On Abelian Subgroups of $p$-Groups

Yakov Berkovich*

Department of Mathematics and Computer Science, University of Haifa, Haifa 31905, Israel

Communicated by Walter Feit
Received January 27, 1997

IN MEMORY OF MY DEAR FRIEND GRISHA KARPILOVSKY
(1940–1997)

This is a continuation of our note (J. Algebra 186 (1996), 120–131). We generalize and present simplified proofs almost all elementary lemmas from Section 8 of the Odd Order Paper. In many places we use Hall’s enumeration principle and other simple combinatorial arguments. A number of related results are proved as well. Some open questions are posed.

Let $G$ be a finite $p$-group, where $p$ is a prime. Let $\Theta$ be a group-theoretic property and $\mathcal{X}$ the set of all $\Theta$-subgroups in $G$. Suppose that $p \mid |\mathcal{X}|$. Let $G$ act on $\mathcal{X}$ by conjugation. Then one of the $G$-orbits on $\mathcal{X}$ contains one element, say $H$. Thus $H \leq G$. Moreover, if $G$ is a normal subgroup of some larger $p$-group $W$, then $\mathcal{X}$ admits the action of $W$ by conjugation and, as previously, $\mathcal{X}$ contains a one-element $W$-orbit. We see that, in many cases, counting theorems are more fundamental than the respective theorems on the existence of normal subgroups. In this note we use this approach extensively as we know, Sylow was the first who used this argument in analogous situations.

We will show how this argument works in another situation. Suppose that a $p$-group $G$ contains a subgroup $H$ of maximal class and index $p$, $|G| > p^{p+1}$. We claim that $\text{Aut}(G)$ is a $\pi$-group, where $\pi = \pi((p(p^2 - 1))$ ($\pi(n)$ is the set of all prime divisors of $n \in \mathbb{N}$). Note that $\pi(\text{Aut}(G)) \subseteq \pi$ for every $p$-group generated by two elements. Therefore, the result is true if $G$ is of maximal class, so suppose that $G$ is not of maximal class. Assume that $\alpha$ is an automorphism of $G$ of prime order $q \notin \pi$. By [6] and [18], the number of subgroups of maximal class and order $|H|$ in $G$ is

* The author was supported in part by the Ministry of Absorption of Israel.
divisible by $p^2$. Since a $p$-group of maximal class is generated by two elements, the minimal number of generators of $G$ is $3$, and so the number of maximal subgroups in $G$ is $1 + p + p^2 < 2p^2$. Therefore $G$ contains exactly $p^2$ subgroups of maximal class and index $p$. Since $q \neq p$, one of these subgroups, say $H$, is $\alpha$-invariant. Since $\text{Aut}(H)$ is a $\pi$-group, $\alpha$ centralizes $H$. Then $\langle \alpha \rangle$ stabilizes the chain $G > H > \{1\}$ (since $q \nmid p - 1$). By [21], Lemma 8.1 or Lemma 14, $o(\alpha)$ is a power of $p$—contradiction. Similarly, if $|G|$ is a 2-group of order at least $2^4$, $H$ a subgroup of maximal class and index 2 in $G$, then $\text{Aut}(G)$ is a 2-group (the condition $|G| \geq 2^3$ is essential). To prove this, we have to use the fact that a group of automorphisms of a 2-group of maximal class and order at least $2^4$ is a 2-group.

We retain, as a rule, the notation and definitions from [21]. If $A$ is a maximal normal abelian subgroup of a $p$-group $G$, then $C_G(A) = A$ (i.e., $A$ is a maximal abelian subgroup of $G$). This “self-centralizer” property allows us to restrict the structure of $G$ if all its maximal abelian normal subgroups are small in some sense. Some more general results in this direction were proved and used in [21] and in the subsequent Thompson’s paper on simple groups all of whose local subgroups are solvable. For example, if $p > 2$ and $A$ is a maximal normal elementary abelian subgroup of $G$, then $\Omega_1(C_G(A)) = A$ (see [21], Lemma 8.3 and [24], Lemma 10.15). Alperin [1] generalized that result in the following way: Let $A$ be a maximal normal abelian subgroup of a $p$-group $G$ such that $\exp(A) \leq p^n$, where $p^n > 2$; then $\Omega_1(C_G(A)) = A$. (For another proof of Alperin’s Theorem, due to N. Blackburn, see [28], Theorem 3.12.1) We will prove the following stronger result (which we consider as the main theorem of this note):

**Theorem 1.** Let $A < B \leq G$, where $A, B$ are abelian subgroups of a $p$-group $G$, $\exp(B) \leq p^n$ and $p^n > 2$. Let $\mathcal{A}$ be the set of all abelian subgroups $T$ of $G$ such that $A \leq T$, $|T:A| = p$ and $\exp(T) \leq p^n$. Then $|\mathcal{A}| = 1 \mod p$.

Let us show that Theorem 1 implies Alperin’s Theorem. Let $A$ be a maximal normal abelian subgroup of $G$ of exponent at most $p^n$, where $p^n > 2$. Let $x \in C_G(A) - A$ such that $o(x) \leq p^n$. Then $A < B = \langle A, x \rangle$ and $B$ is abelian of exponent at most $p^n$. In the notation of Theorem 1, $|\mathcal{A}| = 1 (\mod p)$. Then there exists $T \in \mathcal{A}$ such that $T \leq G$, contradicting the choice of $A$. In what follows, we will deduce from Theorem 1 essentially stronger result (Corollary 2).

**Proof of Theorem 1.** We use induction on $G$.

If $T \in \mathcal{A}$, then $T \leq C_G(A)$. Therefore, without loss of generality, we may assume that $G = C_G(A)$, i.e., $A \leq Z(G)$. If $A = \{1\}$, then $\mathcal{A}$ consists of all subgroups of $G$ of order $p$, and so $|\mathcal{A}| = 1 (\mod p)$ by Sylow’s Theorem. Therefore, in what follows, we assume that $A > \{1\}$. If $|G:A| =
Then, where \( c \) is a subgroup of order \( p \)
\( \ker A \) and it suffices to prove that \( |\ker A| = 1 \) (mod \( p \)).
To prove that \( \ker A \neq \emptyset \) we consider the maximal class.
Let \( A < B \leq M < G \), where \( M \) is maximal in \( G \).
Then the number of elements of \( A \) that are contained in \( M \) is congruent to 1 (mod \( p \)),
and our claim follows. Let \( D = \langle T \mid T \in \ker A \rangle \).
By the definition of \( \ker A \), \( D/A \) is an elementary abelian subgroup of \( Z(G/A) \).
Therefore, the nilpotency class of \( D \) is at most two.
We claim that \( \exp(D) \leq p^n \). By construction, \( D \) is generated by elements of orders at most \( p^n \).
Therefore, if \( x \in D \), then \( x = a_1 \cdots a_i \), where \( \exp(a_i) \leq p^n \) for all \( i \).
Since \( D \) is of class at most 2 (it is essential that \( p^n > 2 \)), we have
\[
x^{p^n} = a_1^{p^n} \cdots a_i^{p^n} \cdot c_1^{p^n} \cdots c_i^{p^n},
\]
where \( c_1, \ldots, c_i \) are elements of \( D' \) (the equality (1) is known for \( s = 2 \); for \( s > 2 \) it is proved by induction on \( s \)).
Since \( \exp(D') \leq \exp(D/Z(D)) = p \) (recall that \( A \leq Z(D) \)), formula (1) is reduced to \( x^{p^n} = 1 \).
Therefore, \( \exp(D) \leq p^n \), as claimed. All elements of \( \ker A \) are contained in \( D \).
If \( H/A \) is a subgroup of order \( p \) in \( D/A \), then \( H \) is abelian, \( H < G \) and \( \exp(H) \leq \exp(D) \leq p^n \), i.e., \( H \in \ker A \).
Therefore, we may assume, without loss of generality, that \( G = D \).
In particular, \( G/A \) is elementary abelian.
Let \( |G/A| = p^k \). By the previous text, \( |\ker A| \) is the number of subgroups of order \( p \) in the elementary abelian group \( G/A \) of order \( p^k \), i.e., \( |\ker A| = 1 + p + \cdots + p^{k-1} = 1 \) (mod \( p \)), proving the theorem.

