# ON CONJUGACY p-SEPARABILITY OF FREE CENTRE-BY-METABELIAN GROUPS 

C. K. GUPTA, N. D. GUPTA and F. LEVIN

(Received 23 February 1988)

Communicated by H. Lausch
Dedicated to Bernhard Neumann on his eightieth birthday


#### Abstract

A group $G$ is said to be conjugacy $p$-separable if two non-conjugate elements of $G$ remain nonconjugate in some finite $p$-group endomorphic image of $G$. We show that the non-cyclic free centre-by-metabelian groups are not conjugacy $p$-separable for any prime $p$. On the other hand, we show that every free centre-by-metabelian group has the solvable conjugacy problem


1980 Mathematics subject classification (Amer. Math. Soc.) (1985 Revision): 20 E 22, 20 E 25, 20 E 99.

## 1. Introduction

A group $G$ is said to be conjugacy $p$-separable if two non-conjugate elements of $G$ remain non-conjugate in some finite $p$-group endomorphic image of $G$. Examples of conjugacy $p$-separable groups include free groups (see, for instance, [ 9 , page 27]) and finitely generated nilpotent groups (Blackburn [1]). While finitely generated torsion free metabelian groups are not in general conjugacy $p$-separable (Wehrfritz [12]), Timoshenko [11] has proved that free metabelian groups are conjugacy $p$-separable. This led Lichtman (verbal communication) to ask if the same were true for free centre-by-metabelian groups. We answer Lichtman's question negatively by exhibiting two nonconjugate elements in the free centre-by-metabelian group $G$ of rank 2 which

[^0]are conjugate modulo every term of the lower central series of $G$. In particular, it follows that non-cyclic free centre-by-metabelian groups are not conjugacy $p$-separable for any prime $p$, which illustrates once again the dichotomy existing between free metabelian and free centre-by-metabelian groups. Further, in this paper we prove the solvability of the conjugacy problem for free centre-by-metabelian groups of arbitrary rank. The solvability of the conjugacy problem for certain centre-by-metabelian groups including the free centre-by-metabelian groups of rank 2 and 3 was established in [4].

## 2. Conjugacy $p$-separability

Matthews' proof [10] of the solvability of the conjugacy problem for free metabelian groups is derived from that for the wreath product of free abelian groups. The result of Timoshenko [11] quoted in the introduction is obtained using this fact and by showing that a wreath product of free abelian groups is conjugacy separable (that is, two non-conjugate elements remain non-conjugate under some finite endomorphic image). For completeness, we include below a direct proof that free metabelian groups are conjugacy $p$ separable. We begin with a direct proof that free metabelian groups have the solvable conjugacy problem.

Theorem 2.1 (cf. Matthews [10]). Free metabelian groups have the solvable conjugacy problem.

Proof. Let $F=\left\langle x_{1}, \ldots, x_{n} ; \varnothing\right\rangle, n \geq 2$, be a free group and let $F^{\prime}, F^{\prime \prime}$ denote respectively the derived group and the second derived group of $F$. The conjugacy problem for the free metabelian group $F / F^{\prime \prime}$ of rank $n$ is that of determining the existence of a solution $g \in F$ to a congruence $u^{g} \equiv$ $w$ (modulo $F^{\prime \prime}$ ) for given $u, w \in F$; or, equivalently, to a congruence $[u, g] \equiv$ $v$ (modulo $F^{\prime \prime}$ ) for given $u \in F$ and $v \in F^{\prime}$. There are two cases to be considered.

Case $1, u \notin F^{\prime}$. In this case there is an automorphism $\theta$ of $F$ such that $u \theta$ is of the form $u \theta=x_{n}^{k} u^{\prime}$ with $k>0$ and $u^{\prime} \in F^{\prime}$. Applying $\theta$ to the congruence $[u, g] \equiv v$ (modulo $F^{\prime \prime}$ ), we may assume, without loss of generality, that $u=x_{n}^{k} u^{\prime}, u^{\prime} \in F^{\prime}$. Let $g=x_{1}^{k(1)} \cdots x_{n}^{k(n)} g^{\prime}, g^{\prime} \in F^{\prime}$. Modulo $\gamma_{3}(F)$, the third term of the lower central series of $F$, the congruence

