The Structure of Subgroups of Metacyclic p-Groups

메타순환 p-군의 부분군의 구조

Advisor : Hyo-Seob Sim

by

Eunjeong 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 2003

The Structure of Subgroups of
Metacyclic p-Groups

A Dissertation

by

Eunjeong Lee

Approved as to style and content by :

Young-Gheel Baik, Ph. D.

Hyun-Jong Song, Ph. D.

Hyo-Seob Sim, Ph. D.

June 21, 2003

Contents

메터순환 p-군의 부분군의 구조

이 은 정

부경대학교 교육대학원 수학교육전공

요 약

정규순환부분군(cyclic normal subgroup) K가 존재하여 그 상군 G/K가 순환군(cyclic group)이 되는 군(group) G를 메터순환군(metacyclic group)이라 부른다. 메터순환군은 가해군(soluble group)의 기본적인 형태로서 여러 학자들의 주목을 받아온 중요한 군의 일종이다.

군 이론의 연구는 때때로 그 부분군들의 구조를 통하여 이루어진다. 본 논문의 주요 목적은 유한 메터순환 p-군의 부분군의 구조를 조사하는 데 있다. 본 논문에서는 두 순환(cyclic) p-군의 곱(direct product)의 모든 부분군을 구체적으로 결정하고, 대응하는 가환군의 부분군의 구조와의 관계를 통하여 유한 메터순환 p-군의 부분군의 구조를 구체적으로 연구하였다.

1 Introduction

Let G be a group. If G has a cyclic normal subgroup K such that G/K is also cyclic, then G is called a *metacyclic group*. If G is a metacyclic group and 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 $G = SK$. Every subgroup and quotient group of a metacyclic group are also metacyclic. Some special classes of metacyclic groups can be found in [3] and Chapter 1 of Coxeter and Moser [4]. As a special subfamily of soluble groups, metacyclic groups have been received considerable attention by many authors.

Various classifications for metacyclic groups of prime power order (simply metacyclic p-groups) may be found in [6, 7], [3], [5] and [9]. 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.

Understanding of the subgroup structures of finite groups is often very useful in the study of finite groups. In this thesis, we investigate the structure of subgroup lattice of finite metacyclic p-groups for odd prime p. The main purpose of this thesis is to give an explicit description of the structure of subgroup lattices of metacyclic p-groups for odd prime p.

First of all, we will consider the subgroups of the direct product of two cyclic p-groups; we will explicitly determine all subgroups of the direct product of two cyclic p-groups. A lattice isomorphism from 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 certain family of finite p-group has a projectivity from some abelian p-groups. We will give an elucidation of this for finite metacyclic p-groups for odd prime p. For this purpose, we will use the following classification of metacyclic p-groups for odd prime p given by Sim [9].

Theorem 1.1. (1) *Every noncyclic metacyclic p-group P for an odd prime p has a presentation of the form:*

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

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 $p^{\alpha+\beta+\delta}$; different 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 throughout this thesis. 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 group. The automorphism group of the group G is denoted by $\mathrm{Aut}(G)$. For a subgroup H of G, the centralizer of H in G is the subgroup consisting of those elements x such that $xh = hx$ for all h in H, and denoted by $\mathbf{C}_G(H)$. Let $\mathrm{Iso}(X, Y)$ denotes the set of all isomorphisms from X onto Y for groups X and Y.

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

Lemma 2.1. *Let A, B and C be any subgroups of a group such that $A \leq B$. Then $A(B \cap C) = B \cap AC$.*

We observe some useful arithmetic facts.

Lemma 2.2. *Let p be an odd prime. Then for each integer i with $i \geq 2$, if p^m divides $i \cdot (i-1) \cdots 2 \cdot 1$ then $m \leq i - 2$.*

Proof. Assume that $i = p^t$ for some integer t, then $m \leq \frac{t(t-1)(p-1)}{2} + t$. By using mathematical induction on the number t, we see that $\frac{t(t+1)(p-1)}{2} < p^t$. Since

$$\frac{t(t+1)(p-1)}{2} = \frac{t(t-1)(p-1)}{2} + t(p-1) > \frac{t(t-1)(p-1)}{2} + t,$$

it follows that $m < \frac{t(t+1)(p-1)}{2} < p^t = i$. Therefore $m \leq i - 2$.

Suppose that $p^t < i < p^{t+1}$. Then $m \leq \frac{t(t+1)(p-1)}{2} < p^t < i$. Thus $m \leq i-2$. □

Lemma 2.3. *Let p be an odd prime. If $\gcd(t,p)=1$, then*

$$(1+tp^s)^k \equiv 1 \bmod p^m \text{ if and only if } p^m \text{ divides } kp^s.$$

Proof. By Binomial Theorem,

$$(1+tp^s)^k = 1 + ktp^s + kp^s \cdot \sum_{i=2}^{k} \frac{(k-1)\cdots(k-i+1)t^i p^{s(i-1)}}{i!}.$$

It follows from Lemma 2.2 that p divides $\frac{(k-1)\cdots(k-i+1)t^i p^{s(i-1)}}{i!}$ for $i \geq 2$. Hence $(1+tp^s)^k = 1 + kp^s(t+t'p)$ where t' is positive integer. If $(1+tp^s)^k \equiv 1 \bmod p^m$, then p^m divides $kp^s(t+t'p)$. And since $\gcd(t,p)=1$, p^m divides kp^s.

