ISSN: 0128-7680
Pertanika J. Sci. & Technol. **19 (1)**: 109 – 116 (2011) © Universiti Putra Malaysia Press

A Description of an Automorphism of a Non-Split Metacyclic *p*-Group

Idham Arif Alias
Institute for Mathematical Research, Universiti Putra Malaysia,
43400 UPM, Serdang, Selangor, Malaysia
E-mail: idham@math.upm.edu.my

ABSTRACT

A map on a group is not necessarily an automorphism on the group. In this paper we study the necessary and sufficient conditions for a map on a non-split metacyclic *p*-group to be an automorphism, where we only consider *p* as an odd prime number. The metacyclic group can be defined by a presentation and it will be beneficial to have a direct relation between the parameters in the presentation and an automorphism of the group. We consider the action of an automorphism on the generators of the group mentioned. Since any element of a metacyclic group will be mapped to an element of the group by an automorphism, we can conveniently represent the automorphism in a matrix notation. We then use the relations and the regularity of the non-split metacyclic *p*-group to find conditions on each entry of the matrix in terms of the parameters in its presentation so that such a matrix does indeed represent an automorphism.

Keywords: Automorphism, matrix notation, non-split metacyclic *p*-group

INTRODUCTION

An automorphism of a non-split metacyclic *p*-group *P* where *p* is an odd prime, will be represented by a matrix notation $\left[\begin{smallmatrix} i & r \\ j & s \end{smallmatrix}\right]$ and denoted by φ, and we write $\varphi \sim \left[\begin{smallmatrix} i & r \\ j & s \end{smallmatrix}\right]$. Our aim is to find conditions on the integers i, j, r and s in terms of parameters in a presentation of the group *P*. We are able to prove that the conditions are sufficient by using the result established by Menegazzo (1993) regarding the order of the automorphism group of a non-split metacyclic *p*-group for an odd prime *p* so that φ does indeed represent an automorphism of the group *P*.

In this paper we show explicitly that the structure of the automorphism group *Aut(P)* of the group *P* mentioned above, depends on the parameters in the presentation of *P*. This result paves the way to find a set of generators and then the class of the automorphism group. This will be the subject of further work. Our approach is direct and computational and therefore different from approach by Bidwell and Curran (2006) who have previously studied the automorphism group of a non-split metacyclic *p*-group.

MATERIALS AND METHODS

We represent an automorphism of the group *P* in a matrix notation and find the direct connection between the entries of the matrix, and the parameters in a presentation of *P*. We recall that if *P* is a metacyclic *p*-group where *p* is a prime number, then the presentation of *P* can be written as

$$P = < x, y \mid x^{p^m} = 1, y^{p^t} = x^{p^q}, yxy^{-1} = x^{1+p^n} > \quad (1)$$

Received: 31 December 2009
Accepted: 10 June 2010

where the parameters m, t, q and n satisfy certain conditions as established by King (1973). We also define any map on the group P by $\varphi(x) = x^i y^j$ and $\varphi(y) = x^r y^s$ where we consider i and r as integers modulo p^m while j and s are considered modulo p^t. The third relation in the presentation above implies that any element of P can be written uniquely in the form $x^\mu y^\upsilon$, where $0 \le u < p^m$ and $0 \le v < p^t$. Therefore we represent φ by the matrix notation $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$ and write $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. This method is similar to the method used by Schulte (2001).

By referring to Theorem 3.2 in a paper written by King (1973), we find that the non-split case can be divided into four cases:
Case 1: $2 \le n < q < m \le t$ where $m \le 2n$,
Case 2: $1 \le n < q < m \le t$ where $2n < m \le q + n$,
Case 3: $3 \le n < q < t < m \le 2n$ and
Case 4: $2 \le n < q < t < m$ where $2n < m \le q + n$.

We will need the following results which will be used throughout this paper.

Lemma 2.1 $(g_1 g_2)^{p^k} = g_1^{p^k} g_2^{p^k}$ for any $g_1, g_2 \in P$ and $k \ge m - n \ge 1$.

