ISRAEL JOURNAL OF MATHEMATICS 115 (2000), 51–75

LIE CENTRE-BY-METABELIAN GROUP ALGEBRAS IN EVEN CHARACTERISTIC, I

BY

RICHARD ROSSMANITH
Am Burggraben 4, 65760 Eschborn/Frankfurt, Germany
e-mail: richard.rossmanith@de.arthurandersen.com

ABSTRACT

We complete the classification of the Lie centre-by-metabelian group algebras over arbitrary fields by solving the case of characteristic 2.

Let G be a group (not necessarily finite), and let $\mathbb{F}G$ be its group algebra over some field $\mathbb{F}$ of characteristic $p \geq 0$. For subsets X, Y of $\mathbb{F}G$, we denote by $[X, Y]$ the $\mathbb{F}$-span of all elements $[x, y] := xy - yx$ with $x \in X$, $y \in Y$. The first and second derived Lie ideals of $\mathbb{F}G$ are defined as $(\mathbb{F}G)' := [\mathbb{F}G, \mathbb{F}G]$ and $(\mathbb{F}G)'' := [(\mathbb{F}G)', (\mathbb{F}G)']$, respectively. (Note that these are Lie ideals, but not necessarily associative ideals of $\mathbb{F}G$.) We call $\mathbb{F}G$ **Lie centre-by-metabelian**, if $[\mathbb{F}G, (\mathbb{F}G)''] = 0$. (In this case $\mathbb{F}G/\mathcal{Z}(\mathbb{F}G)$, regarded as a Lie algebra, is metabelian.)

Sharma and Srivastava showed in [12] that such group algebras are necessarily commutative if $p > 3$. By a general theorem of Passi, Passman and Sehgal [5], the same holds for $p = 0$. The case $p = 3$ is more interesting, since then $\mathbb{F}G$ is Lie centre-by-metabelian if and only if $|G'| \in \{1, 3\}$ (cf. Külshammer–Sharma [4], Sahai–Srivastava [9]). In his survey article [1], A. Bovdi posed the problem for the remaining case $p = 2$. Its solution shall be presented here, as follows:

THEOREM 1: *Let G be a group, and let $\mathbb{F}$ be a field of characteristic 2. Then $\mathbb{F}G$ is Lie centre-by-metabelian, if and only if one of the following conditions is satisfied:*

(i) *$|G'|$ divides 4.*
(ii) *G' is central and elementary abelian of order 8.*

Received March 26, 1998

(iii) *G acts by element inversion 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.

Roughly speaking, this means that either G' has to be "small" (conditions (i), (ii), and (iii)), or G contains a "large" abelian subgroup (condition (iv)).

This paper first handles the (comparatively easy) "if"-direction in section 1. We then prove the converse direction for groups of class 2 in section 2, and for groups with commutator subgroups of exponent 2 in section 3 (by showing that they necessarily are of class 2 in our setting). In a second paper [8], devoted to groups that act more vigorously on their commutator subgroups, the proof of the theorem will be completed. (Both papers have their origin in the author's dissertation thesis [7].)

For elements a, b of the group G, we will use "left" commutators $(a, b) := aba^{-1}b^{-1}$, "left" conjugation ${}^{a}b := aba^{-1}$, and "right normed triple commutators" $(a, b, c) := (a, (b, c))$. The lower central series of G is written as $G = \gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq \gamma_3(G) \trianglerighteq \cdots$, and, if G is nilpotent, its class is denoted by $\mathrm{cl}(G)$. As usual, G' is the commutator subgroup of G, $\Phi(G)$ is the Frattini subgroup of G, and, if G is a p-group, then $\Omega(G)$ is the subgroup generated by all elements of order p. The letters A_n, D_{2n}, Q_8, S_n, V_4, Z_n refer to popular isomorphism types of groups.

Similarly as above, we set $[a, b, c] := [a, [b, c]]$ for elements a, b, c of $\mathbb{F}G$, and we write the lower central Lie series of $\mathbb{F}G$ as $\mathbb{F}G = \gamma_1(\mathbb{F}G) \trianglerighteq \gamma_2(\mathbb{F}G) \trianglerighteq \gamma_3(\mathbb{F}G) \trianglerighteq \cdots$ (note again that this is a descending chain of Lie ideals, and not ideals, of $\mathbb{F}G$). The sum over all elements of a finite subset X of $\mathbb{F}G$ is written as X^+.

If the integer n divides the integer m, we write $n \mid m$.

Let us henceforth **fix the characteristic** of the base field $\mathbb{F}$ as $p = 2$.

It is now a trivial observation that for any subgroup X of G, we have $X^+(1 + x) = 0$ if and only if $x \in X$. Moreover, if $X = \langle x_1, \ldots, x_n \rangle$ has exponent $\exp(X) = 2$, it is easily checked that

$$(1 + x_1)(1 + x_2) \cdots (1 + x_n) = \begin{cases} X^+ & \text{if } |X| = 2^n, \\ 0 & \text{if } |X| < 2^n. \end{cases}$$

Another easy exercise is to show the following: If $G' \subseteq N \trianglelefteq G$ and $G/N = \langle a_1N, \ldots, a_nN \rangle$, then $G' = \langle (a_i, a_j) \colon 1 \leq i < j \leq n \rangle \, (a_1, N) \cdots (a_n, N) \, N'$. We will apply this often to $N := \mathcal{C}_G(G')$ in the case that G' is abelian.

We will also frequently use the fact that $\mathcal{C}_G(G')' \subseteq G' \cap \mathcal{Z}(G)$, which is a direct consequence of the Witt identity [3, Satz III.1.4].

