# Automorphisms of Metacyclic p-Groups With Cyclic Maximal Subgroups

Mark Schulte

**Abstract**

This paper deals with the determination of the automorphism group of the metacyclic $p$-groups, $P(p,m)$, given by the presentation

$$P(p,m) = \langle x, y |\, x^{p^m} = 1, y^p = 1, yxy^{-1} = x^{p^{m-1}+1} \rangle \qquad (1)$$

where $p$ is an odd prime number and $m > 1$. We will show that $\mathrm{Aut}(P)$ has a unique Sylow $p$-subgroup, $S_p$, and that in fact

$$\mathrm{Aut}(P) \cong S_p \rtimes \mathbf{Z}_{p-1}.$$

A general metacyclic $p$-group has a presentation of the form

$$G = \langle x, y | x^{p^m} = 1, y^{p^n} = x^{p^q}, yxy^{-1} = x^{p^l+1} \rangle,$$

with certain restrictions on the parameters $m$, $n$, $q$, and $l$ [4]. Thus, $\langle x \rangle$ is maximal in $G$ if and only if $|G| = p^{m+1}$ [3]. Checking the conditions on the parameters, we see that this forces $n = 1$, $q = 0$, and $l = m - 1$. This implies that the groups $P(p,m)$ described in the abstract are exactly those metacyclic $p$-groups with a cyclic maximal subgroup. Note that when $m = 2$, we get one of the extra-special groups of order $p^3$. While we will restrict our study of automorphisms to metacyclic $p$-groups of odd order, it may be useful to note that $P(2,2)$ is the dihedral group of order 8.

We begin our examination of the group of automorphisms of $P = P(p,m)$, $\mathrm{Aut}(P)$, with the fact that any automorphism is determined by its action on the generators of $P(p,m)$. Also, the third relation in equation 1 implies that any element of $P(p,m)$ can be written uniquely in the form $x^a y^b$, where $0 \le a \le p^m$, and $0 \le b \le p$. We therefore define any automorphism $\phi$ on the group $P(p,m)$ by $\phi(x) = x^i y^j$ and $\phi(y) = x^r y^s$.

Throughout this paper we will represent an automorphism $\phi$ by the matrix $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$ and will write $\phi = \begin{bmatrix} i & r \\ j & s \end{bmatrix}$. This does not imply that $\phi$ is a matrix. Rather, we are merely using matrix notation to organize and represent the action of $\phi$ upon the generators of $P(p,m)$.

**Proposition 1** *If* $\phi = \begin{bmatrix} i & r \\ j & s \end{bmatrix} \in \mathrm{Aut}(P)$, *then* $r \equiv 0 \bmod p^{m-1}$, $j \in \mathbf{Z}_p, s \equiv 1 \bmod p$, *and* $i \in U(p^m)$, *where* $U(p^m)$ *is the group of integers under multiplication mod* $p^m$.

PROOF. From the first and second relations in equation 1 we conclude that $i$ and $r$ are integers considered mod $p^m$ while $j$ and $s$ are integers considered mod $p$. We complete the proof of this proposition by using the results of the following three claims.

**Claim 2** *If $r$ is as in Proposition 1, then $r \equiv 0 \bmod p^{m-1}$.*

PROOF. We begin by noting that for $p > 2$, $P(p,m)$ is a regular group [1]. This implies that for any $g_1, g_2 \in P(p,m)$ and $p$ a prime number, we have that $(g_1 g_2)^{p^k} = g_1^{p^k} g_2^{p^k} z^{p^k}$ where $z \in [P,P]$, the commutator subgroup of $P(p,m)$. From the third relation in the presentation of $P(p,m)$ we see that $[P,P] = \langle x^{p^{m-1}} \rangle$. Thus, for any $k \geq 1$, we have that $(g_1 g_2)^{p^k} = g_1^{p^k} g_2^{p^k}$. As a result, an application of an automorphism in $\mathrm{Aut}(P)$ to the second relation in the presentation of $P(p,m)$ yields

$$1 = \phi(1) = \phi(y^p) = \phi(y)^p = (x^r y^s)^p = x^{rp} y^{sp} = x^{rp}.$$

It follows that $rp \equiv 0 \bmod p^m$, which implies that $r \equiv 0 \bmod p^{m-1}$.

