Centre-by-metabelian Group Algebras

Dissertation

**zur Erlangung des akademischen Grades
doctor rerum naturalium (Dr. rer. nat.)**

vorgelegt dem Rat der Fakultät für Mathematik und Informatik der
Friedrich-Schiller-Universität Jena

von Richard Rossmanith,
geboren am 5. Dezember 1969 in Marktoberdorf

Gutachter:

1. Prof. Dr. Burkhard Külshammer, Jena
2. Prof. Dr. Robert Sandling, Manchester
3. Prof. Dr. Sudarshan Sehgal, Edmonton

Tag des Rigorosums: 21. November 1997

Tag der öffentlichen Verteidigung: 1. Dezember 1997

Contents

Introduction

In nonabelian groups, as well as in noncommutative associative algebras, one may measure the degree of noncommutativity with the help of *commutators.* Based on these, one defines in "both worlds" (the category of groups, and the category of associative algebras) analogous concepts, such as (Lie) solvability, (Lie) nilpotence, ... — here the question arises whether one also obtains parallel properties in both categories. In this context we take as the object of study the group algebra of a (finite or infinite) group over some field. A "parallel property" would then be e.g. commutativity: A group is abelian, if and only if the associated group algebra is commutative. For other, more complex concepts such as the ones mentioned above, such a total correlation cannot be expected, although it should be clear that the commutator properties of the group algebra are derived from the commutator properties of the group we started with.

A complete qualitative description of this correlation has been given by I.B.S. Passi, D.S. Passman, and S.K. Sehgal in [**15**, 1973], where they classify the Lie solvable and the Lie nilpotent group algebras (theorem 1 below). Loosely speaking, they answer the question posed above with "close to –but not quite– parallel". (For an extensive treatment of Lie solvability, Lie nilpotence, as well as further Lie properties of group algebras, see also [**19**, chapter V].)

Based on this result, there have been quantitative examinations, such as towards the determination of the Lie nilpotence class [**1, 4, 10, 20**], or the Lie derived length [**9, 21, 22**] of Lie nilpotent, respectively Lie solvable, group algebras.

Another property of group algebras has also been studied, namely *centre-by-metabelianity*, which is somewhat atypical in this context in that it is located somewhere between Lie solvability of index 2 and 3, but also has a touch of Lie nilpotence (although it does not imply the latter; see the definitions and the theorems 2–4 below).

We want to classify the centre-by-metabelian group algebras: If the underlying field has characteristic 0, the centre-by-metabelian group algebras are known to be abelian; this is easily derived from the Passi-Passman-Sehgal theorem. The case of characteristic greater than 3 has been studied by R.K. Sharma and J.B. Srivastava in [**23**, 1992]. Their result is that here there also are no centre-by-metabelian group algebras except the abelian ones. In characteristic 3, the situation is more interesting since here there are centre-by-metabelian group algebras which are neither metabelian nor Lie nilpotent. Their classification actually was published twice in the Journal of Algebra, namely by B. Külshammer and R.K. Sharma in [**7**, 1996], and by M. Sahai and J.B. Srivastava in [**17**, 1997]; both parties were working independently, using different methods.

As very often in group or ring theory, the problem for the characteristic 2 case is the least handy one. Its solution is the main result of the present thesis (cf. theorem 4).

A converse concept (more exactly: a right adjoined functor) to the construction of the group algebra from a group is given by the determination of the unit group of an algebra. We exploit our classification theorem to study the unit groups of centre-by-metabelian group algebras. In particular, we examine whether the unit group is centre-by-metabelian. This is a natural question since this is true in odd characteristic, as is shown in [**7**]; the question was first raised in [**23**]. Our result is that in characteristic 2, this is not necessarily so, spotlighting once more the capriciousness of this characteristic.

Acknowledgments

Most notably I wish to express my gratitude towards my teacher and advisor Burkhard Külshammer for his guidance and support during my time as a student of mathematics in Augsburg, and throughout the work on my thesis in Jena. Furthermore, I am indebted to R.K. Sharma for introducing me to the questions discussed here, and for acquainting me with his cunning ways of handling (notably very long) commutator computations. Particular thanks goes to my Jena colleagues Markus Deiml, Hubert Fottner, and Thomas Keller for innumerable fruitful discussions. Moreover, I owe Bettina Eick for her concise information on how to simplify the handling of automorphisms in GAP. Last but not least, my wife Julie deserves a big hug for her encouragement and support and for reading through the text and improving my English.

Language

Let $\mathbb{F}$ be a field of characteristic $p \geq 0$, and let L be a Lie algebra over $\mathbb{F}$. Recall that an *ideal* of L is an $\mathbb{F}$-linear subspace $U \subseteq L$ such that $[x, y] \in U$ for all $x \in L$, $y \in U$.

For subsets X, Y of L, we denote by $[X, Y]$ the $\mathbb{F}$-span of all elements $[x, y]$ with $x \in X$, $y \in Y$. If X, Y are ideals of L, then so is $[X, Y]$ by the Jacobi identity.

One has the following descending chains of ideals: The *lower central series* of L, inductively defined by $\gamma_1(L) := L$, $\gamma_{i+1}(L) := [L, \gamma_i(L)]$ for $i = 1, 2, \ldots$; and the *derived series* of L, inductively defined by $\delta^0(L) := L$, $\delta^i(L) := [\delta^{i-1}(L), \delta^{i-1}(L)]$ for $i = 1, 2, \ldots$. We say that L is *nilpotent of class* c, if $\gamma_{n+1}(L) = 0$ for some $n \in \mathbb{N}$, and c is the minimum over all such n; and we call L *solvable of derived length* d, if $\delta^m(L) = 0$ for some $m \in \mathbb{N}$, and d is the minimum over all such m. We use the common abbreviation L' for $\delta^1(L) = [L, L] = \gamma_2(L)$, and L'' for $\delta^2(L)$. Then L is called *abelian (metabelian)*, if $L' = 0$ (resp. $L'' = 0$).

The *centre* $\mathcal{Z}(L) := \{z \in L : [x, z] = 0 \text{ for all } x \in L\}$ of L clearly is an ideal as well. If its factor Lie algebra $L/\mathcal{Z}(L)$ is metabelian, we say that L is ***centre-by-metabelian***. An equivalent description is to say that $L'' \subseteq \mathcal{Z}(L)$. Another equivalent condition is that $[a, [b, c], [d, e]] = 0$ for all $a, b, c, d, e \in L$; note that we use *right normed triple commutators*, defined via $[a, b, c] := [a, [b, c]]$ for $a, b, c \in L$. Obviously, centre-by-metabelian Lie algebras are solvable of derived length at most 3.

Let A be an associative, unitary $\mathbb{F}$-algebra. For subsets X, Y of A, denote by XY the $\mathbb{F}$-span of all elements xy with $x \in X$, $y \in Y$, and by $\mathbb{F}[X]$ or just $\mathbb{F}X$ the $\mathbb{F}$-linear subspace of A spanned by X.

As usual, the *associated Lie algebra* $\mathcal{L}(A)$ of A is defined to be the underlying vector space of A together with the commutator bracket $[.,.]$ defined via $[x, y] := xy - yx$ for all $x, y \in A$. We call A *Lie solvable*, if $\mathcal{L}(A)$ is solvable; the attributes *Lie nilpotent, Lie* *metabelian,* and *Lie centre-by-metabelian* are defined accordingly.* An ideal of $\mathcal{L}(A)$ is called a *Lie ideal* of A.

Since there is no danger of confusion, we simply call A *metabelian* (resp. *centre-by-metabelian*), if it is Lie metabelian (resp. Lie centre-by-metabelian), and we write A', A'', $\delta^n(A)$, $\gamma_n(A)$ instead of $\mathcal{L}(A)'$, $\mathcal{L}(A)''$, $\delta^n(\mathcal{L}A)$, $\gamma_n(\mathcal{L}A)$, respectively.

Let G be a group. We use the "left versions" of *conjugation* and of the *commutators* in G, i.e. for $a, b \in G$, we define ${}^{a}b := aba^{-1}$, and $(a,b) := ab(ba)^{-1} = aba^{-1}b^{-1} = {}^{a}bb^{-1}$. Much as above, we define the *right normed triple commutator* of $a, b, c \in G$ by $(a,b,c) := (a,(b,c))$.

For subsets X, Y of G we set $XY = \{xy\colon\ x \in X, y \in Y\}$ and $(X,Y) := \langle (x,y)\colon\ x \in X, y \in Y\rangle$. The *centralizer* of X in Y is $\mathcal{C}_Y(X) := \{y \in Y\colon\ (x,y) = 1 \text{ for all } x \in X\}$.

In accordance with [**5**], we extend these definitions to the case where a group A acts on G, i.e. where we have a group homomorphism φ from A to the automorphism group $\mathrm{Aut}(G)$ of G. We set ${}^{a}g := (\varphi(a))\,(g)$, and $(a,g) := {}^{a}gg^{-1} \in G$ for $a \in A$, $g \in G$. For subsets $B \subseteq A$, $H \subseteq G$, we then define (B,H), $\mathcal{C}_H(B) \subseteq G$, $\mathcal{C}_B(H) \subseteq A$ in the obvious way.

Frequently, A will act on G by element inversion, i.e. we will have the situation that $|A : \mathcal{C}_A(G)| = 2$ with ${}^{a}g = g^{-1}$ for all $g \in G$, $a \in A \smallsetminus \mathcal{C}_A(G)$. For convenience, we will say that A acts *dihedrally* on G in this case. Note that this implies that G is abelian.

The *lower central series*, $G = \gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq \gamma_3(G) \trianglerighteq \ldots$, and the *derived series*, $G = \delta^0(G) \trianglerighteq G' = \delta^1(G) \trianglerighteq G'' = \delta^2(G) \trianglerighteq \ldots$, of G are defined much as their Lie-theoretic analogues, as well as the notion of *nilpotence* and *solvability* of G. We say that G is *metabelian*, if $G'' = 1$, and we say that G is *centre-by-metabelian*, if $G/\mathcal{Z}(G)$ is metabelian, or equivalently, if $(G, G'') = 1$.

All further notation is standard; check appendix A for details.

Results

As already mentioned, we are interested in the correlation between the commutator properties of the group G on the one hand, and the associated Lie algebra of the group algebra $\mathbb{F}G$ on the other hand. Let us start by quoting some important previously known results.

In 1973, I.B.S. Passi, D.S. Passman, and S.K. Sehgal obtained the following classification of the Lie solvable and the Lie nilpotent group algebras:

1. Theorem ([15]): *Let G be a group, and let $\mathbb{F}$ be a field of characteristic $p \geq 0$.*

(i) If $p = 0$, then $\mathbb{F}G$ is Lie nilpotent or Lie solvable if and only if G is abelian.
(ii) If $p > 0$, then $\mathbb{F}G$ is Lie nilpotent if and only if G' is a finite p-group and G is nilpotent.
(iii) If $p > 2$, then $\mathbb{F}G$ is Lie solvable if and only if G' is a finite p-group.
(iv) If $p = 2$, then $\mathbb{F}G$ is Lie solvable if and only if G contains a subgroup A of index at most 2 such that A' is a finite 2-group.

*in [**7, 17, 23**], the term *Lie centrally metabelian* is preferred over Lie centre-by-metabelian.

F. Levin and G. Rosenberger then focused on the Lie solvable group algebras of derived length at most 2 in positive[†] characteristic:

2. Theorem ([9, 1985]): *Let G be a group, and let $\mathbb{F}$ be a field of characteristic $p > 0$. Then $\mathbb{F}G$ is metabelian if and only if it is Lie nilpotent of class at most 3, and this is the case if and only if one of the following holds:*

(i) $p > 3$ and G is abelian.
(ii) $p = 3$ and G' is central of order dividing 3.
(iii) $p = 2$ and G' is central and elementary abelian of order dividing 4.

The classification of the centre-by-metabelian group algebras in positive[†] odd characteristic, published by R.K. Sharma and J.B. Srivastava [**23**, 1992], B. Külshammer and R.K. Sharma [**7**, 1996], M. Sahai and J.B. Srivastava [**17**, 1997], is given as:

3. Theorem: *Let G be a group, and let $\mathbb{F}$ be a field of characteristic $p > 2$. Then $\mathbb{F}G$ is centre-by-metabelian if and only if one of the following holds:*

(i) $p > 3$ and G is abelian [**23**].
(ii) $p = 3$ and the order of G' divides 3 [**7, 17**].

The paper on hand now closes the gap for even characteristic:

4. Theorem (main result): *Let G be a group, and let $\mathbb{F}$ be a field of characteristic 2. Then $\mathbb{F}G$ is centre-by-metabelian if and only if one of the following conditions is satisfied:*

(i) The order of G' divides 4.
(ii) G' is central and elementary abelian of order 8.
(iii) G acts dihedrally on $G' \cong Z_2 \times Z_4$, and $\mathcal{C}_G(G')' \subseteq \Phi(G')$.
(iv) G contains an abelian subgroup of index 2.

The structure of the proof is as follows: After obtaining some basic formulas in section 1, we show the "if"-direction in section 2, which is comparatively easy. To attack the "only if"-direction, we have to study closely the action of G on G' (by conjugation). The trivial action is handled in section 3. For non-trivial actions, we first concentrate on the case where G' is elementary abelian, which then may be interpreted as a vector space over $\mathbb{F}_2$. Thus we obtain a linear representation of G, which we will examine in section 4. Some properties of the elementary abelian case carry over to the situation where G' is not elementary abelian; see section 5. Under the assumption that $|G'| \in \{8, 16\}$, we construct an algorithm that drastically reduces the number of actions we have to consider; this algorithm may then be run through a computer. (The reader can find the commented listing of a collection of routines designed for this job using the computer algebra system *GAP – Groups, Algorithms, and Programming* [**18**], called `actions.g`, in appendix C.) The "survivors" of this algorithm then have to be looked at more closely in sections 6 and 7. Finally, the cases where $|G'| \notin \{8, 16\}$ are taken care of in section 8 by an inductive argument.

[†] Obviously, theorem 1 (i) includes the classification of both the metabelian and the centre-by-metabelian group algebras in characteristic 0.

The last section then discusses commutator properties of the group of units $\mathcal{U}(A)$ of an (associative) algebra A (notably we will discuss group algebras). A previously known result by N. Gupta and F. Levin [**4**, 1983] is that Lie nilpotence of A implies nilpotence of $\mathcal{U}(A)$. In the case that A is a group algebra in characteristic $p \neq 2$, a similar statement holds for solvability [**19**, V.6.18]. For arbitrary A again, if A is metabelian, then also $\mathcal{U}(A)$ is metabelian, as has been shown by R.K. Sharma and J.B. Srivastava in [**23**]. There they also have raised the question whether $\mathcal{U}(A)$ is necessarily centre-by-metabelian, if A is centre-by-metabelian. According to theorem 3 (i), this is clearly the case if A is a group algebra of characteristic not dividing 6. B. Külshammer and R.K. Sharma show in [**7**], that the same is true if A is a group algebra of characteristic 3. However, V. Tasić presents in [**24**, 1992] a centre-by-metabelian $\mathbb{F}_2$-algebra A such that $\mathcal{U}(A)$ is not centre-by-metabelian (his example is a factor algebra of a power series algebra). The answer to what happens if A is a *group* algebra over a field of characteristic 2 is a second result of this thesis:

5. Theorem (supplementary result): *We adopt the notation of theorem 4.*

If either (i) or (ii) is satisfied, then $\mathcal{U}(\mathbb{F}G)$ *is centre-by-metabelian.*

If (iii) is satisfied, then $\mathcal{U}(\mathbb{F}G)$ *is solvable of derived length at most* 3, *but not necessarily centre-by-metabelian.*

There are groups G *that satisfy (iv) such that* $\mathcal{U}(\mathbb{F}G)$ *is not solvable.*

For the actual examples and a slightly more detailed formulation, see section 9.

* * *

Before one continues reading, I would like to draw attention to a second, more extensive and polished extension package for GAP called *LAG – Lie Algebras of Group Algebras*, that emerged so to speak as a byproduct of my involvement with this classification problem. While it is not directly used in any proof, it was very helpful for the examination of a large number of examples during an initial "experimental stage" of my work (apart from "handmade" examples, the 2-groups library of M.F. Newman and E.A. O´Brien [**11, 12, 13**] that is included into GAP was an indispensable tool here). In general, LAG allows its user to deal with group algebras in the same simple manner as one is used to with groups in GAP (for the protocol of an example GAP session with LAG, see appendix B). It complements P. Osterlunds extension package `grupring.g` [**14**] nicely, since both packages use similar data structures but have a virtually disjoint functional scope. For the future, it would be desirable to have a combined package — unless the new GAP version 4, which will hopefully soon be available, makes this demand obsolete.

Both of my GAP files, i.e. LAG and the previously mentioned `actions.g`, as well as the full text of this dissertation, are available in the WWW under

`http://www.mathematik.uni-jena.de/algebra/skripten/`

Have fun.

1. Preliminaries

General premise: Let $\mathbb{F}$ be a field of characteristic 2 throughout this and all following sections, until otherwise mentioned.

Let G be a group, and $a, b, c \in G$. The most basic formulas for group commutators are somewhat similar to bilinearity:

$$\begin{aligned} (a, bc) &= (a, b)\, {}^{b}(a, c), \\ (ab, c) &= {}^{a}(b, c)(a, c), \\ {}^{a}(b, c) &= ({}^{a}b, {}^{a}c). \end{aligned} \tag{1.1}$$

This may easily be checked by direct expansion, as well as the *Witt identity* [**5**, Satz III.1.4]:

$$ {}^{b}(a, b^{-1}, c)\, {}^{c}(b, c^{-1}, a)\, {}^{a}(c, a^{-1}, b) = 1. \tag{1.2}$$

Now let $a \in G$, $b, c \in \mathcal{C}_G(G')$. The Witt identity then implies that $(a, b, c) = 1$. It follows that

$$\mathcal{C}_G(G')' \subseteq G' \cap \mathcal{Z}(G). \tag{1.3}$$

For subgroups $H, K < G$ it is easy to verify that [**5**, Hilfssatz III.1.6]

$$(H, K) \trianglelefteq \langle H, K \rangle\,. \tag{1.4}$$

If the group A acts on G, then, for all $a \in A$,

$$(a, G) = (\langle a \rangle\,, G) \tag{1.5}$$

is an $\langle a \rangle$-invariant normal subgroup of G, since by 1.1, we have $(a^2, g) = {}^{a}(a, g)(a, g) = (a, {}^{a}g)(a, g) \in (a, G)$, and $(a^{-1}, g) = {}^{a^{-1}}(a, g)^{-1}(a^{-1}a, g) = (a, {}^{a^{-1}}g)^{-1} \in (a, G)$ for all $g \in G$; the rest follows by induction.

Suppose that N is a subgroup of finite index in G that contains G'. Then $N \trianglelefteq G$, and G/N is abelian. We write $G/N = \langle a_1 N, \ldots, a_n N \rangle$ with elements $a_1, \ldots, a_n \in G$. We claim that then

$$G' = \langle (a_i, a_j) \colon\, 1 \le i < j \le n \rangle\; (a_1, N) \ldots (a_n, N)\, N'. \tag{1.6}$$

One inclusion is trivial. To see the other one, consider first the case $n = 1$ with $a := a_1$. For all $g, h \in G$, there are $x, y \in N$ and $i, j \in \mathbb{Z}$ such that $g = a^i x$, $h = a^j y$. By 1.1, $(g, h) = (a^i x, a^j y) = {}^{a^i}(x, a^j) \cdot {}^{a^{i+j}}(x, y) \cdot (a^i, a^j) \cdot {}^{a^j}(a^i, y) \in {}^{a^i}(a, N) \cdot {}^{a^{i+j}}N' \cdot {}^{a^j}(a, N) = (a, N)N'$. (Note that N' is normal in G, since it is a characteristic subgroup of N.)

Assume now that $n > 1$. Observe that for all subgroups U, V of G', we have $(U, V) \subseteq G'' \subseteq N'$, thus $UVN' = VUN'$ also is a subgroup of G'. Set $a := a_1$, $H := \langle a_2, \ldots, a_n, N \rangle$. By the case $n = 1$, we have $G' = (a, H)H'$. By induction, H' is contained in the right hand side of 1.6. Furthermore, for $x \in N$ we have $(a, a_2 x) = (a, a_2)\, {}^{a_2}(a, x) = (a, a_2)(a_2, a, x)(a, x)$, which clearly is contained in the right hand side of 1.6, since $(a_2, a, x) \in (a_2, N)$. Arguing again by induction, we find that all of (a, H) is contained in the right hand side of 1.6, hence G' is also.

Our next claim:

(1.7) If G has an abelian subgroup A of index 2, then G acts dihedrally on G'.

First note that $g^2 \in A$, hence $1 = (g^2, a) = {}^g(g,a)(g,a)$, i.e. ${}^g(g,a) = (g,a)^{-1}$ for all $a \in A$. But $G' = (g,A)A' = (g,A)$ by 1.6, and thus ${}^gh = h^{-1}$ for all $h \in G'$.

A formula connecting the commutator of two elements $a, b \in G$ with their Lie commutator in $\mathbb{F}G$ is given by

$$[a,b] = ab + ba = (a,b)ba + ba = (1 + (a,b))ba. \tag{1.8}$$

(Recall that $\mathbb{F}$ has characteristic 2.) Moreover,

$$[a, ba^{-1}] = aba^{-1} + b = b + {}^ab, \tag{1.9}$$

which easily implies that

$$(\mathbb{F}G)' = \mathbb{F}\{[a,b]\colon\ a,b \in G\} = \mathbb{F}\{x + y\colon\ x,y \text{ are conjugate elements of } G\}. \tag{1.10}$$

For any subset X of G, we denote by $X^+ \in \mathbb{F}G$ the sum over all elements of X. If X is a subgroup of G, then $X^+x = X^+$ for all $x \in X$, and

$$X^+(1+g) = 0 \iff g \in X \tag{1.11}$$

for all $g \in G$.

In particular, if $\langle x_1, x_2, \ldots, x_n\rangle$ is a subgroup of exponent 2 in G, then

$$(1+x_1)(1+x_2)\ldots(1+x_n) = \begin{cases} \langle x_1, x_2, \ldots, x_n\rangle^+ & \text{if } |\langle x_1, \ldots, x_n\rangle| = 2^n, \\ 0 & \text{otherwise.} \end{cases} \tag{1.12}$$

Note also that then $(1+x_1)(1+x_2)\ldots(1+x_n) = (1+x_1x_2)(1+x_2)\ldots(1+x_n)$, etc.

Let now $x_1, \ldots, x_n$ be any elements of G such that for all $i = 1, \ldots, n$, one has $x_i \notin \langle x_1, \ldots, x_{i-1}\rangle$. By an inductive argument, it is easy to see that

$$(1+x_1)(1+x_2)\ldots(1+x_n) \neq 0 \tag{1.13}$$

in $\mathbb{F}G$.

A basic property of the lower central series of the group G (resp. of any Lie algebra L) is that

$$\begin{gathered} (\gamma_i(G), \gamma_j(G)) \subseteq \gamma_{i+j}(G), \\ [\gamma_i(L), \gamma_j(L)] \subseteq \gamma_{i+j}(L) \end{gathered} \tag{1.14}$$

for all $i, j \in \mathbb{N}$ (cf. [**5**, Hauptsatz III.2.11] for groups, and [**2**, section 1.3] for Lie algebras).

In particular, for any group (and any Lie algebra) H, and for all $n \in \mathbb{N}$, we have

$$\delta^n(H) \subseteq \gamma_{2^n}(H). \tag{1.15}$$

This is easily verified using $\gamma_2(H) = H' = \delta^1(H)$, equation 1.14, and induction.

2. The easy direction

2.1. Remark: For any group G we denote by $\omega(\mathbb{F}G) := \mathbb{F}\{1+g\colon\ g \in G\}$ the augmentation ideal of $\mathbb{F}G$. If $H \trianglelefteq G$, then $\omega(\mathbb{F}H)\,\mathbb{F}G = \mathbb{F}G\ \omega(\mathbb{F}H)$ is the kernel of the canonical epimorphism $\mathbb{F}G \to \mathbb{F}[G/H]$ (cf. [**16**, lemma 1.1.8]). In particular, $\mathbb{F}G/\omega(\mathbb{F}G')\mathbb{F}G \cong \mathbb{F}[G/G']$ is abelian, hence $(\mathbb{F}G)' \subseteq \omega(\mathbb{F}G')\,\mathbb{F}G$. Then

$$(\mathbb{F}G)'' \subseteq [\omega(\mathbb{F}G')\,\mathbb{F}G,\ \omega(\mathbb{F}G')\,\mathbb{F}G] \subseteq (\omega(\mathbb{F}G')\,\mathbb{F}G)^2 = \omega(\mathbb{F}G')^2\,\mathbb{F}G.$$

Note moreover that

$$(G')^+\,\mathbb{F}G \subseteq \mathcal{Z}(\mathbb{F}G),$$

since $G' \trianglelefteq G$ obviously implies $(G')^+ \in \mathcal{Z}(\mathbb{F}G)$, and for all $g, h \in G$, we have $[(G')^+g, h] = (G')^+[g,h] = (G')^+(1+(g,h))hg = 0$ by 1.11.

2.2. Lemma: *Let G be a group with $|G'| = 2$. Then $(\mathbb{F}G)' \subseteq (G')^+\,\mathbb{F}G$. In particular, $\mathbb{F}G$ is centre-by-metabelian.*

Proof: We write $G' = \langle x \rangle$. Then $(\mathbb{F}G)' \subseteq \omega(\mathbb{F}G')\,\mathbb{F}G = (1+x)\,\mathbb{F}G = (G')^+\,\mathbb{F}G$.

2.3. Lemma: *Let G be a group with $|G'| = 4$. Then $(\mathbb{F}G)'' \subseteq (G')^+\,\mathbb{F}G$. In particular, $\mathbb{F}G$ is centre-by-metabelian.*

Proof: Case 1: $G' \cong Z_2 \times Z_2$. We write $G' = \langle x, y \rangle$. Since $(1+h)^2 = 1 + h^2 = 0$ for all $h \in G'$, it is easy to see that $\omega(\mathbb{F}G')^2\,\mathbb{F}G = (1+x)(1+y)\,\mathbb{F}G = (G')^+\,\mathbb{F}G$, and hence $(\mathbb{F}G)'' \subseteq (G')^+\,\mathbb{F}G$ by 2.1.

Case 2: $G' \cong Z_4$. We write $G' = \langle x \rangle$, and consider the canonical epimorphism $\mathbb{F}G \to \mathbb{F}[G/\langle x^2 \rangle]$. By 2.2, $\gamma_3(\mathbb{F}[G/\langle x^2 \rangle]) = 0$, so $\gamma_3(\mathbb{F}G) \subseteq \omega(\mathbb{F}\,\langle x^2 \rangle)\,\mathbb{F}G = (1+x^2)\,\mathbb{F}G$. Check that $x^2 \in \mathcal{Z}(G)$ and that $\omega(\mathbb{F}G')^3\,\mathbb{F}G = (G')^+\,\mathbb{F}G$. Then $\gamma_4(\mathbb{F}G) = [\mathbb{F}G, \gamma_3(\mathbb{F}G)] \subseteq [\mathbb{F}G, (1+x^2)\,\mathbb{F}G] = (1+x^2)\,[\mathbb{F}G, \mathbb{F}G] = (1+x)^2\,(\mathbb{F}G)' \subseteq \omega(\mathbb{F}G')^3\,\mathbb{F}G \subseteq (G')^+\,\mathbb{F}G$, and finally $(\mathbb{F}G)'' = \delta^2(\mathbb{F}G) \subseteq \gamma_4(\mathbb{F}G) \subseteq (G')^+\,\mathbb{F}G$ by 1.15.

2.4. Lemma: *Let G be a group of (nilpotence) class 2 with $G' \cong Z_2 \times Z_2 \times Z_2$. Then $(\mathbb{F}G)'' \subseteq (G')^+\,\mathbb{F}G$. In particular, $\mathbb{F}G$ is centre-by-metabelian.*

Proof: We have $\exp(G') = 2$ and $G' \subseteq \mathcal{Z}(G)$. Then by Jennings [**16**, theorem 3.3.7], the second dimension subgroup of G' is trivial, so by [**16**, lemma 3.3.4],

$$\omega(\mathbb{F}G')^n\,\mathbb{F}G = \{(1+x_1)\ldots(1+x_n)\colon\ x_1, \ldots, x_n \in G'\}\,\mathbb{F}G$$

for all $n \in \mathbb{N}$. In particular, $\omega(\mathbb{F}G')^3\,\mathbb{F}G = (G')^+\,\mathbb{F}G$. But then $(\mathbb{F}G)'' = [(\mathbb{F}G)', (\mathbb{F}G)'] \subseteq [\omega(\mathbb{F}G')\,\mathbb{F}G, \omega(\mathbb{F}G')\,\mathbb{F}G] = \omega(\mathbb{F}G')^2\,[\mathbb{F}G, \mathbb{F}G] \subseteq \omega(\mathbb{F}G')^3\,\mathbb{F}G \subseteq (G')^+\,\mathbb{F}G$.

2.5. Lemma: *Let G be a group that acts dihedrally on $G' \cong Z_2 \times Z_4$, and suppose that $\mathcal{C}_G(G')' \subseteq \Phi(G')$. Then $\mathbb{F}G$ is centre-by-metabelian.*

Proof: We write $G' = \langle x, y \rangle$ with $x^2 = 1 = y^4$, and set $C := \mathcal{C}_G(G')$. Then $|G : C| = 2$ and $C' \subseteq \Phi(G') = \langle y^2 \rangle \subseteq \mathcal{Z}(G)$. For $a \in G \smallsetminus C$, we have ${}^a x = x$, ${}^a y = y^3$.

By Jennings [**16**, theorem 3.3.7], the series of dimension subgroups of G' is given as $\langle x, y\rangle \trianglerighteq \langle y^2\rangle \trianglerighteq 1$. By [**16**, lemma 3.3.4], $\omega(\mathbb{F}G')^5 = 0$, and $\omega(\mathbb{F}G')^4 = \mathbb{F}\cdot(G')^+$. Then 2.1 implies that

$$\omega(\mathbb{F}G')^4\,\mathbb{F}G \subseteq \mathcal{Z}(\mathbb{F}G).$$

Note also that

$$1 + C' \subseteq \omega(\mathbb{F}G')^2,$$

since C' is contained in the second dimension subgroup of G'.

Obviously $(\mathbb{F}G)'$ is spanned by all elements of the form

$$[c,d] = cd + {}^{d}(cd), \quad [b,a] = ba + {}^{a}(ba), \quad [a,c] = ac + {}^{c}(ac),$$

with $c, d \in C$, $a, b \in G \smallsetminus C$. Hence it is also spanned by all elements of the form

$$c + {}^{d}c, \quad c + {}^{a}c, \quad a + {}^{c}a,$$

with $c, d \in C$, $a \in G \smallsetminus C$.

