BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 40(2), 149-180

On commutativity and finiteness in groups

Ricardo N. Oliveira and Said N. Sidki

Abstract. The second author introduced notions of weak permutablity and commutativity between groups and proved the finiteness of a group generated by two weakly permutable finite subgroups. Two groups H, K weakly commute provided there exists a bijection $f : H \to K$ which fixes the identity and such that h commutes with its image h^f for all $h \in H$. The present paper gives support to conjectures about the nilpotency of groups generated by two weakly commuting finite abelian groups H, K.

Keywords: commutativity graph, finiteness, weak commutativity, double cosets, nilpotency class, solvablity degree, group extensions.

Mathematical subject classification: Primary: 20F05, 20D15; Secondary: 2F18, 20B40.

1 Introduction

Commutativity in a group can be depicted by its commutativity graph which has for vertices the elements of the group and where two elements are joined by an edge provided they commute. Greater understanding of the commutativity graph of finite groups has been achieved in recent years and this has had important applications; see for example [5].

For a nontrivial finite p-group, it is an elementary and fundamental fact that it has a non-trivial center and therefore each element in its commutativity graph is connected to every element in the center. Now, suppose a finite group G contains a non-trivial p-group A such that every p-element in G commutes with *some* non-trivial element in A. Does it follow that G contains a non-trivial normal p-subgroup? In 1976, the second author proved in [6] results along such lines for $p = 2$ and formulated the following conjecture: *if a finite group G contains a non-trivial elementary abelian 2-group A such that every involution in G commutes with some involution from A then $A \cap O_2(G)$ is non-trivial.*

Received 3 October 2008.

This was settled in 2006 by Aschbacher, Guralnick and Segev in [1]. The proof made significant use of the classification theorem of finite simple groups. It was also shown that the result applies to the Quillen conjecture from 1978 about the Quillen complex at the prime 2; see [4].

A configuration which arises in this context is one where the commutation between elements of A and those of one of its conjugates $B = A^g$ is defined by a bijection. An approach which we had taken in 1980 to such a weak form of commutativity or permutability was through combinatorial group theory. The following finiteness criterion was proven in [7].

Theorem 1. *Let H, K be finite groups having equal orders n and let $f : H \to K$ be a bijection which fixes the identity. Then for any two maps $a : H \to K, b : H \to H$, the group*

$$G(H, K; f, a, b) = \langle H, K \mid hh^f = h^a h^b \text{ for all } h \in H \rangle$$

is finite of order at most $n \exp(n-1)$, where h^f, h^a, h^b denote the images of h under the maps f, a, b, respectively.

It is to be noted that the proof uses the same argument as that given by I.N. Sanov for the local finiteness of groups of exponent 4; see [8].

The notion of weak commutativity between H and K by way of a bijection is formalized by the group

$$G(H, K; f) = \langle H, K \mid hh^f = h^f h \text{ for all } h \in H \rangle.$$

When H is isomorphic to K, we simplify the notation to $G(H; f)$.

If f itself is an isomorphism from H onto K then $G(H; f)$ is the same group as $\chi(H)$ and f as ψ in [7]. In addition to finiteness, the operator χ preserves a number of other group properties such as being a finite p-group. Indeed, it was shown later in [3] that more generally, if H is finitely generated nilpotent then so is $\chi(H)$.

We are guided in this paper by the following conjecture.

Conjecture 1. *Let H and K be finite nilpotent groups of equal order and $f : H^\# \to K^\#$ a bijection. Then $G(H, K; f)$ is also nilpotent.*

The construction $G(H, K; f)$ lends itself well to extensions of groups, as follows. Let $\widetilde{H}, \widetilde{K}$ be groups having normal subgroups M, N respectively and let $\frac{\widetilde{H}}{M} = H$, $\frac{\widetilde{K}}{N} = K$. Let $f : H \to K, \alpha : M \to N$ be bijections both fixing e. Then, f and α can be extended in a natural manner to a bijection $f^* : \widetilde{H} \to \widetilde{K}$

fixing e such that $\widetilde{G} = G\left(\widetilde{H}, \widetilde{K}; f^*\right)$ modulo the normal closure V of $\langle M, N\rangle$ is isomorphic to $G(H, K; f)$. We use this process to produce an ascending chain of groups of $G(H, K; f)$ type. For central extensions, we prove

Theorem 2. *Maintain the above notation. Suppose M, N are central subgroups of $\widetilde{H}, \widetilde{K}$ respectively and that $G(M, N; \alpha)$ is abelian. Then, V is an abelian group. If furthermore H, K are abelian then $\left[V, \widetilde{G}\right]^2$ is central in $\widetilde{G}$.*

Although $G(H, K; f)$ is finite for finite groups, H, K, since f in general does not behave well with respect to inductive arguments, methods from finite group theory are difficult to apply. At the present stage, we have stayed close to the case where the groups H and K are isomorphic finite abelian groups and more specially to elementary abelian p -groups $A_{p,k}$ of rank k.

A step in the direction of proving nilpotency is

Theorem 3. *Suppose A, B are finite abelian groups of equal order n and let $G = G(A, B; f)$. Then, the metabelian quotient group $\frac{G}{G''}$ is nilpotent of class at most n.*

The next lemma is a natural first step in classifying the groups $G(H, K; f)$ for a fixed pair (H, K).

Lemma 1. *Let $a \in Aut(H), b \in Aut(K)$, and $g = afb$. Then, the extension $\gamma : G(H, K; f) \to G(H, K; g)$ of $h \to h^{a^{-1}}, k \to k^b$ is an isomorphism from $G(H, K; f)$ onto $G(H, K; g)$.*

Let H and K be isomorphic groups by $t : H \to K$. Then in the above lemma,

$$f = f't, g = g't, b = t^{-1}b't$$

where $f', g' \in Sym\left(H^{\#}\right)$ and $b' \in Aut(H)$; here $H^{\#}$ denotes $H \setminus \{e\}$ Therefore, $g' = af'b'$ is an element of the double coset $Aut(H)\, f'\, Aut(H)$. Thus, in order to classify $G(H; f)$ one is obliged to determine the double coset decomposition $Aut(H) \setminus Sym\left(H^{\#}\right) / Aut(H)$. When the context is clear, we refer to f simply by its factor f'.

Computations by GAP [2] produce the following data for abelian groups of small rank:

for $A_{2,3}$, $SL(3, 2) \setminus Sym(7) / SL(3, 2)$ has 4 double cosets;

for $A_{2,4}$, $SL(4, 2) \setminus Sym(15) / SL(4, 2)$ has 3374 double cosets;

for $A_{3,3}$, $PGL(3, 3) \setminus Sym(13) / PGL(3, 3)$ has 252 double cosets.

The groups $G\left(A_{p,k};\, f\right)$ have the following nilpotency classes and derived lengths.

Theorem 4.

(i) *Let $A = A_{2,k}$. If $k = 3, 4$ then $G(A;\, f)$ is a 2-group of order at most 2^{2^k+k-1}, has class at most 5 and derived length at most 3;*

(ii) *Let $A = A_{3,3}$. Then $G(A;\, f)$ is a 3-group of order at most 3^9 and has nilpotency class at most 2.*

We discuss a number of other issues. These include the reduction of the number of relations in $G(A;\, f)$, finding a bijection equivalent to f which is "closer" to being an isomorphism and also concerning f inducing a bijection between the nontrivial cyclic subgroups of A.

The paper ends with three general examples. The first is $G(A,\, f)$ where A is a field, seen as an additive group, and where f corresponds to the multiplicative inverse. The second example illustrates the construction of extensions of $G = G(A,\, f)$ which are of the same type as G; this produces metabelian 2-groups having the same order 2^{2^k+k-1} and nilpotency class k as $\chi\left(A_{2,k}\right)$, but not isomorphic to the latter group. The third is $G = G\left(A_{2,k},\, f\right)$ where f corresponds to a transposition of $A_{2,k}^{\#}$.

2 Extensions of groups

Let $\widetilde{H}, \widetilde{K}$ be groups having normal subgroups M, N and let H be a transversal of M in $\widetilde{H}$ with $e \in H$. Similarly, let K be a transversal of N in $\widetilde{K}$ with $e \in K$. We identify H with the quotient group $\widetilde{H}/M$ and K with the quotient group $\widetilde{K}/N$. Let $f : H \to K$, $\alpha : M \to N$ be bijections both fixing e. Given a bijection $\gamma : M \to N$ (not necessarily fixing e), define $f^* : \widetilde{H} \to \widetilde{K}$ by

$$f^* : m \to m^\alpha,\ f^* : mh \to m^\gamma h^f \quad \text{if} \quad h \neq e.$$

Then f^* is a bijection which fixes e and $G = G(H, K;\, f)$ is an epimorphic image of $\widetilde{G} = G\left(\widetilde{H}, \widetilde{K};\, f^*\right)$. The natural epimorphisms $\widetilde{H} \to H, \widetilde{K} \to K$ extend to an epimorphism $\widetilde{G} \to G$ having for kernel V, the normal closure of $\langle M, N\rangle$ in $\widetilde{G}$.

For any group L let v_L denote the exponent of L and $\gamma_i(L)$ the i-th term of the lower central series of L.

Define $\delta : M \to N$, $\varepsilon : M \to M$ by

$$m^\delta = m^\alpha \left(\left(m m^{\alpha\gamma^{-1}}\right)^\gamma\right)^{-1}, \qquad m^\varepsilon = m\left(\left(m^\alpha m^\gamma\right)^{\gamma^{-1}}\right)^{-1}.$$

Clearly, $m^{\delta} = e$ if and only if $m = e$ and similarly, $m^{\varepsilon} = e$ if and only if $m = e$.