1. The easy direction

Remark 1.1: 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. [6, 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

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

Moreover, $(G')^+\,\mathbb{F}G$ is a central ideal of $\mathbb{F}G$, since $G' \trianglelefteq G$ implies $(G')^+ \in \mathcal{Z}(\mathbb{F}G)$, and for $g, h \in G$, we have

$$[(G')^+g, h] = (G')^+[g,h] = (G')^+(1+(g,h))hg = 0.$$

LEMMA 1.2: *Let G be a group with $|G'| = 2$. Then $(\mathbb{F}G)' \subseteq (G')^+\,\mathbb{F}G$. In particular, $\mathbb{F}G$ is Lie centre-by-metabelian.*

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

LEMMA 1.3: *Let G be a group with $|G'| = 4$. Then $(\mathbb{F}G)'' \subseteq (G')^+\,\mathbb{F}G$. In particular, $\mathbb{F}G$ is Lie centre-by-metabelian.*

Proof:

CASE 1: $G' = \langle x, y\rangle \cong V_4$. It is easily verified that $(\mathbb{F}G)'' \subseteq \omega(\mathbb{F}G')^2\,\mathbb{F}G = (1+x)(1+y)\,\mathbb{F}G = (G')^+\,\mathbb{F}G$.

CASE 2: $G' = \langle x\rangle \cong Z_4$. We consider the canonical epimorphism $\mathbb{F}G \to \mathbb{F}[G/\langle x^2\rangle]$. By 1.2, $\gamma_3(\mathbb{F}[G/\langle x^2\rangle]) = 0$, 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 $\omega(\mathbb{F}G')^3\,\mathbb{F}G = (G')^+\,\mathbb{F}G$. Then $(\mathbb{F}G)'' \subseteq \gamma_4(\mathbb{F}G) = [\mathbb{F}G, \gamma_3(\mathbb{F}G)] \subseteq [\mathbb{F}G, (1+x^2)\,\mathbb{F}G] = (1+x^2)\,[\mathbb{F}G, \mathbb{F}G] = (1+x)^2\,(\mathbb{F}G)' \subseteq \omega(\mathbb{F}G')^3 \cdot \mathbb{F}G \subseteq (G')^+\,\mathbb{F}G$. ∎

LEMMA 1.4: *Let G be a group of 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 Lie centre-by-metabelian.*

Proof: We have $\exp(G') = 2$ and $G' \subseteq \mathcal{Z}(G)$. Then by Jennings [6, theorem 3.3.7], the second dimension subgroup of G' is trivial, so by [6, lemma 3.3.4], $\omega(\mathbb{F}G')^n\,\mathbb{F}G = \{(1+x_1)\cdots(1+x_n)\colon x_1,\ldots,x_n \in G'\}\,\mathbb{F}G$ for all $n \in \mathbb{N}$. In particular, $\omega(\mathbb{F}G')^3\,\mathbb{F}G = (G')^+\,\mathbb{F}G$. But then

$$[(\mathbb{F}G)', (\mathbb{F}G)'] \subseteq [\omega(\mathbb{F}G')\,\mathbb{F}G,\; \omega(\mathbb{F}G')\,\mathbb{F}G] = \omega(\mathbb{F}G')^2\,[\mathbb{F}G, \mathbb{F}G] \subseteq \omega(\mathbb{F}G')^3\,\mathbb{F}G \subseteq (G')^+\,\mathbb{F}G.$$ ∎

LEMMA 1.5: *Let G be a group that acts by element inversion on $G' \cong Z_2 \times Z_4$, and suppose that $C_G(G')' \subseteq \Phi(G')$. Then $\mathbb{F}G$ is Lie centre-by-metabelian.*

Proof: Write $G' = \langle x, y\rangle$ with $x^2 = 1 = y^4$, and set $C := C_G(G')$. Then $|G : C| = 2$, and $C' \subseteq \Phi(G') = \langle y^2\rangle \subseteq \mathcal{Z}(G)$, and ${}^a x = x$, ${}^a y = y^3$ for all $a \in G \setminus C$.

Obviously $(\mathbb{F}G)'$ is spanned by all elements of the form $[c,d] = cd + {}^d(cd)$, $[b,a] = ba + {}^a(ba)$, or $[a,c] = ac + {}^c(ac)$, with $c, d \in C$, $a, b \in G \setminus C$. Hence it is also spanned by all elements of the form $c + {}^d c$, $c + {}^a c$, or $a + {}^c a$, with $c, d \in C$, $a \in G \setminus C$.

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

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

with $c, d, e \in C$, $g, h \in G$, $a \in G \setminus C$ (note that if $a, a' \in G \setminus C$, then $a' = da$ for some $d \in C$). It suffices to show that all elements of this form are central in $\mathbb{F}G$.

By Jennings [6, 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 [6, lemma 3.3.4], $\omega(\mathbb{F}G')^5 = 0$, and $\omega(\mathbb{F}G')^4 = \mathbb{F}\cdot(G')^+$. Then 1.1 implies that $\omega(\mathbb{F}G')^4\,\mathbb{F}G \subseteq \mathcal{Z}(\mathbb{F}G)$.

Recall that $(\mathbb{F}G)' \subseteq \omega(\mathbb{F}G')\mathbb{F}G$. Note also that $1 + C' \subseteq \omega(\mathbb{F}G')^2$, since C' is contained in the second dimension subgroup of G'. Hence $(\mathbb{F}C)' \subseteq (1 + C')\,\mathbb{F}C \subseteq \omega(\mathbb{F}G')^2\,\mathbb{F}G$. We now check that

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

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 $\sigma := (1 + (c,a))(1 + (e,da)^{-1}) \in \omega(\mathbb{F}G')^2$.