Proof. The proof is straightforward using the fact that the metacyclic p-group is a regular group.▪

From the third relation in (1) we have $yx = x^{1+p^n} y$. By putting $\alpha = 1 + p^n$ then it follows that $yx = x^\alpha y$. Note that α will have this meaning throughout this paper.

Lemma 2.2 Let x, y, be the generators of P and u, v be integers with $v > 0$. Then $y^v x^u = x^{u\alpha^v} y^v$.

Proof. This result follows from the third relation in P which is $yx = x^{1+p^n} y$. ▪

Before we proceed we need the following definition.

Definition 2.1 Let u > 0 and $v \ge 1$.

We define $\Lambda(u, v)$as

$$\Lambda(u,v) = \begin{cases} 1 + \alpha^u + \alpha^{2u} + \ldots + \alpha^{(v-1)u}, & v > 1 \\ 1, & v = 1 \end{cases}$$

The following lemma is the result of direct calculation.

Lemma 2.3 Let u and v be integers, $u > 0, v > 1$. Then $\Lambda(u, v)(\alpha^u - 1) = \alpha^{uv} - 1$.

We need to write a power of $(x^u y^v)$ as a product of a power of x and a power of y and we write the proof by using induction.

Lemma 2.4 If x and y are the generators of the group P, u is any integer, $v > 0$ and $w > 1$ then $(x^u y^v)^w = x^{u\Lambda(v,w)} y^{vw}$.

Proof. For $u = 0$ the result is trivial.

Consider $u > 0$. For $w = 1$ the result is clear. Assume the result is true for $w - 1$. Then

$$(x^u y^v)^w = (x^u y^v)^{w-1} x^u y^v = x^{u\Lambda(v,w-1)} y^{v(w-1)} x^u y^v = x^{u\Lambda(v,w-1)} x^{u\alpha^{v(w-1)}} y^{vw} = x^{u\Lambda(v,w)} y^{vw}.$$

By induction the result is true for integers $w \ge 1$.

For $u < 0$ the same proof applies on replacing u by $-u'$ for a positive integer u'.▪

Next, we need quite precise information about the smallest power of p dividing terms in binomial coefficients. Thus we have the following series of lemmas and corollaries where we use the notation $p^k \| c$ to indicate that p^k divides c but p^{k+1} does not divide c.

Lemma 2.5 Let $p^{\epsilon} \| w$ where $\epsilon > 0$. If $2 \le k \le w$ then the power of p dividing $\binom{w}{k} p^{ku}$ is at least $p^{\epsilon + 2u}$ for all $u \ge 1$.

Proof. We first consider the case $2 \le k < p^{\epsilon}$.

Write $k = lp^{v}$ for a positive integer l where $(l, p) = 1$. It is clear that the power of p dividing k is the same as the power of p dividing $w– k$, so that the power of p dividing $(k–1)!$ is the same as that dividing $(w–1)\,(w-2)...(w–k+1)$. Now since $k < p^{\epsilon}$ we have $v < \epsilon$. Hence the power of p dividing

$$\binom{w}{k} p^{ku} = \frac{w(w-1)(w-2)...(w-k+1)}{k(k-1)!} p^{ku}$$

is $p^{\epsilon - v + ku}$.

If $v = 0$ then the proof is complete since $\epsilon + ku \ge \epsilon + 2u$ for $2 \le k < p^{\epsilon}$.

For $v \ne 0$, since $u \ge 1$ and $lp^{v} \ge 2 + v$ for $p \ge 3$ then

$$\epsilon - v + ku = \epsilon - v + lp^{v}u = \epsilon + 2u + (lp^{v} - 2)u - v \ge \epsilon + 2u.$$

This completes the proof for the case $2 \le k < p^{\epsilon}$.

We now consider the case $k \ge p^{\epsilon}$.

