Rendiconti del Seminario Matematico della Università di Padova

Izabela Malinowska

On automorphism groups of finite p-groups

Rendiconti del Seminario Matematico della Università di Padova, tome 91 (1994), p. 265-271

<http://www.numdam.org/item?id=RSMUP_1994__91__265_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 91 (1994)

On Automorphism Groups of Finite p-Groups.

IZABELA MALINOWSKA (*) (**)

Numerous papers on automorphism groups of p-groups can be found in the literature. There are a lot of examples of p-groups, whose automorphism groups have a given structure. Most of them are of nilpotency class 2 and all their automorphisms are central. In [6] Jonah and Konvisser constructed a p-group of order p^8, whose the automorphism group is elementary abelian. In 1979 Heineken [4] found a class of finite p-groups all of whose normal subgroups are characteristic.

In this paper we answer the question of Caranti ([7], 11.46 b)) asking whether there exists a finite p-group G of nilpotency class greater than 2, with $\operatorname{Aut} G = \operatorname{Aut}_c G \cdot \operatorname{Inn} G$, where $\operatorname{Aut}_c G$ is the group of central automorphisms of G. We show that no group G of order up to $p^5 (p > 2)$ has the property $\operatorname{Aut} G = \operatorname{Aut}_c G \cdot \operatorname{Inn} G$. The p-group of the smallest order with this property has order p^6 and nilpotency class 3. We also show that for every prime $p > 2$ and every integer $n \geqslant 7$ there is a p-group G of order p^n with $\operatorname{Aut} G = \operatorname{Aut}_c G \cdot \operatorname{Inn} G$. Its automorphism group is a p-group of nilpotency class smaller than the nilpotency class of G. Throughout the paper terminology and notation will follow [1, 5].

Let G_1 be a group generated by a, b, c, d, x with the following relations: $a^{p^r} = b^{p^r} = c^p = d^p = x^p = 1$

(1) $[a, b] = a^p$, (2) $[a, c] = 1$,

(3) $[b, c] = 1$, (4) $[a, d] = b^{p^{r-1}}$,

(5) $[b, d] = 1$, (6) $[c, d] = a^{mp^{r-1}} b^{np^{r-1}}$,

(7) $[a, x] = a^{kp^{r-1}} b^{lp^{r-1}}$, (8) $[b, x] = 1$,

(9) $[c, x] = b^{p^{r-1}}$, (10) $[d, x] = c$,

(*) Indirizzo dell'A.: Institute of Mathematics, Warsaw University, Bialystok Division, Akademicka 2, 15-267 Bialystok, Poland.

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

where $p > 3$, $r > 1$ and $k, l, m, n \not\equiv 0 \pmod p$, or $p = 3$, $r > 1$, $k, l, m, n \not\equiv 0 \pmod 3$ and $ln \not\equiv 1 \pmod 3$.

One can easily show that the following subgroups of G_1 are characteristic:

$$Z(G_1) = \langle a^{p^{r-1}}, b^{p^{r-1}} \rangle, \tag{11}$$

$$\gamma_2(G_1) = \langle a^p, c, b^{p^{r-1}} \rangle, \tag{12}$$

$$\Omega_1(\gamma_2(G_1)) = \langle c, Z(G_1) \rangle, \tag{13}$$

$$C_{G_1}(\Omega_1(\gamma_2(G_1))) = \langle a, b, c \rangle, \tag{14}$$

$$A = \langle c, d, x, Z(G_1) \rangle, \tag{15}$$

$$C_{G_1}(A) = \langle a^p, b \rangle. \tag{16}$$

We show only that A is characteristic. Of course for $p > 5$. (G_1) is regular, so we have $A = \Omega_1(G_1)$. It is easily seen that this holds also for $p = 5$.

The case $p = 3$ is a little more complicated since the group G_1 as well as A is no longer regular. But it is easy to check that $\Omega_1(G_1) = \langle a^{3^{r-2}}, b^{3^{r-2}}, c, d, x \rangle$ since $a^{-m3^{r-2}} b^{(-n+1)3^{r-2}} d^2 x^2$ and $a^{-m3^{r-2}} b^{(-n-1)3^{r-2}} dx^2$ are in $\Omega_1(G_1)$. Furthermore

$$Z_2(G_1) = \langle a^{3^{r-2}}, b^{3^{r-2}}, c \rangle \quad \text{and} \quad \Omega_1(G_1) \leqslant Z_2(G_1) \cdot C_{G_1}(b).$$

Now, if d and x belong to $Z_2(G_1) \cdot C_{G_1}(a^\alpha b^\beta c^\gamma)$, it follows that $\alpha \equiv 0$ and $\gamma \equiv 0 \pmod 3$, so the subgroups $\langle a^3, b \rangle$, $\langle a^{3^{r-1}}, b^{3^{r-2}}, c, d, x \rangle = C_{\Omega_1(G_1)}(a^3, b)$ and $\Omega_1(\langle a^{3^{r-1}}, b^{3^{r-2}}, c, d, x \rangle) = A$ are characteristic in G_1.

