J. Group Theory **20** (2017), 193–225
DOI 10.1515/jgth-2016-0035

More on core-2 2-groups

Bettina Wilkens

Communicated by Evgenii I. Khukhro

Abstract. Let G be a finite 2-group with the property that $|H : H_G| \leq 2$ for all subgroups H of G. Then G has an abelian normal subgroup of index at most 4 in G. This result represents an affirmative answer to Question 18.56 from the current edition of the Kourovka Notebook.

1 Introduction

Let n be a positive integer. A group G is called *core-n* if $|H/H_G| \leq n$ for every subgroup H of G; here, H_G denotes the largest normal subgroup of G contained in H. In [4], it was shown that a locally finite core-n group has a normal abelian subgroup whose index in the group is bounded by a function of n. In [3] the same authors proved that, for *odd* primes p, a finite core-p p-group has an abelian normal subgroup of index p^2, a best possible bound. The paper ([3, Theorem 2]) also contains a proof of the existence of a normal abelian subgroup of index at most 2^6 in a finite core-2 2-group. The authors mention that no examples of finite core-2 2-groups were known that did not possess an abelian subgroup of index at most 4. Later ([5]) it was shown that finite core-2 groups of class 2 indeed must have an abelian subgroup of index at most 4. The present paper is devoted to showing that every finite core-2 2-group has an abelian subgroup of index at most 4. This provides an affirmative answer to Question 18.56 from the 18th edition of the Kourovka Notebook, posed by *G. Cutolo*.

The dihedral groups D_{2^n} are core-2, which shows that core-2-ness does not entail bounded class or bounded subgroup breadth. This places core-2 2-groups in contrast to odd-order core-p p-groups, those being of class at most 3 ([6]). The group $D_8 * Q_8$ is core-2, which shows that 4 is the best possible upper bound for the index of an abelian subgroup in a core-2 2-group. Our main result reads as follows:

Theorem. *Let G be a finite 2-group. Suppose that $|H/H_G| \leq 2$ for every subgroup H of G. Then G has an abelian subgroup that contains $\Phi(G)$ and has index at most four in G.*

We note that the corresponding result for odd p is an immediate corollary of the results of [3]. Letting p be an odd prime and G a finite core-p p-group, G has a normal abelian subgroup A of index p^2 ([3, Theorem 1]). We may obviously take A to be a maximal abelian subgroup of G. Then, according to [3, Lemma 1.1 (iii)], $\mho_1(G) \leq Z(G) \leq A$ and $G' \leq A$, because G/A is too small to be nonabelian.

We conclude this introduction with three very helpful observations: Subgroups as well as quotients of a core-n group are core-n. If G is a core-p p-group, then $\langle x^p \rangle \lhd G$ whenever $x \in G$ and $|E : E \cap Z(G)| \leq p$ if E is an elementary abelian subgroup of G. We also note a corollary.

Corollary. *Let G be a finite core-*2 *group. Then G has an abelian subgroup of index at most* 8*, and this bound is best possible.*

Proof. Let G be a finite core-2 group of composite order, and let $Q = O_{2'}(G)$. Then Q is abelian of odd order, every subgroup of Q is normal in G and $G = QS$ with $S \in Syl_2(G)$. The group S is core-2, and, since $|S : S_G| \leq 2$, $C_S(Q)$ has index at most 2 in S. A direct product of a core-2 2-group with an abelian group of odd order is core-2; if $[S, Q] \neq 1$ and $T = C_S(Q)$, then the corresponding semidirect product SQ is core-2 if and only if S normalises every subgroup of Q, $|S : T| = 2$, S is core-2 and $T \cap U \lhd S$ whenever $U \leq S = TU$. By the theorem, T has an abelian subgroup of index at most 4 and the direct product of this with Q has index at most 8 in G. Now let

$$S = \langle x, y, s, t \mid x^2 = y^8 = s^4 = t^4 = 1,\ [x, y] = y^2, \\ s^2 = t^2 = [s, t] = y^4 \rangle .$$

Then $S \cong D_{16} * Q_8$ is core-2, but there is no abelian subgroup of index 4 in S that does not contain y. Now let $G = SQ$, where $Q \cong C_3$, $C_S(Q) = \langle x, y^2, s, t \rangle$ and y inverts the elements of Q. This G does not have an abelian subgroup of index four. □

The reader interested in the structure of core-p-groups of class 2 may find the results of Lemma 2.9 somewhat relevant.

2 Preliminaries

Lemma 2.1 ([2, Lemma 3.4.1]). *Let X be a finite group and let B be an abelian normal subgroup of X. Let N be the subgroup of X consisting of elements inducing power automorphisms on B. Let $n = \exp B$ and let U be the unit subgroup of $\mathbb{Z}/n\mathbb{Z}$. There is a homomorphism $\epsilon : X \to U$ given by $b^x = b^{\epsilon(x)}$ whenever $b \in B$ and $x \in N$.*

Notation. Let X be a finite group. Following Blackburn's notation, we let

$$j(X) = |\{x \in X \mid x^2 = 1\}|.$$

Lemma 2.2 ([1, Satz 1]). *Let P be a 2-group and let $1 \neq N \leq \Omega_1(Z(P))$. Let $\mathcal{H}$ be the set of maximal subgroups of N. Then*

$$\sum_{U \in \mathcal{H}} j(P/U) = |\mathcal{H}| j(P/N) + j(P).$$

The fact that core-p p-groups have abelian Frattini subgroup is proved in [3, see Lemma 1.1 (ii)–(iii) for odd p and Proposition 2.11 for $p = 2$]. We include a short proof for $p = 2$, as this will be a vital ingredient of the forthcoming proof.

Lemma 2.3 ([3, Proposition 2.11]). *A finite core-2 2-group P has abelian Frattini subgroup.*

Proof. Let P be a counterexample of minimal order. Since $\Phi(P)' \leq \langle u \rangle$ whenever $1 \neq u \in Z(P)$, $Z(P)$ is cyclic and $\Phi(P)' = \Omega_1(Z(P))$. Let s and t be involutions in $\Phi(P)$. If $[s,t] \neq 1$, then $\langle s,t \rangle \cong D_8$. Now P normalises a maximal subgroup V of $\langle s,t \rangle$, of order 4; this, however, implies that $[\Phi(P), V] = 1$, a contradiction. Let $\Omega_1(\Phi(P)) = Y$. We have just seen that Y is elementary abelian, whence $|Y : Y \cap Z(P)| \leq 2$, implying $|Y| \leq 4$ and $Y \leq Z(\Phi(P))$. Let $\Omega_1(Z(P)) = \langle z \rangle$. If $z \in U \leq \Phi(P)$, then $U \trianglelefteq \Phi(P)$. Since $\Omega_1(\langle x \rangle) \leq Z(P)$ for every x in P of order greater than 2, a subgroup U of $\Phi(P)$ not containing z must be contained in Y, hence in $Z(\Phi(P))$. Thus $\Phi(P)$ is Hamiltonian, i.e. $\Phi(P) = Q \times E$ with E elementary abelian and $Q \cong Q_8$. At least one maximal subgroup V of Q must be normal in P, such that $[\Phi(P), V] = 1 = Q'$, a contradiction. □

The following is a variation of [8, Lemma 8] and its proof is analogous to [8, Lemma 2]. We provide a short proof.

Lemma 2.4. *Let P be a finite p-group. Let U and V be subgroups of P satisfying $[S,T] \leq \Omega_1(Z(P))$. If $|U : C_U(v)| \leq p$ for all v in V, then $|[U,V]| \leq p$ or $|U : C_U(V)| = p$.*

Proof. Let $v \in V \setminus C_V(U)$ and $w \in V$. If $[U,w] \not\leq [U,v]$ and $C_U(w) \not\geq C_U(v)$, then $[U, vw] = [C_U(v)C_U(w), vw] = [C_U(w), v][C_U(v), w] = [U,v] \times [U,w]$, of order p^2. It follows that every element of V belongs to $C_V(C_U(v))$ or belongs to the subgroup $\{x \in V \mid [U,x] \leq [U,v]\}$ of V. The assertion follows because V cannot be the union of two proper subgroups. □

A proof of the following lemma could be compiled from references to the available literature on metacyclic groups.

Lemma 2.5. *Let* $U = \langle u, v\rangle$ *be a* 2*-group with* $[u, v] \in \langle u^4\rangle$*. Unless* $o([u, v]) \leq 2$*, there is* $x \in U$ *with* $\langle x^2\rangle \ntrianglelefteq U$*.*

Proof. Assume that $o([u, v]) > 2$; it will suffice to establish the corresponding statement in the quotient $U/\langle [u, v]^4\rangle$. Hence assume $o(u) = 2^{n+2}$ with $n \geq 2$ and $\langle [u, v]\rangle = \langle u^{2^n}\rangle$. Observe that this implies $\gamma_3(U) = 1$. Let $|U : \langle u\rangle| = 2^m$. A generator w of $\langle u\rangle$ may be chosen such that v^{2^m} is equal to a power w^{2^ℓ}; as $C_{\langle u\rangle}(v) = \langle u^4\rangle$ and $C_{\langle v\rangle}(u) = \langle v^4\rangle$, we have $m \geq 2 \leq \ell$.

Assuming $\ell < m$, let $x = wv^{-2^{m-\ell}}$. Note that the order of $x\langle u\rangle$ in $U/\langle u\rangle$ is equal to 2^ℓ. Since $\ell \geq 2$ and $m - \ell \geq 1$,

$$x^{2^\ell} = w^{2^\ell} v^{-2^m} [v, w]^{2^{m-\ell}\binom{2^\ell}{2}} = 1.$$

It follows that $o(x) = o(x\langle u\rangle) = 2^\ell$ and $\langle x\rangle \cap \langle u\rangle = 1$. However,

$$[x^2, v] = [w^2, v] = u^{2^{n+1}}$$

and $\langle x^2\rangle \ntrianglelefteq U$.

We have established that $\ell \geq m$. Letting $y = vw^{-2^{\ell-m}}$, we find that

$$y^{2^m} = v^{2^m} w^{-2^\ell} [w, v]^{2^{\ell-m}\binom{2^m}{2}} \in \langle u^{2^{n+\ell-1}}\rangle.$$

So $y^{2^m} = 1$ unless $\ell = 2 = m$. Now $n \geq 2$ implies $[u^{2^{n-1}}, v]^2 = 1$. Hence if $\ell = 2 = m$, then $(vw^{-1}u^{2^{n-1}})^4 = (u^{2^{n+1}})^2 = 1$. Accordingly, $v\langle u\rangle = x\langle u\rangle$ with $o(x) = 2^m$ and $\langle x\rangle \cap \langle u\rangle = 1$. However, $[v^2, u] \neq 1$ yields $\langle x^2\rangle \ntrianglelefteq U$. □

Notation. As usual, "$\lessdot$" denotes "maximal subgroup of" and $d(P)$ the minimal number of generators of the p-group P.

Observe that the core-p-ness of a p-group G is already guaranteed if $|H : H_G| \leq p$ is required for all subgroups of G generated by (no more than) two elements. Indeed, suppose $|\langle x, y\rangle : \langle x, y\rangle_G| \leq p$ for all elements x, y of the p-group G. This property carries over to subgroups and quotients. Let $Q \leq G$ and let $\overline{G} = G/Q_G$. Subgroups of $\overline{Q}$ are core-free, and if $|\overline{Q}| > p$, then $\overline{Q}$ has a 2-generated subgroup of order greater than p, a contradiction. Another equivalent characterisation of core-p-ness may be found in [3, Lemma 1.3]: The group G enjoys core-p-ness if and only if every nontrivial subgroup H of G has a maximal subgroup M with $[M, G] \leq \Phi(H)$.

For the remainder of this paper, p is a prime and G denotes a finite core-p p-group of order greater than p. The equivalent formulation of core-p-ness of a p-group predominantly used in the proofs to come is a mixture of the two characterisations given in the previous paragraph: Every nontrivial subgroup of a core-p p-group generated by two elements has a maximal subgroup that is normal in the group.

Observe that $\langle x^p \rangle \lhd G$ whenever $x \in G$ and that $|E : E \cap Z(G)| \leq p$ for each elementary abelian subgroup E of G.

Notation. Let $p = 2$. For and $y \in G \setminus \{1\}$, the involution in $\langle y \rangle$ is denoted by $\hat{y}$.

Although our theorem only concerns the prime 2, a few lemmas in this section will be stated for all primes. This was done where it would not increase the length of the respective proof inordinately and it was felt that the information contained in the lemma could be of some interest beyond the requirements of the present paper.

Lemma 2.6. *Let A be an abelian normal subgroup of G such that $[A, G] \leq \Omega_1(Z(G))$ and not every subgroup of A is normal in G. Let p^k be the minimal order of a cyclic subgroup of A that is not a normal subgroup of G. Then $\Omega_{k-1}(A) \leq Z(G)$.*

Proof. Let a be any element of A of order p^k and let $z \in \Omega_{k-1}(A)$. Let $\langle t \rangle$ be a complement of $\langle a \rangle$ in $\langle a, z \rangle$. Note that $o(t) < p^k$. There is $a^* \in \langle a^p \rangle$ satisfying $o(a^*) = o(t)$. Both $\langle t \rangle$ and $\langle a^* t \rangle$ are normal in G, while $a^* \in Z(G)$. Thus $t \in Z(G)$, i.e. $z \in \langle a^p, t \rangle \leq Z(G)$. □

Lemma 2.7. *Assume $|G'| = p$. Then $|G : Z(G)| = p^2$ unless $p = 2$, $\exp G = 4$ and $G = UV \times E$, where E is elementary abelian, $[U, V] = 1$, $V \cong Q_8$, and $U = \langle u, v \rangle$ with $\langle [u, v] \rangle = G'$, $v^2 = 1$ and $\langle u^2 \rangle \neq G'$.*

Proof. The commutator map induces a symplectic form on $G/\Phi(G)$, whence $G/Z(G)$ is elementary abelian of even degree. Let $\exp G = p^n$.

Assume that p is odd. If $n = 1$, then G is a direct product $Q \times E$ with Q extraspecial and E elementary abelian. Letting $|Q| = p^{2m+1}$, m is the degree of a maximal elementary abelian core-free subgroup of Q, i.e. $m = 1$.

Now assume $n > 1$. If $\Phi(P)$ is noncyclic, then there is $1 \neq s \in \Omega_1(Z(P))$ such that $Z(P/\langle s \rangle) = Z(P/\langle s \rangle)$ and the theorem follows by induction. Hence $\Phi(P)$ may be supposed to be cyclic. There is $x \in G \setminus Z(G)$ of order p^n. Since $n > 1$, $\exp \Phi(P) = p^{n-1}$, so $\Phi(P) = \langle x^p \rangle$. Since p is odd, raising elements to their pth power is an endomorphism of G, such that $G = \langle x \rangle \Omega_1(G)$ and $\exp \Omega_1(G) = p$. Hence there is $t \in G$ with $t^p = 1 \neq [x, t]$. Let $Q = C_G(\langle x, t \rangle)$, noting that $G = \langle x, t \rangle Q$. For $u \in \Omega_1(Q) \setminus Z(Q)$, $\langle t, u \rangle$ is core-free elementary abelian of order p^2. Thus $v^p \notin \langle x^{p^2} \rangle$ whenever $v \in Q \setminus Z(Q)$. Yet if $v \in Q$ satisfies $o(v) = o(x)$, then $\Phi(G) = \langle v^p \rangle$ and $Q = \langle v \rangle Q_1$ with $\exp Q_1 = p$, i.e. $Q_1 \leq Z(Q)$. Since Q/Q_1 is cyclic, Q is abelian after all.

Now let $p = 2$, let $G' = \langle z \rangle$ and let $x \in G \setminus Z(G)$ have order 2^n.

We first prove the lemma making the additional assumption that $\Phi(G)$ is cyclic. Then $\Phi(G)$ is a cyclic group generated by elements of order at most 2^{n-1}, i.e. $\Phi(G) = \langle x^2 \rangle$. Let $y \in G \setminus C_G(x)$ and $Q = C_G(\langle x, y \rangle)$, observing that $G = \langle x, y \rangle Q$ and $Q \leq Z(G)$ if and only if Q is abelian.

Assume that $n \geq 3$. For each $v \in G$, there is a generator w of $\langle x \rangle$ such that $v^2 = w^{2^\ell}$ with some $\ell \geq 1$. Either $(vw^{-2^{\ell-1}})^2 = 1$, or $\ell = 1$, $[v, x] \neq 1$ and $(vw^{-1}x^{2^{n-2}})^2 = 1$. In particular, y may be chosen of order 2. Assume that Q is nonabelian. If $\exp Q = 2^n$, then an analogous argument yields an involution s in $Q \setminus Z(Q)$. However, this would mean $\langle s, y \rangle_G = 1$. Thus $\exp Q < 2^n$ and, for $u \in Q$, we have $u^2 \in \langle x^4 \rangle$ and there is an involution s_u satisfying $u\langle x^2 \rangle = s_u \langle x^2 \rangle$. If $u \in Q \setminus Z(G)$, then $s_u \notin Z(Q)$ and $\langle s_u, y \rangle_G = 1$.