Then it is enough to observe that $ku \ge p^{\epsilon}u \ge (\epsilon + 2)u \ge \epsilon + 2u$ since $p^{\epsilon} \ge \epsilon + 2$ for $p \ge 3$. Hence $p^{\epsilon + 2u}$ divides $\binom{w}{k} p^{ku}$ for $k \ge p^{\epsilon}$. ▪

Corollary 2.6 If $p^{\epsilon} \| w$ for $w \ge 2$ and u and c are integers with $u \ge 1, (c, p) = 1$, then for an integer k

$$(1 + cp^{u})^{w} = 1 + cwp^{u} + kp^{\epsilon + 2u}.$$

By using Corollary 2.6 we have:

Corollary 2.7 Let p be an odd prime number and n be a positive integer. Then

a) $p^{n+k} \| (\alpha^{p^{k}} - 1)$ for all integers $k \ge 0$.

b) $\Lambda(u, v) \equiv v + 2^{-1}uv(v-1)p^{n} (mod\ p^{2n})$.

The following corollary relies on Lemma 2.3 and Corollary 2.7(b).

Corollary 2.8 Let u and v be integers, $u > 0$, $v > 1$. Then

$$\alpha^{u} - \alpha \equiv (u-1)p^{n} + 2^{-1}u(u-1)p^{2n} (mod\ p^{3n}).$$

Lemma 2.9 Let φ be an automorphism of P where $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. If x, y are generators of P and m, n are parameters in the presentation (1) of P then

$$x^{r + i\alpha^{s} - r\alpha^{j}} = x^{i(\Lambda(j,\, p^{n}) + \alpha^{jp^{n}})} y^{jp^{n}}.$$

In particular, if $m \le 2n$ then by Corollary 2.7, we obtained

$$x^{r + i\alpha^{s} - r\alpha^{j}} = x^{i\alpha} y^{jp^{n}}.$$

Proof. These results are derived by applying the automorphism φ to both sides of the relation $yxy^{-1} = x^{1+p^n}$ and using the Lemmas 2.1, 2.2 and 2.4.▪

Definition 2.2 Let G be a group. Then G is a 2-generator group if G can be generated by two elements but no smaller set of elements generates G.

We note that if G is a group then $GL(n, G)$ is to denote the general linear group over G of dimension n.

We also note that the intersection of all the maximal subgroups of a non-trivial finite group G is called the Frattini subgroup of G and is denoted by $\Phi(G)$.

Lemma 2.10 If $\varphi \in Aut(P)$ where $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$ then $is - rj$ is not congruent to zero modulo p.
Proof. Since P is a 2-generator group, $P/\Phi(P) \cong Z_p \times Z_p$, and φ defines an automorphism on $P/\Phi(P)$ with matrix $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$, where i, j, r and s are taken modulo p. The matrix is thus in $GL(2, P)$ and so $is - rj$ is not congruent to zero modulo p. ▪

RESULTS AND DISCUSSIONS

In the following theorem we provide the necessary and sufficient conditions for φ to be an automorphism of the group P.

Theorem 3.1 Let P be a non-split metacyclic p-group and φ is a map on P which is represented by $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. Then $\varphi \in Aut(P)$ if and only if
i) $j \equiv 0 (mod\ p^{t-n})$,
ii) $j \equiv 1 (mod\ p^{m-q})$ (for cases 1 & 2) or $i \equiv 1 + rp^{t-q} (mod\ p^{m-q})$ (for cases 3 & 4),
iii) $s \equiv 1 + cp^{q-n} (mod\ p^{m-n})$ where $j = cp^{t-n}$ for $0 \le c < p^n$ and
iv) $r \in Z_{p^m}$.

Proof. Let $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$ and $\varphi \in Aut(P)$.
i) For all cases, $j \equiv 0 (mod\ p^{t-n})$ follows immediately from Lemma 2.9 since $jp^n \equiv 0 (mod\ p^t)$. This result also implies that i and s are not congruent to zero modulo p since from Lemma 2.10, $is - rj$ is not congruent to zero modulo p.
ii) Write $j = cp^{t-n}$ for an integer c where $0 \le c < p^n$.

