Publ. Math. Debrecen
61 / 3-4 (2002), 495–509

Groups of p-automorphisms for finite p-groups

By JAN KREMPA (Warszawa) and IZABELA MALINOWSKA (Białystok)

Abstract. For any finite p-group G put $\mathrm{E}_p(G) = k$ if p^k is the order of a Sylow p-subgroup of $\mathrm{Aut}\, G$.

It is well known that if G is a group of order p^n then $\mathrm{E}_p(G) \leq n(n-1)/2$ and all p-groups for which this upper bound is achieved are described. On the other hand, for any noncyclic p-group G of order p^n, where $n \geq 3$, it is conjectured that $\mathrm{E}_p(G) \geq n$, and it is confirmed in several important cases.

Our aim in this paper is to study, if for any $n \leq r < n(n-1)/2$ there exists a group G of order p^n such that $\mathrm{E}_p(G) = r$. In particular we find all groups of order p^n, such that $\mathrm{E}_p(G) = n(n-1)/2 - 1$.

1. Introduction

In this paper G will always denote a nontrivial finite p-group, where p is a prime number, $A_p(G)$ a Sylow p-subgroup of $\mathrm{Aut}\, G$ and $\mathrm{E}_p(G) = \log_p |A_p(G)|$. Most of notation and terminology used here is standard. In particular, if N is a normal subgroup of a group G then:

$$\mathrm{Aut}^N(G) = \{\alpha \in \mathrm{Aut}\, G \mid N^\alpha = N \text{ and } g^{-1} \cdot g^\alpha \in N,\ \forall\, g \in G\},$$

$$\mathrm{Aut}^N_N(G) = \{\alpha \in \mathrm{Aut}^N(G) \mid n^\alpha = n \ \ \forall\, n \in N\}.$$

Further we will use some abbreviations for sums of natural numbers. Put $s(0) = s(1) = 0$ and $s(n) = (n-1) + \cdots + 1$ for any $n \geq 2$. If $1 \leq d \leq n$ put $s(n,d) = (n-1) + \cdots + (n-d) = s(n) - s(n-d)$. Clearly, for $n \geq 2$ we have $s(n) = s(n,n) = s(n,n-1)$.

Mathematics Subject Classification: 20D15, 20D45.
Key words and phrases: finite p-groups, p-automorphisms.

It is well known that if G is a cyclic group of order p^n then $\mathrm{E}_p(G) = n-1 = s(n,1)$ and, if G is an elementary abelian p-group of order p^n then $\mathrm{E}_p(G) = n(n-1)/2 = s(n,n)$.

The following general result about the upper bound of $\mathrm{E}_p(G)$ is in fact due to P. Hall (see [11] 5.3.3):

Theorem 1.1. *Let G be a group of order p^n generated by d elements. Then $\mathrm{E}_p(G) \leq s(n,d)$. In particular, $\mathrm{E}_p(G) \leq s(n)$.*

G. A. Miller has known the last estimation and, in a paper [9] from 1911, he described all groups G of order p^n with $\mathrm{E}_p(G) = s(n)$ (for details see Theorems 3.2 and 4.6 below).

For the lower bound of $\mathrm{E}_p(G)$ situation is much more complicated. In particular we have the following well known conjecture (see [6], 12.77): *If G is any noncyclic p-group of order at least p^3, then $|G| \mid |\mathrm{Aut}(G)|$ or, equivalently*, $\log_p |G| \leq \mathrm{E}_p(G)$. This conjecture is confirmed, among other cases, for abelian groups, groups of order at most p^7 and for groups of maximal class (see [3], [4], [10]). Inspired by above mentioned results, and some others, we shall consider here the following problems:

1. *Let $n \geq 3$ and $s(n) > k \geq n$. Find a group G_{nk} of order p^n such that $\mathrm{E}_p(G_{nk}) = k$.*
2. *For given $n \geq 3$ and for k close either to n or to $s(n)$ find all p-groups G of order p^n such that $\mathrm{E}_p(G) = k$.*

If G is a noncyclic group of order p^3 then certainly $\mathrm{E}_p(G) = 3 = s(3)$. Hence further we consider in fact only p-groups of order at least p^4.

In this paper we solve Problem 1 in the following cases: $k = s(n,d)$ (Proposition 3.1), $s(n) - 6 \leq k \leq s(n)$ (Theorem 3.6), $n \leq k \leq 2n-3$ (Theorem 3.2) and $n \leq k \leq s(n)$ for all $n \leq 7$ (Corollary 3.9).

We also solve Problem 2 for some special values k in the class of abelian groups (Theorem 3.2, Proposition 3.3), and for $k = s(n) - 1$ where G is an arbitrary group (Theorems 3.2 and 5.3). We use this opportunity to refresh the proof of Miller's result mentioned above.

