Sains Malaysiana 39(6)(2010): 1031–1034

# A Description of an Automorphism of a Split Metacyclic *p*-group

(Pemerihalan Tentang Automorfisme bagi Kumpulan-*p* Metakitaran Belahan)

IDHAM ARIF ALIAS*

ABSTRACT

*A map on a group is not necessarily an automorphism on the group. In this paper we determined the necessary and sufficient conditions of a map on a split metacyclic p-group to be an automorphism, where we only considered 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 considered 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 used the relations and the regularity of the 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 representation; split metacyclic p-group*

ABSTRAK

*Satu pemetaan bagi suatu kumpulan tidak semestinya merupakan suatu automorfisme bagi kumpulan tersebut. Dalam makalah ini kami mengkaji syarat-syarat cukup dan perlu bagi suatu pemetaan kumpulan-p metakitaran belahan untuk menjadi satu automorfisme, dan kami hanya mengambilkira p sebagai suatu nombor perdana ganjil sahaja. Suatu kumpulan metakitaran boleh ditakrifkan dengan suatu pembentangan dan adalah bagus sekiranya terdapat satu kaitan terus di antara parameter-parameter di dalam pembentangan berkenaan dengan sebarang automorfisme kumpulan tersebut. Kami mengambilkira tindakan suatu automorfisme terhadap penjana-penjana kumpulan yang disebutkan. Disebabkan sebarang unsur kumpulan metakitaran tersebut akan dipetakan kepada suatu unsurnya, automorfisme berkenaan boleh diwakilkan dengan suatu simbol berbentuk matriks. Kami kemudiannya menggunakan hubungan dan kenalaran suatu kumpulan-p metakitaran belahan untuk mencari syarat-syarat bagi setiap pemasukan matriks berkenaan dalam sebutan parameter-parameter di dalam pembentangan kumpulan tersebut supaya matriks sedemikian mewakili suatu automorfisma.*

*Kata kunci: Automorfisma; kumpulan-p metakitaran belahan; perwakilan matriks*

## INTRODUCTION

A metacyclic group $G$ is a group which has a cyclic normal subgroup $N$ such that $G/N$ is also a cyclic group. If $P$ is a metacyclic $p$-group where $p$ is a prime number, then the presentation of $P$ can be written as

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

where the parameters $m$, $t$, $q$ and $n$ satisfy some conditions as written by King (1973).

Some examples of metacyclic groups are cyclic groups, direct product of two cyclic groups, dihedral groups and all finite groups whose Sylow subgroups are cyclic. Subgroups and quotients of metacyclic groups are also metacyclic. A metacyclic $p$-group is called split if it has a cyclic normal subgroup with a cyclic complement, and non-split otherwise. For example, dihedral $p$-groups are split metacylic $p$-groups and the quaternion group is non-split.

Bidwell and Curran (2006) have studied the automorphism group of a split metacyclic $p$-group. They used a similar approach to that of a previous paper by Bidwell et al. (2006) where they found the automorphism group of a direct product. In this paper we use a more direct, computational approach by considering the action of an automorphism on the generators of a metacyclic $p$-group. We define any map on the group $P$ by $\varphi(x)= x^i y^j$ and $\varphi(y)= x^r y^s$, and subsequently represent $\varphi$ by the matrix notation $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$ and write $\varphi \sim \begin{bmatrix} i & r \\ j & s \end{bmatrix}$ as written by Schulte (2001). We use the relations of the group and its regularity to find conditions on integers $i$, $j$, $r$ and $s$ in terms of parameters in the presentation of $P$ as in (1). We are able to confirm that the conditions are sufficient from the result of Menegazzo (1993) regarding the order of the automorphism group *Aut(P)* of a split metacyclic $p$-group $P$ for an odd prime $p$. This approach is computational but gives a picture of the automorphism group that we find helpful for further work on the Sylow $p$-subgroup of the automorphism group. In further work we will find a simple structure for the Sylow $p$-subgroup and by finding its upper central series, will determine its nilpotency class.

