GLASNIK MATEMATIČKI
Vol. 50(70)(2015), 101 – 161

# CLASSIFICATION OF FINITE $p$-GROUPS WITH CYCLIC INTERSECTION OF ANY TWO DISTINCT CONJUGATE SUBGROUPS

Zvonimir Janko
University of Heidelberg, Germany

Abstract. We give a complete classification of non-Dedekindian finite $p$-groups in which any two distinct conjugate subgroups have cyclic intersection (Theorems A, B and C).

## 1. Introduction

The purpose of this paper is to give a complete classification of finite non-Dedekindian $p$-groups (i.e., $p$-groups that possess non-normal subgroups) in which any two distinct conjugate subgroups have cyclic intersection (Problem 1572 stated in [3]).

In Theorem 16.2 in [1], Theorem A and Theorem B are completely determined finite non-Dedekindian $p$-groups all of whose non-normal subgroups are either cyclic, abelian of type $(p,p)$ or ordinary quaternion. Since in these groups any two distinct conjugate subgroups have a cyclic intersection, so these results can be considered as a good start in solving problem 1572. Therefore, after proving Theorems A and B, we may always assume that there is in a title group $G$ a non-normal subgroup which is neither cyclic nor abelian of type $(p,p)$ nor an ordinary quaternion group and such groups will be completely determined in Theorem C. Now we state our main results.

Theorem A. *Let $G$ be a $p$-group all of whose non-normal subgroups are cyclic or abelian of type $(p,p)$. Assume in addition that $G$ possesses a non-normal abelian subgroup of type $(p,p)$. Then $G$ is one of the following groups*

2010 *Mathematics Subject Classification.* 20D15.
*Key words and phrases.* Finite $p$-groups, 2-groups of maximal class, Dedekindian $p$-groups, ordinary quaternion group, maximal non-normal subgroups, conjugate subgroups.

*(where* $\mathrm{S}(p^3)$, $p > 2$, *denotes the nonabelian group of order* $p^3$ *and exponent* $p$*):*

(a) $G \cong \mathrm{D}_{16}$ *or* $\mathrm{SD}_{16}$.
(b) $G = LZ$, *where* $L \cong \mathrm{S}(p^3)$, $p > 2$, *is normal in* $G$, $Z \cong \mathrm{C}_{p^2}$, $L \cap Z = \mathrm{Z}(L) = \mathrm{Z}(G)$.
(c) $G$ *is any nonabelian group of order* $p^4$ *with an elementary abelian subgroup of index* $p$.
(d) $p = 2$ *and* $G \cong (\mathrm{D}_8 * \mathrm{Q}_8) \times \mathrm{C}_2$, *where* $\mathrm{D}_8 \cap \mathrm{Q}_8 = (\mathrm{D}_8)'$ *or* $G \cong \mathrm{H}_{16} * \mathrm{Q}_8$ *with* $\mathrm{H}_{16} \cap \mathrm{Q}_8 = (\mathrm{H}_{16})'$, *where* $\mathrm{H}_{16}$ *is the nonmetacyclic minimal nonabelian group of order* 16.
(e) $G \cong \mathrm{M}_{p^{s+1}} \times \mathrm{C}_p$, $s \geq 3$.
(f) $G = (Z * S) \times \mathrm{C}_p$, *where* $Z \cong \mathrm{C}_{p^{s+1}}$, $s \geq 1$, $Z \cap S = S'$, *and either* $p = 2$ *and* $S \cong \mathrm{D}_8$ *or* $p > 2$ *and* $S \cong \mathrm{S}(p^3)$ *or*
$G = Z * S$, *where* $Z \cong \mathrm{C}_{p^{s+1}}$, $s \geq 1$, $Z \cap S = S'$, *and* $S$ *is the nonmetacyclic minimal nonabelian group of order* $p^4$.
(g) $G$ *is an* $\mathrm{A}_2$*-group of order* $p^5$ *from Proposition 71.4(b2) in [2] for* $\alpha = 1$.
(h) $G \cong \mathrm{Q}_8 * \mathrm{Q}_8 * \mathrm{Q}_8$, *an extraspecial group of order* $2^7$ *and type " − ".*
(i) $G = (A_1 * A_2)\mathrm{Z}(G)$, *where* $A_1$ *and* $A_2$ *are minimal nonabelian* $p$*-groups and* $\mathrm{Z}(G)$ *is cyclic. In case* $p = 2$, $A_1$ *and* $A_2$ *are isomorphic to one of* $\mathrm{D}_8$, $\mathrm{Q}_8$ *and* $\mathrm{M}_{2^n}$, $n \geq 4$, *where in case* $A_1 \cong \mathrm{Q}_8$ *and* $A_2 \cong \mathrm{D}_8$ *we must have* $|\mathrm{Z}(G)| > 2$. *In case* $p > 2$, $A_1$ *and* $A_2$ *are isomorphic to one of* $\mathrm{S}(p^3)$ *or* $\mathrm{M}_{p^n}$, $n \geq 3$.

*Conversely, all the above groups satisfy the assumptions of the theorem.*

THEOREM B. *Let* $G$ *be a* 2*-group all of whose non-normal subgroups are either cyclic, abelian of type* $(2,2)$ *or ordinary quaternion. Assume in addition that* $G$ *possesses a non-normal subgroup* $H$ *which is isomorphic to* $\mathrm{Q}_8$. *Then* $G$ *is isomorphic to one of the following groups :*

(a) $G \cong \mathrm{Q}_{32}$ *(a generalized quaternion group of order* 32*).*
(b) $G$ *is a unique* 2*-group of order* $> 2^4$ *with the property that* $\Omega_2(G) \cong \mathrm{Q}_8 \times \mathrm{C}_2$ *and we have* $|G| = 2^5$, *where this group (of class* 3*) is defined in part A2(a) of Theorem 49.1 in [2].*
(c) $G$ *is a splitting extension of a cyclic noncentral normal subgroup of order* 4 *by* $\mathrm{Q}_8$.
(d) $G = H_1 \times H_2$, *where* $H_1 \cong H_2 \cong \mathrm{Q}_8$.
(e) $G = \langle h_0, h_1 \rangle \langle g \rangle$, *where* $\langle h_0, h_1 \rangle \cong \mathrm{Q}_8$, $\mathrm{Z}(\langle h_0, h_1 \rangle) = \langle z \rangle$ , $\langle g \rangle \cong \mathrm{C}_{2^n}$, $n \geq 3$, $\langle h_0, h_1 \rangle \cap \langle g \rangle = \{1\}$, $\Omega_1(\langle g \rangle) = \langle z' \rangle$, $g^2 \in \mathrm{Z}(G)$, $[g, h_0] = 1$, *and* $[g, h_1] = z^\epsilon z'$, $\epsilon = 0, 1$. *Here we have* $|G| = 2^{n+3}$, $n \geq 3$, $G' = \Omega_1(G) = \langle z, z' \rangle \cong \mathrm{E}_4$, $G$ *is of class* 2 *and* $\mathrm{Z}(G) = \langle g^2 \rangle \times \langle z \rangle \cong \mathrm{C}_{2^{n-1}} \times \mathrm{C}_2$.
(f) $G = C * Q$, *where* $C \cong \mathcal{H}_2 = \langle a, b \mid a^4 = b^4 = 1,\ a^b = a^{-1} \rangle$, $Q \cong \mathrm{Q}_8$ *and* $C \cap Q = \langle a^2 b^2 \rangle = Q'$.

*Conversely, all the above groups satisfy the assumptions of the theorem.*

Theorem C. *Let $G$ be a $p$-group with a cyclic intersection of any two distinct conjugate subgroups. Assume in addition that $G$ has a non-normal subgroup which is neither cyclic nor abelian of type $(p,p)$ nor an ordinary quaternion group. Then $G$ is metabelian and $G$ is either a 2-group of maximal class and order $\geq 2^5$ (if $|G| = 2^5$, then $G \cong \mathrm{D}_{32}$ or $\mathrm{SD}_{32}$) or $G$ is a $p$-group of class at most 3 with $G' \neq \{1\}$ elementary abelian of order at most $p^2$ and $G$ is isomorphic to one of the groups defined in Propositions 3(b2), 5, 7, 8, 9, 10, 11 and 12 stated in the section 4.Proof of theorem C.*

*Conversely, all these groups satisfy the assumptions of our theorem.*

In this paper we shall consider only finite $p$-groups and our notation is standard (see [1]).

## 2. Proof of Theorem A

Let $G$ be a $p$-group all of whose non-normal subgroups are cyclic or abelian of type $(p,p)$ and we assume that $G$ possesses a non-normal abelian subgroup $H$ of type $(p,p)$. We set $K = \mathrm{N}_G(H)$ so that we have $H < K < G$ and $K \trianglelefteq G$. Since each subgroup $X$ of $G$ with $X > H$ is normal in $G$, it follows that $K/H$ is Dedekindian and $K/H$ has exactly one subgroup of order $p$. This implies that $K/H \neq \{1\}$ is either cyclic or $p = 2$ and $K/H \cong \mathrm{Q}_8$. Let $L/H$ be a unique subgroup of order $p$ in $K/H$ so that $L \trianglelefteq G$ and $\Omega_1(K) \leq L$. If $g \in G - K$, then $L = \langle H, H^g \rangle$ and so we have $\Omega_1(K) = L$.

Suppose that $K$ does not possess a $G$-invariant abelian subgroup of type $(p,p)$. By Lemma 1.4 in [1], we get $p = 2$ and $K$ is of maximal class. But $H$ is a normal four-subgroup in $K$ and so $K \cong \mathrm{D}_8$. Since $\mathrm{C}_G(H) = \mathrm{C}_K(H) = H$, it follows by a result of M. Suzuki (see Proposition 1.8 in [1]) that $G$ is also a 2-group of maximal class. In this case $H$ has exactly two conjugates in $K = L \cong \mathrm{D}_8$ and so $|G : K| = 2$ and $|G| = 2^4$. It follows that $G \cong \mathrm{D}_{16}$ or $\mathrm{SD}_{16}$ and we have obtained the groups stated in part (a) of our theorem.

In what follows we may assume that $K$ possesses a $G$-invariant abelian subgroup $U$ of type $(p,p)$. Since $\Omega_1(K) = L$, we have $U \leq L$ and so $L = HU$ with $|H \cap U| = p$. If $L$ is abelian, then $L \cong \mathrm{E}_{p^3}$. If $L$ is nonabelian, then in case $p > 2$ we have $L \cong \mathrm{S}(p^3)$ and in case $p = 2$ we must have $L \cong \mathrm{D}_8$. But the last case cannot happen since $U \trianglelefteq G$ and $L$ has exactly two four-subgroups which would imply that also $H \trianglelefteq G$, a contradiction. Hence we have either $L \cong \mathrm{E}_{p^3}$ or $p > 2$ and $L \cong \mathrm{S}(p^3)$.

Suppose that $p > 2$ and $L \cong \mathrm{S}(p^3)$. In that case we have

$$\langle z \rangle = H \cap U = L' = \mathrm{Z}(L) \leq \mathrm{Z}(G).$$

If $\mathrm{C}_G(L) > \langle z \rangle$, then take an element $x \in \mathrm{C}_G(L) - \langle z \rangle$ such that $x^p \in \langle z \rangle$ and consider the abelian subgroup $S = \langle h, z, x \rangle$ of order $p^3$, where $h$ is any element in $H - \langle z \rangle$. By our assumptions, we have $S \trianglelefteq G$. But $L \cap S = H = \langle h, z \rangle$ and so $H \trianglelefteq G$, a contradiction. We have proved that $\mathrm{C}_G(L) = \langle z \rangle$. Since an

$S_p$-subgroup of $\mathrm{Aut}(L)$ is isomorphic to $S(p^3)$, it follows that $|G : L| = p$ and $K = L$ so that $|G| = p^4$. Also note that $G/\langle z\rangle \cong S(p^3)$ and $G/K$ acting on $p+1$ subgroups of order $p^2$ (containing $\langle z\rangle$) fixes $U$ and acts transitively on $p$ other ones. Hence $U$ is the unique $G$-invariant subgroup of order $p^2$ in $L$. Set $V = C_G(U)$ so that $V$ is an abelian normal subgroup of order $p^3$ in $G$ and we have $G = LV$ with $L \cap V = U$. If $V \cong E_{p^3}$, then we get a group stated in part (c) of our theorem. Hence we may assume that there is an element $t$ of order $p^2$ in $V - U$ such that $t^p = z$. We have obtained a group from part (b) of our theorem.

From now on we may assume that $L \cong E_{p^3}$. If $|G/L| = p$, then $K = L$ is elementary abelian of order $p^3$ and index $p$ and again we have obtained the groups from part (c) of our theorem. Thus we may assume in what follows that $|G/L| > p$.

In the rest of the proof we fix our notation for:

$$E_{p^2} \cong H,\ K = N_G(H) \neq G,\ \Omega_1(K) = L,\ E_{p^2} \cong U \trianglelefteq G,$$

where

$$L = HU,\ H \cap U \cong C_p,$$

and $\{1\} \neq K/H$ is either cyclic or $p = 2$ and $K/H \cong Q_8$. Also we fix our assumptions that $L \cong E_{p^3}$ and $|G/L| > p$.

(i) First assume that there is a central element $z$ in $G$ of order $p$ which is contained in $H$.

In that case we have $|G : K| = p$ so that $K > L$ and therefore there is an element $v \in K - L$ of order $p^2$ with $v^p \in L - H$. We may choose a $G$-invariant subgroup $U \leq L$ of order $p^2$ so that $U \leq Z(G)$. The socle $\Omega_1(X)$ of any cyclic subgroup $X$ in $G$ of composite order is contained in $U$.

Indeed, acting with $G/K$ on $p+1$ subgroups of order $p^2$ in $L$ which contain $\langle z\rangle$, we see that $|G : K| = p$. Since $|G/L| > p$, we have $K > L$ and so there is an element $v \in K - L$ of order $p^2$, where $v^p \in L - H$. Considering $\langle v, z\rangle \cong C_{p^2} \times C_p$, we obtain

$$\langle v, z\rangle \trianglelefteq G \text{ and so } \mho_1(\langle v, z\rangle) = \langle v^p\rangle \trianglelefteq G.$$

Then we may set $E_{p^2} \cong U = \langle z, v^p\rangle \leq Z(G)$. Let $X$ be any cyclic subgroup of composite order in $G$ and assume that $\Omega_1(X) \nleq U$. But then $\Omega_1(X) \leq K$ and so $\Omega_1(X) \leq L$. Take an element $1 \neq u \in U \leq Z(G)$ and consider the subgroup $X \times \langle u\rangle \trianglelefteq G$ so that we get $\Omega_1(X) \trianglelefteq G$. Since $\Omega_1(X) \nleq U$, we get $L \leq Z(G)$ and so $H \trianglelefteq G$, a contradiction.

(i1) Suppose that $K/L$ is noncyclic. Then we have $p = 2$, $K/H \cong Q_8$, $|G| = 2^6$ and $K/L \cong E_4$. Since $\mho_1(K) \leq U \leq Z(G)$, $K/U$ is elementary abelian. Considering the Dedekindian group $G/U$ of order $2^4$ which possesses an elementary abelian subgroup $K/U$ of index 2, it follows that $G/U$ is abelian and so $G' \leq U$. Any two non-commuting elements in $G$ generate here a minimal nonabelian subgroup (see Lemma 65.2 in [2]). For any $g, h \in G$ we have $[g^2, h] = [g, h]^2 = 1$ and so $\mho_1(G) \leq Z(G)$. In particular, for any $g \in G - K$, $g^2 \in K - L$ is not possible and so $g^2 \in L$ and this implies $g^2 \in U$. Hence $\mho_1(G) \leq U$ and $\exp(G) = 4$. Since $Z(G) \leq K$, we get $Z(G) = U$. Because $G/L \cong E_8$, we have $C_G(L) > L$ and so $C_G(L) \leq K$ implies $C_K(L) > L$. Thus there is $v \in C_K(L) - L$ such that $v^2 \in U - H$. Let $h \in H - U$ and consider the subgroup $\langle h, v\rangle \cong C_2 \times C_4$ so that $\langle h, v\rangle \trianglelefteq G$ and

$$\Omega_1(\langle h, v\rangle) = \langle h, v^2\rangle \trianglelefteq G.$$

If $\langle h, v^2\rangle \not\leq Z(K)$, then there is $g \in G - K$ centralizing $\langle h, v^2\rangle$, a contradiction. We have proved that $H \leq Z(K)$ and so $C_G(L) = K$.

We have $Z(K) = L$ and so $|K'| = 2$ and $U = K' \times (H \cap U)$. Suppose that $\mho_1(K) = U$. Then there are elements $v_1, v_2 \in K - L$ such that $z_1 = v_1^2 \neq z_2 = v_2^2$, where $z_1, z_2 \in U - H$. Let $h \in H - U$ and $g \in G - K$. Since

$$\langle h, v_1\rangle \cong C_2 \times C_4 \text{ and } \langle h, v_2\rangle \cong C_2 \times C_4,$$

we have

$$\langle h, v_1\rangle \trianglelefteq G \text{ and } \langle h, v_2\rangle \trianglelefteq G \text{ and so } \langle h, z_1\rangle \trianglelefteq G \text{ and } \langle h, z_2\rangle \trianglelefteq G.$$

But this gives $h^g = hz_1 = hz_2$ and $z_1 = z_2$, a contradiction.

We have proved that $\mho_1(K) = \langle u\rangle$ is of order 2, where $u \in U - H$. It follows that $K/\langle u\rangle$ is elementary abelian and so $\mho_1(K) = K' = \langle u\rangle$. Let $k_1, k_2 \in K - L$ be such that $\langle k_1, k_2\rangle$ covers $K/L$. Since $k_1^2 = k_2^2 = u$ and $[k_1, k_2] = u$, we get $Q = \langle k_1, k_2\rangle \cong Q_8$ and $K = H \times Q$, $L = H \times \langle u\rangle$, where $Q \trianglelefteq G$.

Since $G' \leq U$ is elementary abelian, it follows that $G$ induces on $Q$ only inner automorphisms of $Q$ and so we have $G = Q * C$, where $C = C_G(Q)$ and $Q \cap C = \langle u\rangle$, $K \cap C = L$. Also we have $Z(C) = Z(G) = U$. By Lemma 1.1 in [1] we get $|C'| = 2$. On the other hand, let $h \in H - U$, $g \in C - L$ and $v \in Q$ with $v^2 = u$. Since

$$C_2 \times C_4 \cong \langle h, v\rangle \trianglelefteq G, \text{ it follows that } \Omega_1(\langle h, v\rangle) = \langle h, u\rangle \trianglelefteq G.$$

Thus we get $h^g = hu$ and so $u \in C'$. We have proved that $C' = Q' = \langle u\rangle = G'$.

Let $g$ be an element in $C - L$ and $h \in H - U$. If $g^2 \in U - \langle u\rangle$, then $C = \langle g, h\rangle \cong H_{16}$, where $H_{16}$ denotes the nonmetacyclic minimal nonabelian group of order 16. If $g^2 \in \langle u\rangle$, then we have $\langle g, h\rangle \cong D_8$ and so in this case $C = \langle g, h\rangle \times \langle z\rangle$, where $\langle z\rangle = H \cap U$. We have obtained the groups stated in part (d) of our theorem.

(i2) Suppose that $\{1\} \neq K/L$ is cyclic so that $K/H$ is cyclic of order $\geq p^2$. In this case we show that $G/L$ is abelian.

Indeed, assume that $G/L$ is nonabelian. Since $G/L$ is Dedekindian, it follows that $p = 2$ and $G/L \cong Q_8$. We also have $\Omega_1(G) = L$. Since $C_G(L) > L$

and $\mathrm{C}_G(L) \le K$, we get $\mathrm{C}_K(L) > L$. Let $v \in \mathrm{C}_K(L) - L$ with $o(v) = 4$ so that $v^2 \in U - H$ and let $h \in H - U$. Then

$$\mathrm{C}_2 \times \mathrm{C}_4 \cong \langle h, v\rangle \trianglelefteq G, \text{ and } \langle h, v^2\rangle \trianglelefteq G.$$

If $\langle h, v^2\rangle \not\le \mathrm{Z}(K)$, then there is $g \in G - K$ which centralizes $h$, a contradiction. Hence $\langle h, v^2\rangle \le \mathrm{Z}(K)$ and so $H \le \mathrm{Z}(K)$ which implies that $K$ is abelian.

Since $G/U$ is Dedekindian and nonabelian, it follows that $G/U$ is Hamiltonian. Let $Q/U$ be a subgroup in $G/U$ which is isomorphic to $\mathrm{Q}_8$ and set

$$Q_0/U = \mathrm{Z}(Q/U) = (Q/U)'.$$

Let $Q_1/U$ and $Q_2/U$ be two distinct cyclic subgroups of order 4 in $Q/U$ so that $Q_1$ and $Q_2$ are abelian and $Q_1 \cap Q_2 = Q_0$. It follows that $Q_0 \le \mathrm{Z}(Q)$ and so $Q_0 = \mathrm{Z}(Q)$. By Lemma 1.1 in [1], $|Q'| = 2$ and since $Q'$ covers $Q_0/U$, it follows that $Q_0 = U \times Q' \cong \mathrm{E}_8$. But then $Q_0 = \Omega_1(G) = L$ and so $K = \mathrm{C}_G(L) \ge Q$ is nonabelian, a contradiction. We have proved that $G/L$ is abelian and so $G/L$ is either cyclic of order $\ge p^2$ or $G/L$ is abelian of type $(p^s, p)$, $s \ge 1$.

(i2a) Assume that $G/L$ is cyclic. Let $g \in G - K$ so that $\langle g\rangle$ covers $G/L$ and let $\langle t\rangle = \Omega_1(\langle g\rangle)$ be the socle of $\langle g\rangle$, where $t \in U - H$ and $o(g) = p^s$, $s \ge 3$. We may set $t = g^{p^{s-1}}$ and so $\langle g^p\rangle$ covers $K/H \cong \mathrm{C}_{p^{s-1}}$. Also set $v = g^{p^{s-2}}$ so that $\langle v\rangle \cong \mathrm{C}_{p^2}$ and $v^p = t$.

Since $\langle g\rangle$ stabilizes the chain $L > U > \{1\}$, it follows that $\langle g^p\rangle$ centralizes $L$ and so $K$ is abelian. Consider the abelian subgroup $\langle h, v\rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^2}$, where $h$ is any element in $H - U$. Since $\langle h, v\rangle \trianglelefteq G$, we get

$$\Omega_1(\langle h, v\rangle) = \langle h, t\rangle \trianglelefteq G.$$

Thus we get $h^g = ht^i$ for some $i \not\equiv 0 \pmod p$ and so $G' \ge \langle t\rangle$. On the other hand,

$$\mathrm{Z}(G) = \mathrm{C}_K(g) = \langle g^p, U\rangle \text{ and so } |G : \mathrm{Z}(G)| = p^2.$$

By Lemma 1.1 in [1], we get

$$|G| = p|\mathrm{Z}(G)||G'| \text{ and so } |G'| = p \text{ and } G' = \langle t\rangle.$$

We have $\langle g, h\rangle \cong \mathrm{M}_{p^{s+1}}$ and if we set $\langle z\rangle = H \cap U$, then

$$G = \langle z\rangle \times \langle g, h\rangle \cong \mathrm{C}_p \times \mathrm{M}_{p^{s+1}}.$$

We have obtained the groups stated in part (e) of our theorem.

(i2b) Assume that $G/L$ is abelian of type $(p^s, p)$, $s \ge 1$, and $K$ is abelian. Let $v \in K - L$ be such that $\langle v\rangle$ covers $K/L \cong \mathrm{C}_{p^s}$, $s \ge 1$. Then $t = v^{p^s} \in U - H$ so that

$$K/H \cong \mathrm{C}_{p^{s+1}} \text{ and } K = H \times \langle v\rangle \cong \mathrm{E}_{p^2} \times \mathrm{C}_{p^{s+1}}.$$

Since $G/L$ is abelian of type $(p^s, p)$, there is an element $w \in G - K$ such that $w^p \in L$ and so $w^p \in U$. Let $h \in H - U$ and consider the abelian subgroup

$$\langle h, v\rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^{s+1}}, \; s \geq 1.$$

Since $\langle h, v\rangle \trianglelefteq G$, we get $\langle h, t\rangle \trianglelefteq G$ and so $h^w = ht$ (where we replace $h$ with a suitable power $h^j$, $j \not\equiv 0 \pmod p$, if necessary). In particular, we get $G' \geq \langle t\rangle$.

Suppose that $G/U$ is nonabelian so that $p = 2$ and $G/U$ is Hamiltonian. But $G/L$ is abelian and so

$$(G/U)' = \mho_1(G/U) = L/U.$$

Hence there is an element $m \in G$ such that $m^2 \in L - U$, a contradiction. We have proved that $G/U$ is abelian and so $\langle t\rangle \leq G' \leq U \leq \mathrm{Z}(G)$ and therefore $G$ is of class 2 with an elementary abelian commutator subgroup.

Note that

$$\mathrm{C}_p \times \mathrm{C}_{p^{s+1}} \cong \langle h, v\rangle \trianglelefteq G \text{ and so } [h, w] \in \langle h, v\rangle \cap U = \langle t\rangle,$$

which implies that $\langle v\rangle \trianglelefteq G$ and therefore $p-1$ other cyclic maximal subgroups of $\langle h, v\rangle$ are also normal in $G$.

In case $\langle v\rangle \not\leq \mathrm{Z}(G)$ we get $v^w = vt^j$ for some integer $j \not\equiv 0 \pmod p$. Solve the congruence $ij \equiv -1 \pmod p$, where $i \not\equiv 0 \pmod p$. Then we compute:

$$(v^i h)^w = (v^w)^i h^w = (vt^j)^i ht = v^i t^{-1} ht = v^i h,$$

where $\langle v^i h\rangle \cong \mathrm{C}_{p^{s+1}}$ is also a cyclic maximal subgroup in $\langle h, v\rangle$ and $\langle v^i h\rangle \leq \mathrm{Z}(G)$. Thus replacing $\langle v\rangle$ with $\langle v^i h\rangle$, we may assume from the start that $\langle v\rangle \leq \mathrm{Z}(G)$. We get

$$\mathrm{Z}(G) = \mathrm{C}_K(w) = \langle v\rangle U \text{ and so } |G : \mathrm{Z}(G)| = p^2.$$

By Lemma 1.1 in [1] we get

$$|G| = p|\mathrm{Z}(G)||G'| \text{ and so } |G'| = p \text{ and } G' = \langle t\rangle.$$

First suppose that $w^p \in U - \langle t\rangle$. Then $S = \langle h, w\rangle$ is the nonmetacyclic minimal nonabelian group of order $p^4$. If we set $Z = \langle v\rangle$, then we get

$$G = Z * S, \text{ where } Z \cong \mathrm{C}_{p^{s+1}} \text{ and } Z \cap S = S'.$$

Assume that $w^p \in \langle t\rangle$ and set $\langle z\rangle = U \cap H$. Then $S = \langle h, w\rangle$ is isomorphic to $\mathrm{D}_8$ in case $p = 2$ and to $\mathrm{S}(p^3)$ or $\mathrm{M}_{p^3}$ in case $p > 2$. Setting again $Z = \langle v\rangle \cong \mathrm{C}_{p^{s+1}}$ we have $Z \leq \mathrm{Z}(G)$ , $S \cap Z = S'$ and $G = \langle z\rangle \times (S * Z)$. However, in case $p > 2$ and $S \cong \mathrm{M}_{p^3}$, we have $S*Z = S_1*Z$, where $S_1 \cong \mathrm{S}(p^3)$ for a suitable subgroup $S_1$ in $S * Z$. We have obtained all groups stated in part (f) of our theorem.

(i2c) Assume that $G/L$ is abelian of type $(p^s, p)$, $s \geq 1$, and $K$ is nonabelian. We have $K/L \cong \mathrm{C}_{p^s}$, $s \geq 1$. Let $v \in K - L$ be such that $\langle v\rangle$ covers $K/L$. Then $1 \neq t = v^{p^s} \in U - H$ so that $K/H \cong \mathrm{C}_{p^{s+1}}$. Acting with $K$ on $L$, we see that $K$ stabilizes the chain $L > U > \{1\}$. Hence if $s > 1$, then there is an element $v_0$ of order $p^2$ in $K$ which centralizes $L$ and $v_0^p \in U - H$. For an element $h \in H - U$ we consider

$$\mathrm{C}_p \times \mathrm{C}_{p^2} \cong \langle h, v_0 \rangle \trianglelefteq G \text{ and so } \mathrm{E}_{p^2} \cong \langle h, v_0^p \rangle \trianglelefteq G.$$

If $\langle h, v_0^p \rangle \not\leq \mathrm{Z}(K)$, then there is an element $g \in G - K$ which centralizes $h$, a contradiction. Thus we must have $\langle h, v_0^p \rangle \leq \mathrm{Z}(K)$ and this implies that $K$ is abelian, a contradiction. We have proved that $s = 1$ and so $t = v^p$ and $|G| = p^5$. Since $\mathrm{C}_L(v) = U = \mathrm{Z}(K)$, Lemma 1.1 in [1] gives that $|K'| = p$. On the other hand, $K' \leq H$ and since $K' \leq \mathrm{Z}(G)$, we get $K' = H \cap U$. For any $h \in H - U$, we have $\langle [h, v] \rangle = K'$ and so $K$ is the nonmetacyclic minimal nonabelian group of order $p^4$ and $\Phi(K) = U$. Because $G/L \cong \mathrm{E}_{p^2}$, we have $\exp(G) = p^2$ and so for any $x \in G - L$, we have $x^p \in U$ and $\mho_1(G) \leq U$. For $p = 2$, $G/U$ is elementary abelian. For $p > 2$, the fact that $G/U$ is Dedekindian implies that $G/U$ is abelian and so again $G/U$ is elementary abelian. We have proved that $\Phi(G) = U$ and so $G' \leq U$ and $\mathrm{d}(G) = 3$. Since $\mathrm{Z}(G) \leq K$, we also get $\mathrm{Z}(G) = U$. If $G' = K'$, then $H \trianglelefteq G$, a contradiction. Thus, $G' = U$ and so $G$ is special.

By Lemma 146.7 in [4], $G$ has exactly one abelian maximal subgroup $A$ and for each subgroup $X_i$ of order $p$ in $G'$ $(i = 1, 2, \ldots, p+1)$ there are exactly $p$ pairwise distinct maximal subgroups $L_{ij}$ $(j = 1, 2, \ldots, p)$ of $G$ such that $L'_{ij} = X_i$.

Suppose that $G$ possesses a nonabelian subgroup $S$ of order $p^3$ so that $S$ is minimal nonabelian and $S \trianglelefteq G$. But then $\mathrm{E}_{p^2} \cong G' \leq S$ and since $G' = \mathrm{Z}(G)$, we get that $S$ is abelian, a contradiction. Hence $G$ is an $\mathrm{A}_2$-group since each subgroup of index $p^2$ in $G$ is abelian and $K$ is a minimal nonabelian maximal subgroup in $G$. If there is an element $g \in G - K$ of order $p$, then $\langle g, h \rangle$ (with $h \in H - U$) is minimal nonabelian of order $p^3$, a contradiction. We have proved that $\mathrm{E}_{p^3} \cong L = \Omega_1(G)$ and so a unique abelian maximal subgroup $A$ of $G$ is of type $(p^2, p^2)$. Indeed, $A$ contains $U = \Phi(G)$ and $|K \cap A| = p^3$. If $L \leq A$, then there is an element $g \in G - K$ which centralizes $L$, a contradiction. Hence we have $A \cap L = U = \Omega_1(A)$ which shows that $A \cong \mathrm{C}_{p^2} \times \mathrm{C}_{p^2}$.

By the results of §71 in [2], it follows that $G$ is one of $\mathrm{A}_2$-groups from Theorem 71.4(b2) in [2] with $\alpha = 1$. We have obtained the groups from part (g) of our theorem.

(ii) We assume that whenever $H$ is a non-normal abelian subgroup of type $(p, p)$ in $G$, then $H \cap \mathrm{Z}(G) = \{1\}$. Let $z$ be a central element of $G$ which is contained in $L - H$ so that we have $L = \Omega_1(K) = \langle z \rangle \times H \cong \mathrm{E}_{p^3}$ and $L \cap \mathrm{Z}(G) = \langle z \rangle$. For any $1 \neq h \in H$, we have $\langle h, z \rangle \trianglelefteq G$ and therefore $H \cap \langle h, z \rangle = \langle h \rangle \trianglelefteq K$. Thus, $H \leq \mathrm{Z}(K)$ and $\mathrm{C}_G(L) = K$. It follows that $G/K$ acts faithfully on $L$ and stabilizes the chain $L > \langle z \rangle > \{1\}$ and $[H, G] = \langle z \rangle$. Thus $\{1\} \neq G/K$ is elementary abelian of order $\leq p^2$. However, if $|G/K| = p$, then there is an element $g \in G - K$ centralizing an element $1 \neq h \in H$ and so $h \in Z(G)$, a contradiction. We have proved that we have $G/K \cong E_{p^2}$.