$$
\begin{equation*}
\left[x_{n}^{k} u^{\prime}, x_{1}^{k(1)} \cdots x_{n}^{k(n)} g^{\prime}\right] \equiv v\left(F^{\prime \prime}\right) \tag{2.1}
\end{equation*}
$$

uniquely determines the exponents $k(1), \ldots, k(n-1)$. Moreover, using the group identities $\left[u, u^{m} g\right]=\left[g^{m} u, g\right]=[u, g]$, if necessary, we may further
assume $|k(n)|<k$. Thus, without loss of generality, we may assume that in (2.1) all exponents $k(i)$ are known. This reduces the original problem to that of the existence of a solution $g \in F^{\prime}$ to the congruence

$$
\begin{equation*}
\left[x_{n}^{k}, g\right] \equiv v^{\prime}\left(F^{\prime \prime}\right) \tag{2.2}
\end{equation*}
$$

with given $k>0$ and $v^{\prime}=\left[x_{1}^{k(1)} \cdots x^{k(n)}, x_{n}^{k} u^{\prime}\right] v \in F^{\prime}$. For this purpose, we may express $g$ and $v^{\prime}$ uniquely in the normal form as
such that $g(i, j)$ and $v(i, j)$ are elements of the group ring $\mathbf{Z} F$ (reduced modulo $\mathbf{a}=\mathbb{Z} F\left(F^{\prime}-1\right)$ ) involving no $x_{m}$ for $m<i$ (see, for instance, [6, page 82]). Hence, the problem in (2.2) reduces to the existence of a solution to a system of congruences in $\mathbb{Z} F$ of the form

$$
\begin{equation*}
g(i, j)\left(1-x_{n}^{k}\right) \equiv v(i, j)(\bmod \mathbf{a}), \quad 1 \leq i<j \leq n, \tag{2.4}
\end{equation*}
$$

for the unknown $g(i, j)$ 's. This is clearly possible if and only if ( $1-x_{n}^{k}$ ) divides $v(i, j)$ module a and this fact can be effectively decided.

Case $2, u \in F^{\prime}$. In this case the problem reduces to solving for $g \in F$, the congruence $[u, g] \equiv v\left(F^{\prime \prime}\right)$ where

$$
u=\prod_{1 \leq i<j \leq n}\left[x_{i}, x_{j}\right]^{u(i, j)} \text { and } v=\prod_{1 \leq i<j \leq n}\left[x_{i}, x_{j}\right]^{v(i, j)}
$$

are in the normal form as above and, without loss of generality, we may assume $g$ has the form $g=x_{1}^{k(1)} \cdots x_{n}^{k(n)}$. We first find an $m$ such that $u \in$ $\gamma_{m-1}(F) \backslash \gamma_{m}(F)$. Then the congruence $\left[u, x_{1}^{k(1)} \cdots x_{n}^{k(n)}\right] \equiv v\left(\gamma_{m+1}(F) F^{\prime \prime}\right)$ will uniquely determine the exponents $k(1), \ldots, k(n)$, and using these exponents we merely verify whether or not $\left[u, x_{1}^{k(1)} \cdots x_{n}^{k(n)}\right] \equiv v\left(F^{\prime \prime}\right)$.

Theorem 2.2 (cf. Timoshenko [11]). Free metabelian groups are conjugacy p-separable.

Proof. Since finitely generated nilpotent groups are conjugacy $p$-separable (Blackburn [1]), it suffices to show that if a congruence $[u, g] \equiv v\left(F^{\prime \prime}\right)$ has no solution $g \in F$, then the congruence $[u, g] \equiv v\left(\gamma_{m}(F) F^{\prime \prime}\right)$ will have no solution $g \in F$ for some sufficiently large $m$. Suppose first that $u \notin F^{\prime}$. Then as in case 1 of the proof of Theorem 2.1, the problem reduces to showing that if a system of congruences

$$
\begin{equation*}
g(i, j)\left(1-x_{n}^{k}\right) \equiv v(i, j)(\bmod \mathbf{a}), \quad 1 \leq i<j \leq n \tag{2.5}
\end{equation*}
$$

has no solution in $\mathbb{Z} F$ then, for some sufficiently large $m$, the system

$$
\begin{equation*}
g(i, j)\left(1-x_{n}^{k}\right) \equiv v(i, j)\left(\bmod \mathbf{f}^{m}+\mathbf{a}\right), \quad 1 \leq i<j \leq n, \tag{2.6}
\end{equation*}
$$