It remains to show that τ is central in $\mathbb{F}G$, or equivalently, that τ commutes with all $f \in C$, and with a. Recall that $(\mathbb{F}C)' \subseteq (1+y^2)\,\mathbb{F}C$, and that ${}^{a}t(1+y^2) = t(1+y^2)$ for all $t \in G'$. Then check $[f,\tau] = (\sigma(a,d) + {}^{a}\sigma)[f, da^2] \in (\sigma(a,d)+{}^{a}\sigma)\,(\mathbb{F}C)' \subseteq \sigma((a,d)+1)(1+y^2)\,\mathbb{F}C \subseteq \omega(\mathbb{F}G')^5\,\mathbb{F}G = 0$. Finally, observe that ${}^{a}\tau = ({}^{a}\sigma\;{}^{a}(a,d) + {}^{a^2}\sigma)\,{}^{a}da^2 = ({}^{a}\sigma\,(a,d)^{-1} + \sigma)(a,d)da^2 = \tau$. ∎

Remark 1.6: Suppose that G is a group that has an abelian subgroup A of index 2. Then [5, lemma 1.3] provides us with an embedding of $\mathbb{F}G$ into $\mathrm{Mat}(2, \mathbb{F}A)$ (the algebra of all 2×2-matrices over $\mathbb{F}A$). It is an easy exercise to show that $\mathrm{Mat}(2, R)$ is Lie centre-by-metabelian for any commutative ring R. Hence so is $\mathbb{F}G$. This observation concludes the proof of the "if"-direction of Theorem 1.

2. Groups of nilpotence class 2

We are now going to verify Theorem 1 for groups G of class 2. We will freely use the well-known properties of such groups, such as $(ab, c) = (a, c)(b, c)$ for all $a, b, c \in G$, or $G' = \langle (g_i, g_j)\colon 1 \le i < j \le n\rangle$ if $G = \langle g_1, \ldots, g_n\rangle$.

Remark 2.1: Let G be a group of class 2. Following A. Shalev [11], we set

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

for $x \in G'$. If $(a, b) = x$, and $n, m, i, j \in \mathbb{Z}$, then $(a^n b^m, a^i b^j) = x^{nj-mi}$. If n, m are co-prime, then $a^n b^m \in S_x$ (similarly $b^m a^n \in S_x$). Consequently $S_x = S_x^{-1} = S_{x^{-1}}$. (But note that the example $G = D_8$ shows that S_x need not be a subgroup of G.)

We will mainly use the following properties of S_x:

$$(1+x)\,S_x \subseteq [S_x,\, S_x], \quad \text{and} \quad (1+x)^3\,S_x \subseteq (\mathbb{F}G)''.$$

To see this, let $b \in S_x$, and choose an $a \in G$ with $x = (b, a^{-1}) = (a, b)$. Then $(1+x)b = b + (a,b)b = b + aba^{-1} = [a^{-1}, ab] \in [S_x, S_x]$. Apply this to obtain $(\mathbb{F}G)'' \supseteq [(1+x)S_x, (1+x)S_x] = (1+x)^2[S_x, S_x] \supseteq (1+x)^3 S_x$.

Lemma 2.2: *Let G be a group of class 2 such that $\mathbb{F}G$ is Lie centre-by-metabelian. If G is generated by two elements, then $|G'| \mid 4$.*

Proof: We write $G = \langle g, h\rangle$. Then $G' = \langle x\rangle$, where $x := (g, h)$. By 2.1, $(1+x)^4 g \in (1+x)^4 S_x \subseteq [(1+x)^3 S_x, S_x] \subseteq [(\mathbb{F}G)'', \mathbb{F}G] = 0$. Hence $0 = (1+x)^4 = 1 + x^4$, and $x^4 = 1$. ∎

LEMMA 2.3: *Let G be a group of class 2 such that $\mathbb{F}G$ is Lie centre-by-metabelian. If $|\langle x\rangle| \geq 4$ for some $x \in G'$, then $\{y \in G' \colon S_x \cap S_y \neq \emptyset\} \subseteq (S_x, G) \subseteq \langle x\rangle$.*

Proof: It suffices to show the latter inclusion, since the former follows directly from the definition of S_y. W.l.o.g., suppose that $S_x \neq \emptyset$, and let $a \in S_x$, $g \in G$. Then $\langle x\rangle^+(1 + (a,g)) = (1+x)^3[a,g](ga)^{-1} \in (1+x)^3[S_x, \mathbb{F}G](ga)^{-1} = [(1+x)^3 S_x, \mathbb{F}G](ga)^{-1} \subseteq [(\mathbb{F}G)'', \mathbb{F}G](ga)^{-1} = 0$, and thus $(a,g) \in \langle x\rangle$. ∎

LEMMA 2.4: *Let G be a group of class 2. If $\mathbb{F}G$ is Lie 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 2.2. 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 2.3, 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 $(ac, bd) = (a,b)(a,d)(c,b)(c,d) = x^k y$. Now 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 2.3.

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 $(b, ac) = (x(c,b))^{-1} = x$, so $ac \in S_x \cap S_{x^k y}$ and $x^k y \in \langle x\rangle$.

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 $G' = \langle x\rangle \cong Z_4$. ∎

Remark 2.5: The preceding lemma already comes very close to our goal in this section. All which remains to be faced 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 Lie 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 Lie 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 elementary abelian 2-groups. Hence $|G : A| \geq 4$.

We divide our examination of G into four cases (Lemmata 2.6–2.9), depending on the index of (G, A) in G'. In each case, we will show that $\mathbb{F}G$ is not Lie centre-by-metabelian, in contradiction to our assumption.