Kulakoff's Theorem [32] and its analog for \( p = 2 \) (see [4], Section 5) show that \( |\ker A| = 1 + p \) (mod \( p^2 \)) unless \( C_c(A)/A \) is cyclic or a 2-group of maximal class.
The subgroup \( A \) of Theorem 1 is not necessarily of exponent \( p^n \).
Theorem 1 is not true for \( p^n = 2 \) (let \( G \) be a dihedral group of order 8, \( A = Z(G) \); then \( |\ker A| = 2 \)).

**Corollary 2.** Let \( N \) be a normal subgroup of a \( p \)-group \( G \), let \( A \) be a maximal \( G \)-invariant abelian subgroup of \( N \) such that \( \exp(A) \leq p^n \), \( p^n > 2 \).

Then \( \Omega_n(C_N(A)) = A \).

**Proof.** Assume that \( x \in C_N(A) - A \) is of order at most \( p^n \). Set
\[
\mathcal{V}_N = \{ T \leq N \mid A < T, |T:A| = p, T \text{ is abelian, } \exp(T) \leq p^n \}.
\]

Since \( \langle A, x \rangle \) is abelian of order at most \( p^n \), the set \( \mathcal{V}_N \) is nonempty.
By Theorem 1, \( |\mathcal{V}_N| = 1 \) (mod \( p \)). Therefore, there exists \( T \in \mathcal{V}_N \) such that \( T \leq G \), contrary to the choice of \( A \).

This generalizes [21], Lemma 8.3 and the main result in [1].
The following three results are known.
**Lemma 3.** The number of abelian subgroups of index $p$ in a nonabelian $p$-group $G$ is one of the numbers $0, 1, p + 1$.

**Lemma 4 [2].** Suppose that a $p$-group $G$ contains an abelian subgroup $A$ of index $p^2$. Then $G$ contains a normal abelian subgroup of index $p^2$.

**Proof.** Let $A < M < G$, where $M$ is a maximal subgroup of $G$; then $|M:A| = p$. Since the number of abelian subgroups of index $p$ in $M$ is congruent to 1 (mod $p$) (Lemma 3) and $M < G$, the result follows. 

Moreover, by [29], Theorem (iii), the number in Lemma 4 is $2$ or $1$ (mod $p$).

**Lemma 5 [4], Section 5.** Let $G$ be a noncyclic $p$-group. Suppose that $G$ is not a 2-group of maximal class. If $n \in \mathbb{N}$ and $n > 1$, then the number of cyclic subgroups of order $p^n$ is $G$ is divisible by $p$.

For $p > 2$ this result is due to G. A. Miller.

**Corollary 5' ([4]; see also [25], Chapter 5, Exercise 9 and [24], Lemma 10.11).** Let $N$ be a noncyclic normal subgroup of a $p$-group $G$. If $N$ has no G-invariant noncyclic subgroups of order $p^2$, then $N$ is a 2-group of maximal class.

**Corollary 5'** is a generalization of Roquette's Lemma (see [28], Satz 3.7.6).

**Corollary 5".** Let $p > 2$, $N$ a normal subgroup of a $p$-group $G$, $A$ a $G$-invariant elementary abelian subgroup of order $p^2$ in $N$. If $N$ contains an elementary abelian subgroup $B$ of order $p^3$, then $N$ contains a $G$-invariant elementary abelian subgroup $B_1$ such that $A < B_1$.

**Proof.** It follows from $p^2 \nmid |\text{Aut}(A)|$ that $C_p(A) \not\leq A$. Let $D/A$ be a subgroup of order $p$ in $AC_p(A)/A$. Obviously, $D$ is elementary abelian of order $p^3$, and the result follows from Theorem 1.

Corollary 5" implies [21], Lemma 8.9 and the main result in [27].

**Remark 1.** Obviously, Corollary 5" implies [21], Lemma 8.4(i). To prove [21], Lemma 8.4(ii), we use some properties of minimal nonnilpotent groups (see Lemma 10). Let $G$ be a $p$-group of odd order that has no normal elementary abelian subgroups of order $p^2$ and $\alpha \in \text{Aut}(G)^*$. If $o(\alpha) = q$ is a prime, $q \neq p$, then we claim that $q|p^2 - 1$. Let $W = \langle \alpha \rangle \cdot G$ be a natural semidirect product. Take in $W$ a minimal nonnilpotent subgroup $S = \langle \alpha \rangle \cdot P$, where $P = S \cap G$. By Corollary 5", $P$ has no elementary abelian subgroups of order $p^3$. Since $P$ is elementary abelian or special of exponent $p$ (see Lemma 10), it follows that $P$ has two generators, and our claim follows (see the second paragraph of this note).
Remark 2. Let us prove the following result (see [21], Lemma 8.5): Suppose that \( P \in \text{Syl}_p(G) \), where \( p > 2 \) is the smallest prime divisor of \(|G|\); if \( P \) has no elementary abelian subgroups of order \( p^3 \), then \( G \) is \( p \)-nilpotent. Suppose that \( G \) is a counterexample. Then \( G \) contains a non-\( p \)-nilpotent minimal non-nilpotent group \( S \) (by Frobenius' Normal \( p \)-Complement Theorem). We may assume that \( P \cap S \in \text{Syl}_p(S) \). If \( \pi(S) = \{ p, q \} \), then \( q > p + 1 \), and so \( q + p^2 - 1 \), contradicting Remark 1.

Theorem 6. Suppose that a \( p \)-group \( G \), \( p > 2 \), contains an elementary abelian subgroup of order \( p^3 \). Then the number of such subgroups in \( G \) is congruent to 1 mod \( p \).

Proof. For \( H \leq G \), let \( e_3(H) \) denote the number of elementary abelian subgroups of order \( p^3 \) contained in \( H \). We have to prove that \( e_3(G) \equiv 1 \) (mod \( p \)). Let \( \mathcal{M} \) denote the set of all maximal subgroups of \( G \). It is known that \(|\mathcal{M}| \equiv 1 \) (mod \( p \)). By Hall's enumeration principle [26],

\[
e_3(G) \equiv \sum_{H \in \mathcal{M}} e_3(H) \quad (\text{mod } p),
\]

(2)

Suppose that the theorem has proved for all proper subgroups of \( G \).

Take \( H \in \mathcal{M} \). By the induction hypothesis, \( e_3(H) \equiv 0 \) or \( e_3(H) \equiv 1 \) (mod \( p \)). If \( e_3(H) \equiv 1 \) (mod \( p \)) for all \( H \in \mathcal{M} \), then by (2), \( e_3(G) \equiv |\mathcal{M}| \equiv 1 \) (mod \( p \)), proving the theorem. Therefore, we may assume that some maximal subgroup of \( G \), say \( H \), has no elementary abelian subgroups of order \( p^3 \).

Suppose that \( H \) contains a subgroup \( L \) of order \( p^4 \) and exponent \( p \). Let \( A \) be a maximal normal abelian subgroup of \( L \). Since \( A \triangleleft L \) and \( C_L(A) = A \), it follows that \(|A| = p^4 \), contrary to what was proved in the previous paragraph.

By assumption, \( G \) contains an elementary abelian subgroup \( E_0 \) of order \( p^3 \). Let \( E_0 \leq F \in \mathcal{M} \). By the induction hypothesis, \( e_3(F) \equiv 1 \) mod \( p \), and so \( G \) contains an elementary abelian subgroup \( E \) of order \( p^3 \).