We turn to the case $n = 2$. Then $G = D * E$ with D extraspecial and E abelian. The group $D_8 * D_8$ is not core-2, whence either $|G : Z(G)| = 4$ or $D \cong D_8 * Q_8$ and E is elementary abelian, a scenario covered by the assertion.

From now on, $\Phi(G)$ is assumed to be noncyclic; observe this implies that $|\Omega_1(Z(G))| > 2$. Let $\Omega_1(Z(G)) = N$ and $s \in N \setminus \langle z \rangle$. Then $Z(G/\langle s \rangle) = Z(G)/\langle s \rangle$, and $|G : Z(G)| \in \{4, 16\}$ is immediate by induction on the group order. Induction also yields that if $|G : Z(G)| = 16$, then $\mho_2(G) \leq \langle s \rangle$ whenever $s \in N \setminus \langle z \rangle$. Thus $|G : Z(G)| = 16$ implies $\exp G = 4$.

Now assume that $\exp G = 4$, $|G : Z(G)| = 16$ and $d(\Phi(G)) \geq 2$. Let

$$S = \{s \in G \mid s^2 \in \langle z \rangle\}.$$

Then $S < G$, in particular $G \neq S \cup Z(G)$. Let $u \in G \setminus Z(G)$ with $u^2 \notin \langle z \rangle$, let $t \in G \setminus C_G(u)$ and let $C_G(\langle u, t \rangle) = Q$.

For $q \in Q \setminus Z(Q)$ and $r \in \{u, t, ut\}$, $\langle q, r \rangle$ is an abelian subgroup of G with $z \in \langle q^2, r^2 \rangle$. Suppose that $|\langle u^2, t^2, z \rangle| = 8$. If $q \in Q \setminus Z(Q)$, then $\langle q^2 \rangle = \langle q^2, t \rangle \cap \langle q^2, u \rangle = \langle z \rangle$. Consequently, we have $Q = \langle x, y \rangle \times E$ with E elementary abelian, $\langle x, y \rangle \cong Q_8$, and $x^2 = y^2 = z$. Now let $W = \langle ux, ty \rangle$. Then $W \cong C_4 \times C_4$ and $W \cap Z(G) = \Phi(W) = \langle u^2 z, u^2 t^2 \rangle \not\ni z$, so $W_G = \Phi(W)$.

We have seen that $\langle u^2, t^2 \rangle \leq \langle u^2, z \rangle$ whenever $t \in G \setminus C_G(u)$. We shall show that $\Omega_1(G) \not\leq Z(G)$. Assume otherwise. Let $t \in G \setminus C_G(u)$. If $t^2 = u^2 z$, then $(ut)^2 = 1$, so $t^2 \in \{u^2, z\}$. Since $\langle G \setminus C_G(u) \rangle = G > S$, it follows that t may be assumed to satisfy $t^2 = u^2$. Let $Q = C_G(\langle u, t \rangle)$ and $q \in Q \setminus Z(Q)$. Then $tq \notin C_G(u)$, while $(tq)^2 = u^2$ would imply $q^2 = 1$. Hence we have $(tq)^2 = z$, i.e. $q^2 = u^2 z$. Now let $q' \in Q \setminus C_Q(q)$. Then $(q')^2 = u^2 z = (qq')^2 = z$, a contradiction.

We have confirmed the existence of an involution v in the set $G \setminus Z(G)$. Since $G \neq S \cup C_G(v)$, the element u may be assumed to satisfy $[u, v] = z$. Let $U = \langle u, v\rangle$ and let $Q = C_G(U)$. For $w \in Q \setminus Z(Q)$, $z \in \langle w, v\rangle$, so $Q = V \times E$ with $V \cong Q_8$ and elementary abelian E. This completes the proof. □

Notation. The elementary abelian group of order p^m will, as usual, be denoted by E_{p^m}.

Let $U \lhd G$ and $x \in G$. Following [8], we define $b_U(x)$, the *breadth of x in U*, as $b_U(x) = \log_p |U : C_U(x)|$. We write $b(x)$ instead of $b_G(x)$. The breadth $b(A)$ in G of the subgroup A is defined as $\max\{b(a) | a \in A\}$.

Let $N = \Omega_1(Z(G))$. For a subgroup U of N, let D_U be the preimage of $Z(G/U)$ in G.

Lemma 2.8. *Suppose that $p = 2$ and $G' \leq N$. Then $|G : D_U| \in \{2^4, 2^2, 1\}$ for $U \lessdot N$. For any subgroup W of N such that $|N : W| = 4$ and $WG' = N$, there is at most one maximal subgroup M of N with $W \subset M$ and $|G : D_M| = 2^4$.*

Proof. The first assertion is a straightforward application of Lemma 2.7 applied to G/M, where $M \lessdot N$.

For the second assertion, let $|G/N| = 2^n$ and let $W \leq N$ with $|N/W| = 4$ and $N = WG'$. Note that W is contained in exactly three maximal subgroups of N.

Let M be a maximal subgroup of N with $|G : D_M| = 2^4$. Let $G/M = X$ and let $X' = \langle z\rangle$. By Lemma 2.7, $\mho_2(G) \leq M$ and $|\Phi(G)N/N| \leq 2$. Assume that $\Phi(G) \not\leq N$. By Lemma 2.7, $X = UV \times E$, where $E \cong E_{2^{n-5}}$, $V \cong Q_8$ and $U = \langle u, v\rangle$ with $u^2 \notin \Phi(V)$ and $v^2 = 1$. Letting $u^2 = s$ and $V = \langle x, y\rangle$, we have $\Omega_1(UV) = \langle z, s, v\rangle \cong E_8$. Accordingly, $j(X) = 2^{n-2}$. Certainly $j(G/M) < 2^{n+1}$ for any maximal subgroup M of N not containing G'. So if $|G : D_M| = 16$ for at least two maximal subgroups of N containing W, then

$$\sum_{W<M\lessdot N} j(G/M) < 2^{n-1} + 2^{n+1} < 3 \cdot 2^n = 3|G/N|,$$

which Blackburn's formula (Lemma 2.2) makes impossible. Thus $\Phi(G) \leq N$.

We note: For $4 \leq n \in \mathbb{N}$, $j(Q_8 * D_8 \times E_{2^{n-4}}) = 3 \cdot 2^{n-2}$, $j(D_8 \times E_{2^{n-2}}) = 3 \cdot 2^{n-1}$, $j(Q_8 \times E_{2^{n-2}}) = 2^{n-1}$, and $j(Q_8 * C_4 \times E_{2^{n-3}}) = 2^n$.

Let $M \lessdot N$. From Lemma 2.7 and $\Phi(G) = 16$, we deduce that $|G : D_M| = 16$ if and only if $G/M \cong Q_8 * D_8 \times E_{2^{n-4}}$. From $\Phi(G) \leq N$ it also follows that, if $M \lessdot N$ satisfies $|G : D_M| = 4$, then G/M is isomorphic to one of the groups $D_8 \times E_{2^{n-2}}$, $Q_8 \times E_{2^{n-2}}$, or $Q_8 * C_4 \times E_{2^{n-3}}$. Suppose that $|G : D_M| = 16$ for at least two maximal subgroups M containing W. Then, as we have seen,

$$\sum_{W<M\lessdot N} j(G/M) \leq 3 \cdot 2^n = 3|G/N|.$$

However, $j(G/W) > 0$, and Blackburn's formula is good for another contradiction. □

The assertions of the next lemma, describing finite core-p p-groups G with $\Phi(G) \subseteq Z(G)$, are partly contained in [3, Theorem 1] and [5, Theorem]. We shall, however, require more detail than is provided in the referenced sources.

Lemma 2.9. *Suppose that $G' \leq N$. Let A be an abelian subgroup of G of maximal order. Then the following hold:*

- *If p is odd, then $|G : A| \leq p^2$ and if $|G : A| = p^2$, then $|A : Z(G)| = p$.*
- *If $p = 2$, then either $|G : A| \leq 2$ or $|G : A| = 4 \geq |A : Z(G)|$. If $|A : Z(G)| = 4$, then $A = \langle c, d\rangle Z(G)$ with $b(c) = b(d) = 1$, in particular $|[A, G]| \leq 4$.*
- *If $p = 2$ and $\Omega_2(A) \leq Z(G)$, then $|G : A| \leq 2$ or $|A : Z(G)| \leq 2$.*

Proof. Note that $Z(G) \geq \Phi(G) \leq A \trianglelefteq G$.

We start with the case p odd. Let $[A, G] = W$ of order p^n, and let $A/Z(G) = V$ of order p^m. For any maximal subgroup U of W, there is a maximal subgroup U_1 of N satisfying $U_1 \cap W = U$. Applying Lemma 2.7 to the quotient G/U_1, we obtain $|A/U : (A/U \cap Z(G/U))| = p$. Note that this implies that $m \leq n$.

Let $\mathcal{S}$ be the set of pairs $(\langle v\rangle, U)$, where $1 \neq v \in V$, $U \lessdot W$ and $v = aZ(G)$ with $a \in A$ and $[a, G] \leq U$. Let $r = \frac{p^m-1}{p-1}$. We list the subgroups of V of order p as $\langle v_1\rangle, \dots \langle v_r\rangle$. For $i \in 1, \dots, r$, let $v_i = a_i Z(G)$ and let $p^{\ell_i} = |[G, a_i]|$. We assume the v_i listed as to satisfy $\ell_i \geq \ell_{i+1}$ for all i. We count the elements of $\mathcal{S}$ in two ways, to obtain

$$|\mathcal{S}| = \frac{1}{(p-1)^2}(p^n - 1)(p^{m-1} - 1) = \frac{1}{p-1}\sum_{i=1}^{r}(p^{n-\ell_i} - 1),$$

i.e.

$$\sum_{i=1}^{r}(p^{n-\ell_i} - 1) = \frac{1}{p-1}(p^n - 1)(p^{m-1} - 1).$$

Observe that

$$\frac{1}{p-1}(p^n - 1)(p^{m-1} - 1) = \frac{1}{p-1}(p^{n-1} - 1)(p^m - 1) - p^{n-1} + p^{m-1}.$$

Suppose that $\ell_2 > 1$. Then

$$\sum_{i=1}^{r}(p^{n-\ell_i} - 1) \leq \frac{1}{p-1}(p^{n-1} - 1)(p^m - 1) - 2p^{n-1} + p^{n-\ell_1} + p^{n-\ell_2}.$$

However, $p^{n-1} > 2p^{n-2} \geq p^{n-\ell_1} + p^{n-\ell_2}$, whence

$$-2p^{n-1}+p^{n-\ell_1}+p^{n-\ell_2}+p^{n-1}-p^{m-1} = -p^{n-1}+p^{n-\ell_1}+p^{n-\ell_2}-p^{m-1} < 0,$$

a contradiction.

We have established that either $b(A) = 1$ or there is $a \in A$ such that $\langle a, Z(G)\rangle$ contains every element of A of breadth greater than 1. Assume the latter together with $m \geq 2$. Let $b \in A \setminus \langle a\rangle Z(G)$. Then

$$b(b) = b(ab) = 1,$$

and $[a, G] = [b, G]\times[ab, G]$, while $C_G(b)C_G(ab) = G$. Let $x \in C_G(b)\setminus C_G(ab)$ and $y \in C_G(ab) \setminus C_G(b)$. Then $[ab^2, x] = [ab, x]$ and $[ab^2, y] = [b, y]$, i.e. $[a, G] = \langle[ab, x]\rangle \times \langle[b, y]\rangle = [ab^2, G]$, a contradiction. Thus $|A : Z(G)| = p$ or $b(A) = 1$.

Now let $p = 2$. Suppose that A has a subgroup $\langle a, b\rangle$ such that $|\langle a, b\rangle : \langle a, b\rangle \cap Z(G)| = 4$ and $b(a) \geq 2 \leq b(b)$. First suppose that there are subgroups $\langle s, t\rangle$ of $[G, a]$ and $\langle s', t'\rangle$ of $[G, b]$ such that $|\langle s, t\rangle\langle s', t'\rangle| = 16$. Let $U = \langle s, t, s', t'\rangle$ and let V be a complement of U in N. Let $X_1 = \langle ss', tt'\rangle$, $X_2 = \langle ss', ts't'\rangle$, and $X_3 = \langle st', s't\rangle$. For $i = 1, 2, 3$, let $W_i = V \times X_i$. For each index i, we have $U = \langle s, t\rangle \times X_i = \langle s', t'\rangle \times X_i$, while $X_1 \cap X_2 \cap X_3 = 1$ and $W_1 \cap W_2 \cap W_3 = V$. Let $i \in \{1, 2, 3\}$. Let $W_i \leq X \lessdot N$; then neither a nor b belongs to D_X. Now Lemma 2.8 may be invoked to yield that $ab \in D_X$ for at least two out of three different choices of X; thus

$$[ab, G] \leq W_1 \cap W_2 \cap W_3 = V.$$

The intersection over all complements of U in N being trivial, we obtain that $ab \in Z(G)$ in contrast to our assumptions on $\langle a, b\rangle$. If $[a, G] \cap [b, G]$ has a subgroup U of order 4, then, similarly, $[ab, G] \leq V$ whenever $N = U \times V$, which results in $ab \in Z(G)$. The only remaining possibility is that $|[a, G]| = |[b, G]| = 4$, while $|[a, G] \cap [b, G]| = 2$; let $[a, G] = \langle s, t\rangle$ and $[b, G] = \langle s, t'\rangle$, $U = \langle s, t, t'\rangle$, $N = U \times V$, $W_1 = V\langle tt'\rangle$, $W_2 = V\langle tst'\rangle$. Lemma 2.8 again yields

$$[ab, G] \leq W_1 \cap W_2 = V$$

and a contradiction ensues as before.

Suppose that A has an element a of breadth greater than 1. As seen in the two preceding paragraphs, this implies that $A = \langle a\rangle B$, where $Z(G) \leq B$ and $b(b) = b(ab) = 1$ for every b in B that satisfies $|\langle b, a\rangle Z(G) : Z(G)| = 4$. In particular, $b(B) \leq 1$.

Assume that $B \neq Z(G)$. Applying Lemma 2.4, we obtain $|[B, G]| = 2$ or $|G : C_G(B)| = 2$. For b in $B \setminus Z(G)$, we have $[a, G] \leq [b, G][ab, G]$, which implies $[a, G] = [b, G] \times [ab, G]$ and $C_G(a) = C_G(b) \cap C_G(ab)$.

Suppose that $|[B, G]| = 2$. If $|B : Z(G)| > 2$, then there are b and c in B with $G = C_G(b)C_G(c)$. Note that

$$G = C_G(b)C_G(bc) = C_G(c)C_G(bc).$$

For $d \in \{b, c, bc\}$, we have $[ad, G] = [a, C_G(d)]$ because of $[C_G(d), a] \neq 1$ and $b(ad) = 1$. Furthermore, $[ad, G]$ is a complement of $[B, G]$ in $[a, G]$. Since there are only two such complements, b and c may be chosen such that $[ab, G] = [ac, G]$. However, this yields $[bc, G] = [B, G] = [b, G] = [ab, G]$, a contradiction. Consequently, $|[B, G]| = 2$ entails that $A = \langle a, b\rangle$ with $b(b) = 1 = b(ab)$, while $C_G(a) = C_G(b) \cap C_G(ab) = C_G(A) = A$, i.e. $|G : A| = 4$.

We turn to the case $|G : C_G(B)| = 2$. Let $b \in B \setminus Z(G)$. We have $C_G(B) = C_G(b)$ and $G = C_G(b)C_G(ab)$. Letting $x \in C_G(B) \setminus C_G(a)$, we find that

$$\langle [x, a]\rangle = \langle [x, ab]\rangle = [G, ab].$$

Given $b, c \in B$ with $|[G, \langle b, c\rangle]| = 4$, we obtain that $[G, ab] = [G, abc] = [G, c]$, a contradiction. Accordingly, $|B : Z(G)| = 2$ and if $B = \langle b\rangle Z(G)$, then once again $C_G(ab) \cap C_G(b) = C_G(a) = C_G(A) = A$, i.e. $|G : A| = 4$.

Letting p be any prime, assume $|A : Z(G)| = p$. Let $A = \langle a\rangle Z(G)$, i.e. $b(a) = \log_p |G : A|$. It will suffice to derive a contradiction from $|G : A| = p^3$. For $x \in G \setminus A$, the maximality of $|A|$ implies that $C_G(x) = \langle Z(G), x\rangle$ is a maximal abelian subgroup of G. Let $x \in G \setminus Z(G)$ and let $y \in G \setminus Z(G)\langle x\rangle$. One of the maximal subgroups of $\langle x, y\rangle$ is normal in G, say $\langle x, y^p, [x, y]\rangle$. Since $\Phi(\langle x, y\rangle) = \langle x^p, y^p, [x, y]\rangle$, i.e. $d(\Phi(\langle x, y\rangle)) \leq 3$, we must have $[x, G] = \Omega_1(\Phi(\langle x, y\rangle))$. If $o(x) = p$, then $\Phi(\langle x, y\rangle) = \langle y^p, [x, y]\rangle$, so $o(x) > p$ and $\Omega_1(\langle x\rangle) \leq [x, G]$. It follows that there is $v \in G \setminus \langle x, Z(G)\rangle$ with $\langle [v, x]\rangle = \Omega_1(\langle x\rangle)$. This implies that $\Phi(\langle v, x\rangle) = \langle v^p\rangle\langle x^p\rangle$ and there is $w \in \langle v, x\rangle \setminus Z(G)$ with $[w, G] \leq \Phi(\langle v, x\rangle)$, a contradiction.