Let $X$ be any cyclic subgroup of composite order in $G$. Since $\Omega_1(X) \leq K$, we have $\Omega_1(X) \leq L = \Omega_1(K)$. Suppose that $\Omega_1(X) \neq \langle z \rangle$. In this case we have

$$X \times \langle z \rangle \trianglelefteq G \text{ and so } \Omega_1(X) \trianglelefteq G.$$

This is a contradiction since $L \cap Z(G) = \langle z \rangle$. We have proved that the socle of each cyclic subgroup of composite order in $G$ is equal $\langle z \rangle \leq G'$.

We have $Z(G) \leq K$ and so we have

$$Z(G) \cap L = Z(G) \cap \Omega_1(K) = \langle z \rangle.$$

This implies that $Z(G)$ is cyclic and we also have $|G : Z(G)| \geq p^4$.

(ii1) First assume that $K/H \cong Q_8$. In this case we have $|G| = 2^7$. Let $K_i$ be any of the three maximal subgroups of $K$ containing $H$ so that $K_i/H \cong C_4$ and therefore each $K_i$ is abelian. Hence $|K'| = 2$ and so $K' \trianglelefteq G$ and $K' \leq L$ implies that $K' = \langle z \rangle$. Let $v_1, v_2 \in K - L$ be such that $\langle v_1, v_2 \rangle$ covers $K/L$. Because $v_1^2 = v_2^2 = z$ and $[v_1, v_2] = z$, we get $Q = \langle v_1, v_2 \rangle \cong Q_8$ so that $K = H \times Q$ and $Q \trianglelefteq G$. For each $K_i$ $(i = 1, 2, 3)$ we have $K_i \trianglelefteq G$ and so $K_i \cap Q \trianglelefteq G$. Thus $G$ induces on $Q$ only inner automorphisms of $Q$ which gives $G = Q * M$ with $Q \cap M = \langle z \rangle = Q'$ and $M \cap K = L$, where $M = C_G(Q)$ covers $G/K$. We have $\mho_1(M) \leq \langle z \rangle$ and so $Q/\langle z \rangle$ is elementary abelian. We get $G' = \Phi(G) = Z(G) = \langle z \rangle$ and so $G$ is extraspecial of order $2^7$. Since $M' = \Phi(M) = Z(M) = \langle z \rangle$, it follows that $M$ is extraspecial of order $2^5$ containing an elementary abelian subgroup $L$ of order 8 and so $M \cong Q_8 \times Q_8$ and $G \cong Q_8 \times Q_8 \times Q_8$. We have obtained the group stated in part (h) of our theorem.

(ii2) Assume that $K/H$ is cyclic. Then $K = H \times \langle v \rangle$ is abelian, where $\langle v \rangle \cong C_{p^s}$, $s \geq 1$, and $\langle v \rangle \geq \langle z \rangle \leq G' \cap Z(G)$.

(ii2a) First suppose that $G' = \langle z \rangle$. Then each cyclic subgroup of composite order is normal in $G$. Let $x, y \in G$ so that we have $[x^p, y] = [x, y]^p = 1$ and therefore $\mho_1(G) \leq Z(G)$. Hence we have $\Phi(G) = G'\mho_1(G) \leq Z(G)$ and we know that $Z(G)$ is cyclic. Hence $\Phi(G)$ is also cyclic and $G' = \Omega_1(\Phi(G))$. Since $v^p \in Z(G)$, we have $|G : Z(G)| = p^4$ or $p^5$. If $M$ is any minimal nonabelian subgroup in $G$, then either $M \cong S(p^3)$ or $Z(M) = \Phi(M) = \mho_1(M)$ and so in this case $M$ has a cyclic subgroup of index $p$. This gives:

$$\text{If } p = 2, \text{ then } M \in \{D_8, Q_8, M_{2^n},\ n \geq 4\}.$$

$$\text{If } p > 2, \text{ then } M \in \{S(p^3), M_{p^n},\ n \geq 3\}.$$

Let $A_1$ be any minimal nonabelian subgroup in $G$. Then we have $G = A_1 * C$, where $C = C_G(A_1)$ with $A_1 \cap C = Z(A_1)$. If $C$ is abelian, then $C = Z(G)$ and $|G : Z(G)| = p^2$, a contradiction. Thus, $C$ is nonabelian and $Z(C) = Z(G)$, where $|C : Z(C)| = p^2$ or $p^3$. Let $A_2$ be a minimal nonabelian subgroup in $C$. Then we have $C = A_2 * C^*$, where $C^* = \mathrm{C}_C(A_2)$ and $A_2 \cap C^* = \mathrm{Z}(A_2)$. Note that $\mathrm{Z}(C^*) = \mathrm{Z}(C)$ and so if $C^*$ were nonabelian, then we get $|C^* : \mathrm{Z}(C^*)| \geq p^2$ and so $|C : \mathrm{Z}(C)| \geq p^4$, a contradiction. Hence $C^*$ is abelian and so $C^* = \mathrm{Z}(C) = \mathrm{Z}(G)$. We have proved that $G = A_1 * A_2\mathrm{Z}(G)$, where $\mathrm{Z}(G)$ is cyclic. Finally, if $p = 2$ and $A_1 \cong \mathrm{Q}_8$ and $A_2 \cong \mathrm{D}_8$, then we must have $|\mathrm{Z}(G)| > 2$. Indeed, if we have in this case $|\mathrm{Z}(G)| = 2$, then $G \cong \mathrm{Q}_8 * \mathrm{D}_8$ and this group does not possess an elementary abelian subgroup of order 8. We have obtained the groups in part (i) of our theorem.

(ii2b) Finally assume that $G' > \langle z \rangle$. Set $H = \langle h_1, h_2 \rangle$ and we know that $\langle h_1, z \rangle \trianglelefteq G$, $\langle h_2, z \rangle \trianglelefteq G$ and both $G/\langle h_1, z \rangle$ and $G/\langle h_2, z \rangle$ are Dedekindian. If both $G/\langle h_1, z \rangle$ and $G/\langle h_2, z \rangle$ were abelian, then we get $G' \leq \langle h_1, z \rangle \cap \langle h_2, z \rangle = \langle z \rangle$, contrary to our assumption. Hence we must have $p = 2$ and we may assume that $G/\langle h_1, z \rangle$ is Hamiltonian.

Let $Q/\langle h_1, z \rangle$ be an ordinary quaternion subgroup in $G/\langle h_1, z \rangle$ and set

$$C/\langle h_1, z \rangle = (Q/\langle h_1, z \rangle)'$$

so that $Q'$ covers $C/\langle h_1, z \rangle$. Since $G/K \cong \mathrm{E}_4$, we have $G' \leq K$ and we know that $K$ is abelian. It follows that $C = \langle h_1, z \rangle Q' \leq K$ and so $C$ is abelian of order 8. For each $x \in Q - C$ we have $x^2 \in C - \langle h_1, z \rangle$. On the other hand, the socle of each cyclic subgroup of composite order in $G$ is equal $\langle z \rangle$ and so $o(x^2) = 4$ and therefore $C$ is abelian of type $(4, 2)$. We get $\Omega_1(Q) = \langle h_1, z \rangle$, $\Omega_2(Q) = C$, and all elements in $Q - C$ are of order 8. Also we have $Q \cap L = \langle h_1, z \rangle$. If $Q' = C$, then $|Q : Q'| = 4$ and a well known result of O. Taussky would imply that $Q$ is of maximal class (and order $2^5$), contrary to the fact that $\Omega_1(Q) = \langle h_1, z \rangle \cong \mathrm{E}_4$. On the other hand, $Q'$ must cover $C/\langle h_1, z \rangle$ and so we have $Q' \cong \mathrm{C}_4$.

By Lemma 42.1 in [1], we have

$$Q = \langle a, b \mid a^8 = b^8 = 1,\ a^4 = b^4 = z,\ a^b = a^{-1} \rangle,$$

where $Q' = \langle a^2 \rangle$, $\mathrm{Z}(Q) = \langle b^2 \rangle$, $\Omega_2(Q) = \langle a^2, b^2 \rangle$, and $\Omega_1(Q) = \langle z, a^2 b^2 \rangle$. Since $\mathrm{Z}(Q) = \langle b^2 \rangle$, we have $\mathrm{C}_Q(b) = \langle b \rangle$ and so $\mathrm{C}_{\langle h_1, z \rangle}(b) = \langle z \rangle$. On the other hand, $b^2 \in K > L$ and therefore $b^2$ centralizes $L$ and so $b$ induces an involutory automorphism on $L \cong \mathrm{E}_8$. Hence $\mathrm{C}_L(b) \cong \mathrm{E}_4$ and so there exists an involution $e \in H - \langle h_1 \rangle$ such that $[e, b] = 1$.

We have

$$\mathrm{C}_2 \times \mathrm{C}_8 \cong \langle e, b \rangle \trianglelefteq G, \text{ where } \Omega_1(\langle e, b \rangle) = \langle e, z \rangle.$$

On the other hand,

$$b^a = a^{-1} b a = b(b^{-1} a^{-1} b) a = b a^2,$$

which shows that $a^2 \in \langle e, b \rangle$. But then $\langle e, b \rangle$ contains $\langle e, z, a^2 b^2 \rangle \cong \mathrm{E}_8$, contrary to

$$\Omega_1(\langle e, b \rangle) = \langle e, z \rangle \cong \mathrm{E}_4.$$

We have proved that the case $G' > \langle z \rangle$ cannot occur.

It remains to be proved the converse that all groups $G$ stated in our theorem satisfy the assumptions of that theorem. In fact, we have to prove that each noncyclic subgroup of order $\geq p^3$ is normal in $G$ and that $G$ has a non-normal abelian subgroup of type $(p, p)$.

If $G \cong \mathrm{D}_{16}$ or $G \cong \mathrm{SD}_{16}$, a four-subgroup in $G$ is not normal in $G$.

Let $G$ be a $p$-group in part (b) of our theorem. Then we have $L' < G' < L$, where $G' \cong \mathrm{E}_{p^2}$. For an element $l \in L - G'$, set $H = \langle L', l \rangle \cong \mathrm{E}_{p^2}$. If $H \trianglelefteq G$, then $|G/H| = p^2$ implies that $G' \leq H$, a contradiction. Hence $H$ is not normal in $G$.

Let $E$ be an elementary abelian maximal subgroup in a nonabelian $p$-group $G$ of order $p^4$ (from part (c) of our theorem). Then we have $1 \neq G' < E$. Let $\mathrm{E}_{p^2} \cong H$ be any subgroup of order $p^2$ in $E$ which does not contain $G'$. If $H \trianglelefteq G$, then $|G/H| = p^2$ implies that $G' \leq H$, a contradiction. Hence $H$ is not normal in $G$.

Let $G$ be a 2-group of order $2^6$ from part (d) of our theorem. Note that $\mathrm{Z}(G) \cong \mathrm{E}_4$ implies that $G$ has no abelian maximal subgroup. Indeed, if $G$ would have an abelian maximal subgroup, then we may use Lemma 1.1 in [1] and we get

$$|G| = 2^6 = 2|G'||\mathrm{Z}(G)| = 2^3|G'| \text{ and } |G'| = 2^3,$$

which contradicts the fact that $|G'| = 2$. Let $S$ be a noncyclic subgroup of order $\geq 2^3$ and assume that $S$ is not normal in $G$. Then $G' \not\leq S$ and so $S$ is noncyclic abelian. If $|S| = 2^4$, then $S \times G'$ would be an abelian maximal subgroup of $G$, a contradiction. Assume that $|S| = 2^3$. Since $G$ has no elementary abelian subgroups of order $2^4$, we get that $S$ is abelian of type $(4, 2)$. In case $G \cong (\mathrm{D}_8 * \mathrm{Q}_8) \times \mathrm{C}_2$, we have $\mho_1(G) = G'$ and so ( since $G' \not\leq S$ ) we must be in case

$$\mathrm{H}_{16} * \mathrm{Q}_8 \cong G = D * Q, \text{ where } D \cong \mathrm{H}_{16},\ Q \cong \mathrm{Q}_8 \text{ and } D \cap Q = D' = \langle z \rangle = Q',$$

and $z$ is not a square of any element in $D$. Since all elements in $G - D$ are of order 4, we have $\Omega_1(S) \leq D$ and so

$$\mathrm{E}_8 \cong \Omega_1(D) = \Omega_1(S) \times D' = \Omega_1(S) \times \langle z \rangle.$$

We have

$$\mathrm{C}_D(\Omega_1(S)) = \Omega_1(S) \times \langle z \rangle = \Omega_1(D) \text{ and } \mathrm{C}_G(\Omega_1(S)) = \Omega_1(D) * Q,$$
$$\text{where } \mho_1(\mathrm{C}_G(\Omega_1(S))) = \langle z \rangle.$$

But $S \leq \mathrm{C}_G(\Omega_1(S))$ and so $G' = \langle z \rangle \leq S$, a contradiction. It is easy to see that $G$ possesses a non-normal abelian subgroup $H \cong \mathrm{E}_4$. Set $H = \langle t, u \rangle$, where $t$ is a noncentral involution in $G$ and $u$ is a central involution in $G$ such that $\langle u \rangle \neq G'$. Then we have $G' \not\leq H$. If $H \trianglelefteq G$, then there is $g \in G$ such that $[g,t] \neq 1$ and so $G' = \langle [g,t] \rangle \leq H$, a contradiction. Hence $H = \langle t,u \rangle$ is not normal in $G$.

Let $G = M \times \langle t \rangle$, where $M \cong \mathrm{M}_{p^{s+1}}$, $s \geq 3$, and $\langle t \rangle \cong \mathrm{C}_p$ (which are groups of part (e) of our theorem). We have $\Omega_1(G) \cong \mathrm{E}_{p^3}$, $\Omega_2(G)$ is abelian of type $(p^2,p,p)$ with $\mho_1(\Omega_2(G)) = G' = \mathrm{C}_p$. Thus any subgroup of order $\geq p^3$ is normal in $G$. Let $H$ be a complement of $G'$ in $\Omega_1(G)$ so that $H \not\leq \mathrm{Z}(G)$ and so $H$ is not normal in $G$. Indeed, if in this case $H \trianglelefteq G$, then $[G,H] \neq \{1\}$ and $[G,H] \leq H$ and so $G' \leq H$, a contradiction.

Let $G$ be a group of part (f) of our theorem. Let $X$ be any subgroup of $G$ of order $\geq p^3$ which is not normal in $G$. Then we have $G' = S' \not\leq X$ and so $X$ is abelian of order $\geq p^3$ with $X \cap Z = \{1\}$. But $|G/Z| = p^3$ and so $|X| = p^3$ and $G = Z \times X$ is abelian, a contradiction. Let $H = \langle t,u \rangle \cong \mathrm{E}_{p^2}$, where $t$ is a noncentral element of order $p$ in $S$ and $u$ is a central element of order $p$ in $G$ with $\langle u \rangle \neq G'$. Then we have $G' \not\leq H$ and so $H$ is not normal in $G$.

Let $G$ be a group of order $p^5$ given in part (g) of our theorem. Then $G$ is special with $G' \cong \mathrm{E}_{p^2}$ and $G$ is an $\mathrm{A}_2$-group. Let $Y$ be any subgroup of $G$ of order $p^3$ which does not contain $G'$. Since $|G:Y| = p^2$ and $G$ is an $\mathrm{A}_2$-group, it follows that $Y$ is abelian of type $(p^2,p)$. Then $A = G'Y$ is a unique abelian maximal subgroup of $G$ and we know that $A \cong \mathrm{C}_{p^2} \times \mathrm{C}_{p^2}$. But then $\mathrm{E}_{p^2} \cong \Omega_1(A) = \Phi(A) = G'$, a contradiction. Let $H$ be an abelian subgroup of order $p^2$ contained in $\Omega_1(G) \cong \mathrm{E}_{p^3}$ distinct from $G'$. If $H \trianglelefteq G$, then $G = HA$ and $G/H$ is abelian so that $G' \leq H$, a contradiction. Hence $H$ is not normal in $G$.

Let $G \cong \mathrm{Q}_8 * \mathrm{Q}_8 * \mathrm{Q}_8$ be the extraspecial group of order $2^7$ given in part (h) of our theorem. Let $X$ be any subgroup of order $\geq 2^3$ and assume that $X$ is not normal in $G$. Then $X \cap G' = \{1\}$ and so $X$ is elementary abelian. But then $X \times G'$ is an elementary abelian subgroup of order $\geq 2^4$ in $G$. Since $G$ is extraspecial of order $2^7$ and type " $-$ ", there are no such elementary abelian subgroups in $G$. Hence $X \trianglelefteq G$. Let $H$ be a four-subgroup in $G$ with $H \cap G' = \{1\}$. If $H \trianglelefteq G$, then $H \cap \mathrm{Z}(G) \neq \{1\}$, a contradiction.

Finally, let $G$ be a group stated in part (i) of our theorem. Then we have

$$\Omega_1(\mathrm{Z}(G)) = G', \text{ where } \mathrm{Z}(G) \text{ is cyclic.}$$

Also note that $|G:\mathrm{Z}(G)| = p^4$ and so $G$ does not possess an abelian maximal subgroup. Indeed, if $G$ would have an abelian maximal subgroup, then Lemma 1.1 in [1] implies that

$$|G| = p|G'||\mathrm{Z}(G)|, \text{ where } |G'| = p,$$

a contradiction. Let $X$ be any subgroup of order $\geq p^3$ in $G$. Then we claim that $X \trianglelefteq G$. Indeed, assume that $X$ is not normal in $G$. Then we have $G' \not\leq X$ and so $X \cap \mathrm{Z}(G) = \{1\}$ and therefore $X$ is abelian of order $\geq p^3$. But then $\mathrm{Z}(G) \times X$ is an abelian subgroup of index $\leq p$ in $G$, a contradiction. It remains to be shown that $G = (A_1 * A_2)\mathrm{Z}(G)$ possesses an abelian subgroup of type

$(p, p)$ which is not normal in $G$. If $A_1$ and $A_2$ possess noncentral elements $a_1 \in A_1$ and $a_2 \in A_2$ of order $p$, then $H = \langle a_1, a_2 \rangle \cong \mathrm{E}_{p^2}$ and $H$ is not normal in $G$ since $H \cap \mathrm{Z}(G) = \{1\}$. If $p > 2$, then

$$A_1, A_2 \in \{\mathrm{S}(p^3),\ \mathrm{M}_{p^n},\ n \geq 3\}$$

and in this case there are such elements $a_1$ and $a_2$. If $p = 2$, then we have

$$A_1, A_2 \in \{\mathrm{D}_8,\ \mathrm{Q}_8,\ \mathrm{M}_{2^n},\ n \geq 4\}$$

and we may replace $A_1$ and $A_2$ with suitable other minimal nonabelian subgroups of $G$ so that again we find noncentral involutions $a_1 \in A_1$ and $a_2 \in A_2$. Indeed we have:

$$\mathrm{Q}_8 * \mathrm{Q}_8 = \mathrm{D}_8 * \mathrm{D}_8,$$
$$\mathrm{Q}_8 * \mathrm{M}_{2^n} = \mathrm{D}_8 * \mathrm{M}_{2^n},\ n \geq 4,$$

and

$$(\mathrm{D}_8 * \mathrm{Q}_8)\mathrm{Z}(G) = (\mathrm{D}_8 * \mathrm{D}_8)\mathrm{Z}(G),\ \text{ where } |\mathrm{Z}(G)| > 2.$$

Theorem A is completely proved.

## 3. Proof of Theorem B

First we shall prove a series of lemmas about 2-groups $G$ which satisfy the assumptions of Theorem B, where $H$ always denotes a non-normal subgroup in $G$ which is isomorphic to $\mathrm{Q}_8$. Set $K = \mathrm{N}_G(H)$ so that $H < K < G$ and $K \trianglelefteq G$. Let $L$ be a unique subgroup in $G$ which contains $H$ as a subgroup of index 2. We fix this notation in the sequel.

Lemma 3.1. *The factor-group $K/H \neq \{1\}$ is either cyclic or isomorphic to $\mathrm{Q}_8$ and $G/L \neq \{1\}$ is Dedekindian. We have $\Omega_1(K) \leq L$ and if $K$ does not possess a $G$-invariant four-subgroup, then $G \cong \mathrm{Q}_{2^5}$ (the case (a) of Theorem B). From now on we shall assume that $K$ possesses a $G$-invariant four-subgroup $U$. We have in that case $L = HU$ with $U_0 = H \cap U = \mathrm{Z}(H) \leq \mathrm{Z}(G)$ and $G/U$ is also Dedekindian.*

Proof. Since $K/H$ is Dedekindian and $L/H$ is a unique subgroup of order 2 in $K/H$, it follows that $K/H \neq \{1\}$ is either cyclic or isomorphic to $\mathrm{Q}_8$ which also implies that $\Omega_1(K) \leq L$.

Assume that $K$ has no $G$-invariant four-subgroup. By Lemma 1.4 in [1], $K$ is a 2-group of maximal class and then $K = L$ is of order $2^4$. We have $\mathrm{C}_G(H) = \mathrm{C}_K(H) < H$ and then Proposition 10.17 in [1] implies that $G$ is also of maximal class. Since $K \trianglelefteq G$, we must have $|G/K| = 2$ and so $|G| = 2^5$. The only possibility is $G \cong \mathrm{Q}_{2^5}$ and this group obviously satisfies the assumptions of Theorem B.

From now on we shall assume that $K$ has a $G$-invariant four-subgroup $U$. Since $\Omega_1(K) \leq L$, we have $U \leq L$ and so $L = HU$ with $U_0 = H \cap U = \mathrm{Z}(H)$. But $L' \leq H \cap U$ and so we have $L' = U_0 \leq \mathrm{Z}(G)$. Also, $G/U$ is Dedekindian. □

Lemma 3.2. *We have $U = Z(L) \leq G'$, $K = H * C_G(H)$ with $U \leq C_G(H)$ and $H \cap C_G(H) = U_0$. Also, $G/K$ is elementary abelian of order 2 or 4 and $\Omega_1(K) = U$.*

Proof. Since $L' = H' = U_0$, we get $L = H * Z$, where $Z \cong C_4$ or $E_4$ and $H \cap Z = U_0$. However, if $Z \cong C_4$, then $H$ would be a unique subgroup in $L$ which is isomorphic to $Q_8$ and this gives $H \trianglelefteq G$, a contradiction. Hence we have $Z \cong E_4$ and so

$$U = \Omega_1(L) = \Omega_1(K) = Z(L).$$

Let $H_1$ be any cyclic subgroup of order 4 in $H$. Then

$$H_1U \trianglelefteq G \text{ and so } H_1 = (H_1U) \cap H \trianglelefteq K.$$

Thus each element in $K$ induces on $H$ an inner automorphism of $H$ and so we get

$$K = H * C_G(H) \text{ with } U \leq C_G(H) \text{ and } H \cap C_G(H) = U_0.$$

For an element $x \in G-K$, there is an element $h \in H$ of order 4 such that $h^x \in L-H$. But $\langle h\rangle U \trianglelefteq G$ with $h^2 \in U_0$ and so $h^x = hu$ for some $u \in U-U_0$. Then we have $[h,x] = u$ and so we get $U \leq G'$.

There are exactly three maximal subgroups of $L$ which contain $U$ and they all are abelian of type $(4,2)$. The other four maximal subgroups of $L$ which do not contain $U$ are isomorphic to $Q_8$. This gives $1 \neq |G/K| \leq 4$.

For any element $y \in H - U_0$ and any $g \in G - K$, we have

$$y^2 \in U_0,\ U\langle y\rangle \trianglelefteq G \text{ and } y^g = yu, \text{ where } u \in U.$$

This gives

$$y^{g^2} = (yu)^g = (yu)u^g = (yu)uu_0 = yu_0 \text{ with some } u_0 \in U_0.$$

Hence $g^2 \in K$ and so $G/L$ is elementary abelian of order $\leq 4$. □

Lemma 3.3. *If $U \not\leq Z(G)$, then $G$ is the group of order $2^5$ and class 3 from part (b) of Theorem B and this group satisfies the assumptions of that theorem.*

Proof. Assume that $U \not\leq Z(G)$. Note that $K/H \cong C_G(H)/U_0$ is either cyclic or isomorphic to $Q_8$. Hence if $K > L$, then $C_G(H) = C_K(H) > U$ and so there is an element $k$ of order 4 in $C_K(H) - U$ such that $k^2 \in U - U_0$. In that case we have

$$U\langle k\rangle = U_0 \times \langle k\rangle \cong C_2 \times C_4 \trianglelefteq G.$$

But then we get $\langle k^2\rangle \trianglelefteq G$ and so $U \leq Z(G)$, a contradiction.

We have proved that $K = L$. Suppose that $G - K$ contains an element $y$ of order $\leq 4$ which does not centralize $U$. Since $y^2 \in U$, we get $D = U\langle y\rangle \cong$

$D_8 \trianglelefteq G$. Let $V$ be a four-subgroup in $D$ which is distinct from $U$. Because $U \trianglelefteq G$, we get also $V \trianglelefteq G$ and $V \cap K = U_0 = Z(D)$. But then we have

$$[H, V] \le K \cap V = U_0 < H$$

and so $V$ normalizes $H$, a contradiction. Hence each element in $G - K$ of order $\le 4$ centralizes $U$ and since $U \not\le Z(G)$, there is an element $x$ of order 8 in $G - K$ so that we have $x^2 \in L - U$ and $\langle x^4 \rangle = U_0$. Note that $\langle x \rangle U \trianglelefteq G$ and we have either $\langle x \rangle U \cong C_8 \times C_2$ or $\langle x \rangle U \cong M_{16}$. In any case $\langle x^2 \rangle$ is characteristic in $\langle x \rangle U$ and so $\langle x^2 \rangle \trianglelefteq G$. Then there are exactly three maximal subgroups of $K = L$ which contain $\langle x^2 \rangle$, where two of them are isomorphic to $Q_8$ and $\langle x^2 \rangle U \cong C_4 \times C_2$. Thus acting with $G/K$ on four maximal subgroups of $L$ which are isomorphic to $Q_8$, we get $|G : K| = 2$ and so $|G| = 2^5$. Since $U \le Z(K)$ (noting that $K = L$), each element in $G - K$ does not centralize $U$ and so (by the above argument) all elements in $G - K$ are of order 8.

We have proved that $\Omega_2(G) = K = L \cong C_2 \times Q_8$ and so by Theorem 52.1 in [2], $G$ is isomorphic to the group defined in part A2(a) of Theorem 49.1 in [2]. Since $\Omega_1(G) = G' = U$, this group obviously satisfies the assumptions of Theorem B and we are done. □

From now on we shall always suppose that $U \le Z(G)$.

LEMMA 3.4. *The factor-group $G/U$ is abelian and so we have $G' = U \le Z(G)$. Since for all $x, y \in G$ we get $[x^2, y] = [x, y]^2 = 1$, it follows that $\Phi(G) \le Z(G)$.*

PROOF. Assume that $G/U$ is nonabelian so that $G/U$ is Hamiltonian. Let $Q/U$ be an ordinary quaternion subgroup in $G/U$, where by our assumption we have $U \le Z(G)$ (see Lemma 3). Set

$$Q_0/U = (Q/U)' = Z(Q/U), \text{ where } |Q_0 : U| = 2.$$

Let $Q_1/U$ and $Q_2/U$ be two distinct cyclic subgroups of order 4 in $Q/U$ so that $Q_1$ and $Q_2$ are two distinct abelian maximal subgroups in $Q$. This implies that $|Q'| = 2$. On the other hand, $Q'$ covers $Q_0/U = (Q/U)'$ and so $Q_0 = U \times Q' \cong E_8$. For each $l \in Q - Q_0$, we have $l^2 \in Q_0 - U$ and $l^2 \in K$ (since $G/K$ is elementary abelian of order $\le 4$). But then $Q_0 \le K$ which contradicts Lemma 2 which states that $\Omega_1(K) = U$. □

LEMMA 3.5. *There are no involutions in $G - K$ and so we have $U = G' = \Omega_1(G) \le Z(G)$.*

PROOF. Set $Z(H) = H' = \langle z \rangle$ and suppose that there is an involution $i$ in $G - K$. Then $H \neq H^i$ and $i$ normalizes $H_0 = H \cap H^i \cong C_4$. It follows that $H_0\langle i \rangle \cong C_4 \times C_2$ or $D_8$ and $H_0\langle i \rangle \trianglelefteq G$. If $\langle z, i \rangle$ is not normal in $G$, then $H_0\langle i \rangle \cong D_8$ and there is $g \in G$ which induces on $H_0\langle i \rangle$ an outer automorphism (which permutes two four-subgroups in $H_0\langle i \rangle$). But in that case we have $[(H_0\langle i \rangle), \langle g \rangle] = H_0 \cong C_4$, contrary to the fact that $G' = U \cong E_4$. It follows that we have $E = \langle z, i\rangle \trianglelefteq G$. But then we have $[H, E] \le K \cap E = \langle z\rangle$ and so $i$ normalizes $H$, a contradiction. □

LEMMA 3.6. *The factor-group $K/H$ is cyclic.*

PROOF. Assume that $K/H$ is noncyclic so that setting $\mathrm{Z}(H) = H' = \langle z\rangle$ we get

$$\mathrm{Q}_8 \cong K/H \cong \mathrm{C}_G(H)/\langle z\rangle$$

and therefore

$$\mathrm{Z}(\mathrm{C}_G(H)) = U \text{ and } \mathrm{Z}(K) = U = \mathrm{Z}(G).$$

By Lemma 4, we have $\Phi(G) \le \mathrm{Z}(G)$ and so $\Phi(G) = U$. On the other hand, $|K| = 2^6$ and so $|G| \ge 2^7$ and $\mathrm{d}(G) \ge 5$. By Lemma 5, $G$ has no normal elementary abelian subgroup of order 8 and so by the four-generator theorem (see Theorem 50.3 in [2]), we must have $\mathrm{d}(G) \le 4$, a contradiction. □

PROOF OF THEOREM B. We continue with the situation which we have reached after Lemma 6. Hence we have

$$U = G' = \Omega_1(G) \le \mathrm{Z}(G),\ \Phi(G) \le \mathrm{Z}(G),$$

$$K = H \times \langle a\rangle \text{ with } \langle a\rangle \cong \mathrm{C}_{2^n},\ n \ge 1,\ L = H \times \Omega_1(\langle a\rangle),$$

and $G/K \ne \{1\}$ is elementary abelian of order $\le 4$.

(i) First assume $K = L$. In this case $G$ is a special group of order $2^5$ or $2^6$ with

$$\Omega_1(G) = \Phi(G) = \mathrm{Z}(G) = G' = U \cong \mathrm{E}_4 \text{ and we set } \mathrm{Z}(H) = \langle z\rangle.$$

Let $G_0/K$ be any fixed subgroup of order 2 in $G/K$ and let $x \in G_0 - K$. Then $x$ normalizes

$$H_0 = \langle h_0\rangle = H \cap H^x \cong \mathrm{C}_4.$$

If $x$ inverts $h_0$, then for an element $h \in H - H_0$, we have $hx \in G_0 - K$ and $hx$ centralizes $H_0$. Hence there is an element $v \in G_0 - K$ such that $v$ centralizes an element $h_0 \in H$ of order 4. If $v^2 = z$, then $h_0 v$ is an involution in $G - K$, a contradiction. Hence we have $v^2 = z' \in U - \langle z\rangle$. Since $H$ is not normal in in $G_0$, we have for any $h_1 \in H - \langle h_0\rangle$, $[h_1, v] \in \{z', zz'\}$. However, if $[h_1, v] = zz'$, then we get

$$(h_1 v)^2 = h_1^2 v^2 [h_1, v] = zz'(zz') = 1,$$

and so $h_1 v$ is an involution in $G - K$, a contradiction. Thus we get $[h_1, v] = z' = v^2$ and so $\langle v\rangle \trianglelefteq G_0$. It follows that $G_0$ is a splitting extension of the cyclic noncentral normal subgroup $\langle v\rangle$ of order 4 (with $v^2 = z'$) by $H \cong \mathrm{Q}_8$. We have obtained the group stated in part (c) of Theorem B. Note that $(h_0 v)^2 = zz'$, $\langle h_0 v\rangle$ centralizes $\langle h_0\rangle$ and $[h_1, h_0 v] = zz'$ and so $G_0$ is also a splitting extension of the cyclic noncentral normal subgroup $\langle h_0 v\rangle$ of order 4 (with $(h_0 v)^2 = zz'$) by $H \cong \mathrm{Q}_8$.

