer n. The subset U_n of all units in Z_n forms an abelian group under multiplication modulo n. It is well-known that the automorphism group of a cyclic group of order n can be identified with this multiplicative group U_n.

Lemma 2.1. *The automorphism group $\mathrm{Aut}(\mathsf{Z}_n)$ is isomorphic to U_n.*

Proof. It follows from $i\alpha = (1\alpha)i$ that any automorphism α of Z_n is completely specified by 1α. Another easy fact is that $1\alpha_k = k$ determines an automorphism α_k of Z_n if k is non-zero and prime to n; and all the automorphisms of Z_n are determined by such values of k in $1 \leq k < n$. Consider the correspondence in which α_k is paired with k in U_n. That this is an isomorphism of $\mathrm{Aut}(\mathsf{Z}_n)$ with U_n is evident. □

The structure U_n is well-known, see [11] for example. We here just state the special case when n is a power of an odd prime number.

Theorem 2.2. *If p is an odd prime, then U_{p^α} is the cyclic group of order $(p-1)p^{\alpha-1}$.*

We adopt the following well-known fact without proof.

Lemma 2.3. *Let p be an odd prime. If $r \equiv 1 \bmod p$, then the multiplicative order of r in U_{p^n} is equal to $p^n/\gcd(p^n, r-1)$.*

The following well-known result, which is known as **Dedekind Law** [14, Theorem 3.14, p. 26], is useful.

Lemma 2.4. *Let A, B and C be any subgroups of a group such that $A \leq B$. Then $A(B \cap C) = B \cap AC$.*

3 Subgroup lattices of groups

We begin with a brief introduction of the basic concepts of lattice theory, which is largely based on [12].

A **partially ordered set** is a set P together with a binary relation $\leq$ such that the following conditions are satisfied for all $x, y, z \in P$:

(1) $x \leq x$ (Reflexivity).

(2) If $x \leq y$ and $y \leq x$, then $x = y$ (Antisymmetry).

(3) If $x \leq y$ and $y \leq z$, then $x \leq z$ (Transitivity).

An element x of a partially ordered set P is called a **lower bound** for a subset S of P if $x \leq s$ for all $s \in S$. The element x is a **greatest lower bound** of S if x is a lower bound of S and $y \leq x$ for all lower bound y of S. Similar definitions apply to a **upper bound** and a **least upper bound**. By (2), a greatest lower bound and a least upper bound of S are unique respectively

if they are exist.

A lattice is a partially ordered set in which every pair of elements has a least upper bound and a greatest lower bound. The following theorem is well-known.

Theorem 3.1. Let $(L, \leq)$ be a lattice and de¯ne the operations $\wedge$ and $\vee$ on L by $x \wedge y :=$ the greatest lower bound of x, y and $x \vee y :=$ the least upper bound of x, y. Then the following properties hold for all $x, y, z \in L$.

(1) $x \wedge y = y \wedge x$ and $x \vee y = y \vee x$ (Commutativity).

(2) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ and $(x \vee y) \vee z = x \vee (y \vee z)$ (Associativity).

(3) $x \wedge (x \vee y) = x$ and $x \vee (x \wedge y) = x$ (Absorption identities).

(4) $x = x \wedge y$ if and only if $x \leq y$ if and only if $y = x \vee y$.

Let G be a group, and let $L(G)$ be the set of all subgroups of G. Then $L(G)$ is partially ordered with respect to subgroup inclusion $\leq$. Moreover, for each subgroups X and Y of G, the intersection $X \cap Y$ is the greatest lower bound of X and Y, and the join $\langle X, Y \rangle$ is the least upper bound of X and Y. Therefore, $L(G)$ is a lattice, which is called the subgroup lattice of G.

Let L and L^{0} be lattices. A bijective map $\sigma : L \longrightarrow L^{0}$ is called an isomorphism from L onto L^{0} if

$$(*) \qquad (x \wedge y)\sigma = x\sigma \wedge y\sigma \quad \text{and} \quad (x \vee y)\sigma = x\sigma \vee y\sigma$$

for all $x, y \in L$. It is of course that the inverse map of an isomorphism from

a lattice L onto L^0 is an isomorphism from L^0 onto L. If there exists an isomorphism from L onto L^0, then L is called isomorphic to L^0, and denote by $L \cong L^0$.

If G and H are groups, an isomorphism from $L(G)$ onto $L(H)$ is called a projectivity from G onto H. We also say that G and H are lattice-isomorphic if there exists a projectivity from G onto H.

