On quasi-inner automorphisms of a finite $p$-group

By IZABELA MALINOWSKA* (Bialystok)

In [3] Jonah and Konvisser constructed a $p$-group of order $p^8$, whose the automorphism group is elementary abelian of order $p^{16}$. Later a lot of $p$-groups satisfying similar properties have been found. The most interesting one was presented in [1] by Heineken. In fact it has been found a class of finite $p$-groups all of whose normal subgroups are characteristic. All these groups are of nilpotency class 2, they have exponent $p^2$ and their automorphism groups are $p$-groups. Each automorphism $\varphi$ of the $p$-group $G$ of this class satisfies the following condition: for every $g$ in $G$ there exists $h$ in $G$ such that $\varphi(g) = g^h$. We call it a quasi-inner automorphism.

Until recently there were no examples of $p$-groups of class larger than 2 with all automorphisms quasi-inner. In this paper we present an example of a $p$-group of class 3 and order $p^6$ ($p > 3$) with such a property. We also show that for every $r > 2$ there exists a $p$-group $P$ of class $r$ with a quasi-inner automorphism (which is not inner).

Throughout the paper terminology and notation will follow [2,4].

Let $G$ be a group generated by $a, b, c, d$ with the following relations

\[
[a, b] = a^p \quad [a, c] = d \quad [a, d] = b^p
\]
\[
[b, c] = a^{pm}b^{pk} \quad [b, d] = 1 \quad [d, c] = a^{pl},
\]

\[a^{p^2} = b^{p^2} = c^p = d^p = 1, \text{ where } p > 3 \text{ and } k, l, m \not\equiv 0 \pmod{p}.
\]

It is easily seen that $G$ is a $p$-group of order $p^6$ and of nilpotency class 3. Moreover

\[(1) \quad Z(G) = \langle a^p, b^p \rangle\]

*Supported by Polish scientific grant R.P.I.10
\( G' = \langle a^p, b^p, d \rangle \)

(3) \( \Omega_1(G) = \langle c, d, Z(G) \rangle \)

(4) \( \Omega_1(G)' = \langle a^p \rangle \).

**Theorem 1.** All automorphisms of \( G \) are quasi-inner if and only if \( A = m^2 + 4kl \) is a quadratic non-residue for \( p \).

**Proof.** Let \( A \) be a quadratic non-residue for \( p \). The commutator relations imply that

(5) \( C_G(G') = \langle b, G' \rangle \).

Of course \( C_G(G') \) is characteristic in \( G \).

Let \( \varphi \) be an automorphism of \( G \). Then by (2), (3) and (5) \( \varphi \) maps \( b \) to \( b^\alpha d^\beta \) \((\text{mod } Z(G))\), \( c \) to \( c^\gamma d^\delta \) \((\text{mod } Z(G))\) and \( d \) to \( d^\varepsilon \) \((\text{mod } Z(G))\) \((\alpha, \beta, \gamma, \delta, \varepsilon \in \mathbb{Z})\). Furthermore by (4) \( \varphi \) takes \( a \) to \( a^\zeta c^\eta d^\vartheta \) \((\text{mod } Z(G))\) \((\zeta, \eta, \vartheta \in \mathbb{Z})\). Applying \( \varphi \) to the third and the first relations gives \( \eta \equiv 0 \) \((\text{mod } p)\), \( \alpha \equiv 1 \) \((\text{mod } p)\), \( \beta \equiv 0 \) \((\text{mod } p)\) and

(6) \( \zeta \cdot \varepsilon \equiv 1 \) \((\text{mod } p)\).

Applying it to the fourth relation gives \( \gamma \equiv 1 \) \((\text{mod } p)\) and \( \zeta \equiv 1 \) \((\text{mod } p)\). Then \( \varepsilon \equiv 1 \) \((\text{mod } p)\) by (6). So each automorphism \( \varphi \) of \( G \) has the form:

\[
\varphi(a) \equiv ad^r, \quad \varphi(b) \equiv b,
\]
\[
\varphi(c) \equiv cd^s, \quad \varphi(d) \equiv d \pmod{Z(G)}
\]

where \( \varepsilon \in \mathbb{Z} \).