Theorem 5. *Maintain the previous notation. Suppose M, N are central subgroups of $\widetilde{H}, \widetilde{K}$, respectively and that $G(M, N; \alpha)$ is abelian. Then, V is an abelian group such that*

$$V = M + N + \left[V, \widetilde{G}\right],$$
$$\left[V, \widetilde{G}\right] = \left[M^{\delta}, H\right] = \left[N^{\varepsilon}, H\right],$$
$$\left[V, \gamma_i\left(\widetilde{H}\right)\right] = \left[V, i\widetilde{H}\right]^{2^{i-1}}$$

for all $i \geq 1$ and

$$\nu_{\left[V,\widetilde{G}\right]} \mid \gcd\left(\nu_M, \nu_N, \nu_H, \nu_K\right).$$

Both sets

$$\left\{\left(m_1^{\delta}\right)^{-1}\left(m_2^{\delta}\right)^{-1}\left(m_1 m_2\right)^{\delta} \mid m_1, m_2 \in M\right\}, \quad \left\{m^{-1}\left(\left(m^{\delta}\right)^{\alpha^{-1}}\right)^{\varepsilon} \mid m \in M\right\}$$

are central in $\widetilde{G}$. Furthermore, if H, K are abelian then $\left[V, \widetilde{G}\right]^2$ is central in $\widetilde{G}$.

Proof. (1) Let $m \neq e \neq h$. Then,

$$\begin{aligned}\left[m, h^f\right] &= \left[m, m^{\alpha} h^f\right] = \left[\left(m^{\alpha\gamma^{-1}} h\right) m, m^{\alpha} h^f\right] = \left[\left(m m^{\alpha\gamma^{-1}}\right) h, m^{\alpha} h^f\right] \\ &= \left[\left(m m^{\alpha\gamma^{-1}}\right) h, \left(\left(m m^{\alpha\gamma^{-1}}\right)^{\gamma} h^f\right)^{-1} m^{\alpha} h^f\right] \\ &= \left[\left(m m^{\alpha\gamma^{-1}}\right) h, m^{\delta}\right] = \left[h, m^{\delta}\right].\end{aligned}$$

In the same manner,

$$\begin{aligned}\left[h, m^{\alpha}\right] &= \left[mh, m^{\alpha}\right] = \left[mh, m^{\gamma} h^f . m^{\alpha}\right] = \left[mh, m^{\alpha} m^{\gamma} h^f\right] \\ &= \left[\left(\left(m^{\alpha} m^{\gamma}\right)^{\gamma^{-1}} h\right)^{-1} mh, m^{\alpha} m^{\gamma} h^f\right] \\ &= \left[m^{\varepsilon}, m^{\alpha} m^{\gamma} h^f\right] = \left[m^{\varepsilon}, h^f\right].\end{aligned}$$

Since $\left[h, m^{\delta}\right] = \left[m, h^f\right]$ and $m^{\delta} = \left(m'\right)^{\alpha}$ for $m' = \left(m^{\delta}\right)^{\alpha^{-1}}$, we obtain

$$\left[\left(m'\right)^{\varepsilon}, h^f\right] = \left[h, \left(m'\right)^{\alpha}\right],$$
$$\left[\left(\left(m^{\delta}\right)^{\alpha^{-1}}\right)^{\varepsilon}, h^f\right] = \left[h, m^{\delta}\right] = \left[m, h^f\right];$$

that is, $m^{-1}\left(\left(m^{\delta}\right)^{\alpha^{-1}}\right)^{\varepsilon}$ commutes with K and is therefore central in $\widetilde{G}$.

(2) We obtain from $\left[m, h^{f}\right] = \left[h, m^{\delta}\right]$ that the sets $[m, K], \left[H, m^{\delta}\right]$ are equal and H, K normalize the subgroup $\langle [m, K]\rangle$. Also, any $m' \in M$ commutes with $\left[h, m^{\delta}\right] \left(= \left[m, h^{f}\right]\right) \in [M, K]$. Therefore, $M^{K}\left(= M^{\widetilde{K}}\right)$ is abelian.

Since $[M, K] \leq \left[H, M^{\delta}\right] \leq [N, H]$ and $[H, N] \leq [M^{\varepsilon}, K] \leq [M, K]$ we get

$$[M, K] = \left[H, M^{\delta}\right] = [H, N] = \left[M^{\varepsilon}, K\right].$$

Therefore V is abelian and

$$V = M + N + \left[M^{\delta}, H\right], \quad \left[V, \widetilde{G}\right] = \left[M^{\delta}, H\right], \quad \nu_{\left[V,\widetilde{G}\right]} \mid \gcd\left(\nu_{M}, \nu_{N}\right).$$

(3) Let $m_1, m_2 \in M$. Then,

$$\begin{aligned}
\left[m_1 m_2, h^{f}\right] &= \left[h, (m_1 m_2)^{\delta}\right], \\
\left[m_1 m_2, h^{f}\right] &= \left[m_1, h^{f}\right]^{m_2}\left[m_2, h^{f}\right] \\
&= \left[m_1, h^{f}\right]\left[m_2, h^{f}\right] \\
&= \left[h, (m_1)^{\delta}\right]\left[h, (m_2)^{\delta}\right],
\end{aligned}$$

and

$$\left[h, (m_1 m_2)^{\delta}\right] = \left[h, (m_1)^{\delta}\right]\left[h, (m_2)^{\delta}\right].$$

Thus,

$$\left\{\left(m_1^{\delta}\right)^{-1}\left(m_2^{\delta}\right)^{-1}(m_1 m_2)^{\delta} \mid m_1, m_2 \in M\right\}$$

is central in $\widetilde{G}$ and likewise for

$$\left\{\left(m_1^{\varepsilon}\right)^{-1}\left(m_2^{\varepsilon}\right)^{-1}(m_1 m_2)^{\varepsilon} \mid m_1, m_2 \in M\right\}.$$

(4) Since any $h \in H$ centralizes $\left\langle M, h^{f}\right\rangle$, we have for all $m \in M$,

$$\left[m, h^{f}, h\right] = e = \left[m^{\delta}, h, h\right]$$

and so,

$$\left[m^{\delta}, h, h\right] = e, \left[m^{\delta}, h^{i}\right] = \left[m^{\delta}, h\right]^{i}$$

for all $v \in V$ and all integers i. Therefore,

$$\nu_{\left[V,\widetilde{G}\right]} \mid \gcd\left(\nu_{N}, \nu_{H}\right), \gcd\left(\nu_{M}, \nu_{K}\right).$$

We calculate for $h_1, h_2 \in H$

$$\begin{aligned}
\left[m^\delta, (h_1h_2)^{-1}\right] &= \left[m^\delta, h_1h_2\right]^{-1},\\
\left[m^\delta, h_2^{-1}h_1^{-1}\right] &= \left[m^\delta, h_1h_2\right]^{-1},\\
\left[m^\delta, h_1^{-1}\right]\left[m^\delta, h_2^{-1}\right]^{h_1^{-1}} &= \left(\left[m^\delta, h_2\right]\left[m^\delta, h_1\right]^{h_2}\right)^{-1},\\
\left[m^\delta, h_1\right]\left[m^\delta, h_2\right]^{h_1^{-1}} &= \left[m^\delta, h_2\right]\left[m^\delta, h_1\right]^{h_2},\\
\left[m^\delta, h_2\right]^{-1}\left[m^\delta, h_2\right]^{h_1^{-1}} &= \left[m^\delta, h_1\right]^{-1}\left[m^\delta, h_1\right]^{h_2},\\
\left[m^\delta, h_2, h_1^{-1}\right] &= \left[m^\delta, h_1, h_2\right].
\end{aligned}$$

Therefore,

$$\begin{aligned}
\left[m^\delta, h_1, h_2\right] &= \left[m^\delta, h_2, h_1^{-1}\right] = \left[m^\delta, h_1^{-1}, h_2^{-1}\right] = \left[m^\delta, h_1, h_2^{-1}\right]^{-1},\\
\left[m^\delta, h_1, h_2\right]^{-1} &= \left[m^\delta, h_1, h_2^{-1}\right],\\
\left[m^\delta, h_1, h_2\right] &= \left[m^\delta, h_2, h_1^{-1}\right] = \left[m^\delta, h_2, h_1\right]^{-1}.
\end{aligned}$$

Calculate further

$$\begin{aligned}
\left[m^\delta, h_1h_2\right] &= \left[m^\delta, h_2\right]\left[m^\delta, h_1\right]^{h_2} = \left[m^\delta, h_2\right]\left[m^\delta, h_1\right]\left[m^\delta, h_1, h_2\right],\\
\left[m^\delta, h_1h_2, h_1h_2\right] &= \left[m^\delta, h_2, h_1h_2\right]\left[m^\delta, h_1, h_1h_2\right]\left[m^\delta, h_1, h_2, h_1h_2\right]\\
&= \left[m^\delta, h_2, h_1\right]\left[m^\delta, h_2, h_1, h_2\right]\left[m^\delta, h_1, h_2\right]\\
&\quad \left[m^\delta, h_1, h_2, h_2\right]\left[m^\delta, h_1, h_2, h_1\right].\left[m^\delta, h_1, h_2, h_1, h_2\right]\\
&= \left[m^\delta, h_1, h_2, h_1\right]^{h_2} = e.
\end{aligned}$$

We conclude

$$\left[m^\delta, h_2, h_1, h_1\right] = e.$$

Thus,

$$[v, h, h] = e$$

for all $v \in V$.