Suppose now in addition that we have $G/K \cong \mathrm{E}_4$. If a cyclic subgroup $\langle h\rangle$ of order 4 in $H$ is normal in $G$, then acting with $G/K$ on four quaternion subgroups in $K = L$, we see that $G$ interchanges two quaternion subgroups which contain $\langle h\rangle$ and so $G$ interchanges also the other two quaternion subgroups in $K$. But this implies that $|G/K| = 2$, a contradiction. Hence if $G_i/K$ are three subgroups of order 2 in $G/K$, $i = 1, 2, 3$, then each $G_i$ normalizes exactly one of the three cyclic subgroups of order 4 in $H$. This implies that that there is an element $w \in G - G_0$ such that $w$ centralizes $h_1$ (from the previous paragraph), $w^2 = z'$ and $[h_0, w] = z'$ so that $K\langle w\rangle$ is a splitting extension of the cyclic noncentral normal subgroup $\langle w\rangle$ of order 4 (with $w^2 = z'$) by $H \cong \mathrm{Q}_8$. We have

$$[h_0, vw] = z', [h_1, vw] = z', [h_0h_1, vw] = 1,$$

and so $H$ normalizes $\langle vw\rangle$ with $H \cap \langle vw\rangle = \{1\}$. By the above, we must have $(vw)^2 = z'$ and so we have

$$z' = (vw)^2 = v^2w^2[v, w] = z'z'[v, w] = [v, w],$$

which implies that $\langle v, w\rangle \cong \mathrm{Q}_8$ with $\mathrm{Z}(\langle v, w\rangle) = \langle z'\rangle$. But $H$ normalizes both $\langle v\rangle$ and $\langle w\rangle$ and so $H_1 = \langle v, w\rangle \trianglelefteq G$. The structure of $G$ is uniquely determined. We verify that we have also $H_2 = \langle h_1w, h_0v\rangle \cong \mathrm{Q}_8$ with $\mathrm{Z}(\langle h_1w, h_0v\rangle) = \langle zz'\rangle$ and $[H_1, H_2] = \{1\}$. Since $H_1 \cap H_2 = \{1\}$, we have obtained the group $G = H_1 \times H_2$ from part (d) of Theorem B.

Finally, in both cases of groups $G$ in parts (c) and (d) of Theorem B, we have $\Omega_1(G) = G' \cong \mathrm{E}_4$ and so if $X$ is any subgroup in $G$ of order $\geq 2^3$ and if $X$ contains only one involution, then $X \cong \mathrm{Q}_8$ and if $X$ contains more than one involution, then $X \geq G'$ and so $X \trianglelefteq G$. Thus in both cases the assumptions of Theorem B are satisfied.

(ii) Now assume that $K > L$ and so $|\mathrm{C}_G(H) : U| \geq 2$. Since $G/L$ is abelian, $G/K$ is elementary abelian of order 2 or 4, and $K/L$ is cyclic of order $\geq 2$, we have to consider two subcases.

(ii1) $G/K$ has a subgroup $G_0/K$ of order 2 such that $G_0/L$ is cyclic of order $\geq 4$ and either $G = G_0$ or $G = G_0G_1$ with $G_0 \cap G_1 = L$ and $|G_1 : L| = 2$. We set $\mathrm{Z}(H) = \langle z\rangle$. Let $g$ be an arbitrary element in $G_0 - K$ so that $\langle g\rangle$ covers $G_0/L$. Since $g^2 \in \mathrm{Z}(G)$, we have $g^2 \in \mathrm{C}_G(H)$. Because $K/H$ is cyclic but $U \leq \mathrm{C}_G(H)$ is noncyclic and $\mathrm{C}_G(H)/\langle z\rangle \cong$K/H, we get $\mathrm{C}_G(H) = \langle z\rangle \times \langle g^2\rangle$ with $o(g^2) \geq 4$ and so $o(g) \geq 8$. Let $\langle z'\rangle = \Omega_1(\langle g\rangle)$ be the socle of $\langle g\rangle$, where $U = \langle z, z'\rangle$. We have

$$H_0 = \langle h_0\rangle = H \cap H^g \cong \mathrm{C}_4$$

is $\langle g\rangle$-invariant and so $H_0 \trianglelefteq G_0$. But $h_1 \in H - H_0$ inverts $\langle h_0\rangle$ and so $\mathrm{C}_G(h_0)$ covers $G_0/K$. Therefore we may choose $g \in \mathrm{C}_G(h_0) - K$ so that we may assume $[g, h_0] = 1$. But $H$ is not normal in $G_0$ and so $[h_1, g] \in \{z', zz'\}$ and we may set $[h_1, g] = z^\epsilon z'$, where $\epsilon = 0, 1$. We have obtained the groups from part (e) of Theorem B which obviously satisfy the assumptions of that theorem.

Continuing with this case, we assume that $G = G_0G_1$ with $G_0 \cap G_1 = L = HU$ and $|G_1 : L| = 2$. The group $G_1$ is isomorphic to a group in part (c) of Theorem B and so there is an element $v \in G_1 - L$ of order 4 such that $v^2 = z'$ and $H$ normalizes but does not centralize $\langle v \rangle$ (see arguments in (i)). On the other hand, $g^2 \in \mathrm{Z}(G)$ and $o(g^2) \geq 4$ and so there is an element $w$ of order 4 in $\langle g^2 \rangle$. But then $vw$ is an involution in $G - K$, contrary to Lemma 5.

(ii2) $G = KG^*$, where $K \cap G^* = L$ and $G^*/L$ is elementary abelian of order 2 or 4. Also we have $K = H \times \langle a \rangle$, where $o(a) \geq 4$. Also we set $\mathrm{Z}(H) = \langle z \rangle$ and $\Omega_1(\langle a \rangle) = \langle z' \rangle$ so that $U = \langle z, z' \rangle$. In any case, we have in $G^* - L$ an element $v$ of order 4 such that $v^2 = z'$ and $H$ normalizes but does not centralize $\langle v \rangle$. We have $\mathrm{Z}(G) \leq \mathrm{C}_G(H) = U\langle a \rangle$. If $\mathrm{Z}(G) > U$, then there is an element $w$ of order 4 in $\langle a \rangle$ with $w^2 = z'$ and $[v, w] = 1$. But then $vw$ is an involution in $G - K$, contrary to Lemma 5.

We have proved that $\Omega_1(G) = \mathrm{Z}(G) = U$ and so, in particular, $o(a) = 4$ and $a \notin \mathrm{Z}(G)$. This also gives that $\exp(G) = 4$ (because $\mho_1(G) \leq \mathrm{Z}(G)$). Hence $G$ is a special group of order $2^6$ or $2^7$. But $G$ has no normal elementary abelian subgroup of order 8 and so by the four-generator theorem we must have $\mathrm{d}(G) \leq 4$. Since $\Phi(G) = U$, we must have $|G| = 2^6$ and $|G^* : L| = 2$. We may set $H = \langle h_0, h_1 \rangle$ so that $[h_0, v] = 1$ and $[h_1, v] = z'$. Set $[a, v] = u$, where $1 \neq u \in U$. We compute:

$$(va)^2 = v^2a^2u = z'z'u = u \neq 1,$$
$$(v(ah_0))^2 = z'(zz')u = uz \text{ and so } u \neq z,$$
$$(v(ah_1))^2 = z'(zz')uz' = u(zz') \text{ and so } u \neq zz'.$$

It follows that $u = z'$ and so $[a, v] = z'$ and $Q = \langle a, v \rangle \cong \mathrm{Q}_8$ which is normalized but not centralized by $H$ and $Q \cap H = \{1\}$. The structure of $G$ is uniquely determined.

Set $C = \langle h_0, h_1a \rangle$. Since $h_0^2 = z$, $(h_1a)^2 = zz'$ and $[h_0, h_1a] = z$, we have that $C \cong \mathcal{H}_2$ and $C \cap Q = \langle z' \rangle$, where $z'$ is not a square in $C$. Also we have $[C, Q] = \{1\}$ and therefore we have obtained the group in part (f) of Theorem B, which obviously satisfies the assumptions of that theorem, Our result is completely proved. ∎

## 4. Proof of Theorem C

This theorem will be proved with a series of Propositions 1 to 12.

PROPOSITION 4.1. *Let $G$ be a $p$-group with a cyclic intersection of any two distinct conjugate subgroups. Then each non-normal subgroup $X$ in $G$ possesses a cyclic subgroup of index $p$.*

Proof. Let $H$ be a maximal non-normal subgroup of $G$ containing $X$. Let $L > H$ be such that $|L : H| = p$ so that we have $L \trianglelefteq G$. Since $H$ is not normal in $G$, there is $g \in G - L$ such that $H^g \neq H$. Hence we have $L = HH^g$ and $|H : (H \cap H^g)| = p$. By our assumption, $H \cap H^g$ is cyclic and so $H$ has a cyclic subgroup of index $p$. Since $X \leq H$, it follows that $X$ also has a cyclic subgroup of index $p$. □

In the rest of the paper we assume:

($*$) $G$ is a $p$-group with cyclic intersection of any two distinct conjugate subgroups. Assume in addition that $G$ has a maximal non-normal subgroup $H$ which is neither cyclic nor abelian of type $(p,p)$ nor an ordinary quaternion group. We set $K = \mathrm{N}_G(H)$ so that $H < K < G$ and $K \trianglelefteq G$ and let $L/H$ be a unique subgroup of order $p$ in $K/H$, where $L \trianglelefteq G$. This notation will be fixed in the sequel.

Proposition 4.2. *We have that $K/H \neq \{1\}$ is either cyclic or $p = 2$ and $K/H \cong \mathrm{Q}_8$. Also we have $\Omega_1(K) \leq L$.*

*If $K$ does not possess a $G$-invariant subgroup isomorphic to $\mathrm{E}_{p^2}$, then $G$ is a 2-group of maximal class and order $\geq 2^5$ and if $|G| = 2^5$, then $G \cong \mathrm{D}_{32}$ or $\mathrm{SD}_{32}$ and all these groups satisfy our assumption ($*$).*

*From now on we always assume that $K$ has a $G$-invariant subgroup $U$ isomorphic to $\mathrm{E}_{p^2}$ and then we have $L = HU$ with $U_0 = H \cap U \cong \mathrm{C}_p$ and $G/U$ is Dedekindian.*

Proof. Suppose that $K/H$ has two distinct subgroups $K_1/H$ and $K_2/H$ of order $p$. Then $K_1 \trianglelefteq G$, $K_2 \trianglelefteq G$ and so $K_1 \cap K_2 = H \trianglelefteq G$, a contradiction. Hence $L/H$ is a unique subgroup of order $p$ in $K/H$ and so $K/H$ is either cyclic or generalized quaternion. On the other hand, $K/H$ is Dedekindian and so $K/H \neq \{1\}$ is either cyclic or $p = 2$ and $K/H \cong \mathrm{Q}_8$. In any case, we have $\Omega_1(K) \leq L$.

Assume that $K$ does not have a $G$-invariant abelian subgroup of type $(p,p)$. By Lemma 1.1 in [1], we have $p = 2$ and $K$ is a 2-group of maximal class and order $\geq 2^4$. In that case $K/H \cong \mathrm{Q}_8$ cannot happen and so $K/H$ is cyclic. It follows that $K' \leq H$ and $K/K' \cong \mathrm{E}_4$ and so $K = L$ and $K'$ is a cyclic subgroup of index 2 in $H$ and $K' \trianglelefteq G$. Since $H$ has only two conjugates in $G$, we have $|G : K| = 2$ and so $|G| \geq 2^5$. Since $H$ is not normal in $G$, we have $G' > K'$ and so $|G : G'| = 4$. By a well known result of O. Taussky, $G$ is a 2-group of maximal class and order $\geq 2^5$. However, $\mathrm{Q}_{32}$ does not satisfy ($*$) and so if $|G| = 2^5$, then $G \cong \mathrm{D}_{32}$ or $\mathrm{SD}_{32}$ .

Conversely, let $G$ be a 2-group of maximal class and order $\geq 2^5$. Let $Z$ be a unique cyclic subgroup of index 2 in $G$. Let $H$ be any non-normal subgroup in $G$ so that we have $H \not\leq Z$ and set $H_0 = H \cap Z \trianglelefteq G$ with $|H : H_0| = 2$. Hence if $g \in G$ is such that $H^g \neq H$, then we have $H \cap H^g = H_0$ is cyclic.

In the sequel we shall always assume that $K$ possesses a $G$-invariant abelian subgroup $U$ of type $(p,p)$. Since $\Omega_1(K) \leq L$, we have $U \leq L$. On the other hand, $G/U$ is Dedekindian and so $U \nleq H$. We get $L = HU$ with $U_0 = H \cap U \cong C_p$. □

PROPOSITION 4.3. *Assuming that $G$ is not a 2-group of maximal class, then it follows that $|G : K| = p$ and we may choose a $G$-invariant abelian subgroup $U$ of type $(p,p)$ in $L$ so that $C_p \cong U_0 = H \cap U \leq Z(G)$. Also, $G'$ covers $U/U_0$ and we have one of the following possibilities.*

(a) *We have*

$$p = 2,\ H \cong D_8,\ Z(L) = U \leq G' \text{ and } K = H * C_G(H) \text{ with}$$
$$U \leq C_G(H) \text{ and } H \cap C_G(H) = U_0.$$

*Also, the unique cyclic subgroup of order 4 in $H$ is normal in $G$.*

(b) *We have $H \cong M_{p^n}$, $n \geq 3$, ( if $p = 2$, then $n \geq 4$ ) or $H$ is abelian of type $(p^s, p)$, $s \geq 2$. Set $H_0 = \Omega_1(H)$ and then $H_0 \cong E_{p^2}$, $N_G(H_0) = K$ and $K/H_0$ is Dedekindian. There are two subcases:*

(b1) *If $S = H_0U$ is abelian, then $S \trianglelefteq G$ is elementary abelian of order $p^3$ and either $H \cong M_{p^n}$, $n \geq 3$, ( if $p = 2$. then $n \geq 4$ ) and in this case we have $U = \Omega_1(Z(L))$ , $L' = U_0$, and $U \leq G'$, or $H$ is abelian of type $(p^s, p)$, $s \geq 2$, and in this case $L$ is abelian of type $(p^s, p, p)$ with $\mho_1(L) = \mho_1(H) \geq U_0$.*

(b2) *If $S = H_0U$ is nonabelian, then $p > 2$, $S \cong S(p^3) \trianglelefteq G$ (the nonabelian group of order $p^3$ and exponent $p$) with $Z(S) = U_0$. We have*

$$G = (Z * S)\langle e\rangle,\ \text{where } C_{p^m} \cong Z = C_G(S) \trianglelefteq G,\ m \geq 2,\ S \cong S(p^3) \trianglelefteq G,$$
$$Z \cap S = Z(S) = U_0,\ Z\langle e\rangle = \langle e\rangle \cong C_{p^{m+1}} \text{ or } o(e) = p \text{ and } Z\langle e\rangle$$

*is either abelian of type $(p^m, p)$ or $Z\langle e\rangle \cong M_{p^{m+1}}$, where in any case $e$ induces on $S$ an outer automorphism of order $p$ (normalizing $U$ and fusing the other $p$ maximal subgroups of $S$). We have $E_{p^2} \cong G' = U < S$ and $G$ is a group of class 3. We have $\Omega_1(Z * S) = S$ and if $Z\langle e\rangle = \langle e\rangle \cong C_{p^{m+1}}$, then $\Omega_1(G) = S$. Conversely, groups $G$ defined in (b2) satisfy our assumption $(*)$.*

PROOF. By Proposition 1, $H$ possesses a cyclic subgroup of index $p$.

(i) First assume that $H$ is a 2-group of maximal class. In that case $U_0 = U \cap H = Z(H)$. If $|H| > 2^3$, then we have $H/U_0 \cong L/U \cong D_{2^n}$, $n \geq 3$, contrary to the fact that $G/U$ is Dedekindian. It follows that $H \cong D_8$ and because $|L/U| = 4$, we get $L' \leq H \cap U = U_0$ and so $L' = U_0 \leq Z(G)$. Then we have $L = H * Z$, where $Z = C_L(H)$, $Z \cap H = U_0$ and $Z \cong C_4$ or $E_4$.

Let $\langle h\rangle$ be a unique cyclic subgroup of order 4 in $H$ and let $x \in G - K$ so that $H^x \neq H$. Since $H \cap H^x$ is cyclic, we get $H \cap H^x = \langle h\rangle$ for all $x \in G - K$. This gives $\langle h\rangle \trianglelefteq G$. But $L/\langle h\rangle \cong E_4$ and so $L$ contains exactly two distinct conjugates of $H$ in $G$ and this implies $|G : K| = 2$. Let $t$ be an involution in $H - \langle h\rangle$. Because $U\langle t\rangle \trianglelefteq G$ and $H$ is not normal in $G$, we get for an

$x \in G - K$, $t^x \notin H$ and therefore we have $t^x = tu$ with some $u \in U - U_0$. Hence $[t, x] = u \in G'$, which implies that $G'$ covers $U/U_0$ and so in this case $U \leq G'$.

Assume for a moment that $Z \cong \mathrm{C}_4$. In this case it is well known that $L \cong \mathrm{D}_8 * \mathrm{C}_4$ contains a unique subgroup $Q$ isomorphic to $\mathrm{Q}_8$ and so $Q \trianglelefteq G$. For any cyclic subgroup $\langle v \rangle$ of order 4 in $Q$ we have $U_0 < \langle v \rangle$ and $U\langle v \rangle \trianglelefteq G$. But then

$$\langle v \rangle = (U\langle v \rangle) \cap Q \trianglelefteq G,$$

and so $G$ induces on $Q$ only inner automorphisms of $Q$. We get $G = Q * C$, where $C = \mathrm{C}_G(Q)$ and $Q \cap C = U_0$. Since $Q$ does not centralize $U$, we have $U \not\leq C$ and so $U \cap C = U_0 = Q'$. On the other hand, we get

$$G' = Q'C' = U_0 C' \leq C,$$

contrary to $U \leq G'$. We have proved that $Z \cong \mathrm{E}_4$ and $Z = \mathrm{Z}(L) \trianglelefteq G$.

Suppose that $U \neq Z$ so that $U \cap Z = U_0$, $S = UZ \cong \mathrm{E}_8$ and $S \trianglelefteq G$. Acting with an element $x \in G - K$ on three subgroups of order 4 in $S$ which contain $U_0 \leq \mathrm{Z}(G)$, we see that $Z \trianglelefteq G$, $U \trianglelefteq G$ and so also we have $\mathrm{E}_4 \cong S \cap H \trianglelefteq G$. But we know that a cyclic subgroup of order 4 in $H$ is normal in $G$ and so we get $H \trianglelefteq G$, a contradiction. We have proved that $U = Z = \mathrm{Z}(L)$.

Let $t$ be any involution in $H$. Since $U\langle t \rangle \trianglelefteq G$ and $H \trianglelefteq K$, it follows that

$$(U\langle t \rangle) \cap H = \langle t, U_0 \rangle \trianglelefteq K.$$

Thus, each element in $K$ induces on $H$ only inner automorphisms of $H$. It follows

$$K = H * \mathrm{C}_G(H) \text{ with } U \leq \mathrm{C}_G(H) = \mathrm{C}_K(H) \text{ and } H \cap \mathrm{C}_G(H) = U_0.$$

(ii) Now suppose that $H \cong \mathrm{M}_{p^n}$, $n \geq 3$, (where in case $p = 2$ we have $n \geq 4$) or $H$ is abelian of type $(p^s, p)$, $s \geq 2$. Set $H_0 = \Omega_1(H) \cong \mathrm{E}_{p^2}$ so that $H_0 \trianglelefteq K$. It follows that $\mathrm{N}_G(H_0) = K$ and $K/H_0$ is Dedekindian. Set $S = H_0 U \trianglelefteq G$. We have

$$L/U \cong H/U_0, \text{ where } H' \leq U_0 \leq \mathrm{Z}(H), \text{ and so } L' \leq H \cap U = U_0.$$

If $L$ is nonabelian, then $L' = U_0 \leq \mathrm{Z}(G)$. In that case we act with $G/K$ on $p+1$ subgroups of order $p^2$ in $S$ which contain $U_0 \leq \mathrm{Z}(G)$, where $U$ is the only one of them which is normal in $G$ and all $p$ other ones are fused with $G/K$ and so we get $|G : K| = p$. Also, if $h_0 \in H_0 - U_0$ and $x \in G - K$, then $h_0^x = h_0 u$ with $u \in U - U_0$. Hence $G'$ covers $U/U_0$ and so we have in this case $U \leq G'$.

Now assume that $L$ is abelian so that $L$ is of type $(p^s, p, p)$. If $U_0 \leq \mathrm{Z}(G)$, then with the same arguments as above, we get $|G : K| = p$ and $G'$ covers $U/U_0$. Now suppose that $U_0 \not\leq \mathrm{Z}(G)$. Then there is a subgroup $U_1$ of order $p$ in $U$ such that $U = U_0 \times U_1$ and $U_1 \leq \mathrm{Z}(G)$. We have

$$\mho_1(L) = \mho_1(H) \trianglelefteq G \text{ and } \mho_1(H) \neq \{1\} \text{ is cyclic .}$$

Let $H_1$ be the subgroup of order $p$ in $\mho_1(H)$ so that we get $H_1 \le \mathrm{Z}(G)$. Then we replace $U$ with

$$\mathrm{E}_{p^2} \cong U^* = U_1 \times H_1 \le \mathrm{Z}(G),$$

where

$$U_0^* = U^* \cap H = H_1 \le \mathrm{Z}(G)$$

and set $S^* = H_0U^*$. Now, working with $U^*$, $U_0^* \le \mathrm{Z}(G)$ and $S^* = H_0U^*$ (instead of $U$, $U_0$ and $S$), we get with the same arguments as above that $|G : K| = p$ and that $G'$ covers $U^*/U_0^*$. We write again $U$ and $U_0$ instead of $U^*$ and $U_0^*$, respectively, so that we may always assume that $U_0 = U \cap H \le \mathrm{Z}(G)$.

(ii1) Assume that $S = H_0U$ is abelian so that $S \cong \mathrm{E}_{p^3}$ and $S \trianglelefteq G$. Suppose in addition that $H \cong \mathrm{M}_{p^n}$, $n \ge 3$, (where in case $p = 2$ we have $n \ge 4$). Then we have $L' = H' = U_0 \le \mathrm{Z}(G)$ and $U \le G'$. Let $\langle a\rangle$ be a cyclic subgroup of index $p$ in $H$ so that $\langle a\rangle$ covers $H/H_0$ (and $L/S$) and $\langle a\rangle \cap H_0 = U_0 = \langle z\rangle$. Let $t \in H_0 - U_0$ so that we may set $[a, t] = z$. Suppose, by way of contradiction, that $U \not\le \mathrm{Z}(L)$. In that case, $|L : \mathrm{C}_L(U)| = p$ and so $\mathrm{C}_L(U) = \langle a^p\rangle S$. We may choose an element $u \in U - U_0$ so that $[a, u] = z^{-1}$. Then we get $[a, ut] = z^{-1}z = 1$ so that we have

$$\mathrm{Z}(L) = \langle a^p\rangle \times \langle ut\rangle \text{ and } \mathrm{E}_{p^2} \cong \Omega_1(\mathrm{Z}(L)) = \langle ut, z\rangle \trianglelefteq G.$$

But we know that $\mathrm{C}_p \cong G/K$ acts transitively on $p$ maximal subgroups of $S$ which contain $U_0 \le \mathrm{Z}(G)$ and which are distinct from $U$. Since $\langle ut, z\rangle \ne U$, we have a contradiction. Thus we have proved that $U \le \mathrm{Z}(L)$ and so $U = \Omega_1(\mathrm{Z}(L))$.

Now assume that $H$ is abelian of type $(p^s, p)$, $s \ge 2$. Suppose, by way of contradiction, that $L$ is nonabelian. In that case we have $L' = U_0 \le \mathrm{Z}(G)$ and $\mathrm{C}_L(H) = H$. By Lemma 1.1 in [1], we get

$$|L| = p|\mathrm{Z}(L)||L'| \text{ and so } |L : \mathrm{Z}(L)| = p^2.$$

Since $\mathrm{Z}(L) < H$, it follows that $\mathrm{Z}(L)$ is a maximal subgroup of $H$. If $\mathrm{Z}(L) \ge H_0$, then $H_0 = \Omega_1(\mathrm{Z}(L))$, which implies that $H_0 \trianglelefteq G$, a contradiction. It follows that $\mathrm{Z}(L)$ is a cyclic subgroup of index $p$ in $H$ and so $\mathrm{Z}(L)$ covers $H/H_0$ and $L/S$. Hence we get that $L = \mathrm{Z}(L)S$ is abelian, a contradiction. We have proved that $L$ is abelian of type $(p^s, p, p)$. Then we get $\mho_1(L) = \mho_1(H)$ and $\mho_1(H)$ is cyclic of order $\ge p$. Let $H_1$ be the subgroup of order $p$ in $\mho_1(H)$ so that $H_1 \le \mathrm{Z}(G)$ and $H_1 \le H_0$. If $H_1 \ne U_0$, then $H_0 = H_1 \times U_0 \le \mathrm{Z}(G)$, contrary to $\mathrm{N}_G(H_0) = K$. Hence we have $H_1 = U_0$ and so $\mho_1(L) = \mho_1(H) \ge U_0$.

(ii2) Assume that $S = H_0U$ is nonabelian. If $p = 2$, then $S \cong \mathrm{D}_8$. But $U$ and $H_0$ are the only two four-subgroups in $S$ and since $U \trianglelefteq G$, it follows that $H_0 \trianglelefteq G$, a contradiction. Hence we have $p > 2$ and $S \cong \mathrm{S}(p^3)$ (the nonabelian group of order $p^3$ and exponent $p$) with $S' = \mathrm{Z}(S) = U_0$. We know that $U \le G'$. On the other hand, $G/U$ is Dedekindian and so abelian which implies that $G' \le U$ and therefore we have $G' = U < S \trianglelefteq G$. Since $U = G' \not\le \mathrm{Z}(S)$, it follows that $G$ is of class 3. Also, $U$ is a unique normal abelian subgroup of type $(p,p)$ in $G$. Indeed, if $V \cong \mathrm{E}_{p^2}$, $V \trianglelefteq G$ and $V \ne U$, then the fact that $G/V$ is abelian Dedekindian implies that $G' \le V \cap U < U$, a contradiction. Set $Z = \mathrm{C}_G(S)$ so that $Z \trianglelefteq G$ and $Z \cap S = U_0$. We know that $Z$ does not have a $G$-invariant abelian subgroup of type $(p,p)$ and so Lemma 1.4 in [1] implies that $Z \cong \mathrm{C}_{p^m}$, $m \ge 1$, is cyclic and so $\Omega_1(Z * S) = S$. If $Z * S = G$, then $G' = U_0 \cong \mathrm{C}_p$, a contradiction. Hence we have $Z * S < G$. On the other hand, a Sylow $p$-subgroup of $\mathrm{Aut}(S)$ is isomorphic to $\mathrm{S}(p^3)$ and so $G/Z \cong \mathrm{S}(p^3)$ and $|G : (Z * S)| = p$. We know that $|G| \ge p^5$ because $|H| \ge p^3$ and so $L = HU (< G)$ is of order $\ge p^4$. This implies that we have $m \ge 2$. Let $e$ be an element in $G - (Z * S)$ so that $e$ fixes $U$ and fuses the other $p$ maximal subgroups of $S$. Since $G/Z \cong \mathrm{S}(p^3)$ is of exponent $p$, we have $e^p \in Z$. If $Z\langle e\rangle$ is cyclic, then we have

$$Z\langle e\rangle = \langle e\rangle \cong \mathrm{C}_{p^{m+1}}.$$

In this case, $G/S$ is cyclic of order $\ge p^2$ and $\Omega_1(Z * S) = S$ together with $|Z| \ge p^2$ implies $\Omega_1(G) = S$. If $Z\langle e\rangle$ is noncyclic, then $Z\langle e\rangle$ splits over $Z$ and we may assume that $o(e) = p$. In this case $Z\langle e\rangle$ is either abelian of type $(p^m, p)$ or $Z\langle e\rangle \cong \mathrm{M}_{p^{m+1}}$. We have obtained the groups stated in part (b2) of our proposition.

It remains to be proved that these groups $G$ satisfy our condition $(*)$. Let $X$ be any noncyclic and non-normal subgroup of order $\ge p^3$ in $G$. First assume that $|X \cap S| = p^2$ so that we have $X \cap S = S_i$ for some $i \in \{1, 2, \ldots, p\}$, where $\{S_1, S_2, \ldots, S_p\}$ is the set of maximal subgroups of $S$ distinct from $U$ which are acted upon transitively by $G/(Z * S)$. Since $\Omega_1(Z * S) = S$, we have $\Omega_1(X \cap Z * S) = S_i$ and this implies that $X \le Z * S$. Since $X \ge S_i > U_0 = (Z * S)'$, it follows that $\mathrm{N}_G(X) = \mathrm{N}_G(S_i) = Z * S$ and then for each $g \in G - (Z * S)$, the intersection $X \cap X^g$ is cyclic.

Now assume that $|X \cap S| = p$. (If $|X \cap S| = 1$, then $X \cap (Z * S) = \{1\}$ and then $|X| \le p$, a contradiction.) In this case, $X_0 = X \cap (Z * S)$ is cyclic of order $\ge p^2$, $X \not\le Z * S$ and so $|X : X_0| = p$. On the other hand, $\mho_1(Z * S) = \mho_1(Z) \ge U_0$ and so $X_0 \ge U_0$. We get $\mathrm{N}_G(X_0) \ge \langle Z * S, X\rangle = G$. Hence for each $g \in G$ with $X^g \ne X$, we see that $X \cap X^g = X_0$ is cyclic.

Finally, $ZS_i \cong \mathrm{C}_{p^m} \times \mathrm{C}_p$, $m \ge 2$, is not normal in $G$ but $Z \trianglelefteq G$ and so our condition $(*)$ is satisfied. Proposition 3 is completely proved. □

Proposition 4.4. *If $U \cong \mathrm{E}_{p^2}$ is a $G$-invariant subgroup contained in $K = \mathrm{N}_G(H)$ such that $U_0 = H \cap U \le \mathrm{Z}(G)$, then we have $G' \le U$. Hence $G'$ is elementary abelian of order $\le p^2$ and so $G$ is of class at most* 3.

Proof. Assume that $G/U$ is nonabelian so that we have $p = 2$ and $G/U$ is Hamiltonian. Let $Q/U$ be any ordinary quaternion subgroup in $G/U$ and we set

$$Q_0/U = (Q/U)' = \mathrm{Z}(Q/U) = (G/U)'.$$

We have $|Q : \mathrm{C}_Q(U)| \leq 2$ and so $Q_0 < \mathrm{C}_Q(U)$ and let $y \in \mathrm{C}_Q(U) - Q_0$ so that $y^2 \in Q_0 - U$. Hence $U\langle y\rangle$ is an abelian maximal subgroup in $Q$. By lemma 1.1 in [1], we have

$$2^5 = |Q| = 2|Q'||\mathrm{Z}(Q)|, \text{ where } \mathrm{Z}(Q) \leq Q_0 \text{ and } Q_0 \cong \mathrm{E}_8 \text{ or } Q_0 \cong \mathrm{C}_4 \times \mathrm{C}_2.$$

If $Q' = Q_0$, then $|Q : Q'| = 4$ and so by a result of O. Taussky, $Q$ is of maximal class and order $2^5$, contrary to $U \trianglelefteq Q$. Thus, we have $Q' < Q_0$ and $Q'$ covers $Q_0/Q$.

(i) First suppose that $Q_0 \cong \mathrm{E}_8$. We know that $G/Q_0$ is elementary abelian and so in this case $\exp(G) = 4$. In particular, we must have (according to Proposition 3) $H \cong \mathrm{D}_8$ or $\mathrm{C}_4 \times \mathrm{C}_2$. Consider again an abelian maximal subgroup $U \times \langle y\rangle$ of $Q$, where $\langle y\rangle \cong \mathrm{C}_4$ and $y^2 \in Q_0 - U$. Since $U \times \langle y\rangle \trianglelefteq G$, we get $y^2 \in \mathrm{Z}(G)$. Hence $y^2$ is an involution in $K$ and since $\Omega_1(K) \leq L$ (see Propositions 2 and 3), we get $Q_0 = \langle y^2\rangle \times U \leq L$. Set $H_0 = Q_0 \cap H \cong \mathrm{E}_4$, where $H_0 > U_0$ and $\mathrm{N}_G(H_0) = K$. Now act with $G/K$ on three subgroups of order 4 in $Q_0$ which contain $U_0 \leq \mathrm{Z}(G)$. We see that only $U$ is normal in $G$ and $H_0 \neq H_0^g$ with some $g \in G - K$. But $y^2 \in Q_0 - U$ and $y^2 \in \mathrm{Z}(G)$ and so $\langle y^2, U_0\rangle \trianglelefteq G$, a contradiction.