□

**Claim 3** *If $i$ is as in Proposition 1, then $i \in U(p^m)$.*

PROOF. Since $P(p,m)$ is a finite $p$-group, its Frattini subgroup is $\Phi(P) = P^p[P,P]$ [5]. It follows that $\Phi(P) = \langle x^p \rangle$ and $P/\Phi(P) \cong \mathbf{Z}_p \times \mathbf{Z}_p$. Also, $\Phi(P)$ is characteristic so any automorphism $\alpha$ in $\mathrm{Aut}(P)$ restricts to an automorphism of $\Phi(P)$.

Let $\Theta : \mathrm{Aut}(P) \longrightarrow \mathrm{Aut}\,(P/\Phi(P))$ be the natural homomorphism defined by $\Theta(\alpha)\,(x\Phi(P)) = \alpha(x)\Phi(P)$, where $\alpha \in \mathrm{Aut}(P)$ and $x\Phi(P) \in P/\Phi(P)$.

Now, $\mathrm{Aut}\,(P/\Phi(P)) \cong \mathrm{Aut}(\mathbf{Z}_p \times \mathbf{Z}_p) = GL_2(\mathbf{Z}_p)$, the group of $2\times 2$ invertible matrices over $\mathbf{Z}_p$.

Thus, $\Theta(\alpha) = \Theta\left(\begin{bmatrix} i & r \\ j & s \end{bmatrix}\right) = \begin{bmatrix} \overline{i} & \overline{r} \\ \overline{j} & \overline{s} \end{bmatrix}$, where a "bar" signifies that an entry is considered mod $p$. However, $\begin{bmatrix} \overline{i} & \overline{r} \\ \overline{j} & \overline{s} \end{bmatrix} \in GL_2(\mathbf{Z}_p)$ implies that $\overline{i}\overline{s} - \overline{r}\overline{j} \not\equiv 0 \bmod p$, while Claim 2 states that $r \equiv 0 \bmod p$. It follows that $i \not\equiv 0 \bmod p$.

Using this result and the fact that values of $i$ are considered mod $p^m$, we arrive at the conclusion that we can consider $i \in U(p^m)$.

□

We next prove a lemma which will be used extensively in Claim 5.

**Lemma 4** *Let $x, y$ be the generators of $P(p,m)$, $\alpha = p^{m-1} + 1$, and $a, b > 0$. Then $y^b x^a = x^{a\alpha^b} y^b$.*

PROOF. The third relation in equation 1 states that $yxy^{-1} = x^{\alpha}$, which is equivalent to $yx = x^{\alpha}y$. By applying this relation to $y^b x^a$ we have

$$\begin{aligned} y^b x^a &= y^{b-1}(yx)x^{a-1} \\ &= y^{b-1}(x^{\alpha}y)x^{a-1} \\ &\vdots \\ &= x^{\alpha^b} y^b x^{a-1} \\ &\vdots \\ &= x^{2\alpha^b} y^b x^{a-2} \\ &\vdots \\ &= x^{a\alpha^b} y^b. \end{aligned}$$

□

**Claim 5** *If $s$ is as in Proposition 1, then $s \equiv 1 \bmod p$.*

PROOF. We apply an automorphism to both sides of the third relation in equation 1 and then use the result of the previous lemma. By applying $\phi$ to the left hand side of the third relation we have

$$\phi(yxy^{-1}) = (x^r y^s)(x^i y^j)(x^r y^s)^{-1} = x^{r+i\alpha^s - r\alpha^j} y^j.$$

Similarly, an application of $\phi$ to the right hand side yields

$$\phi\left(x^{p^{m-1}+1}\right) = (x^i y^j)^{p^{m-1}}(x^i y^j) = x^{i(p^{m-1}+1)} y^j.$$

This implies that

$$\begin{aligned} & x^{r+i\alpha^s - r\alpha^j} y^j &&= && x^{i\alpha} y^j \\ \Leftrightarrow \quad & r + i\alpha^s - r\alpha^j &&\equiv && i\alpha \bmod p^m \\ \Leftrightarrow \quad & r\left(1 - \alpha^j\right) &&\equiv && i\left(\alpha - \alpha^s\right) \bmod p^m. \end{aligned}$$

Now, $\alpha = (p^{m-1} + 1)$ implies that $\alpha \equiv 1 \bmod p$, so it follows that $\alpha^j \equiv 1 \bmod p$, and hence $1 - \alpha^j \equiv 0 \bmod p$. Likewise, $r \equiv 0 \bmod p^{m-1}$ implies that $r(1 - \alpha^j) \equiv 0 \bmod p^m$. Applying this to our result above, we must have that $i(\alpha - \alpha^s) \equiv 0 \bmod p^m$. However, $i \not\equiv 0 \bmod p$ implies that $i \not\equiv 0 \bmod p^m$. Thus, $i(\alpha - \alpha^s) \equiv 0 \bmod p^m$ if and only if $\alpha \equiv \alpha^s \bmod p^m$.