When V is written additively, the action of h on V can be expressed as

$$v\,(-1+h)^2 = 0.$$

From this we derive the following formulae for the action of H on V:

for $h_1, h_2, \ldots, h_i \in H$,

$$\begin{aligned} h_2 h_1 &= -2 + 2h_1 + 2h_2 - h_1 h_2, \\ h_1^{-1} h_2 h_1 &= -2 + 2h_1 + 3h_2 - 2h_1 h_2, \\ -1 + [h_2, h_1] &= -2\,(-1 + h_1)\,(-1 + h_2)\,, \\ -1 + [h_i, \ldots, h_2, h_1] &= (-2)^{i-1}\,(-1 + h_1)\,(-1 + h_2)\ldots(-1 + h_i)\,. \end{aligned}$$

In other words,

$$\begin{aligned} [v, [h_i, \ldots, h_2, h_1]] &= [v, h_1, h_2, \ldots, h_i]^{(-2)^{i-1}}\,, \\ \left[V, \gamma_i\left(\widetilde{H}\right)\right] &= \left[V, i\widetilde{H}\right]^{2^{i-1}}\,. \end{aligned}$$

(5) Suppose H, K abelian. Then

$$[v, [h_1, h_2]] = [v, h_1, h_2]^2 = \left[[v, h_1]^2, h_2\right] = e.$$

As $\left[V, \widetilde{G}\right] = [V, H] = [V, K]$, we conclude that $\left[V, \widetilde{G}\right]^2$ is central. □

Theorem 6. *Suppose in the above, $\widetilde{H}, \widetilde{K}$ are finite groups and let $M = \langle m\rangle$, $N = \langle n\rangle$ be cyclic central subgroups of $\widetilde{H}, \widetilde{K}$ respectively, each of prime order p. Then, $\langle M, N\rangle^{\widetilde{G}}$ is an elementary abelian p-subgroup of rank at most $|H| + 1$.*

Proof. We have $[M, N] = \{e\}$, $[M, K] = [H, N]$ elementary p-abelian subgroup and M, N centralize $[M, K]$. Therefore,

$$\langle M, N\rangle^{\widetilde{G}} = \langle M, N\rangle^{G} = \left\langle m^K, n\right\rangle = \left\langle m, n^H\right\rangle$$

is an elementary abelian p-subgroup of rank at most $|K| + 1$. □

3 Metabelian quotients of $G(A, B, f)$

It would be interesting to resolve the question of nilpotency of the solvable quotients of $G(H, K; f)$. In the next result we consider metabelian quotients of $G(A, B; f)$.

Theorem 7. *Suppose A, B are finite abelian groups of equal order n and let $G = G(A, B; f)$. Then, the metabelian quotient group G/G'' is nilpotent of class at most n.*

Proof. In a metabelian group M, if $u \in M'$ and $x_i \in M$ $(1 \leq i \leq k)$ then

$$\left[u, x_1, x_2, \ldots, x_k\right] = \left[u, x_{i_1}, x_{i_2}, \ldots, x_{i_k}\right]$$

for any permutation $(i_1, i_2 \ldots, i_k)$ of $\{1, 2, \ldots, k\}$.

We have from the relations of G,

$$[a, b] = \left[a, \left(a^f\right)^{-1} b\right] = \left[a. \left(b^{f^{-1}}\right)^{-1}, b\right].$$

Let $a \in A, b_1, b_2 \in B$. As a^f and $b_1^{f^{-1}}$ commute with both a, b_1, it follows that

$$\begin{aligned} [a, b_1, b_2] &= \left[a, b_1, \left(a^f\right)^{-1}.b_2\right] \\ &= \left[a. \left(b_1^{f^{-1}}\right)^{-1}, b_1, b_2\right] \\ &= \left[a, b_1, \left(a. \left(b_1^{f^{-1}}\right)^{-1}\right)^f b_2\right]. \end{aligned}$$

We observe that if $b_1 = b_2 \neq a^f$, then $b_1 \neq \left(a. \left(b_1^{f^{-1}}\right)^{-1}\right)^f b_2$.

Now, we will work in G modulo G''.

Let $a \in A$, b_i $(2 \leq i \leq k) \in B$. From Witt's formula, as A, B are abelian, we have

$$\left[a, b_2, b_1\right] = \left[a, b_1, b_2\right]$$

and more generally,

$$\left[a, b_1, b_2, \ldots, b_k\right] = \left[a, b_{i_1}, b_{i_2}, \ldots, b_{i_k}\right]$$

for any permutation $(i_1, i_2 \ldots, i_k)$ of $\{1, 2, \ldots, k\}$.

Therefore, if

$$\left\{x_2, \ldots, x_k\right\} = \left\{b_2, \ldots, b_s, a_{s+1}, \ldots, a_k\right\}$$

with $b_2, \ldots, b_s \in B$ and $a_{s+1}, \ldots, a_{s+k} \in A$ then

$$\left[a, b_1, x_2, \ldots, x_k\right] = \left[a, b_1, b_2, \ldots, b_s, a_{s+1}, \ldots, a_k\right].$$

Let again $a \in A$, b_i $(2 \leq i \leq k) \in B$. Suppose that $b_1, b_2, \ldots, b_{k-1}, a^f$ are distinct.

Then,

$$b_k, \left(a.\left(b_1^{f^{-1}}\right)^{-1}\right)^f b_k, \ldots, \left(a.\left(b_{k-1}^{f^{-1}}\right)^{-1}\right)^f b_k$$

are k distinct elements of B.

Suppose further that $b_k = b_j$ for some $1 \leq j \leq k-1$. Then, for some i,

$$b'_{ij} = \left(a.\left(b_i^{f^{-1}}\right)^{-1}\right)^f b_j \notin \{b_1, b_2, \ldots, b_{k-1}\}.$$

In this manner, we have

$$\begin{aligned}
[a, b_1, b_2, .., b_{k-1}, b_k] &= [a, b_1, b_2, \ldots, b_{k-1}, b_j] \\
&= [a, b_i, b_j, b_l, \ldots, b_m] \\
&= [a, b_i, b'_{ij}, b_l, \ldots, b_m] \\
&= [a, b_1, b_2, \ldots, b_{k-1}, b'_{ij}]
\end{aligned}$$

and $b_1, b_2, \ldots, b'_{ij}$ are distinct. If $k = n$ then $[a, b_1, b_2, \ldots, b_n] = e$ and G is nilpotent of class at most n. □

The limit n obtained in the proof is clearly too large, especially when compared with available results. Determining the nilpotency degree seems to stem from a more general problem which can be formulated for commutative rings.

Problem 1. *Let A be a free abelian group of rank m generated by $a_1, \ldots, a_m$ and let A act on a torsion-free $\mathbb{Z}$-module V. Let n be a natural number. Define*

$$S(m,n) = \left\{ \begin{array}{c} a_{i_1}^{l_1} a_{i_2}^{l_2} \ldots a_{i_s}^{l_s} a_{i_s+1} \mid 0 \leq s \leq m-1, \\ 1 \leq i_1 < i_2 < \cdots < i_s < m, \\ 1 \leq l_i \leq n-1 \end{array} \right\}.$$

This set corresponds to a choice of a generator for each of the different cyclic subgroups of order n in A/A^n. For instance, $S(2,3) = \{a_1, a_2, a_1a_2, a_1^2a_2\}$. Let f be a permutation of $S(m,n)$ and define

$$U(m,n;f) = \left\{(1-x)\left(1-x^f\right) \mid x \in S(m,n)\right\}.$$

Suppose that A acts on V such that $U(m,n;f) = \{0\}$. Prove that the action of A on V is nilpotent. Moreover, that it has nilpotency degree at most 3 for $n = 2$ and degree at most 2 for $n \geq 3$. The small bounds have been confirmed by a number of examples using the Groebner basis applied to $Q[a_1, a_2, \ldots, a_n]$ modulo the ideal generated by $U(m,n;f)$.

4 Reduction of the presentation of $\chi(A)$

It is interesting to reduce the number of relations in the definition of $G(A, f)$, particularly for the sake of applications. This is difficult to carry out in general. We treat here the question for the group $\chi(A)$. Given a generating set S of A then define

$$\chi(A, S; m) = \left\langle A, A^{\psi} \mid \left[a, a^{\psi}\right] = e \text{ for all } a \in \cup_{1 \le i \le m} S^i \right\rangle.$$

The construction $\chi(A, S; 1)$ does not conserve finiteness in general. For let $A = A_{2,2}$ be generated by $S = \{a_1, a_2\}$. Then, on defining $x_1 = a_1 a_2^{\psi}, x_2 = a_1^{\psi} a_2$, we find $\chi(A, S; 1) = \langle x_1, x_2 \rangle A$, where $\langle x_1, x_2 \rangle$ is free abelian of rank 2.

We start with

Proposition 1. *Let H be a group generated by x_1, x_2, y_1, y_2 such that $\left[y_1, x_1\right] = e = \left[y_2, x_2\right]$. Then*

(i) $\left[y_1 y_2, x_1 x_2\right] = \left[y_1^{y_2}, x_2\right]\left[y_2, x_1^{x_2}\right]$;

(ii) *if in addition $\left[x_1, x_2\right] = \left[y_1, y_2\right] = e$ holds then*

$$\left[y_1 y_2, x_1 x_2\right] = \left[y_1, x_2\right]\left[y_2, x_1\right] \text{ (*);}$$

(iii) *if furthermore $\left[y_1 y_2, x_1 x_2\right] = e$ holds then H is nilpotent of class at most 2 with derived subgroup $H' = \left\langle \left[y_1, x_2\right] \right\rangle$.*

Proof. The first two items are shown directly. The last item follows from

$$\begin{aligned} \left[y_1, x_2\right] &= \left[x_1, y_2\right], \left[y_1, x_2\right]^{x_1} = \left[y_1, x_2\right], \\ \left[y_1, x_2\right]^{x_2} &= \left[x_1, y_2\right]^{x_2} = \left[x_1, y_2\right]. \end{aligned}$$

□

Corollary 1. *Let A be an abelian group generated by $S = \{a_1, a_2\}$ and let $G = \chi(A, S; 2)$. Then, $G = \chi(A)$.*

For abelian groups A of rank 3, the situation becomes less simple.