The final case left for us to consider is $b(A) = 1$. Then Lemma 2.4 yields $|[G, A]| = p$ or $|G : C_G(A)| = |G : A| = p$. Only the first case needs further consideration. Let $[G, A] = \langle z\rangle$, of order p. We note that for $U \leq A$ we have $z \in U$ or $|U : U \cap Z(G)| \leq p$. Let $A = \langle a_1\rangle \times \cdots \times \langle a_n\rangle$, where z projects nontrivially into $\langle a_1\rangle$ along the given decomposition. Let $\tilde{B} = \langle a_2\rangle \ldots \langle a_n\rangle$. Then $|\tilde{B} : \tilde{B} \cap Z(G)| \leq p$; however, this implies that $A = \langle a\rangle Z(G)$ and $|G : A| = p$ or $A = \langle a, b\rangle Z(G)$ with $A = C_G(a) \cap C_G(b)$, i.e. $|G : A| = p^2$.

At this point, only the final assertion of the lemma has not been taken care of. By way of contradiction, assume that $p = 2$, $\Omega_2(A) \leq Z(G)$ and $|G : A| = 4 = |A : Z(G)|$. Recall that $|[A, G]| \leq 4$.

Let D be a subgroup of $Z(G)$ of maximal order subject to possessing a complement in A and let $A = D \times E$. Setting $E = \langle a_1\rangle \times \ldots \times \langle a_n\rangle$, either $n = 2$, or some c of the form $c = \prod_{i=1}^{n} a_i^{\varepsilon_i}$ with $\varepsilon_i \in \{0,1\}$ belongs to $Z(G)$. For such a c, $\langle c \rangle$ has a complement in E, whence $\langle c \rangle D$ has a complement in G. It follows that $n = 2$ and $A = D \times \langle a \rangle \times \langle b \rangle$ with $D \leq Z(G)$. Note that $o(a) \geq 8 \leq o(b)$.

The following observation is going to be quite helpful: Suppose there is $z \in N \setminus [A,G]$ such that $\Omega_2(A/\langle z \rangle) \leq Z(G)/\langle z \rangle$. Since $Z(G/\langle z \rangle) \cap A/\langle z \rangle = Z(G)/\langle z \rangle$, induction yields that $|A : Z(G)| = 2$ or there is a maximal subgroup B of G with $B' \leq \langle z \rangle$. However, $[B, A \cap B] = 1$, whence $BA = G$ and $A \cap B = Z(G) \lessdot A$.

(∗) Let $z \in N \setminus [A,G]$. Then $\Omega_2(A/\langle z \rangle) \not\leq Z(G)/\langle z \rangle$.

Suppose that $[A,G] \leq \langle \hat{a}, \hat{b} \rangle$. Let $z \in \Omega_1(D)$. Any $d \in A$ satisfying $d^4 = z$ then belongs to $D\langle a^2, b^2 \rangle \leq Z(G)$, and (∗) yields $D = 1$.

Assume that $|[A,G]| = 2$. Since there is $c \in \{a, b, ab\}$ with $[c,G] \leq \langle \hat{a}, \hat{b} \rangle$, this implies that $[A,G] \leq \langle \hat{a}, \hat{b} \rangle$. As we just saw, this means $A = \langle a, b \rangle$, in particular $Z(G) = \Phi(A)$. Let $w \in G \setminus A$. There is $c \in A$ satisfying $w^2 = c^2$, i.e. $(wc^{-1})^2 = [w,c]$. Since $o(a) \geq 8 \leq o(b)$, $[w,c] \in \Phi(Z(G))$ and the coset wA contains an involution. Letting $[A,G] = \langle s \rangle$, it follows that $G = A\langle x, y \rangle$ with involutions x and y satisfying $[a,x] = 1$, $[b,y] = s$, $[a,y] = s$, and $[b,y] = 1$. Now $[x,y] \neq 1$, for none of the elements x, y, xy is in $Z(G)$. Accordingly, we have $\langle x, y \rangle \cong D_8$, and, since a maximal subgroup of $\langle x, y \rangle$ is normal in G, we must have $[x,y] = s$. This implies $G' = \langle s \rangle$ and Lemma 2.7 delivers a contradiction. So $|[A,G]| = 4$.

Assume that $G' = [A,G]$. For $1 \neq v \in G'$, let A_v be the preimage of $Z(G/\langle v \rangle) \cap A/\langle v \rangle$ in A. Since $\exp G/\langle v \rangle > 4$, Lemma 2.7 yields $|A : A_v| = 2$ for each v. Since $|A : Z(G)| = 4$, $A_v \neq A_{v'}$ whenever $\langle v, v' \rangle = G'$, and it follows that each of the three maximal subgroups of A that contain $Z(G)$ is equal to some A_v, i.e. $b(A) = 1$. Now Lemma 2.4 yields $|G : C_G(A)| = 2 = |G : A|$, a contradiction.

We have found that $G' \neq [A,G]$. In particular, $A > \langle a, b \rangle$, which we have seen to imply $[A,G] \neq \langle \hat{a}, \hat{b} \rangle$. Write $D = \langle d \rangle \times E$ with $[A,G] \not\leq \langle a, b \rangle E$. If $1 \neq z \in \Omega_1(E)$, then $\Omega_2(A/\langle z \rangle) \leq Z(G)/\langle z \rangle$. As previously mentioned, there is an element $c \in \{a, b, ab\}$ with $1 \neq [G,c] \leq \langle \hat{a}, \hat{b} \rangle$. Since $|[A,G]| = 4$, it follows that $z \notin [A,G]$, and (∗) is contradicted. Thus $E = 1$, and since $[A,G] < G'$, we have $G' = \Omega_1(\Phi(G)) = \langle \hat{a}, \hat{b}, \hat{d} \rangle$.

Suppose that $o(d) = 4$. There is an element $t \in \langle \hat{a}, \hat{b} \rangle$ satisfying $td^2 \notin [A,G]$. Since $td^2 \notin \mho_2(A) = \langle \hat{a}, \hat{b} \rangle$, condition (∗) yields a contradiction. Hence $o(d) \geq 8$ and $N \leq \mho_2(G)$.

Let $V \lessdot G'$. We have seen that $\exp G/V \geq 8$, and Lemma 2.7 says that the subgroup $A/V \cap Z(G/V)$ is of index at most 2 in A/V. Only two of the three elements a, b, ab have breadth 1 in G, so there is an element $s \in [A,G]$ with

$Z(G/\langle s\rangle)\cap A/\langle s\rangle = Z(G)/\langle s\rangle$. Letting $t \in G' \setminus [A, G]$ and $V = \langle s, t\rangle$, we obtain a final contradiction. □

The following three auxiliary lemmas each dispense with some scenario that makes repeated appearances during coming proofs.

Lemma 2.10. *Let P be a finite 2-group having a maximal abelian normal subgroup $B = \langle a\rangle \times \langle b\rangle \times \langle d\rangle \times E$. If*

(a) $o(a) = 2$, $o(b) \geq 4 \leq o(d)$, $o(b) > \exp E < o(d)$,

(b) $E \leq Z(P)$, $\Phi(P) \leq B$, $[P, B] \leq \Omega_1(Z(P))$,

(c) $b(a) = 1$ *and* $\langle b\rangle \lhd P \rhd \langle d\rangle$,

(d) $|P : B| = 8$,

then P is not core-2.

Proof. Assume otherwise. The four conditions (a)–(d) entail $Z(P) = \Phi(B)E$ and $P = \langle u, v, w\rangle B$ with $[u, a] = [u, d] = 1$, $[u, b] = \hat{b}$, $[v, a] = [v, d] = 1$, $[v, d] = \hat{d}$, and $[w, b] = [w, d] = 1 \neq [w, a]$. Without loss, $o(b) \geq o(d)$. Neither of the subgroups $\langle bd\rangle$ and $\langle abd\rangle$ being normal in P, so $\langle a, (bd)^2\rangle$ is, consequently,

$$[a, w] = \hat{b} \qquad \text{if } o(b) > o(d),$$
$$[a, w] = \hat{b}\hat{d} \quad \text{if } o(w) = o(d) \text{, in particular } [B, P] = \langle \hat{b}, \hat{d}\rangle. \tag{2.1}$$

For $z \in \Omega_1(Z(P)) \setminus \langle \hat{b}, \hat{d}\rangle$, $P/\langle z\rangle$ therefore satisfies (a)–(d) and induction yields a contradiction. Accordingly,

$$\Omega_1(Z(P)) = \langle \hat{b}, \hat{d}\rangle. \tag{2.2}$$

Since E is a complement of $\langle a, b, d\rangle$ in B and contained in $Z(P)$, condition (2.2) yields $B = \langle a, b, d\rangle$. Note that $u^2 \neq 1$, for $\langle u, a\rangle_P = 1$ otherwise. Certainly $u^2 \in C_B(u) = \langle a, b^2, d\rangle$. Set $u^2 = a^i b^{2j} d^\ell$.

Assume that $o(b) > o(d)$. It follows that $o(b) > 4$ and there is $b^* \in \langle b\rangle$ such that $(ub^*)^2 = a^i d^\ell$. Replace u by ub^*. If both i and ℓ are odd, then $[u^2, w] = \hat{b}$ and $[u^2, v] = \hat{d}$, i.e. $\langle u^2\rangle \ntriangleleft P$. If i is odd and ℓ is not, then $u\langle d\rangle$ has an element whose square is a, making $\langle a\rangle$ normal in P, which it is not. Accordingly, we may take $u^2 \in \langle d\rangle$. Since $[u, b] = [ua, b] = [a, w] = \hat{b}$, none of the maximal subgroups of $\langle u, a\rangle$ is normal in P. This proves

$$o(b) = o(d). \tag{2.3}$$

If i is odd, then (2.1) yields that $[u^2, w] = \hat{b}\hat{d}$, i.e. ℓ must be even; yet that implies there is $s \in u\langle d\rangle$ with $s^2 \in a\langle b\rangle$, i.e. $[s^2, w] \notin \langle s^2\rangle$. Hence $u^2 = b^{2j} d^\ell$.

If $o(b) > 4$ or j is even, then there is $s \in u\langle b\rangle$ satisfying $s^2 \in \langle d\rangle$, and none of the maximal subgroups of $\langle a, s\rangle$ is normal in P.

The only possibility left standing is $o(b) = o(d) = 4$ and $u^2 = b^2 d^\ell$. If ℓ is odd, then, as before, $\langle u, a\rangle_P = \langle u^2\rangle$, so, replacing u by an appropriate element of $u\langle d\rangle$, we obtain $u^2 = b^2$. Since this means $\langle u^2, a\rangle \ntriangleleft P$, one of $\langle ua\rangle$ and $\langle u\rangle$ is normal and there is no loss in taking $\langle u\rangle \lhd P$. By (2.3), the situation under consideration is symmetric in b and d, so we may also assume $v^2 = d^2$ and $\langle v\rangle \lhd P$. Let $Q = \langle u, b, v, d\rangle$. Then $Q \cong Q_8 \times Q_8$ and $\langle uv, bd\rangle_Q = \langle b^2 d^2\rangle$, a final contradiction. □

Lemma 2.11. *Let P be a finite 2-group with a normal subgroup Q such that the following conditions are satisfied:*

(a) $Q' = \Omega_1(Q) = \Omega_1(Z(P))$.

(b) $Q = \langle x_1\rangle\langle x_2\rangle\langle x_3\rangle$, *where* $o(x_1) \geq o(x_2) \geq 8$ *and* $o(x_2) \geq o(x_3) \geq 4$, *while* $\langle x_1\rangle \cap \langle x_2\rangle = \langle x_1\rangle\langle x_2\rangle \cap \langle x_3\rangle = 1$.

(c) $P = Q\langle x\rangle$ *with* $u^x \in u^{-1}\Omega_1(Q)$ *for* $u \in Q$.

(d) $[\Omega_1(Q\Phi(P)), Q] = 1$.

Then P is not core-2.

Proof. It will be helpful to be aware of the fact that $(uv)^{2^\ell} = u^{2^\ell} v^{2^\ell}$ whenever $u, v \in Q$ and $\ell \geq 2$. Let $Y = \Omega_1(Q)$. Combining conditions (a) and (b), we see that $\Phi(Q) = \langle x_1^2\rangle \times \langle x_2^2\rangle \times \langle x_3^2\rangle$, while $Q' = Y = \langle [a,b], [a,c], [b,c]\rangle$ whenever $Q = \langle a, b, c\rangle$; in particular $b_Q(u) = 2$ for every $u \in Q \setminus \Phi(Q)$. The condition placed on the orders of the x_i in (b) entails that $Y = \langle \hat{x}_1\rangle \times \langle \hat{x}_2\rangle \times \langle \hat{x}_3\rangle = \{1\} \cup \{\hat{s} | s \in Q \setminus \Phi(Q)\}$. Let $y_1, y_2, y_3 \in Q$. Then (y_1, y_2, y_3) will be called an *admissible triple* if, for $i = 1, 2, 3$, y_i has each of the properties ascribed to x_i in conditions (a) and (b). Note that this implies $o(y_i) = o(x_i)$ for $i = 1, 2, 3$. Next, let $P = Q\langle x\rangle$. By (c), $x^2 \in Z(P)$ and $u^{2x} = u^{-2}$ whenever $u \in Q$, so x inverts every element of the abelian group $\Phi(Q)$. It follows that $\langle x\rangle \cap Q \leq C_{\Phi(Q)}(x) = Y$. Thus condition (a) entails that $o(x) = 2$ or $\hat{x} \in Y$.

Suppose that P is a core-2-group. First assume $o(x) > 4$. Let $\Omega_2(\langle x\rangle) = \langle z\rangle$ and let $a \in Q \setminus \Phi(Q)$ satisfy $\hat{a} = \hat{x}$. If $o(a) = 4$, then $za \in \Omega_1(Q\Phi(P))$, and (d) yields $[Q, a] = 1$, which is not compatible with (a) and (b). Thus $o(a) \geq 8$ and there is an involution s in $z\langle a^2\rangle$. By (d), $[s, Q] = 1$, whence $[s, P] = \langle [s, x]\rangle = \hat{x}$. For $t \in Q \setminus \Phi(Q)$ with $\hat{t} \neq \hat{x}$, we have $\langle s, t\rangle_P \in \{\langle t\rangle, \langle st\rangle\}$; either possibility yields $b_Q(t) \leq 1$, which contradicts $Y = Q'$. Consequently:

(1) $o(x) \leq 4$, in particular $Q \lessdot P$.

For $u \in Q$, let $z_u = u^2[u, x]$, in other words $(ux)^2 = x^2 z_u$. By condition (c),

$\Omega_1(\Phi(\langle u, x\rangle)) = \langle x^2, z_u, \hat{u}\rangle$, while $\Phi(\langle u, x\rangle)Y/Y = \langle u^2\rangle Y/Y$. Let $y \notin Q$. Then it follows from (b) and (c) that $[Q, y]Y/Y$ is abelian of degree at least 2 and neither of the groups $\langle y, u^2, [u, y]\rangle$ and $\langle yu, u^2, [u, y]\rangle$ can be normal in P. Thus:

(2) If $u \in Q \not\ni y$, then $\langle u, y^2, u^2[u, y]\rangle \lhd P$.

We intend to show that $o(x) = 2$. Since x is an arbitrary element of $P \setminus Q$, that will, Q being nonabelian, suffice to establish a contradiction. So let us assume $o(x) = 4$. Let $a \in Q \setminus \Phi(Q)$ satisfy $\hat{a} = x^2$; by condition (2), $[Q, a] = \langle \hat{a}, z_a\rangle$. Let $[Q, a] = W$. Since $b_Q(a) = 2$, we have $Q = \langle a, u_1, u_2\rangle$ with $[u_1, a] = z_a$ and $[u_2, a] = \hat{a}z_a$. For $i \in \{1, 2\}$, $xu_i \in N_P(\langle a\rangle)$, and condition (2) implies that $\langle xu_i, a\rangle_P = \langle a, x^2 z_{u_i}\rangle = \langle a, z_{u_i}\rangle$, while $W = \langle \hat{a}, z_{u_i}\rangle$. Let $u \in u_1\langle a, \Phi(Q)\rangle \cup u_2\langle a, \Phi(Q)\rangle$. Since $Y \cap \langle x, u\rangle \le \langle \hat{a}, z_u, \hat{u}\rangle$ and $[u, Q] \not\le W$, condition (2) yields:

(3) Let $u \in Q\setminus\Phi(Q)$. Unless $u \in N_Q(\langle a\rangle)$, $\hat{u} \notin [a, Q] = \langle x^2, z_a\rangle = \langle x^2, z_u\rangle$.