LEMMA 2.6: *Let G and A be as in 2.5, and suppose that $|G' : (G, A)| \geq 8$. Then $\mathbb{F}G$ is not Lie centre-by-metabelian.*

Proof: Suppose, for contradiction, that $\mathbb{F}G$ is Lie 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, $su \notin C_G(A) = A$, 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 $(1+x)(1+y)(1+z)su = (1+x)(1+y)[s, u] = [(1+x)s, (1+y)u] \in [(1+x)S_x, (1+y)S_y] \subseteq (\mathbb{F}G)''$, and $0 \neq (1+x)(1+y)(1+z)(1+w)asu = (1+x)(1+y)(1+z)[su, a] = [(1+x)(1+y)(1+z)su, a] \in [(\mathbb{F}G)'', \mathbb{F}G] = 0$. This means that our assumption is rubbish, and we may conclude:

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

We will reduce this conclusion to absurdum. For simplicity, and since we will not switch back to G anymore, we will omit the bars $^-$ 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 $(*)$. ∎

LEMMA 2.7: *Let G and A be as in 2.5, and suppose that $|G' : (G,A)| = 4$. Then $\mathbb{F}G$ is not Lie centre-by-metabelian.*

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

Set $\bar{G} := G/(G,A)$, then $\exp(\bar{G}') = 2$ and $|\bar{G}'| = 4$. As in the proof of 2.6, 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 $a \in A \setminus C_A(t) \neq \emptyset$, then $(t, ua) \neq 1$. Thus, by replacing u by ua if necessary, we may assume that $w := (t,u) \in (G,A) \setminus \{1\}$. 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. 2.5). 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 $(g,A) \nsubseteq \langle w\rangle$. The map $\sigma\colon A \to A$, $a \mapsto (g,a)$, is a group homomorphism with image (g,A), hence $\sigma^{-1}(\langle w\rangle) < A$. Consequently $A \neq C_A(t) \cup \sigma^{-1}(\langle w\rangle)$, so there exists an $a \in A$ such that $(t,a) \neq 1$ (i.e. $w = (t,a) = (ta,a)$) and $z := (g,a) \in (G,A) \setminus \langle w\rangle$.

Set $\tilde{x} := (s,ta) = x(s,a) \in x(G,A)$; then $|\langle \tilde{x},y,z,w\rangle| = 16$. By 2.1,

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

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 $\hat{x} := (as,ta) = w\tilde{x} \equiv \tilde{x} \pmod{\langle w\rangle}$, and $\tilde{y} := (as,u) = y(a,u) \equiv y \pmod{\langle w\rangle}$. We obtain

$$\begin{aligned}(1+w)(1+y)(1+\tilde{x})ta^2s &= (1+w)(1+\tilde{y})(1+\hat{x})ta\cdot as\\ &= [(1+w)ta,(1+\tilde{y})as]\end{aligned}$$

$\in (\mathbb{F}G)''$, which leads to the contradiction $0 = [g,(1+w)(1+y)(1+\tilde{x})ta^2s] = a^2(1+w)(1+y)(1+\tilde{x})(1+(st,g))gst = a^2(1+w)(1+y)(1+\tilde{x})(1+z)gst \neq 0$. ∎

LEMMA 2.8: *Let G and A be as in 2.5, and suppose that $|G' : (G,A)| = 2$. Then $\mathbb{F}G$ is not Lie centre-by-metabelian.*

Proof: Assume that $\mathbb{F}G$ is Lie 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:

(*)

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

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 $(s,A) \nsubseteq \langle (s,a),(t,b)\rangle$ or $(t,A) \nsubseteq \langle (s,a),(t,b)\rangle$.

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 $t\notin A=C_G(A)$.

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

Assume now 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 $(s,t)=(gs,t)(g,t)\in(G,A)$. ∎

LEMMA 2.9: *Let G and A be as in 2.5, and suppose that $|G':(G,A)|=1$. Then $\mathbb{F}G$ is not Lie centre-by-metabelian.*

Proof: Assume that $\mathbb{F}G$ is Lie 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 $s \in G \setminus A$.

We claim that in this case $(r,s) \in (r,A)(s,A)$ for all $r,s \in G \setminus A$ with $(r,A) \neq (s,A)$. If not, then there are $r,s \in G \setminus A$ 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 $r,s \in G \setminus A$ with $\mathcal{C}_A(r) \neq \mathcal{C}_A(s)$. Otherwise we have $\mathcal{C}_A(r) = \mathcal{C}_A(s)$ for all $r,s \in G \setminus A$, hence $\mathcal{C}_A(s) = \mathcal{Z}(G)$ for all $s \in G \setminus A$. Let $s \in G \setminus A$, 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. 2.5). Let $r \in G \setminus A$ 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 $(r,A) \neq (s,A) \Longrightarrow r\mathcal{Z}(G) \neq s\mathcal{Z}(G) \Longrightarrow |B : \mathcal{Z}(G)| > 2$, where $B := \langle \mathcal{Z}(G), r, s\rangle$; but then B is abelian in contradiction to a previous statement.

Now let $r,s \in G \setminus A$ with $\mathcal{C}_A(r) \neq \mathcal{C}_A(s)$. If $(r,A) = (s,A)$, there is an element $t \in G \setminus A$ 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 $r,s \in G \setminus A$ 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 choose $t,u \in G \setminus A$ 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

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

and $0 = [r,\sigma](batducsr)^{-1} = (1+(cs,du))(1+z)(1+wy)(1+(r,batducs)) = (1+(u,c)(s,d)(s,u))(1+z)(1+wy)(1+(r,batsu)(r,dc))$. 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 $c,d \in A$. 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

$$d \in A \setminus (\mathcal{C}_A(s) \cup \mathcal{C}_A(r)) \neq \emptyset,$$

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

$$d \in \mathcal{C}_A(r) \setminus \mathcal{C}_A(s) \neq \emptyset,$$

then $E_{c,d} = \langle z,wy,y,x \rangle$.