Since $\alpha$ is relatively prime to $p^m$ we can conclude that $\alpha \in U(p^m)$ and $\alpha^{-1}$ exists mod $p^m$. As a result we have that $\alpha^{s-1} \equiv 1 \bmod p^m$, so $|\alpha| \mid (s-1)$. Furthermore, a binomial expansion of $\alpha^p$ produces

$$\begin{aligned} \alpha^p &= \left(p^{m-1} + 1\right)^p \\ &= p^{(m-1)p} + \binom{p}{1} p^{(m-1)(p-1)} + \cdots + \binom{p}{p-1} p^{m-1} + 1. \end{aligned}$$

Using the fact that $p \mid \binom{p}{k}$ for $1 \leq k \leq p-1$, we see that $\alpha^p \equiv 1 \bmod p^m$. It follows that $|\alpha| = p$, so $p \mid (s-1)$. Hence $s \equiv 1 \bmod p$.

□

Finally, analysis of the relations of $P(p,m)$ yields no limits on $j$ except that its values are evaluated $\bmod p$. This implies that we can consider $j \in \mathbf{Z}_p$, which completes the proof of Proposition 1.

□

Our next task is to use our previous results to determine the structure of $\mathrm{Aut}(P)$. We begin with a definition and several lemmas which will be used extensively in the remainder of this paper.

**Definition 6** *Let $\alpha = p^{m-1}+1$ and $a,b>0$. Then we define $\Lambda(a,b)$ by*

$$\Lambda(a,b) = 1 + \alpha^a + \alpha^{2a} + \cdots + \alpha^{(b-1)a}.$$

**Lemma 7** $\Lambda(a,b) \equiv b \bmod p^k$ *for all* $1 \le k \le m-1$.

Proof. Let $1 \le k \le m-1$. Then we have the following:

$$\begin{aligned}
\Lambda(a,b) &= 1 + \alpha^a + \alpha^{2a} + \cdots + \alpha^{(b-1)a} \\
&= 1 + (p^{m-1}+1)^a + (p^{m-1}+1)^{2a} + \cdots + (p^{m-1}+1)^{(b-1)a} \\
&\equiv 1 + 1^a + 1^{2a} + \cdots + 1^{(b-1)a} \bmod p^k \\
&\equiv b \bmod p^k.
\end{aligned}$$

□

**Lemma 8** *If $x$ and $y$ are the generators of $P(p,m)$ and $a,b,c>0$, then $(x^a y^b)^c = x^{a\Lambda(b,c)} y^{bc}$.*

Proof. We expand $(x^a y^b)^c$ as follows:

$$\begin{aligned}
(x^a y^b)^c &= x^a (y^b x^a)(y^b x^a) * \cdots * x^a y^b \\
&= x^a x^{a\alpha^b} y^{2b} x^a * \cdots * x^a y^b \\
&= x^a x^{a\alpha^b} x^{a\alpha^{2b}} y^{3b} x^a * \cdots * x^a y^b \\
&\vdots \\
&= x^{a\left(1+\alpha^b+\cdots+\alpha^{(c-1)b}\right)} y^{bc} \\
&= x^{a\Lambda(b,c)} y^{bc}.
\end{aligned}$$

□

**Lemma 9** *If $\alpha = p^{m-1}+1$, then $\alpha^{p^k} \equiv 1 \bmod p^m$ for all $k \ge 1$.*

Proof. The result follows from binomially expanding $\alpha^{p^k}$ as shown below:

$$\begin{aligned}
\alpha^{p^k} &= \left(p^{m-1}+1\right)^{p^k} \\
&= \left(p^{m-1}\right)^{p^k} + \binom{p^k}{1}\left(p^{m-1}\right)^{p^k-1} + \cdots + \binom{p^k}{p^k-1} p^{m-1} + 1 \\
&\equiv 1 \bmod p^m \quad \text{for all } k \ge 1.
\end{aligned}$$

□

**Proposition 10** *There exists a one-to-one relationship between the set of matrices of the form given in Proposition 1, and the automorphisms in Aut(P).*

PROOF. We know from Proposition 1 and Claim 5 that every automorphism $\phi$ in Aut$(P)$ can be represented by a matrix of the form $\begin{bmatrix} i & r \\ j & 1 \end{bmatrix}$, where $i \in U(p^m)$, $r \equiv 0 \bmod p^{m-1}$, and $j \in \mathbf{Z}_p$. In order to show the converse is true, we will prove that the homomorphism induced by $\phi = \begin{bmatrix} i & r \\ j & 1 \end{bmatrix}$ is indeed an automorphism by determining its unique inverse.