(ii) We have proved that $Q_0 \cong \mathrm{C}_4 \times \mathrm{C}_2$ so that all elements in $Q_0 - U$ are of order 4 and all elements in $Q - Q_0$ are of order 8. Since $Q'$ covers $Q_0/U$ and $Q' < Q_0$, we get $Q' \cong \mathrm{C}_4$. On the other hand, $\Omega_2(Q) = Q_0 \cong \mathrm{C}_4 \times \mathrm{C}_2$ and so Lemma 42.1 in [1] implies that $Q$ can be defined with:

$$Q = \langle a, b \mid a^8 = b^8 = 1,\ a^4 = b^4 = z,\ a^b = a^{-1}\rangle,$$

where

$$Q' = \langle a^2\rangle \cong \mathrm{C}_4,\ \mathrm{Z}(Q) = \langle b^2\rangle \cong \mathrm{C}_4,\ \Omega_2(Q) = \langle a^2, b^2\rangle = Q_0 \cong \mathrm{C}_4 \times \mathrm{C}_2,$$

$$\Omega_1(Q) = U = \langle z, a^2b^2\rangle \cong \mathrm{E}_4,\ U_0 = \langle z\rangle,$$

and $A = \langle a, b^2\rangle \cong \mathrm{C}_8 \times \mathrm{C}_2$ is a unique abelian maximal subgroup of $Q$. Also, it is easy to see that $\langle a\rangle$ is a characteristic subgroup in $Q$. Indeed, if $\theta \in \mathrm{Aut}(Q)$, then $A^\theta = A$ and so $b^\theta \in Q - A$. Suppose that $\langle a\rangle^\theta \neq \langle a\rangle$. Then we have $\langle a\rangle^\theta = \langle ab^2\rangle$ and we get

$$(ab^2)^{b^\theta} = a^{-1}b^{-2} = a^{b^\theta}(b^2)^{b^\theta} = a^{-1}b^2$$

and so we get $b^4 = 1$, a contradiction.

(iii) We know from Proposition 3 that $G'$ covers $U/U_0$ and since $G/Q_0$ is elementary abelian (and so $\exp(G) = 8$), we have $G' \leq Q_0$. But $Q' = \langle a^2\rangle$ with $\langle a^4\rangle = \langle z\rangle = U_0$ and so we get $G' = Q_0$. In particular, we have $G > Q$ and $|G| \geq 2^6$.

Since $C_Q(U) = A = \langle a, b^2 \rangle$ and $|Q : A| = 2$, we see that $C = C_G(U)$ covers $G/Q$, where $C \cap Q = A$ and $C > A$. On the other hand, $C/U$ does not possess an ordinary quaternion subgroup and so $C/U$ is abelian and therefore $C$ is of class $\leq 2$ with $C' \leq U \leq Z(C)$. Indeed, if $Q_1/U \cong Q_8$ and $Q_1 \leq C$, then by (ii) (since $Q/U$ was an arbitrary ordinary quaternion subgroup in $G/U$), we have $U \not\leq Z(Q_1)$ which is not the case. For any $x, y \in C$, we have $[x^2, y] = [x, y]^2 = 1$ and so we have $\mho_1(C) \leq Z(C)$. Since $a \in C$ and $a^2 \in Q_0 - U$, it follows that $Q_0 \leq Z(C)$ and so $C = C_G(U) = C_G(Q_0)$. In particular, we get $C_G(b^2) \geq \langle Q, C \rangle = G$ which shows that $b^2 \in Z(G)$.

(iv) Now we show that $C_G(Q) = Z(Q) = \langle b^2 \rangle = Z(G)$. Indeed, set $R = C_G(Q)$, where $R \cap Q = Z(Q) = \langle b^2 \rangle \leq Z(G)$ and $b^4 = z$ with $\langle z \rangle = U_0$. First suppose that $R$ has a $G$-invariant four-subgroup $U_1$. If $U_1 > \langle z \rangle$, then set $U_1 = U^*$ and if $U_1 \not\geq \langle z \rangle$, then considering $E_8 \cong U_1 \times \langle z \rangle$, we may choose in $U_1 \times \langle z \rangle$ a $G$-invariant four-subgroup $U^*$ such that $U^* > \langle z \rangle$ and we have in any case $U^* \cap U = \langle z \rangle = U^* \cap Q$. Since $U^* \cap H = \langle z \rangle = U_0 \leq Z(G)$ and $|(HU^*) : H| = 2$, we have $HU^* \leq K = N_G(H)$ and so $L = HU^*$. By Proposition 3 (using $U^*$ instead of $U$), we get that $G'$ covers $U^*/U_0$, contrary to to the fact that $G' = Q_0$. Hence $R$ does not have a $G$-invariant four-subgroup. By Lemma 1.4 in [1], $R$ is either cyclic or $R$ is of maximal class. But $\langle b^2 \rangle \cong C_4$ and $\langle b^2 \rangle \leq Z(R)$ and so $R$ must be cyclic. Assume that $R > \langle b^2 \rangle$ which together with $\exp(G) = 8$ gives $R \cong C_8$. We may choose a generator $r$ of $R$ so that $r^2 = b^{-2}$ and then $i = rb$ is an involution in $G - Q$ since $i^2 = (rb)^2 = r^2 b^2 = b^{-2} b^2 = 1$. We have

$$a^i = a^{rb} = a^b = a^{-1} \text{ and so } [a, i] = a^{-2} \notin U,$$

contrary to the fact that $G/U$ is Hamiltonian, where for each $x \in G$ with $x^2 \in U$ we must have $[G, x] \leq U$.

(v) We study the automorphisms of $Q$ induced on $Q$ by elements of $C$, where $C \cap Q = A$. Now, $A$ induces on $Q$ the inner automorphisms given by:

$$b^a = a^{-1} b a = b(b^{-1} a^{-1} b) a = b a^2, \ b^{a^2} = (ba^2)^a = ba^4 = bz.$$

Let $x \in C - A$ so that $x$ centralizes $Q_0 = \langle a^2, b^2 \rangle$ and $x$ normalizes $\langle a \rangle$ (because $\langle a \rangle$ is characteristic in $Q$ ) which gives $a^x = az^\epsilon$ , where $\epsilon \in \{0, 1\}$. Note that $b^x = by$ with some $y \in A = \langle a, b^2 \rangle$. But $x$ normalizes (centralizes ) $Q_0 = \langle a^2, b^2 \rangle \cong C_4 \times C_2$ and so $x$ must also normalize $\langle a^2, b \rangle \cong M_{16}$ and so $y \in \langle a^2, b^2 \rangle$. Then we get (noting that $b^2 \in Z(G)$):

$$b^2 = (b^2)^x = (b^x)^2 = (by)^2 = byby = b^2(b^{-1} y b) y = b^2 y^b y,$$

and so we have $y^b = y^{-1}$ and this implies $y \in \langle a^2 \rangle$.

(vi) We have proved that each element $x \in C - A$ induces on $Q$ an automorphism given by:

$$b^x = by, \text{ where } y \in \langle a^2 \rangle \text{ and } a^x = az.$$

Indeed, if $\epsilon = 0$, i.e., $a^x = a$, then $x$ would induce on $Q$ an inner automorphism, contrary to $C_G(Q) = Z(Q)$. Since $b^{x^2} = by^2$ and $a^{x^2} = a$, we have $x^2 \in Q$. Setting $G_0 = \langle x \rangle Q$, where $|G_0 : Q| = 2$, we see that $G_0 = G$ and so $G' = Q' = \langle a^2 \rangle \cong C_4$ because

$$[b, x] = y \in \langle a^2 \rangle \text{ and } [a, x] = z = a^4$$

and so $G/\langle a^2 \rangle$ is abelian. On the other hand, we know that $G' = Q_0$. This is a final contradiction and our proposition is proved. □

PROPOSITION 4.5. *Suppose that we have the case (a) of Proposition 3, where $H \cong D_8$. Then $K/H$ is cyclic and we have the following possibilities:*

(a)
$$G = (\langle a \rangle \times \langle b \rangle)\langle i \rangle, \text{ where } \langle a \rangle \cong \langle b \rangle \cong C_4$$
*and $i$ is an involution with $a^i = a^{-1}$ and $b^i = b^{-1}$ or $b^i = ba^2b^2$.*

(b) *$G$ is a unique group of order $2^5$ and class 3 with $\Omega_2(G) \cong C_2 \times D_8$ which is defined in Theorem 52.2(a) in [2] for $n = 2$.*

(c)
$$G = (\langle h \rangle \times \langle g \rangle)\langle i \rangle, \text{ where } \langle h \rangle \cong C_4, \ \langle g \rangle \cong C_{2^m}, \ m \geq 3,$$
*and $i$ is an involution with $h^i = h^{-1}$ and $g^i = g^{1+2^{m-1}}$. Here we have $|G| = 2^{m+3}$, $G' = \langle h^2, g^{2^{m-1}} \rangle \cong E_4$, $G' \leq Z(G)$, $Z(G) = \langle h^2 \rangle \times \langle g^2 \rangle \cong C_2 \times C_{2^{m-1}}$. Finally, $\langle h, i \rangle \cong D_8$ and $\langle g, i \rangle \cong M_{2^{m+1}}$ are not normal in $G$.*

(d) *$G$ is a special group of order $2^6$ given with:*
$$G = (H \times \langle a \rangle)\langle g \rangle, \text{ where } H = \langle h, i \mid h^4 = i^2 = 1, \ h^i = h^{-1}, \ h^2 = z \rangle \cong D_8,$$
$$\langle a \rangle \cong C_4, \ a^2 = z', \ g^2 = zz', \ [g, h] = 1, \ [g, i] = [g, a] = z'.$$
*We have $G' = \langle z, z' \rangle \cong E_4$, $\langle h, i \rangle \cong D_8$ is not normal in $G$ but $\langle h \rangle \trianglelefteq G$, and $\langle i, a \rangle \cong C_2 \times C_4$ is not normal in $G$ but $\langle a \rangle \trianglelefteq G$.*

*Conversely, all the above groups satisfy our assumption* $(*)$.

PROOF. By Proposition 4, we have $G' = U \cong E_4$.

(i) First assume $K/H \cong Q_8$ so that we have $|G| = 2^7$. We set $C = C_G(H) = C_K(H)$ so that we have $K = H * C$ with $U \leq C$, $H \cap C = U_0$ and $C/U_0 \cong Q_8$. Let $C_1/U_0$ and $C_2/U_0$ be two distinct cyclic subgroups of order 4 in $C/U_0$ so that $C_1$ and $C_2$ are abelian and $C_1 \cap C_2 = U$. It follows that $U \leq Z(C)$ and so we get $U = Z(K)$ and $|C'| = 2$ and therefore we have $U = U_0 \times C'$, where we set $U_0 = \langle z \rangle$ and $C' = \langle z' \rangle$. Also we have $C = C_G(L)$ and $C \trianglelefteq G$, $C' \trianglelefteq G$ , which implies $U \leq Z(G)$. Thus we get $U = Z(G) = G'$ and for any $x, y \in G$ we have $[x^2, y] = [x, y]^2 = 1$ and therefore $\mho_1(G) \leq Z(G)$ and so $U = \Phi(G)$, which shows that $G$ is special. Set $H = \langle h, t \mid h^4 = t^2 = 1, \ h^t = h^{-1} \rangle \cong D_8$ and we have $\langle h \rangle \trianglelefteq G$ (Proposition 3(a)).

(i1) Suppose that $C$ splits over $U_0$ and so we have in this case $C = \langle z\rangle \times C_0$, where $C_0 = \langle c_1, c_2\rangle \cong \mathrm{Q}_8$ and $C_0' = \langle z'\rangle$. Since $\langle t\rangle \times C_0$ has no cyclic subgroup of index 2, Proposition 1 implies that $\langle t\rangle \times C_0 \trianglelefteq G$. But then we have

$$C_0 = C \cap (\langle t\rangle \times C_0) \trianglelefteq G$$

and each element in $G$ induces on $C_0$ an inner automorphism (otherwise, a cyclic subgroup of order 4 in $C_0$ would be contained in $G'$, contrary to Proposition 4). This implies

$$G = C_0 * G_0,$$

where

$$G_0 = \mathrm{C}_G(C_0),\ C_0 \cap G_0 = \langle z'\rangle = \mathrm{Z}(C_0),\ G_0 \cap K = L,\ K = H \times C_0,$$

and $G_0$ is special of order $2^5$ with $\mathrm{Z}(G_0) = U$. Since $\langle h\rangle \trianglelefteq G$ and $h^t = h^{-1}$, there is $g \in G_0 - L$ such that $[g, h] = 1$. But $\langle t\rangle U \trianglelefteq G$ and $H$ is not normal in $G$, and so we get $t^g = tu$ with $u \in \{z', zz'\}$. However, if $t^g = tzz'$, then we replace $g$ with $g' = gh$ (noting that $g' \in G_0 - L$ and $g'$ also centralizes $h$ ) and get

$$t^{g'} = (tzz')^h = (tz)zz' = tz'.$$

Hence writing again $g$ instead of $g'$, we may assume from the start that $t^g = tz'$ and so $[t, g] = z'$. We have $g^2 \in U$ and so we have $g^2 \in \{1, z', zz', z\}$.

If $g^2 = 1$, then $[g, t] = z'$ gives that $\langle g, t\rangle \cong \mathrm{D}_8$ with $\langle g, t\rangle' = \langle z'\rangle$, where the unique cyclic subgroup $\langle gt\rangle$ of order 4 in $\langle g, t\rangle$ must be normal in $G$. Indeed, if $\langle g, t\rangle \trianglelefteq G$, then $\langle gt\rangle \trianglelefteq G$, and if $\langle g, t\rangle$ is not normal in $G$, then Proposition 3(a) implies that $\langle gt\rangle \trianglelefteq G$. However, $[gt, h] = z$ but $(gt)^2 = [g, t] = z' \neq z$ and so $\langle gt\rangle$ is not normal in $G$, a contradiction. This kind of argument we shall use here several times.

If $g^2 = z'$, then $c_1^2 = z'$ together with $[g, c_1] = 1$ implies that $gc_1$ is an involution. In that case, $[t, gc_1] = z'$ shows that $\langle t, gc_1\rangle \cong \mathrm{D}_8$ with $\langle t, gc_1\rangle' = \langle z'\rangle$. But then $\mathrm{C}_4 \cong \langle tgc_1\rangle$ is not normal in $G$ since $[tgc_1, h] = z$, a contradiction.

If $g^2 = zz'$, then $(gh)^2 = z' = c_1^2$ together with $[gh, c_1] = 1$ implies that $ghc_1$ is an involution. In that case, $[t, ghc_1] = z'z$ shows that $\langle t, ghc_1\rangle \cong \mathrm{D}_8$ with $\langle t, ghc_1\rangle' = \langle z'z\rangle$. But then $\mathrm{C}_4 \cong \langle tghc_1\rangle$ is not normal in $G$ since $[tghc_1, g] = z'$, a contradiction.

If $g^2 = z$, then $gh$ is an involution. In this case, $[t, gh] = z'z$ shows that $\langle t, gh\rangle \cong \mathrm{D}_8$ with $\langle t, gh\rangle' = \langle z'z\rangle$. But then $\mathrm{C}_4 \cong \langle tgh\rangle$ is not normal in $G$ since $[tgh, g] = z'$, a contradiction.

(i2) We have proved that $C$ does not split over $U_0$. Since $C$ is two-generator with $C' = \langle z'\rangle$, it follows that $C$ is minimal nonabelian. We have $\Omega_1(C) = U \cong \mathrm{E}_4$ and so $C$ is metacyclic. Hence we may choose generators $c_1, c_2$ of $C$ so that we have

$$\mathcal{H}_2 \cong C = \langle c_1, c_2 \mid c_1^4 = c_2^4 = 1,\ c_1^{c_2} = c_1^{-1}\rangle,$$

where $c_1^2 = z'$, $c_2^2 = zz'$, $z$ is not a square in $C$.

Since $\langle h\rangle \trianglelefteq G$ and $h^t = h^{-1}$, it follows that $\mathrm{C}_G(h)$ covers $G/K$. Let $g \in \mathrm{C}_G(h) - K$ so that $[h, g] = 1$ and $g^2 \in \langle z, z'\rangle$. Because $\langle t\rangle U \trianglelefteq G$, $\langle h\rangle \trianglelefteq G$ and $H$ is not normal in $G$, it follows that $t^g = tu$ with $u \in U - U_0$. Replacing $g$ with $gh$, if necessary, we may assume from the start that $t^g = tz'$ and so we have $[g, t] = z'$.

If $g$ normalizes $\langle c_1\rangle$, then replacing $g$ with $g' = gc_2$ (if necessary), we may assume that $g'$ centralizes $\langle c_1\rangle$ (and we note that $g'$ acts the same way on $H$ as $g$ does). In this case we write again $g$ instead of $g'$ and we have $[g, c_1] = z^\epsilon$ with $\epsilon = 0$. If $g$ does not normalize $\langle c_1\rangle$, then we have $[g, c_1] = zz'$ or $[g, c_1] = z$. If in this case $[g, c_1] = zz'$, then again replacing $g$ with $g' = gc_2$, we get

$$[g', c_1] = [gc_2, c_1] = (zz')z' = z.$$

Hence writing again $g$ instead of $g'$, we may assume from the start that $[g, c_1] = z^\epsilon$ with $\epsilon = 1$. Hence we have in any case $[g, c_1] = z^\epsilon$, where $\epsilon \in \{0, 1\}$.

If $g^2 = 1$, then $[g, t] = z'$ shows that $\langle g, t\rangle \cong \mathrm{D}_8$ with $\langle g, t\rangle' = \langle z'\rangle$. But then $\mathrm{C}_4 \cong \langle gt\rangle$ is not normal in $G$ since $[gt, h] = z$, a contradiction.

Assume that $g^2 = z'$. If $\epsilon = 0$, then we have $[g, c_1] = 1$ and so $gc_1$ is an involution. Then $[t, gc_1] = z'$ shows that $\langle t, gc_1\rangle \cong \mathrm{D}_8$ with $\langle t, gc_1\rangle' = \langle z'\rangle$. But then $\mathrm{C}_4 \cong \langle tgc_1\rangle$ is not normal in $G$ since $[tgc_1, h] = z$, a contradiction. Thus we must have $\epsilon = 1$ and so we get $[g, c_1] = z$. We compute

$$(ghc_1)^2 = z'z \cdot z' \cdot [c_1, gh] = zz = 1,$$

and so $ghc_1$ is an involution. Then $[t, ghc_1] = z'z$ shows that $\langle t, ghc_1\rangle \cong \mathrm{D}_8$ with $\langle t, ghc_1\rangle' = \langle z'z\rangle$. But then $\mathrm{C}_4 \cong \langle tghc_1\rangle$ is not normal in $G$ since $[tghc_1, h] = z$, a contradiction.

If $g^2 = z$, then $gh$ is an involution. Then $[t, gh] = z'z$ shows that $\langle t, gh\rangle \cong \mathrm{D}_8$ with $\langle t, gh\rangle' = \langle z'z\rangle$. But then $\mathrm{C}_4 \cong \langle tgh\rangle$ is not normal in $G$ since $[tgh, g] = z'$, a contradiction.

Suppose that $g^2 = zz'$. Assume in addition that $\epsilon = 0$ and so $[g, c_1] = 1$. In this case we have

$$(ghc_1)^2 = zz' \cdot z \cdot z' = 1$$

and so $ghc_1$ is an involution. Then $[t, ghc_1] = z'z$ shows that $\langle t, ghc_1\rangle \cong \mathrm{D}_8$ with $\langle t, ghc_1\rangle' = \langle z'z\rangle$. But then $\mathrm{C}_4 \cong \langle tghc_1\rangle$ is not normal in $G$ since $[tghc_1, g] = z'$, a contradiction. Hence we must have $\epsilon = 1$ and so $[g, c_1] = z$. In this case, $gc_1$ is an involution since $(gc_1)^2 = zz' \cdot z' \cdot z = 1$. Then $[t, gc_1] = z'$ shows that $\langle t, gc_1\rangle \cong \mathrm{D}_8$ with $\langle t, gc_1\rangle' = \langle z'\rangle$. But then $\mathrm{C}_4 \cong \langle tgc_1\rangle$ is not normal in $G$ since $[tgc_1, g] = z'z$, a contradiction. We have finally proved that here $K/H \cong \mathrm{Q}_8$ is not possible.

(ii) Now assume that $K/H \neq \{1\}$ is cyclic. Here we have $K = H \times \langle a \rangle$ with $o(a) = 2^n$, $n \geq 1$, where we set

$$\Omega_1(\langle a \rangle) = \langle z' \rangle,\ U_0 = \langle z \rangle = \mathrm{Z}(H),$$
$$\langle h, h' \mid h^4 = (h')^2 = 1,\ [h, h'] = z,\ z^2 = 1 \rangle \cong \mathrm{D}_8,\ U = \langle z, z' \rangle = G'.$$

Since $\langle h \rangle \trianglelefteq G$ (Proposition 3(a)) and $h^{h'} = h^{-1}$, it follows that $\mathrm{C}_G(h)$ covers $G/H \cong \mathrm{C}_2$. Let $g \in \mathrm{C}_G(h) - K$ so that we have $(h')^g = h'u$ for some $u \in U - U_0$ (noting that $\langle h \rangle \trianglelefteq G$ and $\langle U\langle h' \rangle \rangle \trianglelefteq G$ but $H$ is not normal in $G$) and so replacing $g$ with $gh$ (if necessary), we may assume from the start that $(h')^g = h'z'$ and so we have $[g, h'] = z'$.

(ii1) Assume that $K = L$ and $z' \in \mathrm{Z}(G)$. In this case we have $\mathrm{Z}(K) = \mathrm{Z}(L) = U = \mathrm{Z}(G)$ and $\mho_1(G) \leq \mathrm{Z}(G)$. Hence $G$ is a special group of order $2^5$. In particular, all elements in $G - K$ are of order $\leq 4$. Suppose that there is an involution $t \in \mathrm{C}_G(h) - K$. Then we have $[h', t] = u \in U - \langle z \rangle$ and therefore $\langle h', t \rangle \cong \mathrm{D}_8$ with $\langle h', t \rangle' = \langle u \rangle$. Then we must have $\mathrm{C}_4 \cong \langle h't \rangle \trianglelefteq G$. On the other hand, $[h't, h] = z$, a contradiction. Hence there is no involution in $\mathrm{C}_G(h) - K$. If $g^2 = z$, then $hg$ is an involution in $\mathrm{C}_G(h) - K$, a contradiction. Hence we have

$$g^2 \in \{z', zz'\} \text{ and } \langle h, g \rangle = \langle h \rangle \times \langle g \rangle \cong \mathrm{C}_4 \times \mathrm{C}_4.$$

We set $h' = i$ so that $G = (\langle h \rangle \times \langle g \rangle)\langle i \rangle$ with $h^i = h^{-1}$ and $g^i = gz'$. We have obtained two groups of order $2^5$ stated in part (a) of our proposition, which obviously satisfy our assumption $(*)$.

(ii2) Assume that $K = L$ and $z' \notin \mathrm{Z}(G)$. Then we have $[g, z'] = z$. Suppose that there is an element $y \in G - K$ of order $\leq 4$. We claim that in this case we have $y^2 \in U$. Indeed, if $y^2$ is a noncentral involution in $K = L$, then $y^2$ inverts $\langle h \rangle$ and $y$ normalizes $\langle h \rangle$ (since $\langle h \rangle \trianglelefteq G$), a contradiction. Hence we have $y^2 \in U$ and so $y^2 \in \langle z \rangle$ since $[y, z'] = z$. We get $D = \langle y, U \rangle \cong \mathrm{D}_8$ and $D \trianglelefteq G$ with $\mathrm{Z}(D) = \langle z \rangle = D'$. Since $G' = U$ is elementary abelian, each element in $G$ induces an inner automorphism on $D$. Hence we have $G = D * C$, where $C = \mathrm{C}_G(D)$ and $D \cap C = \langle z \rangle$. Since $|C| = 2^3$ and $z \in \mathrm{Z}(C)$, we have $C' \leq \langle z \rangle$. This gives that $G' = \langle z \rangle$, contrary to Proposition 3(a). We have proved that all elements in $G - K$ are of order 8 and so $\Omega_2(G) \cong \mathrm{C}_2 \times \mathrm{D}_8$. Since $g$ centralizes $\langle h \rangle$, we must have $\langle g^2 \rangle = \langle h \rangle$ and so we may assume that $g^2 = h$. Indeed, if $\langle g^2 \rangle = \langle hz' \rangle$, then $g$ would centralize $h$ and $hz'$ and so $g$ would centralize $z'$, a contradiction. We have obtained a unique group $G$ of order $2^5$ and class 3 with $\Omega_2(G) \cong \mathrm{C}_2 \times \mathrm{D}_8$ which is defined in Theorem 52.2(a) in [2] for $n = 2$ (stated in part (b) of our proposition). This group obviously satisfies our assumption $(*)$.

(ii3) Assume that $K > L$, i.e., $o(a) = 2^n$, $n \geq 2$. Then there is an element $w \in \langle a \rangle$ of order 4 so that $w^2 = z'$. We have

$$\langle z, w \rangle = \langle z \rangle \times \langle w \rangle \trianglelefteq G \text{ and so } \mho_1(\langle z \rangle \times \langle w \rangle) = \langle z' \rangle \trianglelefteq G,$$

which implies that $G' = U \le \mathrm{Z}(G)$. We have also $\mho_1(G) \le \mathrm{Z}(G)$. Since $G/L$ is abelian and $K/L \neq \{1\}$ is cyclic, we have here two subcases.

(ii3a) Suppose that $G/L$ is cyclic and so if $g \in \mathrm{C}_G(h) - K$, then $\langle g\rangle$ covers $G/L$, $[h', g] = z'$ with $\langle z'\rangle = \Omega_1(\langle g^2\rangle)$ and $o(g) = 2^m$, $m \ge 3$. Hence we have $\langle g, h'\rangle \cong \mathrm{M}_{2^{m+1}}$. Setting $h' = i$, we get

$$G = (\langle h\rangle \times \langle g\rangle)\langle i\rangle,$$

where

$$\langle h\rangle \cong \mathrm{C}_4,\ \langle g\rangle \cong \mathrm{C}_{2^m},\ m \ge 3,\ h^i = h^{-1},\ g^i = g^{1+2^{m-1}}.$$

We have obtained the groups stated in part (c) of our proposition. Conversely, let $X$ be a non-normal and noncyclic subgroup of order $\ge 2^3$ in $G$. We see that $A = \langle h\rangle \times \langle g\rangle$ is an abelian maximal subgroup in $G$. If $X \cap A$ is noncyclic, then $X \cap A \ge \langle z, z'\rangle = G'$ and so $X \trianglelefteq G$, a contradiction. Hence $X \cap A$ is cyclic and then $X \not\le A$ so that $|X : (X \cap A)| = 2$. It follows that $\mathrm{N}_G(X \cap A) \ge \langle A, X\rangle = G$ and so $X \cap A \trianglelefteq G$. Thus, if $g \in G$ is such that $X^g \neq X$, then $X \cap X^g = X \cap A$ is cyclic. Finally, $\langle h, i\rangle \cong \mathrm{D}_8$ and $[i, g] = z' \notin \langle h, i\rangle$ and so $\langle h, i\rangle$ is not normal in $G$. Hence our groups satisfy the assumption $(*)$.

(ii3b) $G/L$ is noncyclic abelian so that $G/L$ splits over $K/L$, where $K = H \times \langle a\rangle$ with $o(a) = 2^n$, $n \ge 2$, and $\Omega_1(\langle a\rangle) = \langle z'\rangle$. We have $G = KG_0$, where $K \cap G_0 = L$ and $|G_0 : L| = 2$. Since $G' = U = \langle z, z'\rangle \le \mathrm{Z}(G)$ and $\mho_1(G) \le \mathrm{Z}(G)$), we have that $G_0$ is one of two groups defined in part (a) of this proposition, where there is $g \in G_0 - L$ such that $\langle g, h\rangle = \langle g\rangle \times \langle h\rangle$, $[h', g] = z'$ and $g^2 = z^\epsilon z'$ with $\epsilon = 0, 1$.

Suppose that $\epsilon = 0$ so that $g^2 = z'$ and so $h'$ inverts each element in $\langle g, h\rangle$. Consider the subgroup $H_1 = \langle h', g\rangle \cong \mathrm{D}_8$ with $\mathrm{Z}(\langle h', g\rangle) = \langle z'\rangle$. If $H_1 \trianglelefteq G$, then $\langle g\rangle \trianglelefteq G$ and if $H_1$ is not normal in $G$, then Proposition 3(a) shows that also $\langle g\rangle \trianglelefteq G$. Hence in any case we have $\langle g\rangle \trianglelefteq G$. Since $\langle a\rangle$ centralizes $h'$, it follows that $\langle a\rangle \times \langle z\rangle$ normalizes $H_1$. On the other hand, $[h, h'] = z$ and so $\langle h\rangle$ does not normalize $H_1$ a so we get

$$\mathrm{N}_G(H_1) = H_1(\langle a\rangle \times \langle z\rangle).$$

If $w$ is an element of order 4 in $\langle a\rangle$, then we have $w^2 = z'$ and so $(H_1\langle w\rangle)/H_1$ and $(H_1\langle z\rangle)/H_1$ are two distinct subgroups of order 2 in $\mathrm{N}_G(H_1)/H_1$, contrary to Proposition 2. We have proved that we must have $\epsilon = 1$ and so $g^2 = zz'$.

Assume that there is an element $w \in \langle a\rangle$ of order 4 such that $w^2 = z'$ and $[w, g] = 1$. Then we have

$$(wg)^2 = w^2 g^2 = z' \cdot zz' = z, [wg, h] = 1,$$

and so $hwg$ is an involution. From $[h', hwg] = zz'$ follows that

$$\langle h', hwg\rangle \cong \mathrm{D}_8 \text{ with } \mathrm{Z}(\langle h', hwg\rangle) = \langle zz'\rangle.$$

But then $C_4 \cong \langle h'hwg \rangle$ is not normal in $G$ since $[h'hwg, h] = z$, a contradiction. We have proved that there is no such an element $w \in \langle a \rangle$. This implies

$$n = 2,\ o(a) = 4,\ \exp(G) = 4,\ a^2 = z',\ [a, g] \neq 1,\ Z(G) = U = G' = \Phi(G)$$

and so $G$ is special of order $2^6$. It remains to determine $[a, g] \neq 1$.

Suppose that $[a, g] = z$. Then we get $(ag)^2 = z' \cdot zz' \cdot z = 1$ and so $ag$ is an involution. Since $[h', ag] = z'$, we have $\langle h', ag \rangle \cong D_8$ with $Z(\langle h', ag \rangle) = \langle z' \rangle$. But then $C_4 \cong \langle h'ag \rangle$ is not normal in $G$ since $[h'ag, h] = z$, a contradiction.

Suppose that $[a, g] = zz'$. Then we get $(gah')^2 = zz' \cdot z' \cdot zz' \cdot z' = 1$ and so $gah'$ is an involution. Since $[gah', h'] = z'$, we have $\langle gah', h' \rangle \cong D_8$ with $Z(\langle gah', h' \rangle) = \langle z' \rangle$. But then $C_4 \cong \langle gah'h' \rangle = \langle ga \rangle$ is not normal in $G$ since $[ga, g] = zz'$, a contradiction.

Hence we must have $[a, g] = z'$ and so the structure of $G$ is uniquely determined. We set $h' = i$ and so we get a special group $G$ of order $2^6$ given with:

$$G = (H \times \langle a \rangle)\langle g \rangle,\ \text{where } H = \langle h, i \mid h^4 = i^2 = 1,\ h^i = h^{-1},\ h^2 = z \rangle \cong D_8,$$
$$\langle a \rangle \cong C_4,\ a^2 = z',\ g^2 = zz',\ [g, h] = 1,\ [g, i] = [g, a] = z'.$$

We have $G' = \langle z, z' \rangle \cong E_4$, $\langle h, i \rangle \cong D_8$ is not normal in $G$ but $\langle h \rangle \trianglelefteq G$, and $\langle i, a \rangle \cong C_2 \times C_4$ is not normal in $G$ but $\langle a \rangle \trianglelefteq G$. We have obtained the group stated in part (d) of our proposition.

It remains to be proved that this group $G$ satisfies our assumption $(*)$. We first show that there are no involutions in $G - K$, where $K = H \times \langle a \rangle$. Indeed, suppose that $gh^\alpha i^\beta a^\gamma$ with $\alpha, \beta, \gamma \in \{0, 1\}$ is an involution. Then we get

$$1 = (gh^\alpha i^\beta a^\gamma)^2 = zz' \cdot z^\alpha \cdot (z')^\gamma \cdot (z')^\beta \cdot (z')^\gamma \cdot z^{\alpha\beta} = z^{1+\alpha+\alpha\beta}(z')^{1+\beta},$$

which implies $\beta = 1$ and then we get $z = 1$, a contradiction. We have proved that $\Omega_1(G) = L = HU$, where $U = \langle z, z' \rangle$. There are exactly two conjugate classes of noncentral involutions in $G$ with representatives $i$ (4 conjugates) and $hi$ (4 conjugates) and we have

$$C_G(i) = \langle i, z \rangle \times \langle a \rangle \cong E_4 \times C_4 \text{ and } C_G(hi) = \langle hi, z \rangle \times \langle a \rangle \cong E_4 \times C_4.$$

Let $X$ be a noncyclic non-normal subgroup of order $\geq 2^3$ which contains more than one involution (so that $X \cong Q_8$ is excluded). Then we have $G' = U = \langle z, z' \rangle \nleq X$ and $|X| = 2^3$ or $2^4$ (noting that all subgroups of order $\geq 2^5$ are normal in $G$).

