DERIVED SUBGROUPS OF PRODUCTS OF AN ABELIAN AND A CYCLIC SUBGROUP

by

M. D. E. Conder

Department of Mathematics
University of Auckland
Private Bag 92019, Auckland
NEW ZEALAND

E-mail: conder@math.auckland.ac.nz

and

I. M. Isaacs

Mathematics Department
University of Wisconsin
480 Lincoln Drive
Madison WI 53706
USA

E-mail: isaacs@math.wisc.edu

ABSTRACT: Let G be a finite group and suppose that $G = AB$, where A and B are abelian subgroups. By a Theorem of N. Ito, the derived subgroup G' is known to be abelian. If either of the subgroups A or B is cyclic, then more can be said. In this paper it is shown, for example, that $G'/(G' \cap A)$ is isomorphic to a subgroup of B in this case.

The first author was partially supported by grants from the N.Z. Marsden Fund and Centres of Research Excellence Fund. The second author was partially supported by a grant from the U.S. National Security Agency.

1. Introduction

A number of articles investigating the properties of groups expressible as a product AB of abelian subgroups A and B were published in the 1950s. Perhaps the most significant of these was a 1955 paper by N. Ito [**10**] in which he proved (using a surprisingly easy argument) that any such group is metabelian. In other words, if $G = AB$, where A and B are abelian subgroups, then the derived subgroup G' is necessarily abelian.

The case where A and B are both cyclic was investigated by L. Rédei, J. Douglas, B. Huppert and P. M. Cohn. From a careful reading of Rédei's paper [**11**], one can see that he proved that if $G = AB$, where A is infinite cyclic and B is finite and cyclic, then the derived subgroup G' is generated by an element of B and at most one other element (and hence in particular, if $G' \cap B = 1$ then G' is cyclic).

Rédei also proved a similar result for the case where A and B are both infinite cyclic, provided that one of A or B contains a non-trivial subgroup that is normalized by a non-trivial element of the other. Building on Rédei's work, Cohn [**2**] showed that the latter condition is always satisfied, and he proved also that if $G = AB$, where A and B are infinite cyclic and $G' \cap A = G' \cap B = A \cap B = 1$, then G' is cyclic.

The case where A and B are both finite and cyclic appears not to have been investigated in detail, other than by Huppert [**8**] and by Douglas in a series of four papers [**4, 5, 6, 7**]. Huppert showed that if G is a p-group of odd order, then G' is cyclic. (This also appears as Satz III 11.5 of [**9**].) In the papers by Douglas, the emphasis was on conjugacy of elements, but little was said about the structure of the group G or its derived subgroup.

Let us assume for the moment that $G = AB$ is finite, where A and B are abelian. Instead of limiting our attention to G', which by Ito's theorem we know is abelian, we consider more generally an arbitrary abelian normal subgroup K of G. We might expect (perhaps naively) that the group $K/(K \cap A)$ should somehow be controlled by the structure of B. We note for example that $|K/K \cap A| = |KA : A|$, and this divides $|G : A|$, which divides $|B|$, and so at least the order of $K/(K \cap A)$ is under control. If A is normal in G, we can say more: in that case $K/(K \cap A) \cong AK/A \subseteq AB/A \cong B/(A \cap B)$, and then since B is abelian, we may conclude that $K/(K \cap A)$ is isomorphic to a subgroup of B. In particular, if B is cyclic and $A \lhd G$, then $K/(K \cap A)$ is cyclic.

It is not always the case, however, that $K/(K \cap A)$ is cyclic. This is true if $|K|$ is odd and B is cyclic, but somewhat more generally, we will prove the following.

Theorem A. *Let $G = AB$ be finite, where A is abelian and B is cyclic. If K is any abelian normal subgroup of G with the property that the Sylow 2-subgroup of K is contained in G', then $K/(K \cap A)$ is cyclic.*

If B is not cyclic, then $K/(K \cap A)$ need not be isomorphic to a subgroup of B, even if $|K|$ is odd or $K = G'$. (We present some counter-examples in the final section of this paper.) Perhaps surprisingly, however, if A is cyclic then we do have such an isomorphism.

Theorem B. *Let $G = AB$ be finite, where A is cyclic and B is abelian. If K is any abelian normal subgroup of G with the property that the Sylow 2-subgroup of K is contained in G', then $K/(K \cap A)$ is isomorphic to a subgroup of B.*

It is not really necessary to assume that G is finite to establish results like these; it suffices that B is finite. To see why this is so, observe that if B is finite, then $|G : A| < \infty$, and thus $\overline{G} = G/N$ is a finite group, where $N = \mathrm{core}_G(A)$. In this situation, $NK \cap A = N(K \cap A)$ by Dedekind's lemma, and it is easy to see from this that $K/(K \cap A) \cong \overline{K}/(\overline{K} \cap \overline{A})$. To obtain information about $K/(K \cap A)$, therefore, it suffices to work in the finite group $\overline{G}$. Of course, we have $\overline{G} = \overline{A}\,\overline{B}$, and because B is finite and abelian, subgroups of $\overline{B}$ are isomorphic to subgroups of B.

The requirement on the Sylow 2-subgroup of K in Theorems A and B does not make sense if K is infinite, but since $(\overline{G})' = \overline{G'}$, it is clear that everything works if we take $K = G'$, and so we have the following.

Corollary C. *Let $G = AB$, where A and B are abelian and B is finite. If A or B is cyclic, then $G'/(G' \cap A)$ is isomorphic to a subgroup of B.*

An easy consequence of these results is the following.

Corollary D. *Let $G = AB$, where A and B are cyclic and at least one of A and B is finite. Then two elements suffice to generate G'.*

Proof. We may assume that B is finite, and thus $G'/(G' \cap A)$ is cyclic by Corollary D. Since also $G' \cap A$ is cyclic, the result follows. ▌

If neither A nor B is assumed to be cyclic, then although $K/(K \cap A)$ need not be isomorphic to a subgroup of B, it is nevertheless true that the structure of B does exert some control over the structure of $K/(K \cap A)$. To state one result in this direction, we recall that the **rank** of a finite abelian group X is the smallest number of elements that suffice to generate X, and we denote this by $r(X)$.

Theorem E. *Let $G = AB$ be finite, where A and B are abelian, and let K be an abelian normal subgroup of G. Then $r(K/(K \cap A)) \leq f(r(B))$ for some function f which is independent of the group G.*

As we have already mentioned, there are examples that set limits on how far one can extend Theorems A, B and E.

Theorem F. *Let p be any prime. Then there exists a p-group G expressible as AB, where A and B are abelian subgroups, and such that $G'/(G' \cap A)$ is not isomorphic to any subgroup of B; in fact, $r(G'/(G' \cap A))$ can exceed $r(B)$ by an arbitrarily large amount.*

The structure of this paper is as follows. In section 2 we begin with some preliminary facts about commutators and abelian normal subgroups, including Ito's theorem. We investigate the special case where G' is a 2-group (and other matters) in section 3, and in section 4 we prove some preliminary facts about groups triply factorizable in the form $UV = UK = VK$ where U, V and K are subgroups with pairwise trivial intersections. We prove Theorems A and B in section 5, Theorem E in section 6, and Theorem F in section 7.