CASE 3: $(s,u) \equiv w$ *and* $(r,batsu) \equiv 1$. Choose $c \in A \setminus (\mathcal{C}_A(u) \cup \mathcal{C}_A(r)) \neq \emptyset$ and $d \in \mathcal{C}_A(r) \setminus \mathcal{C}_A(s) \neq \emptyset$, 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 $|(s,A)| \geq 16$. 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 2.1 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 $[\mathbb{F}G, (\mathbb{F}G)''] \ni [t,\sigma] = s^2(1+(s,a))(1+(s,b))(1+(s,c))[t,c] = s^2(1+(s,a))(1+(s,b))(1+(s,c))(1+(t,c))ct \neq 0$, contradiction.

Therefore, we may assume that

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

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 $|(s,A)| \geq 4$. Using similar methods as earlier in the proof, we obtain an element $t \in G$ with $(t,A) \not\subseteq (s,A) < (G,A) = G'$, 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

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

If $r \in G$ with $(r,A) \not\subseteq \langle x,y,z\rangle$, then

$$\begin{aligned} 0 = [r,\sigma] &= (1+x)(1+z)(1+y)(1+(r,dsb))dsbr \\ &= (1+x)(1+z)(1+y)(1+(r,d)(r,sb))dsbr. \end{aligned}$$

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

3. Elementary abelian commutator subgroups

This section deals with groups G such that $\exp(G') = 2$. We will show that $\mathbb{F}G$ Lie centre-by-metabelian implies $G' \subseteq \mathcal{Z}(G)$, so we may apply the results of section 2.

LEMMA 3.1: *Let E be a normal subgroup of exponent 2 of the group G, and suppose that $\mathbb{F}G$ is Lie 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: (i) Let $x \in E$, $a \in G$. Observe that $(x,a) = (a,x) = {}^{a}x x$. Then

$$\begin{aligned}\sigma := [x + {}^{a}x,\, a + {}^{x}a] &= [(1 + {}^{a}xx)x,\, (1 + {}^{a}xx)a] \\ &= (1 + {}^{a}xx)^2 xa + (1 + {}^{a}xx)(1 + {}^{a^2}x\,{}^{a}x)\,{}^{a}xa \\ &= (1 + {}^{a}xx)(1 + {}^{a^2}x\,{}^{a}x)\,{}^{a}xa.\end{aligned}$$

Since $(1 + {}^{a^2}x\,{}^{a}x)({}^{a}x + {}^{a^2}x) = 0$, we furthermore obtain

$$\begin{aligned}0 = [a,\sigma]a^{-2} &= (1 + {}^{a^2}x\,{}^{a}x)(1 + {}^{a^3}x\,{}^{a^2}x)\,{}^{a^2}x + (1 + {}^{a}xx)(1 + {}^{a^2}x\,{}^{a}x)\,{}^{a}x \\ &= (1 + {}^{a^2}x\,{}^{a}x)\big({}^{a^2}x + {}^{a^3}x + {}^{a}x + x\big) = (1 + {}^{a^2}x\,{}^{a}x)(x + {}^{a^3}x) \\ &= (1 + {}^{a^2}x\,{}^{a}x)(1 + {}^{a^3}xx)\,x.\end{aligned}$$

Expanding the parenthesis yields $1 \in \{{}^{a^2}x\,{}^{a}x,\ {}^{a^3}xx,\ {}^{a^3}x\,{}^{a^2}x\,{}^{a}xx\}$. Now if $1 = {}^{a^2}x\,{}^{a}x$, then $x = {}^{a}x$, if $1 = {}^{a^3}xx$, then $x = {}^{a^3}x$, and if $1 = {}^{a^3}x\,{}^{a^2}x\,{}^{a}xx$, then ${}^{a^3}x = {}^{a^2}x\,{}^{a}xx$, i.e. ${}^{a^4}x = {}^{a^3}x\,{}^{a^2}x\,{}^{a}x = {}^{a^2}x\,{}^{a}xx\,{}^{a^2}x\,{}^{a}x = x$.

(ii) We consider E as an $\mathbb{F}_2[\langle aC\rangle]$-module. By Maschke [3, Satz I.17.7], E is semisimple. There are two nonisomorphic simple $\mathbb{F}_2[\langle aC\rangle]$-modules: the trivial one, 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

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

contradiction.

This shows that there is precisely one nontrivial simple submodule V of E. Then $E = V \oplus C_E(a)$, 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 [2, theorem 3.2.2], none of these simple modules is faithful (in the sense that the corresponding linear representation of U 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 $C_U(V) = \langle bC\rangle$. 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.

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 $\exp(G/C) \mid 4$. So suppose that 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 cannot be a subgroup of order 9 by (iii), G/C must have order 3. ∎

Remark 3.2: Let G be a group with $Z_2 \times Z_2 \times Z_2 \cong G' \not\subseteq \mathcal{Z}(G)$. Then $G' \subseteq C := C_G(G') < G$, so G/C is a nontrivial abelian group. We consider G' as an $\mathbb{F}_2$-vector space and choose a basis x, y, z. The conjugation action of G on G' produces a representation $G \to \mathrm{GL}(3,2)$ with kernel C. Below we list representatives of all the abelian subgroup conjugacy classes of $\mathrm{GL}(3,2)$ (cf. [10]), and by changing the basis if necessary, we may assume that G is mapped onto one of these:

$$R := \left\langle \left(\begin{smallmatrix}0&0&1\\1&0&1\\0&1&0\end{smallmatrix}\right) \right\rangle \cong Z_3, \qquad S := \left\langle \left(\begin{smallmatrix}0&0&1\\1&0&0\\0&1&1\end{smallmatrix}\right) \right\rangle \cong Z_3,$$
$$T := \left\langle \left(\begin{smallmatrix}0&1&0\\1&0&0\\0&0&1\end{smallmatrix}\right) \right\rangle \cong Z_2, \qquad U := \left\langle \left(\begin{smallmatrix}0&1&1\\1&1&1\\1&1&0\end{smallmatrix}\right) \right\rangle \cong Z_4,$$
$$V := \left\langle \left(\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&0&1\\1&1&1\\1&0&0\end{smallmatrix}\right) \right\rangle \cong V_2, \qquad W := \left\langle \left(\begin{smallmatrix}0&0&1\\0&1&0\\1&0&0\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1&1\\0&1&0\\1&1&0\end{smallmatrix}\right) \right\rangle \cong V_4.$$

In any of these cases, $\mathbb{F}G$ is not Lie centre-by-metabelian. This is clear by 3.1 in the case that G is mapped onto S. The other cases are handled by 3.3–3.8.