First assume that $|X| = 2^4$. In this case $X \nleq K$ since $\Phi(K) = \langle z, z' \rangle$ and $|K| = 2^5$. We have $|X : (X \cap K)| = 2$ and $|X \cap K| = 2^3$. All elements in $X - K$ are of order 4 and so $\mho_1(X) \neq \{1\}$ and this implies that there is exactly one central involution $z_0$ in $G$ which is contained in $X \cap K$ and therefore we have $\mho_1(X) = \langle z_0 \rangle$ and $d(X) = 3$. But $X \cap K$ must contain another involution $i' \neq z_0$ which is noncentral in $G$ and we know (by the above) that $C_G(i') = C_K(i')$ is abelian. In particular, $X$ is nonabelian and $X' = \langle z_0 \rangle$. Because $d(X) = 3$, $X$ is not minimal nonabelian. Let $X_0$ be any minimal nonabelian subgroup in $X$. If $X_0 \cong D_8$, then (since there are no involutions in $X - K$) we have $X_0 = X \cap K$. Since $G' \cong E_4$, it follows that $X$ induces on $X_0$ only inner automorphisms of $X_0$ which implies that $C_X(i') \not\leq K$, a contradiction. Hence each minimal nonabelian subgroup of $X$ is isomorphic to $Q_8$. By Corollary A.17.3 in [2], we get $X = \langle t \rangle \times Q$, where $t$ is an involution and $Q \cong Q_8$ with $Z(Q) = X' = \langle z_0 \rangle$. Thus $t$ is a noncentral involution in $G$, contrary to the fact that $C_G(t)$ must be abelian.

We have proved that $|X| = 2^3$ and assume first that $X \not\leq K$. Since $X$ contains more than one involution, it follows that $X \cap K$ contains a noncentral involution $i'$ of $G$. We know that $C_G(i') \leq K$ and so $X$ is nonabelian. But then $X \cong D_8$ which is not possible since there are no involutions in $X - K$. We have proved that $X \leq K$.

If $X \cong E_8$, then $X \leq L$, where $L = H \times \langle z' \rangle$. But then $X \geq \langle z, z' \rangle = G'$, a contradiction. It follows that either $X \cong D_8$ or $X \cong C_4 \times C_2$. First assume that $X \cong D_8$. Because in this case $\Omega_1(X) = X$ and $\Omega_1(K) = L$, it follows that $X \leq L$. But then $X$ is conjugate in $G$ to $H = \langle h, i \rangle$ or to $H^* = \langle hz', i \rangle$, where both $\langle h \rangle$ and $\langle hz' \rangle$ are normal in $G$.

Finally, suppose that $X \cong C_4 \times C_2$. Because in this case $\{1\} \neq \mho_1(X) \leq \langle z, z' \rangle$, it follows that $X$ contains exactly one central involution of $G$ and two noncentral involutions of $G$. Then $X$ is conjugate in $G$ to $X_1 = \langle i \rangle \times \langle v \rangle$ or to $X_2 = \langle hi \rangle \times \langle w \rangle$, where $\langle v \rangle \cong \langle w \rangle \cong C_4$. Since

$$X_1 \leq C_G(i) = C_K(i) = \langle i, z \rangle \times \langle a \rangle,$$

we get $X_1 = \langle i \rangle \times \langle a \rangle$ or $X_1 = \langle i \rangle \times \langle az \rangle$. Similarly,

$$X_2 \leq C_G(hi) = C_K(hi) = \langle hi, z \rangle \times \langle a \rangle,$$

gives $X_2 = \langle hi \rangle \times \langle a \rangle$ or $X_2 = \langle hi \rangle \times \langle az \rangle$. On the other hand, we see that $\langle a \rangle \trianglelefteq G$ and $\langle az \rangle \trianglelefteq G$ and we are done. Our proposition is completely proved. □

Proposition 4.6. *Suppose that we have the case (b1) of Proposition 3. Then $H$ possesses exactly one $G$-invariant cyclic subgroup of index $p$.*

Proof. We have $H \cong M_{p^n}$, $n \geq 3$, ( if $p = 2$, then $n \geq 4$ ) or $H$ is abelian of type $(p^s, p)$, $s \geq 2$. Set $H_0 = \Omega_1(H)$ and then we have

$$H_0 \cong E_{p^2},\ N_G(H_0) = N_G(H) = K,\ |G/K| = p,\ U_0 = U \cap H = \langle z \rangle \leq Z(G),$$

and let $g \in G - K$. Note that $H$ has exactly $p$ cyclic subgroups of index $p$. By Proposition 4, we have $G' \leq U$ and so we get $[K, H] \leq H \cap U = U_0 = \langle z \rangle$. This implies that each cyclic subgroup of index $p$ in $H$ is normal in $K$. Assume, by way of contradiction, that $H$ does not have any $G$-invariant cyclic subgroup of index $p$. Since $H \cap H^g$ is a cyclic subgroup of index $p$ in $H$, there is a cyclic subgroup $\langle h\rangle$ of index $p$ in $H$ such that $\langle h\rangle^g = \langle ht\rangle$ for some element $t \in H_0 - \langle z\rangle$. Then we get

$$h^g = htv \text{ with some } v \in \langle (ht)^p\rangle = \langle h^p\rangle.$$

In that case we get

$$h^{-1}h^g = [h, g] = tv \in U \cap H = \langle z\rangle.$$

Since $v \in \langle h^p\rangle$ and (by Proposition 3(b1)) $\langle h^p\rangle \geq \langle z\rangle$, it follows that $t \in \langle h^p\rangle$, a contradiction. Since $H$ is not normal in $G$, then clearly $H$ possesses exactly one $G$-invariant cyclic subgroup of index $p$ and we are done. ∎

Proposition 4.7. *Suppose that we have the case (b1) of Proposition 3 and assume in addition that $K/H_0$ is Hamiltonian (and so $p = 2$), where $H_0 = \Omega_1(H) \cong \mathrm{E}_4$, and that $G$ does not possess any non-normal subgroup isomorphic to $\mathrm{D}_8$. Then $G$ is of order $2^7$ and class 2 which has a normal subgroup $K$ of index 2, where*

$$K = (\langle h\rangle \times Q)\langle t\rangle \text{ with } \langle h\rangle \cong \mathrm{C}_4,\ h^2 = z,\ Q = \langle a, b\rangle \cong \mathrm{Q}_8,\ Q' = \langle u\rangle,$$

*$t$ is an involution commuting with $h$ and $a$ and $[b, t] = z$. There is an element $g \in G - K$ such that either*

(a) $g^2 = uz$, *$g$ centralizes $Q$,* $[g, h] = z$, $[g, t] = u$
*(and here $G$ is a special group with $G' = \langle u, z\rangle \cong \mathrm{E}_4$ and $\Omega_1(G) = G' \times \langle t\rangle \cong \mathrm{E}_8$)*
*or*

(b) $g^2 = h$, *$g$ centralizes $Q$,* $[g, t] = uz$
*(and here $G$ is of exponent 8 with $G' = \langle u, z\rangle \cong \mathrm{E}_4$, $\mathrm{Z}(G) = G'\langle h\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$, $\Omega_1(G) = G' \times \langle t\rangle \cong \mathrm{E}_8$ and $\Omega_2(G) = K$).*

*Conversely, the above two groups satisfy our assumption $(*)$.*

Proof. We have

$$H_0 = \Omega_1(H) \cong \mathrm{E}_4,\ \mathrm{N}_G(H_0) = \mathrm{N}_G(H) = K,\ |G : K| = 2,$$

$$\mathrm{E}_8 \cong S = H_0U \trianglelefteq G,\ U \cap H_0 = U \cap H = U_0 = \langle z\rangle \leq \mathrm{Z}(G),$$

and $K/H_0$ is Hamiltonian. By Proposition 4, we have $G' \leq U$ and this gives

$$(K/H_0)' = S/H_0 = \mho_1(K/H_0),$$

and so $\exp(K) = 4$ and $H \cong \mathrm{C}_4 \times \mathrm{C}_2$. By Proposition 3(b1), $L = HU$ is abelian of type $(4, 2, 2)$, $\mho_1(L) = \mho_1(H) = U_0 = \langle z\rangle$ and so we have $S = \Omega_1(L) = \Omega_1(K)$.

Let $Q/H_0$ be an ordinary quaternion subgroup of $K/H_0$. Since

$$(Q/H_0)' = (K/H_0)' = S/H_0,$$

it follows that $S < Q$. Also, $S/H_0$ is a unique subgroup of order 2 in $Q/H_0$ and so we have $Q \cap H = H_0$ and $Q \cap L = S$. Since $Q/H_0 \cong \mathrm{Q}_8$ is isomorphic to a subgroup of $K/H$, Proposition 2 implies that $K/H \cong \mathrm{Q}_8$ and so we get $K = HQ$ with $H \cap Q = H_0$.

We have $|Q : \mathrm{C}_Q(H_0)| \leq 2$ and so if $a \in \mathrm{C}_Q(H_0) - S$, then $a^2 \in S - H_0$ and so $A = \langle a \rangle \times H_0 \cong \mathrm{C}_4 \times \mathrm{E}_4$ (containing $U$) is an abelian maximal subgroup of $Q$, $A \trianglelefteq G$ and we get $\mho_1(A) = \langle a^2 \rangle \leq \mathrm{Z}(G)$ and $\mathrm{E}_4 \cong \langle a^2, z \rangle \trianglelefteq G$. On the other hand, $G/K$ acts on the three maximal subgroups of $S$ which contain $\langle z \rangle \leq \mathrm{Z}(G)$ fixing $U$ and fusing the other two (since $\mathrm{N}_G(H_0) = K$) and so we get $\langle a^2, z \rangle = U$ and $U \leq \mathrm{Z}(G)$. In particular, $G$ is of class 2 with an elementary abelian commutator subgroup of order $\leq 4$ (contained in $U$) and this implies that $\mho_1(G) \leq \mathrm{Z}(G)$. Indeed, if $x, y \in G$, then we have $[x^2, y] = [x, y]^2 = 1$. We have $\mho_1(K) \leq S$ and since $S \cap \mathrm{Z}(G) = U$, we get $\mho_1(K) \leq U$ and so $\Phi(K) = U$. For each element $k \in K - L$, we have $k^2 \in U - \langle z \rangle$.

By Proposition 6, $H$ possesses exactly one cyclic subgroup $\langle h \rangle$ of index 2 which is normal in $G$ and we have $h^2 = z$. Note that for an element $u \in U - \langle z \rangle$, the cyclic subgroup $\langle hu \rangle \cong \mathrm{C}_4$ is also normal in $G$. But the abelian normal subgroup $L$ possesses exactly four cyclic subgroups of order 4 and so the other two cyclic subgroups of order 4 in $L$ (which are distinct from $\langle h \rangle$ and $\langle hu \rangle$) must be fused in $G$. Indeed, if $t \in H_0 - \langle z \rangle$ and $g \in G - K$, then we have $t^g = tu$ for some $u \in U - \langle z \rangle$ and so we get $\langle ht \rangle^g = \langle htu \rangle$.

By Proposition 4, $G/U$ is abelian and so $G/L$ is abelian and $K/L \cong \mathrm{E}_4$. Assume that $G/L$ is not elementary abelian. Then there is an element $x \in G - K$ such that $x^2 \in K - L$. But then $x^2 \in \mathrm{Z}(G)$, contrary to the fact that $K/H \cong \mathrm{Q}_8$. Hence we have $G/L \cong \mathrm{E}_8$. For any $g \in G - K$, we have $g^2 \in L \cap \mathrm{Z}(G)$ and so either $g^2 \in U$ or $g^2 \in L - S$ and in the second case we have either $g^2 \in \langle h \rangle$ or $g^2 \in \langle hu \rangle$ with $u \in U - \langle z \rangle$. Note that $H_1 = \langle hu, t \rangle$ is also a maximal non-normal subgroup in $G$ with $\Omega_1(H_1) = \Omega_1(H) = \langle z, t \rangle$. Indeed, if $H_1$ is not maximal non-normal, then let $H_1^*$ containing $H_1$ be a maximal non-normal subgroup in $G$. Since $\exp(G) \leq 8$ and $\exp(K) = 4$, it follows that $H_1^* \cong \mathrm{C}_8 \times \mathrm{C}_2$ or $H_1^* \cong \mathrm{M}_{16}$ and so $H_1^* \not\leq K$. But we have

$$\Omega_1(H_1^*) = \Omega_1(H_1) = H_0 = \langle z, t \rangle$$

and so we get $H_0 \trianglelefteq G$, a contradiction. Thus, in case that we have an element $g \in G - K$ with $g^2 \in \langle hu \rangle$, we replace $H$ with $H_1$ (and write again $H$ instead of $H_1$) so that we may assume from the start that $g^2 \in \langle h \rangle$ and then (by a suitable choice of a generator of $\langle g \rangle$) we have $g^2 = h$.

Let $k$ be any element in $K - L$ which commutes with $t \in H_0 - \langle z \rangle$. Then we have $k^2 \in U - \langle z \rangle$ so that $\langle k, t \rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$. We claim that in that case at least one of cyclic subgroups $\langle k \rangle$ or $\langle kt \rangle$ is normal in $G$. If $\langle k, t \rangle \trianglelefteq G$, then both $\langle k \rangle$ and $\langle kt \rangle$ are normal in $G$ because $G' \leq U$. (If there is $x \in G$ such that $k^x = kt$ or $k^x = k^{-1}t$, then we have either $t \in G'$ or $k^2 t \in G'$ and so $t \in U$, a contradiction.) If $\langle k, t \rangle$ is not normal in $G$, then it is easy to see that $\langle k, t \rangle$ is a maximal non-normal subgroup in $G$. Indeed, if $H^* > \langle k, t \rangle$ is a maximal non-normal subgroup in $G$, then by Proposition 3, $H^* \cong \mathrm{C}_8 \times \mathrm{C}_2$

or $H^* \cong \mathrm{M}_{16}$ (noting that $\exp(G) \leq 8$) and so $k$ or $kt$ is a square in $H^*$ and therefore $k$ or $kt$ is contained in $\mathrm{Z}(G)$, contrary to the fact that $K/H \cong \mathrm{Q}_8$. Hence $\langle k, t\rangle$ is a maximal non-normal subgroup in $G$ and so, by Proposition 6, one of $\langle k\rangle$ or $\langle kt\rangle$ is normal in $G$. Since $\langle k, t\rangle \cap \langle h\rangle = \{1\}$ and $\langle h\rangle \trianglelefteq G$, we see that $k$ or $kt$ commutes with $h$. But $t$ commutes with $h$ and so in any case $k$ commutes with $h$. We have proved that whenever an element $k \in K - L$ commutes with $t \in H_0 - \langle z\rangle$, then $k$ also commutes with $h$.

Suppose, by way of contradiction, that $t \in \mathrm{Z}(Q)$. Let $a, b \in Q - S$ be such that $\langle a, b\rangle$ covers $Q/S$ and set $a^2 = u \in U - \langle z\rangle$. By the above, both $a$ and $b$ commute with $h$. We have $[a, b] \in U - \langle z\rangle$ and so $[a, b] \in \{u, uz\}$. Suppose at the moment that $[a, b] = uz$. By the previous paragraph, we know that $\langle a\rangle$ or $\langle at\rangle$ is normal in $G$. On the other hand, we have

$$a^b = a(uz),\ (at)^b = (at)(uz) \text{ with } a^2 = (at)^2 = u,$$

and so both $\langle a\rangle$ and $\langle at\rangle$ are non-normal in $G$, a contradiction. Thus, we must have $[a, b] = u$. Considering the subgroup $\langle ah\rangle \times \langle t\rangle$, we know that one of $\langle ah\rangle$ or $\langle aht\rangle$ must be normal in $G$. But we have

$$(ah)^2 = (aht)^2 = uz,\ (ah)^b = (ah)u,\ (aht)^b = (aht)u,$$

and so both $\langle ah\rangle$ and $\langle aht\rangle$ are non-normal in $G$, a contradiction.

We have proved that $t \notin \mathrm{Z}(Q)$. Then we have $|Q : \mathrm{C}_Q(t)| = 2$. Let $a \in \mathrm{C}_Q(t) - S$ and $b \in Q - \mathrm{C}_Q(t)$ so that

$$\langle a, b\rangle \text{ covers } Q/S,\ [a, b] \in U - \langle z\rangle,\ [a, h] = 1, \text{ and } [b, t] = z.$$

In particular, we get $Q' = G' = U$ and we set $a^2 = u \in U - \langle z\rangle$. If $[a, b] = uz$, then we replace $a$ with $a' = at$ (noting that $[a', h] = 1$ and $(a')^2 = u$) and then we get $[a', b] = [at, b] = uz \cdot z = u$. We write $a$ instead $a'$ so that we may assume from the start that $[a, b] = u$. If $b^2 = uz$, then we replace $b$ with $b' = bt$ (noting that $[a, b'] = [a, bt] = u$ and $[b', t] = [bt, t] = z$) and we obtain

$$(b')^2 = (bt)^2 = b^2t^2[t, b] = uz \cdot z = u.$$

Hence writing $b$ instead of $b'$, we may assume from the start that $b^2 = u$. We have obtained that $Q^* = \langle a, b\rangle \cong \mathrm{Q}_8$. Since $(at)^b = (at)(uz)$ and $(at)^2 = u$, we see that $\langle at\rangle$ is not normal in $G$. This implies that $\langle a\rangle$ is normal in $G$. Also note that $b$ has four conjugates in $Q$ and $Q \trianglelefteq G$. Since $|G'| = 4$, $b$ has exactly four conjugates in $G$ and so $\mathrm{C}_G(b)$ must cover $G/Q$. Let $g \in \mathrm{C}_G(b) - K$ and we know that $g$ normalizes $\langle a\rangle$. If $a^g = a^{-1} = au$, then we replace $g$ with $g' = gb \in G - K$ so that

$$a^{g'} = a^{gb} = (au)^b = (au)u = a.$$

Noting that $g'$ also commutes with $b$, we may write $g$ instead of $g'$ so that we may assume from the start that $g \in G - K$ centralizes $Q^* = \langle a, b\rangle$. Since $t^b = tz$ and $t^g = tu'$ with some $u' \in U - \langle z\rangle$, it follows that the conjugate class of $t$ in $G$ contains four elements (and they all lie in $S - U$).

Now it is easy to see that there are no involutions contained in $G - K$ and so we have $\Omega_1(G) = S = G' \times \langle t \rangle \cong \mathrm{E}_8$. Indeed, assume that there is an involution $i \in G - K$. Then we have $D = \langle i, t \rangle \cong \mathrm{D}_8$ and by our assumption we have $D \trianglelefteq G$. Since $G' \cong \mathrm{E}_4$ is elementary abelian, each element in $G$ induces on $D$ an inner automorphism of $D$. In particular, both four-subgroups in $D$ are normal in $G$. But then $t$ would have only two conjugates in $G$, a contradiction.

It remains to determine:

$$g^2,\ h^g = hz^{\epsilon},\ h^b = hz^{\eta},\ \text{and } t^g = tuz^{\zeta},\ \text{where } \epsilon, \eta, \zeta \in \{0, 1\}.$$

Considering the subgroup $\langle ah \rangle \times \langle t \rangle$, we know (by the above) that at least one of the cyclic subgroups $\langle ah \rangle$ or $\langle aht \rangle$ must be normal in $G$. Since

$$\langle h, a, t \rangle = \langle h \rangle \times \langle a \rangle \times \langle t \rangle \cong \mathrm{C}_4 \times \mathrm{C}_4 \times \mathrm{C}_2$$

is abelian, it is enough to consider the action of elements $b$ and $g$ on these cyclic subgroups. We have

$$(ah)^2 = (aht)^2 = uz,\ \text{and } (ah)^b = (ah)uz^{\eta},\ (ah)^g = (ah)z^{\epsilon},$$
$$(aht)^b = (aht)uz^{\eta+1},\ (aht)^g = (aht)uz^{\epsilon+\zeta}.$$

If $\eta = 1$, then $(aht)^b = (aht)u$ and so $\langle aht \rangle$ is not normal in $G$. Then we must have $\langle ah \rangle \trianglelefteq G$ and so we get $\epsilon = 0$.

If $\eta = 0$, then $(ah)^b = (ah)u$ and so $\langle ah \rangle$ is not normal in $G$. Then we must have $\langle aht \rangle \trianglelefteq G$ which gives $\epsilon + \zeta = 1$.

(i) First assume that $g^2 \in \{u, z, uz\}$. If $\epsilon = 0$, then $h^g = h$ and so $g$ centralizes $\langle h \rangle \times \langle a \rangle \cong \mathrm{C}_4 \times \mathrm{C}_4$ and then there is an involution in $g\langle h, a \rangle$, a contradiction. Hence we must have $\epsilon = 1$. By the above, we get $\eta = 0$ and $\zeta = 0$. Hence we have in this case

$$h^g = hz,\ h^b = h,\ \text{and } t^g = tu.$$

If $g^2 = u$, then $[g, a] = 1$ implies that $ga$ is an involution, a contradiction. If $g^2 = z$, then $(tb)^2 = uz$ and

$$(gtb)^2 = z \cdot uz \cdot [tb, g] = u \cdot u = 1$$

so that $gtb$ is an involution, a contradiction. Hence we must have $g^2 = uz$. The structure of $G$ is determined as given in part (a) of our proposition. We check that there are no involutions in $G - K$. Indeed, assume that $gh^{\alpha}t^{\beta}a^{\gamma}b^{\delta}u'$ with $u' \in U = \mathrm{Z}(G)$ and $\alpha, \beta, \gamma, \delta \in \{0, 1\}$, is an involution. Then we get

$$1 = (gh^{\alpha}t^{\beta}a^{\gamma}b^{\delta}u')^2 = u^{1+\beta+\gamma+\delta+\gamma\delta}z^{1+\beta\delta},$$

and so $\beta = \delta = 1$, which gives $u = 1$, a contradiction.

It remains to prove that this special group $G$ of order $2^7$ satisfies our condition $(*)$. Let $X$ be a noncyclic and non-normal subgroup of order $\geq 2^3$ which has more than one involution. Then $|X \cap S| = 4$ and $X \cap U = \langle u' \rangle$, where $u'$ is a central involution and $S = \Omega_1(G) = U \times \langle t \rangle$. But all four involutions in $S - U$ are conjugate in $G$ noting that $\mathrm{C}_G(t) = \langle h \rangle \times \langle a \rangle \times \langle t \rangle$. Therefore we may assume that $t \in X$ and so we have $\Omega_1(X) = \langle t, u' \rangle = X \cap S$. We have $X \leq \mathrm{N}_G(\langle t, u' \rangle)$ and since $\Omega_1(X)$ contains at most two conjugates $t$ and $tu'$ of $t$, it follows that $X$ cannot cover $G/\mathrm{C}_G(t)$. Therefore we have either $X \leq \mathrm{C}_G(t)$ or $X \not\leq \mathrm{C}_G(t)$ in which case we must have one of the three possibilities: $X \leq \mathrm{C}_G(t)\langle b \rangle$ or $X \leq \mathrm{C}_G(t)\langle g \rangle$ or $X \leq \mathrm{C}_G(t)\langle bg \rangle$.

First assume that $X \not\leq \mathrm{C}_G(t)$ and then we have three subcases.

(1) If $X \leq \mathrm{C}_G(t)\langle b \rangle$, then $t^b = tz$ and so $u' = z$. If $x \in X - \mathrm{C}_G(t)$, then $x^2 \in U - \langle z \rangle$, which gives $X \geq U = G'$, a contradiction.

(2) Assume that $X \leq \mathrm{C}_G(t)\langle g \rangle$ and then we have $t^g = tu$ and so $u' = u$. If in this case $x \in X - \mathrm{C}_G(t)$, then we have

$$x = ga^{\alpha}t^{\beta}h^{\gamma}u'' \ (u'' \in U, \ \alpha, \ \beta, \ \gamma \in \{0,1\}) \text{ and then } x^2 = u^{1+\alpha+\beta}z,$$

which gives that $X \geq U = G'$, a contradiction.

(3) Suppose that $X \leq \mathrm{C}_G(t)\langle bg \rangle$ and then we have $t^{bg} = tuz$ and so $u' = uz$. If in this case $x \in X - \mathrm{C}_G(t)$, then we have

$$x = bga^{\alpha}t^{\beta}h^{\gamma}u'' \ (u'' \in U, \ \alpha, \ \beta, \ \gamma \in \{0,1\}) \text{ and then } x^2 = u^{\beta}z^{1+\beta}.$$

If $\beta = 0$, then $x^2 = z$. If $\beta = 1$, then $x^2 = u$. In any case we get $X \geq U = G'$, a contradiction.

Now assume $X \leq \mathrm{C}_G(t) = (\langle h \rangle \times \langle a \rangle) \times \langle t \rangle$ . Since $X \not\geq G' = U$, we have

$$X \in \{\langle hu^{\mu} \rangle \times \langle t \rangle, \ \langle az^{\nu} \rangle \times \langle t \rangle, \ \langle ahz^{\sigma} \rangle \times \langle t \rangle, \text{ where } \mu, \ \nu, \ \sigma \in \{0,1\}.\}$$

If $X = \langle hu^{\mu} \rangle \times \langle t \rangle$, then we have $\langle hu^{\mu} \rangle \trianglelefteq G$.

If $X = \langle az^{\nu} \rangle \times \langle t \rangle$, then $\langle az^{\nu} \rangle \trianglelefteq G$.

If $X = \langle ahz^{\sigma} \rangle \times \langle t \rangle$, then $\langle ahz^{\sigma}t \rangle \trianglelefteq G$ since

$$(ahz^{\sigma}t)^2 = uz, \ [ahz^{\sigma}t, b] = uz, \text{ and } [ahz^{\sigma}t, g] = uz.$$

We have proved that the condition $(*)$ is satisfied because for example $\langle h \rangle \times \langle t \rangle$ is not normal in $G$ (noting that $t^g = tu$).

(ii) Assume that $g^2 = h$. In this case we have $h \in \mathrm{Z}(G)$ and this gives $\epsilon = 0$ and $\eta = 0$. It follows (from the above) that $\zeta = 1$ and so we have $t^g = tuz$. The structure of $G$ is determined as given in part (b) of our proposition. For each $k \in K$ we have $(gk)^4 = g^4 = z$. Thus, all elements in $G - K$ are of order 8 and so we have $\Omega_1(G) = S = G' \times \langle t \rangle \cong \mathrm{E}_8$.

Conversely, let $X$ be a noncyclic and non-normal subgroup of order $\geq 2^3$ in $G$ which has more than one involution. Since four noncentral involutions in $S - U$ form a single conjugate class in $G$, it follows that we may assume $t \in X$. In addition, $X$ contains exactly one central involution $u' \in U$ so that we have $\Omega_1(X) = \langle t, u' \rangle$.

First suppose that $X \not\leq K$ so that $X$ contains elements of order 8 which implies that $z \in X$ and so we have $\Omega_1(X) = \langle t, z \rangle = H_0$. But then $H_0 \trianglelefteq G$, contrary to $t^g = tuz$.

We have proved that we must have $X \leq K$. Suppose that

$$X \nleq C_G(t) = (\langle h \rangle \times \langle a \rangle) \times \langle t \rangle \text{ and let } x \in X - C_G(t).$$

Then we have $t^x = tz$ and $x^2 \in U - \langle z \rangle$ and so $X \geq U = \langle u, z \rangle = G'$, a contradiction.

Thus, we must have $X \leq C_G(t)$ and since $\langle u, z \rangle \nleq X$, we get $X \cong C_4 \times C_2$. We have three subcases.

If $X = \langle hu^\mu \rangle \times \langle t \rangle$ ($\mu \in \{0, 1\}$), then we have $\langle hu^\mu \rangle \trianglelefteq G$.

If $X = \langle az^\nu \rangle \times \langle t \rangle$ ($\nu \in \{0, 1\}$), then $\langle az^\nu \rangle \trianglelefteq G$.

If $X = \langle ahz^\sigma \rangle \times \langle t \rangle$ ($\sigma \in \{0, 1\}$), then $\langle ahz^\sigma t \rangle \trianglelefteq G$ since

$$(ahz^\sigma t)^2 = uz, \ [ahz^\sigma t, b] = uz, \text{ and } [ahz^\sigma t, g] = uz.$$

We have proved that the condition $(*)$ is satisfied because for example $\langle h \rangle \times \langle t \rangle$ is not normal in $G$ (noting that $t^g = tuz$). Our proposition is completely proved. □

PROPOSITION 4.8. *Suppose that our group $G$ has the commutator group $G'$ of order $p$. Then we have $|G : Z(G)| = p^2$, $Z(G)$ is of rank 2, $\Omega_1(G) \nleq Z(G)$ and $Z(G)$ possesses cyclic subgroups of order $\geq p^2$ which do not contain $G'$.*

*Conversely, all these groups satisfy our condition $(*)$.*

PROOF. By Propositions 2 and 3, we must be in case (b1) of Proposition 3, where $H$ is abelian of type $(p^s, p)$, $s \geq 2$, $L = HU$ is abelian of type $(p^s, p, p)$ with $\mho_1(L) = \mho_1(H) \geq U_0 = H \cap U = \langle z \rangle \leq Z(G)$. By Proposition 3, $G'$ covers $U/\langle z \rangle$ and so we may set $G' = \langle u \rangle$, where $u \in U - \langle z \rangle$ so that $U \leq Z(G)$. We have $N_G(H_0) = N_G(H) = K$, where $H_0 = \Omega_1(H) \cong E_{p^2}$, $S = H_0 U \cong E_{p^3}$ and $S = \Omega_1(K)$. Note that $G/K \cong C_p$ acts transitively on $p$ subgroups of order $p^2$ in $S$ which contain $\langle z \rangle$ and which are distinct from $U$ and so we have $Z(G) \cap S = U$. Since $Z(G) \leq K$, it follows that $Z(G)$ is of rank 2 and $\Omega_1(G) \nleq Z(G)$. By Proposition 3, $G$ does not possess any non-normal subgroup isomorphic to $D_8$ and so by Proposition 7, $K/H_0$ is abelian. This implies that $K$ is abelian and so Lemma 1.1 in [1] gives at once that $|G : Z(G)| = p^2$. By Proposition 6, $H$ has exactly one $G$-invariant cyclic subgroup $\langle h \rangle \cong C_{p^s}$, $s \geq 2$, where $\langle h \rangle \cap U = \langle z \rangle$ and so $G' \nleq \langle h \rangle$. But we have

$$[G, \langle h \rangle] \leq \langle h \rangle \cap G' = \{1\} \text{ and so } \langle h \rangle \leq Z(G).$$

We have proved that $Z(G)$ contains cyclic subgroups of order $\geq p^2$ which do not contain $G'$. We have obtained the groups stated in our proposition.

Conversely, let $X$ be any noncyclic and non-normal subgroup of order $\geq p^3$ in a group $G$ described in our proposition. Since $G' \nleq X$, it follows that $X$ is abelian and so $X$ does not cover $G/Z(G)$ and $X \nleq Z(G)$. We get $|X : (X \cap Z(G))| = p$ and $X_0 = X \cap Z(G)$ is cyclic (since $E_{p^2} \cong \Omega_1(Z(G))$ contains $G'$). For any $g \in G$ with $X^g \neq X$, we see that $X \cap X^g = X_0$ is cyclic. Let $\langle k \rangle$ be a maximal cyclic subgroup of order $\geq p^2$ in $Z(G)$ which does not contain $G'$ and let $i$ be an element of order $p$ in $\Omega_1(G) - \mathrm{Z}(G)$. Then $\langle k \rangle \times \langle i \rangle$ does not contain $G'$ and so $\langle k \rangle \times \langle i \rangle$ is a maximal non-normal subgroup of $G$ of type $(p^r, p)$, $r \geq 2$. Indeed, if $\langle k \rangle \times \langle i \rangle \trianglelefteq G$, then

$$[G, (\langle k \rangle \times \langle i \rangle)] \leq (\langle k \rangle \times \langle i \rangle) \cap G' = \{1\}$$

and so $i \in \mathrm{Z}(G)$, a contradiction. The maximality of the cyclic subgroup $\langle k \rangle$ in $\mathrm{Z}(G)$ also shows that $\langle k \rangle \times \langle i \rangle$ is a maximal non-normal subgroup in $G$ and we are done. □

Proposition 4.9. *Suppose that we have the case (b1) of Proposition 3, where $H \cong \mathrm{M}_{p^n}$, $n \geq 3$ (if $p = 2$, then $n \geq 4$), $G$ is of class 3 and $G$ does not have non-normal subgroups isomorphic to $\mathrm{D}_8$ or such one which lead to the case (b2) of Proposition 3. Then we have $p = 2$, $G$ has the following subgroup of index 2:*

$$\mathrm{M}_{2^{n+1}} \cong \langle g, u \mid g^{2^n} = u^2 = 1,\ [g, u] = z = g^{2^{n-1}} \rangle, n \geq 4,$$

*and $G = \langle g, u \rangle \langle t \rangle$, where $t$ is an involution with $[g, t] = u$ and $[u, t] = 1$.*

*We have*

$$|G| = 2^{n+2},\ n \geq 4,$$

*with*

$$G' = \langle u, z \rangle \cong \mathrm{E}_4,\ [G, G'] = \langle z \rangle,\ \Omega_1(G) = \langle u, z, t \rangle \cong \mathrm{E}_8,$$
$$\mathrm{Z}(G) = \langle g^4 \rangle \cong \mathrm{C}_{2^{n-2}} \text{ and } \langle g^2, t \rangle \cong \mathrm{M}_{2^n}$$

*is a non-normal subgroup in $G$ with $\langle g^2 \rangle \trianglelefteq G$.*

*Conversely, these groups satisfy the condition $(*)$.*

Proof. By Proposition 4, $G' \leq U$ and so we have $G' = U \not\leq \mathrm{Z}(G)$. Also, Proposition 7 implies that $K/\Omega_1(H)$ is abelian, where $\Omega_1(H) \cong \mathrm{E}_{p^2}$ and so we have $K' = H' = \langle z \rangle \leq \mathrm{Z}(G)$. By Proposition 2, $K/H$ is cyclic of order $\geq p$. Finally, Proposition 3 also implies that $U = \Omega_1(\mathrm{Z}(L))$, where $L = HU \trianglelefteq G$. By Proposition 6, $H$ possesses a $G$-invariant cyclic subgroup $\langle h \rangle$ of index $p$ and there is an element $t$ of order $p$ in $H - \langle h \rangle$ so that $\langle [h, t] \rangle = \langle z \rangle$. For any $g \in G - K$, we have $t^g = tu'$ for some $u' \in U - \langle z \rangle$, where $G/K \cong \mathrm{C}_p$, $S = \langle t \rangle U \cong \mathrm{E}_{p^3}$ is normal in $G$ and $S = \Omega_1(K)$. It follows that all $p^2$ subgroups of order $p$ contained in $(S - U) \cup \{1\}$ form a single conjugate class in $G$.