In order to show that a bijective map between two lattices is an isomorphism, it suffices to prove that it has one of the two properties in $(*)$ or that it preserves the order relations of the lattices.

Theorem 3.2. Let σ be a bijective map of a lattice L to a lattice L^0. Then the following properties are equivalent.

(1) For all $x, y \in L$, $x \leq y$ if and only if $x\sigma \leq y\sigma$.

(2) $(x \wedge y)\sigma = x\sigma \wedge y\sigma$ for all $x, y \in L$.

(3) $(x \vee y)\sigma = x\sigma \vee y\sigma$ for all $x, y \in L$.

A subset of a lattice L is called a sublattice of L if it is closed with respect to the operations $\wedge$ and $\vee$. It is obvious that a sublattice is a lattice relative to the induced operations. If $x \leq y$, the interval

$$[y/x] = \{z \in L \mid x \leq z \leq y\}$$

is a sublattice of L.

For projectivities, it is often possible to work with maps between elements.

Let G and H be groups. A bijective map $\sigma : G \longrightarrow H$ such that

$$X \leq G \quad \text{if and only if} \quad X\sigma \leq H$$

for all subset X of G, is called a subgroup-preserving bijective map. A subgroup-preserving bijective map induces a projectivity from G onto H. Of course, the projectivity of groups induced by a subgroup-preserving bijective map between the groups preserves the order of each subgroup.

An isomorphism σ from a group G onto a group H is a subgroup-preserving bijective map, and so induces a projectivity from G onto H. However, it is not true in general that a projectivity from G onto H is induced by an isomorphism from G onto H: for example, for prime numbers p and q, there exists a projectivity from the cyclic group of order p onto the cyclic group of order q. The following result on projectivity of finite cyclic groups was given in [1].

Theorem 3.3. Let $p_1, ..., p_k$ be di®erent primes and let G be a cyclic group of order $p_1^{n_1} \cdots p_k^{n_k}$ and let H be a group. Then $L(G) \cong L(H)$ if and only if H is a cyclic group of order $q_1^{n_1} \cdots q_k^{n_k}$ where $q_1, ..., q_k$ are di®erent primes.

Then we have the following immediate consequences.

Corollary 3.4. Let P be ¯nite cyclic p-groups for a prime p and let Q be a p-group . Then $L(P) \cong L(Q)$ if and only if $P \cong Q$.

Corollary 3.5. Let P and Q be ¯nite p-groups for a prime p. If a map $\sigma : L(P) \longrightarrow L(Q)$ is a projectivity, then $S\sigma \cong S$ for each cyclic subgroup

S of P.

Many abelian groups can admit projectivities onto nonabelian groups.

The following result, which is from a result given by Baer [2], is crucial for our purpose.

Theorem 3.6. If P is a ¯nite metacyclic p-group for an odd prime p, then there exists an abelian p-group A and a subgroup-preserving bijective map from A onto P that induces a projectivity from A onto P.

4 Metacyclic groups and presentations

A **metacyclic** group is a finite group G which has a cyclic normal subgroup K such that G/K is also cyclic. A factorization $G = SK$ is called a **metacyclic factorization** if S is a cyclic subgroup and K is a cyclic normal subgroup of G; every metacyclic group has always a metacyclic factorization. Then S and K are called the **supplement** and the **kernel** of the metacyclic factorization, respectively. In particular, if $S \cap K = 1$, the metacyclic factorization is called **split**. A metacyclic group is called **split** if it has a split metacyclic factorization.

Metacyclic groups are, of course, soluble; in fact, supersoluble.

We here give some basic properties of metacyclic groups; some of them are well-known and others seem to be folklore.

Lemma 4.1. Let G be a metacyclic group with a metacyclic factorization $G = SK$. Let $S = \langle x \rangle$, $K = \langle y \rangle$. Let r be an integer such

that $y^x = y^r$. Define s to be the multiplicative order of r in $U_{|K|}$ and $t := |K|/\gcd(|K|, r-1)$. Then

(i) $G^{(0)} = \langle y^{r-1} \rangle$; so $|G^{(0)}| = t$;

(ii) $Z(G) = C_S(K)C_K(S) = \langle x^s, y^t \rangle$.