Consequently $(\mathbb{F}G)''$ is spanned by all elements of the form

$$\begin{gathered}[c + {}^{d}c, g + {}^{h}g], \quad [c + {}^{a}c, d + {}^{ea}d], \quad [a + {}^{c}a, da + {}^{e}(da)],\\ [c + {}^{a}c, da + {}^{e}(da)],\end{gathered}\tag{$*$}$$

with $c, d, e \in C$, $g, h \in G$, $a \in G \smallsetminus C$. (Note that if $a, a' \in G \smallsetminus C$, then $a' = da$ for some $d \in C$). Now

$$\begin{aligned}[c + {}^{d}c, g + {}^{h}g] &= [(1 + (d,c))c, (1 + (h,g))g]\\ &= (1 + (d,c))(1 + (h,g))[c,g]\\ &= (1 + (d,c))(1 + (h,g))(1 + (c,g))gc\\ &\in \omega(\mathbb{F}G')^4\,\mathbb{F}G,\end{aligned}$$

and

$$\begin{aligned}[c + {}^{a}c, d + {}^{ea}d] &= [(1 + (a,c))c, (1 + (ea,d))d]\\ &= (1 + (a,c))(1 + (ea,d))[c,d]\\ &= (1 + (a,c))(1 + (ea,d))(1 + (c,d))dc\\ &\in \omega(\mathbb{F}G')^4\,\mathbb{F}G,\end{aligned}$$

and

$$\begin{aligned}[c + {}^{a}c, da + {}^{e}(da)] &= [(1 + (a,c))c, (1 + (e,da))da]\\ &= (1 + (e,da))\big((1 + (a,c))cda + (1 + (a,c)^{-1})dac\big)\\ &= (1 + (e,da))\big(1 + (a,c) + (1 + (a,c)^{-1})(da,c)\big)\,cda\\ &= (1 + (e,da))\big(1 + (a,c) + (1 + (a,c)^{-1})(d,c)(a,c)\big)\,cda\\ &= (1 + (e,da))\,(1 + (a,c) + (d,c)(a,c) + (d,c))\,cda\\ &= (1 + (e,da))(1 + (a,c))(1 + (d,c))cda\\ &\in \omega(\mathbb{F}G')^4\,\mathbb{F}G.\end{aligned}$$

Moreover,

$$\begin{aligned}\tau := [a + {}^{c}a, da + {}^{e}(da)] &= [(1+(c,a))a, (1+(e,da))da] \\ &= (1+(c,a))(1+(e,da)^{-1})ada + (1+(e,da))(1+(c,a)^{-1})da^2 \\ &= (\sigma(a,d) + {}^{a}\sigma)da^2,\end{aligned}$$

where $\sigma := (1+(c,a))(1+(e,da)^{-1}) \in \omega(\mathbb{F}G')^2$. We have to show that τ is central in $\mathbb{F}G$. This is equivalent to showing that τ commutes with the elements of C, and with a.

So let $f \in C$. Observe that $(1+(f,da^2))\,{}^{a}t = (1+(f,da^2))t$ for all $t \in G'$, since $(f,da^2) \in C' \subseteq \langle y^2 \rangle = (G,G') \cong Z_2$. It follows that

$$\begin{aligned}[f,\tau] &= (\sigma(a,d) + {}^{a}\sigma)[f, da^2] \\ &= (\sigma(a,d) + {}^{a}\sigma)(1+(f,da^2))da^2 f \\ &= (1+(f,da^2))(\sigma(a,d)+\sigma)da^2 f \\ &= (1+(f,da^2))(1+(a,d))\sigma da^2 f \\ &\in \omega(\mathbb{F}G')^5\,\mathbb{F}G = 0.\end{aligned}$$

Finally, check that ${}^{a}\tau = ({}^{a}\sigma\ {}^{a}(a,d) + {}^{a^2}\sigma)\,{}^{a}da^2 = ({}^{a}\sigma\,(a,d)^{-1} + \sigma)(a,d)da^2 = \tau$.

This shows that all elements of the form $(*)$ are central. Therefore $(\mathbb{F}G)''$ is central, and $\mathbb{F}G$ is centre-by-metabelian.

2.6. Lemma: *Let A be a commutative $\mathbb{F}$-algebra (with unit). Then the algebra $M = \mathrm{Mat}(2,A)$ of all 2×2-matrices over A is centre-by-metabelian.*

Proof: Let $e_{11}, e_{22}, e_{12}, e_{21} \in M$ denote the usual matrix units, i.e. $e_{ij}e_{kl} = \delta_{jk}e_{il}$ for $i,j,k,l \in \{1,2\}$. Then M' is spanned by e_{12}, e_{21}, $e_{11}+e_{22}$, where $e_{11}+e_{22}$ is obviously central. Thus M'' is spanned by $[e_{12},e_{21}] = e_{11}+e_{22} \in \mathcal{Z}(M)$.

2.7. Lemma: *Let G be a group with an abelian subgroup A of index 2. Then $\mathbb{F}G$ is centre-by-metabelian.*

Proof: By [**15**, lemma 1.3], there is an $\mathbb{F}$-algebra monomorphism $\mathbb{F}G \hookrightarrow \mathrm{Mat}(2,\mathbb{F}A)$. By 2.6, $\mathbb{F}G$ is centre-by-metabelian.

2.8. Theorem (summary): *Let G be a group such that one of the following assertions holds:*

(i) $|G'| \mid 4$.
(ii) $G' \cong Z_2 \times Z_2 \times Z_2$ *and* $\mathrm{cl}(G) = 2$.
(iii) *G acts dihedrally on* $G' \cong Z_2 \times Z_4$, *and* $\mathcal{C}_G(G')' \subseteq \Phi(G')$.
(iv) *G contains an abelian subgroup A of index 2.*

Then $\mathbb{F}G$ is centre-by-metabelian.

2.9. Example: (i) Let B be an arbitrary finite abelian group. We may write $B \cong Z_{n_1} \times \ldots \times Z_{n_k}$ with even integers $n_1, \ldots, n_r$, and odd integers $n_{r+1}, \ldots, n_k$. We set $A := Z_{2n_1} \times \ldots \times Z_{2n_r} \times Z_{n_{r+1}} \times \ldots \times Z_{n_k}$, and embed B into A. The map $\alpha\colon A \to A$, $x \mapsto x^{-1}$, is an automorphism of A of order 2 such that $(\alpha, A) = B$. Set $G := A \rtimes \langle\alpha\rangle$

(or let G be any other extension of $\langle\alpha\rangle$ with A). Then $\mathbb{F}G$ is centre-by-metabelian by 2.8 (iv). By 1.6, $G' = (\alpha, A)A' = (\alpha, A) = B$. Obviously, the same construction is possible (just more awkward to formulate) if B is an arbitrary infinite abelian group. This shows that every abelian group may appear as a commutator subgroup of the groups in theorem 2.8. So the situation here in characteristic 2 is quite different from all other characteristics (cf. theorem 3).

(ii) If at least one of the n_i in (i) is odd, then G is not nilpotent. Hence $\mathbb{F}G$ is Lie solvable but not Lie nilpotent by theorem 1. Moreover, $\mathbb{F}G$ is centre-by-metabelian but not metabelian by theorem 2.

(iii) Similarly, $\mathbb{F}A_4$ is centre-by-metabelian by 2.8 (i), since $A_4' \cong V_4$, but neither metabelian nor nilpotent, since A_4 is not nilpotent.

(iv) A group that satisfies 2.8 (iii), but not 2.8 (iv), is e.g. given by the following construction: Let $H := \langle x, d\rangle \cong Z_2 \times Z_8$, where $x^2 = 1 = d^8$, and set $y := d^2$. Then ${}^c x := x$, ${}^c d := d^5 = dy^2$ defines an automorphism c of order 2 of H. Then $C := H \rtimes \langle c\rangle$ is a group of order 32. Obviously $C' = \langle y^2\rangle \cong Z_2$. It is easy to check that ${}^a x := x$, ${}^a d := d^3 = dy$, ${}^a c := cx$ defines an automorphism a of C. Then $G := C \rtimes \langle a\rangle$ is a group of order 64, and by 1.6, $G' = (a, C)C' = \langle x, y\rangle \cong Z_2 \times Z_4$. Since ${}^a y = {}^a d^2 = d^6 = y^3$, G acts dihedrally on G', C centralizes G', and $C' = \langle y^2\rangle = \Phi(G')$.

(v) Note that the condition that $\mathcal{C}_G(G')'$ is contained in $\Phi(G')$ is essential in 2.8 (iii). This stems from the fact that $\Phi(G')$ is the second dimension subgroup of G', as is mentioned in the proof of lemma 2.5. It is not enough to require $\left|\mathcal{C}_G(G')'\right| \leq 2$, as the following example shows: Let $H := \langle x, d\rangle \cong Z_2 \times Z_8$ and $y := d^2$ as above. Then ${}^c x := x$, ${}^c d := dx$ defines an automorphism c of order 2 of H, and $C := H \rtimes \langle c\rangle$ is a group of order 32 with $C' = \langle x\rangle \cong Z_2$. Now ${}^a x := x$, ${}^a d := d^3 = dy$, ${}^a c := cx$ again defines an automorphism a of C. Then $G := C \rtimes \langle a\rangle$ is a group of order 64 that acts dihedrally on $G' = (a, C)C' = \langle x, y\rangle \cong Z_2 \times Z_4$. As above, we have $\mathcal{C}_G(G') = C$, since ${}^c y = {}^c d^2 = (dx)^2 = d^2 = y$. But this time we have $C' = \langle x\rangle \nsubseteq \Phi(G')$. It can be checked that $[d, d + {}^c d, a + {}^d a] = (G')^+ a \neq 0$ (for the actual computation see the proof of lemma 6.11). Hence $\mathbb{F}G$ is not centre-by-metabelian.

2.10. Remark: According to 1.7, the action of G on G' is dihedral in 2.8 (iv). Moreover, G/A is abelian, hence $G' \subseteq A$, and thus $A \subseteq \mathcal{C}_G(G')$.

In turn, this implies that

$$A = \mathcal{C}_G(G') \iff \mathcal{C}_G(G') < G \iff \exists h \in G' \colon h^{-1} \neq h \iff \exp(G') \nmid 2.$$

Therefore the abelian subgroup A is uniquely determined, unless G' is central (which is equivalent to being elementary abelian in this case).

We will use this fact in the proof of the converse of theorem 2.8, when we study the action of G on G': If that action is not dihedral, we may already rule out the existence of an A as above. On the other hand, if the action is dihedral, and if we want to show the existence of such an A, we do not have to search very long for it; what we have to do is precisely to show that $A := \mathcal{C}_G(G')$ is abelian — unless G has class 2, but this case is special anyway in view of 2.8 (ii), so it will be treated separately in the next section.

3. Groups of nilpotence class 2

3.1. Remark: (i) Let G be a group of class 2. Then the formulas in 1.1 reduce to $(ab, c) = (a, c)(b, c)$ and $(a, bc) = (a, b)(a, c)$ for all $a, b, c \in G$. It follows that $(b, a) = (a, b)^{-1} = (a, b^{-1}) = (a^{-1}, b)$, and that $(a, bc) = (a, cb)$.

(ii) Suppose $G = \langle X \rangle$ for some subset X of G. A consequence of (i) is that $G' = \langle (x, y)\colon\, x, y \in X \rangle$. In the particular case $G = \langle g_1, \dots, g_n \rangle$, one obtains $G' = \langle (g_i, g_j)\colon 1 \le i < j \le n \rangle$.

(iii) The following definition (due to A. Shalev [**21**]) has proved to be useful for the study of $(\mathbb{F}G)''$: For $x \in G'$ set

$$S_x := \{a \in G : (a, b) = x \text{ for some } b \in G\}.$$

Using (i), it is easy to check that $S_x = S_x^{-1} = S_{x^{-1}}$ and $\{ad, da, bc, cb : c \in \mathcal{C}_G(a), d \in \mathcal{C}_G(b)\} \subseteq S_x$ for all $a, b \in G$ with $(a, b) = x$; note that especially $c \in \langle a \rangle$ and $d \in \langle b \rangle$ are allowed. The following lemmata state some further properties of S_x:

3.2. Lemma: *Let G be a group of class 2, and let $x, y \in G'$. Then*

(i) $(1 + x)S_x \subseteq [S_x, S_x]$,

(ii) $[(1 + x)S_x, (1 + y)S_y] \subseteq (\mathbb{F}G)''$,

(iii) $(1 + x)^3 S_x \subseteq (\mathbb{F}G)''$,

Proof: (i) For each $b \in S_x$, there is an $a \in G$ with $x = (b, a^{-1}) = (a, b)$. Then $(1 + x)b = b + (a, b)b = b + aba^{-1} = [a^{-1}, ab] \in [S_x, S_x]$ by 3.1 (iii).

(ii) Follows immediately from (i).

(iii) $(\mathbb{F}G)'' \supseteq [(1 + x)S_x, (1 + x)S_x] = (1 + x)^2[S_x, S_x] \supseteq (1 + x)^3 S_x$.

3.3. Lemma: *Let G be a group of class 2 such that $\mathbb{F}G$ is centre-by-metabelian. If G is generated by two elements, then $|G'| \mid 4$.*

Proof: We write $G = \langle g, h \rangle$, and set $x := (g, h)$. Then $G' = \langle x \rangle$ by 3.1 (ii). By 3.2, we have $(1 + x)^4 g \in (1 + x)^4 S_x \subseteq [(1 + x)^3 S_x, S_x] \subseteq [(\mathbb{F}G)'', \mathbb{F}G] = 0$. Hence $0 = (1 + x)^4 = 1 + x^4$, and $x^4 = 1$.

3.4. Lemma: *Let G be a group of class 2 such that $\mathbb{F}G$ is centre-by-metabelian. If there is an $x \in G'$ with $|\,\langle x \rangle\,| \ge 4$, then:*

(i) $(S_x, G) \subseteq \langle x \rangle$.

(ii) If $y \in G'$ with $S_x \cap S_y \neq \emptyset$, then $y \in \langle x \rangle$.

Proof: (i) W.l.o.g. $S_x \neq \emptyset$. Let $a \in S_x$, $g \in G$. Then, by 1.11 and 3.2 (iii),

$$\begin{aligned} \langle x \rangle^+(1 + (a, g)) &= (1 + x)^3[a, g](ga)^{-1} \\ &\in (1 + x)^3[S_x, \mathbb{F}G](ga)^{-1} = [(1 + x)^3 S_x, \mathbb{F}G](ga)^{-1} \\ &\subseteq [(\mathbb{F}G)'', \mathbb{F}G](ga)^{-1} = 0 \\ \iff\quad & (a, g) \in \langle x \rangle\,. \end{aligned}$$

(ii) Let $a \in S_x \cap S_y$, $b \in G$ with $y = (a, b)$. Then by (i), $y = (a, b) \in (S_x, G) \subseteq \langle x \rangle$.

3.5. Lemma: *Let G be a group of class 2. If $\mathbb{F}G$ is centre-by-metabelian, then G' is an elementary abelian 2-group, or $G' \cong Z_4$.*

Proof: By considering the two-generator subgroups of G, we have $(g,h)^4 = 1$ for all $g, h \in G$ by 3.3. If $\exp(G') = 2$ we are done.

Otherwise, there is a commutator of order 4 in G, say $x = (a,b)$. Let $y = (c,d)$ be an arbitrary commutator in G. By 3.4, we know that $(a,b), (a,d), (c,b) \in \langle x \rangle$, so there is a $k \in \{0,1,2,3\}$ such that $(ac, bd) = (a,b)(a,d)(c,b)(c,d) = x^k y$.

Consider $(ac,b) = (a,b)(c,b) = x(c,b)$ and distinguish the following cases:

Case 1: $(c,b) = 1$. Then $(ac,b) = x$, hence $ac \in S_x \cap S_{x^k y}$, and $x^k y \in \langle x \rangle$ by 3.4.

Case 2: $(c,b) = x$. Then $c \in S_x \cap S_y$ and $y \in \langle x \rangle$.

Case 3: $(c,b) = x^2$. Then $(ac,b) = x^3 = x^{-1}$, i.e. $(b,ac) = x$ and $ac \in S_x \cap S_{x^k y}$, so $x^k y \in \langle x \rangle$.

Case 4: $(c,b) = x^3$. Then $(b,c) = x$ and $c \in S_x \cap S_y$, hence $y \in \langle x \rangle$.

In any case, we have $y \in \langle x \rangle$. Therefore $G' = \langle x \rangle \cong Z_4$.

3.6. Remark: The preceding lemma already comes very close to showing the classification theorem 4 for groups G of class 2. All which remains to face are groups G with elementary abelian, central commutator subgroups G' of (2-)rank greater than 3. We have to show that if $\mathbb{F}G$ is centre-by-metabelian, then G contains an abelian subgroup A of index 2.

So suppose that G is a counterexample, and A is a maximal abelian subgroup of G (the existence of A is guaranteed by Zorn's lemma). To make the proofs of the following lemmata work, let us agree upon choosing A in such a way that $|A : \mathcal{Z}(G)| > 2$, if at all possible. In other words, we may assume that if $|A : \mathcal{Z}(G)| \leq 2$, then $|B : \mathcal{Z}(G)| \leq 2$ for all maximal abelian subgroups B of G.

Then $\mathbb{F}G$ is centre-by-metabelian, and $|G : A| > 2$, and $|G'| \geq 16$, and $\exp(G') = 2$, and $G' \subseteq \mathcal{Z}(G) \subseteq A$ (in particular $A \trianglelefteq G$), and $\mathcal{C}_G(A) = A$ (in particular $A > \mathcal{Z}(G)$).

Let $g, h \in G$, then $(g^2, h) = (g,h)^2 = 1$; i.e. all squares are central in G. Therefore $G/\mathcal{Z}(G)$ and G/A are both elementary abelian 2-groups. Then $|G : A| > 2$ implies that $|G : A| \geq 4$.

We divide our examination of G into the following cases:

- $|G' : (G,A)| \geq 8$ (handled by 3.7),
- $|G' : (G,A)| = 4$ (handled by 3.8),
- $|G' : (G,A)| = 2$ (handled by 3.9),
- $|G' : (G,A)| = 1$ (handled by 3.10).

In each case we will show that $\mathbb{F}G$ is not centre-by-metabelian, in contradiction to our assumption.

3.7. Lemma: *Let G and A be as in 3.6, and suppose that $|G' : (G,A)| \geq 8$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Assume that $\mathbb{F}G$ is centre-by-metabelian.

For $\bar{G} := G/(G,A)$, we have $\exp(\bar{G}') = 2$, and $|\bar{G}'| \geq 8$.

Let us at first assume that there are $\bar{s}, \bar{t}, \bar{u}, \bar{v} \in \bar{G}$ with $|\,\langle \bar{s}, \bar{t}, \bar{u}, \bar{v}\rangle'\,| \geq 8$; w.l.o.g. $(\bar{s}, \bar{t}) \neq 1$. If $(\bar{u}, \bar{v}) \in \langle(\bar{s}, \bar{t})\rangle$, then there are elements $\bar{p} \in \{\bar{s}, \bar{t}\}$, $\bar{q} \in \{\bar{u}, \bar{v}\}$ with $(\bar{p}, \bar{q}) \notin \langle(\bar{s}, \bar{t})\rangle$, w.l.o.g. $\bar{p} = \bar{s}$, $\bar{q} = \bar{u}$. Then $\langle \bar{s}, \bar{t}, \bar{u}, \bar{v}\rangle = \langle \bar{s}, \bar{t}, \bar{u}, \bar{s}\bar{v}\rangle$ and $|\langle(\bar{s}, \bar{t}), (\bar{u}, \bar{s}\bar{v})\rangle| = 4$ since $(\bar{u}, \bar{s}\bar{v}) = (\bar{u}, s)(\bar{u}, \bar{v}) \in (\bar{u}, s)\,\langle(\bar{s}, \bar{t})\rangle \neq \langle(\bar{s}, \bar{t})\rangle$. So by replacing $\bar{v}$ by $\bar{s}\bar{v}$ if necessary, we may assume that $|\langle(\bar{s}, \bar{t}), (\bar{u}, \bar{v})\rangle| = 4$. Since $|\,\langle \bar{s}, \bar{t}, \bar{u}, \bar{v}\rangle'\,| \geq 8$, there must be $\bar{p} \in \{\bar{s}, \bar{t}\}$, $\bar{q} \in \{\bar{u}, \bar{v}\}$ with $(\bar{p}, \bar{q}) \notin \langle(\bar{s}, \bar{t}), (\bar{u}, \bar{v})\rangle$, w.l.o.g. $\bar{p} = \bar{s}$, $\bar{q} = \bar{u}$; i.e. $|\langle(\bar{s}, \bar{t}), (\bar{u}, \bar{v}), (\bar{s}, \bar{u})\rangle| = 8$.

We move back into G by choosing preimages $s, t, u, v \in G$ of $\bar{s}, \bar{t}, \bar{u}, \bar{v}$, respectively. We set $x := (s, t)$, $y := (u, v)$, $z := (s, u)$, then $|\langle x, y, z\rangle| = 8$, and $\langle x, y, z\rangle \cap (G, A) = 1$. Moreover, $su \notin \mathcal{C}_G(A) = A$, for otherwise $z = (u, s) = (s, su) \in (G, A)$. Consequently there is an $a \in A$ with $w := (su, a) \neq 1$. Because $w \in (G, A)$, we have $|\langle x, y, z, w\rangle| = 16$. But then

$$\begin{aligned}(1+x)(1+y)(1+z)su = (1+x)(1+y)[s, u] &= [(1+x)s, (1+y)u] \\ &\in [(1+x)S_x, (1+y)S_y] \subseteq (\mathbb{F}G)'',\end{aligned}$$

and

$$\begin{aligned}0 \neq (1+x)(1+y)(1+z)(1+w)asu &= (1+x)(1+y)(1+z)[su, a] \\ &= [(1+x)(1+y)(1+z)su, a] \in [(\mathbb{F}G)'', \mathbb{F}G] = 0.\end{aligned}$$

This means that our assumption at the beginning is rubbish, and we may conclude:

$$(*) \qquad \text{If } \bar{H} \leq \bar{G} \text{ is generated by four elements, then } |\bar{H}'| \leq 4.$$

In the following, we will reduce this conclusion to absurdum. For simplicity, and since we will not switch back to G anymore, we will omit the bars $\bar{\ }$ over the elements of $\bar{G}$ in the following.

Choose $s, t, u, v \in \bar{G}$ with $|\langle x, y\rangle| = 4$ for $x := (s, t)$, $y := (u, v)$. By $(*)$, $\langle s, t, u, v\rangle' = \langle x, y\rangle$. In the case that $\langle s, t, u\rangle' = \langle x\rangle = \langle s, t, v\rangle'$ and $\langle s, u, v\rangle' = \langle y\rangle = \langle t, u, v\rangle'$ we obtain $(\langle s, t\rangle, \langle u, v\rangle) \subseteq \langle x\rangle \cap \langle y\rangle = 1$, and it follows that $(su, t) = (s, t) = x$, $(su, v) = (u, v) = y$, hence $\langle su, t, v\rangle' = \langle x, y\rangle$. In any case, there are three elements $s, t, u \in \bar{G}$ such that $|\langle x, y\rangle| = 4$ with $x := (s, t)$, $y := (s, u)$.

Because of $|\bar{G}'| \geq 8$, there are $g, h \in \bar{G}$ with $z := (g, h) \notin \langle x, y\rangle$. Conclusion $(*)$ then implies that

$$\begin{aligned} & \langle s, t, u, g\rangle' = \langle x, y\rangle = \langle s, t, u, h\rangle', \\ & \langle s, t, g, h\rangle' = \langle x, z\rangle, \\ & \langle s, u, g, h\rangle' = \langle y, z\rangle; \\ \Longrightarrow \quad & (\langle g, h\rangle, s) \subseteq \langle x, y\rangle \cap \langle x, z\rangle \cap \langle y, z\rangle = 1, \\ & (\langle g, h\rangle, u) \subseteq \langle x, y\rangle \cap \langle y, z\rangle = \langle y\rangle, \\ & (\langle g, h\rangle, t) \subseteq \langle x, y\rangle \cap \langle x, z\rangle = \langle x\rangle. \end{aligned}$$

If $(\langle g, h\rangle, u) = \langle y\rangle$ and $(\langle g, h\rangle, t) = \langle x\rangle$, we would have $\langle g, h, u, t\rangle' \supseteq \langle x, y, z\rangle$ in contradiction to $(*)$. So assume w.l.o.g. that $(\langle g, h\rangle, t) = 1$. If $(g, u) = y$ and $(h, u) = y$, then $(gh, u) = y^2 = 1$. Moreover, $z = (g, h) = (h, g) = (gh, g) = (g, gh) = (h, gh) = (gh, h)$. Thus, by permuting $\{g, h, gh\}$ in a suitable way, we may assume that $(g, u) = 1$. But then

$(gs,t) = (s,t) = x$, $(gs,u) = (s,u) = y$, $(gs,h) = (g,h) = z$, and $\langle gs,t,u,h\rangle' \supseteq \langle x,y,z\rangle$ in contradiction to $(*)$.

3.8. Lemma: *Let G and A be as in 3.6, and suppose that $|G' : (G,A)| = 4$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Assume that $\mathbb{F}G$ is centre-by-metabelian.

Set $\bar G := G/(G,A)$, then $\exp(\bar G') = 2$ and $|\bar G'| = 4$. As in the proof of 3.7, there are $\bar s, \bar t, \bar u \in \bar G$ with $\bar G' = \langle \bar s, \bar t, \bar u\rangle' = \langle \bar x, \bar y\rangle$, where $\bar x := (\bar s, \bar t)$, $\bar y := (\bar s, \bar u)$. If $(\bar t, \bar u) = \bar x$ then $(\bar t, \bar s\bar u) = \bar x^2 = 1$ and $(\bar s, \bar s\bar u) = \bar y$; if $(\bar t, \bar u) = \bar y$ then $(\bar s\bar t, \bar u) = \bar y^2 = 1$ and $(\bar s, \bar s\bar t) = \bar x$; and if $(\bar t, \bar u) = \bar x\bar y$ then $(\bar s\bar t, \bar s\bar u) = 1$ and $(\bar s, \bar s\bar t) = \bar x$ and $(\bar s, \bar s\bar u) = \bar y$. Thus, by replacing $\bar t$ (respectively $\bar u$) by $\bar s\bar t$ (respectively $\bar s\bar u$) if necessary, we may assume that $(\bar t, \bar u) = 1$.

Let now $s,t,u,x,y \in G$ be suitable preimages of $\bar s, \bar t, \bar u, \bar x, \bar y$, respectively, such that $x = (s,t)$ and $y = (s,u)$. Certainly $(t,u) \in (G,A)$. If $(t,u) = 1$, let $a \in A \smallsetminus \mathcal{C}_A(t) \neq \emptyset$, then $(t,ua) \neq 1$. Thus, by replacing u by ua if necessary, we may assume that $w := (t,u) \in (G,A) \smallsetminus \{1\}$. Then $(s,tu) = xy$ and

$$\begin{aligned}\sigma &:= (1+x)(1+y)(1+w)ttu = (1+xy)(1+x)(1+w)ttu\\ &= (1+xy)(1+x)[tu,t] = [(1+xy)tu, (1+x)t]\\ &\in [(1+xy)S_{xy}, (1+x)S_x] \subseteq (\mathbb{F}G)''.\end{aligned}$$

If $(u,A) \not\subseteq \langle w\rangle$, and $z := (u,b) \notin \langle w\rangle$ with $b \in A$, then $|\langle x,y,z,w\rangle| = 16$ and therefore $0 = [b,\sigma] = t^2(1+x)(1+y)(1+w)[b,u] = t^2(1+x)(1+y)(1+w)(1+z)bu \neq 0$, contradiction (recall that all squares are central in G, cf. 3.6). Hence $(u,A) \subseteq \langle w\rangle$. Similarly one shows that $(t,A) \subseteq \langle w\rangle$; this implies $(\langle t,u\rangle, A) = (t,A)(u,A) \subseteq \langle w\rangle$.

Now $|G'| \geq 16$ implies $|(G,A)| \geq 4$, so there is an element $g \in G$ with $(g,A) \not\subseteq \langle w\rangle$. The map $\sigma\colon A \to A$, $a \mapsto (g,a)$, is a homomorphism by 3.1 (i) with image (g,A), hence $\sigma^{-1}(\langle w\rangle) < A$. Consequently $A \neq \mathcal{C}_A(t) \cup \sigma^{-1}(\langle w\rangle)$, so there exists an $a \in A$ such that $(t,a) \neq 1$ (i.e. $w = (t,a) = (ta,a)$) and $z := (g,a) \in (G,A) \smallsetminus \langle w\rangle$.

Set $\tilde x := (s,ta) = x(s,a) \in x(G,A)$; then $|\langle \tilde x, y, z, w\rangle| = 16$. By 3.2,

$$(1+y)(1+w)(1+\tilde x)sta = (1+y)(1+w)[s,ta] = [(1+y)s, (1+w)ta] \in (\mathbb{F}G)'',$$

hence $0 = [g,(1+y)(1+w)(1+\tilde x)sta] = (1+y)(1+w)(1+\tilde x)(1+(sta,g))gsta$. This implies $(st,g)z = (sta,g) \in \langle \tilde x, y, w\rangle$, i.e. $(st,g) \equiv z \pmod{\langle \tilde x, y, w\rangle}$. Let $\tilde{\tilde x} := (as,ta) = w\tilde x \equiv \tilde x \pmod{\langle w\rangle}$ and $\tilde y := (as,u) = y(a,u) \equiv y \pmod{\langle w\rangle}$. We obtain $(1+w)(1+y)(1+\tilde x)ta^2s = (1+w)(1+\tilde y)(1+\tilde{\tilde x})ta \cdot as = [(1+w)ta, (1+\tilde y)as] \in (\mathbb{F}G)''$, which leads to the contradiction $0 = [g,(1+w)(1+y)(1+\tilde x)ta^2s] = a^2(1+w)(1+y)(1+\tilde x)(1+(st,g))gst = a^2(1+w)(1+y)(1+\tilde x)(1+z)gst \neq 0$.

3.9. Lemma: *Let G and A be as in 3.6, and suppose that $|G' : (G,A)| = 2$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Assume that $\mathbb{F}G$ is centre-by-metabelian. We have $|(G,A)| \geq 8$.

Suppose at first that there are $s, t \in G$ with $(s,t) \notin (G,A)$ and $|(\langle s,t \rangle, A)| \geq 8$.Then argue as follows:

$$\begin{aligned}
&\forall a, b \in A\colon\ (1+(s,a))(1+(t,b))(1+(s,t))ts = [(1+(t,b))t, (1+(s,a))s] \in (\mathbb{F}G)'' \\
\Longrightarrow\ &\forall a, b, c \in A\colon\ 0 = [c, (1+(s,a))(1+(t,b))(1+(s,t))ts] \\
\Longrightarrow\ &\forall a, b, c \in A\colon\ 0 = (1+(s,a))(1+(t,b))(1+(s,t))(1+(ts,c))cts \\
\Longrightarrow\ &\forall a, b, c \in A\colon\ |\langle (s,a), (t,b), (ts,c), (s,t) \rangle| \leq 8 \\
\Longrightarrow\ &\forall a, b, c \in A\colon\ |\langle (s,a), (t,b), (ts,c) \rangle| \leq 4. \qquad (*)
\end{aligned}$$

Since $(\langle s,t \rangle, A) = (s,A)(t,A)$, assume w.l.o.g. $|(s,A)| \geq 4$. Choose $a, b \in A$ such that $(t,b) \neq 1$ and $(s,a) \notin \langle (t,b) \rangle$. Then $(*)$ implies that $(ts,A) \subseteq \langle (s,a), (t,b) \rangle$. Hence $(s,A) \not\subseteq \langle (s,a), (t,b) \rangle$ or $(t,A) \not\subseteq \langle (s,a), (t,b) \rangle$.

If $(s,A) \cap (t,A) = 1$, then $(\langle s,t \rangle, A) = (s,A)(t,A) = (s,A) \times (t,A)$. Let $c \in A$, then $(s,c)(t,c) = (st,c) \in \langle (s,a), (t,b) \rangle$, hence $(s,c) \in \langle (s,a) \rangle$ and $(t,c) \in \langle (t,b) \rangle$. But this implies that $(\langle s,t \rangle, A) = (s,A)(t,A) \subseteq \langle (s,a), (t,b) \rangle$, contradiction.

So we may assume that $(s,A) \cap (t,A) \neq 1$. Then there are $a, b, d \in A$ with $1 \neq (t,b) = (s,d)$ and $(s,a) \notin \langle (t,b) \rangle$, and $(*)$ implies again that $(ts,A) \subseteq \langle (s,a), (t,b) \rangle = \langle (s,a), (s,d) \rangle \subseteq (s,A)$. It follows that $(\langle s,t \rangle, A) = (s,A)(st,A) = (s,A)$. Conclusion $(*)$ then implies that $|\langle (s,a), (t,b), (s,c) \rangle| \leq 4$ for all $a, b, c \in A$, i.e. (t,A) is contained in all subgroups of (s,A) of order 4. The intersection of all those subgroups is trivial, because $|(s,A)| \geq 8$, but (t,A) cannot be trivial, because $t \notin A = \mathcal{C}_G(A)$.

This shows that $|(\langle s,t \rangle, A)| \leq 4$ for all $s, t \in G$ with $(s,t) \notin (G,A)$.

We now assume that there are $s, t \in G$ with $z := (s,t) \notin (G,A)$ and $|(\langle s,t \rangle, A)| = 4$. Then there is an element $g \in G$ with $(g,A) \not\subseteq (\langle s,t \rangle, A)$.