In cases 1 and 2 where $m \le t$, using Corollary 2.6 we have $\alpha^j \equiv 1 (mod\ p^t) \equiv 1 (mod\ p^m)$, which also implies $\alpha^{jp^n} \equiv 1 (mod\ p^m)$ and $\Lambda(j, p^n) \equiv p^n (mod\, p^m)$. So by Lemma 2.9 we have $x^{r+i\alpha^s - r} = x^{i\alpha} y^{cp^t} = x^{i\alpha} x^{cp^q}$. This implies that

$$i(\alpha^s - \alpha) \equiv cp^q (mod\, p^m). \tag{2}$$

In case 1, $\alpha^s - \alpha \equiv (s-1)p^n (mod\ p^m)$ by Corollary 2.8 since $m \le 2n$. Hence putting this into (2) we obtain

$$i(s-1)p^n \equiv cp^q (mod\ p^m) \tag{3}$$

and so,

$$s \equiv 1 + i^{-1} cp^{q-n} (mod\ p^{m-n}). \tag{4}$$

In case 2, since $m > 2n, \alpha^s - \alpha = (s-1)p^n + kp^{2n}$, for an integer k by the same corollary. Putting this into (2) we have $i((s-1)p^n + kp^{2n}) \equiv cp^q (mod\ p^m)$. Hence

$i((s-1)+kp^n) \equiv cp^{q-n}(mod\ p^{m-n})$ so that

$$s \equiv 1 + i^{-1}cp^{q-n} - kp^n(mod\ p^{m-n}). \tag{5}$$

We now calculate i modulo p^{m-q} in cases 1 and 2. By using the relation $y^{p^t} = x^{p^q}, t \geq m-n, q \geq m-n$ and Lemma 2.1 we have $\varphi(y^{p^t}) = (x^r)^{p^t}(y^s)^{p^t} = (y^s)^{p^t} = x^{sp^q}$

where $(x^r)^{p^t} = 1$ since $t \geq m$ and
$\varphi(x^{p^q}) = (x^i)^{p^q}(y^j)^{p^q} = (x^i)^{p^q}y^{cp^{t-n+q}} = (x^i)^{p^q}(y^{p^t})^{cp^{q-n}} = (x^i)^{p^q}(x^{p^q})^{cp^{q-n}} = x^{ip^q+cp^{2q-n}}$.

Hence $sp^q \equiv ip^q + cp^{2q-n}(mod\ p^m)$. Therefore

$$i \equiv s - cp^{q-n}(mod\ p^{m-q}). \tag{6}$$

In modulus p^{m-q}, from (4) and (5) we see that $s \equiv 1 + i^{-1}cp^{q-n}$ since $n \geq m-q$. Putting this s into (6) and calculating modulo p^{m-q} we have

$$\begin{aligned} i &\equiv 1 + i^{-1}cp^{q-n} - cp^{q-n} \\ &\equiv W - (W-1)i \\ &\equiv W - Wi + i \end{aligned}$$

where $W = 1 + i^{-1}cp^{q-n}$. Thus $Wi \equiv W\ (mod p^{m-q})$ or $W(i-1) \equiv 0 (mod p^{m-q})$ which implies $i \equiv 1 (mod p^{m-q})$ since $W \equiv 1 (mod p)$ and so W is invertible modulo p^{m-q}. Hence we obtain necessity of condition (ii) for cases 1 and 2.

In cases 3 and 4 it is a bit more complicated due to the fact that $t < m$. We first calculate α^j and $\Lambda(j, p^n)$ modulo p^m.