Much of this work resulted from serendipitous observations made by the first author in the study of regular Cayley maps for finite abelian groups, and computations using the Magma system [**1**]. (A **regular Cayley map** for a group A is an orientable map whose orientation-preserving automorphism group acts regularly on the directed edge set and has a subgroup isomorphic to A that acts regularly on the vertex set.) In turn, Corollary C has been used to develop the theory of such regular maps; see [**3**]. The authors are grateful to Tom Tucker (a co-author of [**3**]) for his contributions to this paper, especially Lemma 5.2 and an earlier special case of Theorem B.

2. Ito's Theorem

For completeness, we include a proof of Ito's theorem. (Essentially the same proof can also be found in Huppert's book [**9**].) We begin with an easy observation about the subgroup $[A, B]$ generated by elements of the form $[a, b] = a^{-1}b^{-1}ab$ for $a \in A$ and $b \in B$.

Lemma 2.1. *Let $G = AB$, where A and B are abelian subgroups. Then $G' = [A, B]$.*

Proof. We have $[A, B] \lhd A$ and $[A, B] \lhd B$, so $[A, B] \lhd AB = G$. Moreover, in the group $G/[A, B]$ we see that the images of A and B are abelian subgroups that centralize each other. It follows that $G/[A, B]$ is abelian, and thus $G' \subseteq [A, B]$. The reverse containment is obvious. ▌

Theorem 2.2 (Ito). *Let $G = AB$, where A and B are abelian subgroups. Then the derived subgroup G' is abelian.*

Proof. By Lemma 2.1, we see that G' is generated by commutators of the form $[a, b]$ where $a \in A$ and $b \in B$, and therefore it suffices to prove that any two such commutators commute.

Let $a, c \in A$ and $b, d \in B$ and write b^c as a product ef, where $e \in A$ and $f \in B$. Similarly, write a^d as a product hg where $h \in B$ and $g \in A$. Then we have

$$[a, b]^{cd} = [a^c, b^c]^d = [a, ef]^d = [a, f]^d = [a^d, f^d] = [hg, f] = [g, f]\,,$$

where the third equality holds because a and e commute in A and the last equality holds because f and h commute in B. Similarly,

$$[a,b]^{dc} = [a^d, b^d]^c = [hg, b]^c = [g, b]^c = [g^c, b^c] = [g, ef] = [g, f]$$

since h and b commute in B, and g and e commute in A.

We now have $[a,b]^{cd} = [a,b]^{dc}$, and thus $[c^{-1}, d^{-1}] = cdc^{-1}d^{-1}$ centralizes $[a,b]$ for all choices of elements $c \in A$ and $d \in B$. The result follows. ▮

We close this section with another standard fact about commutators and abelian groups.

Lemma 2.3. *Let K be an abelian normal subgroup of G, and let $a \in G$. Then $[K,a] \cong K/\mathbf{C}_K(a)$ and $[K,a] = (K\langle a \rangle)'$.*

Proof. Since K is abelian, the map $x \mapsto [x,a]$ is an endomorphism of K with kernel $\mathbf{C}_K(a)$ and image $[K,a]$. Thus $[K,a] \cong K/\mathbf{C}_K(a)$, as claimed.

Since $[K,a]^a = [K^a, a] = [K,a]$, we see that $\langle a \rangle$ normalizes $[K,a]$. But a, and hence also $\langle a \rangle$, acts trivially on $K/[K,a]$, and thus we have $[K,a] \supseteq [K, \langle a \rangle] = (K\langle a \rangle)'$, where the latter equality holds by Lemma 2.1. The reverse containment is clear. ▮

3. The special case of 2-groups

As is apparent from the statements of Theorems A and B, extra complications arise when the prime 2 is involved. The following lemma on commutators will be helpful to handle that situation. In the statement of this result, the extended commutator $[u,v,w]$ denotes the element $[[u,v],w]$, and in the proof we use two standard commutator identities, namely $[uv,w] = [u,w]^v[v,w]$ and its inverse, $[w,uv] = [w,v][w,u]^v$.

Lemma 3.1. *Let K be an abelian normal subgroup of G, and suppose that $x, y \in G$ and that $[x,y] \in K$. Then $[x^m, y, x] = [x, y, x^m]$ for every integer $m \geq 0$.*

Proof. The assertion is trivial if $m = 0$, and so we may assume that $m > 0$ and proceed by induction on m. Observe first that since x and y commute modulo K, the elements x^r and y also commute modulo K, and therefore $[x^r, y] \in K$ for every positive integer r. We now find that

$$[x^m, y] = [x^{m-1}x, y] = [x^{m-1}, y]^x[x,y] = [x^{m-1}, y]^x a\,,$$

where $a = [x,y] \in K$. It follows that

$$[x^m, y, x] = [[x^{m-1}, y]^x a, x] = [[x^{m-1}, y]^x, x]^a [a, x]\,,$$

and hence that

$$[x^m, y, x] = [[x^{m-1}, y], x]^{xa}[a,x] = [x^{m-1}, y, x]^{xa}[a,x].$$

But $[x^{m-1}, y]$ and hence also $[[x^{m-1}, y], x]^x$ lies in the abelian normal subgroup K, and therefore $[x^{m-1}, y, x]^x$ is centralized by $a \in K$. Thus

$$[x^m, y, x] = [x^{m-1}, y, x]^{xa}[a, x] = [x^{m-1}, y, x]^x[a, x].$$

Our inductive hypothesis is that $[x^{m-1}, y, x] = [x, y, x^{m-1}] = [a, x^{m-1}]$, and so we obtain

$$[x^m, y, x] = [a, x^{m-1}]^x[a, x] = [a, x][a, x^{m-1}]^x = [a, x^{m-1}x] = [a, x^m],$$

as required. ∎

Next, we introduce what we shall call the **standard notation**. Given a normal subgroup K of $G = AB$, where A and B are subgroups of G, we write $H = KA \cap KB$, and we set $U = H \cap A$ and $V = H \cap B$. Our next result establishes some basic facts about this situation. In its proof, we appeal several times to the following elementary consequence of Dedekind's lemma: if X, Y and H are subgroups of some group and $X \subseteq H \subseteq XY$, then $H = X(H \cap Y)$.

Lemma 3.2. *Suppose that K is a normal subgroup of $G = AB$, and assume the standard notation. Then $H = KU = KV = UV$. Also if H is finite, then $|H|$ divides $|K|^2|U \cap V|$.*

Proof. Observe first that $K \subseteq H$ since $H = KA \cap KB$. We have $K \subseteq H \subseteq KB$, and so by Dedekind's lemma, $H = K(H \cap A) = KU$, and similarly, $H = KV$. Also since $B \subseteq KB \subseteq G = AB$, Dedekind's lemma yields $KB = (KB \cap A)B$. But $KB \cap A = KB \cap KA \cap A = H \cap A = U$, and thus we have $KB = UB$. Moreover, $U \subseteq H \subseteq KB = UB$, and a further application of Dedekind's lemma yields $H = U(H \cap B) = UV$, as required.