If $|(s,A)| = 4$, then $(\langle s,t \rangle, A) = (s,A)$. This implies $|(\langle s,g \rangle, A)| \geq 8$ and $|(\langle s,tg \rangle, A)| \geq 8$, hence $(s,g) \in (G,A)$ and $(s,tg) \in (G,A)$ by the above. But then also $(s,t) = (s,tg)(s,g) \in (G,A)$, contradiction.

Consequently $|(s,A)| = 2$, and similarly $|(t,A)| = 2$, say $(s,A) = \langle x \rangle$ and $(t,A) = \langle y \rangle$. Let $a \in A$. Then $|\langle x,y,z \rangle| = 8$, $s \in S_x$, $ta \in S_y$, $(s,ta) = z(s,a) \equiv z \pmod{\langle x \rangle}$ and

$$(1+x)(1+y)(1+z)tas = (1+x)(1+y)(1+(s,ta))tas = [(1+y)ta, (1+x)s] \in (\mathbb{F}G)''.$$

It follows that $0 = [g, (1+x)(1+y)(1+z)tas] = (1+x)(1+y)(1+z)(1+(g,a)(g,st))tasg$, i.e. $(g,st) \in (g,a)\langle x,y,z \rangle$ for all $a \in A$. But this is ridiculous since $\bigcap_{a \in A} (g,a)\langle x,y,z \rangle = \emptyset$ because of $(g,A) \not\subseteq \langle x,y,z \rangle$.

This shows that $|(\langle s,t \rangle, A)| = 2$ for all $s, t \in G$ with $(s,t) \notin (G,A)$. On the other hand, there surely are $s, t \in G$ with $(s,t) \notin (G,A)$, since $G' \neq (G,A)$. Then $(s,A) = (\langle s,t \rangle, A) = (t,A)$. Let $g \in G$ with $(g,A) \not\subseteq (\langle s,t \rangle, A)$, then $|(\langle g,t \rangle, A)| \geq 4$ and $|(\langle gs,t \rangle, A)| \geq 4$. This implies $(g,t) \in (G,A)$ and $(gs,t) \in (G,A)$, which leads to the contradiction $(s,t) = (gs,t)(g,t) \in (G,A)$.

3.10. Lemma: *Let G and A be as in 3.6, and suppose that $|G' : (G,A)| = 1$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Assume that $\mathbb{F}G$ is centre-by-metabelian. Since $G' = (G, A)$, we have $|(G, A)| \geq 16$.

Let us at first make the additional assumption that $|(s, A)| = 2$ for all $s \in G \smallsetminus A$.

We claim that in this case $(r, s) \in (r, A)(s, A)$ for all $r, s \in G \smallsetminus A$ with $(r, A) \neq (s, A)$. If not, then there are $r, s \in G \smallsetminus A$ such that $|\langle x, y, z\rangle| = 8$, where $(r, A) = \langle x\rangle$, $(s, A) = \langle y\rangle$, and $z := (r, s)$. Since $A \neq \mathcal{C}_A(r) \cup \mathcal{C}_A(s)$, there is an $a \in A$ with $x = (r, a)$, $y = (s, a)$. By hypothesis, $|(G, A)| \geq 16$, hence there are $t \in G$, $c \in A$ with $w := (t, c) \notin \langle x, y, z\rangle$. For any $d \in A$, we then have

$$\begin{aligned}
\sigma := [[s, dr], [s, a]] &= [(1 + (s, dr))drs, (1 + (s, a))as] = (1 + (s, dr))(1 + (s, a))[drs, as] \\
&= (1 + (s, dr))(1 + (s, a))(1 + (drs, as))asdrs \\
&= (1 + \underbrace{(s, d)}_{\in\langle y\rangle}(s, r))(1 + y)(1 + \underbrace{(ds, as)}_{\in\langle y\rangle}(r, a)(r, s))asdrs \\
&= (1 + z)(1 + y)(1 + xz)asdrs \;=\; (1 + z)(1 + y)(1 + x)asdrs,
\end{aligned}$$

and

$$\begin{aligned}
0 = [t, \sigma] &= (1 + z)(1 + y)(1 + x)(1 + (t, asdrs))asdrst \\
&= (1 + z)(1 + y)(1 + x)(1 + (t, ar)(t, d))asdrst.
\end{aligned}$$

This implies that $(t, ar) \in (t, d)\,\langle x, y, z\rangle$ for all $d \in A$; in particular we have $(t, ar) \in (t, c)\,\langle x, y, z\rangle \cap (t, 1)\,\langle x, y, z\rangle = w\,\langle x, y, z\rangle \cap \langle x, y, z\rangle = \emptyset$. This contradiction proves our claim.

We claim next that there are $r, s \in G \smallsetminus A$ with $\mathcal{C}_A(r) \neq \mathcal{C}_A(s)$. Otherwise we have $\mathcal{C}_A(r) = \mathcal{C}_A(s)$ for all $r, s \in G \smallsetminus A$, hence $\mathcal{C}_A(s) = \mathcal{Z}(G)$ for all $s \in G \smallsetminus A$. Let $s \in G \smallsetminus A$, and consider the homomorphism $A \to A$, $a \mapsto (s, a)$. Its image is (s, A) and its kernel $\mathcal{C}_A(s) = \mathcal{Z}(G)$; in particular $A/\mathcal{Z}(G) \cong (s, A)$, and therefore $|A : \mathcal{Z}(G)| = 2$. By the choice of A, this implies $|B : \mathcal{Z}(G)| \leq 2$ for all maximal abelian subgroups B of G (cf. 3.6). Let $r \in G \smallsetminus A$ with $(r, A) \neq (s, A)$, then $(r, s) \in (r, A)(s, A)$ by the previous claim. Since $(r, A)(s, A) = (r, A) \cup (s, A) \cup (rs, A)$ (for order reasons) and $(r, s) = (s, r) = (s, rs) = (rs, s) = (r, rs) = (rs, r)$, we may permute $\{r, s, rs\}$ in a suitable way and assume that $(r, s) \in (r, A)$, i.e. $(r, s) = (r, a)$ for some $a \in A$. Then $(r, sa) = 1$, so we may replace s by sa and assume $(r, s) = 1$. Certainly $(r, A) \neq (s, A) \implies r\mathcal{Z}(G) \neq s\mathcal{Z}(G) \implies |B : \mathcal{Z}(G)| > 2$, where $B := \langle \mathcal{Z}(G), r, s\rangle$; but then B is abelian in contradiction to a previous statement.

Now let $r, s \in G \smallsetminus A$ with $\mathcal{C}_A(r) \neq \mathcal{C}_A(s)$. If $(r, A) = (s, A)$, there is an element $t \in G \smallsetminus A$ with $(r, A) \neq (t, A)$. If $\mathcal{C}_A(r) = \mathcal{C}_A(t)$, then $\mathcal{C}_A(r) \neq \mathcal{C}_A(st)$ and $(r, A) \neq (st, A)$. In any case, there are $r, s \in G \smallsetminus A$ with $(r, A) \neq (s, A)$ and $\mathcal{C}_A(r) \neq \mathcal{C}_A(s)$, w.l.o.g. $\mathcal{C}_A(r) \not\subseteq \mathcal{C}_A(s)$. We choose such r, s and write $(r, A) = \langle x\rangle$, $(s, A) = \langle y\rangle$.

Since $|(G, A)| \geq 16$, we may moreover choose $t, u \in G \smallsetminus A$ such that $|\langle x, y, z, w\rangle| = 16$ with $(t, A) = \langle z\rangle$ and $(u, A) = \langle w\rangle$. By the first claim, $(su, t) \in (su, A)(t, A) = \langle yw, z\rangle$, so there is an $e \in A$ such that $(su, te) = (su, t)(su, e) \in \langle z\rangle$. We replace t by te and henceforth assume that $(su, t) \in \langle z\rangle$. Let now $a, b \in A$ such that $(t, b) = z$ and $(su, ba) = wy$. For

$c, d \in A$, we then have

$$\begin{aligned}\sigma := [[cs, du], [at, b]] &= [(1 + (cs, du))ducs, (1 + (at, b))bat] \\ &= (1 + (cs, du))(1 + (at, b))[ducs, bat] \\ &= (1 + (cs, du))(1 + z)(1 + (ducs, bat))batducs \\ &= (1 + (cs, du))(1 + z)(1 + \underbrace{(ducs, ba)}_{=wy}\underbrace{(ducs, t)}_{\in\langle z\rangle})batducs \\ &= (1 + (cs, du))(1 + z)(1 + wy)batducs,\end{aligned}$$

and

$$\begin{aligned}0 = [r, \sigma] =&(1 + (cs, du))(1 + z)(1 + wy)(1 + (r, batducs))batducsr \\ =&(1 + (u, c)(s, d)(s, u))(1 + z)(1 + wy)(1 + (r, batsu)(r, dc))batducsr.\end{aligned}$$

This implies $|E_{c,d}| < 16$ with $E_{c,d} := \langle z, wy, (u, c)(s, d)(s, u), (r, batsu)(r, dc)\rangle$ for all $c, d \in A$ by 1.12. Now $(s, u) \in \langle w, y\rangle$, so we have $(s, u) \equiv 1$ or $(s, u) \equiv w \pmod{\langle wy, z\rangle}$. Furthermore, $(r, batsu) = (r, ab)(r, stu) \in \langle x, wyz\rangle$, hence $(r, batsu) \equiv 1$ or $(r, batsu) \equiv x \pmod{\langle wy, z\rangle}$. Consider the following cases (all congruences modulo $\langle wy, z\rangle$):

Case 1: $(s, u) \equiv 1$ and $(r, batsu) \equiv 1$. Set $c := 1$ and choose $d \in A \smallsetminus (\mathcal{C}_A(s) \cup \mathcal{C}_A(r)) \neq \emptyset$, then $E_{c,d} = \langle z, wy, y, x\rangle$.

Case 2: $(s, u) \equiv 1$ and $(r, batsu) \equiv x$. Set $c := 1$ and choose $d \in \mathcal{C}_A(r) \smallsetminus \mathcal{C}_A(s) \neq \emptyset$, then $E_{c,d} = \langle z, wy, y, x\rangle$.

Case 3: $(s, u) \equiv w$ and $(r, batsu) \equiv 1$. Choose $c \in A \smallsetminus (\mathcal{C}_A(u) \cup \mathcal{C}_A(r)) \neq \emptyset$ and $d \in \mathcal{C}_A(r) \smallsetminus \mathcal{C}_A(s) \neq \emptyset$, then $E_{c,d} = \langle z, wy, w^2y, x\rangle$.

Case 4: $(s, u) \equiv w$ and $(r, batsu) \equiv x$. Set $c = d = 1$, then $E_{c,d} = \langle z, wy, w, x\rangle$.

In any case we obtain $E_{c,d} = \langle x, y, z, w\rangle$, which leads to the contradiction $|E_{c,d}| = 16$. This shows that our additional assumption at the beginning of the proof was wrong, so there is an element $s \in G$ such that $|(s, A)| \geq 4$.

Assume next that there is an element $s \in G$ such that even $|(s, A)| \geq 16$. Then since $|G : A| \geq 4$, there is a residue class tA (with $t \in G$) distinct from both sA and A.

If there is an element $c \in A$ with $1 \neq (s, c) \neq (t, c) \neq 1$, there are $a, b \in A$ with $|\langle (s, a), (s, b), (s, c), (t, c)\rangle| = 16$ (because of $|(s, A)| \geq 16$). Then $(s, c) = (s, sc)$, and $(sc, b) = (s, b)$, and 3.2 imply that

$$\sigma := (1 + (s, a))(1 + (s, b))(1 + (s, c))s \cdot sc = [(1 + (s, a))s, (1 + (sc, b))sc] \in (\mathbb{F}G)'',$$

and

$$\begin{aligned}[\mathbb{F}G, (\mathbb{F}G)''] \ni [t, \sigma] &= s^2(1 + (s, a))(1 + (s, b))(1 + (s, c))[t, c] \\ &= s^2(1 + (s, a))(1 + (s, b))(1 + (s, c))(1 + (t, c))ct \neq 0,\end{aligned}$$

contradiction.

Therefore, we may assume that

$$(*) \qquad \forall a \in A, t \in G \smallsetminus (A \cup sA)\colon\ (s, a) \neq 1 \neq (t, a) \implies (s, a) = (t, a).$$

Let $t \in G \setminus (A \cup sA)$, $a \in A \setminus (\mathcal{C}_A(s) \cup \mathcal{C}_A(t))$, then $1 \neq (s,a) = (t,a)$ by $(*)$. Set $B_a := \{b \in A\colon\ (s,b) \notin \langle (s,a) \rangle\} \neq \emptyset$.

If there is a $b \in B_a$ with $(t,b) = 1$, then $st \in G \setminus (A \cup sA)$ and $(st,ab) = (s,a)(t,a)(s,b) = (s,a)^2(s,b) \neq 1$ and $(s,ab) = (s,a)(s,b) \neq 1$, but $(s,ab) \neq (s,ab)(t,a) = (s,ab)(t,ab) = (st,ab)$ in contradiction to $(*)$. Consequently $(t,b) \neq 1$, i.e. $(t,b) = (s,b)$, for all $b \in B_a$.

Let now $\tilde{a} \in A$ with $1 \neq (s,\tilde{a}) \neq (s,a)$, then $a \in B_{\tilde{a}}$ and $\tilde{a} \in B_a$; in fact $A \setminus \mathcal{C}_A(s) = B_a \cup B_{\tilde{a}}$. Much as above it follows that $(t,b) = (s,b)$ for all $b \in B_{\tilde{a}}$. Together we obtain $(t,b) = (s,b)$ for all $b \in A \setminus \mathcal{C}_A(s)$. But then also $|(t,A)| \geq 16$, so by symmetry, we find that $(t,b) = (s,b)$ for all $b \in A \setminus \mathcal{C}_A(t)$. It follows that $(t,b) = (s,b)$ for all $b \in A$, hence $(st^{-1}, b) = 1$ for all $b \in A$, so $st^{-1} \in \mathcal{C}_G(A) = A$, in contradiction to $tA \neq sA$.

This shows that $|(s,A)| \leq 8$ for all $s \in G$, and there does exist an $s \in G$ with $|(s,A)| \geq 4$. With similar methods as earlier in the proof, we obtain an element $t \in G$ with $(t,A) \nsubseteq (s,A) < (G,A) = G'$, an element $b \in A$ with $y := (s,b) \neq 1$, $z := (t,b) \notin (s,A)$, and an element $a \in A$ with $x := (s,a) \notin \langle y \rangle$; in short: $|\langle x,y,z \rangle| = 8$.

Let $d \in A$ be arbitrary, and consider

$$\sigma := (1+x)(1+z)(1+y)ds \cdot b = [(1+x)ds, (1+z)b] \in [(1+x)S_x, (1+z)S_z] \subseteq (\mathbb{F}G)''.$$

Let now $r \in G$ with $(r,A) \nsubseteq \langle x,y,z \rangle$, then

$$0 = [r,\sigma] = (1+x)(1+z)(1+y)(1+(r,dsb))dsbr = (1+x)(1+z)(1+y)(1+(r,d)(r,sb))dsbr.$$

This implies $(r,sb) \in (r,d)\,\langle x,y,z \rangle$ for all $d \in A$, but $\bigcap_{d \in A} (r,d)\,\langle x,y,z \rangle = \emptyset$.

This rather innocent contradiction finishes our lengthy proof.

3.11. Theorem (summary): *Let G be a group of class 2. Then $\mathbb{F}G$ is centre-by-metabelian, if and only if one of the following statements holds:*

(i) $G' \cong Z_4$,
(ii) $\exp(G') = 2$ *and* $|G'| \leq 8$,
(iii) G has an abelian subgroup A of index 2.

Remark: Note that both 1.7 and 3.5 imply that $\exp(G') = 2$ also in case (iii).

4. Elementary abelian commutator subgroups

4.1. Lemma: *Let E be a normal subgroup of exponent 2 of the group G, and suppose that $\mathbb{F}G$ is centre-by-metabelian. If we set $C := \mathcal{C}_G(E)$, then:*

(i) The element orders in G/C are 1, 2, 3, or 4.
(ii) If $aC \in G/C$ has order 3, then $E = (a, E) \times \mathcal{C}_E(a)$, and $|(a, E)| = 4$.
(iii) There is no subgroup of order 9 in G/C.
(iv) If G/C is abelian, then $|G/C| = 3$, or $\exp(G/C) \mid 4$.

Proof: We consider E as an $\mathbb{F}_2[G]$-module, and write the action of $\mathbb{F}_2[G]$ on E as exponentiation from the left, in order to distinguish it from addition and multiplication in $\mathbb{F}G$.

(i) Let $x \in E$, $a \in G$. Then $(a, x) = {}^{a}xx = {}^{(1+a)}x = (x, a)$, and

$$\begin{aligned}
[[x, a], [x, a^2]] &= [(1 + {}^{(1+a)}x)xa, (1 + {}^{(1+a^2)}x)xa^2] \\
&= (1 + {}^{(1+a)}x)(1 + {}^{(a+a^3)}x)\, {}^{a}xxa^3 + (1 + {}^{(1+a^2)}x)(1 + {}^{(a^2+a^3)}x)x\, {}^{a^2}xa^3 \\
&= \Big((1 + {}^{(1+a)}x)(1 + {}^{(a+a^3)}x)\, {}^{(1+a)}x + (1 + {}^{(1+a^2)}x)(1 + {}^{(a^2+a^3)}x)\, {}^{(1+a^2)}x\Big)\, a^3 \\
&= \Big({}^{(1+a)}x + 1 + {}^{(1+a^3)}x + {}^{(a+a^3)}x + {}^{(1+a^2)}x + 1 + {}^{(1+a^3)}x + {}^{(a^2+a^3)}x\Big)\, a^3 \\
&= \Big({}^{(1+a)}x + {}^{(a+a^3)}x + {}^{(1+a^2)}x + {}^{(a^2+a^3)}x\Big)\, a^3 \\
&= \Big(1 + {}^{(1+a^3)}x + {}^{(a+a^2)}x + {}^{(1+a+a^2+a^3)}x\Big)\, {}^{(1+a)}xa^3 \\
&= (1 + {}^{(a+a^2)}x)(1 + {}^{(1+a^3)}x)\, {}^{(1+a)}xa^3.
\end{aligned}$$

Furthermore,

$$0 = [a, [x, a], [x, a^2]] = (1 + {}^{(a^2+a^3)}x)(1 + {}^{(a+a^4)}x)\, {}^{(a+a^2)}xa^4 + (1 + {}^{(a+a^2)}x)(1 + {}^{(1+a^3)}x)\, {}^{(1+a)}xa^4.$$

Multiplication by $\big((a^{-4})\, {}^{(1+a)}x\big)$ from the right and expansion of the parentheses yields

$$0 = 1 + {}^{(a+a^2)}x + {}^{(1+a+a^2+a^3)}x + {}^{(1+a^2)}x + {}^{(1+a+a^2+a^4)}x + {}^{(1+a+a^3+a^4)}x.$$

Consider the following cases:

- If $1 = {}^{(a+a^2)}x$, then $x = {}^{a}x$.
- If $1 = {}^{(1+a+a^2+a^3)}x$, then ${}^{a^3}x = {}^{(1+a+a^2)}x$, i.e. ${}^{a^4}x = {}^{(a+a^2+a^3)}x = {}^{(a+a^2+1+a+a^2)}x = x$.
- If $1 = {}^{(1+a^2)}x$, then $x = {}^{a^2}x$.
- If $1 = {}^{(1+a+a^2+a^4)}x$, then ${}^{a^4}x = {}^{(1+a+a^2)}x$. The remaining terms in the sum above yield $0 = {}^{(a+a^2)}x + {}^{(1+a+a^2+a^3)}x + {}^{(1+a^2)}x + {}^{(1+a+a^3+a^4)}x = {}^{(a+a^2)}x + {}^{(1+a+a^2+a^3)}x + {}^{(1+a^2)}x + {}^{(a^3+a^2)}x$. Multiply by ${}^{(a+a^2)}x$, and obtain $0 = 1 + {}^{(1+a^3)}x + {}^{(1+a)}x + {}^{(a^3+a)}x$. Then $x \in \{{}^{a^3}x, {}^{a}x, {}^{a^2}x\}$.

- If $1 = {}^{(1+a+a^3+a^4)}x$, then ${}^{a^4}x = {}^{(1+a+a^3)}x$. Furthermore, $0 = {}^{(a+a^2)}x + {}^{(1+a+a^2+a^3)}x + {}^{(1+a^2)}x + {}^{(1+a+a^2+a^4)}x = {}^{(a+a^2)}x + {}^{(1+a+a^2+a^3)}x + {}^{(1+a^2)}x + {}^{(a^2+a^3)}x$, which is equivalent to $0 = 1 + {}^{(1+a^3)}x + {}^{(1+a)}x + {}^{(a+a^3)}x$. This implies that again $x \in \{ {}^{a^3}x, {}^{a}x, {}^{a^2}x \}$.

In any case, we have $x \in \{ {}^{a}x, {}^{a^2}x, {}^{a^3}x, {}^{a^4}x \}$.

Hence the length of any orbit in E under a is at most 4. If all orbits have length 1, 2, or 4, then $a^4 \in C$, and $|\langle aC \rangle| \mid 4$, and we are done. If all orbits have length 1 or 3, then $a^3 \in C$, and $|\langle aC \rangle| \mid 3$, and we are done as well.

So assume that there are elements $x, y \in E$ such that x has orbit length 2 or 4, and y has orbit length 3. Then ${}^{a^4}(xy) = {}^{a^4}x \cdot {}^{a^4}y = x \cdot {}^{a^4}y \neq xy$, and ${}^{a^3}(xy) = {}^{a^3}x \cdot y \neq xy$, contradiction.

(ii) We consider E as an $\mathbb{F}_2[\langle aC \rangle]$-module. By Maschke [**5**, Satz I.17.7], E is semisimple and thus decomposes into a direct sum of simple modules. There are two nonisomorphic simple $\mathbb{F}_2[\langle aC \rangle]$-modules: the trivial module of dimension 1, and a module of dimension 2, on which $\langle aC \rangle$ acts by cyclic permutation of the three nontrivial elements.

Assumption: There are two distinct nontrivial simple submodules V, W contained in E. Then $\dim V = \dim W = 2$, and we may write $V = \langle x, y \rangle$, $W = \langle z, w \rangle$ such that ${}^{a}x = y$, ${}^{a}y = xy$, ${}^{a}z = w$, ${}^{a}w = wz$. Then

$$\begin{aligned}
[[x,a],[z,a]] &= [(1+(a,x))xa, (1+(a,z))za] = [(1+xy)xa, (1+wz)za] \\
&= (1+xy)(1+z)xwa^2 + (1+wz)(1+x)zya^2 \\
&= \underbrace{(xw + xwz + wyz + yz + xyz + xyw)}_{=:\sigma} a^2,
\end{aligned}$$

and

$$0 = [x, \sigma a^2]a^{-2}x = \sigma[x, a^2]a^{-2}x = \sigma(1 + (x, a^2)) = \sigma(1+y) = z(1+w)(1+x)(1+y) \neq 0,$$

contradiction.

This shows that there is at most one nontrivial simple submodule of E. On the other hand, there is at least one nontrivial simple submodule V of E, for otherwise the action of $\langle aC \rangle$ on E would be trivial. Then $E = V \oplus \mathcal{C}_E(a)$, and $(a, E) = (a, V) = V$ has dimension 2, i.e. order 4.

(iii) Suppose that U is a subgroup of order 9 in G/C. Since G/C does not contain elements of order 9 by (i), U is elementary abelian.

We consider E as $\mathbb{F}_2[U]$-module. Again, we may write E as a sum of simple submodules. By [**3**, theorem 3.2.2], none of these simple modules is faithful[†], since U is abelian but noncyclic. At least one of the simple submodules is nontrivial, say V. The kernel of V in U must then have order 3, so we write $\mathcal{C}_U(V) = \langle bC \rangle$. Take an element $a \in G$ such that $U = \langle aC, bC \rangle$. Then aC acts nontrivially on V. By (ii), aC acts trivially on all simple submodules $W \neq V$ of E.

[†] in the sense that the corresponding linear representation of U is faithful

On the other hand, bC acts nontrivially on E, i.e. nontrivially on some simple submodule $W \neq V$ of E. But then abC is an element of order 3 in G/C which acts nontrivially on both components of $V \oplus W$. This contradicts (ii).

(iv) By (i), the element orders in G/C are bounded by 4. If G/C contains no element of order 3, then $\exp(G/C) \in \{1, 2, 4\}$.

So suppose G/C does contain an element of order 3. If it also contains an element of order 2, then there also is an element of order 6 since G/C is abelian, contradiction. Hence G/C is an elementary abelian 3-group. Since there may not be a subgroup of order 9 by (iii), G/C must have order 3.

4.2. Remark: Let G be a group with elementary abelian commutator subgroup G' of order 8. Let us suppose that $\mathrm{cl}(G) > 2$, i.e. $C := \mathcal{C}_G(G') < G$. Since $G' \subseteq C$, G/C is a nontrivial abelian group. Now G' is a 3-dimensional $\mathbb{F}_2$-vector space, so let us choose a basis x, y, z. The faithful action of G/C on G' then produces a faithful representation $G/C \to \mathrm{GL}(3,2)$, whose image is an abelian subgroup of $\mathrm{GL}(3,2)$, i.e. conjugate to one of the following (cf. [**18**]):

$$\begin{aligned}
R &:= \left\langle \left(\begin{smallmatrix} 0&0&1\\1&0&0\\0&1&0 \end{smallmatrix}\right) \right\rangle \cong Z_3, &
S &:= \left\langle \left(\begin{smallmatrix} 0&0&1\\1&0&0\\0&1&1 \end{smallmatrix}\right) \right\rangle \cong Z_7,\\
T &:= \left\langle \left(\begin{smallmatrix} 0&1&0\\1&0&0\\0&0&1 \end{smallmatrix}\right) \right\rangle \cong Z_2, &
U &:= \left\langle \left(\begin{smallmatrix} 0&1&1\\1&1&1\\1&1&0 \end{smallmatrix}\right) \right\rangle \cong Z_4,\\
V &:= \left\langle \left(\begin{smallmatrix} 0&0&1\\0&1&0\\1&0&0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0&0&1\\1&1&1\\1&0&0 \end{smallmatrix}\right) \right\rangle \cong Z_2 \times Z_2, &
W &:= \left\langle \left(\begin{smallmatrix} 0&0&1\\0&1&0\\1&0&0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0&1&1\\0&1&0\\1&1&0 \end{smallmatrix}\right) \right\rangle \cong Z_2 \times Z_2.
\end{aligned}$$

(In fact, we may choose x, y, z in such a way that the image actually is one of these groups.)

In any of these cases, $\mathbb{F}G$ is not centre-by-metabelian. This is clear by 4.1 in the case that G/C is mapped onto S. The other cases are handled by the following lemmata.

4.3. Lemma: *Let the notation be as in 4.2, and assume that G/C is mapped onto R. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We assume that $\mathbb{F}G$ is centre-by-metabelian, and construct a contradiction.

We write $G/C = \langle aC \rangle$. The action of a on G' is given by 4.2 as the cyclic permutation of x, y, z. This yields $(a, x) = xy$, $(a, y) = yz$, $(a, z) = xz$. Then $\langle xy, yz \rangle = (a, G') = (G, G') = \gamma_3(G) = \gamma_4(G) = \ldots$, and $G' \cap \mathcal{Z}(G) = \mathcal{C}_{G'}(a) = \langle xyz \rangle$.

For all $c, d \in C$, we then have

$$\begin{aligned}
(\mathbb{F}G)'' \ni [x + {}^a x, ca + {}^d(ca)] &= [x + y, (1 + (d, ca))ca]\\
&= (1 + (d, ca))c[x + y, a]\\
&= (1 + (d, ca))c(x + y + y + z)a,
\end{aligned}$$

and

$$\begin{aligned}
0 &= [a, x + {}^a x, ca + {}^d(ca)]\\
&= (1 + (d, ca))(x + z)ca^2 + (1 + {}^a(d, ca))(y + x)aca \qquad (*)\\
&= (1 + (ca, d))(1 + xz)xca^2 + (1 + {}^a(ca, d))(1 + xy)x(a, c)ca^2.
\end{aligned}$$

In particular, we obtain for $c = 1$ after multiplication with $(xca^2)^{-1}$ from the right:

$$\begin{aligned} 0 &= (1 + (a,d))(1 + xz) + (1 + {}^{a}(a,d))(1 + xy) \\ &= (a,d) + xz + (a,d)xz + {}^{a}(a,d) + xy + {}^{a}(a,d)xy. \end{aligned}$$

If $(a,d) \notin \langle xy, yz\rangle \trianglelefteq G$, then the projection of the last sum onto $\mathbb{F}[\langle xy, yz\rangle]$ w.r.t. the vector space decomposition $\mathbb{F}G = \bigoplus_{g \in G} \mathbb{F}g$ is $xz + xy \neq 0$, contradiction. This shows that $(a,d) \in \langle xy, yz\rangle$ for all $d \in C$, i.e. $(a,C) = (a^2,C) \subseteq \langle xy, yz\rangle$.

By 1.6, $(a,C)C' = G' \nsubseteq \langle xy, yz\rangle$, and by 1.3, $C' \subseteq \mathcal{Z}(G) \cap G' = \langle xyz\rangle$. Consequently $C' = \langle xyz\rangle$. Let $c, d \in C$ with $(c,d) = xyz$. Then $(*)$ yields

$$0 = (1 + xyz(a,d))(1 + xz) + (1 + xyz\,{}^{a}(a,d))(1 + xy)(a,c),$$

but the projection of the right hand side onto $\mathbb{F}[\langle xy, yz\rangle]$ is $(1 + xz) + (1 + xy)(a,c) = 1 + xz + (a,c) + xy(a,c)$, which cannot vanish for $(a,c) \in \langle xy, yz\rangle = \{1, xy, yz, xz\}$.

4.4. Lemma: *Let the notation be as in 4.2, and assume that G/C is mapped onto U. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: By way of contradiction, assume that $\mathbb{F}G$ is centre-by-metabelian.

If we write $G/C = \langle aC\rangle$, we obtain ${}^{a}x = yz$, ${}^{a}y = xyz$, ${}^{a}z = xy$. The orbits of this action are $1 \mapsto 1$, $x \mapsto yz \mapsto z \mapsto xy \mapsto x$, $y \mapsto xyz \mapsto y$, $xz \mapsto xz$. The lower central series of G is $G \trianglerighteq \langle x,y,z\rangle \trianglerighteq \langle y, xz\rangle \trianglerighteq \langle xz\rangle \trianglerighteq 1$. By 1.3, we have $C' \subseteq G' \cap \mathcal{Z}(G) = \langle xz\rangle$. It suffices to show that $(a,C) \subseteq \langle y, xz\rangle$, since by 1.6, we then obtain the contradiction $G' = (a,C)C' \subseteq \langle y, xz\rangle$.