Proof. For (i), see [6, (47.10)]; for (ii), see [4, Lemma IV.2.13]. □

Let G be a metacyclic group with kernel K; we can assume that

$$K = \langle y \rangle \cong Z_n,\ G/K = \langle xK \rangle \cong Z_m,$$

with $x, y \in G$, m, n positive integers. Since K is a normal subgroup of index m, both $x^{-1}yx$ and x^m must belong to K, say

$$x^{-1}yx = y^r,\ x^m = y^s,$$

where r, s are integers with $1 \leq r, s \leq n$. Now it follows that for integers a, b with $a \geq 0$,

$$x^{-a}y^b x^a = y^{br^a},$$

so that

$$y = y^{-s}yy^s = x^{-m}yx^m = y^{r^m},$$

whence, $r^m \equiv 1 \bmod n$, since $|y| = |K| = n$. Similarly, we have

$$y^s = x^m = x^{-1}x^m y = x^{-1}y^s y = y^{rs},$$

so that $rs \equiv s \bmod n$. We then have the following fundamental theorem.

Theorem 4.2. Consider the group

$$G = \langle\, x, y \,|\, x^m = y^s,\ y^n = 1,\ x^{-1}yx = y^r \,\rangle,$$

where m, n, r, s are integers and $r, s \leq n$, and $r^m \equiv 1,\ rs \equiv s \bmod n$. Then $K = \langle\, y \,\rangle$ is a normal subgroup of G such that $K \cong Z_n,\ G/K \cong Z_m$. Thus G is a finite metacyclic group and moreover, every finite metacyclic group has a presentation of this form.

For the proof of the above theorem, see [7, p. 21].

5 Classification of metacyclic p-groups

We begin with an observation about subgroups of direct product of finite cyclic groups.

Let $G = H \times K$ be the direct product of two finite cyclic groups H and K, let η and κ be the projection onto the factors H and K, respectively. We regard H and K as subgroups of G. Then we have the following lemma.

Lemma 5.1. Let U be a subgroup of G.

(1) The map $\theta_U : u\eta \longrightarrow u\kappa(U \cap K)$ defines a homomorphism from $U\eta$ onto $U\kappa/(U \cap K)$ with kernel $U \cap H$.

(2) For each $V \leq H,\ W \leq K$ and a homomorphism θ from V to K/W,

$$U = \{hk | h \in V,\ k \in h\theta\}$$

is a subgroup of G with $U\eta = V,\ U\kappa = V\theta,\ W = U \cap K,\ \ker(\theta) = U \cap H$ and $\theta_{\mathsf{U}} = \theta$.

Proof. (1) We denote θ_{U} simply by θ. Let $u_1, u_2 \in U$. It follows from $((u_1\eta)(u_2\eta))\theta = ((u_1u_2)\eta)\theta = (u_1u_2)\kappa(U \cap K) = (u_1\kappa)(u_2\kappa)(U \cap K) = (u_1\eta)\theta\ (u_2\eta)\theta$ that θ is a homomorphism from $U\eta$ onto $U\kappa/(U \cap K)$. Let $u\eta \in \ker(\theta)$. $u\kappa \in U \cap K$. So $u\eta = u(u\kappa)^{\mathsf{i}\,1} \in U \cap H$. Thus $\ker(\theta) \leq U \cap H$. Conversely, if $u\eta \in U \cap H$ then $u\kappa = (u\eta)^{\mathsf{i}\,1}u \in U \cap K$ and so $u\kappa \in U \cap K$; this implies that $U \cap H \leq \ker(\theta)$. Therefore, $U \cap H = \ker(\theta)$.

(2) To show that U is a subgroup of $G = H \times K$, let $h_1, h_2 \in V$ such that $h_1\theta = k_1W$ and $h_2\theta = k_2W$. Then $h_1h_2^{\mathsf{j}\,1}\theta = h_1\theta(h_2\theta)^{\mathsf{i}\,1} = k_1k_2^{\mathsf{j}\,1}W$, and hence $(h_1k_1)(h_2k_2)^{\mathsf{i}\,1} = h_1h_2^{\mathsf{j}\,1}k_1k_2^{\mathsf{j}\,1} \in U$. Therefore U is a subgroup of G. Clearly, we have $U\eta = V$ and $U\kappa = V\theta$. An element of $U \cap H$ is h such that $h\theta = W$. Since θ is a homomorphism from V onto $U\kappa/W$ the element h must belong to $\ker(\theta)$. Conversely, if $h \in \ker(\theta)$, then $1 \in W = h\theta$ and so $h \in U$. Thus, we have $U \cap H = \ker(\theta)$; similarly, $U \cap K = W$. Then, the definitions give us $\theta_{\mathsf{U}} = \theta$. □

Let U be a subgroup of the direct product two finite cyclic p-groups H and K. We regard H and K as subgroups of $H \times K$. Denote

$$H_1 := H \cap UK,\ H_2 := H \cap U,\ K_1 := HU \cap K,\ K_2 = U \cap K.$$

It is easy to show that

$$H_1 = U\eta,\ K_1 = U\kappa.$$

We also have

$$H_1K_1 = H_1U = UK_1$$

by applying Lemma 2.4.