Let $\psi = \begin{bmatrix} a & d \\ c & 1 \end{bmatrix}$. We will determine $a, c$, and $d$, then show that they satisfy the conditions of Proposition 1. In order for $\psi$ to be an inverse map for $\phi$, we need $x = (\psi \circ \phi)(x)$ and $y = (\psi \circ \phi)(y)$. Hence we must have that

$$\begin{aligned} x = (\psi \circ \phi)(x) = (x^a y^c)^i (x^d y)^j &= x^{a\Lambda(c,i)} y^{ci} x^{d\Lambda(1,j)} y^j \\ &= x^{a\Lambda(c,i) + d\Lambda(1,j)\alpha^{ci}} y^{j+ci}. \end{aligned}$$

and

$$\begin{aligned} y = (\psi \circ \phi)(y) = (x^a y^c)^r (x^d y) &= x^{a\Lambda(c,r)} y^{cr} x^d y \\ &= x^{a\Lambda(c,r) + d\alpha^{cr}} y^{cr+1}. \end{aligned}$$

This implies we need the following relationships to hold for some unique $a, d \in \mathbf{Z}_{p^m}$ and $c \in \mathbf{Z}_p$ as discussed in Proposition 1.

$$\begin{aligned} &i) \quad j + ci \equiv 0 \bmod p \\ &ii) \quad a\Lambda(c,i) + d\Lambda(1,j)\alpha^{ci} \equiv 1 \bmod p^m \\ &iii) \quad a\Lambda(c,r) + d\alpha^{cr} \equiv 0 \bmod p^m \\ &iv) \quad cr + 1 \equiv 1 \bmod p \end{aligned}$$

From $(i)$ it can be concluded that $c \equiv -ji^{-1} \bmod p$, which exists since $i \not\equiv 0 \bmod p$. However, $-ji^{-1}$ may range through all values of $\mathbf{Z}_p$, so this does not impose additional restrictions on the value of $c$. Analysis of $(iv)$ yields no further information on $c$ since $r \equiv 0 \bmod p^{m-1}$, and we will later see that $(ii)$ and $(iii)$ also do not limit the value of $c$. As far as determining the value of $a$, we first note that $(iii)$ implies

$$a\Lambda(c,r) + d\alpha^{cr} \equiv a\Lambda(c,r) + d \bmod p^m$$

since $r \equiv 0 \bmod p^{m-1}$. It follows that $d \equiv -a\Lambda(c,r) \bmod p^m$. Substituting this result into $(ii)$ yields

$$a[\Lambda(c,i) - \Lambda(c,r) * \Lambda(1,j) * \alpha^{ci}] \equiv 1 \bmod p^m.$$

Now, $[\Lambda(c,i) - \Lambda(c,r) * \Lambda(1,j) * \alpha^{ci}] \equiv i - rj \bmod p$ by Lemma 7. Furthermore, $i - rj \not\equiv 0 \bmod p$ because $i \not\equiv 0 \bmod p$ and $r \equiv 0 \bmod p$, so it follows that we can choose $a \equiv \left[\Lambda(c,i) - \Lambda(c,r) * \Lambda(1,j)\alpha^{ci}\right]^{-1} \bmod p^m$.

Finally, using this information we have that

$$\begin{aligned} d &= -a\Lambda(c,r) \\ &= -\left[\Lambda(c,i) - \Lambda(c,r) * \Lambda(1,j)\alpha^{ci}\right]^{-1} \Lambda(c,r). \end{aligned}$$

In order to show that $a, c$, and $d$ satisfy the conditions of Proposition 1, we first note that $\Lambda(c,r) \equiv 0 \bmod p^{m-1}$ implies that $d \equiv 0 \bmod p^{m-1}$. Similarly, $c$ can be considered $\bmod p$, and we have already seen that $a \in U(p^m)$. Hence we have determined values for $a$, $c$, and $d$ such that $\psi \circ \phi = 1$, so $\psi = \phi^{-1}$. It follows that every matrix $\begin{bmatrix} i & r \\ j & s \end{bmatrix}$ whose entries satisfy the conditions of Proposition 1 yields an element of $\mathrm{Aut}(P)$. This implies there exists a one-to-one relationship between the set of matrices of this form and the group $\mathrm{Aut}(P)$.