So let $c \in C$. We want to show that $(a,c) \in \langle y, xz\rangle$. Observe that ${}^{a}g \equiv g \pmod{\langle y, xz\rangle}$ for all $g \in G'$. Then

$$\begin{aligned} \alpha := [[a,x],[a,c]] &= [(1 + (a,x))xa, (1 + (a,c))ca] = [(1 + xyz)xa, (1 + (a,c))ca] \\ &= (1 + xyz)xa(1 + (a,c))ca + (1 + (a,c))ca(1 + xyz)xa \\ &= (1 + xyz)(1 + {}^{a}(a,c))x(a,c)ca^2 + (1 + (a,c))(1 + y)yzca^2. \end{aligned}$$

Since $\mathbb{F}G$ is centre-by-metabelian, we have

$$\begin{aligned} 0 = [a,\alpha] &= a(1 + xyz)(1 + {}^{a}(a,c))x(a,c)ca^2 + a(1 + (a,c))(1 + y)yzca^2 \\ &\qquad + (1 + xyz)(1 + {}^{a}(a,c))x(a,c)ca^3 + (1 + (a,c))(1 + y)yzca^3 \\ &= (1 + y)(1 + {}^{a^2}(a,c))yz\,\underbrace{{}^{a}(a,c)(a,c)}_{=(a^2,c)}\,ca^3 + (1 + {}^{a}(a,c))(1 + xyz)z(a,c)ca^3 \\ &\qquad + (1 + xyz)(1 + {}^{a}(a,c))x(a,c)ca^3 + (1 + (a,c))(1 + y)yzca^3 \\ &= \underbrace{(1 + y)y}_{=1+y}\,z\left((1 + {}^{a^2}(a,c))(a^2,c) + 1 + (a,c)\right)ca^3 \\ &\qquad + (1 + \underbrace{xyz}_{\equiv y \pmod{\langle xz\rangle}})(1 + {}^{a}(a,c))\,\underbrace{(x + z)}_{=(1+xz)z}\,(a,c)ca^3 \end{aligned}$$

$$\begin{aligned}
&= z(1+y)\big((a^2,c)+(a^3,c)+1+(a,c)+(1+\underbrace{{}^{a}(a,c)}_{\equiv(a,c)\pmod{\langle y,xz\rangle}})(1+xz)(a,c)\big)ca^3\\
&= z(1+y)\,\big((a^3,c)+(a^2,c)+(1+(a,c))xz\big)\,ca^3
\end{aligned}$$

Suppose $(a,c)=x$. Then $(a^2,c)={}^{a}(a,c)(a,c)={}^{a}xx=yzx\equiv xz\pmod{\langle y\rangle}$, and $(a^3,c)={}^{a^2}(a,c)(a^2,c)\equiv{}^{a^2}x\cdot xz=zxz=x\pmod{\langle y\rangle}$, hence $0=[a,\alpha]=(1+y)(x+xz+(1+x)xz)=(1+y)(x+z)\neq 0$, contradiction. This shows $(a,c)\neq x$.

In a similar manner we dismiss the cases $(a,c)=z$, $(a,c)=xy$, and $(a,c)=yz$. Then $(a,c)\in\langle x,y,z\rangle\smallsetminus\{x,z,xy,yz\}=\langle y,xz\rangle$, and we are done.

4.5. Lemma: *Let the notation be as in 4.2, and assume that G/C is mapped onto V. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We assume that $\mathbb{F}G$ is centre-by-metabelian, and construct a contradiction.

We write $G/C=\langle aC,bC\rangle$ with $a,b\in G$ such that

$$\begin{aligned}
{}^{a}x&=z, & {}^{a}y&=y, & {}^{a}z&=x,\\
{}^{b}x&=yz, & {}^{b}y&=y, & {}^{b}z&=xy.
\end{aligned}$$

Then $\mathcal{C}_{G'}(a)=\mathcal{C}_{G'}(b)=G'\cap\mathcal{Z}(G)=\langle y,xz\rangle$, and the lower central series of G is $G\trianglerighteq\langle x,y,z\rangle\trianglerighteq\langle y,xz\rangle\trianglerighteq 1$. Hence G has class 3.

Let $g,h\in G$. Then $(g^2h,hg)={}^{g^2}(h,hg)(g^2,hg)=(hg,h)(g^2,h)={}^{h}(g,h)\,{}^{g}(g,h)(g,h)$, and thus

$$\begin{aligned}
[[g,h],[g,gh]]&=[(1+(g,h))hg,(1+(g,gh))g^2h]=[(1+(g,h))hg,(1+{}^{g}(g,h))g^2h]\\
&=(1+(g,h))(1+{}^{h}(g,h))hg\cdot g^2h+(1+{}^{g}(g,h))(1+{}^{h}(g,h))g^2h\cdot hg\\
&=(1+{}^{h}(g,h))\,\Big((1+(g,h))+(1+{}^{g}(g,h))\,{}^{h}(g,h)\,{}^{g}(g,h)(g,h)\Big)\,hg^3h\\
&=(1+{}^{h}(g,h))\,(1+(g,h)+(1+{}^{g}(g,h))(g,h))\,hg^3h\\
&=(1+{}^{h}(g,h))(1+{}^{g}(g,h)(g,h))hg^3h\\
&=(1+{}^{h}(g,h))(1+(g,g,h))hg^3h.
\end{aligned}$$

Now $(g,hg^3h)=(g,h)\,{}^{hg^3}(g,h)=(gh,g,h)=(g,g,h)(h,g,h)$, since $(g,g,h),(h,g,h)\in\mathcal{Z}(G)$, and using 1.12, we compute

$$\begin{aligned}
0&=[g,[g,h],[g,gh]]=(1+(g,g,h))[g,(1+{}^{h}(g,h))hg^3h]\\
&=(1+(g,g,h))\,\Big((1+{}^{h}(g,h))+(1+{}^{gh}(g,h))(h,g,h)\Big)\,hg^3hg\\
(*)\qquad&=(1+(g,g,h))\,\Big(1+{}^{h}(g,h)+(h,g,h)+(gh,g,h)(g,h)(h,g,h)\Big)\,hg^3hg\\
&=(1+(g,g,h))\,\Big(1+{}^{h}(g,h)+{}^{h}(g,h)(g,h)+(g,h)\Big)\,hg^3hg\\
&=(1+(g,g,h))(1+{}^{h}(g,h))(1+(g,h))hg^3hg\\
&=(1+(g,g,h))(1+(h,g,h))(1+(g,h))g^4h^2.
\end{aligned}$$

Let us assume that there exists an element $c\in C$ such that $(a,bc)\notin\mathcal{Z}(G)$. Then $(a,a,bc)=xz$ and $(bc,a,bc)=xyz$. If we substitute $g:=a$ and $h:=bc$ into $(*)$, we obtain the contradiction $0 = (1+(a,a,bc))(1+(bc,a,bc))(1+(a,bc)) = (1+xz)(1+xyz)(1+(a,bc)) = (G' \cap \mathcal{Z}(G))^{+}(1+(a,bc)) \neq 0$.

Consequently $(a,bc) \in \mathcal{Z}(G)$ for all $c \in C$; in particular $(a,b), (a,b^{-1}) \in \mathcal{Z}(G)$ since $bC = b^{-1}C$. It follows that $(a,c) = (a,b^{-1}bc) = (a,b^{-1})(a,bc) \in \mathcal{Z}(G)$ for all $c \in C$, and similarly $(a,ac), (a,abc) \in \mathcal{Z}(G)$. Since $G = C \cup aC \cup bC \cup abC$, we find that $(a,G) \subseteq \mathcal{Z}(G)$. But then $(a,g^{-1},h) = (a,g^{-1},h) \cdot 1 \cdot 1 = (a,g^{-1},h)(g,h^{-1},a)(h,a^{-1},g) = 1$ for all $g,h \in G$ by Witt's identity (1.2, recall that G has class 3), which shows that a acts trivially on G', contradiction.

4.6. Lemma: *Suppose that G is a group of class at most 3 such that G' and $G/\mathcal{C}_G(G')$ both have exponent 2, and $|\gamma_3(G)| \leq 2$. If $\mathbb{F}G$ is centre-by-metabelian, then*

$$|\langle (g,h),\ {}^{g}(g,h),\ (g,k)\rangle| \leq 4$$

for all $g,h,k \in G$.

Proof: Let $f,g,h,i,j,k \in G$. Observe that then $(1+(f,g,h))(i,j,k) = (1+(f,g,h))$ and thus $(1+(f,g,h))\,{}^{k}(i,j) = (1+(f,g,h))(i,j)$. Moreover,

$$\begin{aligned}
[g + {}^{k}g, h + {}^{g}h] &= [(1+(g,k))g, (1+(g,h))h] \\
&= (1+(g,k))(1+{}^{g}(g,h))gh + (1+(g,h))(1+{}^{h}(g,k))(g,h)gh \\
&= \underbrace{\Big((1+(g,k))(1+{}^{g}(g,h)) + (1+(g,h))(1+{}^{h}(g,k))\Big)}_{=:\sigma} gh.
\end{aligned}$$

Hence

$$\begin{aligned}
0 &= [g, g + {}^{k}g, h + {}^{g}h] \\
&= \sigma \cdot gh \cdot g + {}^{g}\sigma \cdot g \cdot gh = (\sigma(gh,g) + {}^{g}\sigma)g^2h = (\sigma\,{}^{g}(g,h) + {}^{g}\sigma)g^2h \\
&= (1+{}^{g}(g,h))\Big((1+(g,k))\,{}^{g}(g,h) + (1+{}^{gh}(g,k))\Big)g^2h \\
&\quad + (1+(g,h))\Big((1+{}^{h}(g,k))\,{}^{g}(g,h) + (1+{}^{g}(g,k))\Big)g^2h \\
&= (1+{}^{g}(g,h))((g,k) + {}^{gh}(g,k))g^2h \\
&\quad + (1+(g,h))((1+{}^{h}(g,k))\,{}^{g}(g,h)(g,h) + 1 + {}^{g}(g,k))g^2h \\
&= (1+{}^{g}(g,h))(1+{}^{gh}(g,k)(g,k))(g,k)g^2h \\
&\quad + (1+(g,h))((1+{}^{h}(g,k))(g,g,h) + 1 + {}^{g}(g,k))g^2h \\
&= (1+(g,h))(1+(gh,g,k))(g,k)g^2h \\
&\quad + (1+(g,h))((1+{}^{h}(g,k))(g,g,h) + 1 + {}^{g}(g,k))g^2h \\
&= (1+(g,h))\Big((1+(gh,g,k))\,{}^{g}(g,k) + (1+{}^{h}(g,k))(g,g,h) + 1 + {}^{g}(g,k)\Big)g^2h \\
&= (1+(g,h))\Big((g,g,k)(h,g,k)\,{}^{g}(g,k) + {}^{g}(g,h) + {}^{h}(g,k)\,{}^{g}(g,h) + 1\Big)g^2h \\
&= (1+(g,h))\Big((g,k)(h,g,k) + {}^{g}(g,h) + {}^{h}(g,k)\,{}^{g}(g,h) + 1\Big)g^2h
\end{aligned}$$

$$\begin{aligned}
&= (1 + (g,h)) \left({}^{h}(g,k) + {}^{g}(g,h) + {}^{h}(g,k)\, {}^{g}(g,h) + 1 \right) g^2 h \\
&= (1 + (g,h))(1 + {}^{g}(g,h))(1 + {}^{h}(g,k)) g^2 h \\
&= (1 + (g,h))(1 + {}^{g}(g,h))(1 + (g,k)) g^2 h.
\end{aligned}$$

The claim now follows from 1.12.

4.7. Lemma: *Let the notation be as in 4.2, and assume that G/C is mapped onto W. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Assume that $\mathbb{F}G$ is a counterexample.

We write $G/C = \langle aC, bC \rangle$ with $a, b \in G$ such that

$$\begin{aligned}
{}^{a}x &= z, \quad & {}^{a}y &= y, \quad & {}^{a}z &= x, \\
{}^{b}x &= z, \quad & {}^{b}y &= xyz, \quad & {}^{b}z &= x.
\end{aligned}$$

Then $\mathcal{C}_{G'}(a) = \langle y, xz \rangle$, $\mathcal{C}_{G'}(b) = \langle xy, yz \rangle$, and $G' \cap \mathcal{Z}(G) = \langle xz \rangle$. The lower central series of G is $G \trianglerighteq \langle x, y, z \rangle \trianglerighteq \langle xz \rangle \trianglerighteq 1$. By 4.6,

$$(*) \qquad |\langle (g,h),\, {}^{g}(g,h), (g,c) \rangle| \leq 4.$$

for all $g, h \in G$, $c \in C$.

Note that by 1.6,

$$(**) \qquad \begin{aligned}
G' &= \langle (a,b) \rangle\, (a,C)(b,C)C' \\
&= \langle (a,ab) \rangle\, (a,C)(ab,C)C' \\
&= \langle (ab,b) \rangle\, (ab,C)(b,C)C'.
\end{aligned}$$

By 1.3, $C' \subseteq G' \cap \mathcal{Z}(G) = \langle xz \rangle$. We want to show now that $(a,b) \in \langle xz \rangle$:

Assumption: $(a,b) \in \{x, z\}$. Then $4 \geq |\langle (a,b),\, {}^{a}(a,b), (a,c) \rangle| = |\langle x, z, (a,c) \rangle|$, and $4 \geq \left|\left\langle (b,a),\, {}^{b}(b,a), (b,c) \right\rangle\right| = |\langle x, z, (b,c) \rangle|$ by $(*)$. Therefore, $(a,b), (a,c), (b,c) \in \langle x, z \rangle$ for all $c \in C$. Together with $(**)$, this implies $G' \subseteq \langle x, z \rangle$, contradiction.

Assumption: $(a,b) \in \{xy, yz\}$. Then $4 \geq |\langle (a,b),\, {}^{a}(a,b), (a,c) \rangle| = |\langle xy, yz, (a,c) \rangle|$, and $4 \geq \left|\left\langle (ab,a),\, {}^{ab}(ab,a), (ab,c) \right\rangle\right| = \left|\left\langle (ab,a),\, {}^{ab}\!\left({}^{a}(b,a)\right), (ab,c) \right\rangle\right| = \left|\left\langle {}^{a}(b,a),\, {}^{b}(b,a), (ab,c) \right\rangle\right| = |\langle xy, yz, (b,c) \rangle|$. Similarly as above, this implies $G' \subseteq \langle xy, yz \rangle$, contradiction.

Assumption: $(a,b) \in \{y, xyz\}$. Then $4 \geq \left|\left\langle (b,a),\, {}^{b}(b,a), (b,c) \right\rangle\right| = |\langle y, xyz, (b,c) \rangle|$, and $4 \geq \left|\left\langle (ab,a),\, {}^{ab}(ab,a), (ab,c) \right\rangle\right| = \left|\left\langle {}^{a}(b,a),\, {}^{b}(b,a), (ab,c) \right\rangle\right| = |\langle y, xyz, (a,c) \rangle|$. This produces the contradiction $G' \subseteq \langle y, xyz \rangle$.

Hence $(a,b) \in \langle xz \rangle$, as desired. We want to show next that $(b,C) \subseteq \langle xz \rangle$. Let $d \in C$.

Assumption: $(b,d) \in \{x, z\}$. If $c \in C$, then $(d,c) \in \langle xz \rangle$, and $4 \geq |\langle (bd,b),\, {}^{bd}(bd,b), (bd,c) \rangle| = |\langle x, z, (b,c) \rangle|$, hence $(b,d) \in \langle x, z \rangle$. Moreover, $4 \geq \left|\left\langle (ad,b),\, {}^{ad}(ad,b), (ad,c) \right\rangle\right| = |\langle x, z, (a,c) \rangle|$, hence also $(a,c) \in \langle x, z \rangle$. We arrive at the already familiar contradiction $G' \subseteq \langle x, z \rangle$.

Assumption: $(b,d) \in \{xy, yz\}$. Then $4 \geq \left|\left\langle (ad,b),\, {}^{ad}(ad,b), (ad,d) \right\rangle\right| = |\langle {}^{a}(d,b)(a,b), (d,b)(a,b), (a,d) \rangle| = |\langle xy, yz, (a,d) \rangle|$, hence $(a,d) \in \langle xy, yz \rangle$. But then Witt's formula implies $xz = (a,b,d) = (b^{-1}, d^{-1}, a)(d, a^{-1}, b^{-1}) = (b, d^{-1}, a) = (b, a, d) = 1$, contradiction.

Assumption: $(b,d) \in \{y, xyz\}$. If $c \in C$, then $4 \geq \left|\left\langle (bd,b),\, {}^{bd}(bd,b), (bd,c)\right\rangle\right| = |\langle y,\, xyz,\, (b,c)\rangle|$, and $4 \geq \left|\left\langle (abd,b),\, {}^{abd}(abd,b), (abd,c)\right\rangle\right| = |\langle y, xyz, (ab,c)\rangle|$, hence $(b,c), (ab,c) \in \langle y, xyz\rangle$. This produces the contradiction $G' \subseteq \langle y, xyz\rangle$.

This shows that $(b,d) \in \langle xz\rangle = G' \cap \mathcal{Z}(G)$. Observe now that by Witt's formula, $1 = (b, a^{-1}, d)(a, d^{-1}, b)(d, b^{-1}, a) = (b, a^{-1}, d)$. Consequently $(a, C) = (a^{-1}, C) \subseteq \mathcal{C}_{G'}(b)$. But then $(**)$ implies that $G' \subseteq \mathcal{C}_{G'}(b)$, contradiction.

4.8. Lemma: *Let the notation be as in 4.2, and assume that G/C is mapped onto T. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Let G satisfy the prerequisites of the lemma. Then $|G/C| = 2$, i.e. $G/C = \langle aC\rangle$ for all $a \in G \setminus C$.

In a first step, we claim that there is an element $a \in G \setminus C$ such that $(a, C) = G'$.

We assume otherwise and pick an arbitrary element $a \in G \setminus C$. As usual, $G' = (a, C)C'$ with normal subgroups (a, C) and C' of G. Since $C' \subseteq \mathcal{Z}(G)$ and $G' \not\subseteq \mathcal{Z}(G)$, there is an element $c \in C$ such that ${}^{a}(a,c) \neq (a,c)$. Let $x := (a,c)$, $y := {}^{a}(a,c)$. Then $(a, C) = \langle x, y\rangle$ for order reasons. Furthermore, there must be elements $d, e \in C$ with $z := (d,e) \notin \langle x, y\rangle$. Then $G' = \langle x, y, z\rangle$, and $C' \subseteq G' \cap \mathcal{Z}(G) = \langle xy, z\rangle$.

Now consider (da, C). Similarly as above, it must be a proper subgroup of G' that is normal in G and nontrivially acted upon by G/C. Hence $(da, C) = \langle x, y\rangle$ or $(da, C) = \langle xz, yz\rangle$. Since $(da, e) = (d,e)(a,e) \in (d,e)(a,C) = z\,\langle x, y\rangle$, the case $(da, C) = \langle xz, yz\rangle$ must be the correct one. Because of $z = (d,e) = (ed, e)$, we may replace d by ed in this argumentation, and find that also $(eda, C) = \langle xz, yz\rangle$. But then $(eda, d) = z(da, d) \in (eda, C) \cap z(da, C) = \langle xz, yz\rangle \cap z\,\langle xz, yz\rangle = \emptyset$, contradiction.

We want to show next that $\mathbb{F}G$ is not centre-by-metabelian.

Again, assume otherwise and choose elements $a, x, y, z \in G$ such that $G/C = \langle aC\rangle$, $(a, C) = G' = \langle x, y, z\rangle$, and $axa^{-1} = y$, $aya^{-1} = x$, $aza^{-1} = z$.

The lower central series of G is $G \trianglerighteq \langle x, y, z\rangle \trianglerighteq \langle xy\rangle \trianglerighteq 1$, so lemma 4.6 applies here.

Since $(a, C) = G' \not\subseteq \mathcal{Z}(G)$, there is an element $c \in C$ with $|\langle (a,c),\, {}^{a}(a,c)\rangle| = 4$. On the other hand, 4.6 implies that $|\langle (a,c),\, {}^{a}(a,c), (a,d)\rangle| \leq 4$ for all $d \in C$. Together this shows that $|(a, C)| \leq 4$, in contradiction to $|(a, C)| = |G'| = 8$.

4.9. Theorem: *Let G be a group with elementary abelian commutator subgroup of order 8. If $\mathbb{F}G$ is centre-by-metabelian, then G has class 2.*

Proof: 4.2–4.8.

4.10. Lemma: *Let N be an elementary abelian normal subgroup of order 2^{n+1} ($n \in \mathbb{N}_0$) of a group G such that $N \cap \mathcal{Z}(G) = (G, N)$ has order 2. Write $N = \langle x_1, \ldots, x_n, z\rangle$ with $N \cap \mathcal{Z}(G) = \langle z\rangle$. Then $G/\mathcal{C}_G(N)$ is elementary abelian of order 2^n. More exactly, there are elements $a_1, \ldots, a_n \in G$ such that for all $i, j \in \{1, \ldots, n\}$,*

$$(a_i, x_j) = \begin{cases} 1 & \text{if } i \neq j \\ z & \text{if } i = j \end{cases}$$

Proof: The action of G by conjugation on the $\mathbb{F}_2$-vector space N w.r.t. the basis $x_1, \dots, x_n, z$ defines a matrix representation $\Delta\colon G \to \mathrm{GL}(n+1,2)$ with kernel $\mathcal{C}_G(N)$ and image

$$B \subseteq A := \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ * & \dots & * & 1 \end{pmatrix} \subseteq \mathrm{GL}(n+1,2).$$

The elementary abelian group A may be interpreted as an $\mathbb{F}_2$-vector space of dimension n with subspace B. So let us choose a basis $b_1, \dots, b_k$ of B with $k \leq n$.

Again shifting our point of view, we now interpret the elements b_i, $i = 1, \dots, k$, as $\mathbb{F}_2$-linear mappings $N \to N$, and compute $\dim \mathcal{C}_N(b_i) = \dim \mathrm{Ker}(b_i - \mathrm{id}_N) = \dim N - \mathrm{rk}(b_i - \mathrm{id}_N) = (n+1) - 1 = n$; i.e. $\mathcal{C}_N(b_i)$ is a hyperplane in N. Hence $1 = \dim \mathcal{C}_N(B) = \dim \bigcap_{i=1}^{k} \mathcal{C}_N(b_i) \geq (n+1) - k \geq 1$. This shows $k = n$, or equivalently $B = A$.

If we now choose preimages $a_1, a_2, \dots, a_n \in G$ under Δ of the matrices

$$\begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ 1\,0 & \dots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ 0\,1\,0 & \dots & 0 & 1 \end{pmatrix}, \dots, \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \\ 0 & \dots & 0\,1 & 1 \end{pmatrix} \in B,$$

respectively, we obtain the desired elements.

4.11. Lemma: *Let G be a group that is generated by three elements, with elementary abelian commutator subgroup G' of order 16, such that $(G, G') = G' \cap \mathcal{Z}(G)$ has order 2. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We assume that $\mathbb{F}G$ is centre-by-metabelian, and write $G = \langle g, h, k \rangle$ and $(G, G') = \langle z \rangle$. Note that G has class 3. Then $G/\langle z \rangle$ has class 2, hence its commutator subgroup is generated by the commutators of its own generators (cf. 3.1 (ii)), i.e. $G'/\langle z \rangle = \langle (g,h),\ (g,k),\ (h,k),\ z \rangle / \langle z \rangle$. Since $G'/\langle z \rangle$ has order 8, also $\langle (g,h),\ (g,k),\ (h,k) \rangle$ has order 8.

If we set $w := (g,h)$, $x := (g,k)$, $y := (h,k)$, we obtain $G' = \langle w, x, y, z \rangle$.

Assume that ${}^{g}w \neq w$. Then ${}^{g}w = wz$. So if ${}^{h}w \neq w$, then ${}^{hg}w = w$. Choose $\tilde{h} \in \{h, hg\}$ with ${}^{\tilde{h}}w = w$. Then

$$\begin{aligned} [g + {}^{h}g,\ \tilde{h} + {}^{g}\tilde{h}] &= [g + (h,g)g,\ \tilde{h} + (g,\tilde{h})\tilde{h}] \\ &= [(1+w)g,\ (1+w)\tilde{h}] \\ &= (1+w)[g,\ (1+w)\tilde{h}] \\ &= (1+w)\big((1+wz)g\tilde{h} + (1+w)\tilde{h}g\big) \\ &= (1+w)(1+z)g\tilde{h}. \end{aligned}$$

Observe that ${}^{k}w \equiv w \pmod{\langle z\rangle}$ and $(k, g\tilde{h}) \equiv (k,h) = y \pmod{\langle x, z\rangle}$. Then

$$\begin{aligned} 0 = (1+x)\cdot 0 &= (1+x)[k,\, g + {}^{h}g,\, \tilde{h} + {}^{g}\tilde{h}] \\ &= (1+x)[k,\, (1+w)(1+z)g\tilde{h}] \\ &= (1+x)(1+z)[k,\, (1+w)g\tilde{h}] \\ &= (1+x)(1+z)(1+w)[k, g\tilde{h}] \\ &= (1+x)(1+z)(1+w)(1+(k,g\tilde{h}))g\tilde{h}k \\ &= (1+x)(1+z)(1+w)(1+y)g\tilde{h}k \neq 0, \end{aligned}$$

contradiction.

Therefore $(g,g,h) = (g,w) = 1$. Similarly one shows that

$$(*) \qquad (r,r,s) = 1$$

for all $r,s \in \{g,h,k\}$. Hence $(r,s)(r^{-1},s) = {}^{r^{-1}}(r,s)(r^{-1},s) = (r^{-1}r, s) = 1$, i.e.

$$(**) \qquad (r^{-1},s) = (s,r) = (r,s)$$

for all $r,s \in \{g,h,k\}$.

Since $G/\mathcal{C}_G(G') = \langle g,h,k\rangle/\mathcal{C}_G(G')$ is elementary abelian of order 8 by 4.10, the elements g,h,k all act nontrivially on G'. Together with $(*)$, it follows that $(g,y) = z$, $(h,x) = z$, $(k,w) = z$. But then

$$z = z^3 = (g,y)(h,x)(k,w) = (g,h,k)(h,g,k)(k,g,h) = (g,h^{-1},k)(h,k^{-1},g)(k,g^{-1},h) = 1$$

by $(**)$ and Witt's identity, contradiction.

4.12. Theorem: *Let G be a group with $\exp(G') = 2$ and $|G'| \geq 8$. If $\mathbb{F}G$ is centre-by-metabelian, then G has class 2.*

Proof: Let G be a counterexample. Then $\mathbb{F}G$ is centre-by-metabelian, $\gamma_3(G) \neq 1$, and G' is elementary abelian of order at least 8.

Set $C := \mathcal{C}_G(G')$. Then G/C is abelian. By 4.1, $\exp(G/C) \bigm| 4$ or $|G/C| = 3$. In the latter case, 4.1 also implies that $G' = (G,G') \times \mathcal{C}_{G'}(G) = \gamma_3(G) \times (\mathcal{Z}(G) \cap G')$ and $\gamma_4(G) = (G, \gamma_3(G)) = \gamma_3(G) = (G,G') \cong V_4$. We write $\mathcal{Z}(G) \cap G' = \langle z\rangle \times N$ for some $z \in G'$, $N \leq G'$. Then G/N is a nonnilpotent group with $(G/N)' = G'/N \cong Z_2 \times Z_2 \times Z_2$. Then 4.9 implies that $\mathbb{F}[G/N]$ is not centre-by-metabelian, contradiction. Therefore $\exp(G/C) \bigm| 4$.

We claim next that $\gamma_3(G)$ is a finite 2-group. By 1, there exists a subgroup A of G of index at most 2 such that A' is a finite 2-group. If $G = A$, then our claim follows immediately.

So suppose $G \neq A$, and let $t \in G \setminus A$. Then $G' = (t,A)A' \subseteq A$ by 1.6. Similarly $\gamma_3(G) = (G,G') = (A,G')(t,G') \subseteq A'(t,G')$, since $(A,G') \trianglelefteq G$ and $(ta,h) = {}^{t}(a,h)(t,h) \in (A,G')(t,G')$ for all $a \in A$, $h \in G'$. Now G' is abelian, and thus $(t,xy) = (t,x)(t,y)$ for all $x,y \in G'$ by 1.1. Therefore $(t,G') = (t, A'(t,A)) = (t,A')(t,t,A) \subseteq A'(t,t,A) = A'(t, \langle (t,a)\colon a \in A\rangle) = A' \langle (t,t,a)\colon a \in A\rangle$, hence $\gamma_3(G) \subseteq A' \langle (t,t,a)\colon a \in A\rangle$. But for $a \in A$, one has $(t,t,a) = {}^{t}(t,a)(t,a)^{-1} = {}^{t}(t,a)(t,a) = (t^2,a) \in A'$. This shows $\gamma_3(G) \subseteq A'$. Now since A' is finite, $\gamma_3(G)$ is finite, too (and of exponent 2).

Therefore we may consider the elementary abelian 2-group $\gamma_3(G)$ as a finite-dimensional $\mathbb{F}_2[G/C_G(\gamma_3(G))]$-module. But then $G/\mathcal{C}_G(\gamma_3(G))$ is also finite; in fact, it is a finite 2-group since $\exp\left(G/\mathcal{C}_G(\gamma_3(G))\right) \bigm| \exp(G/C) \bigm| 4$. Hence $\gamma_3(G)$ contains a submodule in every possible dimension. In other words: For any $q \in \{2, 4, 8, \dots, |\gamma_3(G)|\}$, there is a subgroup N of $\gamma_3(G)$ of order q which is normal in G.

Assume that $|G' : \gamma_3(G)| \leq 4$. Pick a subgroup N of $\gamma_3(G)$ such that $N \trianglelefteq G$ and $|G' : N| = 8$. Then G/N is a counterexample to 4.9, contradiction. Hence $|G' : \gamma_3(G)| \geq 8$.

Choose now a normal subgroup N of G with $N \subseteq \gamma_3(G)$ and $|\gamma_3(G) : N| = 2$. Since G/N satisfies the prerequisites of the lemma, it is also a counterexample, so we may replace G by G/N and thus assume that $|\gamma_3(G)| = 2$. Then $\gamma_3(G)$ is central, and G has class 3. We write $\gamma_3(G) = \langle z \rangle$.

Clearly, there is a finite set $X \subseteq G$ such that $\left|\langle X \rangle'\right| \geq 8$ and $\langle X \rangle' \not\subseteq \mathcal{Z}(G)$. By possibly adding one element of G to X which acts nontrivially on some commutator of $\langle X \rangle$, we may assume that also $\langle X \rangle$ has class 3, i.e. $\gamma_3(\langle X \rangle) = \langle z \rangle$. Therefore also $\langle X \rangle$ is a counterexample. So we may replace G by $\langle X \rangle$ and assume that $G = \langle X \rangle$ is finitely generated.

Then $G/\langle z \rangle$ is a finitely generated group of class 2. By 3.1 (ii), it follows that also $G'/\langle z \rangle$ is finitely generated; in fact, it is finite since it is elementary abelian. But then also G' is finite.

So from now on, we may argue by induction on $|G'|$. The case $|G'| = 8$ is taken care of by 4.9. So suppose $|G'| \geq 16$. We write $|G'| = 2^{n+1}$ with $n \in \mathbb{N} \setminus \{1, 2\}$ and assume that the theorem is already proved for every applicable group H with $|H'| \leq 2^n$.

If $s \in (G' \cap \mathcal{Z}(G)) \setminus \{1\}$, then, by induction, $G/\langle s \rangle$ has class 2. Therefore $\langle z \rangle = \gamma_3(G) \subseteq \langle s \rangle$, hence $s = z$ and $G' \cap \mathcal{Z}(G) = \langle z \rangle = \gamma_3(G)$.

We write $G' = \langle x_1, \dots, x_n, z \rangle$ with $x_1, \dots, x_n \in G' \setminus \mathcal{Z}(G)$. By 4.10, there are elements $a_1, \dots, a_n \in G$ such that

$$(a_i, x_j) = \begin{cases} 1 & \text{if } i \neq j \\ z & \text{if } i = j \end{cases}$$

for all $i, j = 1, \dots, n$, and $G/C = \langle a_1 C, \dots, a_n C \rangle$ is an elementary abelian group of order 2^n. Hence $H_1 := \langle a_2, a_3, \dots, a_n, C \rangle$ and $H_2 := \langle a_1, a_3, \dots, a_n, C \rangle$ are normal subgroups of G of index 2 with $G = H_1 H_2$.

In the case $H_1' = G'$, we have $\mathcal{Z}(H_1) \cap H_1' = \mathcal{C}_{G'}(H_1) = \mathcal{C}_{G'}(a_2, \dots, a_n) = \langle z, x_1 \rangle$ and $\langle z \rangle \supseteq (H_1, H_1') = (H_1, G') \supseteq (a_2, G') = \langle z \rangle$. Hence H_1 is a group of class 3, and therefore also a counterexample. Then $H_1/\langle x_1 \rangle$, which also has class 3, is also a counterexample whose commutator subgroup is elementary abelian of order 2^n. But this contradicts the induction hypotheses.

Therefore $H_1' < G'$. Then induction implies that $|H_1'| \leq 4$ or $\operatorname{cl}(H_1) = 2$.

If H_1 has class 2, then $H_1' \subseteq \mathcal{C}_{G'}(H_1) = \langle x_1, z \rangle$. Therefore, we have $|H_1'| \leq 4$ in any case. Moreover, since $G' \subseteq C \subseteq H_1$, we know that $\langle z \rangle = (H_1, G') \subseteq H_1'$, and therefore $|H_1'/\langle z \rangle| \leq 2$.