This paper will focus on the split case, that is when $q \geq m$ and when $p$ is an odd prime. We observe from King (1973) that the split case can be divided into three cases (the work of Schulte (2001) is a particular example of one of these three). By Theorem 3.2 in King's paper (1973) we have the inequality $0 \leq m-n < \min\{t+1, m\}$ and so, $0 \leq m-n < t+1 \leq m$ or $0 \leq m-n < m < t+1$ where the former gives $m \geq n$, $m-n \leq t$ and $t<m$(we take $m>n$ for non-abelian $P$). It follows that $1 \leq t \leq n < m \leq n+t$ or $1 \leq n < t < m \leq n+t$.

Similarly $0 \leq m-n < m < t+1$ implies $m>n$ and $m-n < m$ (which is obvious) and $m \leq t$ so that $1 \leq n < m \leq t$. To summarise these, we break up into three cases:

Case 1: $1 \leq t \leq n < m \leq n+t$

Case 2: $1 \leq n < m \leq t$ and

Case 3: $1 \leq n < t \leq m \leq n+t$.

Before we proceed, we observe that from the first and the second relations in (1), we consider $i$ and $r$ as integers modulo $p^m$ while $j$ and $s$ are considered as modulo $p^t$. The third relation in the presentation above implies that any element of $P$ can be written uniquely in the form $x^u y^v$, where $0 \leq u < p^m$ and $0 \leq v < p^t$.

## PRELIMINARIES

We start with some necessary results which will be used throughout this paper.

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

*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 $yx = x^{1+p^n}y$. We now put $\alpha = 1 + p^n$ so that $yx = x^{\alpha}y$. Note that $\alpha$ 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 $v > 1$. Then we define $\Lambda(u,v) = 1 + \alpha^u + \alpha^{2u} + \ldots + \alpha^{(v-1)u}$ such that $\Lambda(u,1) = 1$.

The following lemma is the result of direct calculation.

Lemma 2.3 Let $u > 0$ and $v > 1$. Then $\Lambda(u,v) \equiv v + 2^{-1}uv(v-1)p^n (mod\ p^{2n})$ and hence $\Lambda(u,v) \equiv v (mod\ p)$.

We will need to be able to write a power of $(x^u y^v)$ as a product of a power of $x$ and a power of $y$. The proof will use induction.

Lemma 2.4 If $x$ and $y$ are the generators of $P$, $u$ 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 $w \geq 1$.

For $u<0$ the same proof applies with $u$ replaced by $-u'$ for a positive integer $u'$. ■

At times we need quite precise information about the smallest power of $p$ dividing terms in binomial coefficients. This is the reason for the following series of lemmas and corollaries. We use the notation $p^k \parallel c$ to indicate that $p^k$ divides $c$ but $p^{k+1}$ does not divide $c$.

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

*Proof.* We first consider the case $2 \leq k < p^{\in}$.

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 $(w-1)(w-2)\ldots(w-k+1)$. Now since $k < p^{\in}$ we have $v < \in$. Hence the power of $p$ dividing

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

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

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

For $v \neq 0$, since $u \geq 1$ and $lp^v \geq 2+v$ for $p \geq 3$ then

$$\in - v + ku = \in - v + lp^v u = \in + 2u + (lp^v - 2)u - v \geq \in + 2u.$$

This completes the proof for the case $2 \leq k < p^{\in}$.
We now consider the case $k \geq p^{\in}$.

It is enough to observe that $ku \geq p^{\in}u \geq (\in + 2)u \geq \in + 2u$ since $p^{\in} \geq \in + 2$ for $p \geq 3$. Hence $p^{\in + 2u}$ divides $\binom{w}{k} p^{ku}$ for $k \geq p^{\in}$. ■

Corollary 2.6 If $p^{\in} \parallel w$ for $w \geq 2$ and $u$ and $c$ are integers with $u \geq 1$, $(c,p) = 1$, then for some integer $k$

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

As a special case of the previous corollary we have

Corollary 2.7 $p^{n+k} \parallel (\alpha^{p^k} - 1)$ for all integers $k \geq 0$.

Lemma 2.8 Let $\varphi$ 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

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

In particular, if $m \leq 2n$ then by Lemma 2.3 and Corollary 2.7,

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

*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. ■

Lemma 2.9 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 i$s - rj$ is not congruent to zero modulo $p$. ■

## Main result

The following proposition is our main result. We note that $U(p^{m})$ denotes the set of units in $Z_{p^{m}}$.