has no solution $g(i, j)$ in $\mathbb{Z} F$, where $\mathbf{f}=\mathbb{Z} F(F-1)$ is the augmentation ideal of $\mathbb{Z} F$. Multiplying (2.5) by a suitable positive word $x_{1}^{q(1)} \cdots x_{n}^{q(n)}, q(i) \geq 0$, we may assume that $v(i, j)$ involves no inverses of the generators. Thus, for some sufficiently large $d$, each $v(i, j)$ can be effectively written as an element of degree at most $d$ in the polynomial ring $\mathbb{Z}\left[\left(x_{1}-1\right), \ldots,\left(x_{n}-1\right)\right]$. Now, with $m=d+1$, it is clear that a solution to (2.6) will determine a solution to (2.5), contrary to the hypothesis. Thus to complete the proof we may assume that $u \in F^{\prime}$. In this case the problem reduces to showing that if the system

$$
\begin{equation*}
u(i, j)(g-1) \equiv v(i, j)(\bmod a), \quad 1 \leq i<j \leq n, \tag{2.7}
\end{equation*}
$$

has no solution $g$ in $F$ then, for some $m$, the system

$$
\begin{equation*}
u(i, j)\left(g_{m}-1\right) \equiv v(i, j)\left(\bmod \mathbf{f}^{m}+\mathbf{a}\right), \quad 1 \leq i<j \leq n, \tag{2.8}
\end{equation*}
$$

has no solution $g_{m}$ in $F$. As before we may assume that for some $d>0$, $u(i, j), v(i, j)$ are elements of degree at most $d$ in $\mathbb{Z}\left[\left(x_{1}-1\right), \ldots,\left(x_{n}-1\right)\right]$. It follows that a solution $g_{m}$ for $m=d+1$ will be a solution to (2.7), contrary to hypothesis.

We now prove the main result of this section.
Theorem 2.3. A non-cyclic free centre-by-metabelian group is not conjugacy $p$-separable for any prime $p$.

Proof. Since any endomorphism of a group $G$ to a finite $p$-group factors through some term of the lower central series of $G$, it clearly suffices to exhibit two elements $u$ and $v$ of the free group $F=\langle x, y ; \varnothing\rangle$ such that $u, v$ are not conjugate modulo $\left[F^{\prime \prime}, F\right]$ but are conjugate modulo $\left[F^{\prime \prime}, F\right] \gamma_{m}(F)$ for all $m$. Indeed, let $u=[x, y][x, y, x]\left[x, y, x^{-1}\right]$ and $v=u[[x, y, x],[x, y]]$. We first prove that $u$ and $v$ are not conjugate modulo $\left[F^{\prime \prime}, F\right]$. Suppose, on the contrary, that $u$ and $v$ are conjugate modulo $\left[F^{\prime \prime}, F\right]$. Then, for some $g \in F$, $[u, g] \equiv u^{-1} v\left(\bmod \left[F^{\prime \prime}, F\right]\right)$, and since $u^{-1} v \in F^{\prime \prime}, g$ will be in $F^{\prime}$ (see, for instance, $\left[6\right.$, page 27]). Thus we may write $g \equiv[x, y]^{g}\left(\bmod F^{\prime \prime}\right), u \equiv$ $[x, y]^{p}\left(\bmod F^{\prime \prime}\right)$ and $u^{-1} v \equiv\left[[x, y]^{x},[x, y]\right]\left(\bmod \left[F^{\prime \prime}, F\right]\right)$, where $q \in Z F$ and $p=1+(x-1)+\left(x^{-1}-1\right) \in \mathbb{Z} F$. On the other hand, for any elements $p, q, r \in \mathbb{Z} F$, a congruence

$$
\begin{equation*}
\left[[x, y]^{p},[x, y]^{q}\right] \equiv\left[[x, y]^{\gamma},[x, y]\right]\left(\bmod \left[F^{\prime \prime}, F\right]\right) \tag{2.9}
\end{equation*}
$$

will hold if and only if $p \bar{q}-\bar{p} q \equiv r-\bar{r}(\operatorname{moda})$ in $\mathbb{Z} F$, where, if $s=$ $s\left(x, y, x^{-1}, y^{-1}\right)$ then $\bar{s}=s\left(x^{-1}, y^{-1}, x, y\right)$ (cf. [4]). Since, in our case, $p=$
$1+(x-1)+\left(x^{-1}-1\right)=\bar{p}$ and $r=x$, it follows that for some $q \in Z\langle x\rangle$, the equation