□

Using this information, we are now able to infer the order of the automorphism group of $P(p,m)$.

**Theorem 11** *If $P = P(p,m)$, then $|\mathrm{Aut}(P)| = p^{m+1}(p-1)$.*

Proof. From the previous proposition, we know that $i$, $j$, and $r$ completely and uniquely determine each matrix representation of an automorphism in $\mathrm{Aut}(P)$. This implies that the order of $\mathrm{Aut}(P)$ is completely determined by the possible combinations of $i$, $j$, and $r$. There are $p$ choices for $j$ since $j \in \mathbf{Z}_p$, $p^{m-1}(p-1)$ possibilities for $i$ since $i \in U(p^m)$ and $|U(p^m)| = p^{m-1}(p-1)$, and $p$ choices for $r$. It follows that $|\mathrm{Aut}(P)| = p^{m+1}(p-1)$.

□

Now that the order of $\mathrm{Aut}(P)$ has been determined, we next factor the matrix representation of an element of this group into the product of more basic matrices. Since $p$ is odd, $U(p^m)$ is cyclic [2]. Hence, we can find a generator $g$ such that $g^{p-1} \equiv 1 \bmod p$. Let $a = g^{p-1}$ and $c = g^{p^{m-1}}$, and note that $a$ and $c$ have order $p^{m-1}$ and $p-1$ respectively. Moreover, $\langle a \rangle \cap \langle c \rangle = \{1\}$ and $|\langle a \rangle \langle c \rangle| = (p-1)p^{m-1}$ implies that $U(p^m) \cong \mathbf{Z}_{p^{m-1}} \times \mathbf{Z}_{p-1}$. Let $V = \langle a \rangle \cong \mathbf{Z}_{p^{m-1}}$ and $B = \langle c \rangle \cong \mathbf{Z}_{p-1}$. Then there exists unique $l_1, l_2 \in \mathbf{Z}$ such that $g = a^{l_1} c^{l_2}$. Furthermore, let $l \in \mathbf{Z}$ and note that $g^l = a^{ll_1} c^{ll_2}$. It follows that $a^{ll_1} \equiv 1 \bmod p$ since $a \equiv 1 \bmod p$. Now, let $i \in U(p^m)$. Then we have shown that there exists unique $v \in V$ and $b \in B$ such that $i = vb$ with $v \equiv 1 \bmod p$.

**Claim 12** *Let $\phi = \begin{bmatrix} i & r \\ j & 1 \end{bmatrix} \in \mathrm{Aut}(P)$. Then there exist $\nu \in V, \beta \in B$, and $j' \in \mathbf{Z}_p$ such that $\phi = \theta_1 \circ \theta_2$, where $\theta_1 = \begin{bmatrix} \nu & r \\ j' & 1 \end{bmatrix}$ and $\theta_2 = \begin{bmatrix} \beta & 0 \\ 0 & 1 \end{bmatrix}$.*

Proof. Let $i = vb$, where $v \in V$ and $b \in B$ as in the discussion above. Also, let $j' = jb^{-1}$ and consider $\Lambda(j', b)$. As an element of $U(p^m)$, we can write

$\Lambda(j',b) = wb$ where $w \in V$ and $w \neq 1$. Now let $\nu = vw^{-1}$ and $\beta = b$, and note that $\nu \in V$ since $v, w^{-1} \in V$. It follows that $\nu\Lambda(j',b) = vw^{-1}wb = vb = i$. Now, consider

$$\begin{aligned}(\theta_1 \circ \theta_2)(x) = \left(\begin{bmatrix} \nu & r \\ j' & 1 \end{bmatrix} \circ \begin{bmatrix} \beta & 0 \\ 0 & 1 \end{bmatrix}\right)(x) &= (x^\nu y^{j'})^\beta \\ &= x^{\nu\Lambda(j',\beta)} y^{j'\beta} \\ &= x^{\nu\Lambda(j',b)} y^{j'b} \\ &= x^i y^j \\ &= \phi(x).\end{aligned}$$

Similarly, $(\theta_1 \circ \theta_2)(y) = \left(\begin{bmatrix} \nu & r \\ j' & 1 \end{bmatrix} \circ \begin{bmatrix} \beta & 0 \\ 0 & 1 \end{bmatrix}\right)(y) = x^r y = \phi(y)$. This implies that $\phi = \theta_1 \circ \theta_2$.