Similarly, we have $|H_2'/\langle z \rangle| \leq 2$.

We now apply 3.1 (ii) to the group $G/\langle z\rangle$, which has class 2 and is generated by the set $C \cup \{a_1, \dots , a_n\}$:

$$(*) \qquad G'/\langle z\rangle = \langle (a_1, a_2)\rangle \, H_1' H_2'/\langle z\rangle \,.$$

It follows that $|G' : \langle z\rangle| \le |\langle (a_1, a_2),\, z\rangle : \langle z\rangle| \cdot |H_1' : \langle z\rangle| \cdot |H_2' : \langle z\rangle| \le 2 \cdot 2 \cdot 2 = 8$. Hence $|G'| \le 16$. In fact, since $|G'| > 8$, we have $|G'| = 16$.

Consequently $n = 3$, $G' = \langle x_1, x_2, x_3, z\rangle$, and $G/C = \langle a_1C, a_2C, a_3C\rangle$. Then (a_1, a_2) must not be contained in $\langle (a_1, a_3),\, (a_2, a_3)\rangle \subseteq H_1' H_2'$, for otherwise $|G'| < 16$ by $(*)$. Similarly one shows that $(a_1, a_3) \notin \langle (a_1, a_2),\, (a_2, a_3)\rangle$ and $(a_2, a_3) \notin \langle (a_1, a_2),\, (a_1, a_3)\rangle$. Hence $|\langle (a_1, a_2),\, (a_1, a_3),\, (a_2, a_3)\rangle| = 8$, i.e. $|\,\langle a_1, a_2, a_3\rangle'\,| \ge 8$. Then $\langle a_1, a_2, a_3\rangle$ acts nontrivially on $\langle a_1, a_2, a_3\rangle'$, i.e. $\mathrm{cl}(\langle a_1, a_2, a_3\rangle) > 2$. By 4.9, $|\,\langle a_1, a_2, a_3\rangle'\,| \ne 8$, hence $|\,\langle a_1, a_2, a_3\rangle'\,| \ge 16$, and thus $\langle a_1, a_2, a_3\rangle' = G' = \langle x_1, x_2, x_3, z\rangle$. But then $\langle a_1, a_2, a_3\rangle$ is a counterexample to 4.11, contradiction.

4.13. Theorem (summary): *Let G be a group such that $\exp(G') = 2$. Then $\mathbb{F}G$ is centre-by-metabelian if and only if one of the following statements holds:*

(i) $|G'| \mid 4$,
(ii) $G' \cong Z_2 \times Z_2 \times Z_2$ *and* $\mathrm{cl}(G) = 2$,
(iii) G has an abelian subgroup of index 2.

Proof: 3.11 and 4.12.

5. Group actions and algorithmic reductions

5.1. Remark: (i) Let G be a group that acts via automorphisms on groups H, K, and let $\varphi\colon G \to \mathrm{Aut}(H)$, $\psi\colon G \to \mathrm{Aut}(K)$, be the corresponding group homomorphisms. The actions of G on H and on K are called *equivalent*, if there exists an isomorphism $\alpha\colon H \to K$ such that the following diagram commutes for all $g \in G$ (cf. [**5**, I.10.1.c]):

$$\begin{tikzcd}
H \arrow[r, "\varphi(g)"] \arrow[d, "\alpha"] & H \arrow[d, "\alpha"] \\
K \arrow[r, "\psi(g)"] & K
\end{tikzcd}$$

Additionally, we will allow renaming the elements of G by an automorphism of G, i.e. we will also consider the two actions to be equivalent in the case that the above diagram commutes with $\psi \circ \beta$ in the place of ψ for a suitable $\beta \in \mathrm{Aut}(G)$.

(ii) Consider the case $H = K$. Two actions of G on H are consequently "essentially the same", if the images of the corresponding homomorphisms $G \to \mathrm{Aut}(H)$ are conjugate in $\mathrm{Aut}(H)$. (Note the analogy to the theory of linear representations of G.) This insight makes it cheaper to compute (and later on work with) "all" group actions on a given group H: Instead of the complete subgroup lattice of $\mathrm{Aut}(H)$, we only need representatives for the conjugacy classes of its subgroups.

(iii) As the reader might have already guessed, we henceforth take $H := G'$ to be the commutator subgroup of G, where G acts on H by conjugation, and ask the following question: Given the isomorphism type of H, what are the possible actions of G on H? For this, set

$$C := \mathcal{C}_G(H),\ A := G/C,\ U := HC/C,\ I := H/(C \cap H) = H/\mathcal{Z}(H).$$

(Cf. the diagram in 5.4.) Then $A' = U \cong I$, or more exactly: We have monomorphisms $\varphi\colon A \hookrightarrow \mathrm{Aut}(H)$, $\psi\colon I \hookrightarrow \mathrm{Aut}(H)$, which are induced by the actions of G on H, respectively of H on itself, by conjugation. Then $\varphi(A)' = \varphi(A') = \varphi(U) = \psi(I) = \mathrm{Inn}(H)$; in words: the commutator subgroup of the image of A in $\mathrm{Aut}(H)$ is the group of inner automorphisms of H.

(iv) As an application of (iii), we show that $H := D_8$ cannot be a commutator subgroup: Assume otherwise, then $Z_2 \times Z_2 \cong D_8/\mathcal{Z}(D_8) = I \cong U = A' \hookrightarrow \mathrm{Aut}(D_8)' \cong D_8' \cong Z_2$, contradiction. (Recall that $\mathrm{Aut}(D_8) \cong D_8$.) We will study the other instances of $|H| \in \{8, 16\}$ in 5.4, but before that, we need two more lemmata which will also be helpful in later sections:

5.2. Lemma: *Let P be a normal finite 2-subgroup of a group G, and set $C := \mathcal{C}_G(P)$. Suppose that $\mathbb{F}G$ is centre-by-metabelian, and that G/C is not a 2-group. Then*

(i) there is a Hall $2'$-subgroup S/C of G/C with $|S : C| = 3$,

(ii) $P = \mathcal{C}_P(S) \times (S, P)$ is abelian with $(S, P) \cong V_4$.

Proof: Since P is finite, G/C is also finite. By theorem 1, G is solvable. Therefore G/C contains a (nontrivial) Hall $2'$-subgroup S/C [**5**, Hauptsatz VI.1.8].

According to Burnside [**3**, theorem 5.1.4], the action of S/C on the elementary abelian group $\bar{P} := P/\Phi(P)$ is also nontrivial and faithful. We set $\bar{G} := G/\Phi(P)$, $\bar{S} := S\Phi(P)/\Phi(P)$, $\bar{C} := C\Phi(P)/\Phi(P)$. Then also $\bar{S}/\bar{C} \cong S/C$ acts nontrivially and faithfully on $\bar{P}$.

Now $\mathbb{F}\left[\bar{G}\right]$ is centre-by-metabelian. By 4.1, $|\bar{S} : \bar{C}| = 3$, $\bar{P} = (S, \bar{P}) \times \mathcal{C}_{\bar{P}}(S)$, and $|(S, \bar{P})| = 4$. In particular, $|S : C| = 3$; this shows (i). We write $S/C = \langle aC \rangle$.

To prove (ii), we first study the case $P = (S, P)$. We claim that then $P \cong V_4$. First note that $\bar{P} = P/\Phi(P) = (S, P)/\Phi(P) = (S, P/\Phi(P)) = (S, \bar{P})$ has order 4. Hence we may write $P/\Phi(P) = \langle x\Phi(P), y\Phi(P) \rangle$ with some elements $x, y \in P$ with ${}^{a}x = y$. Then $P = \langle x, y \rangle$, and $x^2 \equiv y^2 \equiv (x, y) \equiv 1$, ${}^{a}y \equiv xy \pmod{\Phi(P)}$. Then

$$\begin{aligned}
\rho := [x + {}^{a}x, a + {}^{x}a] &= [x + y, a + xy^{-1}a] = [(1 + xy^{-1})y, (1 + xy^{-1})a] \\
&= (1 + xy^{-1})(y(1 + xy^{-1})a + a(1 + xy^{-1})y) \\
&= (1 + xy^{-1})(y + {}^{y}x + {}^{a}y + y)a \\
&= ({}^{y}x + {}^{a}y + x^2y^{-1} + xy^{-1}\,{}^{a}y)a, \qquad \text{and}
\end{aligned}$$

$$\begin{aligned}
0 = [x, \rho]a^{-1} &= x({}^{y}x + {}^{a}y + x^2y^{-1} + xy^{-1}\,{}^{a}y)aa^{-1} + ({}^{y}x + {}^{a}y + x^2y^{-1} + xy^{-1}\,{}^{a}y)axa^{-1} \\
&= x\,{}^{y}x + x\,{}^{a}y + x^3y^{-1} + x^2y^{-1}\,{}^{a}y + yx + {}^{a}yy + x^2 + xy^{-1}\,{}^{a}yy \in \mathbb{F}P.
\end{aligned}$$

Sorting and splitting the last sum w.r.t. the partition of P into cosets of $\Phi(P)$, we obtain

$$\begin{aligned}
&0 = x\,{}^{y}x + x^2 \in \mathbb{F}[\Phi(P)] && 0 = x^2y^{-1}\,{}^{a}y + {}^{a}yy \in \mathbb{F}[x\Phi(P)] \\
&0 = x\,{}^{a}y + xy^{-1}\,{}^{a}yy \in \mathbb{F}[y\Phi(P)] && 0 = x^3y^{-1} + yx \in \mathbb{F}[xy\Phi(P)].
\end{aligned}$$

The first equation implies that ${}^{y}x = x$, i.e. $P = \langle x, y \rangle$ is abelian. The last one shows that $x^2 = y^2$. Hence $\Phi(P) = \left\langle x^2, y^2 \right\rangle$ is cyclic.

Assume that $\Phi(P) \neq 1$. Then $|\Phi(P) : \Phi(\Phi P)| = 2$. Since $\Phi(\Phi P) \trianglelefteq G$, we may replace G by $G/\Phi(\Phi P)$ if necessary, and assume that $|\Phi(P)| = 2$. Then $|P| = 8$, i.e. $P \cong Z_2 \times Z_4$. Then P contains four elements of order 4, and each automorphism that fixes one of them also fixes its inverse. Hence P has no automorphism of order 3, contradiction.

Therefore $\Phi(P) = 1$, and thus $P \cong V_4$, as desired.

We now consider the case that $M := (S, P) < P$. By [**8**, 7.12], we have $P = MQ$, where $Q := \mathcal{C}_P(S)$, and $(S, M) = (S, S, P) = (S, P) = M$. Therefore we are in a similar situation as in the preceding case (with M instead of P, and SM instead of G). Applying its result, we obtain $M \cong V_4$. Since S acts on M by cyclic permutation of the three nontrivial elements, we have $Q \cap M = 1$. Hence $P = M \rtimes Q$, since $M \trianglelefteq P$ by 1.4. Then $(M, Q) \in M \cap P' \subseteq M \cap \Phi(P)$. But $M \cong V_4 \cong M\Phi(P)/\Phi(P) \cong M/M \cap \Phi(P)$, i.e. $M \cap \Phi(P) = 1$. Consequently $(M, Q) = 1$, and $P = M \times Q$.

It remains to show that Q is abelian. We assume that $Q' \neq 1$ and set $U := \langle a, P \rangle$. Then $U' = (a, P)P' = (a, M)Q' = M \times Q'$ by 1.6. Since P is a finite 2-group, there exists a normal subgroup R of P with $R \subseteq Q'$ and $|Q' : R| = 2$ by [**5**, Satz III.7.2]. Since $R \subseteq Q$ is centralized by a, it is even normal in U. Then U/R is a nonnilpotent group with $(U/R)' = (M \times Q')/R \cong M \times Q'/R \cong Z_2 \times Z_2 \times Z_2$. By the summary of section 4, $\mathbb{F}[U/R]$ is not centre-by-metabelian. Contradiction.

5.3. Lemma: *Let G be a group such that $|G'| \nmid 8$. Suppose that M is a subgroup of index 2 in G with $|M'| = 2$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Note that $M' \trianglelefteq G$, hence $M' \subseteq \mathcal{Z}(G)$. We write $M' = \langle z \rangle$ and $G = \langle g, M \rangle$. By 1.6, $G' = (g, M)M'$.

We define maps

$$\begin{aligned}\tau \colon\ &(M \smallsetminus \mathcal{Z}(M)) \times M \times M \to \mathbb{F}[G'],\\ &\qquad (b, c, d) \mapsto (1 + z)(1 + (g, c^{-1}))(1 + (g, d))(1 + (g, b)),\end{aligned}$$

and

$$\varphi \colon\ M \to G'/M',\ a \mapsto (g, a)M'.$$

Then φ is surjective; it even is an epimorphism since for all $a, b \in M$ we have $\varphi(ab) = (g, ab)M' = (g, a)\,{}^{a}(g, b)M' = (g, a)M'(a, g, b)(g, b) = (g, a)(g, b)M' = \varphi(a)\varphi(b)$.

We want to show that $\tau \neq 0$.

Suppose first that there are elements of G' whose order is not a power of 2. Then also G'/M' contains such elements. Then there clearly is also an element $b \in M \smallsetminus \mathcal{Z}(M)$ such that $|\langle \varphi(b) \rangle|$ is not a power of 2; in particular, $(g, b)^4 \notin \langle z \rangle$. Then $(g, b^2) \equiv (g, b)^2 \pmod{\langle z \rangle}$, hence $\tau(b, b^{-2}, b) = (1 + z)(1 + (g, b^2))(1 + (g, b))^2 = (1 + z)(1 + (g, b)^4) \neq 0$.

Suppose now that every element of G' is a 2-element. Then $|G'| \geq 16$, i.e. $|G'/M'| \geq 8$. Then there also is a finite (2-)subgroup H/M' of G'/M' with $|H/M'| \geq 8$. We obviously may choose elements $c, d \in M$ such that $1 \lhd \langle \varphi(c) \rangle \lhd \langle \varphi(c), \varphi(d) \rangle \lhd H/M'$. Then $M_1 := \varphi^{-1}(\langle \varphi(c), \varphi(d) \rangle) < M$. Since also $\mathcal{Z}(M) < M$, there is an element $b \in M \smallsetminus (M_1 \cup \mathcal{Z}(M)) \neq \emptyset$. Hence $1 < \langle \varphi(c) \rangle < \langle \varphi(c), \varphi(d) \rangle < \langle \varphi(c), \varphi(d), \varphi(b) \rangle$, i.e. $1 < \langle z \rangle < \langle z, (g, c) \rangle < \langle z, (g, c), (g, d) \rangle < \langle z, (g, c), (g, d), (g, b) \rangle$. By 1.13, $\tau(b, c^{-1}, d) \neq 0$.

In any case, there is a triple $(b, c, d) \in (M \smallsetminus \mathcal{Z}(M)) \times M \times M$ such that $\tau(b, c, d) \neq 0$. Choose an element $a \in M \smallsetminus \mathcal{C}_M(b) \neq \emptyset$, then $(a, b) = z$, and

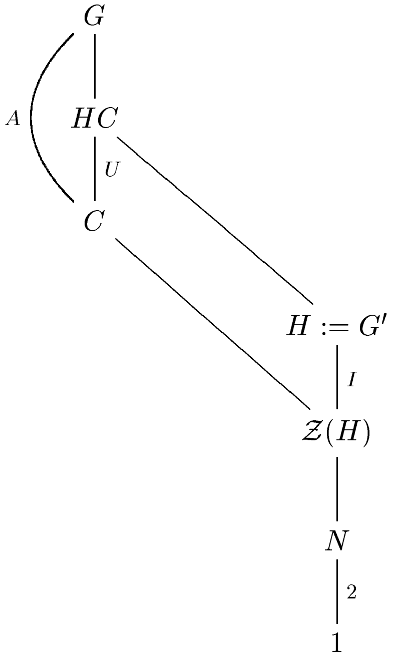
$$\begin{aligned}(\mathbb{F}G)'' \ni [b + {}^{a}b, g + {}^{c}g] &= [(1 + z)b, (1 + (c, g))g]\\ &= (1 + z)(1 + (c, g))[b, g]\\ &= \underbrace{(1 + z)(1 + (c, g))(1 + (g, b))b}_{=:\sigma \in \mathbb{F}M}\, g.\end{aligned}$$

(Note that z is central and (c, g) commutes with b modulo $\langle z \rangle$.) Now $M/\langle z \rangle$ is abelian, in particular $[d, \sigma] = 0$. Then

$$\begin{aligned}0 \neq b\,\tau(b, c, d)\,dg &= (1 + z)(1 + (c, g))(1 + (g, b))b\,(1 + (g, d))dg\\ &= \sigma[d, g] = [d, \sigma g]\\ &\in [\mathbb{F}G, (\mathbb{F}G)''].\end{aligned}$$

Hence $\mathbb{F}G$ is not centre-by-metabelian.

5.4. Remark: Recall the situation of 5.1:



Assume additionally that G is a counterexample to theorem 4, and that H is a finite 2-group. Then H is not elementary abelian (cf. section 4), and $A \neq 1$ (cf. section 3). Furthermore, $\mathbb{F}G$ is centre-by-metabelian, so lemma 5.2 implies that:

(1) If H is nonabelian, then A is a 2-group.
(2) If H is abelian and A is not a 2-group, then A is a $\{2,3\}$-group such that $|S| = 3$ and $(S, H) \cong V_4$ for any Sylow 3-subgroup S of A.

If $|H| = 16$, we may argue by induction and assume that there are no counterexamples with commutator subgroups of order 8. So for all $N \trianglelefteq G$ with $N \subseteq H$ and $|N| = 2$, G/N is not a counterexample. Hence one of the following holds:

(3) $H/N \cong Z_2 \times Z_2 \times Z_2$, and A acts trivially on H/N, i.e. $(A, H) \subseteq N$.
(4) $H/N \cong Z_2 \times Z_4$, and A acts dihedrally on H/N.
(5) G/N contains an abelian subgroup of index 2.

But lemma 5.3 shows that in case (5), also G contains an abelian subgroup of index 2, hence it is not a counterexample. So we may dismiss this case.

We are now able to describe an algorithm that, given any finite 2-group H, computes all possibilities for A:

- Check if H is elementary abelian. If so, stop, otherwise proceed (cf. section 4).
- Compute the conjugacy classes of the subgroups of $\mathrm{Aut}(H)$, and take representatives (cf. 5.1 (ii)).
- Throw away the trivial representative (cf. section 3).
- Throw away all representatives A with $A' \neq \mathrm{Inn}(H)$ (cf. 5.1 (iii)).
- Throw away the representatives A that do not comply with either (1) or (2).

- If $|H| = 16$, then for each A that has survived so far, compute all A-invariant subgroups N of H of order 2. (Then N is normal in G, and in particular also H-invariant.) If there is an N such that neither of the conditions (3) or (4) is satisfied, throw the A away.

This computational effort is better left to a machine rather than a human being. This should not be a problem for any reasonable computer algebra system, even for infinite G, since H finite implies that $\mathrm{Aut}(H)$, $\mathrm{Inn}(H)$, A, I, U are also finite.

I have chosen GAP 3.4 [**18**] to program this algorithm in a routine called `PossibleActions`; you can find its commented source code in appendix C.

If H loops over all groups of orders 8 and 16, `PossibleActions` yields the following results:

```
gap> ls:=AllTwoGroups(Size, [8,16]);;
gap> actions:=List(ls, PossibleActions);;
gap> PrintArray(List([1..Length(ls)], i->[i,
>                                      GroupNames(ls[i]),
>                                      Length(actions[i])]
>                ));;
[ [            1,        [ 8 ],            4 ],
  [            2,      [ 2x4 ],            6 ],
  [            3,       [ D8 ],            0 ],
  [            4,       [ Q8 ],            0 ],
  [            5,    [ 2x2x2 ],            0 ],
  [            6,       [ 16 ],            0 ],
  [            7,      [ 4x4 ],            1 ],
  [            8,             ,            0 ],
  [            9,  [ (2x4).2 ],            0 ],
  [           10,      [ 2x8 ],            5 ],
  [           11,             ,            0 ],
  [           12,      [ D16 ],            0 ],
  [           13,     [ QD16 ],            0 ],
  [           14,      [ Q16 ],            0 ],
  [           15,    [ 2^2x4 ],            3 ],
  [           16,     [ D8x2 ],            0 ],
  [           17,     [ Q8x2 ],            0 ],
  [           18,     [ D8Y4 ],            0 ],
  [           19,      [ 2^4 ],            0 ] ]
```

The first column indexes H as it appears in the 2-group catalogue of GAP, the second states GAP's (obvious) names for H, if GAP has found any, and the third tells us the number of representatives A that have survived the reductions laid out in the algorithm. (In appendix C, it is also described how to extract the actual action of A on H in each case.)

Actually, the results for $|H| = 8$ are not surprising:

The automorphism group of $H := Z_8$ is isomorphic to V_4, so it has 4 nontrivial subgroups, none of which is excluded by the algorithm.

The automorphism group of $H := Z_2 \times Z_4$ is isomorphic to D_8, which has 6 conjugacy classes of nontrivial abelian subgroups, all of which are listed above.

We have shown already in 5.1 (iv) that $H := D_8$ cannot be a commutator subgroup, so our algorithm certainly must give us 0 possibilities in this case.

For $H := Q_8$, we have $\mathrm{Aut}(Q_8) \cong S_4$, $U \cong \mathrm{Inn}(Q_8) \cong H/\mathcal{Z}(H) \cong Z_2 \times Z_2$, and the only subgroup A of S_4 with $A' \cong Z_2 \times Z_2$ is $A \cong A_4$. Since Q_8 is nonabelian, only 2-groups are allowed for A, but A_4 is not a 2-group.

The elementary abelian group $H := Z_2 \times Z_2 \times Z_2$ is ignored anyway because of the results of section 4.

So the algorithm starts to become really helpful in the case $|H| = 16$. Keep in mind however, that here the results are based on our assumption that there are no counterexamples with $|H| = 8$. The existence of such is disproved in section 6 ($4 + 6 = 10$ cases). The $1+5+3 = 9$ cases with $|H| = 16$ that the algorithm could not dismiss are then dealt with in section 7, before we rule out any other counterexamples to theorem 4 with an inductive argument in section 8.

6. Commutator subgroups of order 8

6.1. Remark: Let us assume that G is a counterexample to our main theorem 4 such that $|G'| = 8$. By 5.4, $G' \cong Z_8$ or $G' \cong Z_2 \times Z_4$.

We first study the case $G' = \langle x \rangle \cong Z_8$. Then $\mathrm{Aut}(G') = \langle \alpha, \beta \rangle \cong V_4$, where

$$\alpha\colon\ G' \to G',\ x \mapsto x^{-1},$$
$$\beta\colon\ G' \to G',\ x \mapsto x^{3}.$$

The four possibilities for the action of G mentioned in the list on page 31 are $\langle \alpha, \beta \rangle$, $\langle \alpha \rangle$, $\langle \beta \rangle$, $\langle \alpha\beta \rangle$, i.e. all nontrivial subgroups of $\mathrm{Aut}(G')$.

As usual, we set $C := \mathcal{C}_G(G')$, and study the monomorphism $\varphi\colon\ G/C \hookrightarrow \mathrm{Aut}(G')$ that stems from the action of G on G'. We have to show that if $\mathbb{F}G$ is centre-by-metabelian, then the image of φ is $\langle \alpha \rangle$, and C is abelian. This will be done in lemmata 6.2–6.4.

6.2. Lemma: *Let the notation be as in 6.1, and assume that the image of φ is either $\langle \beta \rangle$ or $\langle \alpha\beta \rangle$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Observe that $\alpha\beta\colon\ G' \to G'$, $x \mapsto x^5$. Hence, there is an exponent $i \in \{3, 5\}$ and an element $b \in G$ such that ${}^{b}x = x^i$. Then $G/C = \langle bC \rangle$, and $G' = (b, C)C' = (b, C)$, since $C' \subseteq \mathcal{Z}(G) \cap G' < G'$, i.e. $C' \subseteq \Phi(G')$.

Consequently, $(b, .)\colon\ C \to G' = \langle x \rangle$ is an epimorphism, so there is an element $c \in C$ such that $(b, c) = x$. Then

$$\begin{aligned}
\tau := [[b, c], [b, cb^{-1}]] &= [(1 + x)cb, (1 + x)c] \\
&= (1 + x)c\,(b(1 + x)c + (1 + x)cb) \\
&= (1 + x)c\,\big((1 + x^i)x + (1 + x)\big)\,cb \\
&= (1 + x)(1 + x^{i+1})c^2 b, \text{ and}
\end{aligned}$$

$$\begin{aligned}
[c, \tau] &= (1 + x)(1 + x^{i+1})c^2[c, b] \\
&= (1 + x)(1 + x^{i+1})c^2(1 + x)cb \\
&= (1 + x^{i+1})(1 + x^2)c^3 b.
\end{aligned}$$

It is easy to see that the last expression is nonzero for any choice of $i \in \{3, 5\}$.

6.3. Lemma: *Let the notation be as in 6.1, and assume that the image of φ is $\langle \alpha, \beta \rangle$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Choose $a, b \in G$ with ${}^{a}x = x^{-1}$, ${}^{b}x = x^3$. Then ${}^{ab}x = x^5$, and $G/C = \langle aC, bC \rangle = \langle abC, bC \rangle$. It follows that $G' = \langle (ab, b) \rangle\,(ab, C)(b, C)C' = \langle (a, b) \rangle\,(ab, C)(b, C)$, since $C' \subseteq \mathcal{Z}(G) \cap G' = \mathcal{C}_{G'}(a) \cap \mathcal{C}_{G'}(b) = \left\langle x^4 \right\rangle \subseteq \Phi(G')$. Since G' is cyclic, we have $G' = \langle (a, b) \rangle$ or $G' = (ab, C)$ or $G' = (b, C)$,

Suppose that $G' = (b, C)$, and set $H := \langle b, C \rangle$. Then $H' = G'$, and $\mathcal{C}_H(H') = C$, and $H/C = \langle bC \rangle$. Hence H satisfies the hypothesis of lemma 6.2, i.e. $\mathbb{F}H$ is not centre-by-metabelian, and certainly $\mathbb{F}G$ is neither.

The same argument is valid for the case $G' = (ab, C)$.

Therefore we may assume that (a, b) has order 8, w.l.o.g. $(a, b) = x$. Then

$$\begin{aligned} \tau := [a + {}^{b}a, b + {}^{a}b] &= [(1 + x^{-1})a, (1 + x)b] \\ &= (1 + x^{-1})(1 + x^{-1})ab + (1 + x)(1 + x^{-3})ba \\ &= \left((1 + x^{-2}) + (1 + x)(1 + x^{-3})x^{-1}\right) ab \\ &= x^4 \left(1 + x + x^2 + x^3\right) ab, \text{ and} \\ [x, \tau] &= x^4(1 + x + x^2 + x^3)[x, ab] \\ &= x^4(1 + x + x^2 + x^3)(1 + x^4)xab = \langle x\rangle^+ab \neq 0. \end{aligned}$$

So $\mathbb{F}G$ is also not centre-by-metabelian in this case.

6.4. Lemma: *Let the notation be as in 6.1, and assume that the image of φ is $\langle\alpha\rangle$. If $\mathbb{F}G$ is centre-by-metabelian, then C is abelian.*

Proof: Suppose that $C' \neq 1$. Since $C' \subseteq \mathcal{Z}(G) \cap G' = \langle x^4 \rangle \cong Z_2$, we have $C' = \langle x^4 \rangle \subseteq \Phi(G')$.

Let $a \in G \setminus C$. Then $G/C = \langle aC\rangle$, ${}^{a}x = x^{-1}$, $G' = (a, C)$, and the map $(a, .)\colon C \to G'$ is an epimorphism. In particular, $U := (a, .)^{-1}(\langle x^2\rangle) < C$. Let $d \in C \setminus \mathcal{Z}(C) \neq \emptyset$, then $V := \mathcal{C}_C(d) < C$. Therefore we may choose an element $c \in C \setminus (U \cup V) \neq \emptyset$. Then $(c, d) = x^4 = (d, c)$, and (a, c) has order 8, w.l.o.g. $(a, c) = x$. Hence

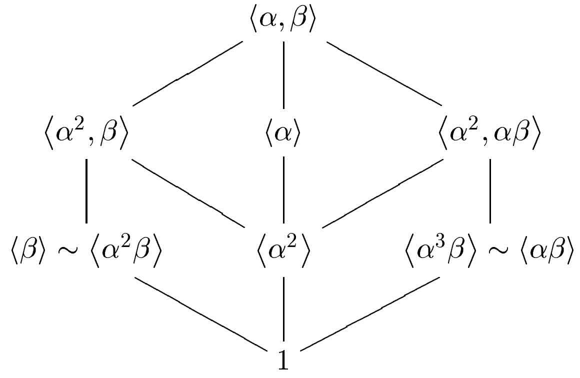
$$\begin{aligned} (\mathbb{F}G)'' \ni [a + {}^{c}a, c + {}^{d}c] &= [\underbrace{(1 + x^{-1})}_{\in \mathcal{C}_{\mathbb{F}G}(c)} a, \underbrace{(1 + x^4)}_{\in \mathcal{Z}(\mathbb{F}G)} c] \\ &= (1 + x^{-1})(1 + x^4)[a, c] \\ &= (1 + x^{-1})(1 + x^4)(1 + x^{-1})ac = \left\langle x^2\right\rangle^+ac, \end{aligned}$$

and $[c, \langle x^2\rangle^+ac] = \langle x^2\rangle^+[c, a]c = \langle x^2\rangle^+(1 + x)cac = \langle x\rangle^+cac \neq 0$. Therefore $\mathbb{F}G$ is not centre-by-metabelian.

6.5. Remark: Now we have seen that groups with cyclic commutator subgroups of order 8 are not counterexamples to the main theorem 4. So let us turn to the case $G' = \langle x, y\rangle \cong Z_2 \times Z_4$, where $x^2 = 1 = y^4$. Then $\mathrm{Aut}(G') = \langle \alpha, \beta\rangle \cong D_8$, where

$$\begin{aligned} \alpha &\colon G' \to G', x \mapsto xy^2, y \mapsto xy, \\ \beta &\colon G' \to G', x \mapsto x, \quad y \mapsto xy; \end{aligned}$$

check that $\beta^2 = \mathrm{id}_{G'} = \alpha^4$, $\beta\alpha\beta^{-1} = \alpha^{-1}$. The subgroup lattice of $\mathrm{Aut}(G')$ looks like:


$\langle\alpha,\beta\rangle$
$\langle\alpha^2,\beta\rangle$
$\langle\alpha\rangle$
$\langle\alpha^2,\alpha\beta\rangle$
$\langle\beta\rangle \sim \langle\alpha^2\beta\rangle$
$\langle\alpha^2\rangle$
$\langle\alpha^3\beta\rangle \sim \langle\alpha\beta\rangle$
1

Here $\sim$ symbolizes conjugacy of subgroups. Set $C := \mathcal{C}_G(G')$ and let $\varphi\colon\ G/C \hookrightarrow \mathrm{Aut}(G')$ be the usual monomorphism. The algorithm in 5.4 leaves us with six “possible” images of φ (cf. the table on page 31). Since $G' \subseteq C$, i.e. G/C is abelian, those are (representatives for the conjugacy classes of) the subgroups of order 2 or 4 .

We will show in the lemmata 6.6–6.11 that if $\mathbb{F}G$ is centre-by-metabelian, then G/C is mapped onto $\langle\alpha^2\rangle$, and that $C' \subseteq \Phi(G') = \langle y^2\rangle$. (Note that $\langle\alpha^2\rangle$ acts dihedrally on G'.)