Now assume that H is finite. Then $|U : U \cap V| = |UV : V| = |KV : V| = |K : K \cap V|$ divides $|K|$, and similarly $|V : U \cap V|$ divides $|K|$. Thus $|H| = |U : U \cap V||V : U \cap V||U \cap V|$ divides $|K|^2|U \cap V|$, and the proof is complete. ∎

Lemma 3.3. *Suppose that $G = AB$, where A and B are abelian. Let $K = G'$ and suppose that K_0 is a normal subgroup of G contained in K, of index $|K : K_0| = 2$. Then there exist 2-elements $a \in A$ and $b \in B$ such that $[b, a] \notin K_0$. Furthermore, neither a nor b can lie in $H = KA \cap KB$.*

Proof. By Lemma 2.1, we have $K = G' = [B, A]$, and since $K_0 < K$, we can choose $b \in B$ and $a \in A$ such that $[b, a] \notin K_0$. Write $a = a_2a_0$ where a_2 has 2-power order and a_0 has odd order and similarly, write $b = b_2b_0$. Now let $\overline{G} = G/K_0$, and use the standard "bar" convention, in which the overbar denotes the canonical homomorphism from G onto $\overline{G}$. (Thus $\overline{g} = K_0g$ for every element $g \in G$.) Observe that $|(\overline{G})'| = 2$, and hence each conjugacy class of $\overline{G}$ has size 1 or 2. It follows that elements of odd order in $\overline{G}$ act trivially on each class, and hence such elements are central. Thus $[\overline{b}, \overline{a}] = [\overline{b_2}, \overline{a_2}]$, and so $[b_2, a_2] \notin K_0$ and we can therefore assume that a and b are 2-elements.

Assuming the standard notation now, and appealing to Lemma 3.2, we see that $[H, A] = [UK, A] = [K, A] \subseteq K_0$, where the second equality holds because U is a subgroup of the abelian group A, and the containment holds since K/K_0 is a normal subgroup of order 2 in G/K_0, and hence is central. But $[b, A] \nsubseteq K_0$, and so $b \notin H$. Similarly, $a \notin H$ and the proof is complete. ▌

We can now prove our first major theorem. Recall that if $G = AB$, where A and B are abelian, then G' is abelian (by Ito's theorem), and so the assertion of the following theorem makes sense.

Theorem 3.4. *Let $G = AB$ be finite, where A is abelian and B is cyclic, and assume that G' is a 2-group. Then $G'/(G' \cap A)$ is cyclic.*

Proof. Assume the contrary, and that G is a counterexample of minimum possible order. Write $K = G'$ and $R = K \cap A$.

We first argue that if $1 < N \lhd G$ with $N \subseteq K$, then K/NR is cyclic. To see this, write $\overline{G} = G/N$, and use the "bar" convention to denote by $\overline{S}$ the image of any subgroup $S \subseteq G$ under the canonical homomorphism from G onto $\overline{G}$. Note that $\overline{G} = \overline{A}\,\overline{B}$, where $\overline{A}$ is abelian and $\overline{B}$ is cyclic. As $\overline{K} = \overline{G'} = (\overline{G})'$ is a 2-group, the minimality of G implies that $K/(K \cap NA) \cong \overline{K}/(\overline{K} \cap \overline{A})$ is cyclic. Also since $N \subseteq K \cap NA \subseteq NA$, it follows by Dedekind's lemma that $K \cap NA = N(K \cap NA \cap A) = N(K \cap A) = NR$, and hence K/NR is cyclic, as claimed.

Suppose now that $\Phi(K) > 1$, so that we can take $N = \Phi(K)$ in the previous paragraph. In this situation, $NR/R = \Phi(K/R)$, and so the Frattini factor group of K/R is isomorphic to K/NR, which is cyclic. It then follows that K/R is cyclic, as desired, and so we can assume that $\Phi(K) = 1$, and hence that K is elementary abelian.

Now let H, U and V be as in the standard notation, and observe that $G' = K \subseteq H$, so that $H \lhd G$. Also $U \cap V$ is centralized by both A and B (since $U \subseteq A$ and $V \subseteq B$), so $U \cap V \subseteq \mathbf{Z}(AB) = \mathbf{Z}(G)$, and by Lemma 3.2, we find that $|H : U \cap V|$ divides $|K|^2$, which is a power of 2. It follows that $H/\mathbf{Z}(H)$ is a 2-group, and so H is nilpotent and all odd-order subgroups of H are central.

If U centralizes K, then $U \lhd KU = H$. In this case, we see by Lemma 3.2 that $K/R = K/(K \cap U) \cong KU/U = UV/U \cong V/(U \cap V)$, which is cyclic, as required. We can assume, therefore, that $\mathbf{C}_K(U) < K$. Writing $Z = \mathbf{C}_K(U)$, we see that $Z = K \cap \mathbf{Z}(KU) = K \cap \mathbf{Z}(H)$, and thus $Z \lhd G$ since $H \lhd G$. Furthermore, Z is non-trivial because H is nilpotent. Also $R = K \cap A \subseteq \mathbf{C}_K(U) = Z$, so taking $N = Z$ in the second paragraph above, we find that $K/Z = K/ZR$ is cyclic, and thus $|K : Z| = 2$ because K is elementary abelian.

We argue next that A centralizes Z. To see this, let A_0 be the Hall 2-complement of A and note that $[K, A_0] \subseteq Z < K$ since K/Z is central in G/Z (because it has order 2 and is normal). It follows by Fitting's lemma that $\mathbf{C}_K(A_0)$ is non-trivial. Furthermore, since the 2-group A/A_0 acts on the non-trivial 2-group $\mathbf{C}_K(A_0)$, it follows that A has non-trivial fixed points in K, and so the subgroup $Y = \mathbf{C}_K(A)$ is also non-trivial. Observe that $R \subseteq Y \subseteq Z$ and that $Y = K \cap \mathbf{Z}(KA) \lhd G$ since $KA \lhd G$ (because $G' = K \subseteq KA$). By our argument in the second paragraph (with N taken as Y) we find that $K/Y = K/RY$ is cyclic. But then $|K : Y| \leq 2$ since K is elementary, and it follows that $Y = Z$. Thus A centralizes Z, as claimed.

Since $Z \lhd G$ and $|K : Z| = 2$, Lemma 3.3 applies, so we can choose 2-elements $a \in A$ and $b \in B$ such that $[b, a] \notin Z$ and $b \notin H$. Let V_2 be the Sylow 2-subgroup of $V = H \cap B$ and note that $V \subseteq V_2\mathbf{Z}(H)$ since odd-order subgroups of H are central. Now $\langle b \rangle$ and V_2 are subgroups of the cyclic Sylow 2-subgroup of B, and since $\langle b \rangle \not\subseteq V_2$ because $b \notin H$, it follows that $V_2 \subseteq \langle b \rangle$. We can thus choose an integer m so that b^m generates V_2, and in particular, $b^m \in H = UK$.

Next, we have $[b^m, a] \in [UK, a] = [K, a]$ because the abelian group A contains both U and a. Since a centralizes Z, we find by Lemma 2.3 that $|[K, a]| = |K : \mathbf{C}_K(a)| \leq |K : Z| = 2$. Also $[K, a] = (K\langle a \rangle)'$, and $K\langle a \rangle \lhd G$ because $K = G'$, and hence $[K, a] \lhd G$. Since $[K, a]$ is a normal subgroup of G of order at most 2, and contains $[b^m, a]$, it follows that $[b^m, a] \in \mathbf{Z}(G)$, and thus $[b^m, a, b] = 1$. By Lemma 3.1, however, we have $[b^m, a, b] = [b, a, b^m]$, and thus $V_2 = \langle b^m \rangle$ centralizes $[b, a] \in G' = K$. Then $V \subseteq V_2\mathbf{Z}(H)$ centralizes $[b, a]$ and we conclude that $[b, a]$ is central in $KV = H$, and $[b, a] \in K \cap \mathbf{Z}(H) = Z$. This is a contradiction, however, completing the proof. ▌

In order to continue our study of 2-subgroups, we make the following definition. Given a group H, suppose that Z and K are normal 2-subgroups of H such that $Z \subseteq K$. We shall say that the triple (H, K, Z) is **good** if K/Z is cyclic and either $Z = K$ or $H' \subseteq \Phi(K_0)$, where K_0 is the unique subgroup of index 2 in K containing Z. Note that if (H, K, Z) is good and $N \lhd H$ is arbitrary, then $(\overline{H}, \overline{K}, \overline{Z})$ is good, where $\overline{H} = H/N$.

