Publ. Math. Debrecen
41 / 1–2 (1992), 73–77

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 φ 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 then 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

$$\begin{aligned} &[a,b] = a^p && [a,c] = d && [a,d] = b^p \\ &[b,c] = a^{pm}b^{pk} && [b,d] = 1 && [d,c] = a^{pl}, \end{aligned}$$

$a^{p^2} = b^{p^2} = c^p = d^p = 1$, where $p > 3$ 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

$$Z(G) = \langle a^p, b^p \rangle \tag{1}$$

*Supported by Polish scientific grant R.P.I.10

(2) $$G' = \langle a^p, b^p, d\rangle$$

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

(6) $$\zeta \cdot \varepsilon \equiv 1 \pmod p.$$

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

$$\begin{aligned} &\varphi(a) \equiv ad^r, \quad \varphi(b) \equiv b,\\ &\varphi(c) \equiv cd^s, \quad \varphi(d) \equiv d \pmod{Z(G)}\\ &\text{where } r, s \in \mathbf{Z}. \end{aligned}$$

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

$$\varphi(g) = g \cdot d^{r\alpha + s\gamma} \cdot a^{p\kappa} b^{p\lambda}$$

for some $\kappa, \lambda \in \mathbf{Z}$. We show that φ maps each element g to one of its conjugates. To do this we need to find integers t, x, y, z such that for $h = a^t b^x c^y d^z$

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

A strightforward computation gives

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

where μ, ν 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 $\alpha \not\equiv 0$ or $\gamma \not\equiv 0$, then there is y and t satisfying the equation (8). Hence for $L_1 = \kappa - \mu$, $L_2 = \lambda - \nu$

$$\left\{ \begin{array}{l} (\alpha - m\gamma)x - l\gamma z \equiv L_1 \pmod{p} \\ -k\gamma x + \alpha z \equiv L_2 \pmod{p}. \end{array} \right. \tag{9}$$

For $\alpha \not\equiv 0$ the system of equations (9) has a unique solution (x, z) if and only if

$$\det \begin{bmatrix} \alpha - m\gamma & -l\gamma \\ -k\gamma & \alpha \end{bmatrix} \not\equiv 0 \pmod{p},$$

which is equivalent to

$$\alpha^2 - m\gamma\alpha - kl\gamma^2 \not\equiv 0 \pmod{p}$$

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

$$\left\{ \begin{array}{ll} -m\gamma x - l\gamma z & \equiv L_1 \\ -k\gamma x & \equiv L_2. \end{array} \right.$$

It has a unique solution (x, z) if and only if $l \not\equiv 0$, $k \not\equiv 0 \pmod{p}$ 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

$$\left\{ \begin{array}{ll} -\beta t + (m\beta + l\delta)y & \equiv M_1 \pmod{p} \\ -\delta t + k\beta y & \equiv M_2 \pmod{p} \end{array} \right. \tag{10}$$

for some M_1, $M_2 \in \mathbf{Z}$ which are expressed in terms of β, δ.

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

Now let φ be the automorphism of G such that

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

Assume that φ is quasi-inner and A is a quadratic residue for p. Consider an element $b^\beta d^\delta \in G$ such that $\beta, \delta \in \mathbf{Z}$. 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

$$\varphi(g) = g^h \quad (t, x, y, z \in \mathbf{Z}).$$

Notice that

$$\begin{aligned} \varphi(g) &= g \cdot a^{p(m\beta + l\delta)} b^{p(k\beta + \delta)} \text{ and} \\ g^h &= g \cdot a^{p(m\beta y + l\delta y - \beta t)} b^{p(k\beta y - \delta t)}, \text{ so} \end{aligned}$$

$$\left\{ \begin{array}{ll} -\beta t + (m\beta + l\delta)y & \equiv m\beta + l\delta \pmod{p} \\ -\delta t + k\beta y & \equiv k\beta + \delta \pmod{p} \end{array} \right. \tag{11}$$

and this system of equations has a solution (t, y) i.e.

$$r\begin{bmatrix} -\beta & m\beta + l\delta \\ -\delta & k\beta \end{bmatrix} = r\begin{bmatrix} -\beta & m\beta + l\delta & m\beta + l\delta \\ -\delta & k\beta & k\beta + \delta \end{bmatrix}$$

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 $\beta \not\equiv 0$, $\delta \not\equiv 0$ 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. $\square$

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

$$a^{p^r} = b^{p^r} = c^p = d^p = x^p = y^p = 1$$

$$[a, b] = a^p \qquad [a, c] = b^{p^{r-1}} \qquad [b, c] = 1$$

$$[a, d] = c \qquad [b, d] = b^{p^{r-1}k} \qquad [c, d] = a^{p^{r-1}m} b^{p^{r-1}n}$$

$$[a, x] = [c, x] = [a, y] = [c, y] = 1$$

$$[x, y] = a^{p^{r-1}m} b^{p^{r-1}n} \qquad [b, y] = 1$$

$$[b, x] = a^{p^{r-1}} \qquad [d, y] = a^{p^{r-1}l}$$

$$[d, x] = 1$$

where $p > 5$, $r > 2$, $\quad k, m, n, l \not\equiv 0 \pmod p$. 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 φ be an automorphism of P such that

$$\varphi(a) = a,\ \varphi(b) = b,\ \varphi(c) = c,\ \varphi(d) = da^{p^{r-1}},\ \varphi(x) = x,\ \varphi(y) = y.$$

φ 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 $\alpha, \beta, \gamma, \delta, \lambda, \mu \in \mathbf{Z}$, then

$$\varphi(g) = g \cdot a^{p^{r-1}\delta}. \tag{12}$$

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 $h = b^{p^{r-2}t}$. 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 $h = a^{p^{r-2}t}$. Thus we get $-\beta t \equiv \delta \pmod p$ by (12).

Assume that $\alpha \equiv 0$, $\beta \equiv 0 \,(\mathrm{mod}\, p)$. 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)

$$\begin{cases} -m\delta t + (l\delta + m\lambda)w & \equiv \delta \,(\mathrm{mod}\;\; p) \\ -n\delta t + n\lambda w & \equiv 0 \,(\mathrm{mod}\;\; p). \end{cases}$$

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

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

i.e. if and only if $\delta \not\equiv 0 \,(\mathrm{mod}\, p)$. $\square$

References

[1] H. Heineken, Nilpotente gruppen, deren sämtliche normalteiler charakteristish sind, *Arch. Math.* **33** (1979), 497–503.

[2] B. Huppert, Endliche Gruppen I., *Springer*, *Berlin*, 1967.

[3] D. Jonah and M. Konvisser, Some non-abelian p-groups with abelian automorphism groups, *Arch. Math.* Vol. **XXVI** (1975), 131–133.

[4] D. J. S. Robinson, A Course in the Theory of Groups, *Springer–Verlag*, *New–York*, 1982.

IZABELA MALINOWSKA
INSTITUTE OF MATHEMATICS
WARSAW UNIVERSITY, BIALYSTOK DIVISION
15––267 BIALYSTOK
AKADEMICKA 2

(Received December 27, 1990)