Every element of Q of order less than $o(x_3)$ belongs to $\Phi(Q)$, so we know $o(a) \ge o(x_3)$. Suppose that $o(a) = o(x_3)$. Then $Q = \langle a\rangle\langle v_1\rangle\langle v_2\rangle$, where $v_1 \notin N_Q(\langle a\rangle)$ and (v_1, v_2, a) is an admissible triple. Suppose that $v_2 \notin N_Q(\langle a\rangle)$. By condition (3) this means that $\hat{v} \notin W$ whenever $v \in v_2\Phi(Q) \cup v_1\Phi(Q)$. Accordingly, $o(v_1) = o(v_2)$, since otherwise some w in $v_2\langle v_1^2\rangle$ would satisfy $\hat{w} = \hat{v}_1\hat{v}_2$. So $v_2 \in N_Q(\langle a\rangle)$ or $o(v_2) = o(v_1)$. If $o(v_2) < o(v_1)$, then there is an element $w \in v_2\langle v_1^2\rangle$ with $\hat{w} \in W$, while of course (v_1, w, a) is admissible. If $o(v_2) = o(v_1)$, then (v_1, v_1v_2, a) is admissible, while, by (3) and because of $\widehat{v_1v_2} = \hat{v}_1\hat{v}_2$, $v_2 \notin N_Q(\langle a\rangle)$ if and only if $\hat{v}_2 \notin W$ if and only if $v_1v_2 \in N_Q(\langle a\rangle)$ if and only if $\widehat{v_1v_2} \in W$.

We have found an admissible triple (v_1, w, a) with $\hat{w} \in W$ and $[w, a] = \hat{a}$. Since $[a, v_1w] = \hat{a}[a, v_1]$ and (v_1w, w, a) is admissible, we may even take $[v_1, a] = z_a$. Recall that $o(w) \ge 8$. From $\langle a, w\rangle_P = \langle a, w^2\rangle$ we get $\hat{w} \ne \hat{a}$. Since $\hat{a} \in [w, Q] \ne W$, it follows that $\hat{w} \notin [w, Q]$. Suppose that $\hat{w} = \hat{a}z_a$. Applying condition (2) with $u = w$ and $y = xa$, we obtain $[w, Q] = \langle \hat{a}z_w, \hat{a}z_a\rangle$, in particular $\hat{w} \in [w, Q]$. Thus the only remaining option is $\hat{w} = z_a$. If $(xv_1)^2 = \hat{w}$ or $(xv_1w)^2 = \hat{w}$, then (2) (with $u = w$ and $y = xv_1$ or xv_1w, respectively) again yields $\hat{w} \in [w, Q] = W$. Since $\{z_{v_1}, z_{v_1w}\} \subseteq \{z_a, \hat{a}z_a\}$, we are forced to conclude that $(xv_1)^2 = \hat{a}z_{v_1} = \hat{a}z_a = (xv_1w)^2 = \hat{a}z_{v_1w}$. It follows that $z_{v_1} = z_{v_1w} = z_a$. Since $z_{v_1w} = z_{v_1}z_w[v_1, w]$, this yields $[v_1, w] = z_w$. Yet now we have $w^{xv_1} = w^{-1}$ and (2) says that $\langle xv_1, w\rangle_P = \langle w, (xv_1)^2\rangle = \langle w, \hat{a}z_a\rangle$. This also implies $[w, Q] = W$.

Thus:

(4) If $a \in Q \setminus \Phi(Q)$ and $\hat{a} = x^2$, then $o(a) > o(x_3)$.

Note that (4) entails $o(x_1) > o(x_3)$. From now on, we take a to be of maximal order subject to $a \in Q \setminus \Phi(Q)$ and $\hat{a} = x^2$. Let $o(a) = 2^\ell$ and write $a = x_1^i x_2^j x_3^k$. It follows from (4) that $\ell > 2$ and

$$\hat{a} = x_1^{2^{\ell-1}i} x_2^{2^{\ell-1}j} x_3^{2^{\ell-1}k} \in \langle \hat{x}_1 \hat{x}_2 \rangle.$$

Hence there is $s \in \langle x_1 \rangle \langle x_2 \rangle$ with $o(a) \leq o(s)$ and $\hat{s} = \hat{a}$. There is thus no loss of generality in assuming $a \in \langle x_1 \rangle \langle x_2 \rangle$.

Now $o(a) \geq 8$ and $\widehat{ar} = \hat{a}$ for all $r \in Q$ of order less than 2^ℓ. This combines with (3) to yield:

(5) If $v \in Q \setminus N_Q(\langle a \rangle)$, then $o(v) \geq o(a)$.

Since $o(x_3) < o(a)$ and $C_Q(a) = \langle a \rangle \Phi(Q) \leq \langle x_1, x_2 \rangle \Phi(Q)$, condition (5) implies that $[x_3, a] = \hat{a}$ and $N_Q(\langle a \rangle) = \langle a, x_3 \rangle \Phi(Q)$.

Suppose that $o(x_2) < o(x_1)$. Then the current restrictions on a entail $\hat{a} = \hat{x}_1$ only if $a \in \langle x_1 \rangle \Phi(Q)$, in particular $o(a) > o(x_2)$. But $x_2 \notin N_Q(\langle a \rangle)$, so this is made impossible by (5). Accordingly, $\hat{a} \in \{\hat{x}_2, \hat{x}_1 \hat{x}_2\}$; since (x_1, y, x_3) is admissible whenever $y \in x_2 \langle x_1^2, x_2^2 \rangle$ satisfies $o(y) = o(x_2)$, we may fix notation such that $a = x_2$. If $o(x_1) = o(x_2)$, then every triple (y_1, y_2, x_3) that satisfies $\langle y_1, y_2 \rangle \Phi(Q) = \langle x_1, x_2 \rangle \Phi(Q)$ is admissible and notation may again be arranged such that $a = x_2$.

Let $W = [a, Q]$ as before. By (3), we have $\hat{x}_1 \notin W$. If $y \in x_3 \langle x_1 \rangle$ satisfies $o(y) = o(x_3)$, then (x_1, x_2, y) is admissible. Thus $\hat{x}_3$ may be assumed to be in W, whence $W = \langle \hat{a}, \hat{x}_3 \rangle$ results. By (3), this implies that $\hat{x}_3 \in \{z_{x_1}, \hat{a} z_{x_1}\}$. Since $o(a) > o(x_3)$, there is $w \in x_3 \langle a^2 \rangle$ with $\hat{w} = \hat{a} z_{x_1}$. Since this means $(x x_1)^2 = \hat{w}$, (1) says that $\langle x x_1, w \rangle_P = \langle w, z_w [x_1, w] \rangle$ and $[w, Q] = \langle \hat{w}, z_w [x_1, w] \rangle$. However, $[a, w] = \hat{a} \neq \hat{w}$ and it follows that $[w, Q] = \langle \hat{w}, \hat{a} \rangle = W$, a contradiction that ends this proof. □

Lemma 2.12. *Let P be a finite 2-group possessing a normal subgroup Q such that the following conditions are satisfied:*

(a) $Q' = \Omega_1(Q) = \Omega_1(Z(P))$.

(b) $|Q'| = 8$.

(c) $Q = \langle x_1, x_2, x_3 \rangle$, *where* $o(x_1) \geq 8$ *and* $o(x_2) = o(x_3) = 4$.

(d) $P = Q\langle x \rangle$, *where* $u^x \in u^{-1} \Omega_1(Q)$ *for* $u \in Q$.

(e) $[Q, \Omega_1(Q\Phi(P))] = 1$.

Then P is not core-2.

Proof. Let $Y = \Omega_1(Q)$, let $o(x_1) = 2^n$ and let $x_1^{2^{n-2}} = z$. Like in the previous proof, a triple (y_1, y_2, y_3) of elements of Q will be called *admissible* whenever (c) continues to be true after replacing x_i by y_i for $i = 1, 2, 3$. Observe that (b) implies $Q' = [u, Q][v, Q]$ whenever $u \in Q \setminus \Phi(Q)$ and $v \in Q \setminus \langle u \rangle \Phi(Q)$, in particular $b_Q(u) = 2$ whenever $u \in Q \setminus \Phi(Q)$. Let $y \in P \setminus Q$. Combining conditions (a) and (d), we obtain $u^y \in u^{-1}Y$, in particular $u^{y^2} = u$ whenever $u \in Q$. Thus $y^2 \in Z(P)$ and (a) implies that $\hat{y} \in Y$ or $o(y) = 2$. Since $Y \leq Z(P)$, we have $\langle x_1 \rangle \cap \langle x_2 \rangle = \langle x_1 \rangle \cap \langle x_3 \rangle = 1$.

Assume that P is core-2. Our first goal is showing that some admissible triple (y_1, y_2, y_3) satisfies $\langle y_3 \rangle \cap (\langle y_1 \rangle \langle y_2 \rangle) = 1$. Assuming that such a triple does not exist, we have $x_3^2 \in \langle x_1 \rangle \langle x_2 \rangle$. Upon replacing x_3 by $x_3 z$ if necessary, we may take $x_3^2 = x_2^2$. If $[x_2, x_3] = x_2^2$, then there is $w \in \{x_2, x_3, x_2 x_3\}$ with $b_Q(w) \leq 1$. If $[x_2, x_3] \notin \langle \hat{x}_1, x_2^2 \rangle$, then $(x_1, x_2, x_2 x_3)$ is an admissible triple endowed with the extra feature we are currently seeking. If $[x_2, x_3] = \hat{x}_1$, then $x_2 x_3 z$ is an involution in $Q \setminus \Phi(Q)$, which leaves $[x_2, x_3] = x_2^2 \hat{x}_1$ the only undiscarded option. Yet that yields $(x_2 x_3)^2 = x_2^2 \hat{x}_1 = (x_2 z)^2 = [x_2 x_3, x_2 z]$; letting $R = \langle x_2 z, x_2 x_3 \rangle$, we have $R \cong Q_8$ with $R \cap \Phi(Q) = \Phi(R)$. One of the three cyclic four-subgroups of R must be normal in P, giving Q an element of breadth 1 and thus clashing with (a). Hence:

(1) Without loss of generality, $\langle x_3 \rangle \cap \langle x_1 \rangle \langle x_2 \rangle = 1$.

Observe that (1) entails $\langle x_k \rangle \cap (\langle x_i \rangle \langle x_j \rangle) = 1$ for $\{i, j, k\} = \{1, 2, 3\}$, while $Y = Q' = \langle \hat{x}_1, x_2^2, x_3^2 \rangle$ and $Q = \langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle$.

Since $\Phi(Q) = \langle x_1^2, x_2^2, x_3^2 \rangle Q' = \langle x_1^2 \rangle Y$, either every element of Y is a square in Q, or $x_2^2 x_3^2$ is not. Assume the latter. If $[x_2, x_3] = \hat{x}_1$, then $x_2^2 x_3^2 = (x_2 x_3 z)^2$ and if $[x_2, x_3] \in x_2^2 x_3^2 \langle \hat{x}_1 \rangle$, then there is an involution in $x_2 x_3 \langle s \rangle$ and condition (a) is contradicted. Accordingly, $[x_2, x_3] \in x_2^2 \langle \hat{x}_1 \rangle \cup x_3^2 \langle \hat{x}_1 \rangle$. Interchanging x_2 and x_3 and replacing x_2 by $x_2 z$ if necessary, we may assume $[x_2, x_3] = x_2^2$. Since $(x_1, x_2, x_2 x_3)$ is admissible and $(x_2 x_3)^2 = x_3^2$, one of the subgroups $\langle x_3, x_2^2 \rangle$ and $\langle x_2, x_3^2 \rangle$ may be taken to be normal. Let $\{i, j\} = \{2, 3\}$ with $\langle x_i, x_j^2 \rangle \lhd P$.

Assume that $o(x) > 4$. By the previous paragraph's results, $\hat{x}$ is a square in Q or $P = Q\langle y \rangle$ with $[y, x_i] = 1$ and $\langle x_i, y^2 \rangle \lhd P$. Since $b_Q(x_i) = 2$, this implies that $\hat{y} \in \{x_j^2, x_i^2 x_j^2\}$. Suppose that $\hat{y} = x_2^2 x_3^2$. Setting $\langle s \rangle = \Omega_2(\langle y \rangle)$, there is an element $v \in \langle x_2, x_3 s \rangle$ with $[v, P] = \langle x_2^2 \rangle$. Since $s \in Z(P)$ and Q does not have elements of breadth 1, this is not possible.

We have found $|P : Q| > 2$ to imply that $\hat{x}$ is a square in Q. Let $\Omega_2(\langle x \rangle) = \langle s \rangle$ and $s^2 = q^2$ with $q \in Q$. Then (e) says that $[Q, sq] = 1$ and $q \in Z(Q) = \Phi(Q)$, which means that $[x, sq] = q^2 = \hat{x}_1$. Letting $sq = t$, we have $\langle t, x_2 \rangle_P = \langle x_2^2 \rangle$, a contradiction. Accordingly:

(2) $|P : Q| = 2$.

By (1), $Z(Q) = \Phi(Q) = \langle x_1^2, x_2^2, x_3^2 \rangle$ and (2) implies that $x^2 \in C_{\Phi(Q)}(x) = Y$. Let $V = \langle x_2, x_3, x_1^{2^{n-2}}, x \rangle$; observe that $\exp V = 4$.

Assume that $V' = Y$. Let U_1, U_2, U_3, and U_4 be the distinct complements of $\langle \hat{x}_1 \rangle$ in Y. For $1 \le i \le 4$, let D_i denote the preimage of $Z(V/U_i)$ in V. Let $1 \le i \le 4$. If $|V : D_i| = 4$, then $x_1^{2^{n-2}} \notin D_i \le Q$ because of $x_1^{2^{n-2}} \in Z(Q)$ and $[x_1^{2^{n-2}}, x] = \hat{x}_1$. Thus $Q = \langle x_1 \rangle D_i$ and $D_i = \langle b_i, c_i \rangle Y$, where $b_i \in \{x_2, x_1^{2^{n-2}} x_2\}$ and $c_i \in \{x_3, x_1^{2^{n-2}} x_3\}$. On the other hand, Lemma 2.8 says that $|V : D_i| = 16$ implies $|V : D_j| = 4$ whenever $j \neq i$. It follows that the commutator $[x_2, x_3]$ lies in the intersection of at least three complements of $\langle \hat{x}_1 \rangle$ in Y, i.e. $[x_2, x_3] = 1$, contradicting (b).

We have seen that $|V'| < 8$. Assume $|V'| = 4$. Let $V' = \langle \hat{x}_1, s \rangle$ and $Y = V' \times \langle t \rangle$. By Lemma 2.8, s may be assumed to satisfy $|V/\langle s, t \rangle : Z(V/\langle s, t \rangle)| = 4$. It follows that $Q = \langle x_1 \rangle D$ with $D \cap \langle x_1 \rangle = \langle \hat{x}_1 \rangle$ and $[V, D] \le \langle s \rangle$. Perhaps upon replacing x_2 and x_3 by other elements of $x_2 \langle x_1^{2^{n-2}} \rangle$ and $x_3 \langle x_1^{2^{n-2}} \rangle$, respectively, we may take $D = \langle x_2, x_3 \rangle Y$; bearing in mind that $[x_2, x_3] \neq 1$, we obtain that $[x_2, x_3] = s$, which implies $V = \langle x_2, x_3 \rangle C_V(\langle x_2, x_3 \rangle)$.

Let $z \in C_V(\langle x_2, x_3 \rangle) \setminus Q$. For $w \in \{x_2, x_3, x_2 x_3\}$, we have $\langle w, z \rangle_P = \langle w, z^2 \rangle$, and $[w, Q] = \langle w^2, z^2 \rangle$, in particular $\langle [x_2, x_3] \rangle = [x_2, Q] \cap [x_3, Q] = \langle z^2 \rangle = \langle s \rangle$. For each $u \in \{x_1 x_2, x_1 x_3, x_1 x_2 x_3\}$, (u, x_2, x_3) is an admissible triple satisfying $\langle u \rangle \langle x_2 \rangle \cap \langle x_3 \rangle = 1$. We are hence free to assume $[x_1, x_i] = x_i^2$ for $i = 2, 3$. Let $V_1 = \langle x_2, x_3, x_1^{2^{n-2}}, x_1 z \rangle$. Then $V_1' \ge \langle \hat{x}_1, x_2^2, x_3^2 \rangle = Y$. Replacing V by V_1 in the preceding paragraph yields the desired contradiction.