This means that \( \varphi \) is the \( p \)-automorphism of \( G \) which induces the identity on \( G/\Phi(G) \). Moreover for \( g = a^\alpha b^\beta c^\gamma d^\delta \) \((\alpha, \beta, \gamma, \delta \in \mathbb{Z})\) we have

\[
\varphi(g) = g \cdot d^{\alpha + s\gamma} \cdot a^{pr} b^{p\lambda}
\]

for some \( \kappa, \lambda \in \mathbb{Z} \). We show that \( \varphi \) maps each element \( g \) to one of its conjugates. To do this we need to find integers \( t, x, y, z \) such that for \( h = a^tb^xc^yd^z \)

(7) \( \varphi(g) = g^h \).

A straightforward computation gives

\[
g^h = g \cdot d^{\mu - \gamma t} a^{p(\mu + (\alpha - m\gamma)x + l\gamma z)} \cdot b^{p(\nu - k\gamma x + \alpha z)}
\]

where \( \mu, \nu \) are expressed in terms of \( t, y, \alpha, \beta, \gamma, \delta \). Thus the equality (7) implies

(8) \( \alpha y - \gamma t \equiv r\alpha + s\gamma \pmod{p} \).
If \( \alpha \neq 0 \) or \( \gamma \neq 0 \), then there is \( y \) and \( t \) satisfying the equation (8). Hence for \( L_1 = \kappa - \mu \), \( L_2 = \lambda - \nu \)

\[
\begin{align*}
(\alpha - m\gamma)x - l\gamma z &\equiv L_1 \pmod{p} \\
-k\gamma x + \alpha z &\equiv L_2 \pmod{p}.
\end{align*}
\]

For \( \alpha \neq 0 \) the system of equations (9) has a unique solution \((x, z)\) if and only if

\[
\det \begin{bmatrix} \alpha - m\gamma & -l\gamma \\ -k\gamma & \alpha \end{bmatrix} \neq 0 \pmod{p},
\]

which is equivalent to

\[
\alpha^2 - m\gamma \alpha - kl\gamma^2 \neq 0 \pmod{p}
\]
i.e. if and only if \( A = m^2 + 4kl \) is a quadratic non-residue for \( p \).

Now assume \( \alpha \equiv 0 \pmod{p} \). Thus the system (9) has the form

\[
\begin{align*}
-m\gamma x - l\gamma z &\equiv L_1 \\
-k\gamma x &\equiv L_2.
\end{align*}
\]

It has a unique solution \((x, z)\) if and only if \( l \neq 0 \), \( k \neq 0 \pmod{p} \) which are satisfied by the assumptions.

Suppose that \( \alpha \equiv 0 \) and \( \gamma \equiv 0 \). Then we take \( x \equiv 0 \), \( z \equiv 0 \) and have

\[
\begin{align*}
-\beta t + (m\beta + l\delta)y &\equiv M_1 \pmod{p} \\
-\delta t + k\beta y &\equiv M_2 \pmod{p}
\end{align*}
\]

for some \( M_1, M_2 \in \Z \) which are expressed in terms of \( \beta, \delta \).

Similarly it can be found \((t, y)\) being the solution of (10).

Now let \( \varphi \) be the automorphism of \( G \) such that

\[
\varphi(a) = ad, \ \varphi(b) = ba^{pm}b^p, \ \varphi(c) = cd, \ \varphi(d) = da^{pl}b^p.
\]

Assume that \( \varphi \) is quasi-inner and \( A \) is a quadratic residue for \( p \). Consider an element \( b^\beta d^\delta \in G \) such that \( \beta, \delta \in \Z \). It follows from the definition of a quasi-inner automorphism of \( G \) that there is an element \( h = a^t b^x c^y d^z \) such that

\[
\varphi(g) = g^h \quad (t, x, y, z \in \Z).
\]

Notice that

\[
\varphi(g) = g \cdot a^{p(m\beta + l\delta)}b^{p(k\beta + \delta)} \quad \text{and} \quad g^h = g \cdot a^{p(m\beta y + l\delta y - \beta t)}b^{p(k\beta y - \delta t)} , \quad \text{so}
\]

\[
\begin{align*}
-\beta t + (m\beta + l\delta)y &\equiv m\beta + l\delta \pmod{p} \\
-\delta t + k\beta y &\equiv k\beta + \delta \pmod{p}
\end{align*}
\]
and this system of equations has a solution \((t, y)\) i.e.

\[
\begin{bmatrix}
-\beta & m\beta + l\delta \\
-\delta & k\beta
\end{bmatrix} = \begin{bmatrix}
-\beta & m\beta + l\delta \\
-\delta & k\beta
\end{bmatrix}
\]

Let \(\mathfrak{A}\) be the coefficient matrix of the system \((10)\) and \(\mathfrak{B}\) be the augmented matrix of this system.