2. Some auxiliary results

For detailed calculation of $\mathrm{E}_p(G)$ for abelian p-groups G the following result from [10] can be used:

Lemma 2.1. *Let G be an abelian group of type $(m_1, \dots, m_s)$, and of order p^n. For every $k \geq 1$ let a_k denote the number of occurrences of k in the sequence $(m_1, \dots, m_s)$, and let* $\exp G = p^r$. *Then*

$$\mathrm{E}_p(G) = \sum_{k=1}^{r} \Big[k\Big(a_{k+1}^2 + 2a_k \cdot \sum_{x>k} a_x \Big) + \frac{1}{2} a_k(a_k - 1) \Big].$$

Using either this lemma or linear argument one can check

Example 2.2. Let $n = kl$ and $G = (C_{p^k})^l$. Then $\mathrm{E}_p(G) = l^2(k-1) + l(l-1)/2 = s(n,l)$.

As a consequence of Theorem I.17.1 from [5] we have

Lemma 2.3. *Let $N \subseteq Z(G)$ be a subgroup. Then the groups* $\mathrm{Aut}_N^N(G)$ *and* $\mathrm{Hom}(G/N,\, N)$ *are isomorphic.*

If, in particular, G is a p-group, $P \subseteq$ $\mathrm{Aut}(G)$ *is a Sylow p-subgroup and N is a P-invariant subgroup then*

$$\mathrm{E}_p(G) = \log_p |P| \leq \mathrm{E}_p(N) + \mathrm{E}_p(G/N) + \log_p |\operatorname{Hom}(G/N, N)|.$$

For our consideration we also need some results on endomorphisms of direct products of groups.

Let $G = K_1 \times K_2$ be a direct product of groups. Then any endomorphism φ of G is uniquely determined by four functions $\varphi_{ij} : K_i \longrightarrow K_j$, for $i, j \in \{1, 2\}$, which are defined by the following formula:

$$(1) \qquad \varphi(k_1, k_2) = (\varphi_{11}(k_1)\varphi_{21}(k_2), \varphi_{12}(k_1)\varphi_{22}(k_2)), \quad \text{for } k_i \in K_i.$$

Proposition 2.4 ([2]). *Let φ be an endomorphism of a group G. Then, under notation as above, the following holds:*

(a) *φ_{11} and φ_{22} are endomorphisms;*

(b) *φ_{12} and φ_{21} are homomorphisms;*

(c) *$[\varphi_{11}(K_1), \varphi_{21}(K_2)] = 1$ and $[\varphi_{12}(K_1), \varphi_{22}(K_2)] = 1$.*

Conversely, if $\varphi_{ij} : K_i \longrightarrow K_j$ are any functions satisfying conditions (a)–(c), *then φ defined by equality* (1) *is an endomorphism of G.*

If G is any p-group then $\Phi(G) = G^pG'$. Hence, if φ is a homomorphism of a p-group G into a p-group H, then we have an induced homorphism $\overline{\varphi}$ of $G/\Phi(G)$ into $H/\Phi(H)$. Under this notation, if $H = G$, then φ is an automorphism if and only if $\overline{\varphi}$ is an automorphism.

Proposition 2.5. *Let a p-group G be the direct product of a group K_1 with $\Omega_m(Z(K_1)) \subseteq \Phi(K_1)$ and an abelian group K_2 with $\exp K_2 = p^m$. If φ is an endomorphism of G then $\varphi \in \operatorname{Aut} G$ if and only if $\varphi_{11} \in \operatorname{Aut} K_1$ and $\varphi_{22} \in \operatorname{Aut} K_2$.*

Proof. Let $\varphi_{11} \in \operatorname{Aut} K_1$ and $\varphi_{22} \in \operatorname{Aut} K_2$. Then, from Proposition 2.4 we know, that $\varphi_{21}(K_2) \subseteq Z(K_1)$. By assumption it means that $\varphi_{21}(K_2) \subseteq \Phi(K_1)$. Now factorizing modulo $\Phi(G) = \Phi(K_1) \times \Phi(K_2)$ we have that for $\overline{\varphi}$ the homomorphism $\overline{\varphi}_{21} = \overline{\varphi_{21}}$ is trivial while, due to the assumption, $\overline{\varphi}_{11} = \overline{\varphi_{11}}$ and $\overline{\varphi}_{22} = \overline{\varphi_{22}}$ are automorphisms. By linear argument it means that $\overline{\varphi}$ is an automorphism, hence φ is an automorphism too.

Conversely, let $\varphi \in \operatorname{Aut} G$. Then, by assumption, $\varphi(K_2) \subseteq Z(G) = Z(K_1) \times K_2$ and consequently $\varphi_{21}(K_2) \subseteq \Omega_m(Z(K_1)) \subseteq \Phi(K_1)$. It means that for the automorphism $\overline{\varphi}$ the homomorphism $\overline{\varphi}_{21}$ is trivial. Hence, linear argument implies that $\overline{\varphi}_{11}$ and $\overline{\varphi}_{22}$ are automorphisms. It means, that φ_{11} and φ_{22} are automorphisms too. □

Corollary 2.6. *Let G, K_1 and K_2 be as above. Then*

(1) $|\operatorname{Aut} G| = |\operatorname{Aut} K_1| \cdot |\operatorname{Hom}(K_1, K_2)| \cdot |\operatorname{Hom}(K_2, \Omega_m(Z(K_1)))| \cdot |\operatorname{Aut} K_2|$.

(2) $|A_p(G)| = |A_p(K_1)| \cdot |\operatorname{Hom}(K_1, K_2)| \cdot |\operatorname{Hom}(K_2, \Omega_m(Z(K_1)))| \cdot |A_p(K_2)|$.