Since $\hat{x}_1 \in V'$, only the case $|V'| = \langle \hat{x}_1 \rangle$ is left. Then $[x_2, x_3] = \hat{x}_1$ and there is $z \in C_V(\langle x_2, x_3 \rangle) \setminus Q$. The argument is continued exactly as in the previous paragraph. □

3 Proof of the theorem

For the remainder of the paper, G denotes a minimal counterexample to the theorem. In particular, $p = 2$. In view of Lemma 2.3, the following definition makes sense:

Definition. Let $\mathcal{A}$ be the set of abelian subgroups of G of maximal order subject to containing $\Phi(G)$. Let $A \in \mathcal{A}$. The map $x \mapsto x^2$ induces a G-isomorphism $A/\Omega_1(A) \to \Phi(A)$, i.e. every subgroup of $A/\Omega_1(A)$ is normal in $G/\Omega_1(A)$. Let $M = \mho_2(A)\Omega_1(A)$ and let H_A be the preimage of $C_{G/M}(A/M)$ in G.

Note that $H_A = \{h \in G \mid [b^2, h] \in \langle b^8 \rangle \text{ for } b \in A\}$. Also observe that $H_A \ge A \ge Z(H_A)$, while Lemma 2.1 entails $|G : H_A| \le 2$.

Notation. We fix an element A of $\mathcal{A}$ and let $H = H_A$. Let $Y = \Omega_1(A)$ and let $Z = \Omega_1(Z(H))$. The characteristic epimorphism $G \to G/Y$ will be denoted by a bar. Reviving earlier notation, we let $N = \Omega_1(Z(G))$.

Since every subgroup of G of order 4 intersects $Z(G)$ nontrivially, $|Y : N| \leq 2$. In particular, $Z = Y$ or $Z = N$. We start off the proof by stating two slight, but useful, observations.

Lemma 3.1. *Let $c \in A$. Then the following hold:*

(a) $[c, N_H(\langle c \rangle)] \leq \Omega_1(\langle c^2 \rangle)$.

(b) *Let $x \in G \setminus H$. If $[x, Y] = 1$, then $\bar{c}^{\bar{x}} = \bar{c}^{-1}$.*

Proof. Let $h \in N_H(\langle c \rangle)$. The assertion being certainly true if $o(c) \leq 4$, we take $o(c) > 4$. Now $\langle [c, h] \rangle = \langle c^2 \rangle$ would imply $\langle [c^2, h] \rangle = \langle c^4 \rangle$, yet $c^4 \notin \langle c^8 \rangle$ because of $o(c) > 4$. Thus $[c, h] \in \langle c^4 \rangle$ and Lemma 2.5 yields (a).

Let $x \in C_G(Y) \setminus H$. Let W be a complement of $\langle \hat{c} \rangle$ in Y. Since x centralises Y, W is normalised by x. Since $x^2 \in A$, conjugation by x induces an automorphism of $\langle c \rangle W/W$ of order 2. Since $x \notin H$, $o(c) \leq 4$ or conjugation by x is nontrivial on $\langle \bar{c} \rangle$. This proves (b). □

Lemma 3.2. *Suppose that $Y \neq Z$. Let $Y = Z \times \langle s \rangle$. Then $A = \langle s \rangle \times \langle b \rangle \times D$, where $\langle b \rangle D \geq [s, H] \not\leq D$, while every subgroup of D is normal in G.*

Proof. Since $\Omega_1(\Phi(A)) \leq Z(G)$, the subgroup $\langle s \rangle$ has a complement C in A. Let $C = \langle c_1 \rangle \times \cdots \times \langle c_r \rangle$. Select $b \in \{c_1, \ldots, c_r\}$ with the property that $[s, H]$ projects onto $\langle \hat{b} \rangle$ along the decomposition. Let $E = \prod_{c_j \neq b} \langle c_j \rangle$. For $e \in E$, we have $\langle e, s \rangle_G \in \{\langle e \rangle, \langle es \rangle\}$, and $\langle s, b \rangle$ therefore possesses a complement D in A that is the direct product of cyclic factors that are normal subgroups of G. In particular, $D \lhd G$. Given d_1, d_2 in D such that $\langle d_i \rangle \lhd G$ for $i = 1, 2$, we have $\langle s, d_1 d_2 \rangle_G \in \{\langle s d_1 d_2 \rangle, \langle d_1 d_2 \rangle\}$. Now $\Phi(\langle s d_1 d_2 \rangle) \leq D$, while, for $x \in H$, we have $[s d_1 d_2, x] \equiv [s, x] \pmod{D}$, which shows that $\langle s d_1 d_2 \rangle$ cannot be normal in G. Hence $\langle d_1 d_2 \rangle$ is. Induction on the length of d as a product of powers of the c_j establishes the assertion. □

Lemma 3.3. $[H, A] \leq Z$.

Proof. We start by establishing $[A, H] \leq Y$. By way of contradiction, assume there is $y \in H$ such that $[\overline{A}, \bar{y}] \neq 1$. Lemma 2.1 yields the existence of $n \in \mathbb{N}$ satisfying $\langle [\bar{b}, \bar{y}] \rangle = \langle \bar{b}^{2^n} \rangle$ whenever $b \in A$. Note that the definition of H implies $n > 1$. Applying Lemma 2.5 to the groups $\langle \bar{b}, \bar{y} \rangle$, $b \in A$, we obtain $\exp A = 2^{n+2}$.

Let $e \in A \setminus \Omega_{n+1}(A)$. By Lemma 3.1, $y \notin N_G(\langle e \rangle)$, so there is $a \in Y \setminus \langle e \rangle$ with $\langle [e, y] \rangle = \langle e^{2^n} a \rangle$. If $[a, y] = 1$, then $\langle a \rangle \lhd \langle e, y \rangle$ and Lemma 2.5, applied to $\langle e, y, a \rangle / \langle a \rangle$, provides a contradiction. It follows that $a \notin Z(H)$. Applying Lemma 3.2 yields a direct decomposition $A = \langle a \rangle \times \langle b \rangle \times C$ with $\langle b, C \rangle \ni [a, y] \notin C$ and all subgroups of C normal in G. Lemma 3.1 then yields $[\overline{C}, \overline{H}] = 1$, and, according to Lemma 2.1, $\exp C < 2^{n+2}$ and $\overline{H} = \langle \bar{y} \rangle C_{\overline{H}}(\overline{A})$.

If $\langle a, b\rangle = \langle a, d\rangle$ with $\langle d\rangle \lhd G$, then Lemma 3.1 implies $[b, y] \in Y \geq [A, H]$; hence the only maximal subgroup of $\langle a, b\rangle$ possibly normal in G is $\langle a, b^2\rangle$. Thus $[a, G] = \Omega_1(\langle b\rangle)$. Since $A = \langle b\rangle\Omega_{n+1}(A)$ and $[A, y, y] \neq 1 = [\Omega_{n+1}(A), y, y]$ we may, perhaps upon replacing a by a different element of aN, assume that $[b, y] = b^{2^n}a$.

Let $x \in C_H(a)\setminus A$. Then $[Y, x] = 1$, and, as seen above, this implies $[\bar{b}, x] = 1$. If $[x, b] \notin Z$, then $\langle [xy, b]\rangle Z = \langle b^{2^n}\rangle Z$ and Lemma 2.5 provides a contradiction when applied to the section $\langle xy, b\rangle\Omega_1(C)/\Omega_1(C)$. Hence $C_H(a) \leq C_H(b^2)$. Thus $C_H(a)$, $C_H(b^2)$ and the preimage of $C_{H/Z}(bZ)$ in H are one and the same – maximal – subgroup.

Let $1 \neq c \in C$ and let $b^* \in \langle b^2\rangle$ with $o(b^*) = o(c)$. Since $\langle a, (b^*c)^2\rangle \ntriangleleft G$, there is $\varepsilon \in \{0, 1\}$ such that $\langle a^\varepsilon b^* c\rangle \lhd G$. Since $[a^\varepsilon b^*, C_H(a)] = 1$, we obtain $[C, C_H(a)] = 1$, in particular $[A, x] = \langle [b, x]\rangle \leq Z$. Since $x^2 \in C_A(x)$, it follows that x^2 is of the form $a^\alpha b^{2\beta} c$ for suitable integers α and β and $c \in C$. Thus we have $(xb^{-\beta})^2 = a^\alpha c[x, b]^\beta$. Since $2^{n+2} > 8$, there is $\tilde{b} \in \langle b^2\rangle \leq C_A(x)$ satisfying $[x, b] \equiv \tilde{b}^2 \pmod{\langle a\rangle\Omega_1(C)}$. It follows that $x\langle b\rangle = u\langle b\rangle$ with $u^2 \in \langle a\rangle C$. Since $\langle ac\rangle \ntriangleleft G$ whenever $c \in C$, $u^2 \in C$. Next we show $u^2 \notin \Phi(C)$. Suppose otherwise; then, since $[u, C] = 1$, there is $c \in C$ with $(uc)^2 = 1$. Letting $w = uc$, we obtain that $\langle a, w\rangle \cong E_4$ with $\langle a, w\rangle_G = 1$.

Thus $u^2 \in C\setminus\Phi(C)$, in particular $o(u) > 2$. Since $o(b) > \exp C$, $2^{n+2} \geq o(u)$. As $\langle a, u^2\rangle \ntriangleleft G$, $\langle a, u\rangle_G = \langle a^\varepsilon u\rangle$ with $\varepsilon \in \{0, 1\}$. It follows that $\langle [b, u]\rangle = [A, u] = \langle \hat{u}\rangle$. Pick $b^* \in \langle b\rangle$ with $o(b^*) = o(u)$. If $o(u) = 2^{n+2}$, then, since $n > 1$, $(ub)^{2^{n+1}} = \hat{u}\hat{b}[u, b]^{\binom{2^n}{2}} = \hat{u}\hat{b}$, if $o(u) < 2^{n+2}$, then $ub^* = b^*u$ anyway. Let $w = b^*u$ and $\varepsilon \in \{0, 1\}$. We have just seen that $\hat{w} = \hat{u}\hat{b}$, whence neither $[a, G]$ nor $\hat{u} = [u, b] = [a^\varepsilon w, b]$ is contained in $\langle w^2\rangle$. It follows that none of the maximal subgroups of $\langle a, w\rangle$ is normal in G.

We are done proving $[A, H] \leq Y$. Assume there is $x \in H$ with $[A, x] \nleq Z$. Then $Y = \langle a, Z\rangle$ with $a \in [A, x]$. We apply Lemma 3.2 to obtain a decomposition $A = \langle a\rangle \times \langle b\rangle \times C$, where $[a, H] \nleq C$ and every subgroup of C is normal in G. Note that $[\langle a, C\rangle, x] \leq Z$, and $[b, x] = az$ with $z \in Z$. Since both $C_H(a)$ and the preimage of $C_{H/Z}(bZ)$ in H are proper subgroups of H, we may additionally assume $[a, x] \neq 1$. This yields $[b, x^2] = [b, x, x] = [a, x] \neq 1$, contradicting $\Phi(G) \subseteq A$. □

If every subgroup of A were normal in H, then $|H : A| = 2$ by Lemmas 2.1 and 3.3. This justifies the following:

Definition. Let $k \in \mathbb{N}$ be minimal with the property that there is $B \in \mathcal{A}$ in which not every subgroup of $\Omega_k(B)$ is normal in H_B.

We shall always assume A to be chosen to actually possess a cyclic subgroup of order 2^k that is not normal in H $(= H_A)$. It may be useful to keep in mind that $\Omega_{k-1}(A) \le Z(H)$ (see Lemma 2.6).

Lemma 3.4. $\exp H' \le 4$ *and* $\exp H' \le 2$ *unless* $k \le 2$.

Proof. Let $u, v \in H$. According to Lemma 3.3, $[\bar{u}, \bar{v}^2] = 1 = [\bar{u}, \bar{v}]^2[\bar{u}, \bar{v}, \bar{v}]$. It follows that $[\bar{u}, \bar{v}]$ is an element of $\bar{A}$ inverted by $\bar{v}$, which is possible only if $o([u, v]) \le 4$.

Suppose that $k \ge 3$. Together with Lemma 2.6, the above implies that $[u, v] \in \Omega_2(A) \le Z(H)$, i.e. $[u, v]^2 = [u^2, v] = [v^2, u] \in \langle \hat{u} \rangle \cap \langle \hat{v} \rangle$. Thus $o([u, v]) > 2$ necessitates $\hat{u} = \hat{v}$. Suppose that $o([u, v]) = 4$. We have seen that $u^2 \notin Z(\langle u, v \rangle) \not\ni v^2$. Lemma 2.6 consequently yields $o(w) \ge 2^{k+1} \ge 2^4$ for $w = u, v$. Without loss, there are positive integers m and ℓ satisfying $\ell \ge m \ge 2$, $u^{2^\ell} = v^{2^m}$ and $\langle u \rangle \cap \langle v \rangle = \langle u^{2^\ell} \rangle$. It follows that

$$(vu^{-2^{\ell-m}})^{2^m} = v^{2^m} u^{-2^\ell} [u, v]^{2^{\ell-m}\binom{2^m}{2}}.$$

Thus $(vu^{-2^{\ell-m}})^{2^m} = 1$ unless $\ell = m = 2$. Assume the latter. Let $o(u) = 2^n$. Then $(vu^{-1})^4 = [u, v]^2 = u^{2^{n-1}}$. Since $n \ge 4$,

$$(vu^{-1}u^{2^{n-3}})^4 = u^{2^n}[u^{2^{n-3}}, v]^2 = 1.$$

Thus $\langle u, v \rangle = \langle u, y \rangle$ with $\langle u \rangle \cap \langle y \rangle = 1$ and $[u, y] = [u, v]$. We have seen this to be incompatible with $o([u, y]) = o([u, v]) = 4$. □

The cases $k \ge 2$ and $k = 1$ have been allocated their own subsection each. It will soon turn out to be the case that $k = 2$ is the most difficult case by far.

3.1 The case $k > 1$

Lemma 3.5. $k \le 2$.

Proof. Assume $k \ge 3$. By Lemmas 2.6, 2.9, and 3.4, $H' \le Z$, $|H : A| \le 4$, and $|A : Z(H)| = 2$. It follows that $G \ne H$. Since $H' \le Z$, we have $\Phi(H) \le Z(H)$, while Lemma 2.1 says that $y^2 \in C_A(y) \le \Omega_2(A) \le Z(H)$ whenever $y \in G \setminus H$. Accordingly, $\Phi(G) \le Z(H)$. Let $G = H\langle x \rangle$ and let $A = \langle a \rangle Z(H)$. Note that $o(a) \ge 8$ because of Lemma 2.6 and that $[a, H] = [A, H]$ is a normal elementary abelian 4-subgroup of G.

Assume there is $s \in Y \setminus Z(G)$. Since $[a, H] = [as, H]$, either $[a, H] = \langle s, \hat{a} \rangle$, or $\langle s, a \rangle_G = \langle s, a^2 \rangle$. In either case $[x, s] = \hat{a}$. Since $[x, s]$ is independent of a, it follows that $o(a) = 2^k = \exp A$ and $\Omega_{k-1}(A) = Z(H)$, i.e. $A = \langle a \rangle \times D$ with

$D \leq \Omega_{k-1}(Z(H)) = Z(H)$. Let $h \in H \setminus A$. Since $h^2 \in C_A(h) = Z(H)$, we have $o(h) \leq 2^k$ and since $k \geq 3$, there is an element $a^* \in \langle a \rangle$ satisfying $(ha^*)^2 \in D$. Yet if $h^2 \in D$, then $\langle s, h^2 \rangle \ntriangleleft G$, whence $\langle s, h \rangle_G \in \{\langle h \rangle, \langle sh \rangle\}$. It follows that $H = A\langle g, h \rangle$ with $g^2 \in D \ni h^2$ and $\langle g \rangle \triangleleft G \triangleright \langle h \rangle$. Since $b(a) = 2$, this forces the conclusion $[a, g] = \hat{g}$, $[a, h] = \hat{h}$ and $\langle g \rangle \cap \langle h \rangle = 1$, from which $[g, h] = 1$ results. However, we have seen that $\Phi(G) \leq Z(H)$, which, since $|Z(H)\langle h, g \rangle| > |A|$, contradicts the fact that $A \in \mathcal{A}$. Accordingly,

$$Y \leq Z(G). \tag{3.1}$$

By (3.1) and part (b) of Lemma 3.1, $\bar{b}^{\bar{x}} = \bar{b}^{-1}$ whenever $b \in A$. Since $\exp A \geq 2^k > 4$, it follows that $C_G(\Omega_2(\Phi(G))) = H$, in particular $H = H_B$ whenever $B \in \mathcal{A}$. Since $Z(H)\langle h \rangle \in \mathcal{A}$ whenever $h \in H \setminus Z(H)$, this implies in conjunction with (3.1) that $\Omega_2(H) \leq Z(H)$, $Y = \Omega_1(H) = \Omega_1(Z(G))$ and $h^x \in h^{-1}Y$ for all $h \in H$. Note that $x^2 \in C_A(x) \leq \Omega_2(A) \leq Z(H)$, so $o(x) \leq 8$ and $x^2 \in Z(G)$.