Since $K' = H'$, we get $\mho_1(K) \leq \mathrm{Z}(K)$ and $K = H * C$, where $C = \mathrm{C}_K(H)$ and $H \cap C = \langle h^p \rangle \geq \langle z \rangle$. On the other hand, $K/H \cong C/\langle h^p \rangle$ is cyclic and so $C$ is abelian of rank 2 (because $\Omega_1(C) = U$), $C = \mathrm{Z}(K)$ and $K_1 = \langle h \rangle C$ is an abelian subgroup of index 2 in $K$ with $\Omega_1(K_1) = U$.

No element in $U - \langle z \rangle$ is a $p$-th power of an element in $G$. Indeed, if there is $x \in G$ such that $x^p \in U - \langle z \rangle$, then we consider the subgroup $U\langle x \rangle \trianglelefteq G$ of order $p^3$. Since $\langle z \rangle \leq \mathrm{Z}(G)$ and $x$ commutes with $x^p$, it follows that $U\langle x \rangle$ is abelian of type $(p^2, p)$. But then we get $\mho_1(U\langle x \rangle) = \langle x^p \rangle \trianglelefteq G$ and so $U \leq \mathrm{Z}(G)$, a contradiction.

Since $\Omega_1(K_1) = U$ and no element in $U - \langle z \rangle$ is a $p$-th power of an element in $K_1$, it follows that we have $K_1 = \langle k \rangle \times \langle u \rangle$ with $u \in U - \langle z \rangle$, $o(k) \geq p^{n-1}$ and $\langle k \rangle \geq \langle z \rangle$. Note that $\mho_1(K_1) = \langle k^p \rangle \leq \mathrm{Z}(K)$ and so $\langle k^p \rangle \times \langle u \rangle \leq \mathrm{Z}(K)$. Suppose that $K > L$ in which case we have $o(k) \geq p^n$. But then we get

$$\Omega_{n-1}(K_1) \leq \langle k^p \rangle \times \langle u \rangle \leq \mathrm{Z}(K)$$

and since $h \in \Omega_{n-1}(K_1)$, we get $h \in \mathrm{Z}(K)$, a contradiction.

We have proved that we have $K = L$. Since $\langle h \rangle \trianglelefteq G$, we get

$$[G, \langle h \rangle] \leq \langle h \rangle \cap G' = \langle h \rangle \cap U = \langle z \rangle \text{ and so } [G, \langle h \rangle] = \langle z \rangle.$$

It follows that $\mathrm{C}_G(h)$ covers $G/K$ and $\mathrm{C}_K(h) = \langle h \rangle U$. Hence, if $g \in \mathrm{C}_G(h) - K$, then we have $g^p \in \langle h \rangle U$ and note that $|\mathrm{C}_G(h) : \langle h \rangle| = p^2$. Thus, if $g^p \in (\langle h \rangle U) - \langle h \rangle$, then $\mathrm{C}_G(h)$ would be abelian and $\mathrm{C}_G(U) \geq \langle \mathrm{C}_G(h), t \rangle = G$, a contradiction. We have proved that $g^p \in \langle h \rangle$ and this gives that either $o(g) = p^n$ in which case we may set $g^p = h$ or we may assume that $o(g) = p$.

First assume that $p > 2$. Assume in addition that $g^p = h$. We have $[g, t] = u$ with some $u \in U - \langle z \rangle$ and $u^g = uz$, where $\langle g^{p^{n-1}} \rangle = \langle z \rangle \leq \mathrm{Z}(G)$. It follows that

$$[g^2, t] = [g, t]^g [g, t] = (uz)u = u^2 z$$

and we claim that we have $[g^i, t] = u^i z^{\binom{i}{2}}$ for all $i \geq 2$. Indeed, we get by induction:

$$\begin{aligned} &= [g^i g, t] = [g^i, t]^g [g, t] = (u^i z^{\binom{i}{2}})^g u = (uz)^i z^{\binom{i}{2}} u \\ &= u^{i+1} (z^{i + \binom{i}{2}}) = u^{i+1} z^{\binom{i+1}{2}}. \end{aligned}$$

This gives

$$[h, t] = [g^p, t] = u^p z^{\binom{p}{2}} = 1,$$

which is a contradiction.

We may assume in case $p > 2$ that $o(g) = p$, where $[g, h] = 1$, $h^{p^{n-2}} = z$, $n \geq 3$, and $z \in \mathrm{Z}(G)$. We may choose a suitable power $t^j$ in $\langle t \rangle$, $j \not\equiv 0 \pmod{p}$, so that we can set from the start that $[h, t] = z$. Then we have $[g, t] = u$ for some $u \in U - \langle z \rangle$ and we have $[g, u] = z^i$ with some $i \not\equiv 0 \pmod{p}$. We note that

$$H^* = \langle g \rangle \times \langle h \rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^{n-1}},\ n \geq 3,$$

is a maximal non-normal subgroup in $G$ since $|G : H^*| = p^2$ and $[g, t] = u \notin H^*$. Since $\Omega_1(H^*)U = \langle g, z \rangle U \cong \mathrm{S}(p^3)$, we are in case (b2) of Proposition 3 with respect to $H^*$. But this was excluded by our assumptions.

We have proved that we must have $p = 2$. Assume in addition that $o(g) = 2$. Then we have $\langle t, g \rangle \cong \mathrm{D}_8$ and $[h, t] = z \notin \langle t, g \rangle$ and so $\langle t, g \rangle$ is a non-normal subgroup isomorphic to $\mathrm{D}_8$, contrary to our assumptions. Thus we have in this case $g^2 = h$. Also we have

$$o(g) = 2^n,\ n \geq 4,\ [g, t] = u \in U - \langle z \rangle,\ z = g^{2^{n-1}},\ [g, u] = z$$

so that

$$\langle g, u\rangle \cong \mathrm{M}_{2^{n+1}}$$

is of index 2 in $G$. Also, $\langle h, t\rangle = \langle g^2, t\rangle \cong \mathrm{M}_{2^n}$ and $\langle h, t\rangle$ is not normal in $G$ since $[g, t] = u$. We have obtained the groups $G$ stated in our proposition.

We check that there are no involutions in $G - K$, where $K = L = \langle g^2, t\rangle \times \langle u\rangle$ and so we have $\Omega_1(G) = \langle u, z, t\rangle \cong \mathrm{E}_8$. Indeed, suppose that $gh^iu^jt^k$ is an element in $G - K$, where $g^2 = h$, $i$ is any integer and $j, k \in \{0, 1\}$. Then we get

$$x = (gh^iu^jt^k)^2 = h^{2i+1}u^kz^{j+ik} \text{ and so } \langle x\rangle \geq \langle z\rangle.$$

If $x = 1$, then $k = 0$ and so $h^{2i+1}z^j = 1$, a contradiction.

Conversely, let $X$ be any noncyclic and non-normal subgroup in $G$ of order $\geq 2^3$ containing more than one involution. Then we may assume (up to conjugacy in $G$) that $t \in X$ and so $\Omega_1(X) = \langle t, u'\rangle$ with some involution $u' \in U$. If $X \not\leq K$, then by the above calculation we see that $X$ contains $z$ and so we have $\Omega_1(X) = \langle t, z\rangle$ . But then for an element $x \in X - K$, we have $[x, t] \in U - \langle z\rangle$ and so in this case $X \geq G' = \langle u, z\rangle$, a contradiction. Hence we have $X \leq K$. Note that $\langle h\rangle \trianglelefteq G$ and $\langle hu\rangle \trianglelefteq G$. Since $|X| \geq 2^3$, it follows that $X \cap \langle h\rangle \neq \{1\}$ and so $z \in X$ and $\Omega_1(X) = \langle t, z\rangle$. Hence we have

$$X = \langle t\rangle(X \cap \langle h\rangle) \text{ or } X = \langle t\rangle(X \cap \langle hu\rangle).$$

But both $X \cap \langle h\rangle$ and $X \cap \langle hu\rangle$ are normal in $G$ and we are done. Our group $G$ satisfies the condition $(*)$. ∎

Proposition 4.10. *Suppose that we have the case (b1) of Proposition 3, where $H \cong \mathrm{M}_{p^3}$, $p > 2$, and $G$ is of class 2. Then we have the following possibilities:*

(a) *$G$ is a splitting extension of a cyclic normal subgroup $\langle g\rangle \cong \mathrm{C}_{p^m}$, $m \geq 3$, by*

$$\mathrm{M}_{p^3} \cong \langle h, t \mid h^{p^2} = t^p = 1,\ [h, t] = h^p = z\rangle,$$

*where $[g, h] = 1$ and $[g, t] = u$ with $\langle u\rangle = \Omega_1(\langle g\rangle)$.*

*We have*

$$|G| = p^{m+3},\ m \geq 3,\ \mathrm{E}_{p^2} \cong G' = \langle u, z\rangle,\ \mathrm{Z}(G) = \langle g^p\rangle \times \langle z\rangle \cong \mathrm{C}_{p^{m-1}} \times \mathrm{C}_p,$$

$$\langle g, h\rangle \cong \mathrm{C}_{p^m} \times \mathrm{C}_{p^2} \text{ is a unique abelian maximal subgroup of } G,$$

$$\Omega_1(G) = \langle u, z, t\rangle \cong \mathrm{E}_{p^3}$$

*and*

$$\langle h, t\rangle \cong \mathrm{M}_{p^3} \text{ and } \langle g, t\rangle \cong \mathrm{M}_{p^{m+1}}$$

*are non-normal subgroups in $G$ with $\langle h\rangle \trianglelefteq G$ and $\langle g\rangle \trianglelefteq G$.*

(b) *$G = (\langle g\rangle \times \langle h\rangle)\langle t\rangle$, where $\langle g\rangle \cong \langle h\rangle \cong \mathrm{C}_{p^2}$, $g^p = u$, $h^p = z$, $t$ centralizes $\langle u, z\rangle$,*

$$[h,t] = z,\ [g,t] = u^i z^j,\ i \not\equiv 0 \,(\mathrm{mod}\ p).$$

*Here $G$ is a special group of order $p^5$ with*

$$\mathrm{E}_{p^2} \cong G' = \langle u, z\rangle,\ \Omega_1(G) = \langle u, z, t\rangle \cong \mathrm{E}_{p^3}$$

*and $\langle h, t\rangle \cong \mathrm{M}_{p^3}$ is non-normal in $G$ with $\langle h\rangle \trianglelefteq G$.*

*Conversely, all groups in (a) and (b) satisfy our assumption $(*)$.*

Proof. By Proposition 6, $H$ possesses a $G$-invariant cyclic subgroup $\langle h\rangle \cong \mathrm{C}_{p^2}$ and then we may set:

$$H = \langle h, t \mid h^{p^2} = t^p = 1,\ [h,t] = h^p = z\rangle.$$

Since $K/\langle t, z\rangle$ is abelian, we have $K' = H' = \langle z\rangle$ and so $K = H * C$ with $H \cap C = \langle z\rangle$, where $C = \mathrm{C}_K(H)$. Also, $K/H \cong C/\langle z\rangle$ is cyclic of order $\geq p$ and so $C$ and $C_1 = \langle h\rangle C$ are abelian, where $\Omega_1(C_1) = U = G' \leq \mathrm{Z}(G)$ and $\mho_1(G) \leq \mathrm{Z}(G)$.

Since $[G, \langle h\rangle] = \langle z\rangle$, we have $G = \langle t\rangle \mathrm{C}_G(h)$. Set $S = U \times \langle t\rangle \cong \mathrm{E}_{p^3}$ and because $|G : \mathrm{C}_G(t)| = p^2$, all $p^2$ subgroups of order $p$ in $(S - U) \cup \{1\}$ form a single conjugate class in $G$. We have $\Omega_1(K) = S$ and we have in fact $\Omega_1(G) = S$. Indeed, if $g$ is an element of order $p$ in $G - K$, then we have

$$\langle g, t\rangle \cong \mathrm{S}(p^3) \text{ with } u' = [g,t] \in U - \langle z\rangle.$$

Because $\langle g, t\rangle \cap K = \langle t, u'\rangle \cong \mathrm{E}_{p^2}$, we have $z \notin \langle g, t\rangle$. But $[h,t] = z$ and so $\langle g, t\rangle$ is not normal in $G$, contrary to Proposition 1.

(i) First assume that $G/L$ is cyclic of order $\geq p^2$, where $L = HU$. Let $g \in \mathrm{C}_G(h) - K$ so that $\langle g\rangle$ covers $G/L$ and $\langle g^p\rangle \leq \mathrm{Z}(G)$ covers $K/H$ (which is cyclic of order $\geq p^2$). Hence we have $\Omega_1\langle g\rangle = \langle u\rangle$, where $o(g) = p^m$, $m \geq 3$, $u \in U - \langle z\rangle$ and $[g,t] = uz^i$ for some integer $i$ (mod $p$). We replace $g$ with $g' = h^{-i}g \in \mathrm{C}_G(h) - K$ so that we have

$$[g', t] = [h^{-i}g, t] = z^{-i}(uz^i) = u, \text{ where } (g')^{p^{m-1}} = (h^{-i}g)^{p^{m-1}} = g^{p^{m-1}}$$

with $\langle g^{p^{m-1}}\rangle = \langle u\rangle$. Thus, we may assume from the start that $[g,t] = u$ and so $\langle g, t\rangle \cong \mathrm{M}_{p^{m+1}}$ with $\langle g\rangle \trianglelefteq G$. But $[h,t] = z = h^p$ and so $z \notin \langle g, t\rangle$ and therefore $\langle g, t\rangle$ is a maximal non-normal subgroup in $G$. Our group $G$ is a splitting extension of $\langle g\rangle$ by $\langle h, t\rangle$ and so we have obtained the groups stated in part (a) of our proposition. We check that

$$\Omega_1(G) = S = \langle u, z, t\rangle \cong \mathrm{E}_{p^3}.$$

Indeed, let $1 \neq t' \in \langle t\rangle$ and suppose that $x = t'g^r h^s$ ($r, s$ are any integers) is an element of order $p$ in $G - \langle g, h\rangle$. Then we have

$$1 = (t'(g^r h^s))^p = (t')^p g^{pr} h^{ps} [g^r h^s, t']^{\binom{p}{2}} = g^{pr} h^{ps}.$$

Hence $r \equiv 0$ (mod $p^{m-1}$), $s \equiv 0$ (mod $p$) and so we get $x \in S$.

Conversely, let $X$ be a noncyclic and non-normal subgroup of order $\geq p^3$ in $G$. We may assume (up to conjugacy in $G$) that $t \in X$ and so $\Omega_1(X) = \langle t, u' \rangle \cong \mathrm{E}_{p^2}$, where $u'$ is an element of order $p$ in $U$. Set $X_0 = X \cap \langle g, h \rangle$ so that $X_0$ is cyclic and $\mathrm{N}_G(X_0) \geq \langle g, h \rangle \langle t \rangle = G$. Our condition $(*)$ is satisfied.

(ii) Assume that either $K = L$ or $K > L$ but $G/L$ is noncyclic so that $G/K$ splits over $K/L$. In any case we have $G = KG_0$ with $K \cap G_0 = L$ and $|G_0 : L| = p$. We have $\mathrm{C}_{G_0}(h) = (\langle h \rangle U)\langle g \rangle$ for some $g \in G_0 - K$. Since there are no elements of order $p$ in $G_0 - K$, we have $o(g) \geq p^2$ and so $g^p \in \mathrm{Z}(G) \cap L$ implies that $1 \neq g^p \in U$. If $g^p \in \langle z \rangle$, then $\langle g, h \rangle$ would contain elements of order $p$ in $G_0 - K$, a contradiction. Hence we must have $g^p = u \in U - \langle z \rangle$.

Suppose that $K > L$. Then there is an element $a \in C - U$ of order $p^2$ so that $a^p = u' \in U - \langle z \rangle$. Considering the subgroup $\langle h \rangle \times \langle g \rangle \cong \mathrm{C}_{p^2} \times \mathrm{C}_{p^2}$, each element in $\mho_1(\langle g, h \rangle) = \langle u, z \rangle$ is a $p$-th power of an element in $\langle g, h \rangle$. Thus, there is $y \in \langle g, h \rangle - K$ such that $y^p = (u')^{-1}$. But then we get:

$$(ay)^p = a^p y^p [y, a]^{\binom{p}{2}} = u'(u')^{-1} = 1,$$

and so $ay$ is an element of order $p$ in $G - K$, a contradiction. Hence we have $K = L$. In this case we have $[g, t] = u^i z^j$ with $i \not\equiv 0 \pmod p$ and so we have obtained a special group of order $p^5$ stated in part (b) of our proposition. We check that

$$\Omega_1(G) = S = \langle u, z, t \rangle \cong \mathrm{E}_{p^3}.$$

Indeed, let $1 \neq t' \in \langle t \rangle$ and suppose that $x = t' g^r h^s$ ($r, s$ are any integers) is an element of order $p$ in $G - \langle g, h \rangle$. Then we have

$$1 = (t'(g^r h^s))^p = (t')^p g^{pr} h^{ps} [g^r h^s, t']^{\binom{p}{2}} = g^{pr} h^{ps}.$$

Hence $r \equiv 0 \pmod p$, $s \equiv 0 \pmod p$ and so we get $x \in S$.

Conversely, let $X$ be a noncyclic and non-normal subgroup of order $p^3$ in $G$. We may assume (up to conjugacy in $G$) that $t \in X$ and so $\Omega_1(X) = \langle t, u' \rangle \cong \mathrm{E}_{p^2}$, where $u'$ is an element of order $p$ in $U$. Set $X_0 = X \cap \langle g, h \rangle$ so that $X_0$ is cyclic of order $p^2$ and $\mathrm{N}_G(X_0) \geq \langle g, h \rangle \langle t \rangle = G$. Our assumption $(*)$ is satisfied. □

PROPOSITION 4.11. *Suppose that we have the case (b1) of Proposition 3, where $H \cong \mathrm{M}_{p^n}$, $n \geq 4$, is a non-normal subgroup of maximal possible order in $G$ ( which is isomorphic to some $\mathrm{M}_{p^m}$, $m \geq 4$), $G$ is of class 2 and assume that $G$ does not have non-normal subgroups isomorphic to $\mathrm{D}_8$ or $\mathrm{M}_{p^3}$ with $p > 2$. Then we have the following possibilities:*

(a) $G = (\langle h \rangle \times \langle g \rangle)\langle t \rangle$, *where*

$$\langle h \rangle \cong \mathrm{C}_{p^{n-1}},\ n \geq 4,\ \langle g \rangle \cong \mathrm{C}_{p^m},\ m \geq 3,\ \langle t \rangle \cong \mathrm{C}_p,$$

$[h, t] = z$ with $\langle z \rangle = \Omega_1(\langle h \rangle)$, $[g, t] = z^i u$ with $\langle u \rangle = \Omega_1(\langle g \rangle)$, $i$ integer, *and $t$ centralizes $\langle u, z \rangle$.*

*Here we have* $|G| = p^{m+n}$, $m \geq 3$, $n \geq 4$,

$$\mathrm{E}_{p^2} \cong G' = \langle u, z\rangle \leq \mathrm{Z}(G),\ \Omega_1(G) = \langle u, z, t\rangle \cong \mathrm{E}_{p^3},$$

$\langle g, h\rangle \cong \mathrm{C}_{p^m} \times \mathrm{C}_{p^{n-1}}$ *is a unique abelian maximal subgroup of* $G$ *and* $\langle h, t\rangle \cong \mathrm{M}_{p^n}$ *is non-normal in* $G$ *with* $\langle h\rangle \trianglelefteq G$.

(b) $G = (\langle k\rangle \times \langle g\rangle)\langle t\rangle$, *where*

$$\langle g\rangle \cong \mathrm{C}_{p^n},\ n \geq 4,\ \langle k\rangle \cong \mathrm{C}_{p^m},\ 2 \leq m \leq n-2,\ \langle t\rangle \cong \mathrm{C}_p,$$

$$[k, t] = z \text{ with } \langle z\rangle = \Omega_1(\langle g\rangle),\ [g, t] = u \text{ with } \langle u\rangle = \Omega_1(\langle k\rangle),$$

*and* $t$ *centralizes* $\langle u, z\rangle$.

*Here we have* $|G| = p^{m+n+1}$, $n \geq 4$, $2 \leq m \leq n-2$,

$$\mathrm{E}_{p^2} \cong G' = \langle u, z\rangle \leq \mathrm{Z}(G),\ \Omega_1(G) = \langle u, z, t\rangle \cong \mathrm{E}_{p^3},$$

$\langle g, k\rangle \cong \mathrm{C}_{p^n} \times \mathrm{C}_{p^m}$ *is a unique abelian maximal subgroup of* $G$ *and* $\langle kg^p, t\rangle \cong \mathrm{M}_{p^n}$ *is non-normal in* $G$ *with* $\langle kg^p\rangle \trianglelefteq G$.

*Conversely, all groups in (a) and (b) satisfy our assumption* $(*)$.

Proof. By Proposition 4, $G' \leq U$ and so $G' = U \leq \mathrm{Z}(G)$ and $\mho_1(G) \leq \mathrm{Z}(G)$. Also, Proposition 7 implies that $K/\Omega_1(H)$ is abelian and so $K/H$ is cyclic (by Proposition 2), where $\Omega_1(H) \cong \mathrm{E}_{p^2}$ and therefore we have $K' = H' = \langle z\rangle \leq \mathrm{Z}(G)$. By Proposition 2, $K/H$ is cyclic of order $\geq p$. Finally, Proposition 3 also implies that $U = \Omega_1(\mathrm{Z}(L))$, where $L = HU \trianglelefteq G$. By Proposition 6, $H$ possesses a $G$-invariant cyclic subgroup $\langle h\rangle$ of index $p$ and there is an element $t$ of order $p$ in $H - \langle h\rangle$ so that $\langle [h, t]\rangle = \langle z\rangle$. For any $g \in G - K$, we have $t^g = tu'$ for some $u' \in U - \langle z\rangle$, where $G/K \cong \mathrm{C}_p$, $S = \langle t\rangle U \cong \mathrm{E}_{p^3}$ is normal in $G$ and $S = \Omega_1(K)$. It follows that all $p^2$ subgroups of order $p$ contained in $(S - U) \cup \{1\}$ form a single conjugate class in $G$.

Since $K' = H'$, we get $K = H * C$, where $C = \mathrm{C}_K(H)$ and $H \cap C = \langle h^p\rangle \geq \langle z\rangle$. On the other hand, $K/H \cong C/\langle h^p\rangle$ is cyclic and so $C$ is abelian of rank 2 (because $\Omega_1(C) = U$), $C = \mathrm{Z}(K)$ and $K_1 = \langle h\rangle C$ is an abelian subgroup of index 2 in $K$ with $\Omega_1(K_1) = U$. Since $\langle h\rangle \trianglelefteq G$, we get

$$[G, \langle h\rangle] \leq \langle h\rangle \cap G' = \langle h\rangle \cap U = \langle z\rangle \text{ and so } [G, \langle h\rangle] = \langle z\rangle.$$

It follows that $G = \langle t\rangle \mathrm{C}_G(h)$.

It is easy to see that there are no elements of order $p$ in $G - K$. Indeed, suppose that there is an element $i$ of order $p$ in $G - K$. Since $[i, t] = u \in U - \langle z\rangle$, we get that $D = \langle i, t\rangle$ is isomorphic to $\mathrm{D}_8$ in case $p = 2$ and $D$ is isomorphic to $\mathrm{S}(p^3)$ in case $p > 2$. On the other hand, $D \cap K = \langle t, u\rangle \cong \mathrm{E}_{p^2}$ and we have $[h, t] = z$, where $\langle z\rangle = \Omega_1(\langle h\rangle)$. Hence $D$ is not normal in $G$. But the case $D \cong \mathrm{D}_8$ is excluded by our assumptions and the case case $D \cong \mathrm{S}(p^3)$ is not possible by Proposition 1.

First we consider the case, where $G/L$ (being abelian as a factor-group of the abelian group $G/U$) is not cyclic of order $\geq p^2$. Hence we have either

$G/L \cong \mathrm{C}_p$ (i.e., $K = L$) or $G/L$ is abelian of type $(p^r, p)$, $r \geq 1$ (noting that $K/H$ is cyclic and so $K/L$ is cyclic). In any case, $G/L$ splits over $K/L$ and so $G$ has a normal subgroup $G_0$ such that $G = KG_0$ with $K \cap G_0 = L$ and $|G_0 : L| = p$. Since $[G_0, \langle h \rangle] = \langle z \rangle$, it follows that $\mathrm{C}_{G_0}(h)$ covers $G_0/L$, where $\mathrm{C}_L(h) = \langle h \rangle U$ and so $\mathrm{C}_{G_0}(h)$ is abelian of rank 2 with $\Omega_1(\mathrm{C}_{G_0}(h)) = U$ (noting that there are no elements of order $p$ in $G_0 - L$). If $\mathrm{C}_{G_0}(h)$ is abelian of type $(p^n, p)$, then there is an element $g_1 \in \mathrm{C}_{G_0}(h) - (\langle h \rangle U)$ such that $(g_1)^p = hu^i$ $(0 \leq i \leq p-1)$, where $u \in U - \langle z \rangle$. But then $(g_1)^p = hu^i \in \mathrm{Z}(G)$ and so $h \in \mathrm{Z}(G)$, a contradiction. Hence $\mathrm{C}_{G_0}(h)$ is of type $(p^{n-1}, p^2)$ and therefore there is an element $g \in \mathrm{C}_{G_0}(h) - K$ such that $g^p = u \in U - \langle z \rangle$. We may assume that $[t, g] = uz^i$ $(0 \leq i \leq p-1)$ (by replacing $t$ with a suitable power $\neq 1$ of $t$, if necessary) and then we choose an element $h' \in \langle h^p \rangle$ such that $(h')^p = z^i$ (noting that $o(h) = p^{n-1} \geq p^3$). Then we take the element $g' = h'g \in G_0 - K$ and compute:

$$(g')^p = (h')^p g^p = uz^i \text{ and } [t, g'] = [t, h'g] = [t, g] = uz^i.$$

Hence, in case $p = 2$ we have $\langle g', t \rangle \cong \mathrm{D}_8$ and then $g't$ is an involution in $G_0 - K$, a contradiction. If $p > 2$, then $\langle g', t \rangle \cong \mathrm{M}_{p^3}$. But we have

$$\langle g', t \rangle \cap K = \langle (g')^p, t \rangle \cong \mathrm{E}_{p^2} \text{ and } 1 \neq [h, t] \in \langle z \rangle \notin \langle g', t \rangle.$$

Thus, $\langle g', t \rangle$ is a non-normal subgroup in $G$ isomorphic to $\mathrm{M}_{p^3}$, $p > 2$, which was excluded by our assumptions.

We have proved that $G/L$ must be cyclic of order $\geq p^2$. Let $g \in \mathrm{C}_G(h) - K$ so that $\langle g \rangle$ covers $G/L$ and we have $g^p \in \mathrm{Z}(G)$. But $K/H$ is cyclic of order $\geq p^2$ and so $\langle g^p \rangle$ (covering $K/L$) covers $K/H$. Hence $\langle g \rangle$ covers $\mathrm{C}_G(h)/\langle h \rangle$ and so $A = \mathrm{C}_G(h)$ is abelian of rank 2 because $\Omega_1(A) = U$. We also have $|A/\langle h \rangle| \geq p^3$.

(i) First assume that $A$ splits over $\langle h \rangle$. Then we may set $A = \langle h \rangle \times \langle g \rangle$ with $o(g) = p^m$, $m \geq 3$, and $\Omega_1(\langle g \rangle) = \langle u \rangle$. We have $[h, t] = z$ with $\Omega_1(\langle h \rangle) = \langle z \rangle$ and $[g, t] = z^i u$, where $i$ is an integer (mod $p$).

We have obtained the groups stated in part (a) of our proposition. Now we check that we have

$$\Omega_1(G) = S = \langle u, z, t \rangle \cong \mathrm{E}_{p^3}.$$

Indeed, let $1 \neq t' \in \langle t \rangle$ and let $x = t'h^r g^s$ ($r, s$ are any integers) be an element of order $p$. Then we get in case $p > 2$:

$$1 = (t'(h^r g^s))^p = (t')^p h^{rp} g^{sp} [h^r g^s, t']^{\binom{p}{2}} = h^{rp} g^{sp}.$$

This implies

$$r \equiv 0 (\text{mod } p^{n-2}) \text{ and } s \equiv 0 (\text{mod } p^{m-1}) \text{ and so } x \in S.$$

Suppose that $p = 2$. Then we have :

$$1 = (t(h^r g^s))^2 = t^2 h^{2r} g^{2s} [h^r g^s, t] = h^{2r} g^{2s} z^r z^{is} u^s = (h^{2r} z^{r+is})(g^{2s} u^s).$$

This implies $r \equiv 0 \pmod{2^{n-3}}$ and $s \equiv 0 \pmod{2^{m-2}}$. Since $n \geq 4$ and $m \geq 3$, this gives $z^{r+is} = u^s = 1$ and then we get $h^{2r}g^{2s} = 1$ and therefore $r \equiv 0 \pmod{2^{n-2}}$, $s \equiv 0 \pmod{2^{m-1}}$ and $x \in S$.

(ii) Assume that $A$ does not split over $\langle h\rangle$. Then we have for an element $g \in A - K$ the following facts:

$$A = \langle h\rangle\langle g\rangle,\ \langle h\rangle \cap \langle g\rangle \geq \langle z\rangle \text{ and } o(h) = p^{n-1} < o(g).$$

Suppose that $o(g) > p^n$. Then we have $o(g^p) \geq p^n$ and $g^p \in \mathrm{Z}(G)$. In this case we get:

$$(hg^p)^{p^{n-1}} = g^{p^n} \geq \langle z\rangle,\ [t, hg^p] = [t, h],\ \langle [t, h]\rangle = \langle z\rangle,\ [t, g] = u' \in U - \langle z\rangle,$$

and this shows that $\langle t, hg^p\rangle \cong \mathrm{M}_{p^r}$, $r \geq n+1$, is non-normal in $G$, contrary to our maximality assumption.

We have proved that we must have $o(g) = p^n$. Also we get:

$$|A : \langle g\rangle| = |\langle h\rangle : (\langle h\rangle \cap \langle g\rangle)| = p^m \text{ with } m \leq n-2 \text{ since } \langle h\rangle \cap \langle g\rangle \geq \langle z\rangle.$$

If $m \leq 1$, then $A = \langle g\rangle U$ and so $\langle g^p\rangle U = A \cap K \leq \mathrm{Z}(G)$, contrary to $h \notin \mathrm{Z}(G)$. Hence we must have $m \geq 2$. Since $\langle g^p\rangle$ (of order $p^{n-1}$) splits in $A \cap K$, we get $A \cap K = \langle k\rangle \times \langle g^p\rangle$ and so we have $A = \langle k\rangle \times \langle g\rangle$ with $o(k) = p^m$, $2 \leq m \leq n-2$. Because $[A \cap K, \langle t\rangle] = \langle z\rangle$, we have $[k, t] = z$, where $\langle z\rangle = \Omega_1(\langle g\rangle)$.