As a special case of this corollary we obtain:

Corollary 2.7. *Let a group G of order p^n be the direct product of a group H with $\Omega_1(Z(H)) \subseteq \Phi(H)$ and an elementary abelian group E. Put*

$$|H| = p^q, \quad |H/\Phi(H)| = p^d \quad \text{and} \quad |\Phi(H)/\Omega_1(Z(H))| = p^c.$$

Then, for $r = n - q$, $|E| = p^r$, G has $d + r$ generators and

$$\mathrm{E}_p(G) = \mathrm{E}_p(H) + s(r) + (q-c)r = \mathrm{E}_p(H) + s(r) + (q-c)(n-q).$$

If, in addition, $\mathrm{E}_p(G) = s(n, d+r) - x$, and $\mathrm{E}_p(H) = s(q, d) - y$ then $x = y + rc$.

Proof. The first claim is evident. For the rest of the proof we follow assumed notation.

By assumption G satisfies all the conditions of Corollary 2.6 with $m = 1$. Also $|\operatorname{Hom}(H, E)| = p^{rd}$, $|\operatorname{Hom}(E, Z(H))| = |\operatorname{Hom}(E, \Omega_1(Z(H)))| =$

$p^{r(q-d-c)}$ and $\mathrm{E}_p(E) = s(r)$. Hence, $\mathrm{E}_p(G) = \mathrm{E}_p(H)+s(r)+rd+r(q-d-c)$, which means that

$$(2)\quad \mathrm{E}_p(G) = \mathrm{E}_p(H) + s(r) + rq - rc = \mathrm{E}_p(H) + s(r) + (q-c)(n-q).$$

It is not hard to check that $s(n) = s(q+r) = s(q) + s(r) + qr$. Hence, $s(n, d+r) = s(q+r, d+r) = s(q+r) - s(q-d) = s(q)+s(r)+rq-s(q-d) = s(q,d) + s(r) + rq$. Thus

$$(3)\qquad s(n, d+r) = s(q,d) + s(r) + rq.$$

With the help of the formulas (2), (3) and the definiton we obtain that

$$\begin{aligned} x &= s(n, d+r) - \mathrm{E}_p(G) \\ &= s(q,d) + s(r) + qr - \mathrm{E}_p(H) - s(r) + (q-c)r. \end{aligned}$$

Hence $x = y + rc$. □

3. Examples

We begin by the result showing that the estimation for $\mathrm{E}_p(G)$ given in Theorem 1.1 is the best possible even if we restrict our attention to the class of abelian p-groups.

Proposition 3.1. *Let $1 \le d \le n$. Then there exists an abelian group G of order p^n with d generators such that $\mathrm{E}_p(G) = s(n,d)$.*

Proof. Write $n = dm + r$ where $m \ge 1$ and $0 \le r < d$ and put

$$G = \begin{cases} (C_{p^m})^d & \text{if } r = 0, \\ (C_{p^{m+1}})^r \times (C_{p^m})^{d-r} & \text{if } r > 0. \end{cases}$$

In both cases, either by Lemma 2.1 or by Example 2.2 and Corollary 2.6 we have the required equality. □

Let G be an abelian group of order $p^n \ge p^4$. In [8] it was shown that $\mathrm{E}_p(G) = n$ if and only if G is of type $(n-1, 1)$ and $\mathrm{E}_p(G) = n+1$ if and only if G is of type $(2,2)$. Using similar arguments we will show some other results on our problems for abelian groups.

Theorem 3.2. *Let G be a noncyclic abelian group of order p^n.*

1. *If $n \geq 5$ then $\mathrm{E}_p(G) = n+2$ if and only if G is either of type $(n-2, 2)$ or $(n-2, 1, 1)$.*
2. *If $n \geq 4$ then $\mathrm{E}_p(G) = s(n)$ if and only if G is either elementary abelian or of type $(2, 1, 1, \ldots, 1)$.*
3. *If $n \geq 4$ then $\mathrm{E}_p(G) = s(n) - 1$ if and only if G is of type $(2, 2, 1, \ldots, 1)$.*
4. *If $n \geq 6$ then $\mathrm{E}_p(G) = s(n) - 3$ if and only if G is of type $(2, 2, 2, 1, \ldots, 1)$.*

Proof. The first point of the theorem can be verified directly, as analogous result from [8], mentioned above.

Let $\mathrm{E}_p(G) \geq s(n) - 2$. Then, by Theorem 1.1 G has at least $n - 2$ generators. Hence we have to consider only the following types: $(1, \ldots, 1)$, $(2, 1, \ldots, 1)$, $(3, 1 \ldots, 1)$ and $(2, 2, 1, \ldots, 1)$. In each of these cases one can use either Lemma 2.1 or Example 2.2 and Corollary 2.7.

The case $\mathrm{E}_p(G) \geq s(n)-3$ implies, by Theorem 1.1, that G has at least $n-3$ generators. Using previous part of the proof it leads to consideration of groups with exactly $n-3$ generators.

From such considerations the result follows easily. □

Let G be an abelian group of order p^n. It appears that, at least for enough large n, some values of $\mathrm{E}_p(G)$, where $n \leq \mathrm{E}_p(G) \leq s(n)$ are impossible. Some of such values are presented in the result below. It can be proved analogously to the previous theorem.