PROPOSITION 1. $\operatorname{Aut} G_1 = \operatorname{Aut}_c G_1 \cdot \operatorname{Inn} G_1$.

PROOF. We prove the proposition for $r > 2$. The proof of the case $r = 2$ is similar.

Let φ be an automorphism of G_1. By (13)-(16) we see at once that $\varphi(c) \in \Omega_1(\gamma_2(G_1))$, $\varphi(a) \in C_{G_1}(c)$, $\varphi(b) \in C_{G_1}(A)$ and $\varphi(d), \varphi(x) \in A$. So the subgroups $H = \langle b^{p^{r-1}} \rangle$ and $B = \{ g \in G_1 \colon \forall h \in \gamma_2(G_1)\ h^g \equiv h \pmod H \} = \langle a, b^{p^{r-2}}, c, x \rangle$ are characteristic in G_1. Hence $\varphi(a) \in B \cap C_{G_1}(c) = \langle a, b^{p^{r-2}}, c \rangle$, $\varphi(x) \in \Omega_1(B) = \langle c, x, Z(G_1) \rangle$ and then

$$\varphi(a) \equiv a^\alpha b^{\beta p^{r-2}} c^\gamma,$$

$$\varphi(b) \equiv a^{\delta p} b^\varepsilon,$$

$$\varphi(c) \equiv c^{\zeta},$$
$$\varphi(d) \equiv c^{\eta} d^{\vartheta} x^{\iota},$$
$$\varphi(x) \equiv c^{\kappa} x^{\lambda},$$

where «$\equiv$» means «congruent modulo $Z(G_1)$».

Applying φ to the (1) and (7) relations gives $\beta \equiv 0 \pmod p$, $\varepsilon \equiv 1 \pmod{p^{r-1}}$, $\lambda \equiv 1 \pmod p$ and

$$l \equiv l\alpha + \gamma \pmod p. \tag{17}$$

Hence by (9) $\zeta \equiv 1 \pmod p$. Applying it to the (10) and (6) relations gives $\vartheta \equiv 1 \pmod p$, $\alpha \equiv 1 \pmod p$ and $\iota \equiv 0 \pmod p$, so by (17) $\gamma \equiv 0 \pmod p$. Now we see that each automorphism φ of G has the form:

$$\varphi(a) \equiv a^{1+\alpha\cdot p},$$
$$\varphi(b) \equiv b a^{\beta p},$$
$$\varphi(c) \equiv c,$$
$$\varphi(d) \equiv c^{\gamma} d,$$
$$\varphi(x) \equiv c^{\delta} x,$$

where $\alpha, \beta, \gamma, \delta \in Z$.

The number $1 + \alpha p$ can be expressed in the form $(1+p)^{\alpha'} \pmod{p^r}$. Now one can easily verify that φ acts as the conjugation by $b^{\alpha'} a^{-\beta} d^{-\delta} x^{\gamma}$ modulo $Z(G_1)$. Thus φ belongs to $\mathrm{Aut}_c G_1 \cdot \mathrm{Inn}\, G_1$, and then $\mathrm{Aut}\, G_1 = \mathrm{Aut}_c G_1 \cdot \mathrm{Inn}\, G_1$.

Let G_2 be a group generated by a, b, c, d, x, z with the following relations: $a^{p^r} = b^{p^r} = c^p = d^p = x^p = z^p = 1$

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

where $p > 2$, $r \geqslant 2$, $k, l, m, n \not\equiv 0 \pmod p$.

Symilarly as in the previous case it can be proved that

PROPOSITION 2. $\mathrm{Aut}\, G_2 = \mathrm{Aut}_c G_2 \cdot \mathrm{Inn}\, G_2$.

This shows that for all $n \geqslant 7$, there is a p-group G of order p^n with $\operatorname{Aut} G = \operatorname{Aut}_c G \cdot \operatorname{Inn} G$.