Proposition 2. *Let A be an abelian group generated by $S = \langle a_i | 1 \le i \le 3 \rangle$. Then the following equations hold in $G = \chi(A, S; 2)$:*

$$\xi = \left[a_1^{\psi} a_2^{\psi} a_3^{\psi}, a_1 a_2 a_3\right] = \left[a_1^{\psi}, a_3\right]^{a_2^{\psi}} \left[a_3^{\psi}, a_1\right]^{a_2},$$

$$\left[a_1^{\psi}, a_3^2\right]^{[a_2, \psi]} = \left[a_1^{\psi}, a_3^2\right].$$

Proof. On substituting $x_1 = a_1a_2$, $x_2 = a_3$, $y_1 = a_1^{\psi}a_2^{\psi}$, $y_2 = a_3^{\psi}$ in (*) of the previous proposition, we obtain

$$\begin{aligned}
\xi &= \left[a_1^{\psi}a_2^{\psi}a_3^{\psi}, a_1a_2a_3\right] \\
&= \left[a_1^{\psi}, a_3\right]^{a_2^{\psi}}\left[a_2^{\psi}, a_3\right]\left[a_3^{\psi}, a_2\right]\left[a_3^{\psi}, a_1\right]^{a_2} \\
&= \left[a_1^{\psi}, a_3\right]^{a_2^{\psi}}\left[a_2^{\psi}, a_3\right]\left[a_3, a_2^{\psi}\right]\left[a_3^{\psi}, a_1\right]^{a_2} \\
&= \left[a_1^{\psi}, a_3\right]^{a_2^{\psi}}\left[a_3^{\psi}, a_1\right]^{a_2}.
\end{aligned}$$

Substitute $a_1 \leftrightarrow a_3$, $a_2 \leftrightarrow a_2$, $\psi \to \psi$ above to obtain

$$\xi = \left[a_3^{\psi}, a_1\right]^{a_2^{\psi}}\left[a_1, a_3^{\psi}\right]^{a_2}.$$

Therefore, since $\left[a_1, a_3^{\psi}\right] = \left[a_1^{\psi}, a_3\right]$, and $\left\langle a_1, a_3, a_1^{\psi}, a_3^{\psi}\right\rangle$ has class at most 2, we have

$$\begin{aligned}
\left[a_1^{\psi}, a_3\right]^{a_2^{\psi}}\left[a_3^{\psi}, a_1\right]^{a_2} &= \left[a_3^{\psi}, a_1\right]^{a_2^{\psi}}\left[a_1, a_3^{\psi}\right]^{a_2}, \\
\left[a_1^{\psi}, a_3\right]^{a_2^{\psi}}\left[a_3^{\psi}, a_1\right]^{a_2} &= \left[a_3, a_1^{\psi}\right]^{a_2^{\psi}}\left[a_1, a_3^{\psi}\right]^{a_2}, \\
\left[a_1^{\psi}, a_3\right]^{2a_2^{\psi}} &= \left[a_1^{\psi}, a_3\right]^{2a_2}, \\
\left[a_1^{\psi}, a_3^2\right]^{a_2^{\psi}} &= \left[a_1^{\psi}, a_3^2\right]^{a_2} \\
\left[a_1^{\psi}, a_3^2\right]^{[a_2,\psi]} &= \left[a_1^{\psi}, a_3^2\right].
\end{aligned}$$

Suppose A has odd order. Then,

$$\left[a_1^{\psi}, a_3\right]^{[a_2,\psi]} = \left[a_1^{\psi}, a_3\right]$$

and therefore $\xi = \left[a_1^{\psi}a_2^{\psi}a_3^{\psi}, a_1a_2a_3\right] = e$. By the previous corollary, we can substitute the a_i's by their powers in this last equation. □

For groups A of odd order the reduction is drastic.

Corollary 2. *Let A be a finite abelian group of odd order generated by S and $G = \chi(A, S; 2)$. Then, $G = \chi(A)$.*

Proof. Let $|S| = m \geq 3$. We proceed by induction on m. By the previous proposition, $\chi(A;2) = \chi(A;3)$. We assume $\chi(A;2) = \chi(A;m-1)$. Then we simply apply our argument to the set.

$$\left\{a_1, a_2, \ldots, a_{m-2,} a_{m-1}a_m\right\}$$

with $m-1$ elements and obtain

$$\left[a_1^{\psi} a_2^{\psi} \ldots a_{m-2}^{\psi} \left(a_{m-1}a_m\right)^{\psi}, a_1 a_2 \ldots a_{m-2} \left(a_{m-1}a_m\right)\right] = e.$$

□

Example 1. The following example provides us with a glimpse into the problem of reduction of the presentation of $G\left(A_{p,k}, f\right)$ in general and how it compares with that of $\chi\left(A_{p,k}\right)$.

Let A, B be isomorphic to $A_{p,3}$ with respective generators $\{a_1, a_2, a_3\}$, $\{b_1, b_2, b_3\}$. Define

$$G = \left\langle \begin{array}{c} A, B \mid \left[a_i, b_i\right] = e \left(i = 1, 2, 3\right), \\ \left[a_1a_2, b_1b_2^{-1}\right] = \left[a_1a_3, b_1b_3\right] = \left[a_2a_3, b_2b_3\right] = e \end{array} \right\rangle.$$

With the use of GAP, we find that the resulting group for $p = 3, 5, 7$ to be finite metabelian of order p^{11} and of nilpotency class 3. We also find that

$$\left[a_1a_2^{-1}, b_1b_2\right] = \left[a_1a_3^{-1}, b_1b_3^{-1}\right] = \left[a_2a_3^{-1}, b_2b_3^{-1}\right] = e$$

hold but

$$\left[a_1a_2a_3, b_1^i b_2^j b_3\right] \neq e \quad \text{for any} \quad 1 \leq i, j \leq p-1.$$

These results should be compared with those for $\chi\left(A_{p,3}\right)$ which has order p^9 and nilpotency class 2.

We go back to the case $\chi\left(A_{p,3}\right)$ for $p = 2$.

Theorem 8. *Let $A_{2,3}$ be generated by*

$$S = \left\{a_1, a_2, a_3\right\}, G = \chi\left(A_{2,3}, S; 2\right) \quad \textit{and} \quad \xi = \left[a_1^{\psi} a_2^{\psi} a_3^{\psi}, a_1a_2a_3\right].$$

Then the kernel K of the epimorphism $\phi : G \to \chi\left(A_{2,3}\right)$ extended from $a_i \to a_i, a_i^{\psi} \to a_i^{\psi}$ $\left(i = 1, 2, 3\right)$ is the normal closure of $\langle\xi\rangle$ in G and is free abelian of rank 4.

Proof. We will show that K is freely generated by

$$\left\{\xi, \xi^{a_i} \ (i = 1, 2, 3)\right\}$$

and that G acts on it as follows: for $\{i, j, k\} = \{1, 2, 3\}$,

$$\xi^{\psi} = \xi^{-1}, \xi^{a_i^{\psi}} = \xi^{-a_i}, \xi^{a_i a_j} = \xi^{-a_k} = \xi^{a_j a_i^{\psi}}.$$

We sketch the proof. First, we derive the table

$$\begin{aligned}
\left[a_3^{\psi}, a_2, a_1\right]^{a_2^{\psi}} &= \left[a_2^{\psi}, a_1, a_3\right]^{-1}, \left[a_3^{\psi}, a_2, a_1\right]^{a_3^{\psi}} = \left[a_1^{\psi}, a_3, a_2\right]^{-1}, \\
\left[a_3, a_2^{\psi}, a_1^{\psi}\right]^{a_2} &= \left[a_2, a_1^{\psi}, a_3^{\psi}\right]^{-1}, \left[a_3, a_2^{\psi}, a_1^{\psi}\right]^{a_3} = \left[a_1, a_3^{\psi}, a_2^{\psi}\right]^{-1}, \\
\left[a_3^{\psi}, a_2, a_1^{\psi}\right]^{a_2} &= \left[a_2^{\psi}, a_1, a_3^{\psi}\right]^{-1}, \left[a_3^{\psi}, a_2, a_1^{\psi}\right]^{a_3} = \left[a_1^{\psi}, a_3, a_2^{\psi}\right]^{-1}, \\
\left[a_1^{\psi}, a_2, a_3^{\psi}\right]^{a_1} &= \left[a_3^{\psi}, a_1, a_2^{\psi}\right]^{-1}, \left[a_1^{\psi}, a_3, a_2^{\psi}\right]^{a_1} = \left[a_2^{\psi}, a_1, a_3^{\psi}\right]^{-1}, \\
\left[a_2^{\psi}, a_1, a_3^{\psi}\right]^{a_2} &= \left[a_3^{\psi}, a_2, a_1^{\psi}\right]^{-1}.
\end{aligned}$$

From this table we conclude that the subgroup generated by

$$\left\{\left[a_3^{\psi}, a_2, a_1\right], \left[a_1^{\psi}, a_3, a_2\right], \left[a_2^{\psi}, a_1, a_3\right], \left[a_3^{\psi}, a_2, a_1\right]^{a_1^{\psi}}\right\}$$

is abelian and normal in G.

Next, we find

$$\begin{aligned}
\xi &= \left[a_1^{\psi} a_2^{\psi} a_3^{\psi}, a_1 a_2 a_3\right] = \left[a_2^{\psi}, \left[a_3^{\psi}, a_1\right]\right]\left[a_3^{\psi}, a_1, a_2\right] \\
&= \left[a_2^{\psi}, \left[a_1^{\psi}, a_3\right]\right]\left[a_1^{\psi}, a_3, a_2\right]
\end{aligned}$$

and by permuting the a_i's, the following holds

$$\begin{aligned}
\xi &= \left[a_3^{\psi}, \left[a_2^{\psi}, a_1\right]\right]\left[a_2^{\psi}, a_1, a_3\right] = \left[a_1^{\psi}, \left[a_3^{\psi}, a_2\right]\right]\left[a_3^{\psi}, a_2, a_1\right] \\
&= \left[a_1^{\psi}, \left[a_2^{\psi}, a_3\right]\right]\left[a_2^{\psi}, a_3, a_1\right].
\end{aligned}$$

It is straightforward to obtain the action of G on $\{\xi, \xi^{a_i} \ (i = 1, 2, 3)\}$, as described above.