Suppose that p^m divides kp^s. It follows from $(1+tp^s)^k = 1+kp^s(t+t'p)$ that $(1+tp^s)^k \equiv 1 \bmod p^m$. □

Lemma 2.4. *Let p be an odd prime. If $r^{p^k} \equiv 1 \bmod p^m$ then*

$$1 + r + r^2 + \cdots + r^{p^k-1} \equiv p^k \bmod p^m.$$

Proof. If $r \equiv 1 \bmod p^n$, then the result is clear,

Assume that $r \not\equiv 1 \bmod p^m$. Since $k \geq 1$, by Fermat's Theorem $r^{p^k} \equiv r \bmod p$ and hence $r \equiv 1 \bmod p$. So $r \equiv 1 + sp^{m-j} \bmod p^m$ where $1 \leq j < m$, $\gcd(s,p)=1$, Then since $r^{p^k} \equiv (1+sp^{m-j})^{p^k}$, by Lemma 2.3 p^j

divides p^k and so $j \leq k$. Then from Binomial Theorem,

$$\frac{r^{p^k}-1}{r-1} \equiv p^k + p^{m-j+k} \cdot \sum_{i=2}^{k} \frac{(p^k-1)\cdots(p^k-i+1)s^{i-1}(p^{m-j})^{i-2}}{i!}.$$

Since $m-j \geq 1$, we have $\frac{r^{p^k}-1}{r-1} \equiv p^k \bmod p^m$ by Lemma 2.2. □

Lemma 2.5. *Let p be an odd prime and m, n integers such that $n < m$. Define $e := 1 + p^{m-n}$ and define $\sigma(k) := 1 + e + e^2 + \cdots + e^{k-1}$. Then*

(1) $\sigma(i+j) = \sigma(i) + e^i \sigma(j)$.

(2) *the induced map* $\sigma : \{1, 2, 3, ..., p^n\} \longrightarrow \mathbb{Z}_{p^n}$ *is bijective.*

Proof. (1) $\sigma(i+j) = 1 + e + \cdots + e^{i-1} + e^i + \cdots + e^{i+j-1} = \sigma(i) + e^i\sigma(j)$.

(2) To prove that σ is bijective, it suffices to show that σ is injective. Since $\sigma(j) = \sigma(i) + e^i\sigma(j-i)$ from (1) and since p does not divide e^i, if $\sigma(i) = \sigma(j)$ in $\mathbb{Z}_{p^n}$ for $1 \leq i < j \leq p^n$ then $\sigma(j-i) = 0$ in $\mathbb{Z}_{p^n}$. By Lemma 2.3, if $\sigma(k) = 0$ for k such that $1 \leq k \leq p^n$, then $k = p^n$. Since $1 \leq j - i < p^n$, this yields a contradiction. Thus σ is injective. □

We finally give some investigation about the automorphism groups of finite cyclic groups.

Let $\mathbb{Z}_n$ denote the additive group of integers modulo n for a positive integer n. The set U_n of integers m modulo n which are relatively prime to n forms an abelian group under multiplication modulio 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 2.6. *The automorphism group* $\mathrm{Aut}(\mathbb{Z}_n)$ *is isomorphic to* U_n.

The structure of U_n is well-known. We here just state the special case when n is a power of an odd prime number.

Theorem 2.7. *If* p *is an odd prime, then* U_{p^α} *is the cyclic group of order* $(p-1)p^{\alpha-1}$.

3 Subgroup lattices of groups

In this section we give a brief introduction of the basic concepts of lattice theory; the presentation is based on [8].

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.

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' be lattices. A bijective map $\sigma : L \longrightarrow L'$ is called an *isomorphism* from L onto L' if

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

for all $x, y \in L$. It is of course that the inverse map of an isomorphism from a lattice L onto L' is an isomorphism from L' onto L. If there exists an isomorphism from L onto L', then L is called *isomorphic* to L', and denote by $L \cong L'$.

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.

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

$$S \leq G \quad \text{if and only if} \quad \sigma(S) \leq H$$

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

4 Subgroups of direct product of cyclic groups

Let $G = HK$ be the direct product of two cyclic subgroups H and K of G, let η and κ be the projection of G onto the factors H and K, respectively. Then we have the following lemma.

Lemma 4.1. *Let C be a subgroup of G. Then $A_1 = \eta(C)$, $A_2 = H \cap C$, $B_1 = \kappa(C)$, $B_2 = K \cap C$ if and only if $A_1C = A_1B_1 = B_1C$, $A_1 \cap C = A_2$, $B_1 \cap C = B_2$.*

Proof. Let $A_1 = \eta(C)$, $A_2 = H \cap C$, $B_1 = \kappa(C)$ and $B_2 = K \cap C$. We want to show that $A_1C = A_1B_1 = CB_1$. If $h \in A_1, k \in B_1$ then $ak \in C$ for some $a \in A_1$, it follows that $hk = ha^{-1}(ak) \in A_1C$. Thus A_1B_1 is contained in A_1C. If $h \in A_1$ and $c \in C$ with $c = ab$ for some $a \in A_1$ and $b \in B_1$ then $hc = hab = (ha)b \in A_1B_1$. Thus A_1C is contained in A_1B_1. Consequently $A_1C = A_1B_1$.

Similarly, $B_1C = A_1B_1$. Therefore $A_1C = A_1B_1 = CB_1$. On the other hand $A_2 = H \cap C = \eta(C) \cap C = A_1 \cap C$ and $B_2 = K \cap C = \kappa(C) \cap C = B_1 \cap C$.