6.6. Lemma: *Let the notation be as in 6.5, and assume that the image of φ is $\langle\alpha\rangle$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Let $a \in G$ such that ${}^{a}h = \alpha(h)$ for all $h \in G'$, i.e. ${}^{a}x = xy^2$, ${}^{a}y = xy$. Then $G/C = \langle aC\rangle \cong Z_4$. Since $C' \subseteq \mathcal{Z}(G) \cap G' = \langle y^2\rangle = \Phi(G')$, we have $G' = (a, C)$ by 1.6, i.e. $(a, .) :\ C \to G'$ is an epimorphism. Choose an element $c \in C$ with $(a, c) = y$. Note that $(a, x) = y^2 = (x, a) \in \mathcal{Z}(G)$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [c + {}^{a}c, a + {}^{x}a] &= [(1+y)c, (1+y^2)a]\\ &= (1+y^2)\big((1+y)ca + a(1+y)c\big)\\ &= (1+y^2)\big((1+y)ca + (1+xy)yca\big)\\ &= (1+y^2)(1+xy^2)ca = \langle x, y^2\rangle^{+}ca,\end{aligned}$$

and $[c, \langle x, y^2\rangle^{+}ca] = \langle x, y^2\rangle^{+}c[c, a] = c\langle x, y^2\rangle^{+}(1+y)ca = c(G')^{+}ca \neq 0$. Therefore, $\mathbb{F}G$ is not centre-by-metabelian.

6.7. Lemma: *Let the notation be as in 6.5, and assume that the image of φ is $\langle\beta\rangle$ or $\langle\alpha^2\beta\rangle$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: Since $\langle\beta\rangle$ and $\langle\alpha^2\beta\rangle$ are conjugate in $\mathrm{Aut}(G')$, we may (by renaming the elements of G' if necessary) w.l.o.g. assume that the image of φ is $\langle\beta\rangle$. Then there is an element $b \in G$ with ${}^{b}x = \beta(x) = x$ and ${}^{b}y = \beta(y) = xy$. Then $G/C = \langle bC\rangle \cong Z_2$ and $C' \subseteq \mathcal{Z}(G) \cap G' = \langle x, y^2\rangle = \Omega(G') \cong Z_2 \times Z_2$.

Since $G' = (b,C)C'$ by 1.6, there is an element $c \in C$ such that $\tilde{y} := (b,c)$ has order 4, i.e. $\tilde{y} \in \{y, xy, y^{-1}, xy^{-1}\}$. In any case, ${}^{b}\tilde{y} = x\tilde{y}$. So we may w.l.o.g. assume that $\tilde{y} = y$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [c + {}^{b}c, b + {}^{y}b] &= [(1+y)c, (1+x)b] \\ &= (1+x)\big((1+y)cb + b(1+y)c\big) \\ &= (1+x)\big((1+y)cb + (1+xy)ycb\big) \\ &= (1+x)(1+xy^2)cb = \big\langle x, y^2\big\rangle^{+} cb,\end{aligned}$$

and $[c, \langle x, y^2\rangle^{+} cb] = \langle x, y^2\rangle^{+} c[c,b] = c\langle x, y^2\rangle^{+}(1+y)cb = c(G')^{+}cb \neq 0$. Therefore, $\mathbb{F}G$ is not centre-by-metabelian.

6.8. Lemma: *Let the notation be as in 6.5, and assume that the image of φ is $\langle\alpha^3\beta\rangle$ or $\langle\alpha\beta\rangle$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: As in the preceding proof, we may w.l.o.g. assume that the image of φ is $\langle\alpha^3\beta\rangle$, and choose an element $b \in G$ with ${}^{b}x = (\alpha^3\beta)(x) = xy^2$ and ${}^{b}y = (\alpha^3\beta)(y) = y$. Then $G/C = \langle bC\rangle \cong Z_2$ and $C' \subseteq \mathcal{Z}(G) \cap G' = \langle y\rangle \cong Z_4$.

Case 1: $C' = \langle y\rangle$. Here there are elements $c, \tilde{c} \in C$ such that $|\langle (c,\tilde{c})\rangle| = 4$; in particular, $(c, .)\colon C \to \langle y\rangle$ is an epimorphism. Then $U := (c,.)^{-1}(\langle y^2\rangle) < C$.

Now $G' = (b,C)C'$ implies that $(b,C) \not\subseteq \langle y\rangle$. Since the map $(b,.)\colon C \to G'$ is a homomorphism, this shows that $V := (b,.)^{-1}(\langle y\rangle) < C$.

Therefore we may choose an element $d \in C \smallsetminus (U \cup V) \neq \emptyset$. Then $(c,d) \in \{y, y^{-1}\}$, and $(b,d) \in x\,\langle y\rangle$. By replacing d by its inverse if necessary, we may assume that $(c,d) = y$. Since for all $i \in \mathbb{Z}$, we have $(c^i b, d) = (c,d)^i (b,d) = y^i (b,d)$, we may replace b by $c^i b$ for a suitable i, and assume that $(b,d) = x$. Note that this does not change the action of b on G'. Then $(cb, d) = xy$, hence

$$\begin{aligned}(\mathbb{F}G)'' \ni [d + {}^{cb}d, c + {}^{d}c] &= [(1+xy)d, (1+y^{-1})c] \\ &= (1+xy)(1+y^{-1})(dc + cd) \\ &= (1+xy)(1+y^{-1})(1+y^{-1})cd \\ &= (1+xy)(1+y^2)cd = \langle xy\rangle^{+} cd,\end{aligned}$$

and $[c, \langle xy\rangle^{+} cd] = \langle xy\rangle^{+} c[c,d] = c\langle xy\rangle^{+}(1+y)cd = c(G')^{+}cd \neq 0$. Therefore, $\mathbb{F}G$ is not centre-by-metabelian in this case.

Case 2: $C' \subseteq \langle y^2\rangle = \Phi(G')$. Then $G' = (b,C)$, i.e. the map $(b,.) : C \to G'$ is an epimorphism. If we choose elements $c, d \in C$ such that $(b,c) = x = (c,b)$, $(b,d) = y$, then

$$\begin{aligned}(\mathbb{F}G)'' \ni [c + {}^{b}c, b + {}^{c}b] &= [(1+x)c, (1+x)b] \\ &= (1+x)\big((1+x)cb + b(1+x)c\big) \\ &= (1+x)\big(1 + x + (1+xy^2)x\big)cb \\ &= (1+x)(1+y^2)cb = \big\langle x, y^2\big\rangle^{+} cb.\end{aligned}$$

Since $(cb, d) = (c,d)(b,d) \in y\,\langle y^2\rangle$, we then have $[d, \langle x, y^2\rangle^{+} cb] = \langle x, y^2\rangle^{+}[d, cb] = \langle x, y^2\rangle^{+}(1 + (cb,d))dcb = (G')^{+}dcb \neq 0$. Therefore, $\mathbb{F}G$ is also not centre-by-metabelian in this case.

6.9. Lemma: *Let the notation be as in 6.5, and assume that the image of φ is $\langle \alpha^2, \beta \rangle$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We may choose elements $a, b \in G$ with ${}^{a}h = \alpha^2(h) = h^{-1}$ for all $h \in G'$, and ${}^{b}x = \beta(x) = x$, ${}^{b}y = \beta(y) = xy$. Then $G/C = \langle aC, bC \rangle = \langle abC, bC \rangle \cong Z_2 \times Z_2$ and $C' \subseteq \mathcal{Z}(G) \cap G' = \langle x, y^2 \rangle = \Omega(G') \cong Z_2 \times Z_2$. Moreover, $G' = \langle (a,b) \rangle \, (ab, C)(b, C)C' = \langle (a,b) \rangle \, (ab, C)(b, C)\Omega(G')$.

Case 1: $\langle (a,b) \rangle \nsubseteq \Omega(G')$. With $\tilde{y} := (a,b)$ we have $G' = \langle \tilde{y}, x \rangle$, ${}^{a}\tilde{y} = \tilde{y}^{-1}$, ${}^{b}\tilde{y} = x\tilde{y}$, so by replacing y by $\tilde{y}$, we may assume that $(a,b) = y$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [b + {}^{a}b, a + {}^{b}a] &= [(1+y)b, (1+y^{-1})a] \\ &= (1+y)(1+xy^{-1})ba + (1+y^{-1})(1+y^{-1})ab \\ &= \big((1 + y + xy^{-1} + x) + (1+y^2)y\big)\, ba \\ &= (1+x)(1+y^{-1})ba =: \tau.\end{aligned}$$

Since $(ba, y) = xy^2$, it follows that $[y, \tau] = (1+x)(1+y^{-1})[y, ba] = (1+x)(1+y^{-1})(1+xy^2)yba = (G')^{+}ba \neq 0$. This shows that $\mathbb{F}G$ is not centre-by-metabelian in this case.

Case 2: $\langle (a,b) \rangle \subseteq \Omega(G')$. Then $(\beta, C) = (b, C) \nsubseteq \Omega(G')$ or $(\alpha^2\beta, C) = (ab, C) \nsubseteq \Omega(G')$. Since β and $\alpha^2\beta$ are conjugate in $\operatorname{Aut}(G')$ (namely ${}^{\alpha}\beta = \alpha^2\beta$), we may "shift" G' by α as described in section 5, and assume w.l.o.g. that $(b, C) = (\beta, C) \nsubseteq \Omega(G')$.

Then there is an element $c \in C$ such that $\tilde{y} := (b, c) \in y\Omega(G')$. It is easy to see that this implies $G' = \langle x, \tilde{y} \rangle$, and $(b, b, c) = (b, \tilde{y}) = x$. So if we set $H := \langle b, C \rangle$, then $H' = G'$, $\mathcal{C}_H(H') = C$, and $H/C = \langle bC \rangle$. But then H satisfies the hypothesis of lemma 6.7, so $\mathbb{F}H$ is not centre-by-metabelian, and neither is $\mathbb{F}G$.

6.10. Lemma: *Let the notation be as in 6.5, and assume that the image of φ is $\langle \alpha^2, \alpha\beta \rangle = \langle \alpha^3\beta, \alpha\beta \rangle$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We may choose elements $a, b \in G$ with ${}^{a}x = (\alpha^3\beta)(x) = xy^2$, ${}^{a}y = (\alpha^3\beta)(y) = y$, and ${}^{b}x = (\alpha\beta)(x) = xy^2$, ${}^{b}y = (\alpha\beta)(y) = y^3$; i.e. a acts trivially on $\langle y \rangle$ and dihedrally on $\langle xy \rangle$, and b acts dihedrally on $\langle y \rangle$ and trivially on $\langle xy \rangle$; note moreover that ${}^{ab}h = h^{-1}$ for all $h \in G'$.

Then $G/C = \langle aC, bC \rangle \cong Z_2 \times Z_2$, and $C' \subseteq \mathcal{Z}(G) \cap G' = \langle y^2 \rangle = \Phi(G') \cong Z_2$, hence $G' = \langle (a,b) \rangle \, (a, C)(b, C)$.

Case 1: $(a, C) = G'$. If we set $H := \langle a, C \rangle$, then $H' = G'$, and H/C is mapped onto $\langle \alpha^3\beta \rangle$ under φ. So H satisfies the hypotheses of lemma 6.8, hence $\mathbb{F}H$ is not centre-by-metabelian.

Case 2: $(b, C) = G'$. Here $H := \langle b, C \rangle$ satisfies the hypotheses of lemma 6.8, since H/C is mapped onto $\langle \alpha\beta \rangle$.

Case 3: $(a,b) \notin \langle x, y^2 \rangle = \Omega(G')$. Then ${}^{a}(a,b) = (a,b)^{-1}$ or ${}^{b}(a,b) = (a,b)^{-1}$. We only consider the case ${}^{b}(a,b) = (a,b)^{-1}$ here, since the case ${}^{a}(a,b) = (a,b)^{-1}$ can be handled completely analogously; we just have to switch y and xy, resp. a and b (this stems again from the fact that $\alpha^3\beta$ and $\alpha\beta$ are conjugate in $\operatorname{Aut}(G')$ under the automorphism β, which does switch y and xy). Then $(a,b) \in \{y, y^3\} \subseteq \mathcal{C}_G(a)$. By replacing a by $a^{-1} \in aC$

if necessary, we may assume that $(a,b) = y$. Then $(a,C)(b,C) \nsubseteq \langle y\rangle$, for otherwise $G' = \langle (a,b)\rangle\,(a,C)(b,C) \subseteq \langle y\rangle$.

If $(a,c) \notin \langle y\rangle$ for some $c \in C$, then

$$\begin{aligned}(\mathbb{F}G)'' \ni [b + {}^{a}b, ab + {}^{b}(ab)] &= [(1+y)b, (1+y^{-1})ab]\\ &= (1+y)(1+y)bab + (1+y^{-1})(1+y^{-1})abb\\ &= (1+y^{2})(ba+ab)b\\ &= (1+y^{2})(1+y^{-1})ab^{2} = \langle y\rangle^{+}ab^{2}.\end{aligned}$$

Since $b^2 \in C$ we have $(b^2,c) \in C' \subseteq \langle y^2\rangle$. Hence $[c, \langle y\rangle^{+}ab^2] = \langle y\rangle^{+}(1+(ab^2,c))cab^2 = \langle y\rangle^{+}(1+(a,c))cab^2 = (G')^{+}cab^2 \neq 0$, and $\mathbb{F}G$ is not centre-by-metabelian.

So we may assume that $(a,C) \subseteq \langle y\rangle$. Then $z := (b,c) \notin \langle y\rangle$ for some $c \in C$, and ${}^{a}z = zy^2$. Furthermore,

$$\begin{aligned}(\mathbb{F}G)'' \ni [a + {}^{b}a, b + {}^{c}b] &= [(1+y^{-1})a, (1+z^{-1})b]\\ &= (1+y^{-1})(1+y^{2}z^{-1})ab + (1+z^{-1})(1+y)ba\\ &= \big((1+y^{-1})(1+y^{2}z^{-1})y + (1+z^{-1})(1+y)\big)\,ba\\ &= (1+y)\left(1+y^{2}z^{-1}+1+z^{-1}\right)ba\\ &= \langle y\rangle^{+}z^{-1}ba.\end{aligned}$$

Since $(ba,c) = {}^{b}(a,c)(b,c) \in \langle y\rangle\,z$, we have $[c, \langle y\rangle^{+}z^{-1}ba] = \langle y\rangle^{+}z^{-1}[c,ba] = z^{-1}\langle y\rangle^{+}(1+z)cba = (G')^{+}cba \neq 0$. Therefore, $\mathbb{F}G$ is not centre-by-metabelian in this case.

Case 4: $(a,b) \notin \Phi(G')$. By case 3, $(a,b) \in \Omega(G') \smallsetminus \Phi(G') = \langle x, y^2\rangle \smallsetminus \langle y^2\rangle = \{x, xy^2\}$. By renaming x if necessary, we may even assume that $(a,b) = x$.

Then there exists an element $c \in C$ such that at least one of (a,c), (b,c) has order 4; by switching the roles of a and b, resp. y and xy as in case 3 if necessary, we may w.l.o.g. assume that $|\langle (a,c)\rangle| = 4$. Then $\langle (a,c)\rangle = \langle y\rangle$ or $\langle (a,c)\rangle = \langle xy\rangle$ (disappointingly there is no w.l.o.g.-ing anymore, since we might have switched y and xy already); by replacing c by c^{-1} if necessary we may assume that $(a,c) \in \{y, xy\}$.

Assume first that $(a,c) = y$. Note that $y \in \mathcal{Z}(\mathbb{F}[\langle a,c\rangle])$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [ca + {}^{c}(ca), c + {}^{a}c] &= [(1+y^{-1})ca, (1+y)c]\\ &= (1+y^{-1})(1+y)[ca,c]\\ &= (1+y^{-1})(1+y)(1+y)c^{2}a = \langle y\rangle^{+}c^{2}a.\end{aligned}$$

Observe that $(b,c^2a) = (b,c)^2(b,a) \in \langle y^2\rangle\,x$, hence $[b, \langle y\rangle^{+}c^2a] = \langle y\rangle^{+}(1+(b,c^2a))c^2ab = \langle y\rangle^{+}(1+x)c^2ab = (G')^{+}c^2ab \neq 0$. Hence $\mathbb{F}G$ is not centre-by-metabelian.

Assume now that $(a, c) = xy$. Note that $(1 + x)ba = (1 + x)ab$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [a + {}^{c}a, b + {}^{a}b] &= [(1 + xy^{-1})a, (1 + x)b]\\ &= (1 + xy^{-1})[a, (1 + x)b]\\ &= (1 + xy^{-1})\big((1 + xy^2)ab + (1 + x)ba\big)\\ &= (1 + xy^{-1})\big(1 + xy^2 + 1 + x\big)\, ab\\ &= (1 + xy^{-1})(1 + y^2)xab = \langle xy\rangle^{+}xab.\end{aligned}$$

Now since $(b, xab) = (b, x)(b, a) \in \left\langle y^2\right\rangle x$, we have $[b, \langle xy\rangle^{+}xab] = \langle xy\rangle^{+}(1+(b, xab))xab^2 = \langle xy\rangle^{+}(1 + x)xab^2 = (G')^{+}xab^2 \neq 0$. Therefore $\mathbb{F}G$ is not centre-by-metabelian, and case 4 is finished.

By the cases 1-4, we may assume that $(a, C) < G'$, $(b, C) < G'$, and $(a, b) \in \Phi(G')$. Then $G' = (a, C)(b, C)$, and consequently $(a, C) \cong Z_4$ or $(b, C) \cong Z_4$. W.l.o.g. $(a, C) \cong Z_4$, i.e. $(a, C) = \langle y\rangle$ (case 5 below) or $(a, C) = \langle xy\rangle$ (case 6).

Case 5: $(a, C) = \langle y\rangle$. Then $(a, .)\colon C \to \langle y\rangle$ is an epimorphism, and $U := (a, .)^{-1}(\left\langle y^2\right\rangle) < C$. The map $(b, .) : C \to G'$ is a homomorphism with image $(b, C) \nsubseteq \langle y\rangle$, so $V := (b, .)^{-1}(\langle y\rangle) < C$. Hence there is an element $c \in C \smallsetminus (U \cup V) \neq \emptyset$. Then $(a, c) \in \{y, y^{-1}\}$ and $(b, c) \in x\,\langle y\rangle$. By replacing c by c^{-1} if necessary, we may even assume that $(a, c) = y$. If (b, c) has order 4, then $(ba, c) = {}^{b}(a, c)(b, c) = y^{-1}(b, c) \in (b, c)\,\langle y\rangle = x\,\langle y\rangle$ has order 2. If we choose $\tilde{b} \in \{b, ba\}$ such that $(\tilde{b}, c)$ has order 2, and if we set $z := (\tilde{b}, c) = (c, \tilde{b})$, then $z \in x\left\langle y^2\right\rangle$ and $(1 + z)\tilde{b}c = (1 + z)c\tilde{b}$. Note that ${}^{\tilde{b}}y = y^{-1}$ and $(a, \tilde{b}) = (a, b) \in \left\langle y^2\right\rangle$ for any choice of $\tilde{b}$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [c + {}^{a}c, \tilde{b} + {}^{c}\tilde{b}] &= [(1 + y)c, (1 + z)\tilde{b}] = (1 + z)[(1 + y)c, \tilde{b}]\\ &= (1 + z)\left((1 + y)c\tilde{b} + (1 + y^{-1})\tilde{b}c\right)\\ &= (1 + z)\left(1 + y + 1 + y^{-1}\right) c\tilde{b}\\ &= (1 + z)(1 + y^2)yc\tilde{b} = \left\langle z, y^2\right\rangle^{+}yc\tilde{b} = \left\langle x, y^2\right\rangle^{+}yc\tilde{b}.\end{aligned}$$

Now $\left\langle x, y^2\right\rangle^{+}$ is central in $\mathbb{F}G$, since $\left\langle x, y^2\right\rangle \trianglelefteq G$. Moreover $(a, yc\tilde{b}) = (a, c)(a, b) \in y\left\langle y^2\right\rangle$. Hence $[a, \left\langle x, y^2\right\rangle^{+}yc\tilde{b}] = \left\langle x, y^2\right\rangle^{+}[a, yc\tilde{b}] = \left\langle x, y^2\right\rangle^{+}(1 + (a, yc\tilde{b}))yc\tilde{b}a = (G')^{+}yc\tilde{b}a \neq 0$. Therefore $\mathbb{F}G$ is not centre-by-metabelian in this case.

Case 6: $(a, C) = \langle xy\rangle$. Similarly as in case 5, we obtain an element $c \in C$ such that $(a, c) = xy$ and $z := (b, c) \notin \langle xy\rangle$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [ca + {}^{a}(ca), a + {}^{c}a] &= [(1 + xy)ca, (1 + xy^{-1})a]\\ &= (1 + xy)(1 + xy)caa + (1 + xy^{-1})(1 + xy^{-1})aca\\ &= (1 + y^2)(ca + ac)a = (1 + y^2)(1 + xy)ca^2\\ &= \langle xy\rangle^{+}ca^2.\end{aligned}$$

Now $(b, ca^2) = (b, c)(b, a^2) = (b, c)(b, a)^2 = (b, c) = z$, and so $[b, \langle xy\rangle^{+}ca^2] = \langle xy\rangle^{+}(1 + (b, ca^2))ca^2b = \langle xy\rangle^{+}(1 + z)ca^2b = (G')^{+}ca^2b \neq 0$. So $\mathbb{F}G$ is also not centre-by-metabelian in this last case.

6.11. Lemma: *Let the notation be as in 6.5, and assume that the image of φ is $\langle \alpha^2 \rangle$. If $C' \not\subseteq \Phi(G')$, then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We may choose an element $a \in G$ with ${}^a h = \alpha^2(h) = h^{-1}$ for all $h \in G'$. Then $G/C = \langle aC \rangle \cong Z_2$ and $C' \subseteq \mathcal{Z}(G) \cap G' = \langle x, y^2 \rangle \cong Z_2 \times Z_2$.

Since $C' \not\subseteq \Phi(G') = \langle y^2 \rangle$, there are elements $c, \tilde{c} \in C$ such that $|\langle (c, \tilde{c}) \rangle| \notin \langle y^2 \rangle$. For the homomorphism $(c, .)\colon C \to \langle x, y^2 \rangle$ this implies that $U := (c, .)^{-1}(\langle y^2 \rangle) < C$.

Now $G' = (a, C)C'$ implies that $(a, C) \not\subseteq \langle x, y^2 \rangle$. Since the map $(a, .) : C \to G'$ is a homomorphism, this shows that $V := (a, .)^{-1}(\langle x, y^2 \rangle) < C$.

Therefore we may choose an element $d \in C \setminus (U \cup V) \neq \emptyset$. Then $(c, d) \in x \langle y^2 \rangle$, and $(a, d) \in y \langle x, y^2 \rangle$; w.l.o.g. $(c, d) = x$, $(a, d) = y$ (rename x and y if necessary). We compute

$$\begin{aligned} (\mathbb{F}G)'' \ni [d + {}^c d, a + {}^d a] &= [(1 + x)d, (1 + y^{-1})a] \\ &= (1 + x)(1 + y^{-1})(da + ad) \\ &= (1 + x)(1 + y^{-1})(1 + y^{-1})ad \\ &= (1 + x)(1 + y^2)ad = \langle x, y^2 \rangle^+ ad, \end{aligned}$$

and $[d, \langle x, y^2 \rangle^+ ad] = \langle x, y^2 \rangle^+ [d, a]d = \langle x, y^2 \rangle^+ (1 + y)dad = (G')^+ dad \neq 0$. This shows that $\mathbb{F}G$ is not centre-by-metabelian.

6.12. Theorem (summary): *Let G be a group with $|G'| = 8$. Then $\mathbb{F}G$ is centre-by-metabelian if and only if one of the following holds:*

(i) $G' \cong Z_2 \times Z_2 \times Z_2$, and G acts trivially on G',
(ii) $G' \cong Z_2 \times Z_4$, $\mathcal{C}_G(G')' \subseteq \Phi(G')$, and G acts dihedrally on G',
(iii) G contains an abelian subgroup of index 2.

Remark: Recall that in case (iii), G acts dihedrally on G', and $\mathcal{C}_G(G')$ is the mentioned abelian subgroup of index 2 (unless $\mathrm{cl}(G) \leq 2$, cf. 2.10).

7. Commutator subgroups of order 16

7.1. Remark: Let us assume that G is a counterexample to our main theorem 4 such that $|G'| = 16$. Then $\mathbb{F}G$ is centre-by-metabelian. By section 5, G' is isomorphic to $Z_4 \times Z_4$ or $Z_2 \times Z_8$ or $Z_2 \times Z_2 \times Z_4$.

Suppose first that $G' \cong Z_4 \times Z_4$. Then by 5.4, we only have to study one particular action of G on G'; this turns out to be the dihedral action; i.e. $|G : C| = 2$ for $C := \mathcal{C}_G(G')$, and ${}^{a}h = h^{-1}$ for all $a \in G \setminus C$, $h \in G'$. Fix an element $a \in G \setminus C$. Then $G' = (a, C)$ by 1.6, since $C' \subseteq G' \cap \mathcal{Z}(G) = \Phi(G')$. Consequently $(a, .)\colon\ C \to G'$ is an epimorphism.

If C is abelian, then G is not a counterexample since $|G : C| = 2$. Therefore $\mathcal{Z}(C) < C$. Since also $U := (a, .)^{-1}(\Phi(G')) < C$, we may choose an element $c \in C \setminus (U \cup \mathcal{Z}(C)) \neq \emptyset$.

We set $x := (a, c) \notin \Phi(G')$. Then $V := (a, .)^{-1}(\langle x, \Phi(G')\rangle) < C$ and $W := \mathcal{C}_C(c) < C$. Choose an element $d \in C \setminus (V \cup W) \neq \emptyset$.

If we set $y := (a, d)$, then $G' = \langle x, y\rangle$, and $(c, d) \in \left\langle x^2, y^2\right\rangle \setminus \{1\}$. Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [d + {}^{a}d, ca + {}^{a}(ca)] &= [(1 + y)d, (1 + x)ca] \\ &= (1 + x)\left((1 + y)dca + (1 + y^{-1})(ca, d)dca\right) \\ &= (1 + x)\left((1 + y) + (1 + y^{-1})(c, d)y\right) dca \\ &= (1 + x)(1 + y)(1 + (c, d))dca =: \tau.\end{aligned}$$

If $(c, d) = x^2$, then $\tau = dc(1 + y)\langle x\rangle^{+}a$, and hence

$$[y, \tau] = dc(1 + y)\langle x\rangle^{+}[y, a] = dc(1 + y)\langle x\rangle^{+}(1 + y^2)ya = dc(G')^{+}a \neq 0,$$

contradiction.

Consequently $\tilde{y}^2 := (c, d) \in \{y^2, x^2y^2\}$. Then $\tau = dc(1 + x)(1 + y)(1 + \tilde{y}^2)a$, and

$$[x, \tau] = dc(1 + x)(1 + y)(1 + \tilde{y}^2)[x, a] = dc(1 + x)(1 + y)(1 + \tilde{y}^2)(1 + x^2)xa = dc(G')^{+}a \neq 0,$$

contradiction.

Therefore $G' \ncong Z_4 \times Z_4$.

7.2. Remark: Let us again start with a counterexample G to our main theorem, and suppose that $G' = \langle x, y\rangle \cong Z_2 \times Z_8$, where $x^8 = 1 = y^2$. Then $\mathbb{F}G$ is centre-by-metabelian, and all subgroups of index 2 in G are nonabelian.

Set $C := \mathcal{C}_G(G')$, and map G/C to $\mathrm{Aut}(G') \cong Z_2 \times D_8$ in the usual way. The reductions of the algorithm described in 5.4 give the following subgroup lattice of possible images of

G/C in $\operatorname{Aut}(G')$:

$$\begin{tikzcd}
& \langle\alpha,\beta,\gamma\rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\alpha\beta,\alpha\gamma\rangle \sim \langle\alpha\beta,\gamma\rangle \arrow[dr, dash] & \langle\alpha\gamma,\alpha\beta\gamma\rangle \arrow[d, dash] & \langle\alpha,\gamma\rangle \sim \langle\alpha,\beta\gamma\rangle \arrow[dl, dash] \\
& \langle\alpha\gamma\rangle \sim \langle\alpha\beta\gamma\rangle &
\end{tikzcd}$$

Here $\langle\alpha,\beta,\gamma\rangle \cong Z_2 \times Z_2 \times Z_2$, where

$$\begin{aligned}
\alpha&\colon\ G' \to G',\, x \mapsto x^3,\, y \mapsto y,\\
\beta&\colon\ G' \to G',\, x \mapsto x^5,\, y \mapsto y,\\
\gamma&\colon\ G' \to G',\, x \mapsto x,\ \ y \mapsto yx^4.
\end{aligned}$$

Note that $(\alpha\gamma, G') = (\langle\alpha,\beta,\gamma\rangle, G') = \langle x^2\rangle = \Phi(G')$. So in any case we have $(G,G') = \Phi(G')$, i.e. $G/\Phi(G')$ has class 2. Then by 3.1 (ii), $\langle g,h\rangle' \,\Phi(G')/\Phi(G') = \langle (g,h)\rangle\, \Phi(G')/\Phi(G')$ for all $g,h \in G$. Hence $\langle g,h\rangle' \subseteq \langle (g,h)\rangle\, \Phi(G')$; in particular:

$$(*) \qquad \forall g,h \in G\colon\ |\langle (g,h)\rangle| = 8 \implies \langle g,h\rangle' = \langle (g,h)\rangle\,.$$

Assumption: $|G:C| \geq 4$.

Let $a,b \in G$ such that $|\langle (a,b)\rangle| = 8$. By renaming x and y if necessary, we may assume that $(a,b) = x$ (note however that this "fixes" the image of G/C in $\operatorname{Aut}(G')$ in the sense that we may not replace $\varphi(G/C)$ by a conjugate subgroup as described in 5.1).

Set $H := \langle a,b\rangle$, then $H' = \langle x\rangle$ by $(*)$. Now 6.12 implies that H acts dihedrally on H'. In particular, $|H : \mathcal{C}_H(x)| = 2$; w.l.o.g. $H/\mathcal{C}_H(x) = \langle a\mathcal{C}_H(x)\rangle$. Then ${}^{b}x = x$ or ${}^{b}x = {}^{a}x$. In the latter case, $ba \in \mathcal{C}_H(x)$. Since $(a,b) = (a,ba)$, we may replace b by ba, and thus assume that $b \in \mathcal{C}_H(x)$.

Now $|G:C| \geq 4$ implies that there is an element $g \in G$ such that $4 = |\langle aC, gC\rangle|$. If $bC \in \langle aC\rangle$, then $\langle aC, gC\rangle = \langle aC, gbC\rangle$, and either (a,g) or $(a,bg) = (a,b)\,{}^{b}(a,g) = x(a,g)$ has order 8, w.l.o.g. $|\langle (a,g)\rangle| = 8$. So after replacing b by g if necessary and working through the preceding paragraphs again, we may assume that $|\langle aC, bC\rangle| = 4$, $(a,b) = x$, ${}^{a}x = x^{-1}$, and ${}^{b}x = x$. Hence $\varphi(aC) \in \{\alpha\beta, \alpha\beta\gamma\}$, and $\varphi(bC) = \gamma$.

Set $K := \langle a,b,y\rangle$. Note that $(G,y) = \langle x^4\rangle$, so $K' = H' = \langle x\rangle$. By 6.12, $\mathcal{C}_K(x)$ must be abelian. But $b,y \in \mathcal{C}_K(x)$, and $(b,y) = (\gamma,y) = x^4 \neq 1$, contradiction.

This shows that $|G:C| = 2$.

Then G/C is mapped onto $\langle\alpha\gamma\rangle$ or $\langle\alpha\beta\gamma\rangle$. Now $\mathcal{C}_{G'}(\alpha\gamma) = \mathcal{C}_{G'}(\alpha\beta\gamma) = \langle yx^2\rangle$, i.e. $C' \subseteq \mathcal{Z}(G) \cap G' = \langle yx^2\rangle \cong Z_4$. If $C' = 1$, then C is an abelian subgroup of index 2 in G, and G is not a counterexample. If $|C'| = 2$, then $\mathbb{F}G$ is not centre-by-metabelian by lemma 5.3, so G is also not a counterexample. Hence $C' = \langle yx^2\rangle$.

Set $N := \langle x^4\rangle = \Phi(\Phi(G')) \trianglelefteq G$, and $\bar{H} := HN/N$ for all $H \leq G$, and $\bar{g} := gN$ for all $g \in G$. Then $\bar{G}' \cong Z_2 \times Z_4$, and $\langle \bar{x}\bar{y}^2\rangle = \bar{C}' \subseteq \mathcal{C}_{\bar{G}}(\bar{G}')'$; in particular, $\mathcal{C}_{\bar{G}}(\bar{G}')' \nsubseteq \Phi(\bar{G}') = \langle \bar{x}^2\rangle$. By 6.12, $\mathbb{F}\bar{G}$ is not centre-by-metabelian, contradiction.