Let $\mathbb{Z}[x, y, z]$ be the polynomial ring in the variables x, y, z with coefficients from $\mathbb{Z}$. The proof is finished by constructing the group as a subgroup of $GL(5, \mathbb{Z}[x, y, z])$:

$$a_1 \to \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ x & -x & y & y & 1 \end{pmatrix}, \quad a_2 \to \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ x & y & -x & y & 1 \end{pmatrix},$$

$$a_3 \to \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ x & y & y & -x & 1 \end{pmatrix}, \quad a_1^{\psi} \to \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ w & w & y & y & 1 \end{pmatrix},$$

$$a_2^{\psi} \to \begin{pmatrix} 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ w & y & w & y & 1 \end{pmatrix}, \quad a_3^{\psi} \to \begin{pmatrix} 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ w & y & y & w & 1 \end{pmatrix}$$

from which we find that

$$\xi \to \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ z & 0 & 0 & 0 & 1 \end{pmatrix}$$

where $z = 4(-x - y + w)$. □

5 Fixing a basis

Let $A = A_{p,k}$ be written additively and let $\mathcal{B}_k$ be the set of bases of A. We will show that for any bijection $f : A \to A$ fixing 0, the set $\mathcal{B}_k \cap \mathcal{B}_k^f$ is nonempty; indeed,

$$\lim_{p\to\infty} \frac{\left|\mathcal{B}_k \cap \mathcal{B}_k^f\right|}{|\mathcal{B}_k|} = 1.$$

Example 2.

(i) The following easy example shows that for p odd, a bijection $f : A \to A$ may be linear when restricted to each of the 1 -dimensional subspaces and may also permute $\mathcal{B}_k$, without being a linear transformation. Let $A = A_{p,2}$ be generated by a_1, a_2 and define $f : A \to A$ by $f : ia_1 \to ia_1, ia_2 \to ia_2, i(a_1 + ja_2) \to i(a_1 - ja_2)$ for $0 \leq i, j \leq p-1, j \neq 0$.

(ii) A map f is *anti-additive* provided $(x+y)^f \neq x^f + y^f$ for all x, y such that $0 \notin \{x, y, x+y\}$. Let F be a field of characteristic different from 3 and such that its multiplicative group $F^{\#}$ does not contain elements of order 3. Then, multiplicative inversion defined by $f : 0 \to 0, x \to x^{-1}$ is anti-additive.

Concerning the first example, the situation for $k \geq 3$ is quite different as can be seen from a result of R. Baer from 1939 ([9], Th. 2, page 35):

> *let G be an abelian p-group such that G contains an element of order p^n and contains at least 3 independent elements of such order. Then any projectivity of G onto another abelian group H is induced by an isomorphism.*

It follows then

Lemma 2. *Let $A = A_{p,k}$. Suppose f is a permutation of $A^{\#}$. If f permutes the set $\mathcal{B}_k$ of bases of A then f is a linear transformation when $k \geq 3$ and when $p = 2, k = 2$.*

Proof. As f permutes the set B_k of bases of A, it induces a projectivity on A. The case $p = 2, k = 2$ is easy. □

Definition 1. *Let $A = A_{p,k}$ and f be a permutation of $A^{\#}$. A subset C of A of linearly independent elements is said to be f-independent if C^f is also a linearly independent set. Let $N(p, j)$ denote the number of f-independent subsets C of A with $|C| = j$.*

Proposition 3. *Maintain the previous notation. Then, the following inequality holds for all $k \geq 1$,*

$$N(p,k) \geq \left(p^k - 1\right) \prod_{1 \leq i \leq k-1} \frac{p^{k-j} - 1}{p-1} \left(p^j - 2p^{j-1} + j + 1\right).$$

Furthermore, $\lim_{p\to\infty} \dfrac{\left|\mathcal{B}_k \cap \mathcal{B}_k^f\right|}{|\mathcal{B}_k|} = 1.$

Proof. Clearly, $N(p,1) = p^k - 1$. Let $k \geq 2$, C be f-independent and $|C| = j \geq 1$. Denote $U = \langle C \rangle$, $W = \langle C^f \rangle$. Then,

$$\begin{aligned} |U| &= |W| = p^j, \\ \left|U^{\#} - C\right| &= \left|W^{\#} - C^f\right| = \left(p^j - 1\right) - j. \end{aligned}$$

Suppose $U \neq A$. There are $\dfrac{p^{k-j}-1}{p-1}$ non-trivial cyclic subgroups in the quotient group A/U. For each such cyclic subgroup, choose a representative P in A and also choose a generator v for each P.

Fix such a $P = \langle v \rangle$. Then, each element in the set

$$L = \left\{u + iv \mid u \in U, 1 \leq i \leq p-1\right\}$$

is independent of C and $|L| = \left|L^f\right| = p^j(p-1)$. The elements of $L^f \backslash W^{\#} = L^f \backslash \left(W^{\#} - C^f\right)$ are independent of C^f and

$$\begin{aligned} \left|L^f \backslash W^{\#}\right| &\geq p^j(p-1) - \left(p^j - 1 - j\right) \\ &= p^{j+1} - 2p^j + j + 1. \end{aligned}$$

Therefore,

$$N(p, j+1) \geq N(p,j) \frac{p^{k-j}-1}{p-1}\left(p^{j+1} - 2p^j + j + 1\right)$$

and

$$N(p,k) \geq \left(p^k - 1\right) \prod_{1 \leq j \leq k-1} \frac{p^{k-j}-1}{p-1}\left(p^{j+1} - 2p^j + j + 1\right).$$

Finally, since

$$\begin{aligned} |\mathcal{B}_k| &= \prod_{0 \leq j \leq k-1} \left(p^k - p^j\right) = p^{\binom{k}{2}} \prod_{0 \leq j \leq k-1} \left(p^{k-j} - 1\right), \\ N(p,k) &= \left|\mathcal{B}_k \cap \mathcal{B}_k^f\right|, \end{aligned}$$

we conclude

$$\frac{\left|\mathcal{B}_k \cap \mathcal{B}_k^f\right|}{|\mathcal{B}_k|} \geq \frac{\prod_{1\leq j\leq k-1}\left(p^{j+1}-2p^j+j+1\right)}{(p-1)^{k-1}\,p^{\binom{k}{2}}}$$

and $\lim_{p\to\infty} \dfrac{\left|\mathcal{B}_k \cap \mathcal{B}_k^f\right|}{|\mathcal{B}_k|} = 1$ follows easily. □

Corollary 3. *Let $f\colon A_{p,k}^{\#} \to A_{p,k}^{\#}$ be a bijection. Then there exists g an element in the double coset $GL(k,p).f.GL(k,p)$ and there exists a basis C of $A_{p,k}^{\#}$ such that g fixes point-wise the elements of C.*

6 Permuting the set of cyclic subgroups

The commutation between two elements in a group imply the commutation of the cyclic groups generated by them. For this reason, it is important to consider commutation correspondence between cyclic subgroups.

Let $A = A_{p,k}$ and let f be a permutation of $A^{\#}$. Define $R \subset A_{p,k}^{\#} \times A_{p,k}^{\#}$ by

$$R = \left\{(a^i, b^j)\ (1 \leq i, j \leq p-1) \mid a^f = b\right\}.$$

We will prove that R contains at least $p-1$ permutations g of $A_{p,k}^{\#}$ such that $\left(a^i\right)^g = \left(a^g\right)^i$ for all $1 \leq i \leq p-1$. Therefore, $G\left(A_{p,k}; f\right)$ is a quotient of $G\left(A_{p,k}; g\right)$ for each one of these g's. For this purpose, we construct a multi-edge digraph L from R, having vertices the non-trivial cyclic subgroups C_i of A and edges $\left(C, C'\right)$ whenever $C = \left\langle a^i \right\rangle$, $C' = \left\langle \left(a'\right)^j \right\rangle$ and $f : a^i \to \left(a'\right)^j$. Then L is a regular graph, in the sense that there are exactly $p-1$ edges coming into and $p-1$ edges leaving each vertex.

We enumerate the vertices of L and let $N = \left(N_{ij}\right)$ be the incidence matrix with respect to this enumeration; that is $N_{ij} = l$ if and only there is a total of l edges connecting the vertex i to the vertex j. Then N is doubly stochastic, as all row and column sums of N are equal to $p-1$. A permutation g contained in R corresponds to a non-zero monomial $N_{1,1^\sigma} N_{2,2^\sigma} \ldots N_{k,k^\sigma}$ for some permutation σ of $\{1, 2, \ldots, k\}$.

Definition 2. *Let $M = \left(M_{ij}\right)$, $N = \left(N_{ij}\right)$ be $k \times k$ matrices over the real numbers. Then, (i) M, N are equivalent provided there exist permutational matrices S, T such that $M = SNT$; (ii) N is said to be totally singular provided*

$$N_{1,1^\sigma} N_{2,2^\sigma} \ldots N_{k,k^\sigma} = 0$$

for all permutations σ *of* $\{1, 2, \ldots, k\}$.

Proposition 4. *Let* N *be a totally singular* $k \times k$ *matrix over the real numbers. Then* N *is equivalent to a matrix which contains a submatrix* $0_{(k-l)\times(l+1)}$ *for some* $l \geq 0$.