Theorem 3.5. *Suppose $G = AB$, where G is finite, A is abelian, B is cyclic, and G' is a 2-group. Let $K = G'$ and $R = K \cap A$, and let $H = KA \cap KB$, as in the standard notation. Then (H, K, R) is good.*

Proof. First, note that $R \subseteq \mathbf{Z}(KA)$ since K and A are abelian, and in particular, $R \subseteq \mathbf{Z}(H)$. Also, by Theorem 3.4, we know that K/R is cyclic. There is nothing to prove if $R = K$, and so we assume that $R < K$, and we let K_0 be the unique subgroup of index 2 in K containing R. We must show that $H' \subseteq \Phi(K_0)$.

Let $V = H \cap B$ as in the standard notation, and note that V is cyclic. By Lemma 3.2, we have $H = KV$, and thus if K is central in H, we see that H is abelian and there is nothing further to prove. We can assume therefore that K is not central in H, and we let $Z = K \cap \mathbf{Z}(H)$. Note that H and Z are normal in G since $G' = K \subseteq H$. We have

$R \subseteq Z < K$, and thus $Z \subseteq K_0$. But K and Z are normal in G and K/Z is cyclic, and as $Z \subseteq K_0 \subseteq K$, it follows that $K_0 \lhd G$.

As in the proof of Theorem 3.4, we observe that $|H : \mathbf{Z}(H)|$ is a power of 2 because K is a 2-group. Odd-order subgroups of H are therefore central, and we have $V \subseteq V_2\mathbf{Z}(H)$, where V_2 is the Sylow 2-subgroup of V.

By Lemma 3.3, we can choose 2-elements $a \in A$ and $b \in B$ such that $[b, a] \notin K_0$ and $b \notin H$. Observe that $[b, a] \in G' = K$ and since K/Z is cyclic and $[b, a] \notin K_0$, we have $K = Z\langle [b, a]\rangle$. Now $H = KV$, and so by Lemma 2.1, we have $H' = [K, V] = [K, V_2] = [Z\langle [b, a]\rangle, V_2] = [\langle [b, a]\rangle, V_2]$, where the second equality holds because $V \subseteq V_2\mathbf{Z}(H)$ and the last equality holds because $Z \subseteq \mathbf{Z}(H)$. Since $\Phi(K_0) \lhd G$, we see that to prove that $H' \subseteq \Phi(K_0)$, we need only show that $[b, a, v] \in \Phi(K_0)$ for some generator v of V_2.

Now a acts on K and centralizes $R = K \cap A$, and hence by Lemma 2.3, we see that $[K, a] \cong K/\mathbf{C}_K(a)$, which is a homomorphic image of K/R, and is therefore cyclic. Also $[K, a] = (K\langle a\rangle)'$, and since $K\langle a\rangle = G'\langle a\rangle \lhd G$, we find $[K, a] \lhd G$. Finally, we observe that $[K, a] \subseteq K_0$ since K/K_0 is central in G/K_0.

As $[K, a]$ is a cyclic 2-group that is normal in G, it follows that $[K, a, b] \subseteq \Phi([K, a]) \subseteq \Phi(K_0)$. Since $b \notin H$, we see that $\langle b\rangle \not\subseteq V_2$ and we can argue as in the proof of the previous theorem to conclude that $V_2 \subseteq \langle b\rangle$. (This follows because V_2 and $\langle b\rangle$ are subgroups of the cyclic Sylow 2-subgroup of B.) Thus b^m generates V_2 for some integer m, and in particular, $b^m \in H$.

Now $H = UK$, where $U = H \cap A$ as in the standard notation. We thus have $[b^m, a] \in [UK, a] = [K, a]$ and $[b^m, a, b] \in [K, a, b]$. By Lemma 3.1, we see that $[b^m, a, b] = [b, a, b^m]$, and thus $[b, a, b^m] \in [K, a, b] \subseteq \Phi(K_0)$. But b^m generates V_2, and as we have seen, that is enough to complete the proof. ▮

4. Triple factorization

As we proved in Lemma 3.2, when we consider a normal subgroup K of $G = AB$, we obtain a subgroup $H = KA \cap KB$ having a triple factorization $H = KU = KV = UV$ (where $U = H \cap A$ and $V = H \cap B$). We now study this situation in a little more detail, beginning with an almost trivial observation, followed by one that is more substantial.

Lemma 4.1. *Suppose $H = UV = UK = VK$, where U, V and K are subgroups of H with pairwise trivial intersections. Then $|U| = |K| = |V|$.*

Proof. We have $|U| = |H : V| = |K| = |H : U| = |V|$. ▮

Lemma 4.2. *Suppose $H = UV = UK = VK$, where U, V and K are subgroups of H with pairwise trivial intersections. Assume that V is cyclic and that K is a normal subgroup of H. Then U is cyclic, and if K is a p-group for some odd prime p, then also K is cyclic.*

We note here that the final assertion of Lemma 4.2 would fail if we were to allow K to be a 2-group. A counterexample in which K is non-cyclic can be constructed by taking H to be the semidirect product KV, where $V = \langle v \rangle$ is cyclic of order 4 and acts nontrivially on the elementary abelian subgroup K of order 4. If x is an element of K not centralized by V, then $U = \langle vx \rangle$ is cyclic of order 4, but its unique involution $(vx)^2$ lies in neither K nor V. Thus $K \cap U = 1 = V \cap U$, and hence also $H = UV = UK = VK$.

Proof of Lemma 4.2. Since $U \cong H/K \cong V$, we see that both U and H/K are cyclic, and also by Lemma 4.1 that $|U| = |K|$. Thus $|H| = |KU| = |K|^2$, and so H is a p-group.

We proceed by induction on $|K|$ to prove that K is cyclic. Suppose that L is any proper subgroup of K such that $L \lhd H$. Since $H = UV$, we can apply Lemma 3.2 to find a subgroup $W \subseteq H$ such that $W = LX = LY = XY$, where $X = W \cap U$ and $Y = W \cap V$. Since $L \subseteq K$, $X \subseteq U$ and $Y \subseteq V$, we see that L, X and Y have pairwise trivial intersections, and that Y is cyclic. Since $|L| < |K|$, it follows by the inductive hypothesis applied in the group W that L is cyclic.

Now assume that the subgroup K itself is not cyclic. Since $K \lhd H$ and H is a p-group, we can choose $L \lhd H$ with $L \subseteq K$ and $|K : L| = p$. By the result of the previous paragraph, L is cyclic, and thus K has a cyclic maximal subgroup. It follows from the known structure of non-cyclic p-groups of odd order with cyclic maximal subgroups that the set of elements of K of order dividing p forms a non-cyclic characteristic subgroup of K of order p^2. This subgroup is normal in H, and by the observations made in the previous paragraph, it cannot be proper in K. Hence we can assume that K is elementary abelian of order p^2. Also $|V| = |U| = |K| = p^2$, and we recall that V is cyclic.