Assuming that $Y \neq H'$, we can find $z \in Y \setminus (H' \cup \{\hat{a}\})$. Induction yields a normal subgroup B of G with $|G : B| \leq 4$, $\Phi(G) \leq B$, and $B' = \langle z \rangle$. If $B \leq H$, then $B \in \mathcal{A}$, a contradiction. Hence $G = HB$. However, $a^2 \in \Phi(G) \leq B$ and if $y \in B \setminus A$, then $a^{2y} = a^{-2}$, leaving $o(a) = 8$ and $z = a^4$ the only possibility. Yet $z \neq \hat{a}$. Accordingly,

$$Y = H'. \tag{3.2}$$

For a supplement Q of $Z(H)$ in H, (3.2) yields $H' = \Omega_1(H) = Q'$, in particular $Q \triangleleft G$. We let $H = Z(H)\langle a, b, c \rangle$ and $Q = \langle a, b, c \rangle$. Note that $\Phi(H) \cap Q = \Phi(Q) = Z(Q) = Z(H) \cap Q$. Let $\exp Q = 2^m$ and let $u \in Q$ be of order 2^m. As a cyclic subgroup of maximal order in $\Phi(Q)$, $\langle u^2 \rangle$ has a complement D in $\Phi(Q)$. Note that $\langle u \rangle \Phi(Q) = \langle u \rangle \times D$. Since $Q' \leq Y$, every coset $w\langle u \rangle \Phi(Q)$ with $w \in Q \setminus \langle u \rangle \Phi(Q)$ contains an element y with $y^2 \in DY$. Since we know that $\Omega_2(H) \leq Z(H)$, it follows that $\exp D > 2$.

Let d be an element of D of maximal order and let $D = \langle d \rangle \times E$. Then

$$Q' \leq \langle u^2 \rangle \times \langle d^2 \rangle E \ngeq \Phi(Q),$$

and there is $v \in Q$ with $v^2 \notin \langle u^2, d^2 \rangle E$, in particular $v \notin \langle u \rangle \Phi(Q)$. Assume that $\langle v \rangle \cap \langle u \rangle \neq 1$. Let $2^n = |\langle v \rangle : \langle u \rangle \cap \langle v \rangle|$. Note that $n \geq 2$. Without loss v^{2^n} is a power u^{2^ℓ}; note that $\ell \geq n$. It follows that $(vu^{-(2^{\ell-n})})^{2^n} = 1$. There is hence no loss in presuming $\langle v \rangle \cap \langle u \rangle = 1$. It follows that $\langle u^2, d \rangle \times E = (\langle u^2 \rangle \times \langle v^2 \rangle)E$, in particular $|\Phi(Q)| = |\langle u^2 \rangle||\langle d \rangle||E| \leq |\langle u^2 \rangle||\langle v^2 \rangle||E|$. If $o(v^2) > o(d)$, then $o(u^2) > o(d)$ and $\hat{v} = \hat{u}$. Accordingly, $\Phi(Q) = \langle u^2 \rangle \times \langle v^2 \rangle \times E$.

Finally, let $w \in Q \setminus \langle u, v \rangle \Phi(Q)$. Since $Q' \leq Y$, there is an element $y \in \langle u, v \rangle$ satisfying $(wy)^2 \in \langle \hat{u}, \hat{v} \rangle \times E$. Since $o(u) \geq 8 \leq o(v)$ and $\Omega_2(H) \leq Z(H)$, there is an element $z \in \Omega_2(\langle u^2, v^2\rangle)$ such that $(wyz)^2 \in E$. Hence we may take $w^2 \in E$ and it follows that $\langle w\rangle \cap \langle u\rangle\langle v\rangle = \langle w^2\rangle \cap \langle u^2, v^2\rangle = 1$. Accordingly, $H' = Q' = \langle \hat{u}, \hat{v}, \hat{w}\rangle$ and $Q = \langle u\rangle\langle v\rangle\langle w\rangle$. Each of the elements u, v, w has order at least 8, in particular $\Omega_2(Q) \leq \Phi(Q)$. Let $P = Q\langle x\rangle$. We have established that P satisfies conditions (a), (b), and (c) of Lemma 2.11. Moreover, we know that $o(x) \leq 8$ and $x^2 \in Z(G)$. Thus either $|P : Q| = 2$ or $o(x) = 8$, $\langle x\rangle \cap Q = \langle x^4\rangle$ and any element s of $\Omega_1(\Phi(P)Q) \setminus Q$ satisfies $s = x^2y$ with $y \in \Omega_2(Q)$. Any such s has to centralise Q, which shows that condition (d) in the premise of Lemma 2.11 applies as well. So Lemma 2.11 yields a contradiction. □

Lemma 3.6. *If $k > 1$, then $\langle [u, v]\rangle \lhd H$ whenever $u, v \in H$.*

Proof. Suppose otherwise. Due to Lemmas 2.6 and 3.4, $k = 2$ and $\exp H' = 4$. Let $u, v \in H$ be such that $\langle [u, v]\rangle \ntriangleleft H$ and let $\langle u, v\rangle = V$. Since $k > 1$, $o([u, v]) = 4$. Let $\{x, y\}$ be a generating set of V. Then $\langle [x, y]\rangle Y = \langle [u, v]\rangle Y$, in particular $\langle [x, y]\rangle \ntriangleleft H$. Since $[x, y, x] = [x^2, y][x, y]^2 \in \langle \hat{x}\rangle[x, y]^2$, the product $U = \langle x\rangle\langle [x, y]\rangle$ is a subgroup of H. Note that

$$H \rhd \mho_1(U) = \Phi(U) = \langle x^2\rangle\langle [x, y]^2\rangle \quad \text{and} \quad [x, y]^2 = [u, v]^2.$$

Next, $y \notin N_G(\langle x\rangle\Phi(U))$ – otherwise $[x, y] \in \langle x^2, [x, y]^2\rangle$, i.e. $[x, y] \in \langle x^2\rangle$ and $\langle [x, y]\rangle \lhd H$. Since $\langle x[x, y]\rangle\Phi(U) = (\langle x\rangle\Phi(U))^y$, the only maximal subgroup of U available for normality in G is $\langle [x, y], x^2\rangle$. Note that this is possible only if $o(x) > 2$.

If $[x, y]^2 \in \langle x^2\rangle$, then a power x^* of x^2 satisfies $([x, y]x^*)^2 = 1$. Letting $[x, y]x^* = w$, $k > 1$ implies $w \in Z(H)$ and $[x, y, H] = [x^*, H] \leq \langle \hat{x}\rangle \leq \langle [x, y]^2\rangle$, a contradiction. We summarise:

(1) Let $x \in V \setminus \Phi(V)$. Then

$$o(x) > 2, \quad \langle x\rangle \cap \langle [u, v]\rangle = 1, \quad [u, v, H] \leq \langle [u, v]^2, \hat{x}\rangle.$$

If $[u, v, x] = 1$, then $[x^2, y] = [u, v]^2 = \hat{x}$, contradicting (1). Thus:

(2) $C_V([u, v]) = \Phi(V)$ and $[u, v, H] = [u, v, V] = \langle \hat{x}, [u, v]^2\rangle$ holds for every $x \in V \setminus \Phi(V)$.

By (2), $V \nleq N_G(\langle [u, v]\rangle)$. We choose notation such that $u \notin N_G(\langle [u, v]\rangle) \ni v$. Let $o(u) = 2^n$, noting that (1) implies $n > 1$. From $[u, v]^2[u, v, u] = [u^2, v] \neq 1$ and Lemma 2.6, we deduce

(3) $n \geq 3$ and $[u^2, v] = [u, v]^2[u, v, u] = \hat{u}$.

Furthermore, (1) implies that $[v^2, u] = [u, v]^2[u, v, v] \in \langle \hat{v}\rangle \cap \langle [u, v]\rangle = 1$, i.e.

(4) $[u, v^2] = 1$ and $[u, v, v] = [u, v]^2$.

Suppose that $o(v) > o(u)$. Let $s \in \langle v^2 \rangle$ be of order 2^n. Then (4) implies that $[u, s] = 1$. In particular, (1) may be used to exclude the possibility that $\hat{u} = \hat{v}$, for this would yield the existence of in $u\langle s \rangle$. Next, (3) implies that

$$[u^2 s^2, v] = [(us)^2, v] = \hat{u} \in \langle us \rangle.$$

But $n > 1$ and, as we have seen, $\widehat{us} = \hat{u}\hat{v} \neq \hat{u}$. It follows that $2^n \geq o(v)$. Since $(uv)^2 = u^2 v^2 [v, u]^v = u^2 v^2 [u, v]$, $\langle u^2 v^2 [u, v] \rangle \lhd G$. By (3), $[u^2 v^2 [u, v], u] = [u, v, u] = \hat{u}[u, v]^2$. By (1), $\hat{u}[u, v]^2 \notin \langle \hat{u} \rangle$, and we obtain that if $o(v) < 2^n$, then $n = 3$.

Assume that $o(v) = 2^n$. If $\hat{u} \neq \hat{v}$, then (2) implies $[u, v]^2 = \hat{u}\hat{v}$, while (3) says $[u, v, u] = \hat{v}$. Thus $[u^2 v^2 [u, v], u] = \hat{v} \in \langle u^4 v^4 [u, v]^2 \rangle$. Thus $n > 3$ – otherwise $o(u^2 v^2 [u, v]) \leq 2$ – and $\hat{v} = \hat{u}\hat{v}$, impossible. Accordingly, $\hat{u} = \hat{v}$. Let $|\langle v \rangle : \langle u \rangle \cap \langle v \rangle| = 2^\ell$, observing that $\ell \geq 2$. Suppose that $\ell = 2$. Then, without loss, $u^4 = v^4$, and $(uv^{-1})^4 = [u, v]^2$, contradicting (1). If $\ell > 3$, then there is a generator v_1 of $\langle v \rangle$ with the property that

$$\Omega_1(\langle u^2 v^2 [u, v] \rangle) = \langle u^{2^{\ell-1}} v_1^{2^{\ell-1}} \rangle.$$

Combined with (3) and (4), this yields

$$[u^2 v^2 [u, v], v] = \hat{u}[u, v]^2 = u^{2^{\ell-1}} v_1^{2^{\ell-1}}.$$

Hence there also is a generator u_1 of $\langle u \rangle$ satisfying

$$u_1^{2^{\ell-1}} v_1^{2^{\ell-1}} = [u, v]^2.$$

Since $\ell > 3$, it follows that $s = u_1^{2^{\ell-2}} v_1^{2^{\ell-2}} [u, v]$ is now an involution contained in $[u, v] Z(H)$, contradicting $k > 1$. Now $\ell = 3$ is the only option left: then there is a generator v_1 of $\langle v \rangle$ satisfying

$$\Omega_1(\langle u^2 v^2 [u, v] \rangle) = \langle u^4 v_1^4 [u, v]^2 \rangle,$$

i.e. $\hat{u}[u, v]^2 = u^4 v_1^4 [u, v]^2$, i.e. $\hat{u} = u^4 v_1^4$. Yet this implies $v^4 \in \langle u \rangle$ and clashes with $\ell = 3$.

The outcome of the preceding two paragraphs is that $o(u) = 8$ and $o(v) = 4$. If $u^4 = v^2$, then $o(uv) = 8$, while $(uv)^4 = u^4 [u, v]^2 \neq u^4$ and the pair (uv, v) satisfies every constraint previously placed on (u, v). We summarise:

(5) $o(u) = 8$, $o(v) = 4$, and u and v may be chosen to satisfy $\langle u \rangle \cap \langle v \rangle = 1$.

We shall assume $\langle u \rangle \cap \langle v \rangle = 1$ from now on. By (2),

$$[u, v, H] = \langle [u, v]^2, \hat{u} \rangle = \langle [u, v]^2, \hat{v} \rangle = \langle u^4, v^2 \rangle.$$

Thus, (1) yields $[u, v]^2 = u^4 v^2$.

Suppose that A has an element b of order 8. Then $(vb)^4 = b^4 \neq 1$, while $[u, vb] \in [u, v]Z$. Every assertion so far made about (u, v) equally applies to (u, vb), whence (5) delivers a contradiction. It follows that

(6) $\exp A = 4$, in particular $G = H$.

Together with $k > 1$, (6) implies that $Y \leq Z(G)$. Let $B = \langle u^2, [u, v]\rangle$. By (1) and (5), $B \cong C_4 \times C_4$, and (6) yields the existence of a complement of B in A, to be called D. For $d \in D$, $\langle d, [u, v]\rangle_G \in \{\langle d, [u, v]^2\rangle, \langle d[u, v], [u, v]^2\rangle\}$; thus D may be taken to be a direct product of subgroups $\langle d\rangle$ with $\langle d, [u, v]^2\rangle \lhd G$. Let $d, d' \in D$ be such that $\langle d, [u, v]^2\rangle \lhd G \rhd \langle d', [u, v]^2\rangle$. Then $\langle dd', [u, v]^2\rangle \lhd G$, because $[dd'[u, v], u] \in u^4\langle\Phi(D), [u, v]^2\rangle$. Thus $\langle E, [u, v]^2\rangle \lhd G$ for all subgroups E of D. Let $d \in D$. We have seen that some element w of $\{u, v, uv\}$ is in $N_G(\langle d\rangle)$. Now $\Phi(\langle w, d\rangle) = \langle w^2, d^2\rangle \in \{\langle u^2, d^2\rangle, \langle v^2, d^2\rangle, \langle u^2v^2[u, v], d^2\rangle\}$, i.e. $\Phi(\langle w, d\rangle)Y \not\ni [u, v] \in [G, w]Y = [G, wd]Y$. This forces the conclusion $\langle d, \hat{w}\rangle \lhd G$. Now $\hat{w} \in \{u^4, v^2\}$ and $[d, H] \in \langle d^2, [u, v]^2\rangle \cap \langle d^2, \hat{w}\rangle$, i.e. $\langle d\rangle \lhd G$.

(7) $A = \langle u^2, [u, v]\rangle \times D$ with every subgroup of D normal in G.

Assuming $\exp D = 4$, let $d \in D \setminus \Omega_1(D)$. Due to $[u, vd] \in \langle [u, v]\rangle Z$, we may replace v by vd in (1)–(4), to obtain $[u, v, G] \leq \langle (vd)^2, [u, v]^2\rangle \cap \langle v^2, [u, v]^2\rangle$. If $[v, d] = 1$, this yields $d^2 \in \langle v^2, u^4\rangle$, a contradiction. By (7), this means that v inverts each element of D. It follows that $\Phi(\langle v, [u, v]d\rangle) = \langle v^2, u^4d^2\rangle$, and, since $[u^2, v] = [u^2, v[u, v]d] = u^4$, we obtain $[[u, v]d, G] \leq \langle v^2, u^4d^2\rangle$. Now $[d, uv] = 1$ is impossible, as it would imply

$$[[u, v]d, uv] = [u, v, u][u, v, v] = u^4.$$

Thus $[D, u] = 1$ – according to (7), $C_G(D) \lessdot G$. Let $\langle u^2d, [u, v]\rangle = W$. From $[u^2d[u, v], u] = [u, v, u] = v^2 \notin \langle u^4d^2, u^4v^2\rangle = \Phi(W)$, we infer that $[u^2d, G] \leq \Phi(W)$. Since both $\langle u^2\rangle$ and $\langle d\rangle$ are normal in G, this yields

$$[u^2d, G] \leq \langle u^4d^2, u^4v^2\rangle \cap \langle u^4, d^2\rangle = \langle u^4d^2\rangle,$$

i.e. $\langle u^2d\rangle \lhd G$. Lemma 2.1 yields $C_G(u^2) = C_G(D)$. By (1)–(4),

$$G = \langle u\rangle N_G(\langle [u, v]\rangle) = \langle u, v\rangle C_G([u, v]).$$

Since $o(v) = 4$ and $G = H$, we have

$$(uv)^2 \cong u^2[u, v] \pmod{Z(G)},$$

i.e. $\langle u^2[u, v]\rangle \lhd G$. Thus we obtain that $C_G([u, v]) \leq C_G(u^2)$, and

$$C_G([u, v]) = C_G(\langle [u, v], u^2, D\rangle) = C_G(A) = A.$$

Accordingly, $|G : A| = 4$.