LEMMA 3.3: *Let the notation be as in 3.2, and assume that G is mapped onto R. Then $\mathbb{F}G$ is not Lie centre-by-metabelian.*

Proof: We assume otherwise. If we write $G/C = \langle aC \rangle$, we have ${}^a x = y$, ${}^a y = z$, ${}^a z = x$. For all $c, d \in C$, we have $\sigma := [x + {}^a x,\ ca + {}^d(ca)] = [x+y,\ (1+(d,ca))ca] = (1 + (d,ca))c\,[x + y, a] = (1 + (d,ca))c\,(x + y + y + z)a = (1 + (d,ca))(x + z)ca$, and

$$(*)\quad 0 = [a,\sigma]\,a^{-2}c^{-1}x = (1 + (d,ca))(x + z)x + (1 + {}^a(d,ca))(y + x)\,{}^a c\,c^{-1}x$$
$$= (1 + (ca,d))(1 + xz) + (1 + {}^a(ca,d))(1 + xy)(a,c).$$

Setting $c = 1$ and expanding parentheses, we obtain

$$0 = (a,d) + xz + (a,d)xz + {}^a(a,d) + xy + {}^a(a,d)xy.$$

If $(a,d) \notin \langle xy, yz \rangle \trianglelefteq G$, then the projection of the right hand side 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. $(a, C) \subseteq \langle xy, yz \rangle$.

Since $C' \subseteq \mathcal{Z}(G) \cap G' = \langle xyz \rangle$ and $(a,C)C' = G' \not\subseteq \langle xy, yz \rangle$, we have $C' = \langle xyz \rangle$. 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 $(a,c) \in \langle xy, yz \rangle = \{1, xy, yz, xz\}$. ∎

LEMMA 3.4: *Let the notation be as in 3.2, and assume that G is mapped onto U. Then $\mathbb{F}G$ is not Lie centre-by-metabelian.*

Proof: We write $G/C = \langle aC \rangle$. Then ${}^a x = yz$, ${}^a y = xyz$, ${}^a z = xy$. By the introductory remarks of this paper, we have $C' \subseteq G' \cap \mathcal{Z}(G) = \langle xz \rangle$ and $G' = (a, C)C'$. Since $G' \not\subseteq \langle y, xz \rangle$, also $(a, C) \not\subseteq \langle y, xz \rangle$.

So let $c \in C$ such that $(a, c) \in G' \setminus \langle y, xz \rangle$. Then

$$\begin{aligned}[x + {}^a x,\, a + {}^c a] &= [x + {}^a x,\, (1 + (a,c))a] = (1 + (a,c))\,[x + {}^a x,\, a] \\ &= (1 + (a,c))(x + {}^{a^2} x)a = (1 + (a,c))(1 + xz)xa =: \sigma,\end{aligned}$$

and

$$\begin{aligned}[a, \sigma]a^{-2}x &= (1 + xz)\,[a,\, (1 + (a,c))x]\,a^{-1}x \\ &= (1 + xz)\,\big((1 + (a,c))xa + (1 + {}^a(a,c))\,{}^a xa\big)\,a^{-1}x \\ &= (1 + xz)\,(1 + (a,c) + yzx + {}^a(a,c)yzx) \\ &= (1 + xz)\,(1 + (a,c) + y + {}^a(a,c)y).\end{aligned}$$

Since (a,c), ${}^a(a,c) \notin \langle y, xz \rangle \trianglelefteq G$, the projection of the last term onto $\mathbb{F}[\langle y, xz \rangle]$ is $(1 + xz)(1 + y) \neq 0$. Hence $[\mathbb{F}G, (\mathbb{F}G)''] \neq 0$. ∎

LEMMA 3.5: *Let the notation be as in 3.2, and assume that G is mapped onto V. Then $\mathbb{F}G$ is not Lie centre-by-metabelian.*

Proof: We assume that $\mathbb{F}G$ is Lie centre-by-metabelian. We write $G/C = \langle aC, bC \rangle$ with $a, b \in G$ such that ${}^a x = z$, ${}^a y = y$, ${}^a z = x$, and ${}^b x = yz$, ${}^b y = y$, ${}^b z = xy$. Then $C_{G'}(a) = C_{G'}(b) = G' \cap \mathcal{Z}(G) = \langle y, xz \rangle$, 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

$$(g^2 h, hg) = {}^{g^2}(h, hg)(g^2, hg) = (hg, h)(g^2, h) = {}^h(g,h)\,{}^g(g,h) \cdot (g,h),$$

and thus

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

Now $(g, hg^3h) = (g,h)^{hg^3}(g,h) = (gh, g, h) = (g,g,h)(h,g,h)$, since $\gamma_3(G) \subseteq \mathcal{Z}(G)$, and ${}^h(g,h)(1+(g,h)) = {}^h(g,h)(g,h)(1+(g,h)) = (h,g,h)(1+(g,h))$. Hence

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

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 $h := bc$ in $(*)$, 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, which shows that a acts trivially on G', contradiction. ∎

LEMMA 3.6: *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 Lie centre-by-metabelian, then $|\langle (g,h),\ {}^g(g,h),\ (g,k)\rangle| \leq 4$ for all $g,h,k \in G$.*