$$
\begin{equation*}
p(q-\bar{q})=\left(x-x^{-1}\right) \tag{2.10}
\end{equation*}
$$

holds in $Z\langle x\rangle$. However, if $q=\sum a_{i} x^{i}, a_{i} \in \mathbf{Z}$, satisfies (2.10), then after multiplying both sides of (2.10) by $x$ we will have $\left(x^{2}-x+1\right)\left(\sum a_{i} x^{i}-\right.$ $\left.\sum a_{i} x^{-i}\right)=x^{2}-1$, which is clearly not possible. Hence, $u$ and $v$ are not conjugate modulo $\left[F^{\prime \prime}, F\right]$. On the other hand, for any $m, q=(1-(p-$ 1) $\left.+(p-1)^{2} \cdots+(-1)^{m-1}(p-1)^{m-1}\right) x$ satisfies (2.10) modulo $\mathbf{f}^{m}+\mathbf{a}$, and it follows that $u$ and $v$ are conjugate modulo $\left[F^{\prime \prime}, F\right] \gamma_{m}(F)$. This completes the proof of the theorem.

## 3. The conjugacy problem for free-centre-by-metabelian groups

The solution of the conjugacy problem for $F / F \cap(1+\mathrm{faf})$, for $F$ of arbitrary rank, has been carried out in [4] and provides a first step towards the solution of the conjugacy problem of free centre-by-metabelian groups. By [3], the subgroup $F \cap(1+\mathrm{faf})$ of $F$ is $K\left[F^{\prime \prime}, F\right]$, where $K$ is the fully invariant closure in $F$ of the word $w^{*}$ defined by

$$
\begin{gather*}
w^{*}=\left[f_{1}^{-1}, f_{2}^{-1} ; f_{3}, f_{4}\right]\left[f_{1}^{-1}, f_{3}^{-1} ; f_{4}, f_{2}\right]\left[f_{1}^{-1}, f_{4}^{-1} ; f_{2} ; f_{3}\right] \\
 \tag{3.1}\\
{\left[f_{3}^{-1}, f_{4}^{-1} ; f_{1}, f_{2}\right]\left[f_{4}^{-1}, f_{2}^{-1} ; f_{1}, f_{3}\right]\left[f_{2}^{-1}, f_{3}^{-1} ; f_{1}, f_{4}\right] .}
\end{gather*}
$$

Moreover, for $F$ of rank $n \geq 4, K\left[F^{\prime \prime}, F\right] /\left[F^{\prime \prime}, F\right]$ is an elementary abelian 2-group of rank $\binom{n}{4}$, and if the rank of $F$ is 2 or 3 then $F \cap(1+\mathrm{faf})=\left[F^{\prime \prime}, F\right]$. Thus, the solution of the conjugacy problem for $F / F \cap(1+$ faf $)$ given in [4] includes that for free centre-by-metabelian groups of rank 2 and 3 . Let $F$ be free of rank $n \geq 4$. By [5, Lemma 4.3], the solution of the conjugacy problem for $F / K\left[F^{\prime \prime}, F\right]$ reduces the conjugacy problem for $F /\left[F^{\prime \prime}, F\right]$ to solving for $v \in F^{\prime}$, the congruence

$$
\begin{equation*}
[u, v] \equiv w\left(\operatorname{modulo}\left[F^{\prime \prime}, F\right]\right) \tag{3.2}
\end{equation*}
$$

for given $u \in F^{\prime}$ and $w \in K$. In fact, we shall prove that (3.2) is not possible unless $w \in\left[F^{\prime \prime}, F\right]$. Moreover, since a free centre-by-metabelian group of rank exceeding 3 is residually a 4 -generator free centre-by-metabelian group [8], it suffices to prove that (3.2) will not be possible for $F$ of rank 4. In this case $K\left[F^{\prime \prime}, F\right] /\left[F^{\prime \prime}, F\right]$ will be cyclic of order 2 generated by $w^{*}\left[F^{\prime \prime}, F\right]$, and since