Now we shall see that the smallest p-group with this property has order p^6 and nilpotency class 3. First we show that there are no groups with this property of order p^4. We use the list of p-groups of order p^4 found in [2], pages 145-146. We use also the numbering of the groups as given replacing of P, Q, R, S, E respectively by a, b, c, d and 1. Since we want to find a group of nilpotency class greater than 2 only groups (xi), (xii), (xiii), (xv) should be considered. One can easily find for them automorphisms which do not belong to $\operatorname{Aut}_c G \cdot \operatorname{Inn} G$. For these groups we define such automorphisms by indicating images of generators. We have then

Group	a	b	c	d
(xi)	ac	b	c	
(xii)	a^{-1}	ba^p	c^{-1}	
(xiii)	a^{-1}	ba^p	c^{-1}	
(xv) $p > 3$	a	b	c	dc
(xv) $p = 3$	a^{-1}	b^{-1}	c	

Now let G be of order p^5. It is clear that G is metabelian and for $p > 3$ is regular.

Case 1. $\operatorname{cl} G = 4$.

Since $|G/\gamma_2(G)| = p^2$ and G is metabelian then by [3] $|\operatorname{Aut} G|$ is divisible by p^6. But $|\operatorname{Inn} G| = p^4$, $|\operatorname{Aut}_c G| = p^2$ and $|\operatorname{Inn} G \cap \operatorname{Aut}_c G| > 1$, so $|\operatorname{Aut}_c G \cdot \operatorname{Inn} G| \leqslant p^5$. Hence $\operatorname{Aut} G \neq \operatorname{Aut}_c G \cdot \operatorname{Inn} G$.

Case 2. $\operatorname{cl} G = 3$.

Let $G = \gamma_1(G) > \gamma_2(G) > \gamma_3(G) > \gamma_4(G) = 1$ be the lower central series of G. Since $|\gamma_i(G)/\gamma_{i+1}(G)| \geqslant p$ for $i = 1, 2, 3$, we have $p^2 \leqslant |G/\gamma_2(G)| \leqslant p^3$.

If G is metacyclic then $G = \langle a, b \colon a^{p^3} = b^{p^2} = 1,\ a^b = a^{1+p} \rangle$. It is easy to see that the correspondence:

$$a \to a^{-1}, \qquad b \to b$$

determines the automorphism of G which does not belong to $\mathrm{Aut}_c G \cdot \mathrm{Inn}\, G$.

Assume that G is not metacyclic.

If $|G/\gamma_2(G)| = p^2$, then $G/\gamma_2(G)$ has the type (p, p) and by Theorem 1.5 [1] $|\gamma_2(G)/\gamma_3(G)| = p$, $\gamma_3(G)$ is elementary abelian of order p^2. Of course $Z(G) = \gamma_3(G)$ and $Z_2(G) = \gamma_2(G)$. Let G be generated by elements a, b. Since G is not metacyclic and $\mho_1(\gamma_2(G)) \leqslant \gamma_3(G)$, by [5], III.11.3. $\mho_1(G) \leqslant Z(G)$ and so $(a^p)^b = a^p$. On the other hand we have

$$(a^b)^p = (a[a, b])^p = a^p [a, b]^{a^{p-1}} \cdot \ldots \cdot [a, b]^a [a, b] =$$

$$= a^p [a, b][a, b, a^{p-1}] \cdot \ldots \cdot [a, b][a, b, a][a, b] =$$

$$= a^p [a, b]^p [a, b, a]^{(p-1)p/2} = a^p [a, b]^p$$

since $\gamma_3(G) = Z(G)$ and $\gamma_3(G)$ is elementary abelian. So we get $\exp \gamma_2(G) = p$.

Now it is easy to see that the correspondence

$$a \to a^{-1}, \qquad b \to b^{-1}$$

determines the automorphism of G, which does not belong to $\mathrm{Aut}_c G \cdot \mathrm{Inn}\, G$.

If $|G/\gamma_2(G)| = p^3$, then by Theorem 1.5 [1] $|\gamma_2(G)/\gamma_3(G)| = |\gamma_3(G)| = p$.

Let $G/\gamma_2(G)$ be of the type (p^2, p). Since G is not metacyclic there exist a, b such that $G = \langle a, b\rangle$ and $a^{p^2}, b^p \in \gamma_3(G)$. By [5], III.11.3 $G/\gamma_3(G)$ is of the type (x) (see [2]). Then the correspondence

$$a \to a^{1+p}, \qquad b \to b$$

determines the automorphism of G, which does not belong to $\mathrm{Aut}_c G \cdot \mathrm{Inn}\, G$.