For the converse, suppose that $A_1C = A_1B_1 = CB_1$, $A_1 \cap C = A_2$, $B_1 \cap C = B_2$ then $\eta(C) = \eta(CB_1) = \eta(A_1B_1) = A_1$, $\kappa(C) = \kappa(A_1C) = \kappa(A_1B_1) = B_1$, $H \cap C = H \cap A_1C \cap C = H \cap A_1B_1 \cap C = A_1 \cap C = A_2$ and $K \cap C = K \cap CB_1 \cap C = K \cap A_1B_1 \cap C = B_1 \cap C = B_2$. □

Lemma 4.2. *For each $\theta \in \mathrm{Iso}(H, K)$, $C := \{a \cdot \theta(a) : a \in H\}$ is a subgroup of G such that $HC = KC = G$, $H \cap C = K \cap C = 1$.*

Proof. Let $C = \{a \cdot \theta(a) : a \in H\}$. For every $x = a \cdot \theta(a)$, $y = b \cdot \theta(b) \in C$ and $a, b \in H$,

$$xy^{-1} = (a \cdot \theta(a))(b \cdot \theta(b))^{-1} = (ab^{-1}) \cdot (\theta(a)\theta(b)^{-1}) = (ab^{-1}) \cdot \theta(ab^{-1}) \in C.$$

Thus C is a subgroup of G. It is clear that $HC = KC = G, H \cap C = K \cap C = 1$.

□

Lemma 4.3. *If $\Omega = \{C : HC = KC = G, H \cap C = K \cap C = 1\}$ then there exists a bijective map $\Phi : \Omega \longrightarrow \mathrm{Iso}(H, K)$.*

Proof. For every $C \in \Omega$, there is the restriction of η to C, denoted by $\eta \downarrow_C$, in the set of all isomorphisms from H to K. Define $\psi_C = (\kappa \downarrow_C)(\eta \downarrow_C)^{-1}$ then $\psi_C \in \mathrm{Iso}(H, K)$. Define $\Phi(C) = \psi_C$. For every $C_1, C_2 \in \Omega$, if C_1 is not equal to C_2 then there exist $x \in H$ and $y \in K$ such that $xy \in C_1$

but $xy \notin C_2$. Since $\eta(C_2) = H$, there exists $z \in K$ such that $xz \in C_2$. Thus y is not equal to z. Then $(\kappa \downarrow_{C_1})(\eta \downarrow_{C_1})^{-1}(x) = (\kappa \downarrow_{C_1})(xy) = y$ and $(\kappa \downarrow_{C_2})(\eta \downarrow_{C_2})^{-1}(x) = (\kappa \downarrow_{C_2})(xz) = z$. Since y is not equal to z, ψ_{C_1} is not equal to ψ_{C_2} i.e. $\Phi(C_1) \neq \Phi(C_2)$. And so Φ is injective. Define $C = \{a \cdot \theta(a) \, : \, a \in H\}$ for all $\theta \in \text{Iso}(H, K)$ then $\Phi(C) = \psi_c = \theta$. Since C is an element of Ω by Lemma 4.2, Φ is surjective. We have shown that Φ is bijective. □

Let $\mathcal{S}$ be a set of all the subgroups of G and let

$$\mathcal{J} = \{(A_1, A_2, B_1, B_2) \, : \, A_2 \trianglelefteq A_1 \leq H, \ B_2 \trianglelefteq B_1 \leq K, \ A_1/A_2 \cong B_1/B_2\}.$$

Define the map $\Phi : \mathcal{S} \longrightarrow \mathcal{J}$ by $\Phi(C) = (\eta(C), H \cap K, \kappa(C), K \cap C)$. Then $\Phi(C)$ is an elment of $\mathcal{J}$ for all $C \in \mathcal{S}$. Suppose that $(A_1, A_2, B_1, B_2) \in \mathcal{J}$. Then $\text{Iso}(A_1/A_2, B_1/B_2)$ is not empty. Let

$$X = A_1B_2/A_2B_2, \ Y = A_2B_1/A_2B_2, \ Z = A_1B_1/A_2B_2.$$

Since $A_1/A_2 \cong X$ and $B_1/B_2 \cong Y$, $\text{Iso}(X, Y)$ is not empty. Then there exists $C \in \mathcal{S}$ such that $X\bar{C} = Z = Y\bar{C}, \ X \cap \bar{C} = Y \cap \bar{C} = 1$ where $\bar{C} = C/A_2B_2$ and then $A_1C = A_1B_1 = B_1C, \ A_1 \cap C = A_2$ and $B_1 \cap C = B_2$. It follows from Lemma 4.1 that

$$A_1 = \eta(C), \ A_2 = H \cap C, \ B_1 = \kappa(C), \ B_2 = K \cap C.$$

Then $\Phi(C) = (\eta(C), H \cap C, \kappa(C), K \cap C) = (A_1, A_2, B_1, B_2) \in \mathcal{J}$ and so we obtain that Φ is surjective.

Define a relation '$\sim$' on by $C_1 \sim C_2$ if and only if $\Phi(C_1) = \Phi(C_2)$ for all $C_1, C_2 \in \mathcal{S}$. Then '$\sim$' is an equivalent relation on $\mathcal{S}$. Let $[C]$ denote the equivalence class containing C for each $C \in \mathcal{S}$.

Put $[\mathcal{S}] = \{[C] : C \in \mathcal{S}\}$. The Φ induces a bijective map $\bar{\Phi}$ from $[\mathcal{S}]$ to $\mathcal{J}$. Suppose that $\Phi(C) = (A_1, A_2, B_1, B_2)$. Then it follows from Lemma 4.1 that

$$[C] = \{C \ : \ A_1C = A_1B_1 = B_1C, \ A_1 \cap C = A_2, \ B_1 \cap C = B_2\}.$$

Since there is a bijective map from $\{\bar{C} \ : \ X\bar{C} = Z = Y\bar{C}, \ X \cap \bar{C} = Y \cap \bar{C} = 1\}$ onto $[C]$, it follows from by Lemma 4.3 that there exists a one-to-one correspondence between $[C]$ and $\mathrm{Iso}(X, Y)$. Since $X \cong A_1/A_2$ and $Y \cong B_1/B_2$, we see that $[C]$ is in one-to-one correspondence with $\mathrm{Iso}(A_1/A_2, B_1/B_2)$.