By Corollary 2.6, $\alpha^j = (1+p^n)^{cp^{t-n}} = 1 + cp^t + kp^{t+n} \equiv 1 + cp^t (mod p^m)$ and so, $(\alpha^j)^l \equiv (1+cp^t)^l \equiv 1 + lcp^t + kp^{2t+\epsilon} \equiv 1 + lcp^t (mod p^m)$ for integers l, k and ϵ where $\epsilon \geq 0$. Hence by calculating modulo p^m,

$$\begin{aligned} \Lambda(j, p^n) &\equiv 1 + (1+cp^t) + ... + (1+cp^t)^{p^n-1} \\ &\equiv p^n + cp^t(1 + 2 + ... + (p^n - 1)) \\ &\equiv p^n + 2^{-1}cp^t p^n(p^n - 1) \\ &\equiv p^n. \end{aligned}$$

It is also clear that $\alpha^{jp^n} \equiv 1 (mod p^{n+t}) \equiv 1 (mod p^m)$.
So by Lemma 2.9 we have $x^{r+i\alpha^s - r\alpha^j} = x^{i\alpha}\ y^{cp^t} = x^{i\alpha}\ x^{cp^q}$. This implies

$$i(\alpha^s - \alpha) \equiv r(\alpha^j - 1) + cp^q \equiv rcp^t + cp^q (mod\ p^m). \tag{7}$$

In case 3, $\alpha^s - \alpha \equiv (s-1)p^n (mod\ p^m)$ by Corollary 2.8 since $m \leq 2n$. Hence putting this into (7), $i(s-1)p^n \equiv rcp^t + cp^q (mod\ p^m)$ and so,

$$s \equiv 1 + i^{-1}cp^{q-n}(1 + rp^{t-q})(mod\ p^{m-n}). \tag{8}$$

In case 4 since $m > 2n, \alpha^s - \alpha = (s-1)p^n + k'p^{2n}$, for an integer k' by the same corollary. Putting this into (7) we have $i((s-1)p^n + k'p^{2n}) \equiv rcp^t + cp^q (mod\ p^m)$ and so,

$$s \equiv 1 + i^{-1}cp^{q-n}(1 + rp^{t-q}) - k'p^n (mod\ p^{m-n}). \tag{9}$$

We now calculate i modulo p^{m-q} in cases 3 and 4. By using the relation $y^{p^t} = x^{p^q}, t \geq m-n$ and $q \geq m-n$ and Lemma 2.1 we have

$$\varphi(y^{p^t}) = (x^r)^{p^t}(y^s)^{p^t} = x^{rp^t + sp^q} \text{ and}$$

$$\varphi(x^{p^q}) = (x^i)^{p^q}(y^j)^{p^q} = x^{ip^q}\, y^{cp^{t-n+q}} = x^{ip^q + cp^{2q-n}}.$$

Hence $rp^t + sp^q \equiv ip^q + cp^{2q-n} (mod\ p^m)$ and so we have

$$i \equiv s + rp^{t-q} - cp^{q-n} (mod\ p^{m-q}). \tag{10}$$

In modulus p^{m-q}, from (8) and (9) we see that $s \equiv 1 + i^{-1}cp^{q-n}(1 + rp^{t-q})$since $n \geq m-q$. Putting this s into (10) and calculating modulo p^{m-q} we have

$$\begin{aligned} i &\equiv 1 + i^{-1}cp^{q-n}(1 + rp^{t-q}) + rp^{t-q} - cp^{q-n} \\ &\equiv (1 + rp^{t-q})(1 + i^{-1}cp^{q-n}) - cp^{q-n} \\ &\equiv (1 + rp^{t-q})W - (W-1)i \end{aligned}$$

where $W \equiv 1 + i^{-1}cp^{q-n} (mod p^{m-q})$ as seen in cases 1 and 2. It follows that $W(i-1) \equiv Wrp^{t-q} (mod p^{m-q})$ and since W is invertible modulus p^{m-q}, this gives $i \equiv (1 + rp^{t-q}) (mod p^{m-q})$ which is the necessity of condition (ii) of the theorem for cases 3 and 4.

(iii) In cases 1 and 3, calculating s modulo p^{m-n} is more simple due to the fact that $m \leq 2n$.