$$
\begin{gather*}
w^{*} \equiv\left[f_{1}, f_{2} ; f_{1}, f_{2}, f_{3}, f_{4}\right]\left[f_{1}, f_{3} ; f_{1}, f_{3}, f_{2}, f_{4}\right]\left[f_{1}, f_{4} ; f_{1}, f_{4}, f_{2}, f_{4}\right] \\
{\left[f_{2}, f_{3} ; f_{2}, f_{3}, f_{1}, f_{4}\right]\left[f_{2}, f_{4} ; f_{2}, f_{4}, f_{1}, f_{3}\right]\left[f_{3}, f_{4} ; f_{3}, f_{4}, f_{1}, f_{2}\right],} \tag{3.3}
\end{gather*}
$$

modulo $\left[F^{\prime \prime}, F\right] \gamma_{7}(F)$ (see [3]), the impossibility of (3.2) follows immediately from the following technical lemma.

Lemma 3.1. Let $F$ be free of rank 4 and let $w^{*}$ be as given by (3.3). Then the congruence

$$
\begin{equation*}
[u, v] \equiv w^{*}\left(\bmod \left[F^{\prime \prime}, F\right]\left(\gamma_{6}(F)\right)^{2} \gamma_{7} F\right) \tag{3.4}
\end{equation*}
$$

is not possible for any $u, v \in F^{\prime}$.
Proof. Suppose, on the contrary, that $u, v \in F^{\prime}$ exist satisfying (3.4). Since $\left[F^{\prime \prime}, F\right]<\gamma_{5}(F)$, it follows that $[u, v]$ is a 4-variable word in $\gamma_{5}(F)$ which also lies in $F^{\prime \prime} \cap\left[F^{\prime \prime}, F\right] \gamma_{6}(F)$. It follows that $[u, v] \in \gamma_{6}(F)[7$, Theorem 1]. There are two cases to consider.

CASE $1, u \in \gamma_{2}(F) \backslash \gamma_{3}(F), v \in \gamma_{4}(F) \backslash \gamma_{5}(F)$. Without loss of generality we may assume that $[u, v]$ has the form

$$
\begin{equation*}
[u, v] \equiv\left[\prod_{i<j}\left[f_{i}, f_{j}\right]^{a(i j)}, \prod_{i<j}\left[f_{i}, f_{j}, f_{k}, f_{l}\right]^{b(i j k l)}\right], \quad k, l \geq i \tag{3.5}
\end{equation*}
$$

where $a(i, j)$ and $b(i, j, k, l)$ are integers modulo 2 and $a(12) \equiv 1(\bmod 2)$. Since $w^{*}$ is invariant under all tame automorphisms of $\left.F /\left[F^{\prime \prime}, F\right]\left(\gamma_{6}(F)\right)^{2} \gamma_{7} F\right)$, the tame automorphism $f_{2} \rightarrow f_{2} f_{3}^{a(13)} f_{4}^{a(14)}, f_{i} \rightarrow f_{i}, i \neq 2$, followed by $f_{1} \rightarrow f_{1} f_{3}^{a(23)} f_{4}^{f(24)}, f_{i} \rightarrow f_{i}, i \neq 1$, does not alter the right hand side of (3.4) but replaces the product $\Pi\left[f_{i}, f_{j}\right]^{a(i j)}$ in (3.5) by a product $\Pi\left[f_{i}, f_{j}\right]^{a^{\prime}(i j)}$ with $a^{\prime}(12) \equiv a(12)(\bmod 2)$ and $a^{\prime}(i j) \equiv 0(\bmod 2)$ for $(i, j) \neq(1,2),(3,4)$. Hence, in (3.5) we may further assume $a(i j) \equiv 0(\bmod 2)$ for any $(i, j) \neq$ $(1,2),(3,4)$. In particular, since $\left[f_{2}, f_{3} ; f_{2}, f_{3}, f_{1}, f_{4}\right]$ is the only factor of $w^{*}$ involving two occurences each of $x_{2}$ and $x_{3}$ and one each of $x_{1}$ and $x_{4}$, the congruence (3.4) induces, in particular, the congruence

$$
\begin{align*}
& {\left[f_{1}, f_{2} ; f_{2}, f_{3}, f_{3}, f_{4}\right]^{a(12) b(2334)}\left[f_{1}, f_{2} ; f_{2}, f_{4}, f_{3}, f_{3}\right]^{a(12) b(2433)}}  \tag{3.6}\\
& \quad\left[f_{3}, f_{4} ; f_{1}, f_{2}, f_{2}, f_{3}\right]^{a(34) b(1223)}\left[f_{3}, f_{4} ; f_{1}, f_{3}, f_{2}, f_{2}\right]^{a(34) b(1322)} \\
& \quad \equiv\left[f_{2}, f_{3} ; f_{2}, f_{3}, f_{1}, f_{4}\right]\left(\bmod \left[F^{\prime \prime}, F\right]\left(\gamma_{6} F\right)^{2} \gamma_{7} F\right) .
\end{align*}
$$