Proof: Since $|\gamma_3(G)| \leq 2$, we have $(1+(f,g,h))(i,j,k) = (1+(f,g,h))$, and thus $(1+(f,g,h))\,{}^k(i,j) = (1+(f,g,h))(i,j)$, for all $f,g,h,i,j,k \in G$. Using this, an easy but lengthy calculation (similar to the ones above) shows that under the given hypothesis, the following equation holds for all $g,h,k \in G$ (cf. [7]):

$$0 = [g,\ g + {}^kg,\ h + {}^gh] = (1+(g,h))(1+{}^g(g,h))(1+(g,k))g^2h.$$

This, together with the remarks in the introduction of this paper, implies the claim. ∎

LEMMA 3.7: *Let the notation be as in 3.2, and assume that G is mapped onto W. Then $\mathbb{F}G$ is not Lie 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 ${}^a x = z$, ${}^a y = y$, ${}^a z = x$, and ${}^b x = z$, ${}^b y = xyz$, ${}^b z = x$. Then $C_{G'}(a) = \langle y, xz\rangle$, $C_{G'}(b) = \langle xy, yz\rangle$, 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 3.6,

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

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

Note that the introductory remarks of this paper imply that

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

We already know that $C' \subseteq G' \cap \mathcal{Z}(G) = \langle xz\rangle$. We show now that also $(a,b) \in \langle xz\rangle$:

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 $G' \subsetneq \langle x, z\rangle$, contradiction.

ASSUMPTION: $(a,b) \in \{xy, yz\}$. Then we have $4 \geq |\langle (a,b),\ {}^a(a,b), (a,c)\rangle| = |\langle xy, yz, (a,c)\rangle|$, and

$$4 \geq \left|\left\langle (ab,a),\ {}^{ab}(ab,a), (ab,c)\right\rangle\right| = |\langle\, {}^a(b,a),\ {}^b(b,a), (ab,c)\rangle| = |\langle xy, yz, (b,c)\rangle|\,.$$

Similarly as above, this implies $G' \subsetneq \langle xy, yz\rangle$, contradiction.

ASSUMPTION: $(a,b) \in \{y, xyz\}$. In this case, $4 \geq \left|\left\langle (b,a),\ {}^b(b,a),\ (b,c)\right\rangle\right| = |\langle y,\ xyz,\ (b,c)\rangle|$, 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 $G' \subsetneq \langle y, xyz\rangle$.

Hence $(a,b) \in \langle xz\rangle$, as desired. We show next that $(b,d) \in \langle xz\rangle$ for all $d \in C$:

ASSUMPTION: $(b,d) \in \{x,z\}$. If $c \in C$, then $(d,c) \in \langle xz \rangle$, and

$$4 \geq |\langle (bd,b),\ {}^{bd}(bd,b),\ (bd,c)\rangle| = |\langle x,\ z,\ (b,c)\rangle|,$$

and therefore $(b,d) \in \langle x,z \rangle$. Moreover,

$$4 \geq |\langle (ad,b),\ {}^{ad}(ad,b),\ (ad,c)\rangle| = |\langle x,\ z,\ (a,c)\rangle|,$$

hence also $(a,c) \in \langle x,z\rangle$. We arrive at the already familiar contradiction $G' \subseteq \langle x,z\rangle$.

ASSUMPTION: $(b,d) \in \{xy, yz\}$. We have $4 \geq \left|\left\langle (ad,b),\ {}^{ad}(ad,b),\ (ad,d)\right\rangle\right| = |\langle {}^{a}(d,b)(a,b),\ (d,b)(a,b),\ (a,d)\rangle| = |\langle xy,\ yz,\ (a,d)\rangle|$. 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. ∎

LEMMA 3.8: *Let the notation be as in 3.2, and assume that G is mapped onto T. Then $\mathbb{F}G$ is not Lie 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 Lie 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 ${}^a x = y$, ${}^a y = x$, ${}^a z = z$.

The lower central series of G is $G \trianglerighteq \langle x, y, z \rangle \trianglerighteq \langle xy \rangle \trianglerighteq 1$, so Lemma 3.6 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, 3.6 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 $|(a, C)| = |G'| = 8$. ∎

Remark 3.9: We have established Theorem 1 for all groups G with $\exp(G') = 2$ and $|G'| \leq 8$. Before we turn to the case where $|G'|$ is arbitrary in 3.12, let us study two particular situations in the following lemmata.

LEMMA 3.10: *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 $x_1, \ldots, x_n, z$ defines a matrix representation $\Delta\colon G \to \mathrm{GL}(n+1, 2)$ with kernel $\mathcal{C}_G(N)$ and image

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

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 $b_1, \ldots, b_k$ of B with $k \leq n$. It clearly suffices to show that $B = A$, or equivalently, $k = n$.

Again shifting our point of view, we now interpret the elements b_i, $i = 1, \ldots, k$, 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 $k = n$. ∎

LEMMA 3.11: *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 Lie centre-by-metabelian.*

Proof: We assume that $\mathbb{F}G$ is Lie 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, 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 ${}^{\tilde{h}} w = w$. Another computation in the usual style (which we will skip here, see [7, lemma 4.11] for details) then leads to the following contradiction:

$$0 = (1+x)\,[k,\, g + {}^h g,\, \tilde{h} + {}^g\tilde{h}] = (1+x)(1+z)(1+w)(1+y)g\tilde{h}k \neq 0.$$

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 3.10, 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

$$\begin{aligned} z = z^3 = (g,y)(h,x)(k,w) &= (g,h,k)(h,g,k)(k,g,h) \\ &= (g,h^{-1},k)(h,k^{-1},g)(k,g^{-1},h) = 1 \end{aligned}$$

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

LEMMA 3.12: *Let G be a group with $\exp(G') = 2$ and $|G'| \geq 8$. If $\mathbb{F}G$ is Lie centre-by-metabelian, then G has class 2.*

Proof: Let G be a counterexample. Then $\mathbb{F}G$ is Lie centre-by-metabelian, $\exp(G') = 2$, $\gamma_3(G) \neq 1$, and, by 3.9, $|G'| \geq 16$.