Let $Z \subseteq K$ have order p, with $Z \subseteq \mathbf{Z}(H)$. Then $|K/Z| = p$, and so $K/Z \subseteq \mathbf{Z}(H/Z)$. Since H/K is cyclic, it follows that H/Z is abelian, and so $H' \subseteq Z$. Now let v generate V and write $v = uk$, with $u \in U$ and $k \in K$. Take $z = [k, u]$ and note that $z \in Z$, and hence that z is central in H. As $ku = ukz$, an easy induction gives $v^p = u^p k^p z^{p(p-1)/2}$. But p is odd and $z^p = 1 = k^p$, so we conclude that $v^p = u^p$. Thus $v^p \in U \cap V = 1$, which is a contradiction since v generates the cyclic group V of order p^2. ▌

Lemma 4.3. *Let $H = UV = UK = VK$, where U, V and K are subgroups of H with pairwise trivial intersections, and where K is finite and normal in H. If V and K are cyclic, and $V = \langle v \rangle$ where $v = uk$ with $u \in U$ and $k \in K$, then $K = \langle k \rangle$.*

Proof. Let $L = \langle k \rangle$ and note that $L \lhd H$ (since $K \lhd H$ and K is cyclic). As $H = UV$, it follows by Lemma 3.2 that there exist subgroups $X \subseteq U$ and $Y \subseteq V$ such that $LX = LY = XY$. The pairwise intersections of L, X and Y are trivial, and so we have $|L| = |Y|$ by Lemma 4.1. Also, since $k \in L$, we can write $k = xy$, with $x \in X$ and $y \in Y$, and we have $u^{-1}v = k = xy$. But since $U \cap V = 1$, each element of UV is uniquely expressible as a product of an element of U with an element of V, and hence $v = y$. As v generates V, it follows that $Y = V$, and thus $|L| = |Y| = |V| = |K|$, where the last equality follows from Lemma 4.1 applied to H. We conclude that $K = L = \langle k \rangle$, as required. ▮

5. Isomorphisms

In this section, we prove Theorems A and B. We shall need an elementary number-theoretic lemma, and to establish it, we begin with the following well known observation.

Lemma 5.1. *Let $s = 1 + p^f m$, where p is prime and $p^f > 2$. Then $s^p = 1 + p^{f+1} n$, where $n \equiv m$ mod p.*

Proof. It suffices to show that $s^p \equiv 1 + p^{f+1} m \mod p^{f+2}$. We have

$$s^p = (1 + p^f m)^p \equiv 1 + p^{f+1} m + \binom{p}{2} p^{2f} m^2 \mod p^{3f},$$

and since $3f \geq f + 2$, it therefore suffices to show that $\binom{p}{2} p^{2f}$ is divisible by p^{f+2}. If p is odd, then this holds because the binomial coefficient is divisible by p, and $2f + 1 \geq f + 2$. If $p = 2$ then by assumption $f \geq 2$, so $2f \geq f + 2$, and the result holds in that case too. ▮

It is convenient to introduce a little notation. If r and s are positive integers, we write $g_s(r) = 1 + s + s^2 + \cdots + s^{r-1}$. Note that if $s > 1$, then $g_s(r) = (s^r - 1)/(s - 1)$.

Lemma 5.2. *Let $q = p^e$, where p is prime and $e > 0$. Fix a positive integer s, and assume that $g_s(q)$ is divisible by q. In the case where $p = 2$, assume in addition that the number $g_s(q/2)$ is not divisible by q, and if $q = 2$, assume that $s = 1$. Then $g_s(q)/q$ is not divisible by p, and if $p = 2$ then $s \equiv 1$ mod 4.*

Proof. If $s = 1$, then $g_s(q) = q$ and there is nothing further to prove. We can assume, therefore, that $s > 1$. By assumption, q divides $g_s(q) = (s^q - 1)/(s - 1)$, and so p divides $s^q - 1$. Hence $s \equiv s^q \equiv 1$ mod p, where the first congruence holds by Fermat's theorem because q is a power of p. We can thus write $s = 1 + p^f m$, where $f \geq 1$ and p does not divide m.

Now assume that $p^f > 2$. By e applications of Lemma 3.2, we can write $s^q - 1 = p^{f+e} n$, where $n \equiv m \not\equiv 0$ mod p. Thus $g_s(q) = (s^q - 1)/(s - 1) = p^e n/m$, and so the integer $g_s(q)/q = n/m$ is not divisible by p, as required. Also, if $p = 2$ in this case, then $f \geq 2$ and so $s \equiv 1$ mod 4.

To complete the proof, we assume that $p^f = 2$ and derive a contradiction. Here we have $s = 1 + 2m$, where m is odd, and since s is odd, we can write $s^2 = 1 + 8j$ for some integer j. Also since $s > 1$, we have $q > 2$ by assumption, and thus $e \geq 2$. Now $s^{q/2} = (s^2)^{q/4}$, and applying Lemma 3.2 a total of $e - 2$ times, starting with s^2 in place of s, we obtain $s^{q/2} = 1 + 2^{(3+(e-2))} n$ for some integer n. Thus $s^{q/2} - 1 = 2^{e+1} n$, and so $g_s(q/2) = (2^{e+1} n)/(2m) = 2^e n/m$. But $2^e n/m$ is an integer and m is odd, so it follows that $g_s(q/2)$ is divisible by $2^e = q$, which is contrary to hypothesis. ▮

Theorem 5.3. *Let $H = KU = KV = UV$, where K is an abelian normal p-subgroup of H, and where U is abelian, V is cyclic, and $V \cap K = 1 = V \cap U$. If $p = 2$, assume in addition that the triple (H, K, Z) is good, where $Z = K \cap U$. Then $U \cong K$.*

Proof. Since $Z \subseteq \mathbf{Z}(H)$, we can work in the group $\overline{H} = H/Z$, and we observe that $\overline{K} \cap \overline{U} = 1$. Also, Dedekind's lemma gives $ZV \cap K = Z(V \cap K) = Z$, and thus $\overline{K} \cap \overline{V} = 1$, and similarly, $\overline{U} \cap \overline{V} = 1$. By Lemma 4.1, it follows that $|\overline{U}| = |\overline{K}| = |\overline{V}| = |V|$, where the last equality holds because $V \cap Z = 1$. Let q be the common order of these subgroups of $\overline{H}$, and observe that q divides $|K|$, so that q is a power of p. We may assume also that $q > 1$, for otherwise $K = Z = U$ and there is nothing further to prove.

Now because $\overline{V} \cong V$ is cyclic, we can apply Lemma 4.2 to deduce that $\overline{U}$ is cyclic, and that if p is odd then $\overline{K}$ is cyclic too. If $p = 2$, then our assumption that (H, K, Z) is good implies that $K/Z = \overline{K}$ is cyclic in that case as well.

The abelian groups K and U intersect in Z, and each of the factor groups K/Z and U/Z is cyclic of order q. To prove that $K \cong U$, it therefore suffices to find an element x that generates K modulo Z, and an element y that generates U modulo Z, such that $x^q = y^q$.