Let

$$\mathcal{T} = \{(A_1, A_2, B_1, B_2, \theta) \ : \ (A_1, A_2, B_1, B_2) \in \mathcal{J}, \ \theta \in \mathrm{Iso}(A_1/A_2, B_1/B_2)\}.$$

Consequently, we have shown that there exists one-to-one correspondence between $\mathcal{S}$ and $\mathcal{T}$. We state the result more precisely as follows:

Theorem 4.4. *Let Ψ be the map from $\mathcal{T}$ into $\mathcal{S}$ defined by*

$$\Psi(A_1, A_2, B_1, B_2, \theta) = \{xy \ : \ \theta(xA_2) = yB_2, \ x \in A_1\}.$$

Then Ψ is a bijective map from $\mathcal{T}$ onto $\mathcal{S}$.

Let $C = \Psi(A_1, A_2, B_1, B_2, \theta)$. The isomorphism θ induces a homomorphism θ^* from A_1 onto B_1/B_2, which is defined by $\theta^*(x) = \theta(xA_2)$. Then

$$C = \{xy : \theta^*(x) = yB_2,\ x \in A_1\} = \{xy : y \in \theta^*(x),\ x \in A_1\}.$$

Let $C' = \Psi(A_1', A_2', B_1', B_2', \theta')$. Then it is easy to see the following fact.

Remark 4.5. *$C \le C'$ if and only if $A_1 \le A_1'$ and $\theta^*(x) \subset \theta'^*(x)$ for all $x \in A_1$.*

5 Subgroup lattices of $\mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\beta}$

Let $G = \langle a \rangle \times \langle b \rangle$, where $\langle a \rangle \cong \mathbb{Z}_{p^\alpha}$ and $\langle b \rangle \cong \mathbb{Z}_{p^\beta}$. We assume $\alpha \le \beta$.We explicitly determine all subgroups of G. Let

$$\mathcal{T}_i = \{(A_1, A_2, B_1, B_2, \theta) \in \mathcal{T} : |A_1||B_2| = p^i\}$$

for each $i = 0, 1, \dots, \alpha + \beta$. Then $\Psi(\mathcal{T}_i)$ is the set of all subgroups of G of order p^i.

Let $|A_1| = p^k$ for some integer k. Then $0 \le k \le \alpha$ and $k \le i$. Then $|B_2| = p^{i-k}$, and so $A_1 = \langle a^{p^{\alpha-k}} \rangle$, $B_2 = \langle b^{p^{\beta-i+k}} \rangle$.

We first consider the case when $i \le \beta$. For each $j = 0, 1, \dots, p^k - 1$, define

$$C(j,k) = \langle a^{p^{\alpha-k}} b^{jp^{\beta-i}}, b^{p^{\beta-i+k}} \rangle.$$

For each $j = 0, 1, \dots, p^k - 1$, $C(j,k)$ is a subgroup of G of order p^i and so $C(j,k)$ is contained in $\Psi(\mathcal{T}_i)$. From Theorem 4.4 , every subgroup of order p^i

is $C(j,k)$ for some integers j,k such that $0 \le j \le p^k - 1,\ 0 \le k \le \alpha,\ k \le i$. Therefore

$$\Psi(\mathcal{T}_i) = \{C(j,k) \,:\, 0 \le j \le p^k - 1,\ 0 \le k \le i\} \text{ for } i < \alpha,$$

and

$$\Psi(\mathcal{T}_i) = \{C(j,k) \,:\, 0 \le j \le p^k - 1,\ 0 \le k \le \alpha\} \text{ for } i \ge \alpha.$$

Consequently, there exist precisely $1 + p + \cdots + p^i$ subgroups of order p^i if $i < \alpha$, and $1 + p + \cdots + p^\alpha$ subgroups of order p^i if $\alpha \le i \le \beta$.

We then consider the remaining case when $\beta < i$. In this case, $i-\beta \le k \le \alpha$. For each $j = 0, 1, \dots, p^k - 1$, define

$$C'(j,k) = \langle\, a^{p^{\alpha-k}} b^j, b^{p^{\beta-i+k}} \,\rangle.$$

Each $C'(j,k)$ for $j = 0, 1, \dots, p^k - 1$ is a subgroup of G of order p^i. Conversely it follows from Theorem 4.4 that every subgroup of G of order p^i is equal to $C'(j,k)$ for some integers j,k such that $0 \le j \le p^k - 1,\ i-\beta \le k \le \alpha$. Therefore, in this case

$$\Psi(\mathcal{T}_i) = \{C'(j,k) \,:\, 0 \le j \le p^k - 1,\ i - \beta \le k \le \alpha\}.$$

Then

$$\Psi(\mathcal{T}_i) = \{C'(j, k - \beta + i) \,:\, 0 \le j \le p^k - 1, 0 \le k \le \alpha + \beta - i\}.$$

So $|\Psi(\mathcal{T}_i)| = \sum_{k=0}^{\alpha+\beta-i} p^k$. Consequently, there exist exactly $1 + p + \cdots + p^{\alpha+\beta-i}$ subgroups of order p^i in this case .

We now summarize the observation as follows:

Theorem 5.1. *Let* $G = \mathbb{Z}_{p^\alpha} \times \mathbb{Z}_{p^\beta}$.