Let \( e_3'(G) \) be the number of normal elementary abelian subgroups of order \( p^3 \) in \( G \). Since \( e_3(G) \equiv e_3'(G) \) (mod \( p \)), it suffices to prove that \( e_3'(G) \equiv 1 \) (mod \( p \)). Therefore, we may assume that \( G \) contains a normal elementary abelian subgroup \( E_1 \) of order \( p^3 \), \( E_1 \neq E \). Set \( D = EE_1 \). By Fitting's Lemma, the nilpotency class of \( D \) is at most two. Therefore (see the proof of Theorem 1), \( \text{exp}(D) = p \). Considering \( D \cap H \) and taking into account that \( H \) has no subgroups of order \( p^4 \) and exponent \( p \), we conclude that \(|D| = p^4 \). By Lemma 3, \( e_3(D) \equiv 1 \) (mod \( p \)). Hence the number of \( G \)-invariant elementary abelian subgroups of order \( p^3 \) in \( D \) is congruent to 1 (mod \( p \)); therefore, we may assume that \( G \) contains a normal elementary abelian subgroup \( E_2 \) of order \( p^3 \) such that \( E_2 \not\leq D \).
(otherwise, all is done). Suppose that \( E \cap E_1 < E_2 \) (since \( |D| = p^4 \) it follows that \( |E \cap E_1| = p^2 \)). Then \( E \cap E_1 \leq Z(EE_1E_2) \) and \( EE_1E_2/E \cap E_1 \) is elementary abelian of order \( p^3 \). In that case, \( EE_1E_2 \) is of order \( p^5 \) and its class is at most two, and so \( \exp(EE_1E_2) = p \) (see the proof of Theorem 1). Then \( H \cap EE_1E_2 \) is a subgroup of order \( p^4 \) and exponent \( p \) in \( H \), contrary to what we have previously proved. Therefore, \( E \cap E_1 \not\subseteq E_2 \).

Since \( |EE_1E_2| = |E_1E_2| = p^4 \) (see the proof of the equality \( |D| = p^4 \)), it follows that \( |E \cap E_2| = p^2 = |E_1 \cap E_2| \). Since \( E \cap E_2, E_1 \cap E_2 \) are different maximal subgroups of \( E_2 \) (since \( E \cap E_1 \not\subseteq E_2 \)), we conclude that \( E_2 = (E \cap E_2)E_1E_2 < EE_1 = D \), contrary to the choice of \( E_2 \). This completes the proof of the theorem.

Theorem 6 was announced in [9]. This theorem is not true for \( p = 2 \) (let \( G \) be the direct product of the dihedral group of order 8 and the cyclic group of order 2). For another proof of this theorem, see [31], Theorem 2.2.

**Question 1.** Classify the \( p \)-groups \( G, p > 2 \), containing an abelian self-centralizer \( A \) of order \( p^3 \). Obviously \( |N_G(A):A| \leq p^3 \) if \( A \) is noncyclic, and \( |N_G(A):A| \leq p^2 \) if \( A \) is cyclic. The case \( |N_G(A):A| = p \) is of some interest.

Let \( E_1(G) \) be the set of normal elementary abelian subgroups of order \( p^k \), \( k \in \mathbb{N} \), in \( G \).

**Theorem 7.** Suppose that a \( p \)-group \( G, p > 2 \), contains an elementary abelian subgroup \( E \) of order \( p^4 \). Then the number of elementary abelian subgroups of order \( p^4 \) in \( G \) is congruent to 1 (mod \( p \)). In particular, \(|E_1(G)| \equiv 1 \pmod{p} \) (obviously these two assertions are equivalent).

**Proof.** Suppose that \( G \) is a counterexample of minimal order. Then \( |G| > p^5 \) by Lemma 3. By Theorem 6, \( G \) contains a normal elementary abelian subgroup \( A \) of order \( p^3 \).

A. Suppose that \( G \) has no normal elementary abelian subgroup \( B \) of order \( p^4 \) such that \( A < B \). It follows from Theorem 1 that

(i) \( A \) is a maximal elementary abelian subgroup of \( G \).

Therefore,

(ii) if \( K \) be a subgroup of \( G \) of exponent \( p \), then \( C_K(A) \leq A \).

Note that a Sylow \( p \)-subgroup of \( \text{Aut}(A) \cong \text{GL}(3, p) \) is nonabelian of order \( p^3 \) and exponent \( p \). Therefore, the following two assertions are true:

(iii) If \( K \) is an elementary abelian subgroup of \( G \) of order \( p^4 \), then \( |A \cap K| = p^2 \). In particular, \( G \) has no elementary abelian subgroups of order \( p^5 \).
(iv) $G$ has no subgroup of order $p^7$ and exponent $p$. If $K$ is a subgroup of $G$ of order $p^5$ and exponent $p$ then $A < K$.

Let $E < M < G$, where $M$ is a maximal subgroup of $G$. By the induction hypothesis, $|\mathcal{C}_4(M)| \equiv 1 \pmod{p}$, so that $M$ contains a $G$-invariant elementary abelian subgroup of order $p^5$. Without loss of generality, we may assume that $E \triangleleft G$. If $E$ is the only normal elementary abelian subgroup of $G$ of order $p^5$, then $|\mathcal{C}_4(G)| = 1$, contrary to the assumption. Therefore, $G$ contains a normal elementary abelian subgroup $E_1$ of order $p^5$ different of $E$. Set $K = EE_1$. Since $K$ is of class at most two and $p > 2$, it is of exponent $p$. Suppose that $|K| = p^6$. Then $A < K$ by (iv). Since $C_K(A) = A$ by (ii), it follows that $E \cap E_1 \neq Z(K) < A$. Since $K/E \cap E_1$ is abelian, it follows that $K/A$ is abelian of order $p^3$. By the remark before (ii) on $GL_3(p)$ it follows that $C_K(A) > A$, contradicting (ii). Thus, $|K| = p^5$. Hence,

(v) If $B, B_1$ are two different normal elementary abelian subgroups of $G$ of order $p^4$, then $|BB_1| = p^5$, i.e., $|B \cap B_1| = p^3$. Moreover, $B \cap B_1 = Z(BB_1)$ since $BB_1$ is nonabelian by the second part of (iii).

Thus, $K = EE_1$ is nonabelian of order $p^3$ and exponent $p$, $E \cap E_1 = Z(K)$ is of order $p^3$. Therefore, by (ii), $A \neq Z(K)$, and so

(vi) $A \notin K$.

Suppose that $K$ contains all elements of the set $\mathcal{C}_4(G)$. By Lemma 3 (since $|K| = p^5$), $|\mathcal{C}_4(K)| \equiv 1 \pmod{p}$. Therefore, $|\mathcal{C}_4(G)| \equiv |\mathcal{C}_4(K)| \pmod{p}$, contrary to the assumption. Thus, there exists $E_2 \in \mathcal{C}_4(G)$ such that $E_2 \notin K$. By (v), $|E \cap E_2| = p^3 = |E_1 \cap E_2| = |E \cap E_1|$. Assume that $E_2 \cap E = E_2 \cap E_1$. Then $E_2 = (E_2 \cap E)(E_2 \cap E_1) = EE_1 = K$, contrary to the choice of $E_2$. Hence $E_2 \cap E = E_2 \cap E_1$. Then $C_{E_2}(E_2 \cap E) \supseteq EE_1 = K$, and so $E_2 \cap K = E \cap E_1 = Z(K)$. Set $L = KE_2 = EE_1E_2$. Then $E_2 \cap K \leq Z(L)$ and $|L| = p^6$. Since $L/Z(K) = E/Z(K) \times E_2/Z(K)$ is elementary abelian of order $p^5$, the nilpotency class of $L$ is two and since $L = EE_1E_2$ is generated by elements of order $p$, it follows that $\exp(L) = p$. By (iv), $A < L$. Then $C_{E_2}(A) > A$ (since $|Z(L)| = p^3 = |A|$), contrary to (ii).