Proposition 3.1 Let $P$ be a 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

Case 1: $r \equiv 0 \ (mod\ p^{m-t}),\ i \in U(p^{m}),\ s \equiv 1 \ (mod\ p^{m-n}),\ j \in Z_{p^{t}}$ or

Case 2: $r \in Z_{p^{m}},\ i \in U(p^{m}),\ s \equiv 1 \ (mod\ p^{m-n}),\ j \equiv 0 \ (mod\ p^{t-n})$ or

Case 3: $r \equiv 0 \ (mod\ p^{m-t}),\ i \in U(p^{m}),\ s \equiv 1 \ (mod\ p^{m-n}),\ j \equiv 0 \ (mod\ p^{t-n})$.

*Proof.*

We will do the proof by each case and as before, we write $\varphi(x)= x^{i}y^{j}$ and $\varphi(y)= x^{r}y^{s}$ where $i, r$ are taken modulo $p^{m}$ and $j, s$ are taken modulo $p^{t}$.

Consider $\varphi \in Aut(P)$.

CASE 1:

$1 = \varphi(1)= \varphi(y^{p^{t}})= (x^{r}y^{s})^{p^{t}}= (x^{r})^{p^{t}}(y^{s})^{p^{t}}= (x^{r})^{p^{t}}$ where $t \geq m-n$ in this case. Thus we have $rp^{t} \equiv 0 \ (mod\ p^{m})$ or $r \equiv 0 \ (mod\ p^{m-t})$.

Now by Lemma 2.9, $is-rj$ is not congruent to zero modulo $p$. But $r \equiv 0 \ (mod\ p^{m-t})$ implies $r \equiv 0 \ (mod\ p)$ and thus $is$, is not congruent to zero modulo $p$ and so $i$ is not congruent to zero modulo $p$. Since $i \in Z_{p^{m}}$, we have $i \in U(p^{m})$ as there is no further information on value of $i$.

Now by Lemma 2.8, $x^{r+i\alpha^{s}-r\alpha^{j}}y^{j}= x^{i\alpha}y^{j\alpha}$ where $n>m-n$ and $n \geq t$ in this case. Hence $r+i\alpha^{s}- r\alpha^{j} \equiv i\alpha \ (mod\ p^{m})$ or $r(1- \alpha^{j}) \equiv i(\alpha- \alpha^{s})(mod\ p^{m})$. Now since $\alpha \equiv 1 \ (mod\ p^{n})$, we have $\alpha^{j} \equiv 1 \ (mod\ p^{n}) \equiv 1 \ (mod\ p^{t})$ and so $r(1- \alpha^{j}) \equiv 0 \ (mod\ p^{m})$. Thus $i(\alpha- \alpha^{s}) \equiv 0 \ (mod\ p^{m})$ and since $i$ is not congruent to zero modulo $p^{m}$, it follows that $\alpha \equiv \alpha^{s} \ (mod\ p^{m})$.

Now since $(\alpha, p^{m})= 1$, we can say that $\alpha \in U(p^{m})$ so that $\alpha^{-1}$ exists in modulo $p^{m}$ which implies $\alpha^{s-1} \equiv 1 \ (mod\ p^{m})$. By Corollary 2.7, $p^{n+m-n} \parallel (\alpha^{p^{m-n}}- 1)$ and hence $\alpha^{p^{m-n}} \equiv 1 \ (mod\ p^{m})$ so that the order of α in $U(p^{m})$ is $p^{m-n}$. It follows that $p^{m-n} \mid (s- 1)$ and thus $s \equiv 1 \ (mod\ p^{m-n})$ where in this case $m-n \leq t$.

Finally since there are no limits on $j$ except that its values are evaluated modulo $p^{t}$, we can consider $j \in Z_{p^{t}}$.

These gives the necessity of the conditions for Case 1.

CASE 2:

By Lemma 2.8, $x^{r+i\alpha^{s}-r\alpha^{j}}y^{j}= x^{i(\Lambda(j,\, p^{n})+ \alpha^{jp^{n}}})y^{j\alpha}$ which implies $r+i\alpha^{s}-r\alpha^{j} \equiv i(\Lambda(j, p^{n})+ \alpha^{jp^{n}}) \ (mod\ p^{m})$ and $j \equiv j\alpha \ (mod\ p^{t})$.