Let $G/\gamma_2(G)$ be of the type (p, p, p). If $Z(G) \neq \gamma_3(G)$, then G is either a direct product of groups A and B or a central product of groups A and C, where A is a group of order p^4 and class 3, B is a group of order p, C is a cyclic group of order p^2. In both cases we can extend considered automorphisms of the groups of order p^4 and class 3 to the whole group G. Of course such automorphisms do not belong to $\mathrm{Aut}_c G \cdot \mathrm{Inn}\, G$.

Therefore we may assume that $Z(G) = \gamma_3(G)$. Then by [5], III.2.13a) $Z_2(G)/Z(G)$ is of exponent p. Since $|G/Z_2(G)| = p^2$ we can choose a, b, c such that $G = \langle a, b, c\rangle$, $a^p, b^p \in \gamma_2(G)$, $c \in Z_2(G)$ and $c^p \in Z(G)$. Since $Z_2(G)$ is not cyclic ([5], III.7.7a)) either $\gamma_2(G)$ is elementary abelian or cyclic. In the second case there exists $c \in Z_2(G)$ such that $c^p = 1$. In both cases we can find b with $[b, c] = 1$, as $[a, c]$, $[b, c] \in Z(G) = \gamma_3(G)$. If $c^p = 1$, then the correspondence

$$a \to ac, \quad b \to b, \quad c \to c,$$

determines the automorphism of G, which does not belong to $\mathrm{Aut}_c G \cdot \mathrm{Inn}\, G$.

Assume that $c^p \neq 1$. Since $\gamma_2(G)$ is elementary abelian we have

$$[a^p, b] = [a, b]^{a^{p-1}} \cdot \ldots \cdot [a, b]^a [a, b] =$$

$$= [a, b][a, b, a^{p-1}] \cdot \ldots [a, b][a, b, a][a, b] = [a, b]^p [a, b, a]^{(p-1)p/2} = 1$$

so $a^p \in Z(G) = \langle c^p \rangle$ and in the similar way $b^p \in Z(G)$. So there exist a, b of orders p such that $G = \langle a, b, c \rangle$ and $[b, c] = 1$. If $[a, b, b] = 1$ then the correspondence

$$a \to a^{-1}, \quad b \to b, \quad c \to c,$$

determines the desired automorphism of G. If $[a, b, b] \neq 1$ then there exists a with $[a, b, a] = 1$. Hence the correspondence

$$a \to a, \quad b \to b^{-1}, \quad c \to c,$$

determines the automorphism of G, which does not belong to $\mathrm{Aut}_c G \cdot \mathrm{Inn}\, G$.

EXAMPLE. We end the paper with the example of the group G of order p^6 and class 3 with $\mathrm{Aut}\, G = \mathrm{Aut}_c G \cdot \mathrm{Inn}\, G$:

$$G = \langle a, b, c, d\colon\ a^{p^2} = b^{p^2} = c^p = d^p = 1,\ [a, b] = a^p,\ [a, c] = b^p,$$

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

where $p > 3$ and $k, l, m \neq 0 \pmod p$ or $p = 3$, $l = 1$, $k, m \neq 0 \pmod 3$.

REFERENCES

[1] N. BLACKBURN, *On a special class of p-groups*, Acta Math., **100** (1958), pp. 45-92.

[2] W. BURNSIDE, *Theory of Groups of Finite Order*, Cambridge University Press (1911).

[3] A. CARANTI - C. M. SCOPPOLA, *Endomorphisms of two-generated metabelian groups that induce the identity modulo the derived subgroup*, UTM, **286** (Ottobre 1989).
[4] H. HEINEKEN, *Nilpotente gruppen, deren sämtliche normalteiler characteristish sind*, Arch. Math., **33** (1979), pp. 497-503.
[5] B. HUPPERT, *Endliche Gruppen I*, Springer-Verlag, Berlin and New York (1967).
[6] D. JONAH - M. KONVISSER, *Some non-abelian p-groups with abelian automorphism groups*, Arch. Math., **26** (1975), pp. 131-133.
[7] *Kouroskaja tetrad'*, Nowosybirsk (1990).

Manoscritto pervenuto in redazione il 30 aprile 1992
e, in forma revisionata, il 28 novembre 1992.