(1) *If* $i < \alpha$ *then there exist precisely* $1 + p + \cdots + p^i$ *subgroups of order* p^i *and the subgroups can be listed as follows:*

$$\langle\, a^{p^{\alpha-k}} b^{jp^{\beta-i}},\, b^{p^{\beta-i+k}} \,\rangle,\ 0 \le j \le p^k - 1,\ 0 \le k \le \alpha$$

(2) *If* $\alpha \le i \le \beta$ *then there exist precisely* $1 + p + \cdots + p^\alpha$ *subgroups of order* p^i *and the subgroups can be listed as follows:*

$$\langle\, a^{p^{\alpha-k}} b^{jp^{\beta-i}},\, b^{p^{\beta-i+k}} \,\rangle,\ 0 \le j \le p^k - 1,\ 0 \le k \le \alpha$$

(3) *If* $i > \beta$ *then there exist precisely* $1 + p + \cdots + p^{\alpha+\beta-i}$ *subgroups of order* p^i *and the subgroups can be listed as follows:*

$$\langle\, a^{p^{\alpha+\beta-i-k}} b^j,\, b^{p^k} \,\rangle,\ 0 \le j \le p^k - 1,\ 0 \le k \le \alpha + \beta - i$$

Now we shall draw the subgroup lattices of the special groups G for

$$G = \mathbb{Z}_p \times \mathbb{Z}_p,\ \mathbb{Z}_p \times \mathbb{Z}_{p^2},\ \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}.$$

(1) The subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$

Let $H = \langle\, a \,\rangle \cong \mathbb{Z}_p$, $K = \langle\, b \,\rangle \cong \mathbb{Z}_p$. Consider (A_1, A_2, B_1, B_2) such that $A_1/A_2 \cong B_1/B_2 \cong 1$. There are two cases.

CASE 1) $A_1 = A_2 = H, B_1 = B_2 = K$.

The only subgroup in this case is $H \times K$.

CASE 2) $A_1 = A_2 = 1, B_1 = B_2 = 1$.

The only subgroup in this case is the trivial subgroup 1.

We then consider (A_1, A_2, B_1, B_2) such that $A_1/A_2 \cong B_1/B_2 \cong \mathbb{Z}_p$. In this case $A_2 = B_2 = 1$. So $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(H, K)$. Let $\theta_i : H \longrightarrow K$ be the isomorphism defined by $\theta_i(a^k) = b^{ik}$ for $i = 1, 2, \ldots, p-1$. Then $\{\theta_i : i = 1, 2, \ldots, p-1\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy : \theta_i(x) = y,\ x \in H\} = \langle ab^i \rangle$. So the subgroup consider in this case is $\langle ab^i \rangle$ for each $i = 1, 2, \ldots, p-1$. Consequently, we can list all subgroups of G as follows :

$$1,\ H,\ K, H \times K,\ \langle ab^i \rangle \text{ for } i = 1, 2, \ldots, p-1.$$

Then we can draw the diagram of the subgroup lattice of $\mathbb{Z}_p \times \mathbb{Z}_p$ as shown in Figure 1.

(2) The subgroups of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$

Let $H = \langle a \rangle \cong \mathbb{Z}_p$, $K = \langle b \rangle \cong \mathbb{Z}_{p^2}$. Consider (A_1, A_2, B_1, B_2) such that $A_1/A_2 \cong B_1/B_2 \cong 1$. In this case there exists only one isomorphism θ from A_1/A_2 to B_1/B_2. The subgroups in this case are

$$1,\ H,\ K,\ \langle b^p \rangle,\ H \times \langle b^p \rangle,\ H \times K.$$

We then consider (A_1, A_2, B_1, B_2) such that $A_1/A_2 \cong B_1/B_2 \cong \mathbb{Z}_p$.

CASE 1) $A_1 = H, A_2 = 1, B_1 = \langle b^p \rangle, B_2 = 1$.

Since $A_2 = B_2 = 1$ in this case, $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(H, \langle b^p \rangle)$. Let $\theta_i : H \longrightarrow \langle b^p \rangle$ be the isomorphism defined by $\theta_i(a^k) = b^{ikp}$ for $i = 1, 2, \ldots, p-1$. Then $\{\theta_i : i = 1, 2, \ldots, p-1\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy : \theta_i(x) = y, x \in H\} = \langle ab^{ip} \rangle$. So the subgroups considered in this case is $\langle ab^{ip} \rangle$ for each $i = 1, 2, \ldots, p-1$.

CASE 2) $A_1 = H, A_2 = 1, B_1 = K, B_2 = \langle b^p \rangle$.

In this case $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(H, K/\langle b^p \rangle)$. Let $\theta_i : H \longrightarrow K/\langle b^p \rangle$ be the isomorphism defined by $\theta_i(a^k) = b^{ik}\langle b^p \rangle$ for $i = 1, 2, \ldots, p-1$. Then $\{\theta_i : i = 1, 2, \ldots, p-1\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy : \theta_i(x) = y^i\langle b^p \rangle, x \in H\} = \langle ab^i \rangle$. So the subgroups considered in this case is $\langle ab^i \rangle$ for each $i = 1, 2, \ldots, p-1$.

Consequently, we can list all subgroups of G as follows :

$$1, H, K, H \times K, \langle b^p \rangle, H \times \langle b^p \rangle, \langle ab^{ip} \rangle, \langle ab^i \rangle \text{ for } i = 1, 2, \ldots, p-1.$$

Then we can draw the diagram of the subgroup lattice of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ as shown in Figure 2.

(3) The subgroups of $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$

Let $H = \langle a \rangle \cong \mathbb{Z}_{p^2}$, $K = \langle b \rangle \cong \mathbb{Z}_{p^2}$. Consider (A_1, A_2, B_1, B_2) such that $A_1/A_2 \cong B_1/B_2 \cong 1$. In this case there exists only one isomorphism θ from A_1/A_2 to B_1/B_2. The subgroups in this case are

$$1,\ \langle a^p \rangle,\ H,\ \langle b^p \rangle,\ K,\ \langle a^p \rangle \times \langle b^p \rangle,\ H \times \langle b^p \rangle,\ \langle a^p \rangle \times K,\ H \times K.$$

We then consider (A_1, A_2, B_1, B_2) such that $A_1/A_2 \cong B_1/B_2 \cong \mathbb{Z}_p$.

CASE 1) $A_1 = \langle a^p \rangle, A_2 = 1, B_1 = \langle b^p \rangle, B_2 = 1$.