Proof. By induction on k. The cases $k = 2, 3$ are easy; that is, if $k = 2$ then N is equivalent to $\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$ and the if $k = 3$ then N is equivalent to one of

$$\begin{pmatrix} * & * & 0 \\ * & * & 0 \\ * & * & 0 \end{pmatrix}, \quad \begin{pmatrix} * & * & * \\ * & 0 & 0 \\ * & 0 & 0 \end{pmatrix}.$$

Suppose that the assertion is true for k. We consider N of dimension $k + 1$. Then, we can assume that there exist an $l \geq 0$ such that

$$N = \begin{pmatrix} a_{11} & \ldots & U_{1\times(l+1)} \\ V_{l\times 1} & B_{l\times(k-l-1)} & C_{l\times(l+1)} \\ W_{(k-l)\times 1} & D_{(k-l)\times(k-l-1)} & 0_{(k-l)\times(l+1)} \end{pmatrix}.$$

If $U_{1\times(l+1)}$ or any row of $C_{l\times(l+1)}$ is null then we obtain the desired form. We can also assume that $U_{1\times(l+1)} = (\ldots, a_{1k})$, $a_{1k} > 0$. Therefore, we have the $(l + 1) \times (l + 1)$ matrix

$$\begin{pmatrix} U_{1\times(l+1)} \\ C_{l\times(l+1)} \end{pmatrix} = \begin{pmatrix} \ldots & a_{1k} \\ R_{l\times l} & S_{l\times 1} \end{pmatrix}.$$

We have

$$Y_{(k-l)\times(k-l)} = \begin{pmatrix} W_{(k-l)\times 1} & D_{(k-l)\times(k-l-1)} \end{pmatrix}$$

and therefore

$$N = \begin{pmatrix} * & Z_{(l+1)\times(l+1)} \\ Y_{(k-l)\times(k-l)} & 0_{(k-l)\times(l+1)} \end{pmatrix}.$$

Now, one of $Y_{(k-l)\times(k-l)}$, $Z_{(l+1)\times(l+1)}$ is totally singular; suppose it is the first one. Then we may assume

$$Y_{(k-l)\times(k-l)} = \begin{pmatrix} \ldots & Y'_{m\times(m+1)} \\ \ldots & 0_{(k-l-m)\times(m+1)} \end{pmatrix}.$$

Hence

$$N = \begin{pmatrix} & * & Z_{(l+1)\times(l+1)} \\ \ldots & Y'_{m\times(m+1)} & \\ \ldots & 0_{(k-l-m)\times(m+1)} & 0_{(k-l)\times(l+1)} \end{pmatrix}$$

and we obtain in N a $(k - l - m) \times (m + 1 + l + 1)$ block of zeroes where the sum of the dimensions is $k + 1$. □

Corollary 4. *Maintain the previous notation. Suppose the entries of N are non-negative. If in addition N is doubly stochastic then $N = 0$.*

Proof. Let the row sum be s. There exists $l \geq 0$ such that

$$N = \begin{pmatrix} X_{l\times(k-l)} & Z_{l\times(l+1)} \\ Y_{(k-l)\times(k-l)} & 0_{(k-l)\times(l+1)} \end{pmatrix}.$$

Therefore the column sum of $\begin{pmatrix} Z_{l\times(l+1)} \\ 0_{(k-l)\times(l+1)} \end{pmatrix}$ is $(l+1)\,s$ whereas the row sum is at most ls; hence $s = 0$. □

We go back to our graph L and its incidence matrix N which is doubly stochastic with $s = p - 1$. Then there exists a monomial $N_{1,1^\sigma} N_{2,2^\sigma} \ldots N_{k,k^\sigma} \neq 0$ and so $N_{i,i^\sigma} \neq 0$ for all i. This produces for us a bijection $g : A^{\#}_{p,k} \to A^{\#}_{p,k}$. By removing the edges corresponding to g, the graph L is reduced to one which is $(s-1)$-regular. Therefore, we can produce in this manner $p-1$ permutations g. Clearly, if f is an isomorphism on the cyclic subgroups then all the permutations g are equal.

7 Classification of $G(A; f)$ for A of small rank

We treat in this section groups $G(A, B; f)$ were A, B are finite abelian groups generated by at most 4 elements.

Proposition 5. *Suppose $A = \langle a \rangle, B = \langle b \rangle$ are cyclic groups having equal finite orders n. Then, $G = G(A, B; f)$ is isomorphic to $A \times B$.*

Proof. Suppose G is not abelian. Let $1 < r, s < n$ be minimal integers such that $[a, b^r] = e = [a^s, b]$. Then,

$$\begin{aligned} f &: \left\{a^i \mid 1 < i < n, \gcd(i,s) = 1\right\} \\ &\to \left\{b^j \mid 1 \leq j < n, r|j\right\}, \\ \phi(s)\frac{n}{s} &< \frac{n}{r}; \\ f^{-1} &: \left\{b^i \mid 1 < i < n, \gcd(i,r) = 1\right\} \\ &\to \left\{a^j \mid 1 \leq j < n, s|j\right\}, \\ \phi(r)\frac{n}{r} &< \frac{n}{s}; \\ \phi(s)\phi(r)\frac{n}{r} &< \phi(s)\frac{n}{s} < \frac{n}{r} \end{aligned}$$

which is a contradiction. □

Example 4. The following example shows that relaxing f from bijection to surjection may not maintain the finiteness of $G(A, B; f)$.

Let $A = \langle a \rangle$ de a cyclic group of order p^3, $B = \langle b \rangle$ be cyclic of order p^2 and define $f : A \to B$ by choosing surjective maps

$$\begin{array}{rcl} f & : & e \to e, \\ A \setminus \langle a^p \rangle & \to & \langle b^p \rangle \setminus \{e\}, \\ \langle a^p \rangle \setminus \{e\} & \to & B \setminus \langle b^p \rangle. \end{array}$$

Then the relations $\left[a, a^f\right] = e$ in $G(A, B; f)$ are equivalent to $\langle a^p, b^p \rangle$ being central in G. Therefore, $G/\langle a^p, b^p \rangle$ is isomorphic to the free product $C_p * C_p$.

Proposition 6. *Let $A = \langle a_1, a_2 \rangle$, $B = \langle b_1, b_2 \rangle$ be homogenous abelian groups of rank 2, both having finite exponent n. Then $G = G(A, B; f)$ is nilpotent of class at most 2 and its derived subgroup is cyclic of order divisor of n.*

Proof. Let us call an element of A which is part of some 2-generating set of A *primitive*. The non-primitive elements are of the form is $a_1^i a_2^j$ where $\gcd(i, n) \neq 1 \neq \gcd(j, n)$; therefore, their number is $(n - \varphi(n))^2$. The number of primitive elements is $n^2 - (n - \varphi(n))^2 = 2n\varphi(n) - \varphi(n)^2$.

The difference between the number of primitive elements and the non-primitives is positive:

$$2n\varphi(n) - \varphi(n)^2 - (n - \varphi(n))^2 = 4n\varphi(n) - 2\varphi(n)^2 - n^2$$

and

$$2\frac{\varphi(n)}{n} + 2\frac{\varphi(n)}{n} \geq 1 + 2\left(\frac{\varphi(n)}{n}\right)^2,$$

since

$$\frac{1}{2} \leq \frac{\varphi(n)}{n} < 1.$$

Since f is a bijection we may suppose $f : a_1 \to b_1$. Now, any 2-generating set of A containing a_1 has the form $\left\{a_1, a_1^l a_2^m\right\}$ where $\gcd(m, n) = 1$; there are $n\varphi(n)$ such elements $a_1^l a_2^m$. As $n\varphi(n) > (n - \varphi(n))^2$, we may suppose $f : a_2 \to b_2$.

As $f : a_1^i a_2^j \to b_1^k b_2^l$, we have

$$\left[a_1^i a_2^j, b_1^k b_2^l\right] = \left[a_1^i, b_2^l\right]\left[a_2^j, b_1^k\right] = e.$$

Since a_1, b_2 commute with $\left[a_2^j, b_1^k\right]$, while a_2, b_1 commute with $\left[a_1^i, b_2^l\right]$, we conclude that $\left[b_1^k, a_2^j\right] = \left[a_1^i, b_2^l\right]$ is central. We note that the size of

$$\left\{a_1^i a_2^j \mid \gcd(i, n) = 1,\, j \neq 0\right\}$$

is $\varphi(n)(n-1)$, whereas the size of

$$\left\{b_1^k b_2^l \mid k \neq 0, \gcd(l, n) \neq 1, l \neq 0\right\}$$

is $(n-1)(n-\varphi(n)-1)$.

As the first set is larger than the second, there exist i, j with $\gcd(i, n) = 1, j \neq 0$ such that $f : a_1^i a_2^j \to b_1^k b_2^l$ where $\gcd(l, n) = 1$. We rewrite a_1^i as a_1 and b_2^l as b_2 and conclude that $[a_1, b_2]$ is central. Similarly, $[a_2, b_1]$ is also central.

Hence,

$$\left[a_1, b_2\right]^n = \left[a_2, b_1\right]^n = e$$

and there exist $0 \leq s, t \leq n-1$ such that

$$\left[a_1, b_2\right] = \left[a_2, b_1\right]^s, \left[a_2, b_1\right] = \left[a_1, b_2\right]^t$$

and $G' = \langle\left[a_1, b_2\right]\rangle = \langle\left[a_2, b_1\right]\rangle$. □

7.1 The groups $G\left(A_{p,k}; f\right)$ for $p = 2, 3$ and $k = 3, 4$

We consider the groups

$$G\left(A_{2,3}; f\right), G\left(A_{2,4}; f\right), G\left(A_{3,3}; f\right),$$

their orders, nilpotency classes c and derived lengths d. We write the group $A_{p,k}$ additively.