Proposition 3.3. *Let G be an abelian group of order p^n.*

1. *If $n > 6$ then $\mathrm{E}_p(G) \neq n + 3$.*
2. *If $n > 4$ then $\mathrm{E}_p(G) \neq s(n) - 2$.*
3. *If $n > 6$ then $\mathrm{E}_p(G) \neq s(n) - 4$.*
4. *If $n > 7$ then $\mathrm{E}_p(G) \neq s(n) - 5$.*

Now we will indicate that the estimations on n in the two above results are the best posssible.

Example 3.4. In the table below we present maximal values of $n \geq 4$ for which single statements of the above results are not valid.

Type of G	$\|G\|$	$\mathrm{E}_p(G)$	Comments
$(1,1,1,1)$	p^4	6	$= 4+2$
$(3,3)$	p^6	9	$= 6+3$
$(3,1)$	p^4	4	$= s(4)-2$
$(3,1,1)$	p^5	7	$= s(5)-3$
$(3,2,1)$	p^6	11	$= s(6)-4$
$(3,2,1,1)$	p^7	16	$= s(7)-5$

Now we will show that some of gaps in values of $\mathrm{E}_p(G)$ for abelian groups G can be realized in the case of nonabelian groups.

Example 3.5. Let G_1 be the central product of a nonabelian group of order p^3 and the cyclic group of order p^2. Then it is easy to check that $|G_1| = p^4$, $\Phi(G_1) = \Omega_1(Z(G_1))$ is of order p and $\mathrm{E}_p(G_1) = 4 = s(4) - 2$.

Let G_2 be the central product of two nonisomorphic nonabelian groups of order p^3. Then $|G_2| = p^5$, $\Phi(G_2) = \Omega_1(Z(G_2)) = Z(G_2)$ is of order p and $\mathrm{E}_p(G_2) = 6 = s(5) - 4$.

Let G_3 be the direct product of the group G_1 and the cyclic group of order p^2. Then we have: $|G_3| = p^6$, $\Phi(G_3) = \Omega_1(Z(G_3))$ is of order p^2 and $\mathrm{E}_p(G_3) = 10 = s(6) - 5$.

Theorem 3.6. *For $n \geq 5$ and any $s(n) - 6 \leq k \leq s(n)$ there exists a group G_{nk} of order p^n with $\mathrm{E}_p(G_{nk}) = k$.*

Proof. For $s(n) - k \in \{0, 1, 3, 6\}$ it is enough to apply Proposition 3.1, because in this case we have $k = s(n, d)$ for suitable d.

Let $k = s(n) - 2$. Put $G = G_1 \times C_p^{n-4}$, where G_1 is taken from Example 3.5. Then by Corollary 2.7 we obtain that $\mathrm{E}_p(G) = s(n) - 2$.

Using groups G_2 and G_3 from the above example and similar arguments one can verify the case $k = s(n) - 4$ and $k = s(n) - 5$ for $n > 5$. In the case $n = 5$ and $k = s(5) - 5$ it is enough to take $G = C_{p^4} \times C_p$. □

Observe that for any abelian group G of type $(n - m, m)$, where $2m < n$ we have $\mathrm{E}_p(G) = n + 2m - 2$. In this case, as above, gaps can be filled by nonabelian groups.

Lemma 3.7. *Let numbers $n > m$ be given and G be a group of order p^n with presentation:*

$$G = \langle x, y, z \mid x^{p^{n-m-1}} = y^{p^m} = z^p = 1,\ [y,x] = z,\ [y,z] = [x,z] = 1\rangle.$$

a) *If $n = 2m+1$, then $\mathrm{E}_p(G) = (n-1) + (n-3) = 2n-4$;*

b) *If $n > 2m+1$, then $\mathrm{E}_p(G) = (n-1) + 2m = n + 2m - 1$.*

Immediately from the above results and Theorem 1.1 we obtain

Theorem 3.8. *Let G be a noncyclic group of order p^n. If G is generated by two elements then $\mathrm{E}_p(G) \le 2n-3$. Conversely, for any $n \le k \le 2n-3$ there exists a group G of order p^n and generated by two elements such that $\mathrm{E}_p(G) = k$.*

As an easy consequence of previous results we have

Corollary 3.9. *For any $n \le 7$ and $n \le k \le s(n)$ there exists a group G_{nk} of order p^n such that $\mathrm{E}_p(G_{nk}) = k$.*

Proof. The case $n = 4$ is evident. For $n = 5$ and 6 we have $2n-3 \ge s(n) - 6$. Hence our claim follows from Theorems 3.8 and 3.6.