Now $j(1- \alpha) \equiv 0 \ (mod\ p^{t})$ so that $j(-p^{n}) \equiv 0 \ (mod\ p^{t})$ or $j \equiv 0 \ (mod\ p^{t-n})$.

Now by Lemma 2.9, $is - rj$ is not congruent to zero modulo $p$. But $j \equiv 0 \ (mod\ p^{t-n})$ implies $j \equiv 0 \ (mod\ p)$. Thus $is$ is not congruent to zero modulo $p$ so that $i$ is not congruent to zero modulo $p$. Since $i \in Z_{p^{m}}$, we have $i \in U(p^{m})$ as there is no further information on value of $i$.

In addition, $r-r\alpha^{j} \equiv i(\Lambda(j, p^{n})+ \alpha^{jp^{n}}- \alpha^{s}) \ (mod\ p^{m})$ from above. Now by Corollary 2.7, $p^{n+t-n} \parallel (\alpha^{p^{t-n}}- 1)$ so that $\alpha^{p^{t-n}} \equiv 1 \ (mod\ p^{t})$. Since $j \equiv 0 \ (mod\ p^{t-n})$, we have $\alpha^{j} \equiv 1 \ (mod\ p^{t}) \equiv 1 \ (mod\ p^{m})$ because $m \leq t$ in this case. Thus $\Lambda(j, p^{n}) = 1+ \alpha^{j}+ \alpha^{2j}+ \ldots + \alpha^{(p^{n}-1)j} \equiv p^{n} \ (mod\ p^{m})$. Also $\alpha^{jp^{n}} \equiv 1 \ (mod\ p^{m})$ and hence, $r(1- \alpha^{j}) \equiv i\ (p^{n}+1-\alpha^{s})(mod\ p^{m})$ which implies $0 \equiv i(\alpha- \alpha^{s}) \ (mod\ p^{m})$.

By a similar argument as in Case 1, $\alpha^{s-1} \equiv 1 \ (mod\ p^{m})$ and by Corollary 2.7, $p^{n+m-n} \parallel (\alpha^{p^{m-n}}- 1)$ so that $\alpha^{p^{m-n}} \equiv 1 \ (mod\ p^{m})$ and order of α in $U(p^{m})$ is $p^{m-n}$. Hence $p^{m-n} \mid (s-1)$ which gives $s \equiv 1 \ (mod\ p^{m-n})$ where in this case $m-n \leq t$ since $m \leq t$.

Finally since there are no limits on $r$ except that its values are evaluated modulo $p^{m}$, we can consider $r \in Z_{p^{m}}$.

These gives the necessity of the conditions for Case 2.

CASE 3:

As in Case 1, since $t \geq m-n$, we have $r \equiv 0 \ (mod\ p^{m-t})$. Then $i \in U(p^{m})$ will be proved either as in Case 1 or 2.

Also as in Case 2 the proof is the same to have $j \equiv 0 \ (mod\ p^{t-n})$ as well as $r(1- \alpha^{j}) \equiv i(\Lambda\ (j,p^{n})+\alpha^{jp^{n}}- \alpha^{s})(mod\ p^{m})$ and $\alpha^{j} \equiv 1 \ (mod\ p^{t})$.

Now since $r \equiv 0 \ (mod\ p^{m-t})$ and $(1- \alpha^{j}) \equiv 0 \ (mod\ p^{t})$, we have $r(1- \alpha^{j}) \equiv 0(mod\ p^{m})$.