We have seen that $\exp D = 2$, i.e. $A = BZ$. By (1), $B \lhd G$, according to (3), $\langle[u^2, G]\rangle = \langle u^4\rangle = \langle[u^2, v]\rangle$ and according to (3) and (4), $[u, v, G] = \langle u^4, v^2\rangle = [u, v, \langle u, v\rangle]$. If $s \in G$ satisfies $[u, v, s] = 1 \neq [u^2, s]$, then $[u^2[u, v], s] = u^4 \neq u^4[u, v]^2$; however, $\langle u^2[u, v]\rangle \lhd G$. Consequently, $G = \langle u, v\rangle C_G(\langle u^2, [u, v]\rangle) = \langle u, v\rangle A$, a contradiction that finishes this proof. □

Lemma 3.7. *If $k = 2$, then $H' \leq Z$.*

Proof. Assume otherwise. Pick $x \in H$ with $x^2 \notin Z(H)$ and let $y \in H \setminus C_H(x^2)$. By Lemma 2.6, $\Omega_1(\Phi(G)) \leq Z$ and $\langle[x, y]\rangle \lhd H$ by Lemma 3.6, so $[x^2, y] = \hat{x} = [x, y]^2[x, y, x] = [x, y]^2$. In particular, $[x, y, x] = 1$ and Lemmas 2.1 and 3.6 yield $[H, x, x] = 1$. The assumption $[x, y, y] = 1$, however, implies that $\hat{x} = [x, y^2] = \hat{y}$. If this is true, we may assume $x^{2^m} = y^{2^\ell}$, where $m \geq \ell \geq 2$ and $2^\ell = |\langle y\rangle/(\langle x\rangle \cap \langle y\rangle)|$. Either $m = \ell = 2$, or $w = yx^{-2^{m-\ell}}$ satisfies $\langle w\rangle \cap \langle x\rangle = 1$, $\langle[x, w]\rangle = \langle[x, y]\rangle$, and $[x, w, w] = 1$, a contradiction. If $m = \ell = 2$, we have $o(x^2y^{-2}) = 2$; yet $[y, x^2y^{-2}] \neq 1$ and $k > 1$ is contradicted.

Accordingly, $[x, y, y] \neq 1$; by Lemma 3.6, this means $[x, y]^y = [x, y]^{-1}$. If $o(x) > 8$, then there is $x^* \in \langle x^4\rangle < Z(H)$ such that $o([x, y]x^*) = 2$, and $k > 1$ forces the conclusion $[x, y, y] = 1$. Thus $o(x) = 8$. Suppose there is $u \in H$ such that $[u^2, x] \neq 1$. Then, as we have seen, $o(u) = 8$ and $u^4 = x^4 = [x, u]^2$. It follows that $z = u^2x^2$ is an involution with $[z, x] \neq 1$. Finally, Lemmas 2.1 and 3.6 say that $[v, y]^y = [v, y]^{-1}$ whenever $v \in H$, implying $y^2 \in Z(H)$. We summarise:

(1) If $y \in H \setminus C_H(\Phi(H))$, then $y^2 \in Z(H)$. Any element v of H with $v^2 \notin Z(H)$ has order 8 and centralises $\Phi(H)$.

Let $\Phi(H) \cap Z(H) = T$ and let $K = C_H(\Phi(H))$. For all $g, h \in K$ we have $1 = [g^2, h] = [g, h]^2$, i.e. $K' \leq Z$. By (1), the Hughes subgroup of H/T is contained in K/T, whence $K \lessdot H$ and every element of K is inverted by y modulo T. Suppose there is $u \in K$ with $o(u) > 8$. By (1), $u^2 \in Z(H)$, whence $[w, u^2] = [w, u]^2 = 1$ whenever $w \in H$, in particular $(xu)^2 = x^2u^2[x, u] \in x^2Z(H)$. However, $(xu)^8 = u^8 \neq 1$, contradicting (1). Hence $\exp K = 8$. Let $L = \Omega_2(K)$, noting that, since $K' \leq Z$, we have $\exp L \leq 4$. If $v \in K \setminus \langle x\rangle L$, then $v^4 \neq x^4$ and $(vx)^2 \equiv v^2x^2 \pmod{Z}$. It follows that y normalises every subgroup of $\langle v^2, x^2\rangle = \langle v^2\rangle \times \langle x^2\rangle$. Accordingly, $[v, y]^2 = [v^2, y] = v^4 \neq 1$ and $Z(H/Z) = L/Z$. Applying Lemma 3.3, we obtain $A \leq L$. We summarise:

(2) $L/Z = Z(H/Z)$, in particular $\exp A = 4$ and $G = H$.

From $K \lessdot H = G$ and Lemma 2.9, we further infer:

(3) $|K : A| = 4$ and either $|A : Z(K)| = 2$, or $A = \langle c, d\rangle Z(K)$ with $b_K(c) = b_K(d) = 1$. In particular, $|[A, K]| \leq 4$ and $|K'| \leq 8$.

Suppose there is an element $z \in Y \setminus K'$. Via induction, G has a normal subgroup B of index 4 satisfying $B' = \langle z \rangle$. Unless B is abelian, $B \not\leq K$. Given $t \in B \setminus K$, we have $\bar{B} \ni [\bar{t}, \bar{x}] = [\bar{y}, \bar{x}]$, and $z = [x, t, t] = [x, y, y] = x^4$. It is, however, possible to choose z distinct from x^4. Thus:

(4) $Y = K'$.

We consider the possibility that $|A : Z(K)| = 2$ and $|Y| = 8$. First suppose that $|K : L| = 4$, i.e. $L = A$. Letting $A = \langle v \rangle Z(K)$, we obtain $K = \langle v, w, x \rangle Z(K)$ with $o(w) = o(x) = 8$ and $\langle w \rangle \cap \langle x \rangle = 1$. Since $o(v) = 4$ and "$v^2 \in \langle w^4, x^4 \rangle$" would necessitate the existence of involutions in $A \setminus Z$, $(\langle v \rangle \langle w \rangle) \cap \langle x \rangle = 1$ and $K = \langle w \rangle \langle x \rangle \langle v \rangle Z(K)$. Let $Q = \langle x, w, v \rangle$. By (4), $Y = \langle x^4, w^4, v^2 \rangle = \Omega_1(Q)$. As y inverts the elements of $\langle w^2 \rangle \times \langle x^2 \rangle$, $Z(G) \cap Q = Y$. Since $\exp A = 4$, $o(y) \leq 8$. Let $P = Q\langle y \rangle$. We have already noted that P satisfies (a)–(c) in the premise of Lemma 2.11. Suppose that $\Phi(P)Q > Q$. It follows that $o(y) = 8$ and any $t \in \Omega_1(\Phi(P)Q) \setminus Q$ must be of the form $t = y^2 q$ with $q \in \Omega_2(Q)$. Now $\Omega_2(Q) \leq L \cap Q = A \cap Q$ so that $t \in A$ and $k = 2$ implies $[Q, t] = 1$. Hence P satisfies the hypothesis of Lemma 2.11 and is not core-2. Thus:

(5) If $Z(K)| = 2$ and $|Y| = 8$, then $|K : L| = 2$.

We continue to work from the assumptions $|A : Z(K)| = 2$ and $|Y| = 8$. By (5), we may write $L = \langle a, v \rangle Z(K)$. Letting $Q = \langle a, v, x \rangle$, we have $K = Z(K)Q$ and $Y = Q'$. Let $G = K\langle y \rangle$. Since $\bar{x}^y = \bar{x}^{-1}$ and $[L, y] \leq Y$, $y \in N_G(Q)$. From (1) and (2) we know that $\Phi(G) \leq Z(K)$, so if $w \in L \setminus Z(K)$, then $\langle w, Z(K) \rangle \in \mathcal{A}$ and $k > 1$ implies $\Omega_1(\langle w, Z(K) \rangle) \leq Z(G)$. Suppose that $o(y) = 8$. Then we have $y^2 \in Z(G) \leq L$. Any involution in $Q\langle y^2 \rangle \setminus Q$ is equal to a product $y^2 q$ with $q \in \Omega_2(Q)$, in particular $q \in L \ni y^2$ and $y^2 q \in \Omega_1(L) \leq Z(G)$. Letting $P = Q\langle y \rangle$, P therefore satisfies the hypothesis of Lemma 2.12 and is not core-2. Consequently:

(6) If $|A : Z(K)| = 2$, then $|Y| \leq 4$.

We stick to the hypothesis $|A : Z(K)| = 2$. As $|K : Z(K)| = 2^3$, it follows that $Z(K/W) \not\leq Z(K)/W$ whenever $W \lessdot Y$. By (6), $|K'| \leq 4$, and there is $v \in K$ with $b_K(v) = 1$. For such a v, though, $C_K(v)$ is an abelian subgroup of K containing $\Phi(G)$ and of greater order than A. So:

(7) $|A : Z(K)| = 4$.

By (3), $|[A, K]| \leq 4$. Whenever $K = \langle x, u \rangle A$, we have $Y = [A, K]\langle [x, u] \rangle$. Let W be a maximal subgroup of Y not containing x^4. By Lemma 2.7, we have that $|K/W : Z(K/W)| \leq 4$ and $A/W \cap Z(K/W)$ has index at most 2 in A/W.

Assume that $|[A, K]| = 4$. From (2) and $k = 2$, $A = \langle a, b \rangle Z(K)$, where $b(a) = b(b) = 1$ and $b(ab) = 2$. By Lemma 2.6, $k > 1$ implies $\langle a, b \rangle \cong C_4 \times C_4$. Note that this excludes $K' = [A, K]$. Indeed, if that was the case, then (4) would imply $Y = \langle a^2 \rangle \times \langle b^2 \rangle$ and there would be $c \in A \setminus Z(K)$ satisfying $c^2 = x^4$. However, this would make cx^2 an involution outside $Z(G)$.

Let $[a, K] = \langle s \rangle$ and $[b, K] = \langle t \rangle$. We have seen $|Y| = 8$. So set $Y = \langle s, t, r \rangle$. If $x^4 \notin \langle s, t \rangle$, then $W = \langle x^4 s, st \rangle$ is a maximal subgroup of Y not containing x^4 and satisfying $|A/W : A/W \cap Z(K/W)| = 4$, a contradiction. This places x^4 inside $[A, K]$. Set $[A, K] = \langle x^4, z \rangle$. Lemma 2.8 says that

$$|A/\langle z, r \rangle : Z(K/\langle z, r \rangle) \cap A/\langle z, r \rangle| \leq 2,$$

which implies $[a, K] \leq \langle z \rangle$ or $[b, K] \leq \langle z \rangle$. Thus $\{s, t\} = \{z, x^4 z\}$. However, Lemma 2.8 also says that $|A/W : A/W \cap Z(K/W)| \leq 2$ for at least two of the three maximal subgroups W of Y that do contain x^4, namely $\langle s, x^4 \rangle$, $\langle r, x^4 \rangle$, and $\langle rs, x^4 \rangle$. This is not the case.

(8) $|A : Z(K)| = 4$ and $|[A, K]| = 2$.

By (4) and (7), $Y \cong E_4$. The fact that $\langle a, b \rangle \cong C_4 \times C_4$ remains unchanged, and we arrive at a contradiction as in the preceding paragraph. The proof is done. □

Lemma 3.8. $k = 1$.

Proof. Assume $k > 1$. The proof follows similar lines to those of Lemmas 3.5 and 3.7. Lemmas 2.9, 3.5, and 3.7 say that:

(1) $k = 2$, $H' \leq Z$, $G \neq H$, $|H : A| = 4$, and $|A : Z(H)| \in \{2, 4\}$.

From $G \neq H$ we deduce $\exp A > 4$. Let $G = \langle y \rangle H$.

If $s \in Y \setminus Z(G)$ and $v \in H$, then either $[s, y] = \hat{v}$ or $\langle v, s \rangle_G \in \{\langle v \rangle, \langle vs \rangle\}$, the latter forcing $\langle v \rangle \lhd H$. Let $C_4 \cong \langle a \rangle \leq A$ with $\langle a \rangle \ntriangleleft H$. We have seen that $a^2 = [s, y]$. Since $k = 2$ and $\Phi(A) \leq Z(H)$, it follows that $a^2 \notin \mho_2(A)$ and $\langle a \rangle$ has a complement in A. Let $A = \langle a \rangle \times D$ and let b be an element of maximal order in D. Since $G \neq H, o(b) > 4$. Let $\Omega_2(\langle b \rangle) = \langle b^* \rangle$, noting that $b^* \in Z(H)$. Each of the subgroups $\langle b \rangle$, $\langle ab \rangle$, and $\langle ab^* \rangle$ is normal in H, in particular $[a, H] = [ab^*, H] = \langle a^2 \hat{b} \rangle$. Let $v \in H \setminus C_H(a)$. Then $[v, ab] = a^2 \hat{b}[v, b]$. It is therefore impossible that both $[v, b]$ and $[v, ab]$ are elements of $\in \langle \hat{b} \rangle$. Accordingly:

(2) $Y \leq Z(G)$.

Suppose that $Y > H'$. Let b be an element of A of order 8. Letting $z \in H' \setminus Y$, induction yields a normal subgroup B of G with $\Phi(G) \leq B$, $|G : B| = 4$ and $B' \leq \langle z \rangle$. Since $H \cap B$ is abelian, $B \not\leq H$. In conjunction with Lemma 3.1 (b), (2) implies that, for $c \in A$, there is $z_c \in Y$ with $c^y = c^{-1} z_c$. In particular, we have $b^{2x} = b^{-2}$ for $x \in B \setminus H$. Now $b^2 \in B$ implies that $z = b^4$; yet if $Y \neq H'$, then $Y \neq H' \cup \{b^4\}$. Hence:

(3) $Y = H'$.

Since $b^2 \in \bigcap_{B \in \mathcal{A}} B$ and $b^{2x} = b^{-2}$ whenever $x \notin H$, Lemma 3.3 says that:

(4) For every $B \in \mathcal{A}$, $C_G(b^2) = H = H_B$.

Suppose that $|A : Z(H)| = 2$ and $|Y| = 8$. By condition (3), $b_H(h) = 2$ holds for $h \in H \setminus Z(H)$. Since H thus is void of elements of breadth 1, it follows that $x^2 \in \Omega_2(Z(H))$ whenever $x \in G \setminus H$. Accordingly, $\Phi(G) \leq Z(H)$ and $C_H(h) = \langle Z(H), h\rangle \in \mathcal{A}$ whenever $h \in H \setminus Z(H)$. It now follows from (4), from (b) in Lemma 3.1 and from the definition of k that $Y = \Omega_1(H)$ and that, for $h \in H$, there is an element $z_h \in Y$ with $h^y = h^{-1}z_h$. Let $H = \langle u, v\rangle A$, where $o(u) = 2^n = \exp H > 4$. Because of $k > 1$, $v^2 \notin \langle u^4\rangle$; if $u^2 = v^2$, then $(uv^{-1})^2 = [u, v]$, and, since the coset $uv^{-1}\Phi(H)$ is not permitted to contain involutions, $[u, v] \notin \langle u\rangle$. In any case there is $w \in v\langle u\rangle$ with $\langle u, v\rangle = \langle u, w\rangle$ and $\langle u\rangle \cap \langle w\rangle = 1$. We replace v by w if necessary.

Since $k = 2$, it follows that $A = \langle a\rangle Z(H)$, where $o(a) = 4$. If $o(v) > 4$, then $k > 1$ forces $\langle a\rangle \cap \langle u\rangle\langle v\rangle = 1$. Let $Q = \langle a, u, v\rangle$. By (2) and (4), we have $Y = Q' = \Omega_1(Q)$, in particular $Q \lhd G$. Let $P = Q\langle y\rangle$. If $\Phi(P) \nleq Q$, then $o(y) = 8$ and an involution in $\Phi(P)Q \setminus Q$ is equal to qy^2 is for some $q \in Q$. If $q \notin Z(H)$, then $\langle qy^2, Z(H)\rangle \in \mathcal{A}$, contradicting $k > 1$. Accordingly, $[qy^2, Q] = 1$. If $o(v) > 4$, then P satisfies Lemma 2.11 with $x_1 = u$, $x_2 = v$, $x_3 = a$, if $o(v) = 4$, then P fits the criteria of Lemma 2.12. Thus G is not core-2. Consequently:

(5) $|Y| < 8$ or $|A : Z(H)| > 2$.

Suppose that $|Y| = 8$. By (5), we have $|A : Z(H)| > 2$. By Lemma 2.9 and since $|H' : [A, H]| = 2$, $[A, H] = \langle s, t\rangle \cong E_4$, and $H = \langle u, v, a, b\rangle Z(H)$, where $\langle a, b\rangle Z(H) = A$, $[u, a] = s$, $[u, b] = 1$, $[v, a] = 1$, $[v, b] = t$, and $Y = [A, H] \times \langle [u, v]\rangle$. Let $B = \langle u, b\rangle Z(H)$; then B is a maximal normal abelian subgroup of H, though not necessarily an element of $\mathcal{A}$. Lemma 2.9 nevertheless yields the existence of $w \in \{u, ub\}$ with $b_H(w) = 1$, i.e. $[w, H] = \langle s\rangle$. However, this implies that $Y = [A, H]$, a contradiction. Hence

(6) $|Y| < 8$.

Assume that $|A : Z(H)| = 2$, and let $\langle a\rangle Z(H) = A$ and $H = A\langle u, v\rangle$. Since $Y = \langle [a, u], [a, v]\rangle$, either $[u, v] = 1$ or there is an element $w \in \{u, v, uv\}$ such that $[u, v] = [a, w]$. In either case, $H = AC_H(w)$ for some $w \in H \setminus A$. No element of A has breadth 1 in H, whence $\Phi(G) \leq Z(H) \leq C_H(w)$. Thus we have $C_H(w) \in \mathcal{A}$, a contradiction. Hence

(7) $|A : Z(H)| = 4$.