B. Every normal elementary abelian subgroup of $G$ of order $p^3$ is contained in some elementary abelian subgroup of $G$ of order $p^5$. Then every $A \in \mathcal{C}_3(G)$ is contained in some $B \in \mathcal{C}_4(G)$ by Theorem 1. Since the number of conjugates (in $G$) of every nonnormal subgroup is a multiple of $p$, it suffices to prove that $|\mathcal{C}_4(G)| = 1 \pmod{p}$. Set

$$\mathcal{C}_3(G) = \{A_1, \ldots, A_r\}, \quad \text{and} \quad \mathcal{C}_4(G) = \{B_1, \ldots, B_s\}.$$
We have to prove that \( s = 1 \pmod{p} \). Suppose that \( A_i \) is contained in \( \alpha_i \) elements of the set \( \mathcal{E}_2(G) \), and \( B_j \) contains \( \beta_j \) elements of the set \( \mathcal{E}_3(G) \). Then the number of pairs \( \{A_i, B_j\} \) \( (A_j \in \mathcal{E}_2(G), B_j \in \mathcal{E}_3(G), i = 1, \ldots, r, j = 1, \ldots, s) \) is

\[
\alpha_1 + \cdots + \alpha_r = \beta_1 + \cdots + \beta_s.
\]

We have \( \beta_j = (p^4 - 1)/(p - 1) \equiv 1 \pmod{p} \) for \( j = 1, \ldots, s \). By Theorem 1, \( \alpha_i \equiv 1 \pmod{p} \) for \( i = 1, \ldots, r \). Therefore, reading (3) by modulo \( p \), we obtain \( r \equiv s \pmod{p} \). Since \( r = 1 \pmod{p} \) by Theorem 6, it follows that \( s = 1 \pmod{p} \), completing the proof.

Using the method of the proof of Theorem 7, we can give another, shorter, proof of Theorem 6.

Theorem 7 was announced in [5], Theorem 11. For another proof, see [31], Theorem 2.2. In the same paper Konvisser and Jonah proved that if \( p > 2 \), then \( |\mathcal{E}_3(G)| = 1 \pmod{p} \) unless \( \mathcal{E}_3(G) = \emptyset \) (but there exists \( G \) such that \( \mathcal{E}_3(G) = 2 \) [29]).

**Corollary 8.** Let \( N \) be a normal subgroup of a \( p \)-group \( G \), \( p > 2 \). Suppose that \( N \) has no \( G \)-invariant elementary abelian subgroups of order \( p^3 \). Then \( N \) has no elementary abelian subgroups of order \( p^3 \) (and hence, the structure of \( N \) is completely determined in [17]).

This follows from Theorem 6. If \( N = G \) in Corollary 8, we obtain Hobby’s Theorem [27]. See also [31] and [24], Proposition 10.17.

**Corollary 9.** Let \( N \) be a normal subgroup of a \( p \)-group \( G \), \( p > 2 \). If \( N \) contains an elementary subgroup of order \( p^4 \), then \( N \) contains a \( G \)-invariant elementary abelian subgroup of order \( p^4 \).

This follows from Theorem 7. If \( N = G \) in Corollary 9, we obtain Hobby’s result. See also [31] and [24], Proposition 10.17.

**Lemma 10.** (O. J. Schmidt [34], J. A. Gol’fand [23]; see also [28], Satz 3.5.2.) Let \( S \) be a minimal non-nilpotent group. Then \( S \) is a \( \langle p, q \rangle \)-group, \( p, q \) are different primes. Let \( P \in \text{Syl}_p(S) \), \( Q \in \text{Syl}_q(S) \). One of Sylow subgroups of \( S \), say \( Q \), is normal in \( S \). The subgroup \( Q = S' \) is elementary abelian or special, \( P \) is cyclic and \( |P : P \cap Z(S)| = p \). If \( q > 2 \), then \( \exp(Q) = q \). \( p \) is a Zsigmondy prime for the pair \( \langle q, \log_q|Q/Z(G) \cap Q| \rangle \). If \( Q \) is nonabelian, then \( \log_q|Q/Z(Q)| \) is even.

**Theorem 11** ([21], Lemma 8.8). Suppose that \( Q \) is a \( q \)-group, \( q > 2 \), \( \alpha \) an automorphism of \( Q \) of prime order \( p \). If \( p = 1 \pmod{q} \), and \( Q \) contains a maximal subgroup \( Q_0 \) such that \( Q_0 \) has no normal elementary abelian subgroups of order \( q^3 \), then \( p = 1 + q + q^2 \) and \( Q \) is elementary abelian of order \( q^3 \).
Proof. By Corollary 8, $Q_0$ has no elementary abelian subgroups of order $q^3$. Therefore, every subgroup of exponent $q$ in $Q_0$ is generated by two elements and its order is at most $q^3$. In particular, $Q$ has no elementary abelian subgroups of order $q^3$.

Let $W = \langle \alpha \rangle \cdot G$ be a natural semidirect product. By assumption, $p > q + 1$ so that $p + q^2 - 1$ and $|Q| > q^2$. Let $S$ be a minimal nonnilpotent subgroup of $W$. Without loss of generality, we may assume that $\langle \alpha \rangle = P \in \text{Syl}_p(S)$. Suppose that $|Q| = q^3$. Since $p + q^2 - 1$, it follows that $Q$ is elementary abelian. Since $(p, q^2 - 1) = 1$, it follows that $p|q^3 - 1$ (in fact, $p|\text{Aut}(Q)| = (q - 1)(q^2 - 1)(q^3 - 1)$). Then $p = q^2 + q + 1$ by [21], Lemma 5.1. Now let $|Q| > q^3$. Obviously, $S \cap Q \leq \text{Syl}_q(S)$. By Lemma 10, $\exp(S \cap Q) = q$. Since $|S \cap Q| \leq q^3$ by the result of the first paragraph of the proof, it follows that $|S \cap Q| \leq q^4$.

Assume that $|S \cap Q| = q^4$. Then $S \cap Q_0$ is nonabelian (since it is of order $q^3$ and exponent $q$). In particular, $\Phi(S \cap Q) > (1)$. Since $P$ centralizes $\Phi(S \cap Q)$, the minimal number of generators of $S \cap Q$ is 3 (recall that $p + q^2 - 1$). But this contradicts Lemma 10 (indeed, since $S \cap Q$ is nonabelian, the minimal number of generators of $S \cap Q$ is even).

Assume that $|S \cap Q| = p^2$. Then $S \cap Q$ is elementary abelian by Remark 1. In that case $\alpha$ is a fixed-point-free automorphism of $S \cap Q$. As previously, $p = q^2 + q + 1$. Let $Z_1 = \Omega_1(Z(Q))$. Since $(S \cap Q)Z_1$ is elementary abelian and $Q$ has no elementary abelian subgroups of order $q^4$, it follows that $Z_1 = S \cap Q$, and so $\langle \alpha, Z_1 \rangle$ is a Frobenius group with kernel $Z_1$. Since $Z_1 \cap \Phi(Q)$ is $\alpha$-invariant, $Z_1 \not\leq Q_0$ ($Q_0$ has no elementary abelian subgroups of order $q^3$) and $\Phi(Q)$ is $\langle \alpha \rangle$-invariant, it follows that $Z_1 \cap \Phi(Q) = (1)$. Therefore, $Z(Q) \cap \Phi(Q) = (1)$ so that $\Phi(Q) = (1)$.

In the case considered, $Q = Z_1$ (an elementary abelian group of order $q^3$). This completes the proof.

Theorem 12 (compare with [4], Theorem 5.4). Let $G$ be a $p$-group of order $p^n$, $p > 2$, $n \in \mathbb{N}$, $n \geq 4$. Then the number of metacyclic subgroups of order $p^n$ in $G$ is divisible by $p$, unless $G$ is metacyclic or a 3-group of maximal class.

Proof. We use induction on $|G|$. Assume that $G$ is not metacyclic (otherwise the result follows by Sylow’s Theorem, since all subgroups of $G$ are metacyclic). In that case, $n < m$. Let $\mathfrak{M}(G)$ denote the set of all metacyclic subgroups of order $p^n$ in $G$.