Also since $j \equiv 0 \ (mod\ p^{t-n})$ so that $jp^{n} \equiv 0 \ (mod\ p^{t})$, by using Corollary 2.7 we have $\alpha^{jp^{n}} \equiv 1 \ (mod\ p^{n+t}) \equiv 1 \ (mod\ p^{m})$ because $m \leq n+t$. Now for $1 \leq k \leq p^{n}-1$ by Corollary 2.6, $\alpha^{kj} \equiv 1+kjp^{n} \ (mod\ p^{n+t})$ and thus

$$\begin{aligned} \Lambda(j, p^{n}) &= 1+ \alpha^{j}+ \alpha^{2j}+ \ldots + \alpha^{(p^{n}-1)j} \\ &\equiv 1+(1+jp^{n})+ (1+2jp^{n})+\ldots+(1+(p^{n}-1)jp^{n})(mod\ p^{n+t}) \end{aligned}$$

$\equiv p^n + 2^{-1}jp^n(p^n)(p^n - 1)$ $(mod\ p^{n+t})$
$\equiv p^n$ $(mod\ p^{n+t})$ (since $jp^n$ $(p^n) \equiv 0$ $(mod\ p^{n+t})$
$\equiv p^n$ $(mod\ p^m)$ (since $m \leq n+t$).

As in previous case, $\alpha^{s-1} \equiv 1$ $(mod\ p^m)$ and by a similar argument as in Case 2 we have $s \equiv 1$ $(mod\ p^{m-n})$

These give the necessity of the conditions for Case 3. Now we show that the condition of the theorem are sufficient by calculating the number of distinct mappings allowed by this condition, in each case.

CASE 1:
Since $r \equiv 0$ $(mod\ p^{m-t})$, $i \in U(p^m)$, $s \equiv 1$ $(mod\ \ p^{m-n})$ and $j \in Z_{p^t}$, the number of choices for each parameter is as in the following table:

| Parameter | Choice |
|---|---|
| $r$ | $p^t$ |
| $i$ | $p^{m-1}(p-1)$ |
| $s$ | $p^{t+n-m}$ |
| $j$ | $p^t$ |

Therefore the number of distinct mappings allowed is $p^{3t+n-1}(p-1)$ which is also the order of the automorphism group *Aut(P)* of *P* by Menegazzo (1993).

CASE 2:
Since $r \in Z_{p^m}$, $i \in U(p^m)$, $s \equiv 1$ $(mod\ p^{m-n})$ and $j \equiv 0$ $(mod\ p^{t-n})$, the number of choices for each parameter is as in the following table:

| Parameter | Choice |
|---|---|
| $r$ | $p^m$ |
| $i$ | $p^{m-1}(p-1)$ |
| $s$ | $p^{t+n-m}$ |
| $j$ | $p^n$ |

Therefore the number of distinct mappings allowed is $p^{t+m+2n-1}(p-1)$ which is also the order of *Aut(P)* by Menegazzo (1993).

CASE 3:
Since $r \equiv 0$ $(mod\ p^{m-t})$, $i \in U(p^m)$, $s \equiv 1$ $(mod\ p^{m-n})$ and $j \equiv 0$ $(mod\ p^{t-n})$, the number of choices for each parameter is as in the following table:

| Parameter | Choice |
|---|---|
| $r$ | $p^t$ |
| $i$ | $p^{m-1}(p-1)$ |
| $s$ | $p^{t+n-m}$ |
| $j$ | $p^n$ |

Therefore the number of distinct mappings allowed is $p^{2t+2n-1}(p-1)$ which is also the order of *Aut(P)* by Menegazzo (1993). ■

## Conclusion

In this paper we have found the necessary and sufficient conditions for a map of a 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.

## REFERENCES

Bidwell, J.N.S. & Curran, M.J. 2006. The automorphism group of a split metacyclic p-group. *Arch. Math.* 87(6): 488-497.

Bidwell, J.N.S., Curran, M.J. & McCaughan, D.J. 2006. Automorphisms of direct products of finite groups. *Arch. Math.* 86(6): 481-489.

King, B.W. 1973. Presentations of metacyclic groups. *Bull. Austral. Math. Soc.* 8: 103-131.

Menegazzo, F. 1993. Automorphisms of p-groups with cyclic commutator subgroup. *Rend. Sem. Mat. Univ. Padova* 90: 81-101.

Schulte, M. 2001. Automorphisms of metacyclic p-groups with cyclic maximal subgroups. *Rose-Hulman Undergraduate Research Journal* 2(2).

Institute for Mathematical Research
Faculty of Science, Universiti Putra Malaysia
43400 UPM Serdang, Selangor D.E.
Malaysia

*Corresponding author; email: idham@math.upm.edu.my

Received: 17 November 2009
Accepted: 17 February 2010