Set $C := \mathcal{C}_G(G')$. Then G/C is abelian. By 3.1, $\exp(G/C) \mid 4$ or $|G/C| = 3$. In the latter case, 3.1 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 non-nilpotent group with $(G/N)' = G'/N \cong Z_2 \times Z_2 \times Z_2$. Then by 3.9, $\mathbb{F}[G/N]$ is not Lie centre-by-metabelian, contradiction. Therefore, $\exp(G/C) \mid 4$.

We claim next that $\gamma_3(G)$ is a finite 2-group. By [5], G has a subgroup A 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 $t \in G \smallsetminus A$. Then $G' = (t, A)A' \subseteq A$ as usual. 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 $x, y \in G'$. 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).

Then $G/\mathcal{C}_G(\gamma_3(G))$ is also a finite group; in fact, it is a finite 2-group, because of $\exp(G/\mathcal{C}_G(\gamma_3(G))) \mid \exp(G/C) \mid 4$. Considered as $\mathbb{F}_2[G/\mathcal{C}_G(\gamma_3(G))]$-module, $\gamma_3(G)$ contains a submodule in every possible dimension. In other words: For any $q \in \{2, 4, 8, \ldots, |\gamma_3(G)|\}$, 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 3.9, contradiction. Hence $|G' : \gamma_3(G)| \geq 8$.

We now choose a normal subgroup N of G with $N \subseteq \gamma_3(G)$ and $|\gamma_3(G) : N| = 2$. Then G/N is also a counterexample, so after replacing G by G/N, we may 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 $|\langle X \rangle'| \geq 16$ 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, and after replacing G by $\langle X \rangle$, we may assume that G is finitely generated.

Then $G/\langle z \rangle$ is a finitely generated group of class 2, so $G'/\langle z \rangle$ is finitely generated, too. In fact, it is finite since it is elementary abelian. But then also G' is finite.

From now on, we may argue by induction on $|G'|$. We write $|G'| = 2^{n+1}$ with

$n \geq 3$, and assume that the lemma 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 $G' = \langle x_1, \ldots, x_n, z\rangle$ with $x_1, \ldots, x_n \in G' \setminus \mathcal{Z}(G)$. By 3.10, there are elements $a_1, \ldots, a_n \in G$ such that

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

and $G/C = \langle a_1C, \ldots, a_nC\rangle$ is an elementary abelian group of order 2^n. Hence $H_1 := \langle a_2, a_3, \ldots, a_n, C\rangle$ and $H_2 := \langle a_1, a_3, \ldots, a_n, C\rangle$ are normal subgroups of G of index 2 with $G = H_1H_2$.

In the case $H_1' = G'$, we have $\mathcal{Z}(H_1) \cap H_1' = \mathcal{C}_{G'}(H_1) = \mathcal{C}_{G'}(a_2, \ldots, a_n) = \langle z, x_1\rangle$ 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 $\mathrm{cl}(H_1) = 2$.

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

Since $G/\langle z\rangle$ has class 2 and is generated by $C \cup \{a_1, \ldots, a_n\}$, we have

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

It follows that $|G' : \langle z\rangle| \leq |\langle (a_1, a_2),\, z\rangle : \langle z\rangle| \cdot |H_1' : \langle z\rangle| \cdot |H_2' : \langle z\rangle| \leq 2 \cdot 2 \cdot 2 = 8$, and thus $16 \leq |G'| = 2\,|G' : \langle z\rangle| \leq 16$.

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 $|G'| < 16$. 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. $|\,\langle a_1, a_2, a_3\rangle'\,| \geq 8$. Then $\langle a_1, a_2, a_3\rangle$ acts nontrivially on $\langle a_1, a_2, a_3\rangle'$, hence $\mathrm{cl}(\langle a_1, a_2, a_3\rangle) > 2$. By 3.9, $|\,\langle a_1, a_2, a_3\rangle'\,| \geq 16$, and thus $\langle a_1, a_2, a_3\rangle' = G'$. But then $\langle a_1, a_2, a_3\rangle$ is a counterexample to 3.11, contradiction. ∎

References

[1] A. Bovdi, *The group of units of a group algebra of characteristic p*, Publications Mathematicae Debrecen **52** (1998), 193–244.

[2] D. Gorenstein, *Finite Groups*, Harper & Row, New York, 1968.

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

[4] B. Külshammer and R. K. Sharma, *Lie centrally metabelian group rings in characteristic* 3, Journal of Algebra **180** (1996), 111–120.

[5] I. B. S. Passi, D. S. Passman and S. K. Sehgal, *Lie solvable group rings*, Canadian Journal of Mathematics **25** (1973), 748–757.

[6] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley, New York, 1977.

[7] R. Rossmanith, *Centre-by-metabelian group algebras*, Dissertation, Friedrich-Schiller-Universität, Jena, 1997.

[8] R. Rossmanith, *Lie centre-by-metabelian group algebras in even characteristic, II*, Israel Journal of Mathematics, this volume.

[9] M. Sahai and J. B. Srivastava, *A note on Lie centrally metabelian group algebras*, Journal of Algebra **187** (1997), 7–15.

[10] 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.

[11] A. Shalev, *The derived length of Lie soluble group rings I*, Journal of Pure and Applied Algebra **78** (1992), 291–300.

[12] R. K. Sharma and J. B. Srivastava, *Lie centrally metabelian group rings*, Journal of Algebra **151** (1992), 476–486.