Since $i \equiv 1 (mod p^{m-q})$ in case 1, we have $i = 1 + zp^{m-q}$ for an integer z. Note that $p^{q-n} \equiv p^{q-n}(1 + zp^{m-q}) (mod\ p^{m-n})$. Substituting this into (4) so that calculating modulo p^{m-n},

$$\begin{aligned} s &\equiv 1 + i^{-1}cp^{q-n} \\ &\equiv 1 + i^{-1}cp^{q-n}(1 + zp^{m-q}) \\ &\equiv 1 + i^{-1}cp^{q-n}i \\ &\equiv 1 + cp^{q-n}. \end{aligned}$$

This gives the necessity of condition (iii) for case 1.
Similarly, since $i \equiv 1 + rp^{t-q} (mod\ p^{m-q})$ in case 3, we have $i = 1 + rp^{t-q} + z'p^{m-q}$ for an integer z'. Note that $p^{q-n}(1 + rp^{t-q}) \equiv p^{q-n}(1 + rp^{t-q} + z'p^{m-q}) (mod\ p^{m-n})$ so that substituting this into (8) and calculating modulo p^{m-n},

$$\begin{aligned} s &\equiv 1 + i^{-1}cp^{q-n}(1 + rp^{t-q}) \\ &\equiv 1 + i^{-1}cp^{q-n}(1 + rp^{t-q} + z'p^{m-q}) \end{aligned}$$

$$\equiv 1 + i^{-1}cp^{q-n}i$$

$$\equiv 1 + cp^{q-n}.$$

This gives the necessity of condition (iii) for case 3.

Now we calculate s modulo p^{m-n} in cases 2 and 4. Since $m > 2n$ in these two cases, the proof is harder and we divide into two subcases as follows:

a) If $q \leq 2n$

then $m \leq q + n \leq 3n$. Hence from Corollary 2.8,

$$\alpha^s - \alpha \equiv (s-1)p^n + 2^{-1}s(s-1)p^{2n}(mod\ p^m).$$

But from (5) and (9), $s - 1 \equiv 0(mod\ p^{q-n})$ since $n \geq q - n$ and so $(s-1)p^{2n}$ is divisible by $p^{q-n}p^{2n} = p^{q+n} \equiv 0(mod\ p^m)$. Thus $\alpha^s - \alpha \equiv (s-1)p^n(mod\ p^m)$.

In case 2, using this in (2) we obtain $i(s-1)p^n \equiv cp^q(mod\ p^m)$ so that $i(s-1) \equiv cp^{q-n}(mod\ p^{m-n})$ which implies $s \equiv 1 + i^{-1}cp^{q-n}(mod\ p^{m-n})$. Then the rest of the proof to obtain $s \equiv 1 + cp^{q-n}(mod\ p^{m-n})$ is the same as in case 1.

In case 4, using this in (7) we obtain $i(s-1)p^n \equiv rcp^t + cp^q \,(\mathrm{mod}\ p^m)$ and so $s \equiv 1 + i^{-1}cp^{q-n}(1 + rp^{t-q})(mod\ p^{m-n})$. Then the rest of the proof to obtain $s \equiv 1 + cp^{q-n}(mod p^{m-n})$ is the same as in case 3.

b) If $q > 2n$

then from (5) and (9), $s = 1 + fp^v$ where f is prime to p and $v \geq n$. Now we calculate $\alpha^s - \alpha$ modulo p^q.

We have i and α are invertible modulo p^q since both are congruent to one modulo p. Hence from (2) and (7) and calculating modulo p^q,

$$\begin{aligned} 0 &\equiv (\alpha^s - \alpha) \\ &\equiv (\alpha^{s-1} - 1) \\ &\equiv (\alpha^{fp^v} - 1) \\ &\equiv (1 + \alpha^{p^v} + \alpha^{2p^v} + ... + \alpha^{(f-1)p^v})(\alpha^{p^v} - 1) \text{ (by Lemma 2.3).} \end{aligned}$$

But $(1 + \alpha^{p^v} + \alpha^{2p^v} + ... + \alpha^{(f-1)p^v}) \equiv f\ (mod\ p)$ and thus it is not congruent to zero modulo p since f is prime to p. Hence $\alpha^{p^v} - 1 \equiv 0\ (mod\ p^q)$. Since by Corollary 2.7 the highest power of p dividing $\alpha^{p^v} - 1$ is p^{n+v}, we must have p^{n+v} is divisible by p^q so that p^v is divisible by p^{q-n}. Thus $s - 1 = fp^v \equiv 0(mod\ p^{q-n})$. We now calculate $\alpha^s - \alpha$ modulo p^m.