Let v be a generator for the cyclic group V, and write $v = uk$ with $u \in U$ and $k \in K$. Since $k^u \in K$ and K/Z is cyclic of order q, we can write $k^u = k^s z$ for some element $z \in Z$ and some integer s with $1 \leq s < q$. We prove now by induction that $k^{u^r} = k^{s^r} z^{g_s(r)}$ for every positive integer r. First, note that this is true when $r = 1$ because $k^u = k^s z$ and $g_s(1) = 1$. Assume now that $r > 1$ and that $k^{u^{r-1}} = k^{s^{r-1}} z^{g_s(r-1)}$. Then because $z \in K \cap U \subseteq \mathbf{Z}(H)$, we have

$$\begin{aligned} k^{u^r} = (k^{u^{r-1}})^u &= (k^{s^{r-1}} z^{g_s(r-1)})^u \\ &= (k^u)^{s^{r-1}} z^{g_s(r-1)} \\ &= (k^s z)^{s^{r-1}} z^{g_s(r-1)} \\ &= k^{s^r} z^{s^{r-1} + g_s(r-1)} \\ &= k^{s^r} z^{g_s(r)} \,, \end{aligned}$$

as required.

Next, set $h_s(1) = 0$ and write $h_s(r) = g_s(1) + g_s(2) + \cdots + g_s(r-1)$ for $r > 1$. Since $v = uk$, an easy calculation gives

$$v^r = (uk)^r = u^r k k^u k^{u^2} \cdots k^{u^{r-1}} = u^r k^{g_s(r)} z^{h_s(r)}$$

for all $r \geq 1$. Because v generates V (which has order q) and $K \cap V = 1$, we know that $v^r \notin K$ for $0 < r < q$, and hence that $u^r \notin Z$ for integers r in this interval. In other words, u generates U modulo Z. Also we can apply Lemma 4.3 to the group $\overline{H} = H/Z$, to conclude that k generates K modulo Z.

Now take $r = q$ in the previous calculation. Since $v^q = 1$ and $u^q \in Z$, we have $k^{g_s(q)} \in Z$. But K/Z is cyclic of order q and k generates K modulo Z, and therefore q divides $g_s(q)$. Also, since $V \cap U = 1$, we see that $v^r \notin U$ for $0 < r < q$, and thus $k^{g_s(r)} \notin Z$ for integers r in the same range. It follows that q does not divide $g_s(r)$ for $0 < r < q$.

We conclude from Lemma 5.2 that the number $m = g_s(q)/q$ is not divisible by p, and that if $p = 2$ then $s \equiv 1 \bmod 4$. (Note that if $q = 2$, then the assumption $1 \leq s < q$ implies that $s = 1$, and hence Lemma 5.2 does apply.)

We now claim that the quantities $g_s(r)$ are distinct modulo q for $0 < r \leq q$. If $g_s(a) \equiv g_s(b) \bmod q$ with $0 < a < b \leq q$, then q divides $g_s(b) - g_s(a) = s^a + s^{a+1} + \cdots s^{b-1} = s^a g_s(b-a)$, and then since p does not divide s, it follows that q divides $g_s(b-a)$. This is not the case, however, because $b - a < q$. In particular, as $g_s(q) \equiv 0 \bmod q$, we see that the numbers $g_s(1), g_s(2), \ldots, g_s(q-1)$ are congruent mod q to the numbers $1, \ldots, q-1$ in some order, and thus $h_s(q) \equiv q(q-1)/2 \bmod q$. Hence if p is odd, then $h_s(q)$ is a multiple of q, and if $p = 2$ then $2h_s(q)$ is a multiple of q.

Next, since V has order q we have

$$1 = v^q = u^q k^{g_s(q)} z^{h_s(q)} = u^q k^{mq} z^{h_s(q)},$$

where p does not divide m. If p is odd, then $h_s(q) = tq$ for some integer t, so we find

$$(u^{-1})^q = k^{mq} z^{h_s(q)} = (k^m z^t)^q,$$

and since m is coprime to p, this implies that the qth power of a generator u^{-1} of U modulo Z equals the qth power of a generator $k^m z^t$ of K modulo Z. It follows in this case that the abelian groups U and K are isomorphic, as required.

Now suppose $p = 2$, so that by assumption, (H, K, Z) is good. Since $q > 1$, we have $Z < K$, and thus $H' \subseteq \Phi(K_0)$, where K_0/Z is the subgroup of index 2 in the cyclic group K/Z, and hence all commutators in H are squares in K_0. We have $k^u = k^s z$, and so $k^{s-1} z = k^{-1} k^u = [k, u]$, and therefore $k^{s-1} z$ is a square in K_0. Moreover, we know that $s - 1$ is a multiple of 4, and since $k^2 \in K_0$, it follows that k^{s-1} is a square in K_0. We deduce from this that also z is a square in K_0, say $z = y^2$ with $y \in K_0$. Writing $2h_s(q) = tq$ for some integer t, we find

$$(u^{-1})^q = k^{mq} z^{h_s(q)} = k^{mq} y^{2h_s(q)} = (k^m y^t)^q\,,$$

and since m is coprime to 2, again this means that appropriate generators of U and K modulo Z have equal qth powers. The proof is now complete. ∎

If we drop the assumption that $V \cap K = 1 = V \cap U$ in Theorem 5.3, we can no longer conclude that $K \cong U$. We do have the following, however.

Corollary 5.4. *Let $H = UV = UK = VK$, where K is an abelian normal p-subgroup of H, and where U is abelian and V is cyclic. Write $R = K \cap U$ and $S = K \cap V$ and assume that (H, K, R) is good if $p = 2$. Then K/S is isomorphic to a subgroup of U, and K/R is isomorphic to a subgroup of V.*

Proof. We first show that K/S is isomorphic to a subgroup of U. Since $S = K \cap V \subseteq \mathbf{Z}(H)$, we have $S \triangleleft H$, and so we can work in $\overline{H} = H/S$, which clearly satisfies the hypotheses with respect to $\overline{U}$, $\overline{V}$ and $\overline{K}$. (Note that since U is abelian, every subgroup of $\overline{U}$ is isomorphic to a subgroup of U.) It follows that for this part of the proof, we can assume that $S = 1$, and hence need only show that K is isomorphic to a subgroup of U.

Now let $D = U \cap V \subseteq \mathbf{Z}(H)$, and redefine $\overline{H} = H/D$. Then $\overline{H}$ satisfies the hypotheses, and we note that $\overline{K} \cong K$ since $D \cap K \subseteq S = 1$. Also $D = SD = (K \cap V)D = KD \cap V$ by Dedekind's lemma, and so $\overline{K} \cap \overline{V} = 1$. Again using the fact that subgroups of homomorphic images of U are isomorphic to subgroups of U, we can replace H by $\overline{H}$, and this puts us into the situation of Theorem 5.3. Thus $K \cong U$, and the first part of the proof is complete.

We now return to the original situation, and show that K/R is isomorphic to a subgroup of V. Observe that $U/R \cong H/K \cong V/S$ is cyclic. Reasoning as in the first part of the proof, we can pass from H to H/R, and therefore we can assume that $R = 1$ and that U is cyclic. We can now interchange the roles of U and V, and deduce from the first part of the proof that K is isomorphic to a subgroup of V, as required. ▌

We are now ready to prove Theorems A and B of the introduction, which we combine as follows.