(i) Let $G$ be a 3-group of maximal class. Then it contains only one metacyclic subgroup of index 3 [20] (it is essential that $n > 3$; a Sylow 3-subgroup of the symmetric group $S_9$ is a group of maximal class containing exactly two metacyclic subgroups of index 3). We claim that in that case $|\mathfrak{M}(G)| \equiv 1 \pmod{p}$. By what we have just said, our claim is true for
Let $n = m - 1$. Let $n < m - 1$. Let $\mathcal{M}$ denote the set of all maximal subgroups of $G$ (obviously, $|\mathcal{M}| = 4$). Let $H \in \mathcal{M}$. If $H$ is of maximal class, then by the induction hypothesis, $|\mathcal{M}(H)| = 1 \pmod{3}$. If $H$ is metacyclic, then $|\mathcal{M}(H)| = 1 \pmod{3}$ by Sylow's Theorem. Any subgroup of index 3 in $G$ is metacyclic or of maximal class (since $m \geq 5$). Hence, by Hall's enumeration principle [26], $|\mathcal{M}(G)| = \sum_{H \in \mathcal{M}}|\mathcal{M}(H)| = |\mathcal{M}| = 4 \equiv 1 \pmod{3}$. In what follows, $G$ is not a 3-group of maximal class.

(ii) Let $n = m - 1$. Without loss of generality, we may assume that $H \in \mathcal{M}$ is metacyclic (otherwise, $\mathcal{M}(G) = 0$). By what we have proved, (i) and [17], $G$ contains a normal subgroup $R$ of order $p^2$ and exponent $p$. In view of the existence of $H$, $G$ has no subgroups of order $p^4$ and exponent $p$ and $G$ is generated by three elements (since $H$ is generated by two elements). If $R < F \in \mathcal{M}$, then $F$ is not a 3-group of maximal class (by [20], a $p$-group of maximal class and order at least $p^{p+2}$ has no normal subgroups of order $p^4$ and exponent $p$; note that $n \geq 3 + 2$) and is not metacyclic. Let $\mathcal{C}$ be the set of all normal subgroups of $G$ of order $p^3$ and exponent $p$. By [6] or [17] and (i), $|\mathcal{C}| = 1 \pmod{p}$. Let $\mathcal{M}_1$ be the set of all normal subgroups $L$ of $G$ such that $L$ contains an element of the set $\mathcal{C}$. By [6], the number of elements of the set $\mathcal{C}$ in any element of $\mathcal{M}_1$ is 1 (mod $p$). Therefore, arguing as in the end of the proof of Theorem 7, we obtain $|\mathcal{M}_3| = 0 \pmod{p}$. Let $T \in \mathcal{M} - \mathcal{M}_1$. Then by [6], $T$ is metacyclic or a 3-group of maximal class. The number of subgroups of maximal class and index $p$ in $G$ is divisible by $p^2$ by [6] or [17]. Since $|\mathcal{M}_1| = 1 \pmod{p}$, it follows that $|\mathcal{M} - \mathcal{M}_1| = 1 \pmod{p}$. The number of subgroups of maximal class and index $p$ in $G$ is divisible by $p^2$ by [6] or [17]. Therefore, $|\mathcal{M}(G)| = 0 \pmod{p}$.

(iii) $n < m - 1$. Applying Hall's enumeration principle, (i) and (ii), we complete the proof.

Note, that Theorem 12 is true for $n = 3$ (see [6, 9, 15]. It is interesting to study $|\mathcal{M}(G)| \pmod{2}$ for 2-groups $G$.

**Lemma 13.** Let $G = G_0 > G_1 > \cdots > G_n = \{1\}$ be a chain of normal subgroups of a group $G$. Set

$$A = \{a \in \text{Aut}(G) \mid (xG_i)^a = xG_i \text{ for all } x \in G_{i-1} - G_i, i = 1, \ldots, n\},$$

(i.e., $A$ stabilizes that chain). Let $p$ be a prime number such that $p \nmid |Z(G_{i-1}/G_i)|$ for $i = 2, \ldots, n$. Then $p \nmid |A|$.

**Proof.** We use induction on $n$. We may assume that $n > 1$ (otherwise the lemma is true). Obviously, $A$ is a subgroup of $\text{Aut}(G)$. Suppose that $A$ contains an element $\alpha$ of order $p$. Let $W = \langle \alpha \rangle \cdot G$ be the natural direct product. By the induction hypothesis, $\langle \alpha \rangle \cdot G_{n-1} < W$. By assumption, $\alpha$
centralizes $G_{n-1}$ so that $\langle \alpha \rangle \cdot G_{n-1} = \langle \alpha \rangle \times G_{n-1}$. Assume that $\langle \alpha \rangle$ is not characteristic in $H = \langle \alpha \rangle \times G_{n-1}$. Then there exists $\phi \in \text{Aut}(H)$ such that $\phi(\langle \alpha \rangle) = \langle \beta \rangle \neq \langle \alpha \rangle$. Obviously, $\langle \beta \rangle \triangleleft H$ and $\langle \alpha, \beta \rangle$ is a subgroup of $Z(H)$ of order $p^2$. Then $\langle \alpha, \beta \rangle \cap G_{n-1}$ is a subgroup of $Z(G_{n-1})$ of order $p$, contradicting the assumption. Thus, $\langle \alpha \rangle$ is characteristic in $\langle \alpha \rangle \times G_{n-1}$. Then $\langle \alpha \rangle \triangleleft W$, so that $\alpha$ centralizes $G$. In that case, $\alpha = \text{id}$, which is a contradiction.

\textbf{Lemma 14 (21, Lemma 8.1).} If $G$ is a $p$-group, then the stability group $A$ of a chain $G = G_0 > G_1 > \cdots > G_n = \{1\}$ is a $p$-group.

\textbf{Proof.} We use induction on $n$. Suppose that $A$ contains an element $a$ of order $p$ for some $p \in \pi'$. By the induction hypothesis, $a$ centralizes $G_1$. Let $x \in G_1$; then $x^a = xy$ with $y \in G_1$. Then $x = x^{xy}$. It follows that $y = 1$ so that $a = 1$—contradiction.

\textbf{Lemma 15.} Let $G$ be a $p$-group and suppose that $D$ is a subgroup generated by all elements of $G$ of orders $4$, $p$ for all $p \in \pi$. Let $\alpha$ be a $p$-automorphism of $G$. If $\alpha$ centralizes $D$, then $\alpha = \text{id}$.

\textbf{Proof.} Suppose that the lemma is false. Without loss of generality, we may assume that $o(\alpha) = q \in \pi'$. Let $W = \langle \alpha \rangle \cdot G$. For every $p \in \pi$ there exists $P \in \text{Syl}_p(G)$ such that $P^\alpha = P$. Since $\alpha \neq \text{id}$, we may assume that $\alpha$ induces a nonidentity automorphism of $P$. Let $H$ be a minimal nonnilpotent subgroup in $G_1 = \langle \alpha \rangle \cdot P(\leq W)$. Without loss of generality, we may assume that $\alpha \in H$. Obviously, $H \cap P \in \text{Syl}_p(H)$. By Lemma 10, $H \cap P \leq D$. This means that $\alpha$ centralizes $H \cap P$ so $H$ is nilpotent—contradiction.

\textbf{Lemma 16.} Let $U$ be an abelian subgroup of a $p$-group $G$, let $\alpha$ be a $p'$-automorphism of $G$. If $\alpha$ centralizes $C_U(U)$, then $\alpha = \text{id}$.

This is exactly what was proved in [21], Lemma 8.12.

\textbf{Corollary 17} (compare with [21], Lemma 8.12). Let $U$ be an abelian subgroup of a $p$-group $G$. Let $\epsilon = 1$ if $p > 2$ and $\epsilon = 2$ if $p = 2$. Let $\alpha$ be a $p'$-automorphism of $G$ that centralizes $\Omega_\epsilon(C_G(U))$. Then $\alpha = \text{id}$.