In this case $A_2 = B_2 = 1$. So $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(\langle a^p \rangle, \langle b^p \rangle)$. Let $\theta_i : \langle a^p \rangle \longrightarrow \langle b^p \rangle$ be the isomorphism defined by $\theta_i(a^{kp}) = b^{ikp}$ for $i = 1, 2, \dots, p-1$. Then $\{\theta_i : i = 1, 2, \dots, p-1\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy : \theta_i(x) = y, x \in \langle a^p \rangle\} = \langle a^p b^{ip} \rangle$. So the subgroup consider in this case is $\langle a^p b^{ip} \rangle$ for each $i = 1, 2, \dots, p-1$.

CASE 2) $A_1 = \langle a^p \rangle, A_2 = 1, B_1 = K, B_2 = \langle b^p \rangle$.

In this case $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(\langle a^p \rangle, K/\langle b^p \rangle)$.
Let $\theta_i : \langle a^p \rangle \longrightarrow K/\langle b^p \rangle$ be the isomorphism defined by $\theta_i(a^{kp}) = b^{ik}\langle b^p \rangle$ for $i = 1, 2, \dots, p-1$. Then $\{\theta_i : i = 1, 2, \dots, p-1\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy : \theta_i(x) = y\langle b^p \rangle, x \in \langle a^p \rangle\} = \langle a^p b^i \rangle$. So the subgroup consider in this case is $\langle a^p b^i \rangle$ for each $i = 1, 2, \dots, p-1$.

CASE 3) $A_1 = H, A_2 = \langle a^p \rangle, B_1 = \langle b^p \rangle, B_2 = 1$.

In this case $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(H/\langle a^p \rangle, \langle b^p \rangle)$.
Let $\theta_i : H/\langle a^p \rangle \longrightarrow \langle b^p \rangle$ be the isomorphism defined by $\theta_i(a^k\langle a^p \rangle) = b^{ikp}$ for $i = 1, 2, \dots, p-1$. Then $\{\theta_i : i = 1, 2, \dots, p-1\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy : \theta_i(xA_2) = y, x \in H\} = \langle ab^{ip} \rangle$. So the subgroup consider in this case is $\langle ab^{ip} \rangle$ for each $i = 1, 2, \dots, p-1$.

CASE 4) $A_1 = H, A_2 = \langle a^p \rangle, B_1 = K, B_2 = \langle b^p \rangle$.

In this case $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(H/\langle a^p \rangle, K/\langle b^p \rangle)$.

Let $\theta_i : H/\langle a^p \rangle \longrightarrow K/\langle b^p \rangle$ be the isomorphism defined by $\theta_i(a^k\langle a^p \rangle) = b^{ik}\langle b^p \rangle$ for $i = 1, 2, \dots, p-1$. Then $\{\theta_i : i = 1, 2, \dots, p-1\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy : \theta_i(xA_2) = yB_2, x \in H\} = \langle ab^i, b^p \rangle$. So the subgroup consider in this case is $\langle ab^i, b^p \rangle$ for each $i = 1, 2, \dots, p-1$.

Then consider (A_1, A_2, B_1, B_2) such that $A_1/A_2 \cong B_1/B_2 \cong \mathbb{Z}_{p^2}$. In this case $A_2 = B_2 = 1$. So $\text{Iso}(A_1/A_2, B_1/B_2) = \text{Iso}(H, K)$. Let $\theta_i : H \longrightarrow K$ be the isomorphism defined by $\theta_i(a^k) = b^{ik}$ for each i such that $\gcd(p, i) = 1$, $1 \le i \le p^2$. Then $\{\theta_i \mid \gcd(p, i) = 1, 1 \le i \le p^2\} = \text{Iso}(A_1/A_2, B_1/B_2)$. Let $C_i = \{xy \mid \theta_i(x) = y, x \in H\} = \langle ab^i \rangle$. So the subgroup consider in this case is $\langle ab^i \rangle$, for each i such that $\gcd(p, i) = 1, 1 \le i \le p^2$. Consequently, we can list all subgroups of G as follows :

$$1,\ \langle a^p \rangle,\ H,\ \langle b^p \rangle,\ K,\ \langle a^p \rangle \times \langle b^p \rangle,\ H \times \langle b^p \rangle,\ \langle a^p \rangle \times K,\ H \times K,\ \langle a^p b^{ip} \rangle,\ \langle a^p b^i \rangle,$$

$$\langle ab^{ip} \rangle,\ \langle ab^i, b^p \rangle,\ \langle ab^t \rangle \text{ for } i = 1, 2, \dots, p-1 \text{ and } \gcd(p, t) = 1, 1 \le t \le p^2.$$

Moreover, for each integers i, t such that $i = 1, 2, \dots, p-1$, $\gcd(p, t) = 1$, $1 \le t \le p^2$, if $t \equiv i \mod p$ then $\langle ab^t \rangle \le \langle ab^i, b^p \rangle$.

Then we can draw the diagram of the subgroup lattice of $\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2}$ as shown in Figure 3.

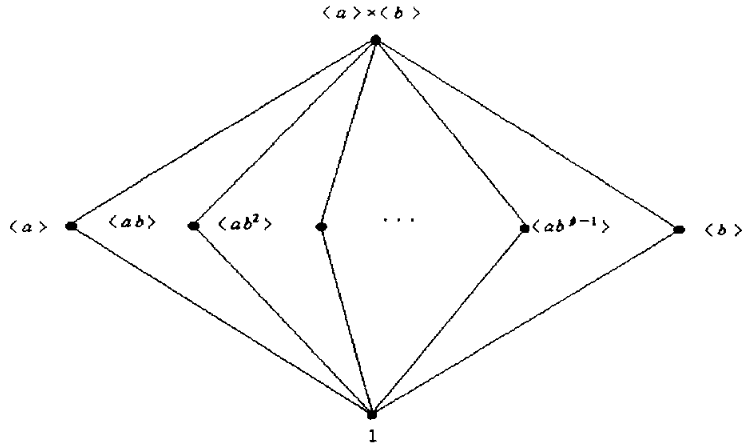

Figure 1. The subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$.