This shows that $G' \not\cong Z_2 \times Z_8$.

7.3. Remark: Let G be a group with $G' = \langle x, y, z\rangle \cong Z_2 \times Z_2 \times Z_4$, where $x^2 = y^2 = z^4 = 1$.

As usual, set $C := \mathcal{C}_G(G')$ and map G/C to $\operatorname{Aut}(G')$. By 5.4, G may only be a counterexample to the main theorem, if the image of G/C is (conjugate to) one of the following elementary abelian groups:

$$\langle\alpha\rangle\,,\quad \langle\beta,\gamma\rangle\,,\quad \langle\alpha,\beta,\gamma\rangle\,,\qquad \text{where}$$

$$\begin{aligned}
\alpha &\colon G' \to G',\, x \mapsto x, \quad\, y \mapsto y, \quad\, z \mapsto z^3,\\
\beta &\colon G' \to G',\, x \mapsto xz^2,\, y \mapsto y, \quad\, z \mapsto z,\\
\gamma &\colon G' \to G',\, x \mapsto x, \quad\, y \mapsto yz^2,\, z \mapsto z.
\end{aligned}$$

(In fact, $\langle\alpha\rangle$ and $\langle\alpha,\beta,\gamma\rangle$ are normal in $\operatorname{Aut}(G')$, while $\langle\beta,\gamma\rangle$ is not.)

We will study those cases in 3 separate lemmata.

7.4. Lemma: *Given the notation of 7.3, suppose that $|G : C| = 2$, and that $\mathbb{F}G$ is centre-by-metabelian. Then G contains an abelian subgroup of index 2.*

Proof: By 7.3, G/C is mapped onto $\langle\alpha\rangle$.

By 1.3, $C' \subseteq \mathcal{Z}(G) \cap G' = \left\langle x, y, z^2\right\rangle$. Set $N := \langle x\rangle \trianglelefteq G$. Then $G'/N \cong Z_2 \times Z_4$. Since $\mathbb{F}[G/N]$ is centre-by-metabelian, 6.12 implies that $C'/N \subseteq \mathcal{C}_{G/N}(G'/N)' \subseteq \Phi(G'/N) = \left\langle z^2N\right\rangle$. Therefore $C' \subseteq \left\langle x, z^2\right\rangle$. Similarly $C' \subseteq \left\langle y, z^2\right\rangle$, so together we have $C' \subseteq \left\langle x, z^2\right\rangle \cap \left\langle y, z^2\right\rangle = \left\langle z^2\right\rangle \cong Z_2$.

Now lemma 5.3 implies that $|C'| \neq 2$. Hence $C' = 1$, and C is abelian.

7.5. Lemma: *Given the notation of 7.3, suppose that $|G : C| = 4$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: By 7.3 and 5.1, we may assume that G/C is mapped onto $\langle\beta,\gamma\rangle$. Then $C' \subseteq \mathcal{Z}(G) \cap G' = \langle z\rangle$. We write $G/C = \langle aC, bC\rangle$ where ${}^a h = \gamma(a)$, ${}^b h = \beta(h)$ for all $h \in G'$. Then

$$\begin{aligned}
{}^a x = x \quad {}^a y = yz^2\, {}^a z = z,\\
{}^b x = xz^2\, {}^b y = y \quad\; {}^b z = z.
\end{aligned}$$

Set $H := \langle b, C\rangle$. Then $H' = (b, C)C'$ and $C \subseteq \mathcal{C}_H(H')$.

Case 1: $H' = G'$. Then H does not act dihedrally on H', hence C cannot be abelian by remark 1.7, so by lemma 7.4, $\mathbb{F}H$ is not centre-by-metabelian.

Case 2: $H' \cong Z_2 \times Z_2 \times Z_2$. Then $H' = \left\langle x, y, z^2\right\rangle$, hence $b \in H \smallsetminus \mathcal{C}_H(H')$, and so $\operatorname{cl}(H) > 2$. By 6.12, $\mathbb{F}H$ is not centre-by-metabelian.

Case 3: $H' \cong Z_2 \times Z_4$.

If H does not act dihedrally on H', or if $C' \not\subseteq \Phi(H')$, then $\mathbb{F}H$ is not centre-by-metabelian by 6.12.

So we may assume that ${}^{b}h = h^{-1}$ for all $h \in H'$, and that $C' \subseteq \langle z^2 \rangle$. It is easy to check that $\{h \in G' : {}^{b}h = h^{-1}\} = \langle y, xz \rangle$. Therefore $\langle y, xz \rangle = H' = (b, C)C' = (b, C)$, i.e. $(b, .) \colon C \to H'$ is an epimorphism.

Now if $(a, b) \notin H'$, then $(a, b) \in xH'$. Note that $(ca, b) = (c, b)(a, b)$ for all $c \in C$, so by replacing a by a suitable element of Ca if necessary, we may assume that $(a, b) = x = (b, a)$. Let $c \in C$ such that $(b, c) = y = (c, b)$. Then

$$\begin{aligned}
(\mathbb{F}G)'' \ni [a + {}^{b}a, b + {}^{c}b] &= [(1 + x)a, (1 + y)b] \\
&= (1 + x)(1 + yz^2)ab + (1 + y)(1 + xz^2)ba \\
&= (1 + x)(1 + yz^2)xba + (1 + y)(1 + xz^2)ba \\
&= \left(x + yz^2 + y + xz^2\right) ba \\
&= (x + y)(1 + z^2)ba = x\langle xy, z^2 \rangle^{+} ba,
\end{aligned}$$

and $[a, x\langle xy, z^2 \rangle^{+} ba] = x\langle xy, z^2 \rangle^{+}[a, b]a = x\langle xy, z^2 \rangle^{+}(1 + x)ba^2 = \langle x, y, z^2 \rangle^{+} ba^2 \neq 0$, i.e. $\mathbb{F}H$ is not centre-by-metabelian.

Hence we may assume that $(a, b) \in H' = (b, C)$. As above, we may replace a by a suitable element of Ca and assume that $(a, b) = 1$.

Then $G' = \langle (a, b) \rangle\, (a, C)(b, C)C' = (a, C)H'$. Since $G' \nsubseteq H'$, we have $(a, C) \nsubseteq H'$. Then $(a, .) \colon C \to G'$ is a homomorphism with $U := (a, .)^{-1}(H') < C$. Similarly, $(b, .) \colon C \to H'$ is an epimorphism, i.e. $V := (b, .)^{-1}(\langle y, z^2 \rangle) < C$. Let $c \in C \smallsetminus (U \cup V) \neq \emptyset$, then $(b, c) \in H'$ has order 4, and $(a, c) \notin H'$.

Then $z^2 \in \langle (a, c),\, (b, c) \rangle \cong Z_2 \times Z_4$. Since $G/\langle z^2 \rangle$ has class 2, also $\langle a, b, c \rangle / \langle z^2 \rangle$ has class 2. By 3.1 (ii), $\langle a, b, c \rangle' / \langle z^2 \rangle = \langle (a, b),\, (a, c),\, (b, c) \rangle / \langle z^2 \rangle = \langle (a, c),\, (b, c) \rangle / \langle z^2 \rangle$. Therefore $\langle a, b, c \rangle' = \langle (a, c),\, (b, c) \rangle$, in particular $\langle a, b, c \rangle' \cong Z_2 \times Z_4$. Now b does neither act trivially on $\langle a, b, c \rangle'$, since ${}^{b}(b, c) = (b, c)^{-1}$, nor dihedrally, since $(a, c) \notin H' = \{h \in G' \colon {}^{b}h = h^{-1}\}$. By 6.12, $\mathbb{F}\langle a, b, c \rangle$ is not centre-by-metabelian.

By the cases 1-3, we may assume that $|H'| \leq 4$. Furthermore $z^2 = (b, x) \in (b, C) \subseteq (b, C)C' = H'$.

For $K := \langle a, C \rangle$, we argue similarly as in the cases above to show that $|K'| \geq 8$ implies that $\mathbb{F}G$ is not centre-by-metabelian. So we may assume that $|K'| \leq 4$. Note that $z^2 = (a, y) \in (a, C)C' = K'$.

Then $|H'K'| \leq 8$. Now $G' = \langle (a, b) \rangle\, (a, C)(b, C)C' = \langle (a, b) \rangle\, H'K'$. For order reasons,

$$Z_2 \times Z_2 \times Z_2 \cong G'/\langle z^2 \rangle = \langle (a, b), z^2 \rangle / \langle z^2 \rangle \times H'/\langle z^2 \rangle \times K'/\langle z^2 \rangle ,$$

In particular, $C' \subseteq H' \cap K' = \langle z^2 \rangle$. Then $H' = (b, C)$, $K' = (a, C)$, and $|K'| = |H'| = 4$.

Suppose that $(b, C) \cong Z_4$. As usual, we find an element $c \in C$ such that $w := (b, c)$ has order 4, and $(a, c) \notin \langle w \rangle$. Note that $1 = (b^{-1}b, c) = {}^{b^{-1}}(b, c)(b^{-1}, c) = {}^{b}w(b^{-1}, c)$. Hence $(b^{-1}, c) \in \{w^{-1}, {}^{b}w^{-1}\} \subseteq \{w^{\pm 1}\}$. Since $(b^{-1}, c^{-1}) = (b^{-1}, c)^{-1}$, there is an element

$d \in \{c, c^{-1}\}$ such that $(b^{-1}, d) = w$. Then also $(cb^{-1}, d) = w$, and thus

$$\begin{aligned}(\mathbb{F}G)'' \ni [b + {}^{c^{-1}}b,\ cb^{-1} + {}^{d^{-1}}(cb^{-1})] &= [(1+w)b, (1+w)cb^{-1}] \\ &= (1+w)(1+{}^{b}w)bcb^{-1} + (1+w)(1+{}^{b}w)c \\ &= (1+w)(1+{}^{b}w)(c+{}^{b}c) \\ &= (1+w)(1+{}^{b}w)(1+w)c \\ &= (1+w^2)(1+w^{\pm 1}) = \langle w\rangle^{+}c,\end{aligned}$$

and $[a, \langle w\rangle^{+}c] = \langle w\rangle^{+}(1+(a,c))ca \neq 0$, so $\mathbb{F}G$ is not centre-by-metabelian.

Hence we may assume that $H' = (b, C) \cong Z_2 \times Z_2$, and similarly $K' = (a, C) \cong Z_2 \times Z_2$. Then $(a, b) \notin \langle x, y, z^2\rangle = H'K'$. As usual, we find elements $c, d \in C$ such that $(b, d) = z^2$, and $t := (b, c) \in H' \smallsetminus \langle z^2\rangle$, and $s := (a, c) \in K' \smallsetminus \langle z^2\rangle$. Then $\langle s, t, z^2\rangle = H'K' = \langle x, y, z^2\rangle$. Note that b commutes with s modulo $\langle z^2\rangle \subseteq \mathcal{Z}(G)$, so

$$\begin{aligned}(\mathbb{F}G)'' \ni [b + {}^{d}b, c + {}^{a}c] &= [(1+z^2)b, (1+s)c] = (1+z^2)(1+s)[b, c] \\ &= (1+z^2)(1+s)(1+t)cb = \langle z^2, s, t\rangle^{+}cb = \langle x, y, z^2\rangle^{+}cb.\end{aligned}$$

Since a and c commute modulo $\langle x, y, z^2\rangle$, we furthermore have

$$\begin{aligned}[a, \langle x, y, z^2\rangle^{+}cb] &= \langle x, y, z^2\rangle^{+}[a, cb] = c\langle x, y, z^2\rangle^{+}[a, b] \\ &= c\langle x, y, z^2\rangle^{+}(1+(a,b))ba = c(G')^{+}ba \neq 0.\end{aligned}$$

Hence $\mathbb{F}G$ is not centre-by-metabelian.

7.6. Lemma: *Given the notation of 7.3, suppose that $|G : C| = 8$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: By 7.3, G/C is mapped onto $\langle \alpha, \beta, \gamma\rangle = \langle \beta, \gamma, \alpha\beta\gamma\rangle$.

Choose elements $g, h, k \in G$ such that ${}^{g}v = \beta(v)$, ${}^{h}v = \gamma(v)$, ${}^{k}v = \alpha\beta\gamma(v)$ for all $v \in G'$. Then

$$\begin{aligned}&{}^{g}x = xz^2, &&{}^{g}y = y, &&{}^{g}z = z,\\ &{}^{h}x = x, &&{}^{h}y = yz^2, &&{}^{h}z = z,\\ &{}^{k}x = xz^2, &&{}^{k}y = yz^2, &&{}^{k}z = z^3.\end{aligned}$$

It is easy to check that

$$(*)\qquad \begin{aligned}&\mathcal{C}_{G'}(g) = \langle y, z\rangle, &&\{v \in G' :\ {}^{g}v = v^{-1}\} = \langle y, xz\rangle,\\ &\mathcal{C}_{G'}(h) = \langle x, z\rangle, &&\{v \in G' :\ {}^{h}v = v^{-1}\} = \langle x, yz\rangle,\\ &\mathcal{C}_{G'}(k) = \langle xy, xz\rangle, &&\{v \in G' :\ {}^{k}v = v^{-1}\} = \langle xy, z\rangle.\end{aligned}$$

Set $H := \langle g, h, C\rangle$. Then $H' = \langle (g, h)\rangle\,(g, C)(h, C)C'$ by 1.6. If $H' = G'$ then $\mathbb{F}H$ is not centre-by-metabelian by lemma 7.5. Hence we may assume that $|H'| \leq 8$. If $H' \cong Z_2 \times Z_2 \times Z_2$, then $H' = \langle x, y, z^2\rangle$. Since H does not act trivially on $\langle x, y, z^2\rangle$, the results of section 4 implies that $\mathbb{F}H$ is not centre-by-metabelian. Suppose next that $H' \cong Z_2 \times Z_4$. If $\mathbb{F}H$ was centre-by-metabelian, then by 6.12, $\langle g, h\rangle$ would act dihedrally on H', which is not possible by $(*)$. Hence we may assume that $|H'| \leq 4$.

If we set $K := \langle g, k, C\rangle$ and $L := \langle h, k, C\rangle$, we similarly may assume that

$$K' = \langle (g,k)\rangle\,(g,C)(k,C)C' \text{ and } \left|K'\right| \leq 4,$$
$$L' = \langle (h,k)\rangle\,(h,C)(k,C)C' \text{ and } \left|L'\right| \leq 4.$$

Note that $z^2 \in (g,G')\cap(h,G')\cap(k,G') \subseteq (g,C)\cap(h,C)\cap(k,C) \subseteq H'\cap L'\cap K'$. Moreover, since $G' = \langle (g,h),(g,k),(h,k)\rangle\,(g,C)(h,C)(k,C)C'$ by 1.6, we have $G' = H'K'L'$. For order reasons,

$$Z_2 \times Z_2 \times Z_2 \cong G'/\left\langle z^2\right\rangle = H'/\left\langle z^2\right\rangle \times K'/\left\langle z^2\right\rangle \times L'/\left\langle z^2\right\rangle.$$

In particular,

$$(g,C)C' \subseteq H' \cap K' = \left\langle z^2\right\rangle = \Phi(G'),$$
$$(h,C)C' \subseteq H' \cap L' = \left\langle z^2\right\rangle,$$
$$(k,C)C' \subseteq K' \cap L' = \left\langle z^2\right\rangle.$$

Therefore $G' = \langle (g,h),(g,k),(h,k)\rangle$. Choose $r, s \in \{g,h,k\}$ such that $w := (r,s)$ has order 4, and let $t \in \{g,h,k\} \smallsetminus \{r,s\}$. Then $w^2 = z^2$, and

$$(**) \qquad G' = \langle (r,s),(r,t),(s,t)\rangle\,,\ (r,s) = w \text{ with } |\langle w\rangle| = 4.$$

Note that $(r,w),\ (s,w) \in (G,G') = \left\langle w^2\right\rangle$.

Assume first that $(r,w) = 1 = (s,w)$, then

$$\begin{aligned}(\mathbb{F}G)'' \ni [r + {}^{s}r, s + {}^{r}s] &= [(1+w^3)r,(1+w)s]\\ &= (1+w^3)(1+w)[r,s] = (1+w^3)(1+w)(1+w)sr\\ &= \langle w\rangle^{+}sr.\end{aligned}$$

Now $\langle w\rangle \trianglelefteq G$, i.e. $\langle w\rangle^{+} \in \mathcal{Z}(\mathbb{F}G)$. Moreover $(sr,t) \notin \langle w\rangle$. Hence

$$[t, \langle w\rangle^{+}sr] = \langle w\rangle^{+}[t,sr] = \langle w\rangle^{+}(1+(t,sr))srt \neq 0.$$

Therefore $\mathbb{F}G$ is not centre-by-metabelian in this case.

So we may w.l.o.g. assume that $(r,w) = w^2 = z^2$. By possibly replacing s by sr, we even may assume that $(s,w) = w^2$ (since $(r,sr) = (r,s)$ and $(sr,t) = {}^{s}(r,t)(s,t) \in \left\langle w^2,(r,t)\right\rangle(s,t) \subseteq \langle (r,s),(r,t)\rangle\,(s,t)$, this does not change $(**)$). Then

$$\begin{aligned}(\mathbb{F}G)'' \ni [r + {}^{s}r, s + {}^{r}s] &= [(1+w^3)r,(1+w)s]\\ &= (1+w^3)(1+w^3)rs + (1+w)(1+w)sr = (1+w^2)(rs+sr)\\ &= (1+w^2)(1+w)sr = \langle w\rangle^{+}sr.\end{aligned}$$

As before, $[t,\langle w\rangle^{+}sr] = \langle w\rangle^{+}(1+(t,sr))srt \neq 0$. Hence $\mathbb{F}G$ is also not centre-by-metabelian in this case.

7.7. Theorem (summary): *Let G be a group with $|G'| = 16$. Then $\mathbb{F}G$ is centre-by-metabelian if and only if G has an abelian subgroup of index* 2.

8. Finish

8.1. Lemma: *Let $\mathbb{F}G$ be a centre-by-metabelian group algebra. If G' is a finite 2-group of order at least 16, then G has an abelian subgroup of index 2.*

Proof: We argue by induction on $|G'|$. By the results of section 7, we may assume that $|G'| \geq 32$. Set $C := \mathcal{C}_G(G')$. Note that G/C is finite, since G' is finite.

It suffices to show that $G' \cap \mathcal{Z}(G) \neq 1$, because then we may proceed as follows: Choose an involution $z \in G' \cap \mathcal{Z}(G)$, and set $N := \langle z \rangle$. Then $N \trianglelefteq G$, and $|(G/N)'| = |G'|/2 \geq 16$. By induction, G/N has an abelian subgroup A/N of index 2, i.e. $|G : A| = 2$ and $|A'| \leq 2$. Now 5.3 implies $|A'| \neq 2$, and we are done.

If $\Phi(G') = 1$, then G' is elementary abelian, i.e. $1 \neq G' \subseteq \mathcal{Z}(G)$ by the summary of section 4. Hence we may assume that $\Phi(G') \neq 1$.

If G/C is a 2-group, then $G' \rtimes G/C$ is also a (finite) 2-group, and $(G' \rtimes 1) \cap \mathcal{Z}(G' \rtimes G/C) \neq 1$, i.e. $G' \cap \mathcal{Z}(G) \neq 1$.

So suppose that G/C is not a 2-group. Then by 5.2, G/C has a Hall $2'$-subgroup which centralizes $\Phi(G')$. Therefore $G/\mathcal{C}_G(\Phi(G'))$ is a finite 2-group, and similarly as above, we find that $1 \neq \Phi(G') \cap \mathcal{Z}(G) \subseteq G' \cap \mathcal{Z}(G)$.

8.2. Remark: The preceding lemma shows that if G is a counterexample to the main theorem 4, then G' is not a finite 2-group. Then, by theorem 1, G contains a subgroup A of index 2 such that A' is a finite 2-group. We set

$$\mathfrak{A}(G) := \big\{ A \leq G \colon\ |G : A| = 2 \text{ and } A' \text{ is a finite 2-group} \big\} \neq \emptyset,$$
$$\mathfrak{a}(G) := \min \big\{ |A'| \colon\ A \in \mathfrak{A}(G) \big\} \in \mathbb{N},$$

and we have to show that if $\mathbb{F}G$ is centre-by-metabelian, then $\mathfrak{a}(G) = 1$.

But before we do so in 8.4, let us quickly insert another lemma:

8.3. Lemma: *Let G be a group with a normal subgroup U that is isomorphic to V_4. Set $C := \mathcal{C}_G(U)$, and let $\varphi : G/C \to \mathrm{Aut}(U) \cong S_3$ be the usual monomorphism. If φ is surjective, then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We write $\langle x, y \rangle = U \cong V_4$. If φ is surjective, then there are elements $g, h \in G$ with ${}^{g}x = y$, ${}^{g}y = x$, ${}^{h}x = y$, ${}^{h}y = xy$. Set $a := (g, h)$, then ${}^{a}x = y$ and ${}^{a}y = xy$; in particular, $a \in G \smallsetminus U$. Then

$$\begin{aligned} \rho := [x + {}^{a}x, h + {}^{g}h] &= [x + y, h + (g,h)h] = (x+y)(h+ah) + (h+ah)(x+y) \\ &= (x+y)h + (x+y)ah + (y+xy)h + (xy+x)ah = (x + ya + xy + xya)h, \end{aligned}$$

and

$$\begin{aligned} [x, \rho] &= [x, (x+xy)h] + [x, (y+xy)ah] = (x+xy)[x,h] + (y+xy)[x,ah] = \\ &= (x+xy)(1+(h,x))xh + (y+xy)(1+(ah,x))xah = \\ &= \left((x+xy)(1+xy)x + (y+xy)(1+y)xa\right) h = \big(U^{+} + U^{+}a\big)\, h \neq 0. \end{aligned}$$

8.4. Lemma: *Let G be a group. Suppose that G' is not a finite 2-group, and that $\mathfrak{a}(G) \geq 2$. Then $\mathbb{F}G$ is not centre-by-metabelian.*

Proof: We argue by induction on $\mathfrak{a}(G)$, which clearly is a power of 2. If $\mathfrak{a}(G) = 2$, then $\mathbb{F}G$ is not centre-by-metabelian by 5.3.

So we may assume that $\mathfrak{a}(G) \geq 4$. Let $A \in \mathfrak{A}(G)$ such that $|A'| = \mathfrak{a}(G)$.

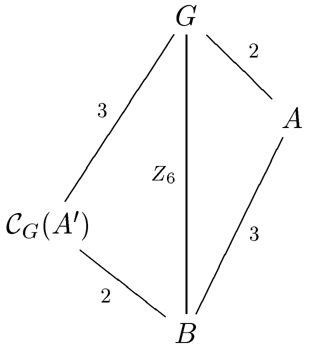
Assume there is a normal subgroup N of G with $1 < N < A'$. Then also $(G/N)' = G'/N$ is not a finite 2-group. Let $B/N \in \mathfrak{A}(G/N)$ with $|(B/N)'| = \mathfrak{a}(G/N)$. Since then $B \in \mathfrak{A}(G)$ and $A/N \in \mathfrak{A}(G/N)$, we have $\mathfrak{a}(G)/\left|N\right| \leq |B'N| / |N| = |(B/N)'| = \mathfrak{a}(G/N) \leq |A' : N| = \mathfrak{a}(G)/\left|N\right|$; in particular $1 < \mathfrak{a}(G/N) < \mathfrak{a}(G)$. By induction, $\mathbb{F}[G/N]$ is not centre-by-metabelian, and we are done.

So we may assume that A' is a minimal normal (2-)subgroup of G. Then $\Phi(A') = 1$, so A' is elementary abelian.

Assume $\mathrm{cl}(A) = 2$; i.e. $A \subseteq \mathcal{C}_G(A')$. In this case, A' may be regarded as an $\mathbb{F}_2[G/A]$-module. Let N be a simple submodule of A'. Then $N \cong Z_2$, since $G/A \cong Z_2$. But then $N \trianglelefteq G$ and $N < A'$ in contradiction to the minimality of A'.

Consequently $\mathrm{cl}(A) \geq 3$. If $|A'| \geq 8$, then $\mathbb{F}A$ is not centre-by-metabelian by the summary of section 4. Therefore we may assume that $|A'| \leq 4$, in fact $|A'| = 4$, i.e. $A' \cong V_4$.

The action of G on A' gives a monomorphism $\varphi\colon\ G/\mathcal{C}_G(A') \to \mathrm{Aut}(A') \cong S_3$. By 8.3, we may assume that φ is not surjective. If $|G : \mathcal{C}_G(A')| = 2$, we again find a (trivial) simple submodule N of the $\mathbb{F}_2[G/\mathcal{C}_G(A')]$-module A' in contradiction to the minimality of A'. Therefore $|G : \mathcal{C}_G(A')| = 3$. Then $G' \subseteq A \cap \mathcal{C}_G(A') =: B$, and $G/B \cong Z_6$.



We write $G = \langle g, B\rangle$. Then $g^6 \in B$, $g^3 \in \mathcal{C}_G(A')$, $g^2 \in A$. We also may write $A' = \langle x, y\rangle$ with ${}^g x = y$ and ${}^g y = xy$. Then

$$(\mathbb{F}G)'' \ni [g + {}^x g, x + {}^g x] = [(1+xy)g, x+y] = (1+xy)(x+y+y+xy)g = (A')^+ g.$$

Clearly $G = \langle g, A\rangle$, so by 1.6, $G' = (g, A)A'$. Since $G' > A'$, there is an element $a \in A$ with $(g, a) \notin A'$. But then

$$[\mathbb{F}G, (\mathbb{F}G)''] \ni [a, (A')^+ g] = (A')^+ [a, g] = (A')^+ (1 + (g,a))ag \neq 0.$$

9. Applications to the unit group

Let $\mathbb{F}$ be a field of *(at first arbitrary)* characteristic $p \geq 0$.

9.1. Remark: (i) It is well-known that the functor $\mathbb{F}[\,.\,]$ from the category of groups to the category of $\mathbb{F}$-algebras, that assigns to each group G the group algebra $\mathbb{F}[G]$, is a left adjoint of the functor $\mathcal{U}$ in the converse direction, which assigns to each $\mathbb{F}$-algebra A its unit group $\mathcal{U}(A)$. So far we have focused on the one direction; in this section we will apply our results to the other: Namely we will show that a centre-by-metabelian group algebra in characteristic $p = 2$ need not have a centre-by-metabelian unit group; even worse: it may not be solvable at all. This is contrary to the case $p \neq 2$.

(ii) Several commutator properties of the unit group $\mathcal{U}(A)$ do go along with the commutator properties of an algebra A. E.g., if A is Lie nilpotent, then $\mathcal{U}(A)$ is nilpotent, where the class of $\mathcal{U}(A)$ is bounded by the class of A [**4**]. Or, if A is metabelian, then so is $\mathcal{U}(A)$ [**23**]. And if $p \neq 2$, then every Lie solvable group algebra has a solvable unit group [**19**, V.6.17].

(iii) More exactly, it is shown in [**23**] that for any algebra A, we have $\delta^n(\mathcal{U}(A)) - 1 \subseteq \delta^n(A) \cdot A = A \cdot \delta^n(A)$ for $n = 0, 1, 2$.

(iv) The question, whether $\mathcal{U}(A)$ is necessarily centre-by-metabelian, if only A is centre-by-metabelian, was raised in [**23**]. As already mentioned, this is true if A is a centre-by-metabelian group algebra in the case $p \neq 2$. This is clear for $p \notin \{2, 3\}$, since by [**23**] (theorem 3 (i)), all centre-by-metabelian group algebras are in fact abelian. The result for $p = 3$ is shown in [**7**]. (It is not known whether the same is true for other $\mathbb{F}$-algebras than group algebras.)

(v) An example of a centre-by-metabelian algebra A in characteristic $p = 2$ with unit group $\mathcal{U}(A)$ that is not centre-by-metabelian is given in [**24**]. There, A is a factor algebra of some power series algebra.

From now on, *let* $p = 2$ *again,* and let us examine what happens if A is a group algebra:

9.2. Lemma: *Let G be a group that satisfies either condition (i) or (ii) of theorem 4. Then $\mathcal{U}(\mathbb{F}G)$ is centre-by-metabelian.*

Remark: Recall that satisfying condition (i) means that $|G'| \bigm| 4$, and condition (ii) requires that $Z_2 \times Z_2 \times Z_2 \cong G' \subseteq \mathcal{Z}(G)$.

Proof: By the lemmata 2.2–2.4, we have $(\mathbb{F}G)'' \cdot \mathbb{F}G \subseteq (G')^+ \cdot \mathbb{F}G \subseteq \mathcal{Z}(\mathbb{F}G)$. By 9.1 (iii), $\mathcal{U}(\mathbb{F}G)'' - 1 \subseteq (\mathbb{F}G)'' \cdot \mathbb{F}G$. Hence $\mathcal{U}(\mathbb{F}G)'' \subseteq \mathcal{U}(\mathbb{F}G) \cap \mathcal{Z}(\mathbb{F}G) \subseteq \mathcal{Z}(\mathcal{U}(\mathbb{F}G))$.

9.3. Example: Now we will construct a group G that satisfies the conditions (iii) and (iv) of theorem 4, but $\mathcal{U}(\mathbb{F}G)$ is not centre-by-metabelian. Recall that a group G satisfies both of these conditions, if and only if it acts dihedrally on $G' \cong Z_2 \times Z_4$, and $\mathcal{C}_G(G')$ is abelian.

Let $C := \langle c, d, x \rangle \cong Z_8 \times V_4$, where $c^8 = d^2 = x^2 = 1$. Then $a : C \to C$, $c \mapsto c^3$, $d \mapsto dx$, $x \mapsto x$, defines an automorphism of order 2 with $(a, c) = c^2 =: y$, $(a, d) = x$, $(a, x) = 1$, and $(a, y) = (a, c^2) = c^4 = y^2$. So $G := C \rtimes \langle a \rangle$ is a group of order 64 with $G' = \langle x, y \rangle \cong Z_2 \times Z_4$. Moreover, $\mathcal{C}_G(G') = C$ is abelian, and ${}^a x = x = x^{-1}$ and ${}^a y = y^3 = y^{-1}$, i.e. G acts in a dihedral manner on G'.

By theorem 4, $\mathbb{F}G$ is centre-by-metabelian. We will show that $U := \mathcal{U}(\mathbb{F}G)$ is not. The following statements may be checked by direct expansion:

$$\begin{aligned}
(1+a+c)^{-1} &= 1 + y^2 + y^3 + c + y^2a + y^3a + ya + y^3ca + y^2ca, \\
(1+a+c,\, d) &= 1 + y + y^2 + y^3 + xy + xy^2 + xy^3 + y^2c + y^3c + xy^2c + xy^3c \\
&\quad + a + ya + y^2a + xa + xya + xy^2a + yca + xyca \\
&= (1+a+c,\, d)^{-1}, \\
((1+a+c,\, d),\, (a,c)) &= 1 + ya + y^3a + xya + xy^3a + yca + y^3ca + xyca + xy^3ca \\
&= ((1+a+c,\, d),\, (a,c))^{-1}, \\
(a,\, (1+a+c,\, d),\, (a,c)) &= 1 + (G')^+ca \neq 1.
\end{aligned}$$

This shows that $(U, U'') \neq 1$, hence U is not centre-by-metabelian.

However, U still has derived length 3, as the following lemma shows.

9.4. Lemma: *Let G be a group that satisfies condition (iii) of theorem 4, and let $U := \mathcal{U}(\mathbb{F}G)$. Then U' is nilpotent of class at most 2. In particular, U is solvable of derived length at most 3.*

Proof: Note that we are in the situation of lemma 2.5. So let us adopt the notation used in its proof, and let us restate some of the facts we have established there: $\omega(\mathbb{F}G')^5 = 0$, $\omega(\mathbb{F}G')^4\,\mathbb{F}G \subseteq \mathcal{Z}(\mathbb{F}G)$, and $(\mathbb{F}G)'' \subseteq \omega(\mathbb{F}G')^4\,\mathbb{F}G + X\,\mathbb{F}G$, where $X := \{\sigma h + {}^a\sigma\colon\ \sigma \in \omega(\mathbb{F}G')^2,\ h \in G'\}$. Recall that $G' = \langle x, y \rangle$, $C := \mathcal{C}_G(G')$, and $G/C = \langle aC \rangle$.