\textbf{Proof.} Obviously $C_G(U)$ is $\alpha$-invariant. $\alpha$ centralizes $C_G(U)$ by Lemma 15. Now the result follows from Lemma 16.

\textbf{Corollary 18} (19); see also [22], Lemma 2.3. Let $p$, $G$, and $\epsilon$ be such as in Corollary 17. Let $U$ be a maximal abelian subgroup of $G$ of exponent $p^n$, where $n \geq \epsilon$. If a $p'$-automorphism $\alpha$ of $G$ centralizes $U$, then $\alpha = \text{id}$.
Proof. Let $x$ be an element of $C_G(U)$ of order at most $p^n$. Since $\langle U, x \rangle$ is abelian of exponent at most $p^n$, it follows that $x \in U$ by the maximal choice of $U$. Thus, $\Omega_c(C_G(U)) = U$, and the result follows from Corollary 17.

If in Corollary 18, $U$ is $\alpha$-invariant and $\alpha$ centralizes $\Omega_c(U)$, then $\alpha = \text{id}$ (by Lemma 15 and Corollary 18).

Proposition 19. Let $B$ be a subgroup of a $p$-group $G$ such that $C_G(B) \leq B$.

(a) If $B$ is nonabelian of order $p^3$, then $G$ is of maximal class.

(b) (M. Suzuki) If $|B| = p^3$, then $G$ is of maximal class.

Proof. We may assume that $|G| \geq p^4$ and the proposition has proved for groups of order $< |G|$.

(a) It is known that a Sylow $p$-subgroup of $\text{Aut}(B)$ is nonabelian of order $p^3$. Now, $C_G(B) = Z(B) = Z(G)$. Therefore, $N_G(B)/Z(G)$ is nonabelian of order $p^3$ (in particular, $|N_G(B)| = p^4$). Then $C_{G/Z(G)}(N_G(B)/Z(G)) < N_G(B)/Z(G)$ (otherwise $|N_G(B)| > p^4$). By the induction hypothesis, we see that $G/Z(G)$ is of maximal class. Since $|Z(G)| = p$, (a) is proved.

(b) Since $p^3 \leq |\text{Aut}(B)|$, it follows that $N_G(B)$ is nonabelian of order $p^3$. Since $C_G(N_G(B)) \leq C_G(B) = B < N_G(B)$, the result follows from (a).

Remark 3. We claim that a $p$-group $G$ is of maximal class if it contains a subgroup $H$ such that $N = N_G(H)$ is of maximal class. We may assume that $N < G$ and $|N| > p^3$ (by Proposition 19(a)). We use induction on $|G|$. Then $Z(G) = Z(N)$ so that $|Z(G)| = p$. Since $N < G$, $H$ is not characteristic in $N$. Therefore $|N:H| = p$. In particular, $Z(G) = Z(N) \leq \Phi(N) < H$. Then, $N_{G/Z(G)}(H/Z(G)) = N/Z(G)$ is of maximal class, and so, by the induction hypothesis, $G/Z(G)$ is of maximal class. Since $|Z(G)| = p$, the claim follows.

Question 2. Study the $p$-groups $G$ containing a subgroup $M$ of maximal class such that $C_G(M) < M$. (If $|M| > p^3$, then $G$ is not necessarily of maximal class.) The case $p = 2$ is of special interest.

Proposition 20 (compare with [24], Lemma 10.27). Let $A$ be a subgroup of a $p$-group $G$ such that $C_G(A)$ is metacyclic. If $|A| \leq p^2$, then $G$ has no normal subgroups of order $p^{n+1}$ and exponent $p$.

Proof. We may assume that $A \notin Z(G)$. Suppose that $D$ is a normal subgroup of $G$ of exponent $p$. We may assume that $|D| > p$ and $|A| > p^2$; then $C_D(A) > 1$. It follows from $H = AC_D(A) \leq C_G(A)$ that $H$ is
metacyclic, and so it is of order \( p^2 \) (since \( \exp(H) = p \)). We have \( C_{AD}(H) = H \). Therefore, \( AD \) is of maximal class by Proposition 19(b). By [20], \( AD \) has no subgroups of order \( p^{p+1} \) and exponent \( p \), so that \( |D| < p^{p+1} \).

**Question 3.** Study the groups \( G \) of Proposition 20 in the case when \( |A| = p \), in detail.

**Proposition 20**. Let \( G \) be a metacyclic \( p \)-group, containing a nonabelian subgroup \( B \) of order \( p^3 \). Then

(a) If \( p = 2 \), then \( G \) is of maximal class.

(b) If \( p > 2 \), then \( |G| = p^3 \).

**Proof.** Let the proposition has proved for all groups of order < \( |G| \). We may assume that \( |G| > p^3 \).

Let \( B \leq M < G \), where \( M \) is maximal in \( G \).

(a) By the induction hypothesis, \( M \) is of maximal class. Since \( G \) has exactly three maximal subgroups, the number of subgroups of maximal class and index 2 in \( G \) is not divisible by 4. Therefore, \( G \) is of maximal class by 5, Section 5.

(b) By the induction hypothesis, \( |M| = p^3 \), and so \( |G| = p^4 \). Obviously, \( G/G' \) is abelian of type \( (p^2, p) \). Let \( C_1/G', \ldots, C_{p}/G' \) be all cyclic subgroups in \( G/G' \) of order \( p^2 \). Then \( C_1, \ldots, C_p \) are distinct abelian subgroups of \( G \) of index \( p \). By Lemma 3, all maximal subgroups of \( G \) are abelian, contradicting the existence of \( B \).

**Proposition 20**. Let \( B \) be a nonabelian subgroup of order \( p^3 \) in a \( p \)-group \( G \), \( p > 2 \). Suppose that \( G \) has no element \( x \) such that \( \langle B, x \rangle = B \times \langle x \rangle \). Then:

(a) \( C_G(B) \) is cyclic.

(b) \( G \) has no \( B \)-invariant subgroups of order \( p^{p+1} \) and exponent \( p \).

**Proof.** (a) Obvious.

(b) Assume that \( H \) is a \( B \)-invariant subgroup of order \( p^{p+1} \) and exponent \( p \) in \( G \). Without loss of generality, we may assume that \( G = BH \). By [20], \( G \) is not of maximal class. Therefore, \( C_G(B) \nleq B \) by Proposition 19(a). In particular, \( |C_G(B)| > p \) and \( B \nleq H \), i.e., \( G \neq H \). By (a), \( |C_G(B) \cap H| = p \). It follows that \( C_G(B) \cap H = B \cap H \leq Z(H) \). Let \( C \) be a cyclic subgroup of order \( p^2 \) in \( C_G(B) \). Then \( K = BC \cap H \) is a normal noncyclic subgroup of order \( p^2 \) in \( BC \), \( |BC| = p^4 \). Since \( BC/Z(B) = B/Z(B) \times K/Z(B) \) is abelian and \( p > 2 \), it follows that \( \exp(BC) = p \), which is a contradiction (since \( C \) is cyclic of order \( p^2 \)).
It is essential, in the proof of (b), that $\Omega_1(BC) = B$.

**Remark 4.** Let $H$ be a normal subgroup of $G$ and $H \leq \Phi(G)$. Suppose that, whenever $N \triangleleft H$ and $H' \neq N$, then $N \triangleleft G$. We claim that $H$ is abelian. Suppose that $G$ is a counterexample of minimal order. Let $S$ be a normal subgroup of $H$ such that $H/S$ is nonabelian but every proper epimorphic image of $H/S$ is abelian. By assumption, $S \triangleleft G$. By the induction hypothesis, $S = \{1\}$. In particular $|H'| = p$. Let $K$ be a $G$-invariant subgroup of order $p^2$ in $H$. Then $H \leq \Phi(G) < C_G(K)$, since $|G:C_G(K)| \leq p$. In particular, $K \leq Z(H)$, and so $H$ is not of maximal class.