For $n = 7$, due to the same arguments, we need only to consider cases $k = 12$, 13 and 14. For $k = 12$ it is enough to take $G = C_{p^4} \times (C_p)^3$, for $k = 13$ – $G = (C_{p^3})^2 \times C_p$, and for $k = 14$ – $G = H \times (C_{p^2})^2$, where H is a nonabelian group of order p^3. □

4. Miller's theorem

In this section we are going to prove Miller's theorem mentioned in Secton 1. However first we formulate some auxiliary results, which will also be used in the next section. It is not very difficult to verify the following:

Lemma 4.1 ([12]). *Let G be a nonabelian p-group and $N \subseteq G$ be a maximal subgroup. Then $|\operatorname{Aut}_N^N(G)| \le |Z(N)|$. If, in addition, N is abelian and $g \in G \setminus N$ then the mapping: $\sigma \to g^{-1}\sigma(g)$ is a bijection from $\operatorname{Aut}_N^N(G)$ to $\{n \in N : (gn)^p = g^p\}$. Moreover, $|N| = |Z(G)| \cdot |G'|$.*

Lemma 4.2. *Let G be a nonabelian group of order p^n with $\Omega_1(Z(G))\subseteq \Phi(G)$ and $\mathrm{E}_p(G) \geq s(n)-1$. Then $p \leq |\Phi(G)| \leq p^2$, there exists a maximal subgroup $N \subseteq G$ which is abelian and $Z(G) = \Omega_1(Z(G))$.*

Proof. The inequality $p \leq |\Phi(G)| \leq p^2$ follows directly from the assumption and Theorem 1.1.

Let $P \subseteq \operatorname{Aut} G$ be a Sylow p-subgroup and let $N \subseteq G$ be a maximal subgroup of G which is P-invariant. Each automorphism from P induces the identity map on G/N. Hence $P \subseteq \operatorname{Aut}^N(G)$. Then the restriction map $\Psi : P \longrightarrow \operatorname{Aut} N$ is a homomorphism with the kernel $\operatorname{Aut}_N^N(G)$.

Theorem 1.1 gives

$$|\operatorname{Im}\Psi| \leq |A_p(N)| \leq p^{(n-2)+\cdots+1}.$$

From the assumption $|P| \geq p^{(n-1)+\cdots+2}$, and it follows

$$|\operatorname{Aut}_N^N(G)| = |\operatorname{Ker}\Psi| = \frac{|P|}{|\operatorname{Im}\Psi|} \geq p^{n-2}.$$

Hence, Lemma 4.1 yields

$$p^{n-2} \leq |\operatorname{Aut}_N^N(G)| \leq |Z(N)| \leq |N| = p^{n-1},$$

which implies that N is abelian.

Put $|Z(G)| = p^q$ and $|\Omega_1(Z(G))| = p^k$. Assume that $k < q$. Our subgroup $Z(G) \subseteq G$ is characteristic. In particular, with the help of Lemma 2.3 and an assumption we have

$$p^{s(n)-1} \leq |A_p(Z(G))| \cdot |A_p(G/Z(G))| \cdot |\operatorname{Hom}(G/Z(G), Z(G))|. \tag{4}$$

But $|A_p(Z(G))| \leq p^{s(q)}$, $|A_p(G/Z(G))| \leq p^{s(n-q)}$ and $G/Z(G)$ is certainly noncyclic. If $G/Z(G)$ is elementary abelian then

$$|\operatorname{Hom}(G/Z(G), Z(G))| = |\operatorname{Hom}(G/Z(G), \Omega_1(Z(G)))| = p^{(n-q)k}.$$

This means that $|A_p(G)| \leq p^{s(q)+s(n-q)+(n-q)k}$. By assumption $\mathrm{E}_p(G) \geq s(n) - 1$. Hence,with the help of formula (4), we have

$$\begin{aligned} s(n) - 1 &= s(n-q) + s(q) + q(n-q) - 1 \\ &\leq s(q) + s(n-q) + (n-q)k \end{aligned}$$

and consequently, $(q-k)(n-q) \leq 1$. But the equality means that $Z(G)$ is of index p in G. However it is impossible.

Thus $G/Z(G)$ is neither cyclic nor elementary abelian. Then

$$|\operatorname{Hom}(G/Z(G), Z(G))| \leq p^{(n-q-1)q}.$$

Thus, as in the previous case

$$\begin{aligned} s(n)-1 &= s(n-q)+s(q)+q(n-q)-1 \\ &\leq s(q)+s(n-q)+(n-q-1)q \end{aligned}$$

and consequently, $q \leq 1$. But it is impossible, since $k < q$. In this way we have proved, that $q = k$ and $Z(G) = \Omega_1(Z(G))$. □

Corollary 4.3. *Let G be a nonabelian group of order p^n with $\Omega_1(Z(G)) \subseteq \Phi(G)$ and $\mathrm{E}_p(G) \geq s(n)-1$. Then the following conditions are equivalent:*

(1) $\mathrm{E}_p(G) = s(n)$,

(2) $|\Phi(G)| = p$,

(3) $n = 3$.

Proof. Let $\mathrm{E}_p(G) = s(n)$. Then, by the assumption and Theorem 1.1 we have $|\Omega_1(Z(G))| = |G'| = |\Phi(G)| = p$.

From the equality $|\Phi(G)| = p$ and Lemma 4.2 we obtain that $|Z(G)| = p$ and by Lemma 4.1, we have a maximal abelian subgroup $N \subset G$ of order p^2, and it has to be $|G| = p^3$.