Further we have $[g, t] = uz^i$ ($i$ some integer) with $\langle u\rangle = \Omega_1(\langle k\rangle)$. We may replace $g$ with $g' = k^{-i}g$ so that we have:

$$(g')^{p^{n-1}} = (k^{-i}g)^{p^{n-1}} = g^{p^{n-1}},$$
$$\langle g^{p^{n-1}}\rangle = \langle z\rangle,$$
$$[g', t] = [k^{-i}g, t] = z^{-i}(uz^i) = u,$$

and so writing again $g$ instead of $g'$, we can assume from the start that $[g, t] = u$. Also we have:

$$1 \neq (kg^p)^{p^{n-2}} = g^{p^{n-1}} \geq \langle z\rangle, \quad [kg^p, t] = z,\ [g, t] = u,$$

and so $\langle kg^p, t\rangle \cong \mathrm{M}_{p^n}$ is non-normal in $G$ with $\langle kg^p\rangle \trianglelefteq G$. We have obtained the groups stated in part (b) of our proposition.

Now we check that we have

$$\Omega_1(G) = S = \langle u, z, t\rangle \cong \mathrm{E}_{p^3}.$$

Indeed, let $1 \neq t' \in \langle t\rangle$ and let $x = t'k^rg^s$ ($r, s$ are any integers) be an element of order $p$. Then we get in case $p > 2$:

$$1 = (t'(k^rg^s))^p = (t')^p k^{rp} g^{sp} [k^rg^s, t']^{\binom{p}{2}} = k^{rp}g^{sp}.$$

This implies

$$r \equiv 0 (\mathrm{mod}\ p^{m-1}) \text{ and } s \equiv 0 (\mathrm{mod}\ p^{n-1}) \text{ and so } x \in S.$$

Suppose that $p = 2$. Then we have :

$$1 = (t(k^r g^s))^2 = t^2 k^{2r} g^{2s} [k^r g^s, t] = k^{2r} g^{2s} z^r u^s = (k^{2r} u^s)(g^{2s} z^r).$$

This implies $s \equiv 0 \pmod{2^{n-2}}$ and so $1 = k^{2r}(g^{2s} z^r)$ and $r \equiv 0 \pmod{2^{m-1}}$ which gives $g^{2s} = 1$ and $s \equiv 0 \pmod{2^{n-1}}$. Hence we get again $x \in S$.

It remains to prove in case of both groups in parts (a) and (b) of our proposition that the assumption $(*)$ is satisfied. Indeed, let $A$ be a unique abelian maximal subgroup of $G$, where $t \in G - A$ (since $\Omega_1(A) = U = G'$). Let $X$ be a noncyclic and non-normal subgroup of order $\geq p^3$ in $G$ which in case $p = 2$ has more than one involution. Since $X \not\geq G'$ and all noncentral subgroups of order $p$ form a single conjugate class in $G$ (with a representative $\langle t \rangle$), we may assume that $t \in X$. We set $X_0 = X \cap A$, where $X_0$ is cyclic since

$$\Omega_1(X) = \langle t, u' \rangle \text{ for some } 1 \neq u' \in G' = \Omega_1(A).$$

But then we have $N_G(X_0) \geq \langle A, t \rangle = G$ and we are done. Our proposition is completely proved. □

In the next proposition we collect all the remaining $p$-groups satisfying the condition $(*)$.

Proposition 4.12. *Suppose that $G$ is a $p$-group satisfying $(*)$ which is not a 2-group of maximal class, $G$ has no non-normal subgroups isomorphic to $D_8$ or $M_{p^n}$, $|G'| = p^2$, $K/\Omega_1(H)$ is abelian for each abelian noncyclic maximal non-normal subgroup $H$ of order $\geq p^3$ in $G$, and $G$ has no non-normal abelian subgroups which lead to the case (b2) of Proposition 3. Then we have the following possibilities.*

(a) *$G$ has a maximal subgroup*

$$M_{p^{s+2}} \cong \langle g, u \mid g^{p^{s+1}} = u^p = 1,\ [u, g] = z,\ \langle z \rangle = \Omega_1(\langle g \rangle) \rangle, p > 2,\ s \geq 2,$$

*$G = \langle g, u \rangle \langle t \rangle$, where $o(t) = p$, $[g, t] = u$ and $[u, t] = 1$.*

*These groups are actually $A_2$-groups defined in Proposition 71.3(i) in [2], where $\langle g^p, t \rangle \cong C_{p^s} \times C_p$ is non-normal in $G$ with $\langle g^p \rangle \trianglelefteq G$.*

(b) *$G$ is a special group of order $2^5$ with a unique abelian maximal subgroup*

$$K = \langle h \rangle \times \langle u \rangle \times \langle t \rangle,\ \langle h \rangle \cong C_4,\ h^2 = z,\ \langle u \rangle \cong \langle t \rangle \cong C_2,$$

*and $G = K\langle g \rangle$, where $g^2 = z$, $[g, h] = z$, $[g, u] = 1$, $[g, t] = u$.*

*Here we have $G' = \langle u, z \rangle \cong E_4$, $\Omega_1(G) = \langle u, z, t \rangle \cong E_8$ and $\langle h, t \rangle \cong C_4 \times C_2$ is a non-normal subgroup in $G$ with $\langle h \rangle \trianglelefteq G$.*

(c) *$G$ has a maximal subgroup*

$$\langle h, g \mid h^{p^s} = g^{p^r} = 1,\ h^{p^{s-1}} = z,\ [g, h] = z \rangle, s \geq 4,\ 3 \leq r < s$$

*and*

$$G = \langle h, g \rangle \langle t \rangle \text{ with } t^p = 1,\ [h, t] = 1,\ [g, t] = uz^i,\ i \not\equiv 0 \pmod p,$$
$$\langle u \rangle = \Omega_1(\langle g \rangle),\ [u, t] = 1.$$

*We have* $|G| = p^{r+s+1}$, $\mathrm{E}_{p^2} \cong G' = \langle u, z\rangle \le \mathrm{Z}(G)$, $\Omega_1(G) = \langle u, z, t\rangle \cong \mathrm{E}_{p^3}$,

$$K = \langle t, h, g^p\rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^s} \times \mathrm{C}_{p^{r-1}}$$

*is a unique abelian maximal subgroup in* $G$ *and*

$$\langle h, t\rangle \cong \mathrm{C}_{p^s} \times \mathrm{C}_p$$

*is an abelian maximal non-normal subgroup in* $G$ *with* $\langle h\rangle \trianglelefteq G$.

(d) $G$ *is a* 2*-group which possesses a normal subgroup* $G_0 = L\langle g\rangle$, *where*

$$L = \langle h\rangle \times \langle u\rangle \times \langle t\rangle,\ \langle h\rangle \cong \mathrm{C}_4,\ h^2 = z,\ \langle u\rangle \cong \langle t\rangle \cong \mathrm{C}_2,$$

$$g^2 = z,\ [g, h] = z,\ [g, u] = 1,\ [g, t] = u,$$

*which is a special group of order* $2^5$ *with* $G_0' = \langle u, z\rangle \cong \mathrm{E}_4$. *Then we have the following possibilities for* $G = G_0\langle k\rangle$:

(d1) $k^4 = u$, $[k, g] = 1$, $[k, t] = z$, $[k, h] = z$, *and here we have* $|G| = 2^7$, $exp(G) = 8$ *and* $\mathrm{Z}(G) = G'\langle k^2\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$.

(d2) $k^2 = u$, $[k, g] = [k, t] = [k, h] = 1$, *and here we have* $|G| = 2^6$, $exp(G) = 4$ *and* $\mathrm{Z}(G) = G'\langle k\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$.

(d3) $k^2 = uz$, $[k, g] = [k, h] = 1$, $[k, t] = z$ *and here* $G$ *is a special group of order* $2^6$ *with* $\mathrm{Z}(G) = \langle u, z\rangle \cong \mathrm{E}_4$.

*In all three cases we have* $\mathrm{E}_4 \cong G' = \langle u, z\rangle \le \mathrm{Z}(G)$, $\Omega_1(G) = G' \times \langle t\rangle \cong \mathrm{E}_8$ *and* $\langle h, t\rangle \cong \mathrm{C}_4 \times \mathrm{C}_2$ *is an abelian maximal non-normal subgroup in* $G$ *with* $\langle h\rangle \trianglelefteq G$.

(e) *We have* $G = (\langle a\rangle \times \langle b\rangle)\langle t\rangle$, *where*

$$\langle a\rangle \cong \mathrm{C}_{p^{s+1}},\ \langle b\rangle \cong \mathrm{C}_{p^r},\ \langle t\rangle \cong \mathrm{C}_p,\ s \ge 2,\ 2 \le r \le s+1,$$

$$z = a^{p^s},\ u = b^{p^{r-1}},\ [b, t] = z,\ [a, t] = u^i z^j,\ i \not\equiv 0 (\mathrm{mod}\ p),\ [z, t] = [u, t] = 1.$$

*If* $r = s+1$, *then* $j \not\equiv \xi - i\xi^{-1} (\mathrm{mod}\ p)$ *for all integers* $\xi \not\equiv 0 (\mathrm{mod}\ p)$.

*We have here* $|G| = p^{r+s+2}$, $G' = \langle u, z\rangle \cong \mathrm{E}_{p^2}$, $\Omega_1(G) = G' \times \langle t\rangle \cong \mathrm{E}_{p^3}$, $G$ *is of class* 2 *with*

$$\Phi(G) = \mho_1(G) = \mathrm{Z}(G) = \langle a^p\rangle \times \langle b^p\rangle \cong \mathrm{C}_{p^s} \times \mathrm{C}_{p^{r-1}}.$$

*Finally,* $\langle a^p\rangle \times \langle t\rangle \cong \mathrm{C}_{p^s} \times \mathrm{C}_p$ *is a maximal non-normal subgroup of* $G$ *with* $\langle a^p\rangle \trianglelefteq G$.

*Conversely, all the above groups from (a) to (e) satisfy our condition* $(*)$.

Proof. Let $G$ be a $p$-group satisfying all assumptions of this proposition. Let $H$ be a maximal non-normal subgroup of a maximal possible order in $G$ which is abelian of type $(p^s, p)$, $s \ge 2$.

Set $U_0 = U \cap H = \langle z\rangle \le \mathrm{Z}(G)$ and $H_0 = \Omega_1(H) = \langle t, z\rangle$ so that $S = H_0U \cong \mathrm{E}_{p^3}$, $S = \Omega_1(K) = \Omega_1(L)$ and $L$ is abelian with $\mho_1(L) = \mho_1(H) \ge U_0$. Also, $K/H_0$ is abelian and since $G' \le U$ (Proposition 4), we have here $G' = U$ (see Proposition 3(b1)) because by our assumption $|G'| = p^2$ and so $K' \le \langle z\rangle$ and $G/L$ is abelian. By Proposition 6, $H$ possesses a $G$-invariant cyclic subgroup $\langle h\rangle \cong C_{p^s}$ which contains $z$ and so we have $H = \langle h\rangle \times \langle t\rangle$. Also, $N_G(H_0) = K$ and by Proposition 2, $K/H$ is cyclic of order $\geq p$. By Proposition 3, for each $g \in G - K$, we have $[g,t] = u \in U - \langle z\rangle$, where $|G/K| = p$. We shall use all these facts in the proof of this proposition.

First we prove that there are no elements of order $p$ in $G - K$ and so we have $\Omega_1(G) = S = G' \times \langle t\rangle \cong E_{p^3}$. Indeed, let $i$ be an element of order $p$ in $G - K$. We have $[i,t] = u' \in U - \langle z\rangle$ and so $\langle h,i\rangle$ is not normal in $G$ because $\langle h,i\rangle \cap K = \langle h\rangle$. It follows that

$$H^* = \langle h,i\rangle = \langle h\rangle \times \langle i\rangle$$

is abelian and the fact that $|H^*| = |H|$ together with the maximality of $|H|$ implies that $H^*$ is another maximal non-normal subgroup in $G$ of type $(p^s,p)$. Since $H^* \cap U = \langle z\rangle \leq Z(G)$, it follows that $H^*U$ is the unique normal subgroup of $G$ which contains $H^*$ with $|(H^*U) : H^*| = p$. By our assumptions, we have that $\Omega_1(H^*) = \langle z,i\rangle$ centralizes $U$. Thus $C_G(U) \geq L\langle i\rangle$ and since $u'$ commutes with $i$ and $t$, we get together with $[i,t] = u'$ that $D = \langle i,t\rangle \cong D_8$ if $p = 2$ and $D = \langle i,t\rangle \cong S(p^3)$ if $p > 2$ and in any case we get $D' = Z(D) = \langle u'\rangle$.

If $D \cong D_8$, then our assumptions imply $D \trianglelefteq G$ and if $D \cong S(p^3)$, then Proposition 1 gives that $D \trianglelefteq G$. Hence in any case we have $D \trianglelefteq G$ and so $D' = \langle u'\rangle \leq Z(G)$. This gives that $G' = U = \langle z\rangle \times \langle u'\rangle \leq Z(G)$ and therefore $G$ is of class 2 with $\mho_1(G) \leq Z(G)$. Since $D \cap G' = \langle u'\rangle$, it follows that no element in $G$ induces an outer automorphism on $D$. We get $G = D * C$, where $C = C_G(D)$ and $C \cap D = \langle u'\rangle$.

Note that $\langle h\rangle U \leq C$ and $C_G(t) = C \times \langle t\rangle$, which together with the fact that no element in $G - K$ centralizes $t$ implies that $C_G(t) = K$. Also, we have $|G : C_G(i)| = p$ and so if $K$ would be abelian, then $C = C_K(i)$ is abelian and then $G' = D' = \langle u'\rangle$ is of order $p$, a contradiction. Hence $K$ is nonabelian and so $K' = \langle z\rangle = C'$ since $K = C \times \langle t\rangle$. If $\langle h\rangle \leq Z(K)$, then $L \leq Z(K)$ and so the fact that $K/L$ is cyclic gives that $K$ is abelian, a contradiction. Hence we get $\langle h\rangle \not\leq Z(K)$ and so, in particular, we have $K > L$.

We have $K = C_K(i) \times \langle t\rangle$ and since $K/H$ is cyclic of order $\geq p^2$ and

$$K/H \cong C_K(i)/C_H(i) = C_K(i)/\langle h\rangle,$$

we may choose $k \in C_K(i) = C$ so that $\langle k\rangle$ covers $C_K(i)/\langle h\rangle$ and $[h,k] = z$. Since

$$C = C_K(i) = \langle h,k\rangle \text{ with } [h,k] = z,\ \langle z\rangle = \langle h\rangle \cap U \text{ and } U = \Omega_1(C) \leq Z(G)$$

and noting that $\Omega_1(K) = U \times \langle t\rangle \cong E_{p^3}$, it follows that $C$ is metacyclic minimal nonabelian without a cyclic subgroup of index $p$. Hence we may set

$$C = \langle a,b \mid a^{p^\alpha} = b^{p^\beta} = 1,\ [a,b] = z = a^{p^{\alpha-1}}\rangle,$$

where $\alpha \geq 2$, $\beta \geq 2$ and $b^{p^{\beta-1}} = u \in U - \langle z\rangle$. Also we know that we have $G = C * \langle i,t\rangle$ with $C \cap \langle i,t\rangle = \langle u'\rangle,\ u' \in U - \langle z\rangle$ and $D = \langle i,t\rangle \cong D_8$ or $S(p^3)$.

We consider the subgroup $H_1 = \langle b \rangle \times \langle i \rangle \cong \mathrm{C}_{p^\beta} \times \mathrm{C}_p$, $\beta \geq 2$. Since $H_1 \cap C = \langle b \rangle$ and $[a, b] = z \notin H_1$, it follows that $H_1$ is non-normal in $G$. Suppose that $H_1$ is not a maximal non-normal subgroup in $G$. Then there is an element $b' \in G$ such that $b = i^\gamma (b')^p$, where $\gamma$ is an integer mod $p$ and $(b')^p \in \mho_1(G) \leq \mathrm{Z}(G)$. Then we get

$$[a, b] = [a, i^\gamma (b')^p] = [a, i]^\gamma = 1,$$

a contradiction. Hence $H_1$ is a maximal non-normal subgroup in $G$. By Proposition 6, $H_1$ possesses a $G$-invariant subgroup $\langle bi^\delta \rangle$ of index $p$, where $\delta$ is an integer mod $p$ and $\Omega_1(\langle bi^\delta \rangle) = \langle u \rangle$. On the other hand, we have $[a, bi^\delta] = [a, b] = z$, a contradiction. We have proved that there are no elements of order $p$ in $G - K$.

Now assume that $G$ is of class 3. In that case no element in $U - \langle z \rangle$ is a $p$-th power of an element in $G$. Indeed, if there is $x \in G$ such that $x^p \in U - \langle z \rangle$, then we consider the subgroup $U\langle x \rangle \trianglelefteq G$ of order $p^3$. Since $\langle z \rangle \leq \mathrm{Z}(G)$ and $x$ commutes with $x^p$, it follows that $U\langle x \rangle$ is abelian of type $(p^2, p)$. But then we get $\mho_1(U\langle x \rangle) = \langle x^p \rangle$ is normal in $G$ and so $G' = U \leq \mathrm{Z}(G)$, a contradiction.

Note that $G/K \cong \mathrm{C}_p$ acts transitively on $p$ subgroups of order $p^2$ in $S = U \times \langle t \rangle$ which contain $\langle z \rangle$ and which are distinct from $U$. Assume for a moment that $t \notin \mathrm{Z}(K)$. Then we have $K' = \langle z \rangle$ and $K > L$. Let $k \in K - \mathrm{C}_K(t)$ so that $\langle k \rangle$ covers $K/H$. Suppose that $\langle k' \rangle = \Omega_1(\langle k \rangle) \not\leq U$. Then we have $k' \in \mathrm{Z}(K)$ and if $U \not\leq \mathrm{Z}(K)$, then $\Omega_1(\mathrm{Z}(K)) = \langle z, k' \rangle \trianglelefteq G$, a contradiction. Hence $U \leq \mathrm{Z}(K)$ and so $S \leq \mathrm{Z}(K)$ which implies that $t \in \mathrm{Z}(K)$, a contradiction. Thus we have $\Omega_1(\langle k \rangle) \leq U$ and so $\Omega_1(\langle k \rangle) = \langle z \rangle$ and $o(k) \geq p^3$. Since $\langle [k, t] \rangle = \langle z \rangle$, we have

$$\langle k, t \rangle \cong \mathrm{M}_{p^m}, \ m \geq 4.$$

On the other hand, for an element $g \in G - K$ we have $[g, t] = u' \in U - \langle z \rangle$ and so $\langle k, t \rangle$ is not normal in $G$, contrary to our assumptions. We have proved that $t \in \mathrm{Z}(K)$ and so we have $\mathrm{C}_G(t) = K$.

If $U \not\leq \mathrm{Z}(K)$, then $H_0 = \Omega_1(\mathrm{Z}(K)) \trianglelefteq G$, a contradiction. Hence we have $U \leq \mathrm{Z}(K)$ and so $S = \Omega_1(\mathrm{Z}(K)) = \Omega_1(G)$. Let $x \in G - K$ so that we have $\mathrm{C}_U(x) = \langle z \rangle$ and therefore, by the above, $\mathrm{C}_S(x) = \langle z \rangle$. In particular, we get $p > 2$ and $\Omega_1(\langle x \rangle) = \langle z \rangle$.

Suppose that for some $y \in K$ we have $y^p \in S - U$. Then we have $\langle y \rangle S \trianglelefteq G$ and

$$\mho_1(\langle y \rangle S) = \langle y^p \rangle \leq \mathrm{Z}(G),$$

a contradiction. Hence for each element $x \in G$ of composite order, the socle $\Omega_1(\langle x \rangle)$ is equal $\langle z \rangle$.

Assume that $\langle h \rangle \not\leq \mathrm{Z}(K)$ so that we have $K > L$. Let $k \in K$ be such that $\langle k \rangle$ covers $K/H$ and since $\Omega_1(\langle k \rangle) = \langle z \rangle$, we get $o(k) \geq p^3$. It follows that $\langle h, k \rangle$ is a splitting metacyclic minimal nonabelian subgroup with $\langle [h, k] \rangle =$

$\langle z\rangle$. We may set

$$\langle h,k\rangle = \langle a,b \mid a^{p^{\alpha}} = b^{p^{\beta}} = 1,\ [a,b] = z = a^{p^{\alpha-1}}\rangle,$$

where $\alpha \geq 3$ and $\beta \geq 1$. By the previous paragraph, we must have $\beta = 1$ and then $b \in \mathrm{Z}(K)$, a contradiction.

We have proved that $h \in \mathrm{Z}(K)$ and so $L \leq \mathrm{Z}(K)$ which together with the fact that $K/L$ is cyclic implies that $K$ is abelian. Hence $K$ is abelian of rank 3 and therefore we may set

$$K = \langle a\rangle \times \langle u\rangle \times \langle t\rangle \text{ with } \Omega_1(\langle a\rangle) = \langle z\rangle,\ o(a) \geq p^s, \text{ and } \langle z,u\rangle = U.$$

Since $[t,g] \in U - \langle z\rangle$ for each element $g \in G - K$, we have that $\langle a\rangle \times \langle t\rangle$ is non-normal in $G$ which together with the maximality of $|H|$ gives $o(a) = p^s$ and so we have $K = L$.

Let $g \in G - K$. Since $\mathrm{C}_S(g) = \langle z\rangle$, it follows that $\mathrm{C}_K(g)$ is cyclic. By Lemma 1.1 in [1], $\mathrm{C}_K(g) = \langle h'\rangle$ covers $K/S$ and so $\langle h'\rangle \cong \mathrm{C}_{p^s}$ and $\langle h'\rangle = \mathrm{Z}(G)$ so that $g^p \in \langle h'\rangle$. But there are no elements of order $p$ in $G - K$ and so $\langle g,h'\rangle = \langle g\rangle$ is cyclic of order $p^{s+1}$. We may assume without loss of generality that $g^p = h$. Then we may set $[g,t] = u \in U - \langle z\rangle$ and $[u,g] = z$, where $\langle z\rangle = \Omega_1(\langle g\rangle)$. The group $G$ has a maximal subgroup

$$\mathrm{M}_{p^{s+2}} \cong \langle g,u \mid g^{p^{s+1}} = u^p = 1,\ [u,g] = z,\ \langle z\rangle = \Omega_1(\langle g\rangle)\rangle,$$

where $p > 2$, $s \geq 2$ and $G = \langle g,u\rangle\langle t\rangle$ with $o(t) = p$, $[g,t] = u$ and $[u,t] = 1$. We have obtained the groups stated in part (a) of our proposition. It turns out that these groups are actually $\mathrm{A}_2$-groups which are defined in Proposition 71.3(i) in [2]. Conversely, it is easy to check that these groups satisfy our condition $(*)$.

From now on we may assume that $G$ is of class 2. Since $G' = U \cong \mathrm{E}_{p^2}$, we also have $\mho_1(G) \leq \mathrm{Z}(G)$. Also we have $\Omega_1(\mathrm{Z}(G)) = U$ and so no element in $S - U$ is a $p$-th power of any element in $G$.

(i) Assume that $K = L$. In this case Lemma 1.1 in [1] gives that $|G/\mathrm{Z}(G)| = p^3$. We have $\langle h\rangle \trianglelefteq G$ but $\langle h\rangle \not\leq \mathrm{Z}(G)$ and so we have $\mathrm{Z}(G) = U\langle h^p\rangle$. Hence for each $g \in G - K$, we get $1 \neq g^p \in U\langle h^p\rangle$.

(i1) First suppose that $1 \neq g^p \in \langle h^p\rangle \geq \langle z\rangle$. Since there are no elements of order $p$ in $\langle g,h\rangle - \langle h\rangle$ and $\langle g,h\rangle$ is nonabelian (because $\langle h\rangle \not\leq \mathrm{Z}(G)$) with $\Omega_1(\langle g,h\rangle) = \langle z\rangle$, it follows that we have $p = 2$ and $\langle g,h\rangle \cong \mathrm{Q}_8$. Hence $\langle h\rangle \cong \mathrm{C}_4$, $g^2 = z$, $[g,h] = z$ and $[g,t] = u \in U - \langle z\rangle$. We have obtained the special group of order $2^5$ stated in part (b) of our proposition and this group satisfies our condition $(*)$.

(i1) Now we assume that $g^p \in (U\langle h^p\rangle) - \langle h^p\rangle$ so that we may set $g^p = uh'$, where $u \in U - \langle z\rangle$, $\langle z\rangle = \Omega_1(\langle h\rangle)$ and $h' \in \langle h^p\rangle$. Let $h_0$ be an element in $\langle h\rangle$ such that $h_0^p = (h')^{-1}$. Then we replace $g$ with $gh_0 \in G - K$ and we compute

$$(gh_0)^p = g^p h_0^p [h_0,g]^{\binom{p}{2}} = (uh')(h')^{-1}z' = uz' \in U - \langle z\rangle,$$

where

$$[h_0, g]^{\binom{p}{2}} = z' \in \langle z \rangle.$$

It follows that in this case we may choose from the start an element $g \in G - K$ so that $g^p = u \in U - \langle z \rangle$. Then we have $[g, t] = uz^i$ for some integer $i$ mod $p$ ( where we have replaced $t$ with a suitable power $t^j$ ($j \not\equiv 0$ mod $p$ ). Let $h^* \in \langle h \rangle$ be such that $(h^*)^p = z^i$.

Assume that either $p > 2$ or $p = 2$ and $s \geq 3$ (where in the last case we have $[h^*, g] = 1$). Then we consider the subgroup $\langle g', t \rangle$, where $g' = gh^* \in G - K$. We have

$$(g')^p = g^p (h^*)^p [h^*, g]^{\binom{p}{2}} = uz^i = [g, t] = [gh^*, t] = [g', t],$$

and so we get $\langle g', t \rangle \cong \mathrm{D}_8$ if $p = 2$ and $\langle g', t \rangle \cong \mathrm{M}_{p^3}$ if $p > 2$. On the other hand, $1 \neq [h, g'] \in \langle z \rangle$ and so $\langle g', t \rangle$ is non-normal in $G$, contrary to our assumptions.

We have proved that we must have $p = 2$ and $s = 2$ so that we have $\langle h \rangle \cong \mathrm{C}_4$ and $G$ is a special group of order $2^5$ with $g^2 = u \in U - \langle z \rangle$, $h^2 = z$, $[g, h] = z$ and $[g, t] = uz^i$, $i = 0, 1$. However, if $i = 0$, then $\langle g, t \rangle \cong \mathrm{D}_8$ is non-normal in $G$, a contradiction. Thus we have $i = 1$ and so $[g, t] = uz$. The structure of $G$ is uniquely determined.

We claim that the special 2-group obtained in the previous paragraph is in fact isomorphic to the special group of order $2^5$ from part (i1) of our proof. Indeed, set $g' = gt$ and $u' = uz$. Then we have

$$(g')^2 = (gt)^2 = u(uz) = z = h^2,$$
$$[g', h] = [gt, h] = z,$$
$$[g', t] = [gt, t] = uz = u'.$$

In addition we have $[g', u'] = [h, t] = 1$ and so writing again $g, u$ instead of $g', u'$, respectively, we see that we have obtained the relations for the special group of order $2^5$ defined in ($i$1).

From now on we shall always assume that $K > L$.

(ii) Suppose that $G/L$ is cyclic of order $\geq p^2$. Let $g \in G - K$ so that $\langle g \rangle$ covers $G/L$. But $g^p \in \mathrm{Z}(G)$ and $\langle g^p \rangle$ covers $K/L \neq \{1\}$. Since $K/H$ is cyclic of order $\geq p^2$, it follows that $\langle g^p \rangle$ covers $K/H$ and so $K = H\langle g^p \rangle$ is abelian. Since $G' = U \cong \mathrm{E}_{p^2}$, Lemma 1.1 in [1] implies that $|G : \mathrm{Z}(G)| = p^3$. On the other hand, $\langle h^p, g^p \rangle \leq \mathrm{Z}(G)$ and $|K_1 : \langle h^p, g^p \rangle| = p$, where $K_1 = \langle h, g^p \rangle$ and $K = \langle t \rangle \times K_1$ is of rank 3. It follows that $\mathrm{Z}(G) = \langle h^p, g^p \rangle$. In particular, (since $U \leq \mathrm{Z}(G)$) we must have $U \leq \langle h^p, g^p \rangle$ so that $\Omega_1(K_1) = U$ and $h \notin \mathrm{Z}(G)$. We may set $[g, h] = z$. There are exactly $p$ conjugate classes of non-central subgroups of order $p$ in $G$ with the representatives $\langle tz^i \rangle$, $0 \leq i \leq p - 1$. It follows (using also Proposition 6) that any abelian maximal non-normal subgroup in $G$ of type $(p^r, p)$, $r \geq 2$ is contained in $\mathrm{C}_G(tz^i) = K$.

Suppose that $K_1$ is of exponent $p^r$, where $r > s$. Let $k$ be an element of order $p^r$ in $K_1$ and consider the subgroup $\langle t\rangle \times \langle k\rangle$. If $\langle t\rangle \times \langle k\rangle$ is non-normal in $G$, then $\langle t\rangle \times \langle k\rangle$ is maximal non-normal in $G$ of order $> |H| = p^s$, contrary to our assumptions. Hence we have $\langle t\rangle \times \langle k\rangle \trianglelefteq G$. Since $[g,t] \in U - \langle z\rangle$, it follows that $\Omega_1(\langle k\rangle) = \langle u\rangle$ with $u \in U - \langle z\rangle$. Since $[g,h] = z$, we have $[g,K_1] = \langle z\rangle$ and so the fact that $k \in K_1$ implies that $[g,k] \in \langle z\rangle$. But we have $\Omega_1(\langle t,k\rangle) = \langle t,u\rangle$ and so $[g,k] = 1$ and therefore $k \in \mathrm{Z}(G)$. Now consider the subgroup $\langle t\rangle \times \langle hk\rangle$, where $hk \in K_1$ $o(hk) = p^r$ and $\Omega_1(\langle hk\rangle) = \langle u\rangle$. If $\langle t\rangle \times \langle hk\rangle$ is not normal in $G$, then $\langle t\rangle \times \langle hk\rangle$ is maximal non-normal in $G$ of order $> |H|$, a contradiction. Hence we have $\langle t\rangle \times \langle hk\rangle \trianglelefteq G$. But $[g,hk] = [g,h][g,k] = z$ and $z \notin \Omega_1(\langle t\rangle \times \langle hk\rangle) = \langle t,u\rangle$, a contradiction. We have proved that $\exp(K) = \exp(K_1) = p^s$ and therefore $o(g) \le p^{s+1}$ and all elements in $G - K$ are of order $\le p^{s+1}$.

There are elements of order $p^s$ or $p^{s+1}$ in $G - K$. Indeed, assume that $o(g) \le p^{s-1}$ for some $g \in G - K$. In that case we must have $s \ge 3$ since $\Omega_1(G) = U \times \langle t\rangle$. Then we compute

$$(gh)^{p^{s-1}} = g^{p^{s-1}} h^{p^{s-1}} [h,g]^{\binom{p^{s-1}}{2}} = h^{p^{s-1}} = z,$$

where $\langle z\rangle = \Omega_1(\langle h\rangle)$ and so we get $o(gh) = p^s$.

If there is an element $g \in G-K$ of order $p^{s+1}$, then all elements in $G-K$ are of order $p^{s+1}$. Indeed, for any $x \in K$ and and any integer $i \not\equiv\ 0 \pmod p$we have:

$$(g^i x)^{p^s} = (g^i)^{p^s} x^{p^s} [x,g^i]^{\binom{p^s}{2}} = (g^i)^{p^s} \ne 1.$$

(ii1) Suppose that $G - K$ contains elements of order $p^s$. Let $g$ be an element of the minimal possible order $p^r$ in $G - K$. Then we have $3 \le r \le s$. Indeed, $\langle g\rangle$ covers $G/L$ (which is cyclic of order $\ge p^2$) and there are no elements of order $p$ in $G - L$ and so $o(g) \ge p^3$.

The element $g^{p^{r-1}}$ is of order $p$ and is contained in $U$. Assume that $g^{p^{r-1}} = z$, where $\langle z\rangle = \Omega_1(\langle h\rangle)$. Let $h'$ be an element in $\langle h\rangle$ such that $(h')^{p^{r-1}} = z^{-1}$. Then we compute (noting that $r \ge 3$):

$$(h'g)^{p^{r-1}} = (h')^{p^{r-1}} g^{p^{r-1}} [g,h']^{\binom{p^{r-1}}{2}} = z^{-1}z = 1,$$

and so $o(h'g) \le p^{r-1}$, a contradiction. We have proved that $\langle g\rangle$ splits over $\langle h\rangle$ and so we have $\Omega_1(\langle g\rangle) = \langle u\rangle$ with $u \in U - \langle z\rangle$.