We have to show that $(U', U'') = 1$, or equivalently, $[U', U''] = 0$. By 9.1 (iii), we have $U' + 1 \subseteq (\mathbb{F}G)'\,\mathbb{F}G \subseteq \omega(\mathbb{F}G')\,\mathbb{F}G$, and $U'' + 1 \subseteq (\mathbb{F}G)''\,\mathbb{F}G$. So it suffices to show that $[\omega(\mathbb{F}G')\,\mathbb{F}G,\ X\,\mathbb{F}G] = 0$.

By [**16**, lemma 3.1.1], $\omega(\mathbb{F}G')\,\mathbb{F}G = \{1+x,\ 1+y\}\,\mathbb{F}G$, and $\omega(\mathbb{F}G')^2\,\mathbb{F}G = \{(1+x)(1+y),\ 1+y^2\}\,\mathbb{F}G$. We are going to check that

$$[\tau f,\ (\sigma h + {}^a\sigma)g] = 0$$

for all $f, g \in G$, $h \in G'$, $\tau \in \{1+x,\ 1+y\}$, $\sigma \in \{(1+x)(1+y),\ 1+y^2\}$.

First, since $x \in \mathcal{Z}(G)$ and $x^2 = 1$, we have $[(1+x)f,\ ((1+x)(1+y)h + (1+x)(1+y^3))g] = (1+x)(1+x)[f,\ (1+y)hg + (1+y^3)g] = 0$.

Recall that h commutes with f modulo $\langle y^2 \rangle$, hence

$$\begin{aligned}
[(1+x)f,\ ((1+y^2)h + (1+y^2))g] &= (1+x)(1+y^2)[f,\ (h+1)g] \\
&= (1+x)(1+y)^2(h+1)[f,\ g] \in \omega(\mathbb{F}G')^4\,(\mathbb{F}G)'\,\mathbb{F}G \subseteq \omega(\mathbb{F}G')^5\,\mathbb{F}G = 0.
\end{aligned}$$

Observe next that for $y_1,\ y_2 \in \langle y \rangle$, we have $(1+y_1)(1+y_2) \in \{0,\ (1+y^2),\ (1+y^2)y\}$. So there are $i,\ j \in \{0,1\}$ with $(1+y)(1+{}^f y) = (1+y^2)y^i$, and $(1+y)(1+{}^g y) = (1+y^2)y^j$.

Recall also that $(1+y^2)y^3 = (1+y^2)y$ and $(1+y^2)\,{}^{f}h = (1+y^2)h$. Then

$$\begin{aligned}
[(1+y)f,\, ((1+x)(1+y)h + (1+x)(1+y^3))g] &= (1+x)[(1+y)f,\, (1+y)hg + (1+y^3)g] \\
&= (1+x)\big((1+y)(1+\,{}^{f}y)\,{}^{f}hfg + (1+y)(1+\,{}^{f}y^3)fg \\
&\qquad + (1+y)(1+\,{}^{g}y)hgf + (1+y^3)(1+\,{}^{g}y)gf\big) \\
&= (1+x)\big((1+y^2)y^i\,{}^{f}hfg + (1+y)(1+\,{}^{f}y)\,{}^{f}y^3fg \\
&\qquad + (1+y^2)y^jhgf + y^3(1+y)(1+\,{}^{g}y)gf\big) \\
&= (1+x)\big((1+y^2)y^ihfg + (1+y^2)y^i\,{}^{f}y^3fg + (1+y^2)y^jhgf + (1+y^2)y^jy^3gf\big) \\
&= (1+x)(1+y^2)\,\big(y^ihfg + y^iyfg + y^jhgf + y^jygf\big) \\
&= (1+x)(1+y^2)\,\big(y^i(h+y)fg + y^j(h+y)gf\big) \\
&= (1+x)(1+y^2)(h+y)(y^ifg + y^jgf) \\
&= (1+x)(1+y)^2(h+y)(y^i(f,g) + y^j)gf \in \omega(\mathbb{F}G')^5\,\mathbb{F}G = 0.
\end{aligned}$$

Finally,

$$\begin{aligned}
[(1+y)f,\, ((1+y^2)h + (1+y^2))g] &= (1+y^2)[(1+y)f,\, (h+1)g] \\
&= (1+y^2)(1+y)(h+1)[f,\, g] \in \omega(\mathbb{F}G')^4\,(\mathbb{F}G)'\,\mathbb{F}G \subseteq \omega(\mathbb{F}G')^5\,\mathbb{F}G = 0.
\end{aligned}$$

9.5. Example: Not all centre-by-metabelian group algebras have unit groups of bounded derived length. In fact, they do not even have to be solvable at all. As an example, we will study $\mathbb{F}_2D_{10}$. (See also appendix B.)

Write $D_{10} := \langle a, x\rangle$ with $a^2 = 1 = x^5$, ${}^{a}x = x^{-1}$. Then $\langle x\rangle$ is an abelian subgroup of index 2 in D_{10}, so $\mathbb{F}_2D_{10}$ is centre-by-metabelian by theorem 4. Let us examine the structure of $\mathbb{F}_2D_{10}$ more closely:

Consider $\mathbb{F}_2\langle x\rangle \subseteq \mathbb{F}_2D_{10}$ first. By Maschke [**25**, §108], $\mathbb{F}_2\langle x\rangle$ is semisimple, and thus, according to Wedderburn [**25**, §102], decomposes into a direct sum of simple $\mathbb{F}_2$-algebras, which are isomorphic to full matrix algebras over some $\mathbb{F}_2$-division algebras. But $\mathbb{F}_2\langle x\rangle$ is commutative, so it is in fact isomorphic to a direct sum of field extensions of $\mathbb{F}_2$. Since x has multiplicative order 5, at least one of these fields contains $\mathbb{F}_{16}$. Checking dimensions, we find that $\mathbb{F}_2\langle x\rangle \cong \mathbb{F}_2 \oplus \mathbb{F}_{16}$ as an $\mathbb{F}_2$-algebra. The adequate Wedderburn decomposition of $\mathbb{F}_2\langle x\rangle$ is determined by the central, orthogonal idempotents $e := \langle x\rangle^+$ and $f := 1+e$, where $e\mathbb{F}_2\langle x\rangle = \mathbb{F}_2e \cong \mathbb{F}_2$, and $f\mathbb{F}_2\langle x\rangle \cong \mathbb{F}_{16}$.

Since $\langle x\rangle \trianglelefteq D_{10}$, the idempotents e, f are also central in $\mathbb{F}_2D_{10}$, so we obtain a decomposition $\mathbb{F}_2D_{10} = e\mathbb{F}_2D_{10} \oplus f\mathbb{F}_2D_{10}$ into ideals. We are going to combine this with the vector space decomposition $\mathbb{F}_2D_{10} = \mathbb{F}_2\langle x\rangle \oplus \mathbb{F}_2\langle x\rangle\, a$.

Observe that as a vector space, $e\mathbb{F}_2D_{10} = e\mathbb{F}_2\langle x\rangle \oplus e\mathbb{F}_2\langle x\rangle\, a = \mathbb{F}_2e \oplus \mathbb{F}_2ea = \mathbb{F}_2\{e, ea\}$. Now $\{e, ea\}$ is a multiplicative group with neutral element e, hence $e\mathbb{F}_2D_{10} \cong \mathbb{F}_2Z_2$. It follows that $\mathcal{U}(e\mathbb{F}_2D_{10}) \cong Z_2$. (To complete the picture, let us point out that $\mathcal{J}(e\mathbb{F}_2D_{10}) = \mathbb{F}_2(e+ea) = \mathbb{F}_2(D_{10})^+$; we are going to see that this also is the Jacobson radical of $\mathbb{F}_2D_{10}$.)

Let us fix an $\mathbb{F}_2$-algebra isomorphism $f\mathbb{F}_2\langle x\rangle \to \mathbb{F}_{16}$, and thus identify $f\mathbb{F}_2\langle x\rangle$ with $\mathbb{F}_{16}$ (and f with $1 = 1_{\mathbb{F}_{16}}$). Then, as a vector space, $A := f\mathbb{F}_2D_{10} = f\mathbb{F}_2\langle x\rangle \oplus f\mathbb{F}_2\langle x\rangle\, a = \mathbb{F}_{16} \oplus \mathbb{F}_{16}a$, i.e. A is an $\mathbb{F}_{16}$-vector space with basis $\{1, a\}$, plus a multiplicative structure, which we are going to determine now: Conjugation by a leaves the subspace $\mathbb{F}_{16} \subseteq A$ invariant. This defines a field automorphism $\alpha\colon \mathbb{F}_{16} \to \mathbb{F}_{16}$. The Galois group of $\mathbb{F}_{16}$ over $\mathbb{F}_2$ is cyclic of order 4, with generator $\beta\colon \mathbb{F}_{16} \to \mathbb{F}_{16}$, $s \mapsto s^2$. Since $\alpha(fx) = {}^{a}f\,{}^{a}x = fx^4 = (fx)^4$, we have $\alpha(s) = s^4$ for all $s \in \mathbb{F}_{16}$. Then $\alpha = \beta^2$, and $\langle\alpha\rangle = \mathrm{Gal}(\mathbb{F}_{16}|\mathbb{F}_4)$. Hence $\mathbb{F}_4$ is the centre of A. By [**25**, §94.3], A is (isomorphic to) the crossed product of $\mathbb{F}_{16}$ with $\mathrm{Gal}(\mathbb{F}_{16}|\mathbb{F}_4)$. In particular, A is a central simple $\mathbb{F}_4$-algebra (ibid). By Wedderburn, $A \cong \mathrm{Mat}(n, D)$ for some $n \in \mathbb{N}$ and an $\mathbb{F}_4$-division algebra D. But finite division algebras are fields, so D is in fact commutative. Since A is not commutative, we obtain $n \geq 2$. Then $2^8 = |A| = (4^{\dim_{\mathbb{F}_4} D})^{n^2}$ implies that $\dim_{\mathbb{F}_4} D = 1$ and $n = 2$, i.e. $f\mathbb{F}_2 D_{10} = A \cong \mathrm{Mat}(2, \mathbb{F}_4)$.

Summarizing, we obtain $\mathcal{U}(\mathbb{F}_2 D_{10}) = \mathcal{U}(e\mathbb{F}_2 D_{10} \oplus f\mathbb{F}_2 D_{10}) \cong \mathcal{U}(e\mathbb{F}_2 D_{10}) \times \mathcal{U}(f\mathbb{F}_2 D_{10}) \cong Z_2 \times \mathrm{GL}(2,4)$. Since $\mathrm{SL}(2,4) \cong A_5$ is simple, $\mathcal{U}(\mathbb{F}_2 D_{10})$ is not solvable.

9.6. Remark (summary): 9.2-9.5 imply theorem 5.

Bibliography

[1] A.K. Bhandari and I.B.S. Passi, Lie nilpotency indices of group algebras, Bull. London Math. Soc. 24 (1992), 68-70

[2] R. Carter, G. Segal, I. Macdonald, Lectures on Lie groups and Lie algebras, LMS Student texts 32, Cambridge University Press 1995

[3] D. Gorenstein, Finite groups, Harper & Row, New York 1968

[4] N. Gupta and F. Levin, On the Lie ideals of a ring, J. Algebra 81 (1983), 225-231

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

[6] S.A. Jennings, On rings whose associated Lie rings are nilpotent, Bull. Amer. Math. Soc. 53 (1947), 593-597

[7] B. Külshammer and R.K. Sharma, Lie centrally metabelian group rings in characteristic 3, J. Algebra 180 (1996), 111-120

[8] H. Kurzweil, Endliche Gruppen, Springer-Verlag, Berlin 1977

[9] F. Levin and G. Rosenberger, Lie metabelian group rings, in: Proceedings of the international conference on group and semigroup rings at the University of Witwatersrand 1985, Mathematics studies 126, 153-161, North-Holland, Amsterdam 1986

[10] F. Levin and S. Sehgal, On Lie nilpotent group rings, J. Pure Appl. Algebra 37 (1985), 33-39

[11] M.F. Newman and E.A. O´Brien, A CAYLEY library for the groups of order dividing 128, in: Group theory, Proceedings of the 1987 Singapore conference, 437-442, Walter de Gruyter, Berlin 1989

[12] E.A. O´Brien, The p-group generation algorithm, J. Symbolic Computation 9 (1990), 677-698

[13] E.A. O´Brien, The groups of order 256, J. Algebra 142 (1991),

[14] P. Osterlund, grupring.g, A GAP extension package designed for group rings, available under ftp://ftp.math.rwth-aachen.de/pub/incoming/groupring (1996)

[15] I.B.S. Passi, D.S. Passman, and S.K. Sehgal, Lie solvable group rings, Canad. J. Math. 25 (1973), 748-757

[16] D.S. Passman, The algebraic structure of group rings, John Wiley & Sons, New York 1977

[17] M. Sahai and J.B. Srivastava, A note on Lie centrally metabelian group algebras, J. Algebra 187 (1997), 7-15

[18] M. Schönert et.al., GAP – Groups, algorithms, and programming, fifth edition, version 3, release 4, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen 1995

[19] S.K. Sehgal, Topics in group rings, Marcel Dekker, New York 1978

[20] A. Shalev, Lie dimension subgroups, Lie nilpotency indices, and the exponent of the group of normalized units, J. London Math. Soc. 43 (1991), 23-36

[21] A. Shalev, The derived length of Lie soluble group rings I, J. Pure Appl. Algebra 78 (1992), 291-300

[22] A. Shalev, The derived length of Lie soluble group rings II, J. London Math. Soc. 49 (1994), 93-99

[23] R.K. Sharma and J.B. Srivastava, Lie centrally metabelian group rings, J. Algebra 151 (1992), 476-486

[24] V. Tasić, On unit groups of Lie centre-by-metabelian algebras, J. Pure Appl. Algebra 78 (1992), 195-201

[25] B.L. van der Waerden, Algebra II, Springer-Verlag, Berlin 1967

APPENDIX A. Notation

A_n	alternating group acting on $\{1, \dots, n\}$
$\omega(\mathbb{F}G)$	augmentation ideal of $\mathbb{F}G$
$\mathrm{Aut}(G)$	automorphism group of G
$\mathcal{C}_G(A)$	centralizer of A in G
$\gamma_n(H)$	nth term of the lower central series of (the group or Lie algebra) H
$\mathrm{cl}(G)$	(nilpotence) class of G (if G is not nilpotent, set $\mathrm{cl}(G) := \infty$)
(x, y)	group commutator of x and y in G, defined as $xyx^{-1}y^{-1}$
$[x, y]$	Lie commutator of x and y in $\mathbb{F}G$, defined as $xy - yx$
L'	commutator (Lie-)subalgebra of L
G'	commutator subgroup of G
D_{2n}	dihedral group of order $2n$
$\delta^n(H)$	nth term of the derived series of (the group or Lie algebra) H
$n \mid m$	n divides m
$\mathbb{F}_q$	field with q elements
$\Phi(G)$	Frattini subgroup of G
$\mathrm{Gal}(L \vert K)$	Galois group of the field extension $L \supseteq K$
$\mathrm{GL}(n, q)$	general linear group of degree n over $\mathbb{F}_q$
id_G	identity map on G
$\mathrm{Inn}(G)$	group of inner automorphisms of G
$\mathcal{J}(A)$	Jacobson radical of A
$\mathrm{Mat}(n, A)$	matrix algebra of $n \times n$-matrices with coefficients in A
$\mathbb{N}$	set of positive integers (natural numbers)
$\mathbb{N}_0$	set of nonnegative integers
$\Omega(G)$	subgroup of the p-group G generated by all elements of order p
p'	set of all primes excluding p
Q_8	quaternion group of order 8
$G \rtimes A$	semidirect product of A with G (A acts on G)
$\mathrm{SL}(n, q)$	special linear group of degree n over $\mathbb{F}_q$
H^+	sum (in $\mathbb{F}G$) over all elements of $H \subseteq G \subseteq \mathbb{F}G$
S_n	symmetric group acting on $\{1, \dots, n\}$
$\mathcal{U}(A)$	group of units of the algebra A
V_4	Klein's *Vierergruppe* (isomorphic to $Z_2 \times Z_2$)
$\mathbb{Z}$	set of integers
Z_n	cyclic group of order n
$\mathcal{Z}(H)$	centre of (the group or algebra) H

APPENDIX B. The GAP extension package LAG

The following is an example session with the GAP extension package *LAG – Lie Algebras of Group Algebras*, which may be downloaded from

`http://www.mathematik.uni-jena.de/algebra/skripten/`

We examine $\mathbb{F}_2 D_{10}$ and its unit group (cf. example 9.5):

```
gap> Read("lag.g");
Lag: Lie Algebras of Group Algebras
gap>  F:=GF(2); G:=DihedralGroup(10);
GF(2)
Group( (1,2,3,4,5), (2,5)(3,4) )
gap> FG:=GroupAlgebra(F,G);
GroupAlgebra( GF(2), Group( (1,2,3,4,5), (2,5)(3,4) ) )
gap> a:=GroupAlgebraElement([(1,2,3,4,5), (2,5)(3,4)], [One(F), One(F)]);
(2,5)(3,4)+(1,2,3,4,5)
gap>  b:=a+(2,5)(3,4)*(1,2,3,4,5);
(2,5)(3,4)+(1,2)(3,5)+(1,2,3,4,5)
gap> Lie(a,b);
(2,5)(3,4)+(1,2,3,4,5)+(1,3)(4,5)+(1,5,4,3,2)
gap>  Lie(a,a);
Lag.Zero()
gap> IsCentreByMetabelian(FG);
true
gap> List(DerivedSeries(FG), Dimension);
[ 10, 6, 2, 0 ]
gap> IsSubset(Centre(FG), DerivedSeries(FG)[3]);
true
gap> U:=Units(FG);;
gap> List(DerivedSeries(U), Size);
[ 360, 60 ]
gap> IsSolvable(U);
false
gap> GroupId(DerivedSubgroup(U));
rec(
  catalogue := [ 60, 13 ],
  names := [ "A5", "PSL(2,4)", "PSL(2,5)" ],
  size := 60 )
gap> quit;
```

APPENDIX C. The GAP file actions.g

The computer algebra system GAP [**18**] has the built-in command `AutomorphismGroup(h)` to compute the automorphism group of some previously defined group `h`. Although this works very nicely if `h` is not too big, the handling of the automorphism group itself later on in the GAP session can become awkward. That is so because automorphisms are represented by rather complex data structures in GAP. A possibility to size down this complexity is to simply convert automorphisms to permutations. Fortunately GAP already provides a command for this task, namely

```
gap> aut:=Operation(AutomorphismGroup(h), Elements(h));
```

The file `actions.g`, which is available under

`http://www.mathematik.uni-jena.de/algebra/skripten/`,

provides some useful general routines in this situation. Additionally, the specific algorithm described in section 5 is programmed in this file. Since this algorithm is part of the proof of theorem 4, and since the file is not too long, a commented listing shall be included (see end of this appendix).

To start our algorithm for all groups of order 8 or 16, one has to issue the following commands:

```
gap> Read("actions.g");
gap> ls:=AllTwoGroups(Size, [8,16]);;
gap> actions:=List(ls, PossibleActions);;
gap> PrintArray(List([1..Length(ls)], i->[i,
>                                       GroupNames(ls[i]),
>                                       Length(actions[i])]
>                 ));;
# The first column gives the number of 'h' in the group catalogue, the
# second its names (if GAP has found any), and the third the number of
# "possible" ways that 'g' (respectively 'a') may act on 'h'.
[ [            1,        [ 8 ],            4 ],
  [            2,      [ 2x4 ],            6 ],
  [            3,       [ D8 ],            0 ],
  [            4,       [ Q8 ],            0 ],
  [            5,    [ 2x2x2 ],            0 ],
  [            6,       [ 16 ],            0 ],
  [            7,      [ 4x4 ],            1 ],
  [            8,             ,            0 ],
  [            9,  [ (2x4).2 ],            0 ],
  [           10,      [ 2x8 ],            5 ],
  [           11,             ,            0 ],
  [           12,      [ D16 ],            0 ],
  [           13,     [ QD16 ],            0 ],
  [           14,      [ Q16 ],            0 ],
  [           15,    [ 2^2x4 ],            3 ],
  [           16,     [ D8x2 ],            0 ],
  [           17,     [ Q8x2 ],            0 ],
  [           18,     [ D8Y4 ],            0 ],
  [           19,      [ 2^4 ],            0 ] ]
```

The remaining $4+6+1+5+3=10$ cases have then to be examined more closely. As an example, we define the second instance of `h` $\cong Z_2 \times Z_4$ (10th row, 5 possible actions, we take the second):

```
gap> h:=ls[10]; # 10th group
2x8
gap> a:=actions[10][2]; # 2nd action on 10th group
Subgroup( Group( (5,6)(7,8)(13,14)(15,16), (5,6)(7,8)(9,10)(11,12),
(3,4)(7,8)(9,12)(10,11)(13,16)(14,15), (9,13)(10,14)(11,15)(12,16) ),
[ (9,10)(11,12)(13,14)(15,16), (3,4)(5,6)(9,11)(10,12)(13,16)(14,15) ] )
```

In order to study this action, we have to define the global variable

```
gap> el:=Elements(h);;
```

The operation

```
gap> op:=function(x,perm)
>   local i;
>   i:=Position(el,x);
>   return el[i^perm];
> end;
```

then returns for each `x` in `h` the image under the automorphism corresponding to the permutation `perm` in `a`. We may use this operation to compute the images of the generators of `h` under the action of the generators of `a`. The results of this examination may be found in sections 6 and 7.

And here comes the source code of `actions.g`:

Beginning of the file actions.g

```
GroupNames:=function(g)
  local n;
  # Returns a list of commonly used names of the group 'g', if GAP can
  # find any, and the empty list otherwise.
  n:=GroupId(g).names; # See description of GroupId for list of names.
  if Length(n)=1 then  # if 'g' has only one name,
    g.name:=n[1];      # remember that name.
  fi;
  return n;
end;;
```

```
Fixpoints:=function(a, d, op)
  # ’a’ is a group that acts on the domain ’d’ via the operation ’op’.
  # The function returns the fixpoints as a subset of ’d’.
  return Union(Filtered(Orbits(a,d,op), o -> Length(o)=1));
end;;

Fixgroup:=function(a,h)
  # ’a’ is a permutation group that acts on the list Elements(h) like some
  # group of automorphisms of the group ’h’. The function returns the
  # centralizer of ’a’ in ’h’, which is not defined in standard GAP since
  # ’a’ and ’h’ do not have a common parent group.
  return Subgroup(h, Elements(h){Fixpoints(a,[1..Size(h)],OnPoints)});
end;;

CommSubgroup:=function(a,h)
  # ’a’ and ’h’ as above. Returns the commutator subgroup of ’a’ with
  # ’h’ (as a subgroup of ’h’).
  local comm,i,p,e;
  e:=Elements(h);
  comm:=[];
  for i in [1..Size(h)] do
    for p in Elements(a) do
      Add(comm, e[i]^(-1)*e[i^p]);
    od;
  od;
  return Subgroup(h, comm);
end;;

IsInvariantSubgroup:=function(a,h,s)
  local el,pos;
  # ’a’ and ’h’ as above, ’s’ a subgroup of ’h’. Tests if ’s’ is invariant
  # under the action of ’a’.
  el:=Elements(h);
  pos:=List(s.generators, x -> Position(el,x));
  return ForAll(pos,
                i -> ForAll(a.generators,
                            perm -> (el[i^perm] in s)
                           )
               );
end;;

FactorGroupOperation:=function(a,h,n)
  # ’a’ and ’h’ as above, ’n’ an ’a’-invariant normal subgroup of ’h’.
  # Returns a permutation group whose action on Elements(h/n) is
  # induced by the action of 'a' on Elements(h).
  local f,t,el,op;
  if not IsInvariantSubgroup(a,h,n) then
    Error("<n> must be an a-invariant normal subgroup of <h>");
  else
    f:=FactorGroup(h,n);
    t:=NaturalHomomorphism(h,f);
    el:=Elements(h);
    op:=function(x,perm)
      local i;
      i:=Position(el,PreImagesRepresentative(t,x));
      return Image(t,el[i^perm]);
    end;
    return Operation(a,Elements(f),op);
  fi;
end;;

IsDihedralAction:=function(a,h)
  # 'a' and 'h' as above. Checks if action is dihedral, i.e. Size(a)=2 and
  # 'a' acts on 'h' by element inversion.
  local el,perm;
  if Size(a)=2 then
    el:=Elements(h);
    perm:=Filtered(Elements(a), x -> (Order(a,x)=2) )[1];
    return ForAll([1..Size(h)], i -> (el[i^perm]=el[i]^-1) );
  else
    return false;
  fi;
end;;

MayBeCounterexample16:=function(a,h)
  # 'a' and 'h' as above, with Size(h)=16.
  # We think of 'h' as the commutator subgroup of some (finite or infinite)
  # group 'g', and of 'a' as the (finite) factor group g/Centralizer(g,h).
  # (Note that the function trusts that 'a' contains the inner
  # automorphisms of 'h'. Otherwise the call to 'FactorGroup' in the
  # function body might produce an error.)
  # If the function returns "false", then 'g' cannot be a counterexample
  # to the classification of centre-by-metabelian group algebras in
  # characteristic 2. No information is gained if the function returns
  # "true".
  # The function works by reduction to the case Size(h)=8, which is
  # assumed to be already handled:
```

```
  # Let 'x' be the list of all elements of order 2 of 'h' which are fixed
  # by 'a', and let 'z' run through 'x' (we think of 'z' as being central
  # in 'g'). Then k:=h/<z> has order 8.
  # Now if 'g' is a counterexample, then 'k' must be isomorphic to
  # 2x2x2 or 2x4. In the case 2x2x2, 'a' must act trivially on 'k',
  # and in the case 2x4, 'a' must act dihedrally on 'k'.
  # The function tests just that.
  local x,z,k,n,i,b;
  if (Size(h)<>16) then
    Error("<h> must be a group of order 16");
  else
    x:=Filtered(Elements(Fixgroup(a,h)), x -> (Order(h,x)=2) );
    for z in x do
      n:=Subgroup(h,[z]);
      k:=FactorGroup(h,n);
      i:=GroupNames(k);
      if i=["2x2x2"] then
        if not IsSubgroup(n,CommSubgroup(a,h)) then
          return false;
        fi;
      elif i=["2x4"] then
        b:=FactorGroupOperation(a,h,n);
        if not IsDihedralAction(b,k) then
          return false;
        fi;
      elif Length(i)<>1 then
        Error("Obscure Error: <k> has more or less than one Name");
      else
        return false;
      fi;
    od;
  fi;
  return true;
end;;

PossibleActionsNonabelianCase:=function(h)
  # If we adopt the notation of above, this function computes all
  # possibilities for the group 'a' acting on 'h', where 'h' must be a
  # nonabelian 2-group.
  # All groups 'a', that already here lead to a situation where it is
  # known that (the undefined --see above-- group) 'g' cannot be a
  # counterexample to our classification theorem, are thrown away.
  # In particular, 'a' must be a 2-group and its commutator subgroup must
  # correspond to the inner automorphisms of 'h'.
  local aut,u,subs;
  if IsAbelian(h) or (not Set(Factors(Size(h)))=[2]) then
    Error("<h> must be a nonabelian 2-group");
  fi;
  aut:=Operation(AutomorphismGroup(h),Elements(h));
    # permutation representation of action of Aut(h) on Elements(h)
  u:=AsSubgroup(aut,Operation(h,Elements(h)));
    # u corresponds to the inner automorphisms
  subs:=List(ConjugacyClassesSubgroups(aut), Representative);
    # take representatives of conjugacy classes of subgroups of aut
  subs:=Filtered(subs, a -> (
                             Set(Factors(Size(a)))=[2]
                             and (DerivedSubgroup(a)=u)
                            )
                );
    # We only need representatives 'a' which are 2-groups, and whose
    # commutator subgroup is the inner automorphism group 'u' of 'h'.
  return subs;
end;;

IsLegal3Action:=function(a,h)
  # Under the situation described above, if 'h' is an abelian 2-group,
  # then the order of 'a' may be divided by 3, but not by 9.
  # In this case, let 's' be the Sylow-3-subgroup of 'a' of order 3, then
  # the commutator subgroup of 's' with 'h' must be 2x2 -- otherwise the
  # imaginary group 'g' (see above) cannot be a counterexample to our
  # classification theorem.
  local s;
  s:=SylowSubgroup(a,3);
  if Size(s)=1 then
    return true;
  elif Size(s)>3 then
    return false;
  else
    return GroupNames(CommSubgroup(s,h))=["2x2"];
  fi;
end;

PossibleActionsAbelianCase:=function(h)
  # Similar to nonabelian case. Differences: 'a' and 'h' must be abelian,
  # 'h' must be a 2-group, and 'a' must be a 2,3-group whose order is not
  # divided by 9. If its order is divided by 3, a special condition
  # applies, see the function 'IsLegal3Action'.
  # Since 'g' cannot be a counterexample if its nilpotence class
  # is at most 2, we only need to consider nontrivial 'a'.
  # Similarly if 'h' is elementary abelian of size greater than 4.
  local aut,subs;
  if not (IsAbelian(h) and Set(Factors(Size(h)))=[2]) then
    Error("<h> must be an abelian 2-group");
  elif IsElementaryAbelian(h) and (Size(h)>4) then
    # nothing can act on 'h' in this case
    return [];
  fi;
  aut:=Operation(AutomorphismGroup(h),Elements(h));
    # permutation representation of action of Aut(h) on Elements(h)
  subs:=List(ConjugacyClassesSubgroups(aut), Representative);
    # take representatives of conjugacy classes of subgroups of 'aut'
  subs:=Filtered(subs, a-> IsAbelian(a)
                           and Size(a)>1
                           and IsSubset( [2,3], Set(Factors(Size(a))) )
                           and IsLegal3Action(a,h));
    # We only need nontrivial abelian reps which are 2,3-groups.
    # The 3-part of 'a' has to pass an additional test.
  return subs;
    # return the found groups.
end;;

PossibleActions:=function(h)
  # Checks whether 'h' is abelian or not and sends 'h' to the appropriate
  # subroutine. In the case Size(h)=16, an additional test is performed.
  local subs;
  if (Size(h)=1) or (Set(Factors(Size(h)))<>[2]) then
    Error("<h> must be a nontrivial 2-group");
  elif IsAbelian(h) then
    subs:=PossibleActionsAbelianCase(h);
  else
    subs:=PossibleActionsNonabelianCase(h);
  fi;
  if Size(h)=16 then
    subs:=Filtered(subs, a -> MayBeCounterexample16(a,h));
  fi;
  return subs;
end;;
```

End of the file actions.g

Lebenslauf (Curriculum Vitae)

Persönliche Daten:

Name:	Rossmanith, Richard Martin
Geburtsdatum:	5.12.1969
Geburtsort:	Marktoberdorf
Familienstand:	verheiratet

Ausbildungs- und Berufsdaten:

1976–1980:	Adalbert-Stifter-Grundschule Marktoberdorf
1980–1989:	Peter-Dörfler-Gymnasium Marktoberdorf
24.6.1989:	Abitur
1989–1990:	Grundwehrdienst, zunächst in Budel (Niederlande), dann bei der Technischen Schule der Luftwaffe in Kaufbeuren
WS 90/91–SS 93:	Studium der Mathematik (Nebenfach Physik) an der Universität Augsburg
WS 91/92–SS 93:	Anstellung als hilfswissenschaftlicher Mitarbeiter
19.2.1993:	Vordiplom
1.3.–30.4.1993:	Praktikum bei der Deutschen Forschungsanstalt für Luft- und Raumfahrt (DLR) in Oberpfaffenhofen
WS 93/94–SS 94:	Mathematikstudium an der Iowa State University in Ames, Iowa (USA) Anstellung als “teaching assistant”
17.12.1994:	Master of Science
WS 94/95:	Mathematikstudium an der Universität Augsburg Anstellung als hilfswissenschaftlicher Mitarbeiter
seit 1.4.1995:	wissenschaftlicher Mitarbeiter am Mathematischen Institut der Friedrich-Schiller-Universität Jena

Selbständikeitserklärung

Ich erkläre, daß ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Hilfsmittel und Literatur angefertigt habe.

Jena, den 15.7.1997 Richard Rossmanith