We then have:

Lemma 5.2. (1) U is cyclic if and only if $H_2 = 1$ or $K_2 = 1$.

(2) $(H \times K)/U$ is cyclic if and only if $H_1 = H$ or $K_1 = K$.

Proof. (1) Since both of H_2 and K_2 are contained in U, one of them must be trivial if U is cyclic. On the other hand, we know $H_1K_1 = H_1U = UK_1$ and $H_1 \cap U \leq H_2$, $U \cap K_1 \leq K_2$. It follows that $H_2 = 1$ implies that $U \cong K_1$, and $K_2 = 1$ implies $U \cong H_1$. Consequently, U is cyclic if and only if $H_2 = 1$ or $K_2 = 1$.

(2) Suppose that $H_1 = H$. Then $H \cap UK = H$, and so $H \leq UK$. Thus $UK = HK$. It follows that $HK/U = UK/U \cong K/(U \cap K)$ is cyclic. Similarly, $K_1 = K$ yields that HK/U is cyclic. Conversely, suppose that HK/U is cyclic. Since

$$H/H_1 \times K/K_2 \cong HK/H_1K_1 = HK/H_1U$$

is a homomorphic image of HK/U, $H/H_1 \times K/K_2$ is a cyclic p-group. It follows that either $H = H_1$ or $K = K_1$. □

We state an immediate consequence of the above lemma.

Corollary 5.3. Suppose that $|H| \geq |K|$. Then U and $(H \times K)/U$ are cyclic if and only if (i) $H_2 = 1, K_1 = K, K_2 \neq 1,$ or (ii) $H_1 = H, K_2 = 1, K_1 \neq K,$

or (iii) $K_1 = K, K_2 = 1$.

Now we have a consequence of Theorem 3.6.

Lemma 5.4. *Let P be a finite metacyclic p-group for an odd prime p. Then P has a projectivity from a direct product of two cyclic p-groups onto P which is induced by a subgroup-preserving bijective map.*

Proof. From Theorem 3.6, there exists an abelian p-group A and a subgroup-preserving bijective map τ from A onto P, which induces a projectivity from A onto P. The inverse τ^{-1} of τ is obviously a subgroup-preserving bijective map from P onto A. Let $P = SK$ be a metacyclic factorization of P. Then $A = S\tau^{-1}K\tau^{-1}$ by regarding τ^{-1} as the induced projectivity from P onto A. By Corollary 3.5, we see that $S\tau^{-1}$ and $K\tau^{-1}$ is cyclic p-group. This implies that A is a direct product of two cyclic p-groups. □

We need the following lemma.

Lemma 5.5. *Let A be a finite abelian p-group and let $X = \langle x \rangle$ be a cyclic subgroup with $|X| = \exp(A)$. Let Y be a subgroup of A maximal subject to $X \cap Y = 1$. Then A is a direct product of X and Y.*

Proof. Suppose that $XY \neq A$. Then there exists $a \in A \setminus XY$ but $a^p \in XY$. So $a^p = hk$ for some $h \in X, k \in Y$. Assume that $h = x^i$ for some integer such that $\gcd(i, p) = 1$. Then $|a^p| = (|\langle x^i \rangle||\langle k \rangle|)/\gcd(|\langle x^i \rangle|, |\langle k \rangle|) \geq \exp(A)$. Therefore $|\langle a \rangle| \geq p \cdot \exp(A)$, a contradiction. Thus $h = h_1^p$ for some $h_1 \in X$. Thus $a^p = h_1^p k$. Let $\bar{a} = ah_1^{-1}$. Then $\bar{a}^p \in Y$. If $\bar{a} \notin Y$, then there exists

$h_2 \in \langle\, \bar{a}, Y \,\rangle \cap X \neq 1$. Then $h_2 = \bar{a}^r k_1$ for some r not divisible by p and for some k_1 in Y. Thus $\bar{a} \in XY$ and so $a \in XY$. This yields a contradiction. So $A = XY$. Since $X \cap Y = 1$, $A = XY$ is direct. □

The following lemma is crucial for our purpose.