However, if (3.6) were to hold, then identifying $f_{2}$ with $f_{1}$ and $f_{3}$ with $f_{4}$ would yield $\left[f_{1}, f_{3} ; f_{1}, f_{3}, f_{1}, f_{3}\right] \in\left[F^{\prime \prime}, F\right]\left(\gamma_{6}(F)\right)^{2} \gamma_{7}(F)$, which is not possible [7, Theorem 3].

Case 2, $u, v \in \gamma_{3}(F) \backslash \gamma_{4}(F)$. Without loss of generality we may assume that $[u, v]$ in (3.4) has the form

$$
\begin{equation*}
[u, v]=\left[\prod_{\kappa \geq i<j}\left[f_{i}, f_{j}, f_{k}\right]^{a(i j k)}, \prod_{\kappa \geq i<j}\left[f_{i}, f_{j}, f_{k}\right]^{b(i j k)}\right] . \tag{3.7}
\end{equation*}
$$

Assume first that $a(121) \equiv 1(\bmod 2)$. Then since $[u, v]=[u, u v]$, we may assume $b(121) \equiv 0(\bmod 2)$. Substituting $\left.f_{2} f_{3}^{a(131)} f_{4}^{a(141)}\right)$ for $f_{2}$ we may further
assume, as in Case 1, that $a(131)=a(141)=0$ in (3.7). Since $\left[F^{\prime \prime}, F\right]-1$ is in the ideal faf, it follows that $\left[F^{\prime \prime}, F\right]\left(\gamma_{6}(F)\right)^{2} \gamma_{7}(F)-1$ is in the ideal $\mathbf{f a f}+2 \mathbb{Z} F+\mathbf{f}^{7}$. Hence, $[u, v]-1 \equiv 0\left(\bmod \mathbf{f a f}+2 \mathbb{Z} \mathbf{f}+\mathbf{f}^{7}\right)$, and a routine expansion in $\mathbb{Z} F$ yields that $a(121) b(i j k) \equiv 0(\bmod 2)$ for any $(i, j) \neq(1,2)$. On the other hand, for $k \neq 1$,

$$
\left[f_{1}, f_{2}, f_{1} ; f_{1}, f_{2}, f_{k}\right] \equiv\left[f_{1}, f_{2} ; f_{1}, f_{2}, f_{1}, f_{k}\right] \notin\left[F^{\prime \prime}, F\right]\left(\gamma_{6}(F)\right)^{2} \gamma_{7}(F)
$$

(see [7, Theorem 3]), and we obtain similarly that $a(121) b(12 k) \equiv 0(\bmod 2)$ if $k \neq 1$. Thus, if $a(121) \equiv 1(\bmod 2)$, then all $b(i j k) \equiv 0(\bmod 2)$ and $[u, v] \equiv 1\left(\bmod \left[F^{\prime \prime}, F\right]\left(\gamma_{6}(F)\right)^{2} \gamma_{7}(F)\right)$. Hence, we may assume $a(121) \equiv$ $0(\bmod 2)$ and, by symmetry, that $a(i j i) \equiv 0(\bmod 2)$ for all $i, j$. Finally, if $a(123) \equiv 1(\bmod 2)$ then the tame automorphism $f_{3} \rightarrow f_{3} f_{1}, f_{i} \rightarrow f_{i}$, $i \neq 3$, now maps (3.7) to an expression with $a(121) \equiv 1(\bmod 2)$, and the above argument applies to show the impossibility of (3.4). This completes the proof of the lemma.

Combined with the remarks preceding Lemma 3.1, we have thus proved the following theorem.

Theorem 3.2. (a) Two elements of a free group $F$ are conjugate modulo [ $\left.F^{\prime \prime}, F\right]$ if and only if they are conjugate modulo $K\left[F^{\prime \prime}, F\right]$.
(b) Free centre-by-metabelian groups have the solvable conjugacy problem.