By Corollary 2.6, $\alpha^{s-1} = (1 + p^n)^{fp^v} = 1 + (s-1)p^n + kp^{(q-n)+2n}$. Since $q + n \geq m$ this gives $\alpha^{s-1} \equiv 1 + (s-1)p^n(mod\ p^m)$. Hence modulo p^m,

$\alpha^s - \alpha \equiv \alpha(\alpha^{s-1} - 1) \equiv \alpha(s-1)p^n \equiv (1 + p^n)(s-1)p^n \equiv (s-1)p^n$

since $(s-1)p^{2n} \equiv 0(mod\ p^{q+n}) \equiv 0(mod\ p^m)$ where $m \leq q + n$. Then the rest of the proof is similar to case (a) above to obtain $s \equiv 1 + cp^{q-n}(mod\ p^{m-n})$.

(iv) In all cases, we have no further restriction about r and so r can be any element in Z_{p^m}.

On the other hand, we now show that the conditions of the theorem are sufficient by calculating the number of distinct mappings allowed by these conditions.

In all cases, it is clear that the number of choices for j is p^n and the number of choices for r is p^m since $r \in Z_{p^m}$.

In addition for each $j = cp^{t-n}$ where $0 \leq c < p^n$, the number of choices for s is $p^{t-(m-n)} = p^{t-m+n}$. From this, we see that the number of choices for the pair (s, j) is $p^{t-m+n}p^n = p^{t-m+2n}$ in all cases.

Now, for cases 1 and 2 we have $i \equiv 1 (mod\ p^{m-q})$ and thus, it is clear that the number of choices for i is p^q.

Therefore the number of distinct mappings in cases 1 and 2 is $p^q p^{t-m+2n} p^m = p^{2n+q+t}$ which is also the order of *Aut(P)* as established by Menegazzo (1993).

Now, for cases 3 and 4 we have $i \equiv 1 + rp^{t-q} (mod\ p^{m-q})$ so for each r there are p^q choices of i. As in cases 1 and 2, the number of choices for the pair (s, j) is $(p^{t-m+n})(p^n) = p^{t-m+2n}$. Hence for a distinct $r \in Z_{p^m}$, the number of distinct mapping s allowed is $p^m p^{2n+q+t-m} = p^{2n+q+t}$ which is also the order of *Aut(P)* as established by Menegazzo (1993).

Therefore in all cases, the conditions of the theorem are sufficient. ▪

CONCLUSIONS

In this paper we have found the necessary and sufficient conditions for a map of a non-split metacyclic p-group where p is an odd prime number, to be an automorphism. This result is beneficial since it is directly related to the parameters in the presentation of the metacyclic group, and this may open the way to do further research on the class of the automorphism group of non-split metacyclic p-groups.

ACKNOWLEDGEMENT

I would like to thank very much Dr. Elizabeth Ormerod of The Australian National University for many valuables suggestions.

REFERENCES

Bidwell, J. N. S. and Curran, M. J. (2006). The automorphism group of a split metacyclic p-group. *Archives of Mathematics (Basel.)*, *87*(6), 488-497.

King, B. W. (1973). Presentations of metacyclic groups. *Bulletin of the Australian Mathematical Society*, *8*, 103-131.

Menegazzo, F. (1993). Automorphisms of p-groups with cyclic commutator subgroup. *Rendiconti del Seminario Matematics dell' Universitá di Padova*, *90*, 81-101.

Schulte, M. (2001). Automorphisms of metacyclic p-groups with cyclic maximal subgroups. *Rose-Hulman Undergraduate Research Journal*, *2*(2). Retrieved from http://www.rose-hulman.edu/mathjournal.