Lemma 5.6. Let P be a finite metacyclic p-group for an odd prime p. If K is a cyclic normal subgroup of P such that P/K is cyclic, then there exists a cyclic subgroup S of P such that $P = SK$ and $|S| = \exp(P)$.

Proof. Since P/K is cyclic, it follows that K contains P^0. Let $\tau : A \longrightarrow P$ be a subgroup-preserving bijective map from a direct product A of two cyclic p-groups onto P, which is given in Lemma 5.4. By Lemma 5.5, $A = X \times Y$ for some cyclic subgroup X and Y with $|X| = \exp(P)$. Let $U = K\tau^{-1}$. Then U is cyclic by Corollary 3.5. Suppose that $Y_1 := XU \cap Y$ is Y. Then $XU = XY$. We define $S := X\tau$. Then S is cyclic by Corollary 3.5, and $P = SK$ because $SK = X\tau U\tau = (XU)\tau = (XY)\tau = P$. Since $|S| = |X| = \exp(P)$, we have done for this case. Now we suppose that $Y_1 \neq Y$. Since τ induces a projectivity from the sublattice $[A/U] \cong L(A/U)$ onto the sublattice $[P/K] \cong L(P/K)$, A/U is cyclic. Thus $X_1 := X \cap UY$ is equal to X and $Y_2 := U \cap Y$ is trivial from Lemma 5.2. Choose a homomorphism θ from X onto Y. We denote the kernel of θ by X_0. We now define V to be the set $\{xy \,|\, x\theta = y,\ x \in X\}$. It follows from Lemma 5.1 that V is a subgroup of A

and

$$X \cap VY = X,\ XV \cap Y = Y,\ X \cap V = X_0, V \cap Y = 1,\ |S| = |X| = \exp(P).$$

We observe that V is cyclic from Lemma 5.2 since $V \cap Y = 1$. On the other hand, $X_2 := X \cap U$ contains X_0 properly since $Y_1 \neq Y$. Thus $X_0 = V \cap X_2 = V \cap U \cap X = U \cap V$. Let $S := V\tau$ Then

$$|SK| = |VU| = |V||U|/|V \cap U| = |X||X|/|X_0| = |X||Y| = |P|,$$

and so we have $P = SK$. □

We are now in a position to give our classification theorem.

Theorem 5.7. (1) Every noncyclic metacyclic p-group P for an odd prime p has a presentation of the form:

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

where $\alpha, \beta, \gamma, \delta$ are nonnegative integers such that $\alpha \geq \beta \geq \gamma \geq \delta,\ \gamma \geq 1$.

(2) Each such a presentation defines a metacyclic p-group of order $p^{\alpha+\beta+\gamma+\delta}$; different values of the parameters $\alpha, \beta, \gamma, \delta$ with the above condition give non-isomorphic metacyclic p-groups.

Proof. Choose a metacyclic factorization $P = SK$ so that $|S| = \exp(P)$ and K is of the least order among possible choices; this is always possible by Lemma 5.6. Let x, y be generators of S, K, respectively. Then $|\langle x \rangle| = p^{\alpha+\delta},\ |\langle y \rangle| = p^{\beta+\gamma},\ |S \cap K| = p^\delta,\ |P^{p^\beta}| = p^{\beta+\delta}$, for some nonnegative integers $\alpha, \beta, \gamma, \delta$. It follows that $x^{p^\alpha} = y^{sp^\beta},\ y^{p^{\beta+\gamma}} = 1,\ y^x = y^r$ for

some nonnegative integer r and nonnegative integer s relatively prime to p. By Lemma 4.1(i), $r = 1 + tp^{\circ}$ for some nonnegative integer t relatively prime to p since $|P^{0}| = p^{-+\pm i^{\circ}}$. By Lemma 2.3, there exists a positive integer t^{0} such that $(1 + tp^{\circ})^{t^{0}} = 1 + p^{\circ}$. Let $a := x^{t^{0}}$ and $b := y^{st^{0}}$. It follows that $a^{p^{\circledR}} = b^{p^{-}}$, $b^{p^{-+\pm}} = 1$, $b^{a} = b^{1+p^{\circ}}$.