Since \(A\) is a quadratic residue for \(p\), there is \(\beta \neq 0, \delta \neq 0\) such that the rank \(r(\mathfrak{A}) = 1\). Therefore \(r(\mathfrak{B}) = 1\), but it is easy to see that \(r(\mathfrak{B}) = 2\). This gives a contradiction. \(\Box\)

Now let \(P\) be a group generated by \(a, b, c, d, x, y\) with the following relations:

\[
\begin{align*}
a^p b^r &= c^p = d^p = x^p = y^p = 1 \\
[a, b] &= a^p [a, c] = b^{p-1} [b, c] = 1 \\
[a, d] &= c [b, d] = b^{p-1} k [c, d] = a^{p-1} m b^{p-1} n \\
[a, x] &= [c, x] = [a, y] = [c, y] = 1 \\
[x, y] &= a^{p-1} m b^{p-1} n [b, y] = 1 \\
[b, x] &= a^{p-1} [d, x] = 1 \\
[d, y] &= a^{p-1} l
\end{align*}
\]

where \(p > 5, r > 2, k, m, n, l \neq 0 \pmod{p}\). One can easily show that \(G\) is regular and of nilpotency class \(r\).

**Theorem 2.** \(P\) has a quasi-inner automorphism which is not inner.

**Proof.** Let \(\varphi\) be an automorphism of \(P\) such that

\[
\varphi(a) = a, \quad \varphi(b) = b, \quad \varphi(c) = c, \quad \varphi(d) = d a^{p-1}, \quad \varphi(x) = x, \quad \varphi(y) = y.
\]

\(\varphi\) is not inner since \(C_P(x) \cap C_P(y) \cap C_P(c) = \langle a^p, b^p, c \rangle\).

If \(g = a^\alpha b^\beta c^\gamma d^\delta x^\lambda y^\mu\) for \(\alpha, \beta, \gamma, \delta, \lambda, \mu \in \mathbb{Z}\), then

\[
\varphi(g) = g \cdot a^{p-1} \delta.
\]

We need to find an element \(h\) such that \(\varphi(g) = g^h\). Of course if \(\delta \equiv 0 \pmod{p}\) then \(\varphi(g) = g\). Assume that \(\delta \not\equiv 0 \pmod{p}\).

If \(\alpha \not\equiv 0 \pmod{p}\), then we take \(h = b^{p-2} t\). Hence we get \(\alpha t \equiv \delta \pmod{p}\) by \((12)\). Clearly there exists \(t\) satisfying this equation.

If \(\beta \not\equiv 0 \pmod{p}\), then we take \(h = a^{p-2} t\). Thus we get \(-\beta t \equiv \delta \pmod{p}\) by \((12)\).
Assume that $\alpha \equiv 0$, $\beta \equiv 0 \pmod{p}$. Now we take $h = c^t y^w$. Thus

$$g^h = g \cdot a^{p^r-1}(-m\delta t + l\delta w + m\lambda w)b^{p^r-1}(-n\delta t + n\lambda w).$$

Hence by (12)

$$\begin{cases}
-m\delta t + (l\delta + m\lambda)w \equiv \delta \pmod{p} \\
-n\delta t + n\lambda w \equiv 0 \pmod{p}.
\end{cases}$$

This equation has a unique solution $(t, w)$ if and only if

$$\det \begin{bmatrix}
-m\delta & l\delta + m\lambda \\
-n\delta & n\lambda
\end{bmatrix} \not\equiv 0 \pmod{p},$$

i.e. if and only if $\delta \not\equiv 0 \pmod{p}$. □

References