Theorem 5.5. *Let $G = AB$ be finite, where A is abelian and B is cyclic. If K is any abelian normal subgroup of G with the property that the Sylow 2-subgroup of K is contained in G', then $K/(K \cap A)$ is isomorphic to a subgroup of B, and $K/(K \cap B)$ is isomorphic to a subgroup of A.*

Proof. Let p be a prime divisor of $|K|$ and let P be the Sylow p-subgroup of K. It suffices to show for each choice of p that $P/(P \cap A)$ is isomorphic to a subgroup of B and that $P/(P \cap B)$ is isomorphic to a subgroup of A. We can assume, therefore, that K is a p-group. If $p = 2$, then by hypothesis, $K \subseteq S$, where S is the Sylow 2-subgroup of the abelian group G'. But $K/(K \cap A)$ and $K/(K \cap B)$ are isomorphic to subgroups of $S/(S \cap A)$ and $S/(S \cap B)$ respectively, and so it is no loss to assume that $K = S$ in this case. Finally, let H, U and V be as in the standard notation and observe that $K \cap A = K \cap U$ and $K \cap B = K \cap V$.

If p is odd, then the existence of the desired isomorphisms is immediate from Corollary 5.4. We can assume, therefore, that $p = 2$ and that K is a Sylow 2-subgroup of G'. Next, we let M be the Hall 2-complement of G' and we argue that it suffices to consider $\overline{G} = G/M$ in place of G. It is clear that $\overline{G}$ satisfies the hypotheses, and also since

$K \cap M = 1$, we see that the map $x \mapsto \overline{x}$ from K to $\overline{K}$ is an isomorphism. The pre-image in K of $\overline{K} \cap \overline{A}$ is $K \cap AM$, which equals $K \cap A$ since every normal 2-subgroup of AM is contained in A. Thus $K/(K \cap A) \cong \overline{K}/(\overline{K} \cap \overline{A})$, and a similar isomorphism holds with B in place of A. We observe also that $\overline{K} = \overline{G'} = (\overline{G})'$. It follows from all of this that we can replace G by $\overline{G}$, as claimed, and thus we can assume that $K = G'$ is a 2-group.

By Theorem 3.5, the triple (H, K, R) is good, where $R = K \cap A$ and H is as in the standard notation. The required result now follows by Corollary 5.4. ▌

6. Ranks and Theorem E

In this section we prove a strong form of Theorem E. We begin with the following.

Lemma 6.1. *Let G be a p-group such that $G = KA = KB$, where K is an elementary abelian normal subgroup of order p^t, and $A \cap B = 1$. Then the exponent of each of A and B is less than p^2t.*

Proof. By symmetry, it suffices to prove the result for A. Let $C = \mathbf{C}_G(K)$, and write $R = C \cap A$ and $S = C \cap B$. Now R is the kernel of the action of A on K by conjugation, and thus A/R can be isomorphically embedded in $GL(t, p)$. As is well known, each p-element of this general linear group is conjugate to $I + U$, where I is the $t \times t$ identity matrix and U is some strictly upper triangular matrix. If $I + U$ has order p^{e+1}, then we see that $U^{p^e} \neq 0$, and thus $t > p^e$. It follows that each element of A/R has order less than pt, and so to prove that the exponent of A is less than p^2t, it suffices to show that R has exponent at most p.

Observe that $K \subseteq C \subseteq G = KB$, and so $C = K(C \cap B) = KS$ by Dedekind's lemma. Also $R \cap S \subseteq A \cap B = 1$, and $S \triangleleft C$ since $K \subseteq \mathbf{Z}(C)$. It follows that $R \cong RS/S \subseteq C/S = KS/S \cong K/(K \cap S)$. But K has exponent p, and so R also has exponent p, and the proof is complete. ▌

Recall that the rank of an abelian group is the minimum number of elements needed to generate it, and that we are writing $r(X)$ to denote the rank of X.

Lemma 6.2. *Let $H = KU = KV = UV$, where K is an elementary abelian normal subgroup of order p^t, V is abelian, and $U \cap K = 1 = U \cap V$. Then $r(V) > t/(2 + \log_p(t))$.*

Proof. We have $|H : K| = |U| = |H : V|$ since $UK = H = UV$ and $U \cap K = 1 = U \cap V$. Thus $|V| = |K|$, and in particular, V is a p-group, and hence also $H = KV$ is a p-group. By Lemma 6.1, the elements of V all have order less than p^2t, and thus $|V| < (p^2t)^r$, where $r = r(V)$. But $|V| = |K| = p^t$, and this yields $p^t < (p^2t)^r$. The result now follows by taking logarithms with base p. ▌

The following establishes Theorem E, and indeed shows that the bound in that theorem can be taken to be very nearly linear.

Theorem 6.3. *Given $\epsilon > 0$, there exists a positive real number N (depending on ϵ) such that whenever K is a normal abelian subgroup of the finite group $G = AB$, where A and B are abelian and $r(B) = r$, then $r(K/(K \cap A)) \leq Nr^{1+\epsilon}$.*

Proof. Write $1/(1+\epsilon) = 1 - \delta$. Since $\delta > 0$, we see the function $(2 + \log_2(x))/x^\delta$ has the limit 0 as $x \to \infty$, and so this function attains some maximum value M for $x \geq 1$. It follows that $2 + \log_p(x) \leq 2 + \log_2(x) \leq Mx^\delta$ for every prime p, and this yields $Mx/(2 + \log_p(x)) \geq x^{1-\delta}$. Therefore

$$x \leq M^{1+\epsilon} \left(\frac{x}{2 + \log_p(x)} \right)^{1+\epsilon}$$

for all $x \geq 1$ and for every prime p. Now let $N = M^{1+\epsilon}$, and suppose that G is a minimal counterexample to the assertion that $r(K/(K \cap A)) \leq Nr^{1+\epsilon}$.

Since $K/(K \cap A)$ is abelian and has "large" rank, it follows that a Sylow p-subgroup of this group has equally large rank for some prime p. Now if P is the Sylow p-subgroup of K, then $P/(P \cap A)$ is isomorphic to the Sylow p-subgroup of $K/(K \cap A)$, and so we can replace K by P, and assume that K is a p-group.

By reasoning that we have used previously, we see that $K \cap A\Phi(K) = \Phi(K)(K \cap A)$, and hence if we write $\overline{G} = G/\Phi(K)$, we see that $\overline{K}/(\overline{K} \cap \overline{A})$ is isomorphic to the Frattini factor group of $K/(K \cap A)$. Moreover, as $r(\overline{K}/(\overline{K} \cap \overline{A})) = r(K/(K \cap A))$ and $r(\overline{B}) \leq r(B)$, we see that $\overline{G}$ is also a counterexample. By the minimality of G, it follows that $\Phi(K) = 1$, and so K is elementary abelian. Next, we may redefine $\overline{G} = G/\mathrm{core}_G(A)$ and observe that $K/(K \cap A) \cong \overline{K}/(\overline{K} \cap \overline{A})$. Again $r(\overline{B}) \leq r(B)$ and $\overline{G}$ is a counterexample, and this time we conclude that $\mathrm{core}_G(A) = 1$, and in particular, $A \cap B = 1$ since $A \cap B \subseteq \mathbf{Z}(AB) = \mathbf{Z}(G)$.