## 4. Centralizers in $F /\left[F^{\prime \prime}, F\right]$

Two elements $u, v$ of a free group $F$ commute modulo $F^{\prime \prime}$ if and only if they both lie in $F^{\prime}$ or they are both powers of a common element $w$ in $F$ (see, for instance, [6, page 27]). If $u, v$ are in $F^{\prime}$ with $u \equiv w^{r}\left(\bmod F^{\prime \prime}\right)$, $v \equiv w^{s}\left(\bmod F^{\prime \prime}\right)$ for some $w \in F^{\prime}$ and $r, s \in \mathbb{Z} F$ satisfying $r \bar{s} \equiv \bar{r} s(\bmod \mathbf{a})$, then using the congruence $\left[x, y^{g}\right] \equiv\left[x^{g^{-1}}, y\right]\left(\bmod \left[F^{\prime \prime}, F\right]\right), x, y \in F^{\prime}$, it is elementary to verify that $u$ and $v$ commute modulo $\left[F^{\prime \prime}, F\right]$. In this section we shall prove

Theorem 4.1. Two elements $u, v$ of a free group $F$ commute modulo $\left[F^{\prime \prime}, F\right]$ if and only if either $u$ and $v$ are both powers of a common element, or $u$ and $v$ are both in $F^{\prime}$ with $u \equiv w^{r}\left(\bmod F^{\prime \prime}\right), v \equiv w^{s}\left(\bmod F^{\prime \prime}\right)$ for some $w \in F^{\prime}$, and $r, s \in \mathbb{Z} F$ satisfying $r \bar{s} \equiv \bar{r} s(\bmod \mathbf{a})$.

Proof. We may assume that $u, v$ are not powers of a common element and that $u, v \in F^{\prime}$. By Lemma 3.1, we first observe that $[u, v] \equiv 1\left(\bmod \left[F^{\prime \prime}, F\right]\right)$
if and only if $[u, v] \equiv 1\left(\bmod \left[F^{\prime \prime}, F\right] K\right)$. Thus, the proof reduces to that of determining for given $u \in F^{\prime}$ the solutions $v \in F^{\prime}$ to the congruence

$$
\begin{equation*}
[u, v] \equiv 1\left(\bmod \left[F^{\prime \prime}, F\right] K\right) \tag{4.1}
\end{equation*}
$$

Since $F \cap(1+\mathrm{faf})=\left[F^{\prime \prime}, F\right] K$ by [2], (4.1) reduces, equivalently, to the congruence

$$
\begin{equation*}
(u-1)(v-1) \equiv(v-1)(u-1)(\bmod \mathrm{faf}) \tag{4.2}
\end{equation*}
$$

Since, for any $g$ in $F,\left[x_{i}, x_{j}\right]^{g}-1 \equiv\left(\left[x_{i}, x_{j}\right]-1\right) g \equiv\left(\left(x_{i}-1\right)\left(x_{j}-1\right)-\right.$ $\left.\left(x_{j}-1\right)\left(x_{i}-1\right)\right) g(\bmod f a)$ and $\left[x_{i}, x_{j}\right]^{g}-1 \equiv g^{-1}\left(\left[x_{i}, x_{j}\right]-1\right) \equiv g^{-1}\left(\left(x_{i}^{-1}-\right.\right.$ 1) $\left(x_{j}^{-1}-1\right)-\left(x_{j}^{-1}-1\right)\left(x_{i}^{-1}-1\right)(\bmod a f) ;$ it follows that if, for $w \in F^{\prime}$ $w-1 \equiv \sum_{i=1, \ldots, n}\left(x_{i}-1\right) r_{i}(\bmod \mathbf{f a}), r_{i} \in \mathbb{Z} F$, then $w-1 \equiv \sum_{i=1, \ldots, n} \bar{r}_{i}\left(x_{i}^{-1}-\right.$ 1) (modaf), where, as above, if $r=r\left(x_{1}, \ldots, x_{n}, x_{1}^{-1}, \ldots, x_{n}^{-1}\right)$ then $\bar{r}=$ $x_{1}^{-1}, \ldots, x_{n}^{-1}, x_{1}, \ldots, x_{n}$ ). Applying this to the congruence (4.2) with $u-1 \equiv$ $\sum_{i=1, \ldots, n}\left(x_{i}-1\right) p_{i}(\bmod f a)$ and $v-1 \equiv \sum_{i=1, \ldots, n}\left(x_{i}-1\right) q_{i}(\bmod \mathrm{fa})$ yields the congruence

$$
\begin{equation*}
\sum_{i, j}\left(x_{i}-1\right)\left(p_{i} \bar{q}_{j}-q_{i} \bar{p}_{j}\right)\left(x_{j}^{-1}-1\right) \equiv 0(\bmod \operatorname{faf}) \tag{4.3}
\end{equation*}
$$