□

**Proposition 13** *Let* $L = \left\{ \begin{bmatrix} v & r \\ j' & 1 \end{bmatrix} \middle| \begin{array}{l} v \in V \\ r \equiv 0 \bmod p^{m-1} \\ j' \in \mathbf{Z}_p \end{array} \right\}$ *and let* $\mathcal{L}$ *be the corresponding subset of Aut(P). Then* $\mathcal{L} = S_p$*, the unique Sylow p-subgroup of Aut(P).*

Proof. From Sylow theory we know that $|\mathrm{Aut}(P)| = p^{m+1}(p-1)$ implies that $\mathrm{Aut}(P)$ has a unique Sylow $p$-subgroup of order $p^{m+1}$. In order to prove $\mathcal{L} = S_p$ we may show that $\mathcal{L} \leq \mathrm{Aut}(P)$ and $|\mathcal{L}| = p^{m+1}$.

It can be proved that $\mathcal{L} \leq \mathrm{Aut}(P)$ by showing that $\mathcal{L}$ satisfies the axioms of closure and existence of inverse.

a) Closure: Let $l_1 = \begin{bmatrix} v_1 & r_1 \\ j_1' & 1 \end{bmatrix}$ and $l_2 = \begin{bmatrix} v_2 & r_2 \\ j_2' & 1 \end{bmatrix} \in \mathcal{L}$. We must show that $(l_1 \circ l_2) \in \mathcal{L}$.

$$\begin{aligned}\text{Consider} \quad (l_1 \circ l_2)(x) &= l_1\left(x^{v_2} y^{j_2'}\right) \\ &= \left(x^{v_1} y^{j_1'}\right)^{v_2} (x^{r_1} y)^{j_2'} \\ &= x^{v_1\Lambda(j_1',v_2) + r_1\Lambda(1,j_2')\alpha^{j_1'v_2}} y^{j_1'v_2 + j_2'}.\end{aligned}$$

Hence we need the following relations to hold.

$$\begin{aligned} &i) \quad j_1'v_2 + j_2' \in \mathbf{Z}_p \\ &ii) \quad v_1\Lambda(j_1',v_2) + r_1\Lambda(1,j_2')\alpha^{j_1'v_2} \in V.\end{aligned}$$

By definition, $(i)$ is true. In order to show that $v_1\Lambda(j_1',v_2) + r_1\Lambda(1,j_2')\alpha^{j_1'v_2} \in V$, we must prove that $\left[v_1\Lambda(j_1',v_2) + r_1\Lambda(1,j_2')\alpha^{j_1'v_2}\right]^{p^k} \equiv 1 \bmod p^m$, for some $1 \leq k \leq m-1$. The binomial expansion of this polynomial is equal to

$$[v_1\Lambda(j_1',v_2)]^{p^k} + \begin{pmatrix} p^k \\ 1 \end{pmatrix} [v_1\Lambda(j_1',v_2)]^{p^k-1} \left[r_1\Lambda(1,j_2')\alpha^{j_1v_2}\right] + \cdots$$

$$\cdots + \begin{pmatrix} p^k \\ p^k - 1 \end{pmatrix} [v_1\Lambda(j_1', v_2)] \left[r_1\Lambda(1, j_2')\alpha^{j_1' v_2}\right]^{p^k - 1} + \left[r_1\Lambda(1, j_2')\alpha^{j_1' v_2}\right]^{p^k}.$$

Now, notice that each term in the binomial expansion which contains a factor of $r_1\Lambda(1, j_2')\alpha^{j_1' v_2}$ is equivalent to 0 $\bmod p^m$ since $r_1 \equiv 0 \bmod p^{m-1}$ and each of these terms will have a coefficient which is divisible by $p$. The only exception is the final term of the expansion, but this is raised to a power of $p$ so it is equivalent to 0 $\bmod p^m$ also. Therefore we must simply check to see if $[v_1\Lambda(j_1', v_2)]^{p^k} \equiv 1 \bmod p^m$.