If $n = 3$ then G is noncyclic and evidently $\mathrm{E}_p(G) = 3 = s(3)$. □

An analogue of the above corollary for $\mathrm{E}_p(G) = s(n)-1$ is more complicated. However we have

Corollary 4.4. *Let G be a nonabelian group of order p^n with $\Omega_1(Z(G)) \subseteq \Phi(G)$ and $\mathrm{E}_p(G) \geq s(n)-1$. Then $\mathrm{E}_p(G) = s(n)-1$ if and only if $|\Phi(G)| = p^2$. In this case $Z(G) = \Omega_1(Z(G))$ and we have one of the following cases:*

(1) *$|Z(G)| = p$, $|G'| = p^2$ and $|G| = p^4$;*

(2) *$|Z(G)| = p^2$, $|G'| = p$ and $|G| = p^4$;*

(3) $|Z(G)| = p^2$, $|G'| = p^2$ *and* $|G| = p^5$.

Proof. Our first claim follows directly from the assumptions, from Lemma 4.1 and Corollary 4.3. By the same arguments we also have $Z(G) = \Omega_1(Z(G)) \subseteq \Phi(G)$.

Let $|Z(G)| = p^k$, and $|G'| = p^l$. Then $1 \le k, l \le 2$ and, by Lemma 4.1, $n = k+l+1$. By Corollary 4.3 the case $k = l = 1$ is impossible. Hence, we have only the possibilities listed in the formulation of our corollary. □

Proposition 4.5. *Any nonabelian p-group can be represented as $H \times E$, where $\Omega_1(Z(H)) \subseteq \Phi(H)$ and E is elementary abelian.*

Proof. Take E as a maximal subgroup of $\Omega_1(Z(G))$ having trivial intersection with $\Phi(G)$, and H as a subgroup of G with minimal set of generators, such that $G = EH$. It is easy to check that this is a proper choice. □

All abelian groups of order p^n with $\mathrm{E}_p(G) = s(n)$ are described by Theorem 3.2. Hence, for proving Miller's Theorem we need only to consider the nonabelian case.

Theorem 4.6 (Miller [9]). *Let G be a nonabelian group of order p^n. Then $\mathrm{E}_p(G) = s(n)$ if and only if G is a direct product of a nonabelian group of order p^3 and an elementary abelian group.*

Proof. Let $G = H \times E$, where H is non-abelian of order p^3 and E is elementary abelian. Then all the assumptions of Corollary 2.7 are satisfied with $q = 3$, $d = 2$, $c = 0$ and $y = 0$. Hence in this case we have $\mathrm{E}_p(G) = s(n)$.

For the converse, assume that G is a nonabelian group of order p^n such that $\mathrm{E}_p(G) = s(n)$. Then by Theorem 1.1 $|\Phi(G)| = p$. By Proposition 4.5 we can write $G = H \times E$, where $\Omega_1(Z(H)) \subseteq \Phi(H)$ and E is elementary abelian. Hence $|\Phi(H)| = p$. If we put $|H| = p^q$, then all the assumptions of Corollary 2.7 are satisfied with $d = q - 1$ and $x = c = 0$. Hence, from this Corollary we have $y = 0$ and $\mathrm{E}_p(H) = s(q)$. Then, by Corollary 2.7 we obtain that $|H| = p^3$. □

One might expect that, if $|\Phi(G)| = p$, then $\mathrm{E}_p(G) = s(n)$ or is very close to this number. However it is not the case (see groups from Example 3.5).

5. A generalization of Miller's theorem

Now we shall prove a generalization of the theorem of Miller: The abelian case is completely covered by Theorem 3.2. Hence we can restrict our attention only to the nonabelian case.

The result below is in fact contained in Table 1 in [8] (see also [1]).

Lemma 5.1. *Let G be a group of maximal class and of order p^4. Then $\mathrm{E}_p(G) = 5$ if and only if G is one of the following groups:*

(1) $G = \langle x, y \mid x^8 = y^2 = 1,\ [x, y] = x^{-2}\rangle$,

(2) $G = \langle x, y \mid x^8 = y^4 = 1,\ [x, y] = x^{-2},\ y^2 = x^4\rangle$,

(3) $G = \langle x, y, z \mid x^9{=}y^3{=}1,\ [x, y]{=}x^3,\ [x, z]{=}y,\ [y, z] = 1,\ z^3 = x^6\rangle$,

(4) $G = \langle x, y, z \mid x^9 = y^3 = z^3 = 1,\ [x, y] = 1,\ [x, z] = y,\ [y, z] = x^6\rangle$,

(5) $G = \langle x, y, z, t \mid x^p = y^p = z^p = t^p = 1,\ [z, t] = y,\ [y, t] = x,$
$[x, t] = [y, z] = [x, z] = [x, y] = 1\rangle$, *(where $p > 3$)*,

(6) $G = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1,\ [x, y] = x^p,\ [x, z] = y,\ [y, z] = 1\rangle$.

Lemma 5.2. *Let M be a nonabelian group of order p^q. Then $\mathrm{E}_p(M) = s(q) - 1$ and $\Omega_1(Z(M)) = \Phi(M)$ if and only if one of the following cases holds:*

(1) $M = \langle x, y \mid x^{p^2} = y^{p^2} = 1, [x, y] = x^p\rangle$;

(2) $M = \langle x, y, z \mid x^{p^2} = y^p = z^p = 1, [x, z] = y, [x, y] = 1, [y, z] = 1\rangle$.