Now assume the standard notation. We have $H = UK = VK = UV$, where $U \subseteq A$ and $V \subseteq B$, and we see that $K \cap U = K \cap A$ and that $r(V) \leq r(B)$. Thus H is a counterexample, and hence we have $H = G$. But this implies $U \cap K \subseteq \mathbf{Z}(G)$, and thus $U \cap K \subseteq \mathrm{core}_G(A) = 1$. We are now in the situation of Lemma 6.2, and if we write $|K| = p^t$, then we have $t = r(K) > Nr^{1+\epsilon}$, and in particular, $t \geq 1$.

By Lemma 6.2 we have $r \geq r(V) > t/(2 + \log_p(t))$, and thus

$$Nr^{1+\epsilon} > M^{1+\epsilon} \left(\frac{t}{2 + \log_p(t)} \right)^{1+\epsilon} \geq t = r(K)\,.$$

This is a contradiction, and the proof is complete. ▮

7. A family of examples

In this section, we prove Theorem F. Given an arbitrary prime p, we construct examples of finite p-groups $G = AB$, where A and B are abelian, and where $r(G'/(G' \cap A))$

exceeds $r(B)$ by an arbitrarily large amount. Each such example G has an elementary abelian normal subgroup K and a triple factorization $G = KA = KB = AB$, with $K \cap A = K \cap B = A \cap B = 1$, and its derived subgroup G' has index p in K.

Proof of Theorem F. Let F be the field of order p and fix an integer $n > 0$. We construct a "truncated polynomial algebra" in the indeterminate X by setting $R = F[X]/(X^n)$. If we write x for the image of X in R, then R can be viewed as the set of polynomials in x of degree less than n, and we see that $|R| = p^n$. Now let A be the set of polynomials in R with constant term 1. Then $A = 1 + xR$ is closed under multiplication, and we see that $|A| = p^{n-1}$. Each member of xR is nilpotent since $x^n = 0$, and thus the elements of A are invertible in R. The inverses of these elements all lie in A, and hence A is a subgroup of the unit group of R. Also, A is abelian since R is a commutative ring.

Next, we consider the additive group of the ring R, which of course is elementary abelian of order p^n. We intend to write this group multiplicatively, and so to avoid confusion, we rename it and call it V. Since multiplication in R defines an action of A on V via automorphisms, we can construct the semidirect product $P = VA$, of order $|P| = p^{2n-1}$.

Now fix the element $a = 1+x \in A$. If we take n large enough, then the order of a can be made arbitrarily large. Specifically, if $n > p^e$ then $x^{p^e} \neq 0$ and $a^{p^e} = (1+x)^{p^e} = 1+x^{p^e} \neq 1$, and so the order of a exceeds p^e. Since $|A| = p^{n-1}$, we have $|A/\langle a\rangle| < p^{n-1-e}$, and thus $r(A/\langle a\rangle) < n-1-e$. It follows that $r(A) < n-e$, where e is unbounded.

Because $P/V \cong A$ is abelian, we see that $P' \subseteq V$, and so P' is elementary abelian. We now argue that $|P'| = p^{n-1}$. In fact, we claim that P' is exactly the subgroup W of V corresponding to the ideal xR of R. Since $(xR)(1+xR) \subseteq xR$, we see that W is A-invariant, and hence A centralizes the factor group V/W of order p. Thus $P/W = (V/W)(AW/W)$ is abelian, and so $P' \subseteq W$. On the other hand, if $v \in V$ corresponds to a polynomial $f \in R$, then $[v,a] = v^{-1}v^a$ corresponds to $-f + (1+x)f = xf$. But multiplication by x maps R onto xR, and thus $W = [V,a] \subseteq P'$. It follows that $W = P'$, as claimed.

Let $u \in V$ be the element corresponding to $1 \in R$, and write $C = \mathbf{C}_P(ua)$. Then $|P:C|$ is the size of the conjugacy class of ua in P, and thus $|P:C| \le |P'| = p^{n-1}$. On the other hand, $C \cap A = \mathbf{C}_A(u)$ is trivial (because u corresponds to $1 \in R$ and the action of A is by multiplication in R). Hence $|P:C| \ge |A| = p^{n-1}$, and therefore $|P:C| = p^{n-1}$ and $|C| = p^n$. Also $|P:C| = |A|$, and since $A \cap C = 1$, it follows that $AC = P$.

Next, write $Z = C \cap V = \mathbf{C}_V(ua)$. Since $u \in V$, we find $Z = \mathbf{C}_V(a)$, and this corresponds to the annihilator in R of x. This annihilator is the 1-dimensional subspace Fx^{n-1}, and hence $|Z| = p$, and we note that $Z \subseteq W = P'$. Since $|C| = p^n = |V|$, it follows that $|CV| = |C||V|/|Z| = p^{2n-1} = |P|$, and thus $CV = P$. Also, $Z \lhd C$ and V is abelian, and thus $Z \lhd P$.

We can now define $G = \overline{P} = P/Z$, so that $|G| = p^{2n-2}$. Since $Z \subseteq V$, we see that $Z \cap A = 1$, and so $\overline{A} \cong A$ and we may identify A with $\overline{A}$, and view A as a subgroup of G.

Writing $B = \overline{C}$ and $K = \overline{V}$, we observe that each of A, B and K has order p^{n-1}. Also $G = KA = KB = AB$, and the pairwise intersections of these three subgroups are trivial. We see that K is elementary abelian, G' has index p in K, and $B \cong G/K \cong A$, so that B is abelian and the rank of B falls short of n by an arbitrarily large amount.

Finally, note that $G' \cap A = 1$ and $r(G') = n-2$. Thus $r(G'/(G' \cap A)) = n-2$, and so if we take n to be large enough, this will exceed $r(B)$ by an arbitrarily large amount. In particular, if n is sufficiently large, then $G'/(G' \cap A)$ cannot be isomorphic to any subgroup of B. This completes the proof. ▮

REFERENCES

1. W. Bosma, J. Cannon and C. Playoust, The Magma Algebra System I: The User Language. *J. Symbolic Comput.* **24** (1997), 235–265.

2. P. M. Cohn, A remark on the general product of two infinite cyclic groups. *Arch. Math.* **7** (1956), 94–99.

3. M. D. E. Conder, R. Jajcay and T.W. Tucker, Regular Cayley maps for finite abelian groups, preprint.

4. J. Douglas, On finite groups with two independent generators, I. *Proc. Nat. Acad. Sci. U.S.A.* **37** (1951), 604–610.

5. J. Douglas, On finite groups with two independent generators, II. *Proc. Nat. Acad. Sci. U.S.A.* **37** (1951), 677–691.

6. J. Douglas, On finite groups with two independent generators, III: Exponential substitutions. *Proc. Nat. Acad. Sci. U.S.A.* **37** (1951), 749–760.

7. J. Douglas, On finite groups with two independent generators, IV: Conjugate substitutions. *Proc. Nat. Acad. Sci. U.S.A.* **37** (1951), 808–813.

8. B. Huppert, Über das Produkt von paarweise vertauschbarren zyklischen Gruppen. *Math. Zeit.* **58** (1953), 243–264.

9. B. Huppert, *Endliche Gruppen, I.* Springer-Verlag (Berlin-New York), 1967.

10. N. Ito, Über das Produkt von zwei abelschen Gruppen. *Math. Z.* **62** (1955), 400–401.

11. L. Rédei, Zur Theorie der faktorisierbaren Gruppen, I. *Acta Math. Acad. Sci. Hungar.* **1** (1950). 74–98.