Let a be some element of A of order 4 with $\langle a\rangle \ntriangleleft H$. As previously noted, $\langle a\rangle$ has a complement in A of exponent greater than 4. Let $A = \langle a\rangle \times D$. By (6) and since $d(A) = d(\Omega_1(A))$, $A = \langle a\rangle \times \langle d\rangle$ with $o(d) = \exp A$. If $x \in G \setminus H$, then

$x^2 \in \Omega_2(A)$, whence $\Phi(G) \leq \langle a, d^2 \rangle$. According to Lemma 2.9, we may assume $b_H(d) = 1$ and $A = \langle d, c \rangle$ with $b_H(c) = 1$. Note that

$$\Phi(H) \leq Z(H) = Z(H) \cap A = \Phi(A) = \langle a^2 \rangle \times \langle d^2 \rangle.$$

This and $o(d) \geq 8$ entail that, for $u \in H$, there is an element $d^* \in \langle d \rangle$ satisfying $(ud^*)^2 \in \langle a^2 \rangle$.

We shall now show that $b_H(a) > 1$. Assuming otherwise, there is $u \in H \setminus A$ with $[u, a] = 1$ and $u^2 \in \langle a^2 \rangle$. Thus $\langle u, a, d^2 \rangle$ becomes an element of $\mathcal{A}$ that contains an involution not centralised by H, contradicting $k > 1$ and (4). Together with (6), $Y = [A, H] = [a, H]$ and the element c from the last paragraph may be taken to be ad.

Since $Y = [a, H]$, there is $u \in H$ with $u^2 \in \langle a^2 \rangle$ and $[u, a] = \langle a^2 \rangle$. Since $\langle a \rangle \ntriangleleft G$, we may take $[u, G] = \langle a^2 \rangle = \langle [u, a] \rangle$; interchanging d and ad, if necessary, there is no loss in taking $[u, d] = 1$. If $\Phi(G) \nleq \Phi(A)$, then $a\langle d^2 \rangle = e\langle d^2 \rangle$ with $b_H(e) \leq 1$; yet this implies $b_H(a) = 1$ which we have seen to be false. Thus $\Phi(G) = \Phi(A)$ and $B = \langle u, a^2, d \rangle \in \mathcal{A}$. Now $k = 2$ yields $u^2 = a^2$, in particular $B = \langle u \rangle \times \langle d \rangle$. Let $\Omega_2(d) = \langle d^* \rangle$; then $\langle ud^* \rangle$ is cyclic of order 4, of breadth 1 in H and not normal in H on account of $[a, ud^*] = a^2$. Replacing A by B in the preceding paragraph yields a contradiction. □

3.2 The case $k = 1$

This final section is devoted to deriving a contradiction from the assumption $k = 1$, by now the only remaining case. We start by arranging some notation.

Let a be an involution in $A \setminus Z(H)$. By Lemma 3.2, we have $A = \langle a \rangle \times \langle b \rangle \times D$, where $\Omega_1(\langle b \rangle D) = Z$, $[a, H] \nleq D$ and every subgroup of D is normal in G. Let $o(b) = 2^n$. We note that, unless $n = 1$, any $c \in b\langle a, D \rangle$ of order 2^n may replace b without harm. Let $x \in G \setminus H$.

Our first goal is establishing that $G = H$ and we assume this is not so for the time being. Recall that $G > H$ entails $\exp A > 4$. Then $[A, x]$ is of exponent greater than two and each of its elements is inverted by x. Now $\Phi(\langle a, x \rangle) = \langle x^2, [a, x] \rangle \leq C_A(x)$, whence neither $\langle x \rangle \Phi(\langle a, x \rangle)$ nor $\langle ax \rangle \Phi(\langle a, x \rangle)$ is a normal subgroup. It follows that $\langle a, x^2, [a, x] \rangle \triangleleft G$, in other words:

(1) $[a, G] \leq \langle y^2, [a, y] \rangle$ whenever $y \in G \setminus H$.

Suppose that $b_H(a) < b(a)$. By (1), this entails that $b_H(a) = 1$. For $u \in C_H(a)$, $\langle u^2, a \rangle$ cannot be normal in G, whence one of $\langle u \rangle$ and $\langle au \rangle$ must be normal. In particular, $\langle u \rangle \triangleleft C_H(a)$, which makes $C_H(a)$ a Dedekind group. But $C_H(a)$ cannot be Hamiltonian – that would imply $\exp A = 4$ and $G = H$. So $C_H(a)$ is an abelian subgroup of G properly containing A.

Accordingly, $G = HC_G(a)$ and we may assume $x \in C_G(a) \setminus H$. By (1), we have $[a, H] \leq \langle \hat{x} \rangle$, in particular $b(a) = 1$. Observe that $o(x) > 2$ because of $\langle a \rangle \ntrianglelefteq H$. We know that $x \notin H$ implies that $\exp C_A(x) \leq 4$ and $o(x) \leq 8$. By (1), $\hat{b}D = \hat{x}D$. Note that $[x, Y] = 1$, whence part (b) of Lemma 3.1 yields that $\bar{x}$ inverts the elements of $\overline{A}$. Assume that $o(x) = 8$. Then $n \geq 2$ and there is a generator b^* of $\langle b^{2^{n-2}} \rangle$ such that $x^2 \equiv a^\varepsilon b^* \pmod{D}$ for some $\varepsilon \in \{0, 1\}$. Thus b^* is not inverted by x and $n = 2$, whence there is no loss in taking $b = x^2$. Since $\exp A > 4$, we must have $\exp D > 4$. Pick $d \in \mho_1(D)$ of order 4. Then $[x^2 d, x] = d^2 = [ax^2 d, x]$, and (1) yields $\langle a, x^2 d \rangle_G = 1$, a contradiction. It follows that every element of $xC_H(a)$ has order four, while (1) yields that $\langle (ux)^2 \rangle = [a, G] = \langle x^2 \rangle$ whenever $u \in C_H(a)$. This implies that $C_H(a)$, whose every element is now inverted by x, is an abelian maximal subgroup of H properly containing A. Accordingly:

(2) $G = H$.

If $b(a) > 1$, then $\langle a, c^2 \rangle \ntrianglelefteq G$ for $c \in A$, and, since $\langle c \rangle$ or $\langle ac \rangle$ is therefore normal in G, $C_G(a)$ is a Dedekind group. It will become evident that this fact provides a quick finish to the proof, but we need to dispense with the case $b(a) = 1$ first. Hence we assume $b(a) = 1$ for now.

Assume that $\exp D > 2^n$. Pick $d \in D$ with $o(d) = \exp D$ and let $d^* \in \langle d^2 \rangle$ be of order 2^n. Replacing b by ab, bd^* or abd^* if necessary, we may assume that $[a, G] \nleq \langle b \rangle \lhd G$. Observe that $\langle a, (bd)^2 \rangle \ntrianglelefteq G$. If $\langle abd \rangle \lhd G$, then, since $[a, G] \nleq \langle \hat{d} \rangle$, $C_G(b) \cap C_G(d) \leq C_G(a)$. Since every subgroup of D is normal in G, Lemma 2.1 says $C_G(d) = C_G(D)$; thus $C_G(d) \cap C_G(b) = C_G(A) = A$, i.e. $|G : A| \leq 4$. This leaves $\langle bd \rangle$ the only candidate for a maximal subgroup of $\langle a, bd \rangle$ to be normal in G. However, $\langle b \rangle \lhd G \rhd \langle d \rangle$, so $\langle bd \rangle \lhd G$ means $b \in Z(G)$ and $A = C_G(a) \cap C_G(d)$ has index at most 4 in G. Therefore:

(3) If $b(a) = 1$, then $\exp A = 2^n$.

Assume that $\exp D = 2^n$ and let $d \in D$ be of order 2^n. At least one of the subgroups $\langle a, (bd)^2 \rangle$ and $\langle a, b^2 \rangle$ is not normal in G, which makes one of the subgroups $\langle b \rangle, \langle ab \rangle, \langle bd \rangle, \langle abd \rangle$ normal. Replacing b accordingly, we may once again assume $\langle b \rangle \lhd G$. If $C_G(a) \leq N_G(\langle bd \rangle)$, then every subgroup of A is normalised by $C_G(a)$. Lemma 2.1 then says $|C_G(a) : A| = 2$, a contradiction. Thus neither $\langle bd \rangle$ nor $\langle abd \rangle$ is a normal subgroup, whence $\langle a, (bd)^2 \rangle$ must be one. Thus $[a, G] = \langle \hat{b}\hat{d} \rangle$, in particular $\mho_{n-1}(D) = \langle \hat{d} \rangle$. Hence $D = \langle d \rangle \Omega_{n-1}(D)$, while Lemma 2.1 says $\Omega_{n-1}(D) \leq Z(G)$. Furthermore,

$$C_G(a) \cap C_G(b) \cap C_G(d) = C_G(A) = A,$$

whence G fits the hypothesis of Lemma 2.10 and a contradiction ensues. We note:

(4) If $b(a) = 1$, then $\exp D < 2^n$.

We discard the possibility that $n = 2$. By (4), $n = 2$ implies that $D \leq \Omega_1(Z(G))$. Either at least one of $\langle b \rangle$ and $\langle ab \rangle$ is therefore normal in G, or $\Phi(G) \leq Y$. Since $aZ \cap Z(G) = \emptyset$, it follows that $\Phi(G) \leq Y$ would entail $\Phi(G) \leq Z$, to which Lemma 2.9 provides a contradiction. It follows that we may take $\langle b \rangle \lhd G$. But then $A = C_G(a) \cap C_G(b)$ has index at most four in G.

(5) If $b(a) = 1$, then $n > 2$.

Suppose that neither of the subgroups $\langle b \rangle$ and $\langle ab \rangle$ is normal in G. Let $\exp D = 2^m$ and let $\langle b_1 \rangle = \Omega_m(\langle b \rangle)$. Our most recent assumption entails that $\langle a, b^2 \rangle \lhd G$, i.e. $[a, G] = \langle \hat{b} \rangle$. Since $\langle a, (b_1 d)^2 \rangle$ cannot be normal in G, either $\langle b_1 d \rangle \lhd G$, i.e. $D \leq Z(G)$, or $\langle ab_1 d \rangle \lhd G$ and $C_G(a) = C_G(D)$. Thus $C_G(a) \leq C_G(D)$ in either case. Let $u \in C_G(a) \setminus A$. Then $u^2 \in C_A(u) = \langle a, b^2 \rangle D$ and (5) yields the existence of $b^* \in \langle b \rangle$ satisfying $(ub^*)^2 \in \langle a \rangle D$. Let $d \in D$ and $x \in G \setminus C_G(a)$; then $[ad, x] \in \hat{b}\langle \hat{d} \rangle$, and $\langle ad \rangle \ntriangleleft G$. Consequently, every element of $C_G(a)$ is in a coset $u\langle b \rangle$, where $u^2 \in D$. Take $u \in C_G(a)$ with $u^2 \in D$. Certainly, $\langle a, u^2 \rangle \ntriangleleft G$, so that one of $\langle u \rangle$, $\langle ua \rangle$ is a normal subgroup of G, in particular $\langle u \rangle \lhd C_G(a)$. Letting $L = \{u \in C_G(a) | u^2 \in D\}$, L has emerged to be a subgroup of G that is even a Dedekind group. Note that $L \cap A = \langle a, \hat{b} \rangle D$ and $|G : L\langle b^2 \rangle| = 4$. Suppose L is Hamiltonian. Then $L = Q \times E$, where $Q = Q_8$ and E is elementary abelian with $a \in E$. Let $v \in Q$ be of order 4. Since $v \in L$, $\langle v^2 \rangle = Q' \neq \langle \hat{b} \rangle$. Since $n > 2$, we have $[vb^{2^{n-2}}, Q] = Q' = [avb^{2^{n-2}}, Q]$, whence none of the three maximal subgroups of $\langle a, vb^{2^{n-2}} \rangle$ is normal in G. Accordingly:

(6) If $b(a) = 1$, then $\langle b \rangle \lhd G$ or $\langle ab \rangle \lhd G$.

By (6), we are free to assume that $\langle b \rangle \lhd G$. Thus $D \not\leq Z(G)$ – otherwise $C_G(a) \cap C_G(b) = A$ and $|G : A| = 4$. As before, we consider $d \in D$ of order $2^m = \exp D$. By Lemma 2.1, the fact that $D \not\leq Z(G)$ is equivalent to $d \notin Z(G)$. Now (4) yields the existence of an element b^* of $\langle b^2 \rangle$ with $o(b^*) = 2^m$ and $\langle b^* d \rangle \ntriangleleft G$. If $\langle ab^* d \rangle \lhd G$, then

$$C_G(a) = C_G(d) = C_G(D),$$

and

$$A = C_G(a) \cap C_G(b),$$

of index at most 4. Accordingly, $\langle a, (b^* d)^2 \rangle \lhd G$, i.e. $[a, G] = \langle \hat{b}\hat{d} \rangle$. It follows that $D = \langle d \rangle \Omega_{m-1}(D)$ and D is a direct product $\langle d \rangle \times E$, where $E \leq \Omega_{m-1}(Z(G))$. But now G satisfies the hypothesis of Lemma 2.10, and we finally obtain:

(7) $b(a) > 1$.

Let $L = C_G(a)$. As has been pointed out, (7) implies that L is a Dedekind group. Assume that L is Hamiltonian, i.e. $L = Q \times E$, where $Q \cong Q_8$ and E is elementary abelian. Considering the subgroups $\langle a, w \rangle_G$ with $w \in Q$, we see that Q

can be chosen to satisfy $[Q, G] = Q'$. This in turn entails $G = QC_G(Q)$. So A, being a maximal abelian normal subgroup of L, is of the form $A = \langle u, E\rangle$ for some $u \in Q \setminus Z(Q)$. Let $C_G(Q) = K$. For $x \in K$, we have $x^2 \in C_A(Q) = Y$, so $\Phi(K) \leq Z$, since no element of aZ is a square in G. However, this yields that $\Phi(G) = \Phi(K)\Phi(Q) \leq Z$, and Lemma 2.9 says $|G : A| \leq 4$. Accordingly:

(8) $C_G(a) = A$.

By (8), $b(a) \geq 3$. At the possible expense of interchanging b and ab, we may assume $\langle b\rangle \lhd G$. Let $d \in D$. If $\langle abd\rangle \lhd G$, then

$$[a, G] \leq [bd, G][abd, G] \leq \langle \hat{b}, \hat{d}\rangle,$$

a contradiction. This yields $\langle a, bd\rangle_G = \langle bd\rangle$. It follows that:

(9) Every subgroup of $\langle b\rangle D$ is normal in G.

Now (9) and $b(a) \geq 3$ combine to yield $\langle ac\rangle \not\lhd G$ whenever $c \in \langle b\rangle D$, in particular:

(10) $\Phi(G) \leq \langle b\rangle D$.

Let $K = C_G(\langle b\rangle D)$. By (9), $|G : K| \leq 2$ and (10) says that $[K, \Phi(G)] = 1$. Let $v \in G \setminus K$ and $u \in K$. Then $[u, v^2] = 1$, (10) and Lemma 3.4 together imply that either $[u, v] \in \Omega_1(\langle b\rangle D) = Z$ or $[u, v]$ has order four and is inverted by v. However, $\langle a, v^2, [a, v]\rangle \not\lhd G$, whence $[v, G] \leq \langle v^2\rangle Z \leq C_A(v)$, so the latter cannot happen. It follows that $G' \leq Z$, and Lemma 2.9 completes the proof.

Acknowledgments. The author would like to thank the referee for many helpful suggestions and corrections of large and small mistakes.

Bibliography

[1] N. Blackburn, Über Involutionen in 2-Gruppen, *Arch. Math.* **35** (1980), 75–78.

[2] C. D. H. Cooper, Power automorphisms of a group, *Math. Z.* **107** (1968), 355–356.

[3] G. Cutolo, E. I. Khukhro, J. C. Lennox, J. Wiegold, S. Rinauro and H. Smith, Finite core-p p-groups, *J. Algebra* **188** (1997), 701–719.

[4] G. Cutolo, E. I. Khukhro, J. C. Lennox, J. Wiegold, S. Rinauro and H. Smith, Locally finite groups all of whose subgroups are boundedly finite over their cores, *Bull. Lond. Math. Soc.* **29** (1997), 563–570.

[5] G. Cutolo, H. Smith and J. Wiegold, On core-2-groups, *J. Algebra* **237** (2001), 813–841.

[6] J. C. Lennox, H. Smith and J. Wiegold, Finite p-groups in which subgroups have large cores, in: *Infinite Groups 1994* (Ravello 1994), Walter de Gruyter, Berlin (1995), 163–169.

[7] V. D. Mazurov and E. I. Khukhro, *The Kourovka Notebook. Unsolved Problems in Group Theory. 18th Edition*, Russian Academy of Sciences, Novosibirsk, 2014.

[8] G. Parmeggiani and B. Stellmacher, p-groups of small breadth, *J. Algebra* **213** (1999), 52–68.

Received November 11, 2015; revised July 1, 2016.

Author information

Bettina Wilkens, Department of Mathematics, University of Namibia,
Private Bag 13301, Windhoek, Namibia.
E-mail: bwlklk@gmail.com