(i) The group $A_{2,3}$ is

$$\left\{0, a_1, a_2, a_3, a_1 + a_2, a_1 + a_3, a_2 + a_3, a_1 + a_2 + a_3\right\},$$

which we enumerate lexicographically and identify its elements with their positions in this order. The group $SL(3, 2)$ in its linear action on $A_{2,3}^{\#}$, is generated by the permutations $(2, 7, 4, 6, 5, 8, 3), (2, 8, 7)(3, 4, 6)$. Using GAP, we find that there are 4 double cosets in $SL(3, 2)\backslash Sym(7)/SL(3, 2)$, which are represented by the permutations

$$\left\{\,(),\, (6, 7),\, (6, 7, 8),\, (5, 6, 7, 8)\,\right\}.$$

Each permutation produces for us a bijection f and a group as in the table below

f	$\left\|G\left(A_{2,3}; f\right)\right\|$	c	d
()	2^{10}	3	2
(6, 7)	2^{10}	3	2
(6, 7, 8)	2^8	2	2
(5, 6, 7, 8)	2^8	2	2

Further analysis shows that these 4 groups are non-isomorphic.

(ii) The group $A_{2,4}$ is treated in a similar manner. We find that there are 3374 double cosets in $SL(4, 2)\backslash Sym\ (15)\ /SL(4, 2)$. The corresponding groups $G\left(A_{2,4}; f\right)$ have orders

$$2^9, 2^{10}, 2^{11}, 2^{12}, 2^{13}, 2^{15}, 2^{19}.$$

There are 5 representatives f for which the groups have maximum order. We list them below with their invariants c, d:

f	$\left\|G\left(A_{2,4}; f\right)\right\|$	c	d
()	2^{19}	4	2
(15, 16)	2^{19}	3	3
(11, 14)(15, 16)	2^{19}	5	3
(9, 11)(10, 13)(12, 14)	2^{19}	5	3
(9, 12)(10, 13)(11, 14)	2^{19}	4	2

Further analysis shows that these 5 groups are non-isomorphic.

(iii) The set of 1-dimensional subspaces of $A_{3,3}$ has size 13. The group $GL(3, 3)$ in its linear action on $A_{3,3}$ induces the group $PGL(3, 3)$. There are 252 double cosets in $PGL(3, 3)\backslash Sym(13)/PGL(3, 3)$. A double coset representative corresponds to a bijection g of $A_{3,3}^{\#}$ which is linear on the 1-dimensional subspaces of $A_{3,3}$. We find that the corresponding groups have orders $3^6, 3^7, 3^8, 3^9$. The groups of order 3^6 are clearly isomorphic to $A_{3,3} \times A_{3,3}$. Those of higher order have nilpotency class 2. There is a unique group of maximum order 3^9 which clearly is isomorphic to $\chi\left(A_{3,3}\right)$.

8 Three general examples

Working by hand with $G = G(H, K; f)$, it is easy to produce many consequences from the defining relations: given $h \in H, k \in K$, then the equalities

$$[h, k] = [h, h^f k] = [k^{f^{-1}} h, k]$$

hold and these serve to define the two maps

$$\alpha : (h, k) \to \left(h, h^f k\right), \beta : (h, k) \to \left(k^{f^{-1}} h, k\right)$$

on the set $H \times K$. Finding equivalent forms for $[h, k]$ according to the above process corresponds to calculating the orbits of the group $\langle \alpha, \beta \rangle$ in its action on $H \times K$. We will illustrate this sort of analysis in the examples below.

8.1 The multiplicative inverse function

Let F, $\dot{F}$ be isomorphic fields, via $a \to \dot{a}$. Define $f : 0 \to 0, k \to \dot{k}^{-1}$ for $k \neq 0$ and let

$$G = G(F, inv) = \left\langle F, \dot{F} \mid \left[a, \frac{1}{\dot{a}}\right] = e \text{ for } a \neq 0 \right\rangle.$$

Given an integer m , we have $\left[a, \frac{m}{\dot{a}}\right] = e$. Therefore, if $F = GF(p)$ or $\mathbb{Q}$, the group G is isomorphic to $F \times F$.

We will prove

Theorem 9. *Let $F = GF\left(2^k\right)$ where $2^k - 1$ is a prime number. Then, $G(F; inv)$ is nilpotent of class at most 2.*

It appears that this result holds more generally. We develop below formulas for general fields F.

Lemma 3. *Let $i \geq 1, b \in F, b \neq 0$ and suppose $(2i-1)!$ is invertible in F. Then*

$$(\alpha\beta)^i \quad : \quad (0, b) \to \left(\frac{(2i-1)!}{\left(2^{i-1}(i-1)!\right)^2} \frac{1}{b}, \frac{2^{2i-2}\left((i-1)!\right)^2}{(2i-2)!} b \right),$$

$$(\alpha\beta)^i \alpha \quad : \quad (0, b) \to \left(\frac{(2i-1)!}{\left(2^{i-1}(i-1)!\right)^2} \frac{1}{b}, \frac{2i\left(2^{i-1}(i-1)!\right)^2}{(2i-1)!} b \right).$$

Let p be an odd prime number. Then,

$$(\alpha\beta)^{\frac{p+1}{2}} : (0, b) \to \left(0, (-1)^{\frac{p-1}{2}} b\right)$$

modulo p.

Proof. The first formulae can be verified in a straightforward manner.

In case the characteristic of F is a prime number p then

$$(\alpha\beta)^{\frac{p+1}{2}} : (0, b) \to \left(0, \frac{2^{p-2}\left(\frac{p-1}{2}\right)!\left(\frac{p-3}{2}\right)!}{(p-2)!} b\right)$$

and by Wilson's theorem,

$$\begin{aligned}(p-1)! &= \left(-1^2\right)\left(-2^2\right)\ldots\left(-\left(\frac{p-1}{2}\right)^2\right)\\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}!\right)^2 \equiv -1 \text{ modulo } p,\\ \left(\frac{p-1}{2}!\right)^2 &\equiv (-1)^{\frac{p+1}{2}} \text{ modulo } p.\end{aligned}$$

□

Lemma 4. *Let $L = GF(p)$ when $charac(F) = p$ and $L = \mathbb{Z}$ when $charac(F) = 0$. Let*

$$T = \left\{(a, b) \mid a \neq 0 \neq b, ab \notin L\right\}.$$

Then, $\alpha, \beta : T \to T$ and for all integers $i_1, \ldots, i_s, j_1, \ldots, j_s$,

$$\alpha^{i_1}\beta^{j_1}\ldots\alpha^{i_s}\beta^{j_s} : (a, b) \to \left(a', b'\right),$$

where

$$\begin{aligned}a' &= \frac{\Pi_{1\leq s\leq k}\left(i_1+\cdots+i_s+j_1+\cdots+j_s+ab\right)}{\Pi_{1\leq s\leq k}\left(i_1+\cdots+i_s+j_1+\cdots+j_{s-1}+ab\right)}a,\\ b' &= \frac{\Pi_{1\leq s\leq k}\left(i_1+\cdots+i_s+j_1+\cdots+j_{s-1}+ab\right)}{ab\Pi_{1\leq s\leq k-1}\left(i_1+\cdots+i_s+j_1+\cdots+j_s+ab\right)}b.\end{aligned}$$

The relations $\left[\alpha^i, \beta^j\right] = \left[\alpha^j, \beta^i\right]$ hold on the set T, for all integers i, j.

Proof. We calculate only the action of $\alpha^{i_1}\beta^{j_1}$:

$$\begin{aligned}(a,b) &\to^{\alpha^{i_1}} \left(a, \frac{i_1}{a}+b\right) = \left(a, \frac{i_1+ab}{ab}b\right)\\ &\to^{\beta^{j_1}} \left(a+\frac{j_1}{i_1+ab}a, \frac{i_1+ab}{ab}b\right)\\ &= \left(\frac{i_1+j_1+ab}{i_1+ab}a, \frac{i_1+ab}{ab}b\right).\end{aligned}$$

It is direct to check that the first general non-trivial relation happens for $k=3$:

$$j_1 = -i_1 - i_2, j_2 = i_1, i_3 = -i_1 - i_2, j_3 = i_2;$$

that is,

$$\alpha^{i_1}\beta^{-i_1-i_2}\alpha^{i_2}\beta^{i_1}\alpha^{-i_1-i_2}\beta^{i_2} = e$$

which in turn is equivalent to

$$\left[\alpha^i, \beta^j\right] = \left[\alpha^j, \beta^i\right].$$

□

Lemma 6. *Let charac $(F) = 2$, $a, b \in F$ such that $a \neq 0 \neq b$, $ab \neq 1$. Define $c = c(a,b) = \frac{ab}{1+ab}$. Then, $\alpha^2 = \beta^2 = e$ and for all integers k,*

$$\begin{aligned}(\alpha\beta)^k &: (a,b) \to \left(c^k a, c^{-k} b\right),\\ (\alpha\beta)^k\beta &: (a,b) \to \left(c^{k-1} a, c^{-k} b\right).\end{aligned}$$

The orbit of (a,b) under the action of $\langle\alpha,\beta\rangle$ has length $2.o(c)$. As both $ac^i \in F$ and $\dot{b}\dot{c}^{-i} \in \dot{F}$ invert $w = \left[a, \dot{b}\right]$ for all $i \geq 0$, we conclude that the subgroup $\left\langle \left(1+c^i\right)a, \left(1+\dot{c}^i\right)\dot{b} \mid i \neq 0\right\rangle$ centralizes w. If c satisfies a monic polynomial over $GF(2)$, which is the sum of an odd number of monomials, then a and $\dot{b}$ centralize w and so $\left(a\dot{b}\right)^4 = e$.

Proof of Theorem 10. Let $a \neq 0 \neq b$, $ab \neq 1$. Since $c = \frac{ab}{1+ab}$ is a generator of the multiplicative group $F^{\#}$ we have $\left\{\left(1+c^i\right)a \mid i \geq 0\right\} = F^{\#}$ and so, $w = \left(a\dot{b}\right)^2 = \left[a, \dot{b}\right]$ is central in G. Therefore, G is nilpotent of class at most 2.