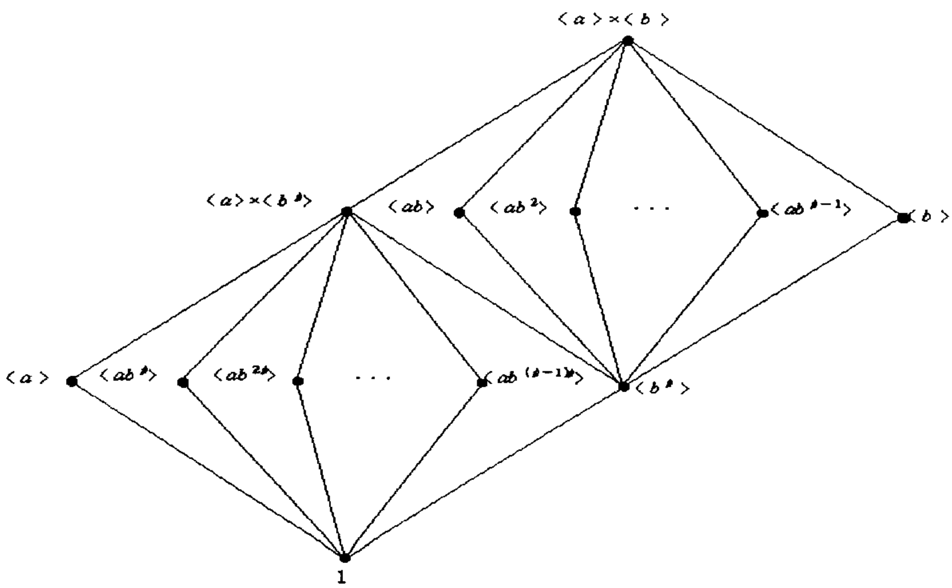

Figure 2. The subgroups of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$.

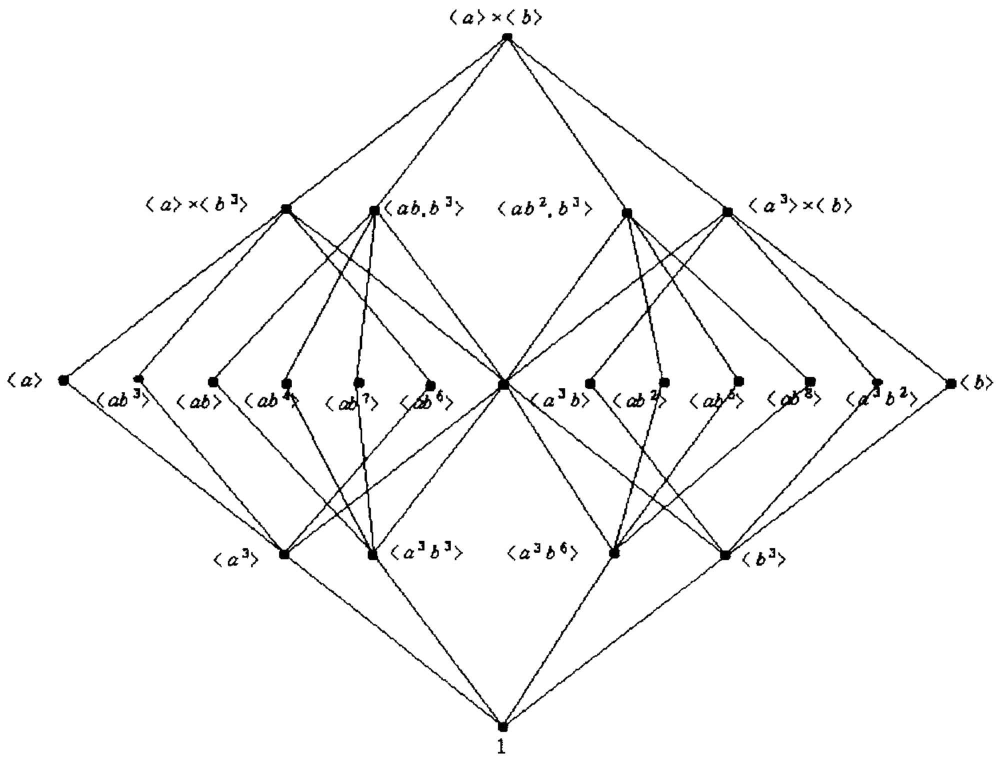

Figure 2. The subgroups of $\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2}$.

6 Subgroups of metacyclic p-groups

Let P be a finite noncyclic metacyclic p-group for an odd prime p. Then P has a presentation of the form:

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

where $\alpha, \beta, \gamma, \delta$ are nonnegative integers such that $\alpha \geq \beta \geq \gamma \geq \delta,\ \ \gamma \geq 1$. Let $B := C_P(\langle\, b \,\rangle)$. Then $B = \langle\, a^{p^{\beta+\delta-\gamma}}, b \,\rangle$, and B is an abelian normal subgroup of P. We also have $|P/B| = p^{\beta+\delta-\gamma}$.

Let A is the abelian group obtained by adjoining to B an element w, subject to the relation $w^{p^{\beta+\delta-\gamma}} = a^{p^{\beta+\delta-\gamma}}$, that is

$$A = \langle\, B, w \,|\, w^{p^{\beta+\delta-\gamma}} = a^{p^{\beta+\delta-\gamma}},\ u^w = u\ (u \in B) \,\rangle.$$

Then $A = \{uw^i \,:\, u \in B,\ i = 0, 1, 2, ..., p^{\beta+\delta-\gamma} - 1\}$ and $A \cong \mathbb{Z}_{p^{\alpha+\delta}} \times \mathbb{Z}_{p^\beta}$.