(3) $M = \langle x, y, z, u, v \mid x^p = y^p = z^p = u^p = v^p = 1, [x, y] = u, [x, z] = v,$
$[x, u] = [x, v] = [y, z] = [z, u] = [y, u] = [z, v] = [y, v] = [u, v] = 1\rangle$,
where $p > 2$;

(4) $M = \langle x, y, z, u \mid x^{p^2} = y^p = z^p = u^p = 1, [x, y] = u, [x, z] = x^p,$
$[x, u] = [y, z] = [z, u] = [y, u] = 1\rangle$, *where $p > 2$*;

(5) $M = \langle x, y, z \mid x^4 = y^4 = z^2 = 1, [x, z] = x^2, [y, z] = y^2, [x, y] = 1\rangle$;

(6) $M = \langle x, y, z \mid x^4 = y^4 = 1, z^2 = x^2, [x, z] = x^2, [y, z] = y^2, [x, y] = 1\rangle$.

Proof. Let M be one of listed group. Then it is not hard to check that $\mathrm{E}_p(M) = s(q) - 1$ and $\Omega_1(Z(M)) = \Phi(M)$.

Now let $\mathrm{E}_p(M) = s(q) - 1$ and $\Omega_1(Z(M)) = \Phi(M)$. Then, by Corollary 4.4 we have to consider only the following cases:

1. $|M| = p^4$ and $|M'| = p$;

2. $|M| = p^5$ and $|M'| = p^2$.

In the first case, by the presentations of groups of order p^4 given by Burnside in [1] (see also [5, Satz III.12.6, Aufgaben III.12.29–30]) we obtain that M is either of type 1 or of type 2.

Let us consider now the second case. Let, as in the proof of Lemma 4.2, $P \subseteq \operatorname{Aut} M$ be a Sylow p-subgroup and $N \subseteq M$ be a maximal subgroup which is P-invariant. We can also assume, that $Z(M) \subseteq N$.

By Lemma 4.2 N is abelian. Since $|M| = p^5$, by Corollary 4.4, $Z(M) = \Phi(M) = M'$ is elementary abelian of order p^2, so $\exp M \leq p^2$.

We already know that the restriction map $\Psi : P \longrightarrow \operatorname{Aut} N$ is a homomorphism with the kernel $\operatorname{Aut}_N^N(M)$. Our assumption and Theorem 1.1 give

$$|\operatorname{Im} \Psi| \leq |A_p(N)| \leq p^6 \quad \text{and} \quad |\operatorname{Aut}_N^N(M)| \cdot |\operatorname{Im} \Psi| = |P| = p^9.$$

Hence, Lemmas 4.1 and 4.2 yield

$$p^3 \leq |\operatorname{Aut}_N^N(G)| \leq |Z(N)| = |N| = p^4.$$

Assume, that $|\operatorname{Aut}_N^N(M)| = p^3$. Then $|\operatorname{Im} \Psi| = p^6$ and, by Theorem 1.1, $\operatorname{Im} \Psi$ is a Sylow p-subgroup of $\operatorname{Aut} N$. It means, by Theorem 3.2, that N is either elementary abelian or abelian of type $(2, 1, 1)$.

Let T be a maximal subgroup of N such that $T^\alpha = T$ for all $\alpha \in \operatorname{Im} \Psi$. We can assume that T is elementary abelian and $Z(M) \subseteq T$.

Take $u_0 \in N$ such that $N = \langle u_0, T \rangle$. Of course $|\operatorname{Aut}_T^T(N)| = p^3$. Then we have p^3 automorphisms $\alpha_u \in \operatorname{Aut}_T^T(N)$ such that $u_0^{\alpha_u} = u_0 u$ for $u \in T$. The corresponding automorphisms $\varphi_u \in P$ possess properties $\varphi_{u|N} = \alpha_u$ and $g^{\varphi_u} = g h_u$ for some $h_u \in N$. Then since $\alpha_u \in \operatorname{Aut}_T^T(N)$, $[u_0, g] = [u_0, g]^{\alpha_u} = [u_0, g]^{\varphi_u} = [u_0^{\varphi_u}, g^{\varphi_u}] = [u_0 u, g h_u] = [u_0 u, g] = [u_0, g][u, g]$. Then $T \subseteq Z(M)$. So we have a contradiction.

In this way we have proved that $|\operatorname{Aut}_N^N(M)| = p^4$. Thus, by Lemma 4.1, for fixed $g \in M \setminus N$ and for every $n \in N$ we obtain $(gn)^p = g^p$.

First let $p = 2$. Then $n^g = n^{-1}$ and $n^2 \neq 1$, so we have the group (3), if $g^2 = 1$; and the group (4), if $g^2 \neq 1$.

Now let $p > 2$. Then $n^p = 1$ and we have the group (1), if $g^p = 1$; and the group (2) if $g^p \neq 1$. □

Theorem 5.3. *Let G be a nonabelian group of order p^n. Then $\mathrm{E}_p(G) = s(n) - 1$ if and only if either G is a group of maximal class listed in Lemma 5.1 or G is the direct product of an elementary abelian group and a group M, where M is listed in Lemma 5.2.*

Proof. If G is of maximal class and as in Lemma 5.1 then $|G| = p^4$ and $\mathrm{E}_p(G) = 5 = s(4) - 1$.