By Corollary 5 we may assume that $K$ is noncyclic. Then $Z(H)$ contains a subgroup $L$ of order $p$ such that $L \neq H'$. Obviously, $L \triangleleft G$. Then $H/L$ is nonabelian, contrary to the choice of $S$.

**Remark 5.** Suppose that a $p$-group $G$ contains an elementary abelian subgroup of order $p^3$. Let $E$ denote the subgroup generated by all elementary abelian subgroups of order $p^3$ in $G$. Suppose that $\Omega_1(G) \neq E$, i.e., $G$ contains a subgroup $L$ of order $p$ such that $L \geq E$. If $D$ is an $L$-invariant subgroup of exponent $p$ in $E$ then $|D| \leq p^p$ (by Proposition 19 and [20], if $|D| > p^p$, then $|C_{LD}(L) \cap D| > p^3$).

**Proposition 21** (compare with [36], p. 69, Lemma). Let $G$ be a nilpotent group and let $G/G'$ be abelian of rank $d$. Suppose that $|G|^d \leq |G/Z(G)|$. If an automorphism $\alpha$ of $G$ leaves every element of $G/G'$ fixed, then $\alpha$ is an inner automorphism of $G$.

**Proof.** Let $G/G' = \langle x_1G' \rangle \times \cdots \times \langle x_dG' \rangle$. Since $G' \leq \Phi(G)$, it follows that $G = \langle x_1, \ldots, x_d \rangle$. Let $A$ be the set of all automorphisms of $G$ which leave every element of $G/G'$ fixed; then $\text{Inn}(G) \leq A \leq \text{Aut}(G)$ (since every coset of $G'$ is $G$-invariant). If $\alpha \in A$, then, for $i = 1, \ldots, d$, we obtain $x_i'^{\alpha} = x_i y_i$ where $y_i \in G'$. Obviously, $\alpha$ is uniquely determined by elements $y_1, \ldots, y_d$. There are $|G'|^d$ distinct $d$-sequences $\{y_1, \ldots, y_d\}$ of elements in $G'$. Hence we have $|A| \leq |G'|^d$. On the other hand, by what we have just proved and assumption, $|G'|^d \leq |G/Z(G)| = |\text{Inn}(G)| \leq |A| \leq |G'|^d$. This proves that $A = \text{Inn}(G)$. In particular, $\alpha \in \text{Inn}(G)$. $\square$

It is possible to replace $G'$ (in Proposition 21) by a subgroup $N$ such that $G' \leq N \leq \Phi(G)$ and $|N|^d \leq |G/Z(G)|$. Extra-special $p$-groups and nonabelian $p$-groups $G$ with two generators and $|G'| = p$ satisfy the assumptions of Proposition 21.

**Corollary 22** (compare with [36], (4.17)). Let $G \leq W$, where $W$ is a group and $G$ is a nilpotent subgroup such that $G/G'$ is abelian of rank $d$ and $|G'|^d \leq |G/Z(G)|$. If $[G, W] \leq G'$, then $W = GC_w(G)$.

**Proof.** By assumption $G \leq W$. Let $w \in W$. Conjugation by $w$ induces an automorphism $\alpha$ in $G$. If $g \in G$, then by assumption, $[w, g] = y \in G'$.
so that \((g^{-1})^\alpha = w^{-1}g^{-1}w = yg^{-1}\). Hence \(\alpha\) leaves every element of 
\(G/G\) fixed. Therefore, by Proposition 21, \(\alpha \in \text{Inn}(G)\). This means that 
for each \(w \in W\), there exists \(u \in G\) such that \(w^{-1}gw = u^{-1}gu\) for all 
\(g \in G\). Thus, \(wu^{-1} \in C_w(G)\), and so \(w \in C_w(G)G\) for each \(w \in W\). This 
means that \(W = C_w(G)\).

A \(p\)-group \(G\) is said to be generalized regular if, whenever \(x^p = y^p\) 
\((x, y \in G)\), then \((x^{-1}y)^p = 1\). If \(G\) is a generalized regular \(p\)-group, then 
\(\exp(G) = p\). Regular \(p\)-groups are generalized regular (see [28], Kapitel 3).

**Proposition 23** (compare with [36], p. 73, Lemma). *Let a \(p\)-group \(Q\) 
act on a generalized regular \(p\)-group \(G\). If \(Q\) acts trivially on \(\Phi(G)\), then 
\([G, Q] \leq \Omega_{1}(G)\).*

*Proof.* If \(x \in G\), then \(x^p \in \Phi(G)\). Hence, for any \(y \in Q\), we have 
\(x^p = (x^p)^y = (x^y)^p\). Therefore, \([x, y]^p = (x^{-1}x^y)^p = 1\) (since \(G\) is 
generalized regular), so that \([G, Q] \leq \Omega_{1}(G)\).

**Lemma 24.** *Let \(G\) be a solvable group of odd order, \(p \in \pi(G)\), \(O_p(G)\) 
\(= \{1\}. If O_p(G) has no elementary abelian subgroups of order \(p^3\), then a 
Sylow \(p\)-subgroup is normal in \(G\).*

*Proof.* Let \(B\) be a critical Thompson’s subgroup of \(O_p(G)\) (for its 
construction and properties, see [3], Corollary 3) and set \(T = \Omega_{1}(B)\). Since 
\(B\) is of class at most two and \(p > 2\), \(\exp(T) = p\). Obviously, \(B \leq G\). Since 
\(C_T(O_p(G)) \leq O_p(G)\), it follows from [3], Corollary 3(e) that \(C_B(B) \leq B\). 
Therefore, by Lemma 15, \(C_G(T)\) is a normal \(p\)-subgroup of \(G\). Since \(T\) has 
no elementary abelian subgroups of order \(p^3\), it follows that \(|T| \leq p^3\) 
(recall that \(T\) is of exponent \(p\)). If \(|T| = p\), then \(|G/C_G(T)||p - 1\), and 
therefore \(C_G(T)\) is a normal Sylow \(p\)-subgroup of \(G\). Let \(|T| = p^2\). Then 
\(G/C_G(T)\) is isomorphic to a subgroup of odd order of \(\text{Aut}(T) \cong GL(2, p)\). 
Since in that case a Sylow \(p\)-subgroup of \(G/C_G(T)\) is normal (this follows 
from the structure of \(GL(2, p)\)), all is done. Let now \(|T| = p^3\). By assumption, 
\(T\) is nonabelian of exponent \(p\). By Hall’s Lemma on \(p\)-automorphisms of 
\(p\)-groups, \(C_{G/T}(T/T')\) is a normal \(p\)-subgroup of \(G/T\). Since 
\((G/T)/C_{G/T}(T/T')\) is isomorphic to a subgroup of odd order in \(GL(2, p)\), 
the result follows as in the case \(|T| = p^2\).*

**Proposition 25** ([21], Lemma 8.13). *Let \(P\) be a Sylow \(p\)-subgroup of 
a solvable group \(G\) of odd order. Suppose that \(P\) has no elementary abelian 
subgroups of order \(p^3\). Then \(G'\) centralizes all chief \(p\)-factors of \(G\).*

*Proof.* Without loss of generality we may assume that \(O_p(G) = \{1\}\). 
Then \(P \not\leq G\), where \(P \in \text{Syl}_{p}(G)\) (by Lemma 24). If \(A/B\) is a chief factor 
of \(G\) of order \(p\), then \(G/C_{G/A}(A/B)\) is cyclic of order dividing \(p - 1\), and
so \( G' / B \leq C_{G/B}(A / B) \). The chief \( p \)-factors of \( G \) are of orders \( p \) or \( p^2 \) (see [17]). Let \( K / L \) be a chief factor of \( G \) of order \( p^2 \). If \( K \neq G' \), it follows that \( G' \) centralizes \( K / L \). Hence we have to consider the case when \( K \leq G' \). Without loss of generality we may assume that \( L = (1) \). Then \( K \leq P \leq F(G) \), and so \( P \) centralizes \( K \). Next, \( G / G_0(K) \) as a \( p' \)-subgroup of odd order in \( GL(2, p) \), is abelian. Therefore, \( G' \) centralizes \( K \). 