Define $e := 1 + p^\gamma$ and define $\sigma(k) := 1 + e + e^2 + \cdots + e^{k-1}$. Then from Lemma 2.5 the induced map $\sigma : \{1, 2, 3, \ldots, p^{\beta+\delta-\gamma}\} \longrightarrow \mathbb{Z}_{p^{\beta+\delta-\gamma}}$ is bijective.

Define the map $\tau : A \longrightarrow P$ by $\tau(uw^i) = u^{e^{-\sigma^{-1}(i)}} a^{\sigma^{-1}(i)}$ for every uw^i in A with $u \in B$.

Lemma 6.1. (1) *τ is bijective.* (2) *If S be a subgroup of A then*

$$\tau(x)\tau(y) = \tau(x^{e^{\sigma^{-1}(j)}} y) \in \tau(S) \textit{ for every } x = uw^i,\ y = vw^j \in S.$$

Proof. $\tau(x^{e^{\sigma^{-1}(j)}} y) = \tau(u^{e^{\sigma^{-1}(j)}} v w^{(ie^{\sigma^{-1}(j)}+j)})$

$$= (u^{e^{\sigma^{-1}(j)}}v)^{e^{-\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)}}a^{\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)}$$
$$= u^{e^{\sigma^{-1}(j)-\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)}}v^{e^{-\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)}}a^{\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)}.$$

$$\begin{aligned}\tau(x)\tau(y) &= u^{e^{\sigma^{-1}(i)}}a^{\sigma^{-1}(i)}v^{e^{-\sigma^{-1}(j)}}a^{\sigma^{-1}(j)} \\ &= u^{e^{\sigma^{-1}(i)}}a^{\sigma^{-1}(i)}v^{e^{-\sigma^{-1}(j)}}a^{-\sigma^{-1}(i)}a^{\sigma^{-1}(i)}a^{\sigma^{-1}(j)} \\ &= u^{e^{\sigma^{-1}(i)}}v^{e^{-\sigma^{-1}(j)-\sigma^{-1}(i)}}a^{\sigma^{-1}(j)+\sigma^{-1}(i)}.\end{aligned}$$

By Lemma 2.5, we see that $\sigma(\sigma^{-1}(j) + \sigma^{-1}(i)) = j + e^{\sigma^{-1}(j)}i$. Then $\sigma^{-1}(j) + \sigma^{-1}(i) = \sigma^{-1}(j + e^{\sigma^{-1}(j)}i)$. So it is clear that

$$a^{\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)} = a^{\sigma^{-1}(j)+\sigma^{-1}(i)}.$$

It is also clear that $v^{e^{-\sigma^{-1}(j)-\sigma^{-1}(i)}} = v^{e^{-\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)}}$ and

$$u^{e^{\sigma^{-1}(j)-\sigma^{-1}(ie^{\sigma^{-1}(j)}+j)}} = u^{e^{\sigma^{-1}(j)-\sigma^{-1}(j)+\sigma^{-1}(i)}} = u^{e^{\sigma^{-1}(i)}}.$$

Therefore $\tau(x)\tau(y) = \tau(x^{e^{\sigma^{-1}(j)}}y)$. □

Lemma 6.2. *For every $x \in A$, $\langle \tau(x) \rangle = \tau(\langle x \rangle)$.*

Proof. Since $\tau(x) \in \tau(\langle x \rangle), \langle \tau(x) \rangle$ is contained in $\tau(\langle x \rangle)$. Put p^m is the order of x. Then $\tau(x)^n = 1$ if and only if $\tau(x^{\frac{t^n-1}{t-1}}) = 1$ where $t = e^{\sigma^{-1}(i)}$ if and only if $\frac{t^n-1}{t-1} = 1$ if and only if p^m divides $\frac{t^n-1}{t-1}$ if and only if p^m divides n by Lemma 2.3. Thus p^m is the order of $\tau(x)$. Therefore the order of $\langle \tau(x) \rangle$ is equal to the order of $\tau(\langle x \rangle)$. This yields that $\langle \tau(x) \rangle = \tau(\langle x \rangle)$ □

Lemma 6.3. *$S \leq A$ if and only if $\tau(S) \leq P$.*

Proof. Let $\tau(x), \tau(y) \in \tau(S)$. If $x = uw^i, y = vw^j \in S$ then $x^{e^{\sigma^{-1}(j)}} \in S$. It follows from Lemma 6.1 that $\tau(x)\tau(y) = \tau(x^{e^{\sigma^{-1}(j)}}y) \in \tau(S)$. Thus $\tau(S) \leq P$.

Conversely, if $\tau(S) \leq G$ and $x \in S$ then $\tau(x) \in \tau(S)$. It follows from Lemma 6.2 that $\tau(\langle x \rangle)$ is contained $\tau(S)$. Thus $\langle x \rangle$ is contained S. If $x = uw^i, y = vw^j \in S$ then $x^{e^{\sigma^{-1}(j)}} \in S$, and so $\tau(xy) = \tau(x^{e^{\sigma^{-1}(j)}})\tau(y) \in \tau(S)$. Thus $xy \in S$. Therefore $S \leq A$. □

We can now state the following consequence. We note that it can be obtained also from a general observation given by Baer [2].

Theorem 6.4. *If P is a finite 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.*

References

[1] Reinhold Baer, 'The significance 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 classicfication of metacyclic p-groups*, PhD thesis (Cornell University, 1972).

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

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

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

[7] Wolfgang Lindenberg, 'Struktur und Klassifizierung bizyklischer p-Gruppen', *Gesellschaft f(ü)r Mathematik und Datenverarbeitung* **40** (1971).

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

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