First note that $\Lambda(j_1', v_2) \equiv v_2 \bmod p^{m-1}$. Thus, $\Lambda(j_1', v_2) = v_2 + cp^{m-1}$ for some constant $c \in \mathbf{Z}$. This implies that $|\Lambda(j_1', v_2)| = |v_2 + cp^{m-1}|$. Now, using binomial expansion we see that $|v_2 + cp^{m-1}| \leq |v_2| = p^l$, for some $1 \leq l \leq m-1$. It follows that $|\Lambda(j_1', v_2)|$ is equal to some power of $p$, so $\Lambda(j_1', v_2) \in V$.

$$\begin{aligned} \text{Thus,} \quad & v_1\Lambda(j_1', v_2) \in V \\ \Rightarrow \quad & \left(v_1\Lambda(j_1', v_2) + r_1\Lambda(1, j_2')\alpha^{j_1' v_2}\right)^{p^k} \equiv 1 \bmod p^m, \quad \text{for} \quad 1 \leq k \leq m-1 \\ \Rightarrow \quad & v_1\Lambda(j_1', v_2) + r_1\Lambda(1, j_2')\alpha^{j_1' v_2} \in V. \end{aligned}$$

$$\begin{aligned} \text{Next we consider} \quad (l_1 \circ l_2)(y) &= l_1(x^{r_2} y) \\ &= (x^{v_1} y^{j_1'})^{r_2} (x^{r_1} y) \\ &= x^{v_1\Lambda(j_1', r_2) + r_1\alpha^{j_1' r_2}} y^{j_1' r_2 + 1}. \end{aligned}$$

Hence we need the following relations to hold.

$$\begin{aligned} &i) \quad j_1' r_2 + 1 \equiv 1 \bmod p \\ &ii) \quad v_1\Lambda(j_1', r_2) + r_1\alpha^{j_1' r_2} \equiv 0 \bmod p^{m-1} \end{aligned}$$

Both of these items follow immediately from the fact that $r_2 \equiv 0 \bmod p^{m-1}$.
b) Inverse: From Proposition 10, we already know that for any $l = \begin{bmatrix} v & r \\ j' & 1 \end{bmatrix}$ there exists a unique $l^{-1} = \begin{bmatrix} a & d \\ c & 1 \end{bmatrix}$ such that $l^{-1} \circ l = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. The values of $a, c$, and $d$ are derived as $a = [\Lambda(c, v) - \Lambda(c, r)\Lambda(1, j')\alpha^{cv}]^{-1}$, $c = -j'v^{-1}$, and $d = -[\Lambda(c, v) - \Lambda(c, r)\Lambda(1, j')\alpha^{cv}]^{-1} \Lambda(c, r)$. Our next task is to show if $l^{-1} = \begin{bmatrix} a & d \\ c & 1 \end{bmatrix}$, then $l^{-1} \in L$ by verifying the following.

$$\begin{aligned} &i) \quad a \in V \\ &ii) \quad c \in \mathbf{Z}_p \\ &iii) \quad d \equiv 0 \bmod p^{m-1} \end{aligned}$$

From the proof of Proposition 10 we have already shown that $l^{-1} \in \mathrm{Aut}(P)$ implies that $a, c$, and $d$ satisfy the conditions of Proposition 1. Thus, $(ii)$ and $(iii)$ are accounted for. In order to prove $a \in V$, we must show that $a^{p^k} \equiv 1 \bmod p^m$ for some $1 \leq k \leq m-1$. For ease of computation, we use the fact that $|a| = |a^{-1}|$ and instead show that $\left[a^{-1}\right]^{p^k} \equiv 1 \bmod p^m$ by expanding $\left[a^{-1}\right]^{p^k}$ below.

$$\begin{aligned}\left[a^{-1}\right]^{p^k} &= [\Lambda(c,v) - \Lambda(c,r)\Lambda(1,j')\alpha^{cv}]^{p^k} \\ &= \Lambda(c,v)^{p^k} - \begin{pmatrix} p^k \\ 1 \end{pmatrix} [\Lambda(c,v)]^{p^k-1} [\Lambda(c,r)\Lambda(1,j')\alpha^{cv}] + \cdots + \\ &\quad \begin{pmatrix} p^k \\ p^k - 1 \end{pmatrix} \Lambda(c,v) [\Lambda(c,r)\Lambda(1,j')\alpha^{cv}]^{p^k-1} - [\Lambda(c,r)\Lambda(1,j')\alpha^{cv}]^{p^k}.\end{aligned}$$

Now, notice that $\Lambda(c,r) \equiv 0 \bmod p^{m-1}$ implies that each term in the binomial expansion which includes a factor of $\Lambda(c,r)$ is equivalent to $0 \bmod p^m$ since each of these terms will either be raised to a power of $p$ or be multiplied by a coefficient which is divisible by $p$. Therefore, we may simply check to see if $[\Lambda(c,v)]^{p^k} \equiv 1 \bmod p^m$.