Set $h^{p^{s-1}} = z$, $s \ge 3$, and then replacing $g$ with $g^j$ for some integer $j \not\equiv 0 \pmod p$, we see that we may set $[g,h] = z$. Replacing $t$ with $t^l$ for some suitable integer $l \not\equiv 0 \pmod p$, we may assume that $[g,t] = uz^i$ for some integer $i \pmod p$. If $[g,t] = u$ (i.e.,$i \equiv 0 \pmod p$), then we have $\langle g,t\rangle \cong \mathrm{M}_{p^{r+1}}$, $r \ge 3$. But $[g,h] = z \notin \langle g,t\rangle$ and so $\langle g,t\rangle$ is not normal in $G$, contrary to our assumptions. Hence we have $i \not\equiv 0 \pmod p$ .

Assume that $r = s$ and so $o(g) = p^s$. We set $g^{p^{s-1}} = u$ and then changing $t$ with a suitable power $t^j$, $j \not\equiv 0 \pmod p$, we may set $[g,t] = uz^i$ with $i \not\equiv 0$

( mod $p$). Let $h' \in \langle h \rangle$ be such that $(h')^{p^{s-1}} = z^i$. Then we have (noting that $s \geq 3$):

$$(gh')^{p^{s-1}} = uz^i[h', g]^{\binom{p^{s-1}}{2}} = uz^i,$$

and since $[gh', t] = [g, t] = uz^i$, we obtain that $\langle gh', t \rangle \cong \mathrm{M}_{p^{s+1}}$. On the other hand, we have $1 \neq [gh', h] \in \langle z \rangle$ and so $\langle gh', t \rangle$ is non-normal in $G$, a contradiction. We have proved that we must have $o(g) = p^r$ with $3 \leq r < s$ and this gives $s \geq 4$. We have obtained the groups stated in part (c) of our proposition which obviously satisfy our condition $(*)$.

(ii2) Suppose that all elements in $G - K$ are of order $p^{s+1}$.

(ii2a) First assume that there is $g \in G - K$ such that $\langle g \rangle$ splits over $\langle h \rangle$. We may choose a generator $g$ in $\langle g \rangle$ so that $[g, h] = z = h^{p^{s-1}}$, $s \geq 2$. Then we set $u = g^{p^s} \in U - \langle z \rangle$ and we may choose a generator $t \in \langle z \rangle$ so that $[g, t] = uz^i$, where $i$ is an integer mod $p$. Suppose that $i \equiv 0 \pmod p$. Then we have $\langle g, t \rangle \cong \mathrm{M}_{p^{s+2}}$. But $[g, h] = z \notin \langle g, t \rangle$ and so $\langle g, t \rangle$ is not normal in $G$, contrary to our assumptions. Hence we have $i \not\equiv 0 \pmod p$. Note that the socle $\Omega_1(\langle x \rangle)$ is equal $\langle u \rangle$ for each $x \in G - K$.

Consider the subgroup $X = \langle t, h^\alpha g^p \rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^s}$, where $g^p \in \mathrm{Z}(G)$ and $\alpha$ is any fixed integer with $\alpha \not\equiv 0 \pmod p$. We have for every integer $j$ (mod $p$ ):

$$(t^j h^\alpha g^p)^{p^{s-1}} = (h^{p^{s-1}})^\alpha g^{p^s} = z^\alpha u,$$

and so $\langle t^j h^\alpha g^p \rangle \cong \mathrm{C}_{p^s}$ is a maximal cyclic subgroup in $G$ since its socle is $\langle z^\alpha u \rangle$. We have $\Omega_1(X) = \langle t, z^\alpha u \rangle$ and

$$[g, h^\alpha g^p] = [g, h^\alpha] = z^\alpha \notin X$$

implies that $X$ is not normal in $G$. This gives

$$\mathrm{N}_G(X) = \mathrm{N}_G(\Omega_1(X)) = K.$$

We have $[g, t] = uz^i$ and so $z^i u \notin \Omega_1(X) = \langle t, z^\alpha u \rangle$. In particular, $i \not\equiv \alpha$ (mod $p$) for any integer $\alpha \not\equiv 0 \pmod p$. But this implies that we must have $i \equiv 0$ (mod $p$), a contradiction.

(ii2b) We have proved that for each $g \in G - K$, $\langle g \rangle$ does not split over $\langle h \rangle$. Hence we have:

$$\langle g \rangle \cap \langle h \rangle \geq \langle z \rangle, \ \langle g, h \rangle' = \langle z \rangle = \Omega_1(\langle h \rangle)$$

and therefore

$$\langle g \rangle \trianglelefteq \langle g, h \rangle \text{ with } p \leq |\langle g, h \rangle : \langle g \rangle| \leq p^{s-1}.$$

Since $\langle g^p \rangle$ is of order $p^s = \exp(\langle g^p, h \rangle)$, it follows that $\langle g^p \rangle$ splits in $\langle g^p, h \rangle$ and so we have:

$$\langle g^p, h \rangle = \langle k \rangle \times \langle g^p \rangle \text{ with } K = \langle t \rangle \times (\langle k \rangle \times \langle g^p \rangle) \text{ and}$$
$$\langle k \rangle \langle g \rangle = \langle g, h \rangle \text{ with } \langle k \rangle \cap \langle g \rangle = \{1\}.$$

Because $\langle [k,g]\rangle = \langle z\rangle$ and $\Omega_1(\langle k\rangle\langle g\rangle) = U \le \mathrm{Z}(G)$, we get $o(k) = p^r$, $2 \le r \le s-1$ and so $s \ge 3$. We may set $u = k^{p^{r-1}} \in U - \langle z\rangle$ and $[g,k] = z = g^{p^s}$. Also note that the socle $\Omega_1(\langle x\rangle)$ for each $x \in G-K$ is equal $\langle z\rangle$.

We may choose a suitable generator $t$ in $\langle t\rangle$ so that $[g,t] = uz^i$ for some integer $i \bmod p$. Consider the subgroup $Y = \langle k\rangle\times\langle t\rangle \cong \mathrm{C}_p\times\mathrm{C}_{p^r}$, $2 \le r \le s-1$, which is not normal in $G$ since $[g,k] = z \notin Y$. We have $\mathrm{N}_G(Y) = K$ and so $\mathrm{N}_G(\langle t,u\rangle) = K$, where $\langle t,u\rangle = \Omega_1(Y)$. We have $[g,t] = uz^i \notin \Omega_1(Y)$ and so we must have $i \not\equiv 0 \pmod p$.

Choose an element $g'$ in $\langle g^p\rangle$ such that $o(g') = p^r$ and $(g')^{p^{r-1}} = z$ and note that $g' \in \mathrm{Z}(G)$. Now we consider for each $\alpha \not\equiv 0$ ( mod $p$) the subgroup

$$V = \langle k^\alpha g'\rangle \times \langle t\rangle \cong \mathrm{C}_{p^r}\times \mathrm{C}_p \text{ with } (k^\alpha g')^{p^{r-1}} = u^\alpha z \text{ so that } \Omega_1(V) = \langle t, u^\alpha z\rangle.$$

Since $[g, k^\alpha g'] = z^\alpha \notin \Omega_1(V)$, we have $\mathrm{N}_G(V) = K$ and so also $\mathrm{N}_G(\langle t, u^\alpha z\rangle) = K$. Because $[g,t] = uz^i$, it follows that $uz^i \notin \langle u^\alpha z\rangle$ for each $\alpha \not\equiv 0$ ( mod $p$). We can find an integer $j \not\equiv 0$ ( mod $p$) so that $ij \equiv 1$ ( mod $p$). We get

$$(uz^i)^j = u^j z^{ij} = u^j z \notin \langle u^\alpha z\rangle$$

for each $\alpha \not\equiv 0$ ( mod $p$), a contradiction.

(iii) We consider the remaining case, where $G/L$ is not cyclic and $G > L$. Since $G/L$ is abelian and $K/L \ne \{1\}$ is cyclic, it follows that $G/L$ splits over $K/L$ and so we have $G = KG_0$ with $K \cap G_0 = L$ and $|G_0 : L| = p$. Also, $K/H$ is cyclic of order $\ge p^2$ and we have:

$$H = \langle h\rangle \times \langle t\rangle \cong \mathrm{C}_{p^s}\times \mathrm{C}_p,\ s \ge 2, \text{ where } \mathrm{C}_{p^s} \cong \langle h\rangle \trianglelefteq G,\ \langle t\rangle \cong \mathrm{C}_p,$$

$$\Omega_1(H) = \langle z\rangle,\ G' = U \cong \mathrm{E}_{p^2},\ L = UH \text{ is abelian and } U \le \mathrm{Z}(G).$$

(iii1) Suppose first that $\langle h\rangle \not\le \mathrm{Z}(G_0)$ so that we have $U = G_0' \cong \mathrm{E}_{p^2}$ and therefore by (i) we get $p = 2$ and $G_0$ is the uniquely determined special 2-group of order $2^5$ (stated in part (b) of our proposition):

$$L = \langle h\rangle \times \langle u\rangle \times \langle t\rangle \cong \mathrm{C}_4\times\mathrm{C}_2\times\mathrm{C}_2,\ \langle h\rangle \cong \mathrm{C}_4,\ h^2 = z,\ \langle u\rangle \cong \langle t\rangle \cong \mathrm{C}_2,$$

$$G_0 \cong L\langle g\rangle \text{ with } g^2 = z,\ [g,h] = z,\ [g,u] = 1, \text{ and } [g,t] = u.$$

Since $\mathrm{Z}(G_0) = U$, it follows that for each $x \in K-L$ such $x^2 \in L$, we must have $1 \ne x^2 \in U$. Let $k \in K-L$ be such that $\langle k\rangle$ covers the cyclic group $K/H$ of order $\ge 4$. Thus $\Omega_1(\langle k\rangle) = \langle u\rangle$ or $\langle uz\rangle$ and so $K$ splits over $H$.

Because $\mathrm{C}_{G_0}(g) = U\langle g\rangle$ and so $|G_0 : \mathrm{C}_{G_0}(g)| = 4$, we get together with $|G'| = 4$ that $|G : \mathrm{C}_G(g)| = 4$. But we have $G = K\langle g\rangle$ and so $\mathrm{C}_G(g) = \mathrm{C}_K(g)\langle g\rangle$ which implies that $|K : \mathrm{C}_K(g)| = 4$. On the other hand, we have $|H : \mathrm{C}_H(g)| = 4$ and therefore $\mathrm{C}_K(g)$ covers $K/H$. It follows that we may choose our element $k \in \mathrm{C}_K(g)$ such that $\langle k\rangle$ covers $K/H$. Hence we may assume $[g,k] = 1$.

Case (1). Suppose that $|K : L| > 2$ so that $o(k) \ge 8$. Then there is an element $k'$ of order 4 in $\langle k\rangle$ such that $k' \in \mathrm{Z}(G)$. Note that $(tg)^2 = uz$ and so if $(k')^2 = uz$, then $k'(tg)$ is an involution in $G - K$, a contradiction. Hence we must have in this case $(k')^2 = u$. We set $o(k) = 2^n$, $n \geq 3$, and then we have $k^{2^{n-1}} = u$. Assume for a moment that that $[k,h] = [k,t] = 1$ which together with $[k,g] = 1$ (from the previous paragraph) then implies that $k \in \mathrm{Z}(G)$. In that case we have $(gk)^{2^{n-1}} = u$ and $[gk,t] = u$ so that $\langle gk, t\rangle \cong \mathrm{M}_{2^{n+1}}$ with $n \geq 3$. But $[h, gk] = z \notin \langle gk, t\rangle$ and so $\langle gk, t\rangle$ is not normal in $G$, contrary to our assumptions. We have proved that $k \notin \mathrm{Z}(G)$.

Assume that $[k,t] = 1$. Then we have $[k,h] = z$. Consider in this case the subgroup

$$\langle t\rangle \times \langle k\rangle, \text{ where } o(k) = 2^n = \exp(\mathrm{G}),\ n \geq 3.$$

Since $[h,k] = z \notin \langle t,k\rangle$, it follows that $\langle t,k\rangle$ is a maximal non-normal subgroup in $G$ of order $> |H|$, contrary to our assumptions. We have proved that we must have $[k,t] = z$ (noting that we have $K' \leq \langle z\rangle$).

Now we consider the subgroup $\langle t\rangle \times \langle hk'\rangle$, where $k'$ is an element of order 4 in $\langle k\rangle$ and $k' \in \mathrm{Z}(G)$. Here we have $\Omega_1(\langle t, hk'\rangle) = \langle t, uz\rangle$. Because $[g,t] = u$, it follows that $\langle t, hk'\rangle \cong \mathrm{C}_2 \times \mathrm{C}_4$ is abelian non-normal in $G$. By the maximality of $|H|$, it follows that $\langle t, hk'\rangle$ is a maximal non-normal subgroup in $G$. Then Proposition 6 implies that either $\langle hk'\rangle \trianglelefteq G$ or $\langle thk'\rangle \trianglelefteq G$. But $[hk', g] = z$ and so $\langle hk'\rangle$ is not normal in $G$. Hence we must have $\langle thk'\rangle \trianglelefteq G$. From $[thk', k] = z[h,k]$ follows that $[h,k] = z$.

Finally assume that $n > 3$ so that the subgroup $\langle t\rangle \times \langle k^2\rangle \cong \mathrm{C}_2 \times \mathrm{C}_{2^{n-1}}$ is non-normal in $G$ ( since $[t,k] = z$), contrary to the maximality of $|H|$. Hence we get $n = 3$, $o(k) = 8$ and $|G| = 2^7$. We have obtained the group stated in part (d1) of our proposition.

Case (2). Suppose that $|K : L| = 2$ and $k \in \mathrm{Z}(G)$. Here we have $o(k) = 4$ and $k^2 \in \{u, uz\}$. If $k^2 = uz$, then $(gt)^2 = uz$ together with $[k, gt]$=1 implies that $gtk$ is an involution in $G - K$, a contradiction. Hence in this case we have $k^2 = u$ and we have obtained the group of order $2^6$ stated in part $(d2)$ of our proposition.

Case (3). Assume that $|K : L| = 2$ and $k \notin \mathrm{Z}(G)$. We have

$$k^2 = uz^{\epsilon},\ \epsilon \in \{0,1\},\ [k,t] = z^{\eta},\ [k,h] = z^{\delta},\ \eta, \delta \in \{0,1\},$$

and $\eta = \delta = 0$ is not possible.

Then the fact that there are no involutions in $G - K$ gives a unique solution

$$\epsilon = 1,\ \eta = 1,\ \delta = 0$$

and so we have obtained the special group of order $2^6$ stated in part (d3) of our proposition.

Conversely, all groups from part (d) of our proposition satisfy the condition $(*)$.

(iii2) Suppose that $\langle h\rangle \le Z(G_0)$. We have for each $g \in G_0 - L$, $G_0' = \langle [g,t]\rangle$ with $[g,t] = u \in U - \langle z\rangle$ and $\langle z\rangle = \Omega_1(\langle h\rangle)$. We have

$$Z(G_0) = \langle h\rangle \times \langle u\rangle \cong C_{p^s} \times C_p,\ s \ge 2.$$

Since $1 \ne g^p \in Z(G_0)$ and there are no elements of order $p$ in $G - K$, it follows that $A = Z(G_0)\langle g\rangle$ is abelian of rank 2. Hence $A$ is either of type $(p^s, p^2)$ or $(p^{s+1}, p)$.

Suppose, by way of contradiction, that $A$ is of type $(p^s, p^2)$. In that case there is an element $g_0 \in A - Z(G_0)$ such that $g_0^2 = u$, where $\langle u\rangle = G_0'$. If $p = 2$, then $\langle g_0, t\rangle \cong D_8$ and so $g_0 t$ is an involution in $G_0 - K$, a contradiction. Hence we must have $p > 2$ and $M = \langle g_0, t\rangle \cong M_{p^3}$. By our assumptions, we have $M \trianglelefteq G$. Note that $G' \cap M = U \cap M = \langle u\rangle$ and set $C = C_G(M)$ so that $C \cap M = \langle u\rangle$. If $C * M < G$, then $G/C \cong S(p^3)$ (which is an $S_p$-subgroup of $\mathrm{Aut}(M)$), contrary to $U = G' \le C$. Hence we have $G = M * C$. Since $\langle h\rangle \le C$, $\langle h\rangle \trianglelefteq G$ and $t$ centralizes $C$, we have $C \le K$ and so $K = C \times \langle t\rangle$. Because $C < K$ and $K' \le \langle z\rangle$, we have $C' \le \langle z\rangle$ . If $C' = \{1\}$, then $G' = C'M' = \langle u\rangle$, a contradiction. Hence we have $C' = \langle z\rangle$. Note that $\{1\} \ne K/L$ is cyclic, where $L = (\langle h\rangle U) \times \langle t\rangle$ and $K = CL$ with $C \cap L = \langle h\rangle U$. Thus $\{1\} \ne C/(\langle h\rangle \times \langle u\rangle)$ is cyclic. Let $c \in C$ be such that $\langle c\rangle$ covers $C/(\langle h\rangle \times \langle u\rangle)$ and so we must have $\langle [h,c]\rangle = \langle z\rangle$. Since $K/H$ is cyclic of order $\ge p^2$, $\langle c\rangle$ also covers $K/H$ and so $\langle c\rangle$ covers $C/(H \cap C) = C/\langle h\rangle$. It follows that $C$ is metacyclic minimal nonabelian without a cyclic subgroup of index $p$ (noting that $E_{p^2} \cong \Omega_1(C) = U \le Z(G)$ ). Hence we may set

$$C = \langle a\rangle\langle b\rangle \text{ with } \langle a\rangle > \langle z\rangle = C',\ \langle a\rangle \cap \langle b\rangle = \{1\},\ \langle b\rangle \cong C_{p^r},\ r \ge 2,$$

and $\Omega_1(\langle b\rangle) = \langle uz^i\rangle$, where $i$ is an integer mod $p$. Consider the subgroup

$$\langle b\rangle \times \langle t\rangle \cong C_{p^r} \times C_p,$$

which is non-normal in $G$ since $\langle [a,b]\rangle = \langle z\rangle$ and $z \notin \langle b,t\rangle$. We claim that $\langle b,t\rangle$ is a maximal non-normal subgroup in $G$. Indeed, let $X > \langle b,t\rangle$ be a maximal non-normal subgroup in $G$. If $X \cap C > \langle b\rangle$, then $\langle z\rangle \le X$ and so $\langle z, uz^i\rangle = G' \le X$, a contradiction. Hence we have $X \cap C = \langle b\rangle$. Because $G/C \cong E_{p^2}$, it follows that $X$ must contain an element $x \in G - (C \times \langle t\rangle) = G - K$. On the other hand, $C_G(t) = C \times \langle t\rangle = K$ and so $[x,t] \ne 1$ and $X$ is nonabelian, contrary to our assumptions. Finally, by Proposition 6, we have $\langle bt^j\rangle \trianglelefteq G$ for some integer $j$ mod $p$, where $\Omega_1(\langle bt^j\rangle) = \langle uz^i\rangle$. On the other hand, we have

$$[a, bt^j] = [a,b],\ \text{where } \langle [a,b]\rangle = \langle z\rangle \ne \langle uz^i\rangle,$$

a final contradiction.

We have proved that $A = Z(G_0)\langle g\rangle$ is abelian of type $(p^{s+1}, p)$. It follows that all elements of order $p^s$ in $\langle h\rangle U$ are central in $G$ (noting that $U \le Z(G)$). Replacing $H$ with $H^* = \langle t\rangle \times \langle hu^i\rangle$ for some integer $i$ mod $p$ (which is also a maximal non-normal abelian subgroup of type $(p^s, p)$) so that $\langle g^p\rangle = \langle hu^i\rangle$

and then working with $H^*$ instead of $H$, we see that we may assume from the start that there is $g \in G - K$ such that $g^p = h$, where $\langle h \rangle \le \mathrm{Z}(G)$ and we set $g^{p^s} = z$. If $t \in \mathrm{Z}(K)$, then $L \le \mathrm{Z}(K)$ and since $K/L$ is cyclic, $K$ would be in that case abelian.

(iii2a) First assume that $K$ is nonabelian, i.e., $t \notin \mathrm{Z}(K)$. Then we have $K' = \langle z \rangle$ and so if $k \in K - L$ is such that $\langle k \rangle$ covers $K/H$ (which is cyclic of order $\ge p^2$), then we may set (by choosing a suitable generator $t$ of $\langle t \rangle$) $[k, t] = z$.

It is easy to see that $\langle k \rangle$ splits over $H$. Indeed, if $\langle k \rangle$ does not split over $H$, then $\langle k \rangle \cap H = \langle k \rangle \cap \langle h \rangle$ since $\mathrm{Z}(G) \cap L = \langle h \rangle U$ and so we have $\langle k \rangle > \langle z \rangle$. It follows that $\langle k, t \rangle \cong \mathrm{M}_{p^{n+1}}$ with $n \ge 3$ since $[k, t] = z$. On the other hand, $[g, t] \in U - \langle z \rangle$ and so $[g, t] \notin \langle k, t \rangle$ which implies that $\langle k, t \rangle$ is not normal in $G$, contrary to our assumptions. Hence $\langle k \rangle$ splits over $H$ and we may set $o(k) = p^r$, $r \ge 2$, and $k^{p^{r-1}} = u \in U - \langle z \rangle$.

If $o(k^p) > p^s$, then $\langle t \rangle \times \langle k^p \rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^{r-1}}$ is non-normal in $G$ (since we have $[k, t] = z \notin \langle t, k^p \rangle$), contrary to the maximality of $|H| = p^{s+1}$. Hence we have $r \le s + 1$. We set $[g, t] = u^i z^j$ with $i \not\equiv 0 \pmod p$.

We have here

$$\Phi(G) = \mho_1(G) = \mathrm{Z}(G) = \langle g^p \rangle \times \langle k^p \rangle \text{ and so } |G : \Phi(G)| = p^3.$$

By Lemma 146.7 in [4], $G$ possesses a unique abelian maximal subgroup $A^*$. Because we have $|G : \mathrm{C}_G(t)| = p^2$, it follows that $t \in G - A^*$ and

$$\mathrm{C}_{A^*}(t) = \mathrm{Z}(G) = \langle h \rangle \times \langle k^p \rangle,\ A^*/\mathrm{Z}(G) \cong G' = U = \Omega_1(A^*)$$

so that $A^*$ is of rank 2 and of type $(p^{s+1}, p^r)$, where $s \ge 2$ and $2 \le r \le s + 1$. Indeed, the map $a \to [a, t]$ $(a \in A^*)$ is a homomorphism from $A^*$ onto $G'$ and so $A^*/\mathrm{Z}(G) \cong G'$.

Case (a): $r < s + 1$. In this case we may set

$$A^* = \langle a \rangle \times \langle b \rangle,\ \text{where } \langle a \rangle \cong \mathrm{C}_{p^{s+1}},\ \langle b \rangle \cong \mathrm{C}_{p^r},\ z = a^{p^s},\ u = b^{p^{r-1}}.$$

Take an element $a' \in \langle a^p \rangle \le \mathrm{Z}(G)$ such that $o(a') = p^r$ and $(a')^{p^{r-1}} = z$. Suppose that $[b, t] \notin \langle z \rangle$. Then we have $[b, t] = z^i u$ ($i$ is an integer mod $p$) for a suitable choice of a generator $t$ of $\langle t \rangle$. We get

$$((a')^i b)^{p^{r-1}} = z^i u \text{ and } [(a')^i b, t] = [b, t] = z^i u$$

and therefore we have either $p = 2$, $r = 2$ and $\langle (a')^i b, t \rangle \cong \mathrm{D}_8$ or $\langle (a')^i b, t \rangle \cong \mathrm{M}_{p^{r+1}}$ (where in case $p = 2$, we have $r \ge 3$). But $|G : \mathrm{C}_G(t)| = p^2$ and so for some $g \in G$ we get $\langle [g, t] \rangle \ne \langle z^i u \rangle$ and so $\langle (a')^i b, t \rangle$ is not normal in $G$, contrary to our assumptions. Hence choosing a suitable generator $t$ of $\langle t \rangle$, we must have $[b, t] = z$. Then we also get $[a, t] = u^i z^j$ with $i \not\equiv 0 \pmod p$.

Case (b): $r = s + 1$. Let $b \in A^* - \Phi(G)$ be such that $[b, t] = z$ and set $b^{p^s} = u$, where $\langle u \rangle \ne \langle z \rangle$. Let $a \in A^* - \Phi(G)$ be such that $a^{p^s} = z$ and then we have

$$A^* = \langle a \rangle \times \langle b \rangle \cong \mathrm{C}_{p^{s+1}} \times \mathrm{C}_{p^{s+1}} \text{ and } [a,t] = u^i z^j,\ i \not\equiv 0 \pmod p.$$

In this critical case we must also have $j \not\equiv \xi - i\xi^{-1} \pmod p$ for all integers $\xi \not\equiv 0 \pmod p$. Indeed, assume that for some $\xi \not\equiv 0 \pmod p$, we have $j \equiv \xi - i\xi^{-1} \pmod p$. In that case we solve the congruence $i\mu \equiv \xi \pmod p$ with some $\mu \not\equiv 0 \pmod p$. We compute (noting that $s \geq 2$):

$$(a^\mu b)^{p^s} = (a^{p^s})^\mu b^{p^s} [b, a^\mu]^{\binom{p^s}{2}} = z^\mu u$$

and

$$[a^\mu b, t] = (u^i z^j)^\mu z = z^{1+j\mu} u^{i\mu} = z^{1+(\xi - i\xi^{-1})\mu} u^\xi =$$

$$z^{1+\xi\mu - \xi^{-1} i\mu} u^\xi = z^{1+\xi\mu-1} u^\xi = z^{\xi\mu} u^\xi = (z^\mu u)^\xi.$$

It follows that $\langle a^\mu b, t \rangle \cong \mathrm{M}_{p^{s+2}},\ s \geq 2$, and since $[b,t] = z \notin \langle a^\mu b, t\rangle$, it follows that $\langle a^\mu b, t \rangle$ is not normal in $G$, contrary to our assumptions. We have obtained the groups stated in part (e) of our proposition.

Conversely, we see that in any group $G$ from part (e) of our proposition, for each $x \in A^* - \mathrm{Z}(G)$, $\langle x \rangle$ is not normal in $G$ and so $\mathrm{D}_8$ or $\mathrm{M}_{p^n}$ cannot be subgroups of $G$, where $A^*$ is the unique abelian maximal subgroup of $G$. Furthermore, let $X$ be any maximal non-normal abelian subgroup of $G$ of order $\geq p^3$ which has more than one subgroup of order $p$. Since $G$ has exactly one conjugacy class of noncentral subgroups of order $p$ with the representative $\langle t \rangle$, we may assume that $t \in X$. It follows that $X = \langle t \rangle \times X_0$, where $X_0$ is any maximal cyclic subgroup in $\mathrm{Z}(G)$. Hence our condition $(*)$ holds.

(iii2b) It remains to consider the case $t \in \mathrm{Z}(K)$ so that $K$ is abelian and $K > L$. Since $K/\mathrm{C}_K(g) \cong G'$ (Lemma 1.1 in [1]), there is $k \in K - L$ such that $\langle k \rangle$ covers $K/H$ and $[g,k] = z = g^{p^s}$, $s \geq 2$, where $[g,t] \in U - \langle z \rangle$ with $p^r = o(k) \geq p^2$. Since $K = \langle t \rangle \times \langle h, k \rangle$ and $\mathrm{Z}(G) = \langle h, k^p \rangle$, it follows that $U \leq \langle h, k^p \rangle$ because $U \leq \mathrm{Z}(G)$. Hence we have $\Omega_1(\langle h, k \rangle) = U = G'$. Consider the subgroup

$$\langle t \rangle \times \langle k \rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^r},\ r \geq 2.$$

If $\Omega_1(\langle k \rangle) = \langle z \rangle$, then $[g,t] \in U - \langle z \rangle$ shows that $\langle t, k \rangle$ is not normal in $G$. If we have $\Omega_1(\langle k \rangle) = \langle u \rangle$ with $u \in U - \langle z \rangle$, then $[g,k] = z$ shows that again $\langle t, k \rangle$ is not normal in $G$. The maximality of $|H|$ shows that we must have $r \leq s$ and so we have $\exp(K) = p^s$. It follows that $\langle h \rangle$ splits in $\langle h, k \rangle$ and so we have

$$\langle h, k \rangle = \langle h \rangle \times \langle k' \rangle \text{ with } \Omega_1(\langle k' \rangle) = \langle u \rangle,\ u \in U - \langle z \rangle \text{ and } o(k') \geq p^2.$$

Since $[g,t] \in U - \langle z \rangle$, there is an integer $j$ mod $p$ so that $[g, t^j k'] = z$. Because $\Omega_1(\langle t^j k' \rangle) = \langle u \rangle$, we may assume from the start that (replacing $k$ with $t^j k'$

and writing $k$ again):

$$K = \langle t\rangle \times \langle h\rangle \times \langle k\rangle,\ o(k) = p^r,\ 2 \le r \le s,$$
$$k^{p^{r-1}} = u \in U - \langle z\rangle \text{ and } [g,k] = z = g^{p^s}.$$

Replacing $t$ with some other generator of $\langle t\rangle$ (if necessary), we may assume from the start that $[g,t] = uz^i$ for some integer $i$ mod $p$.

For any integer $\alpha \not\equiv 0 \pmod p$ and any $x \in K$, we have (noting that $s \ge 2$)

$$(g^\alpha x)^{p^s} = z^\alpha [x, g^\alpha]^{\binom{p^s}{2}} = z^\alpha$$

and so $\Omega_1(G) = \langle t\rangle \times U \cong \mathrm{E}_{p^3}$ and the socle of each cyclic subgroup of $G$ which is not contained in $K$ is equal $\langle z\rangle$.

Let $h'$ be an element of order $p^r$ in $\langle h\rangle$ such that $(h')^{p^{r-1}} = z$. For any fixed $\alpha \not\equiv 0 \pmod p$ we consider the subgroup

$$\langle t\rangle \times \langle (h')^\alpha k\rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^r},\ \text{where } ((h')^\alpha k)^{p^{r-1}} = z^\alpha u$$

and note that $\langle (h')^\alpha k\rangle \cong \mathrm{C}_{p^r}$, $r \ge 2$, is a maximal cyclic subgroup in $G$ with the socle $\langle z^\alpha u\rangle$. We have $[g, (h')^\alpha k] = z \notin \langle t, (h')^\alpha k\rangle$ so that $\langle t, (h')^\alpha k\rangle$ is a maximal non-normal subgroup in $G$. By Proposition 6, there is a unique integer $j$ ( mod $p$ ) such that $\langle t^j (h')^\alpha k\rangle \trianglelefteq G$. Hence we must have:

$$[g, t^j (h')^\alpha k] = (uz^i)^j z = z^{1+ij} u^j \in \langle z^\alpha u\rangle,$$

which shows that $j \not\equiv 0 \pmod p$ and we get

$$z^{1+ij} u^j = z^{\alpha j} u^j \text{ so that } 1 + ij \equiv \alpha j \text{ or } j(\alpha - i) \equiv 1 \pmod p.$$

Hence for any fixed $\alpha \not\equiv 0 (\mathrm{mod}\ p)$, there must exist $j \not\equiv 0 (\mathrm{mod}\ p)$ such that $j(\alpha - i) \equiv 1 \pmod p$ and this gives that we must have $i \equiv 0 \pmod p$. We have obtained the relation $[g,t] = u$.

Because $[g,k] = z$ and $\langle k\rangle \cong \mathrm{C}_{p^r}$, $r \ge 2$, is a maximal cyclic subgroup in $G$ with the socle $\langle u\rangle$, it follows that $\langle t\rangle \times \langle k\rangle \cong \mathrm{C}_p \times \mathrm{C}_{p^r}$ is a maximal non-normal subgroup in $G$. By Proposition 6, there is a unique integer $m$ ( mod $p$ ) such that $\langle t^m k\rangle \trianglelefteq G$. But we have

$$[g, t^m k] = [g,t]^m [g,k] = u^m z,$$

a final contradiction (since $\Omega_1(\langle t^m k\rangle) = \langle u\rangle$). Our proposition is completely proved. □

Proof of Theorem C. By inspection of all Propositions 1 to 12, we see that all possible cases have been investigated and so our theorem is proved.

□

## References

[1] Y. Berkovich, Groups of prime power order, Vol. 1, Walter de Gruyter, Berlin-New York, 2008.
[2] Y. Berkovich and Z. Janko, Groups of prime power order, Vol. 2, Walter de Gruyter, Berlin-New York, 2008.
[3] Y. Berkovich and Z. Janko, Groups of prime power order, Vol. 3, Walter de Gruyter, Berlin-New York, 2011.
[4] Y. Berkovich and Z. Janko, Groups of prime power order, Vol. 4, Walter de Gruyter, Berlin-New York, to appear 2014.

Z. Janko
Mathematical Institute
University of Heidelberg
69120 Heidelberg
Germany
*E-mail*: janko@mathi.uni-heidelberg.de

*Received*: 1.3.2014.