Since $\mathbf{f}$ is a free right $\mathbf{Z} F$-module on the ( $x_{i}-1$ )'s and a left $\mathbb{Z} F$-module on the ( $x_{i}^{-1}-1$ )'s (cf. [6, page 5]), the congruence (4.3) yields a system of congruences $p_{i} \bar{q}_{j}-q_{j} \bar{p}_{j} \equiv 0(\bmod \mathbf{a}), i, j \in\{1, \ldots, n\}$. Thus $[u, v] \equiv$ $1\left(\bmod \left[F^{\prime \prime}, F\right] K\right)$ is possible if and only if $p_{i} \bar{q}_{j}-q_{i} \bar{p}_{j} \equiv 0$ for all $i, j$. The latter, however, is possible if and only if, for some fixed $r, s \in \mathbb{Z}\left(F / F^{\prime}\right)$, each $q_{i}=s p_{i} / r$, where $r$ and $s$ are relatively prime, $r$ divides g.c.d. $\left\{p_{i} ; i=1, \ldots, n\right\}$ and $s \in \mathbf{Z} F$ satisfies $r \bar{s} \equiv \bar{r} s(\bmod a)$. Thus, with $p_{i}=r p_{i}^{\prime}$ we may then write $u$ as $w^{r}$ and $v$ as $w^{s}$ where $w \in F^{\prime}$ satisfies $w-1 \equiv \sum_{i-1, \ldots, n}\left(x_{i}-1\right) p_{i}^{\prime}(\bmod \mathbf{f a})$ (cf. [6, pages 7-9]). This completes the proof of the theorem.

## Acknowledgement

The third author wishes to thank the University of Manitoba for its hospitality during the preparation of this paper.

## References

[1] N. Blackburn, ‘Conjugacy in nilpotent groups’, Proc. Amer. Math. Soc. 16 (1965), 143-148.
[2] C. K. Gupta, 'A faithful matrix representation for certain centre-by-metabelian groups', J. Austral. Math. Soc. Ser. A 10 (1969), 451-464.
[3] C. K. Gupta, "The free centre-by-metabelian groups", J. Austral. Math. Soc. Ser. A 16 (1973), 294-299.
[4] C. K. Gupta, W. Herfort and F. Levin, 'The conjugacy problem for centre-by-metabelian groups', Arch Math. 52 (1989), 117-121.
[5] C. K. Gupta and N. D. Gupta, 'Generalized Magnus embeddings and some applications', Math. Z. 160 (1978), 75-87.
[6] N. Gupta, 'Free group rings', Contemp. Math. 66 (1987).
[7] N. D. Gupta, T. C. Hurley and F. Levin, 'On the lower central factors of free centre-bymetabelian groups', J. Austral. Math. Soc. Ser. A 38 (1985), 65-75.
[8] N. Gupta and F. Levin, 'Generating groups of certain soluble varieties', J. Austral. Math. Soc. Ser. A 17 (1974), 222-233.
[9] R. C. Lyndon and P. E. Schupp, ‘Combinatorial group theory’, Ergeb. Math. Grenzgeb. 89 (1977).
[10] J. Matthews, 'The conjugacy problem in wreath products and free metabelian groups', Trans. Amer. Math. Soc. 121 (1966), 329-339.
[11] E. I. Timoshenko, 'Conjugacy in free metabelian groups', Algebra i Logika 6 (1967), 89-94.
[12] B. A. F. Wehrfritz, 'Two examples of soluble groups that are not conjugacy separable', J. London Math. Soc. (2) 7 (1973), 312-316.

Department of Mathematics
Ruhr University
Bochum
West Germany

Department of Mathematics
University of Manitoba
Winnipeg R3T 2N2
Canada

Department of Mathematics
University of Manitoba
Winnipeg R3T 2N2
Canada


[^0]:    (c) 1989 Australian Mathematical Society $0263-6115 / 89 \$ A 2.00+0.00$