First note that $\Lambda(c,v) \equiv v \bmod p^{m-1}$. Thus, $\Lambda(c,v) = v + kp^{m-1}$ for some $k \in \mathbf{Z}$. This implies that $|\Lambda(c,v)| = |v + kp^{m-1}|$. Now, using binomial expansion we see that $|v+kp^{m-1}| \leq |v| = p^l$, for some $1 \leq l \leq m-1$. It follows that $|\Lambda(c,v)|$ is equal to some power of $p$. Thus, $a^{p^k} \equiv 1 \bmod p^m$ for some $1 \leq k \leq m-1$, which implies that $a \in V$. It follows that $\mathcal{L} \leq \mathrm{Aut}(P)$.

We now show that $|\mathcal{L}| = p^{m+1}$. First note that $v, j'$, and $r$ completely and uniquely determine each matrix representation of an automorphism in $\mathcal{L}$. This implies that the order of $\mathcal{L}$ is completely determined by the possible combinations of $v, j'$, and $r$. There are $p$ choices for $j'$ since $j' \in \mathbf{Z}_p$, $p^{m-1}$ choices for $v$ since $v \in V$, and $p$ choices for $r$. It follows that $|\mathcal{L}| = p^{m-1} * p * p = p^{m+1} = |S_p|$. Combining this with the fact that $\mathrm{Aut}(P)$ has a unique $p$-Sylow subgroup of order $p^{m+1}$, the conclusion can be made that $\mathcal{L} = S_p$.

□

**Theorem 14** $\mathrm{Aut}(P) \cong S_p \rtimes \mathbf{Z}_{p-1}$.

Proof. Recall from Claim 12 that any automorphism $\phi$ in $\mathrm{Aut}(P)$ can be represented as $\phi = \begin{bmatrix} i & r \\ j & 1 \end{bmatrix} = \begin{bmatrix} v & r \\ j' & 1 \end{bmatrix} \circ \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix}$ where $v \in V$, $r \equiv 0 \bmod p^{m-1}$, $j' = jb^{-1} \in \mathbf{Z}_p$, and $b \in B$, the subgroup of $U(p^m)$ that is isomorphic to $\mathbf{Z}_{p-1}$.

Let $\hat{B} = \left\{ \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix} | b \in B \cong \mathbf{Z}_{p-1} \right\}$ and let $\hat{\mathcal{B}}$ be the corresponding subgroup of $\mathrm{Aut}(P)$. We now check to see whether $\mathrm{Aut}(P) \cong \mathcal{L} \rtimes \hat{\mathcal{B}}$ by confirming the following items.

$$\begin{aligned} &i) \quad \mathcal{L} \cap \hat{\mathcal{B}} = e \\ &ii) \quad \mathcal{L}\hat{\mathcal{B}} = \mathrm{Aut}(P) \\ &iii) \quad \mathcal{L} \lhd \mathrm{Aut}(P) \end{aligned}$$

Again by Claim 12 we see that $(ii)$ is true, while $(i)$ is confirmed by inspection. Similarly, $\mathcal{L} = S_p$ implies that $\mathcal{L} \lhd \mathrm{Aut}(P)$, so $(iii)$ holds also.

□

The author first determined the structure of the automorphism group of some metacyclic 2-groups while a student in an Abstract Algebra II course at

St. Olaf College. The study of automorphism groups progressed to include metacyclic $p$-groups of odd order as an independent research project under the direction of Professor Jill Dietz.

# References

[1] Huppert, B. *Endliche Gruppen I.* Grundlehren der Mathematischen Wissenchaften 134. Berlin: Springer-Verlag, 1967.

[2] Ireland, K., and M. Rosen. *A Classical Introduction To Modern Number Theory, 2nd Ed.* Graduate Texts in Mathematics 84. New York: Springer-Verlag, 1990.

[3] Johnson, D. L. *Presentations of Groups.* Cambridge [Eng.]; New York: Cambridge University Press, 1976.

[4] Liedahl, S. "Presentations of Metacyclic $p$-Groups with Applications to $K$-Admissibility Questions." *Journal of Algebra* 169, no. 3 (1994): 965-983.

[5] Robinson, D. *A Course in the Theory of Groups.* New York: Springer-Verlag, 1996.