**Proposition 26.** Suppose that \( (1) \leq A < B \leq G \), where \( G \) is a \( p \)-group, \( B \) elementary abelian of order \( p^k \), \( 2 \leq k \leq 4 \). Then the number of elementary abelian subgroups of \( G \) of order \( p^k \) that contain \( A \) is congruent to 1 mod \( p \), unless \( p = 2 = k \), \( G \) is maximal class.

**Proof.** Suppose that the proposition has proved for all \( p \)-groups of order \( < |G| \).

The result is true for \( A = (1) \) by Lemma 5, Theorems 6 and 7. Let \( A > (1) \). We may assume that \( B < G \). If \( |C_{G}(A)| = p^2 \), then \( G \) is of maximal class (by Proposition 19(b)), \( |A| = p \), and \( B \) is the unique elementary abelian subgroup of order \( p^2 \) containing \( A \). In that case, all is done. If \( C_{G}(A) \) is a 2-group of maximal class then \( G \) is (since, in that case \( G = C_{G}(A) \)). Therefore, without loss of generality, we may assume that \( A \leq Z(G) \). Let \( \mathcal{A} \) be the set of all maximal subgroups of \( G \) containing \( A \). By Sylow's Theorem, \( |\mathcal{A}| = 1 \) (mod \( p \)). For \( A \leq H \leq G \), let \( s_k(H) \) denote the number of elementary abelian subgroups of \( H \) of order \( p^k \) containing \( A \). By Hall's enumeration principle [26],

\[
s_k(G) = \sum_{H \in \mathcal{A}} s_k(H) \pmod{p}. \tag{4}
\]

If \( s_k(H) \equiv 1 \pmod{p} \) for all \( H \in \mathcal{A} \), then \( s_k(G) \equiv 1 \pmod{p} \) by (4). If every elementary abelian subgroup of \( G \) of order \( p^k \) contains \( A \), the result follows from Lemma 5, Theorems 6 and 7. Therefore, we may assume that there exists in \( G \) an elementary abelian subgroup \( T \) of order \( p^k \) such that \( A \not\leq T \). Then (the elementary abelian subgroup since \( A \leq Z(G) \)) \( A \) contains an elementary abelian subgroup \( F \) such that \( A < F \), \( |F| = p^{k+1} \), and \( L \cap F \) is elementary abelian of order at least \( p^k \) for every maximal subgroup \( L \) of \( G \) (and so \( s_k(L) > 0 \) since \( A \leq Z(L) \)). A's previously, we may assume that \( s_k(H) \equiv 1 \pmod{p} \) for some \( H \in \mathcal{A} \). Therefore, by the induction hypothesis, \( p = 2 \), \( |A| = 2 \), and \( k = 2 \), \( H \) is cyclic, dihedral, or semidihedral, \( A \leq Z(H) \). Then \( A < \Phi(G) \). Suppose that \( G \) is not a 2-group of maximal class. If \( H \) is cyclic, then \( s_k(G) = e_k(G) = 1 \) (this follows from the classification of 2-groups with cyclic subgroups of index 2). If \( H \) is dihedral or semidihedral, then \( s_k(H) \) is even. If \( F \) is a maximal subgroup of \( G \) that does not contain \( A \), then \( G = A \times F \) and \( \mathcal{A} \) has no
subgroups of maximal class. Now the result follows from (4) by induction (since, in that case, the number of elements of maximal class in \( \mathcal{M}_4 \) is divisible by 4; see [4] Section 5).

By [31], Proposition 26 is true for \( k = 5 \) as well.

**Question 4.** Consider the case \( p = 2 \) in all propositions of this note.

**Conjecture.** Let \( A < B < G \), where \( G \) is a \( p \)-group, \( p > 2 \), \( |A| = p \), \( B \) is abelian of type \((p^n, p)\), \( n > 1 \). Then the number of subgroups of \( G \), that are isomorphic to \( B \) and contain \( A \), is congruent to 0 (mod \( p \)) (with a small number of exceptions).

Let \( D_8 \) be the dihedral group of order 8, \( C_2 \) the group of order 2.

**Remark 6.** The following assertion is an analog of Theorem 1 for \( p = 2 \):

Let \( A < B \leq G \), where \( G \) is a 2-group, \( \exp(B) = 2 \), \( |A| \geq 4 \). If \( G \) has no subgroups isomorphic to \( D_8 \times C_2 \), then the number of elementary abelian subgroups \( L < G \) such that \( A < L \) and \( |L:A| = 2 \) is odd.

We will prove that the preceding assertion is trivial. Indeed, let \( E \) be a maximal elementary abelian subgroup of \( G \), \( |E| > 4 \). Suppose that an involution \( u \) normalizes \( E \) but \( u \notin C_G(E) \). Then \( E \) contains an involution \( v \) such that \( uv \neq vu \). In that case, \( D = \langle u, v \rangle \cong D_8 \) (indeed, the dihedral group \( D \) is contained in the subgroup \( \langle E, v \rangle \) of exponent 4). Set \( Z(D) = \langle c \rangle \); then \( D \cap E = \langle c \rangle \times \langle v \rangle \). By Proposition 19(b), \( |C_E(u)| > 2 \) (since \( \langle E, u \rangle \) is not of maximal class: it contains an elementary abelian subgroup of order 8). Since \( D \cap E \) does not centralize \( D \), there exists in \( C_E(u) \) an involution \( w \neq c \). Obviously, \( w \) centralizes \( D = \langle D \cap E, u \rangle \). Therefore, \( \langle D, w \rangle \cong D_8 \times C_2 \), contrary to the assumption of the theorem. Thus, every involution that normalizes \( E \), also centralizes \( E \). Hence \( \Omega_1(N_G(E)) = E \), and so \( E \) is characteristic in \( N_G(E) \). In that case, \( N_G(E) = G \) and \( E = \Omega_1(G) \). Our assertion follows immediately (since we may assume without loss of generality that \( \Omega_1(G) = E \)).

The foregoing reasoning shows that if \( G \) is a 2-group such that \( \Omega_1(G) \) is nonabelian and \( G \) has no subgroups isomorphic to \( D_8 \times C_2 \), then it has no elementary abelian subgroups of order 8.

Numerous counting theorems for \( p \)-groups (which are, as we saw previously, assertions on the existence of normal subgroups with given structure) were proved or announced in [3–16] (some of foregoing results are taken from these papers, but here we offer new proofs), [29, 31, 33]. In particular, A. Mann proved that the number of nonabelian subgroups of order \( p^3 \) in a \( p \)-group \( G \) of order at least \( p^3 \) is divisible by \( p^7 \) (and so the
number of abelian subgroups of order $p^3$ in $G$ is $\equiv 1 + p \pmod{p}$ by Kulakov's Theorem [32] (see also [35]) and [6], Section 5. Next, Mann proved (see [16], Theorem B) that if noncyclic Sylow $p$-subgroup $S$ of $G$ is of order $p^n$, $S$ is not a 2-group of maximal class, $n \in \mathbb{N}$ and $p^n < |S|$, then the number of subgroups of order $p^n$ in $G$ is $\equiv 1 + p \pmod{p^2}$. Note that about all of the papers [3–16] were inspired by [21], Section 8 and [17–20].

REFERENCES

6. Y. Berkovich, A generalization of theorems of Ph. Hall and Blackburn and applications to irregular $p$-groups, Math USSR Izv. 35 (1971), 815–844.
16. Y. Berkovich, On the number of solutions of $x^{p^k} = 1$ in a finite $p$-group, Rend. Lincei, Mat. Appl. 6 (1995), 5–12.