We want to show that $S \cap K \leq P^{0}$. If P is abelian, $S \cap K = 1$ from Lemma 5.5 and the choice of K; so the result is obvious. We assume that P is nonabelian. Suppose that $P^{0} < S \cap K$. Let $\tau : A \longrightarrow P$ be a subgroup-preserving bijective map from a direct product A of two cyclic p-groups onto P, which is given in Lemma 5.4. Let $X := S\tau^{i1}$, $Q := P^{0}\tau^{i1}$; note that these subgroups are all cyclic. Then, by Lemma 5.5, there exists a cyclic subgroup Y such that $A = XY$ and $X \cap Y = 1$. Let T be the subgroup of X such that $T/Q \cong Y$ and let $\theta : T \longrightarrow Y$ be the natural subjective homomorphism with $\ker(\theta) = Q$. Define $U := \{ab \,|\, a\theta = b,\ a \in T,\ b \in Y\}$. Then $U \leq A$ and $X \cap UY = T$, $XU \cap Y = Y$, $X \cap U = Q$, $U \cap Y = 1$. Thus U and A/U are cyclic by Corollary 5.3. It follows that $U\tau$ contains $Q\tau = P^{0}$, and $U\tau$ and $P/U\tau$ are cyclic by Corollary 3.5. Since $|U\tau| > |K|$, we have a contradiction to the choice of K. So we have proved $S \cap K \leq P^{0}$. This yields that $\beta \geq \gamma$. Since $b^{p^{-}} = b^{p^{-}(1+p^{\circ})}$, we have $p^{-+\circ} = 0 \bmod p^{-+\pm}$, that is $\gamma \geq \delta$. If $\beta = 0$, the P must be cyclic; this is not the case. So $\beta > 0$; thus P is not cyclic. We note that $P/\Phi(P) \cong \mathbb{Z}_{p} \times \mathbb{Z}_{p}$. So $\Phi(P) \geq P^{0}$ but $\Phi(P)$ does not contain K since P/K is cyclic, and so P^{0} is a proper subgroup of K. Therefore,

$\gamma \geq 1$.

Consequentely, we have the presentation

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

where $\alpha, \beta, \gamma, \delta$ are nonnegative integers such that $\alpha \geq \beta \geq \gamma \geq \delta,\ \gamma \geq 1$. By Theorem 4.2, the presentation defines a metacyclic group of order $p^{\alpha+\beta+\gamma}$, and so P is isomorphic with the group defined by the presentation. Further, we observe $P/P^{0} \cong Z_{p^{\alpha}} \times Z_{p^{\delta}}$ and $\exp(P) = p^{\alpha+\gamma}$. It follows that α, β, γ and δ are invariants of P. □

References

[1] Reinhold Baer, `The signi¯cance of the system of subgroups for the structure of the group', Amer. J. Math. 61 (1939), 1-44.

[2] Reinhold Baer, `Crossed isomorphisms', Amer. J. Math. 66 (1944), 341-404.

[3] F. R. Beyl, The classic¯cation of metacyclic p-groups, PhD thesis (Cornell University, 1972).

[4] F. R. Beyl and J. Tappe, Group Extensions, Representations, and the Schur Multiplicator, Lecture Notes in Math., 958, Splinger-Verlag (1982).

[5] H. S. M. Coxeter and W. O. J. Moser, Generators and Relations for Discrete Groups, Springer-Verlag (1972).

[6] C. W. Curtis and I. Reiner, Representation Theory of Finite Groups Associative Algebras, Pure and Appl. Math. 11, Interscience, New York (1962).

[7] D. L. Johnson, Topics in the Theory of Group Presentations, London Math. Soc. Lecture Note Ser. 42, Cambridge University Press (1980).

[8] Bruce W. King, `Presentations of metacyclic groups', Bull. Austral. Math. Soc., 8 (1973), 103-131.

[9] Wolfgang Lindenberg, `Über die Struktur zerfallender bizyklischer p-Gruppen', J. Reine Angew. 241 (1970), 118-146.

[10] Wolfgang Lindenberg, `Struktur und Klassi¯zierung bizyklischer p-Gruppen', Gesellschaft für Mathematik und Datenverarbeitung 40 (1971).

[11] Ian D. Macdonald, The Theory of Groups, Oxford University Press (1968).

[12] R. Schmidt, Subgroup Lattices of Groups, Walter de Gruyter (1994).

[13] Hyo-Seob Sim, Metacyclic Groups of Odd Order, PhD thesis (Australian National University, 1992).

[14] Michio Suzuki, Group Theory I, Springer-Verlag (1982).