Let $G = M \times E$, where M is as required and E is an elementary abelian p-group. Denote $|M| = p^q$. From Lemma 5.2 we have $\mathrm{E}_p(M) = s(q) - 1$. Since $\Phi(M) = \Omega_1(Z(M))$ then Corollary 2.7 gives $\mathrm{E}_p(G) = s(n) - 1$.

On the contrary, let G be of order p^n with $\mathrm{E}_p(G) = s(n) - 1$. By Proposition 4.5 we can write $G = M \times E$, where E is elementary abelian (possibly trivial) and $\Omega_1(Z(M)) \subseteq \Phi(M)$. Let $|M| = p^q$ and $|M/\Phi(M)| = p^d$. Then $|E| = p^r$, where $r = n - q$. We have $\Phi(G) = \Phi(M) \times 1$. Hence, G has $d+r$ generators and by Theorem 1.1 $d+r \geq q+r-2$. It means that either $d = q-1$ or $d = q-2$, because M is nonabelian. As in Corollary 2.7 put

$$x = s(n, d+r) - \mathrm{E}_p(G), \quad y = s(q,d) - \mathrm{E}_p(M)$$
$$\text{and } |\Phi(M)/\Omega_1(Z(M))| = p^c.$$

Then, from this corollary we have

$$x = y + rc. \tag{5}$$

Let $d = q - 1$. Then, $x = 1$, $|\Phi(M)| = p$ and $c = 0$. Thus, by the formula (5), $y = 1$. Hence, from Corollary 4.3 we have that M is a nonabelian group of order p^3. Therefore, by Theorem 4.6, $\mathrm{E}_p(G) = s(n)$, a contradiction.

In this way we have proved, that $d = q - 2$. Hence $x = 0$ and by formula (5) we have $y = 0$ and $rc = 0$. This means that $\mathrm{E}_p(M) = s(q) - 1$.

If $c > 0$ then $r = 0$, hence $G = M$. Moreover, $\Omega_1(Z(G)) \neq \Phi(G)$. With the help of Corollary 4.4 it is clear that G is of order p^4 and of maximal class with $\mathrm{E}_p(G) = 5$. Hence G satisfies all the conditions of Lemma 5.1.

Let $c = 0$. Then $\Omega_1(Z(M)) = \Phi(M)$ and, by Corollary 4.4 M satisfies all the conditions of Lemma 5.2, which completes the proof. □

Another full proof of the above theorem can be found in [7].

Acknowledgement. Both authors would like to thank Dr Czesław Bagiński for helpful conversations and useful remarks about the subject of this paper.

References

[1] W. Burnside, Theory of Groups of Finite Order, (2nd edn), *Cambridge University Press*, *Cambridge*, 1911; Reprint: *Dover Publications, Inc., New York*, 1955.

[2] J. Dauns and K. H. Hofmann, Nilpotent groups and automorphisms, *Acta Sci. Math. (Szeged)* **29** (1968), 225–246.

[3] Th. G. Exarchakos, On p-groups of small order, *Publ. Inst. Math. (Beograd) (N.S.)* **45**(59) (1989), 73–76.

[4] N. Gavioli, The number of automorphisms of groups of order p^7, *Proc. Roy. Irish Acad. Sect.* A **93** no. 2 (1993), 177–184.

[5] B. Huppert, Endliche Gruppen I, *Springer-Verlag*, *Berlin*, 1967.

[6] E. I. Khukhro and V. D. Mazurov (eds.), The Kourovka Notebook, Unsolved Problems in Group Theory, Fourteenth augmented edition, *Institute of Mathematics, Siberian brunch of the Russian Academy of Sciences*, *Novosibirsk*, 1999.

[7] I. Malinowska, Groups of automorphisms of finite p-groups, PhD Thesis, *Warsaw University*, 1999. (in *Polish*)

[8] I. Malinowska, Finite p-groups with few p-automorphisms, *J. Group Theory* **4** (2001), 395–400.

[9] G. A. Miller, Isomorphisms of a group whose order is a power of a prime, *Trans. Amer. Math. Soc.* **12** (1911), 387–402.

[10] A. D. Otto, Central automorphisms of a finite p-group, *Trans. Amer. Math. Soc.* **125** (1966), 280–287.

[11] D. J. S. Robinson, A Course in the Theory of Groups, (2nd edn), *Springer-Verlag*, *New York*, 1995.

[12] U. H. M. Webb, An elementary proof of Gaschütz theorem, *Arch. Math.* **35** (1980), 23–26.

JAN KREMPA
INSTITUTE OF MATHEMATICS
WARSAW UNIVERSITY
UL. BANACHA 2
02–097 WARSZAWA
POLAND

E-mail: jkrempa@mimuw.edu.pl

IZABELA MALINOWSKA
INSTITUTE OF MATHEMATICS
UNIVERSITY OF BIAŁYSTOK
UL. AKADEMICKA 2
15–267 BIAŁYSTOK
POLAND

E-mail: izabelam@cksr.ac.bialystok.pl

(Received October 12, 2001; revised May 9, 2002)