Example 5. We obtain by using GAP:

for $F = GF\left(2^3\right)$, the group G has order 2^8 and nilpotency class 2;
for $F = GF\left(2^4\right)$ the group G has order 2^{11} and nilpotency class 2;
for $F = GF\left(3^3\right)$ the group G is abelian, isomorphic to $F \times F$.

8.2 Group extension of $\chi(A)$

Let $\widetilde{A}, \widetilde{B}$ be groups isomorphic to $A_{2,k}$, $k \geq 3$, generated by $\{a_i \mid 1 \leq i \leq k\}$, $\{b_i \mid 1 \leq i \leq k\}$, respectively. Define

$$A = \langle a_i \mid 2 \leq i \leq k \rangle, \quad B = \langle b_i \mid 2 \leq i \leq k \rangle$$

and let $f\colon A \to B$ be the isomorphism extended from the map $a_i \to b_i \left(2 \leq i \leq k\right)$. Then, $G(A, B; f)$ is isomorphic to $\chi\left(A_{2,k-1}\right)$. Both $\widetilde{A}, \widetilde{B}$ are central extensions of A, B, respectively. Define $f^* : \widetilde{A} \to \widetilde{B}$ by

$$a_1 \to b_1, h \to b_1 h^f, a_1 h \to h^f \quad \text{for} \quad h \in A^{\#};$$

this corresponds to choosing the bijections $\alpha : e \to e, a_1 \to b_1$, $\gamma : e \to b_1, a_1 \to e$.

We sketch below a proof that the group $G = G\left(\widetilde{A}, \widetilde{B}; f^*\right)$ is metabelian, has order 2^{2^k+k-1} and has nilpotency class k. Yet, G is not isomorphic to $\chi\left(A_{2,k}\right)$: for whereas the commutator subgroup of $\chi\left(A_{2,k}\right)$ is of exponent 2, G' is of exponent 4. Indeed, G' is generated by $\left[a_j^f, a_1\right]$ for $j > 1$ (their number is $k-1$, each of order 2) and by

$$\left[a_{j_1}^f, a_{j_2}, a_{j_3}, \ldots, a_{j_r}\right] \quad \text{where} \quad j_1 > j_2 > \ldots > j_r > 1$$

(their number is $2^{k-1} - k$, each of order 4).

We develop the proof in steps.

Let $t : \widetilde{A} \to \widetilde{B}$ be the natural isomorphism extended from $a_i \to b_i$.

(1) The set $\left\{\left(x, y^t\right) \mid x, y \in \widetilde{H}\right\}$ partitions under the substitutions α, β into three types of orbits. Let $u \neq w \in A$. Then orbits types are as follows:

(i) $\left\{\left(a_1, u^t\right), \left(u, u^t\right), \left(u, b_1\right), \left(a_1 u, b_1\right), \left(a_1 u, b_1 u^t\right), \left(a_1, b_1 u^t\right)\right\}$;

(ii) $\left\{\left(u, w^t\right), \left(a_1 uw, w^t\right), \left(a_1 uw, u^t\right), \left(w, u^t\right), \left(w, b_1 u^t w^t\right), \left(u, b_1 u^t w^t\right)\right\}$;

(iii) $\{(a_1u, b_1w^t),\ (a_1uw, b_1w^t),\ (a_1uw, b_1u^t),\ (a_1w, b_1u^t),\ (a_1w, b_1u^tw^t),\ (a_1u, b_1u^tw^t)\}$.

(2) The following equalities hold for all $x, y, z \in \widetilde{A}$:

$$[x, y^t] = [y, x^t], \quad [x^t, y, z^t] = [z, y^t, x]^{-1}, \quad [z, y^t, x] = [y, x^t, z].$$

Proof of (2). In each orbit we find (x, y^t), (y, x^t).

We conclude that for all $x, y, z \in \widetilde{A}$,

$$\begin{aligned}
&[x, (yz)^t] = [x, (zy)^t] = [y, x^t][z, x^t][x, z^t, y^t],\\
&[x, (yz)^t] = [yz, x^t] = [y, x^t][y, x^t, z][z, x^t],\\
&[z, x^t][x, z^t, y^t] = [y, x^t, z][z, x^t],\\
&[x, z^t, y^t]^{[x^t, z]} = [y, x^t, z],\\
&[x, z^t, y^t]^{[z^t, x]} = [y, x^t, z],\\
&[y^t, [z^t, x]] = [y, x^t, z],\\
&[z^t, x, y^t] = [y, x^t, z]^{-1}
\end{aligned}$$

and

$$[z^t, x, y^t] = [y, x^t, z]^{-1} = [x, y^t, z]^{-1} = [x^t, y, z^t] = [z, y^t, x]^{-1}.$$

(3) We will show that a_1 inverts $[u, w^t]$ for all $u, w \in \widetilde{A}$.

Proof of (3). Clearly a_1 inverts $[a_1, w^t]$.

In the calculations below, given a word $**x**$ we introduce dots around x as $**.x.**$ indicating that x will be substituted by $x^{f^*}xx^{f^*}$, if $x \in \widetilde{A}$, or by $x^{(f^*)^{-1}}xx^{(f^*)^{-1}}$, if $x \in \widetilde{B}$.

Let $u, w \in A$. Then,

$$\begin{aligned}
[u, w^t]^{a_1} &= (a_1u).w^t.uw^ta_1 = (uw)\,w^t.\,(a_1uw).w^ta_1\\
&= (uw)\,u^t\,(a_1uw).u^t.a_1 = (uw)\,u^twu^tu = (wu^twu^t)^u\\
&= [w, u^t]^u = [u, w^t]^u = [u, w^t]^{-1}.
\end{aligned}$$

Furthermore,

$$\begin{aligned}\left[a_1u, b_1w^t\right]^{a_1} &= u.b_1w^t.a_1ub_1w^ta_1 = uw\left(b_1w^t\right).a_1uw.b_1w^ta_1\\ &= uw\left(b_1u^t\right)(a_1uw).b_1u^t.a_1 = uw\left(b_1u^t\right).a_1w.\left(b_1u^t\right)a_1u\\ &= uw.b_1u^tw^t.(a_1w)\left(b_1u^tw^t\right)a_1u\\ &= \left(b_1u^tw^t\right).a_1u.\left(b_1u^tw^t\right)a_1u\\ &= \left(b_1w^t\right).a_1u.\left(b_1w^t\right)a_1u. = \left[b_1w^t, a_1u\right].\end{aligned}$$

(4) We claim

$$\left[\left[z^t, x\right], \left[z^t, x\right]^y\right] = e, \left[z^t, x\right]^y = \left[z^t, x\right]^{y^t}$$

and the group G is metabelian.

Proof of (4). Apply a_1 to

$$\left[x, (yz)^t\right] = \left[x, (zy)^t\right] = \left[x, y^t\right]\left[x, z^t\right]\left[x, z^t, y^t\right].$$

Then

$$\begin{aligned}\left[(yz)^t, x\right] &= \left[y^t, x\right]\left[z^t, x\right]\left[x, z^t, y^t\right]^{a_1}\\ &= \left[y^tz^t, x\right] = \left[y^t, x\right]^{z^t}\left[z^t, x\right]\\ &= \left[y^t, x\right]\left[y^t, x, z^t\right]\left[z^t, x\right],\end{aligned}$$

$$\begin{aligned}\left[x, z^t, y^t\right]^{a_1} &= \left[y^t, x, z^t\right]^{\left[z^t, x\right]}\\ &= \left[z, x^t, y\right]^{-\left[z^t, x\right]}\\ &= \left[z^t, x, y\right],\\ \left[x, z^t, y^t\right] &= \left[z^t, x, y\right]^{a_1}\\ &= \left[x, z^t, y\right]\end{aligned}$$

$$\begin{aligned}\left[x, z^t, y^t\right] &= \left[x, z^t, y\right],\\ \left[x, z^t, y\right] &= \left[x^t, z, y^t\right]^{-1}\\ &= \left[z^t, x, y^t\right]^{-1},\\ \left[\left[x, z^t\right]^{-1}, y^t\right] &= \left[\left[x, z^t\right], y^t\right]^{-1}.\end{aligned}$$

Thus,

$$\left[x, z^t\right]^{y^t} = \left[x, z^t\right]^y$$

and

$$\left[x, z^t\right] \text{ commutes with } \left[x, z^t\right]^{y^t}.$$

Observe that

$$\left[x, y^t\right]^{uv^t} = \left[x, y^t\right]^{u^t v^t} = \left[x, y^t\right]^{(uv)^t} = \left[x, y^t\right]^{uv}$$

and so, $\left[x, y^t\right]^{\left[u, v^t\right]} = \left[x, y^t\right]$. It follows that G is metabelian.

(4.1) The commutator subgroup is generated by

$$\left[a_j^t, a_i\right]^w \quad \text{where } j > i, w \in \langle a_r \mid r \neq 1, i, j\rangle .$$

We can improve upon the description of this generating set by using:

$$\begin{aligned}
\left[a_j^t, a_i, a_k\right]^{a_i}\left[a_k, a_j^t, a_i\right]^{a_j^t} &= e,\\
\left[a_i, a_j^t, a_k\right]\left[a_j, a_k^t, a_i\right]^{a_j} &= e,\\
\left[a_i, a_j^t, a_k\right]\left[a_k^t, a_j, a_i\right] &= e,
\end{aligned}$$

$$\begin{aligned}
\left[a_j^t, a_i, a_k\right] &= \left[a_k^t, a_j, a_i\right] = \left[a_j^t, a_k, a_i\right]\\
&= \left[a_i^t, a_k, a_j\right] = \left[a_k^t, a_i, a_j\right] = \left[a_i^t, a_j, a_k\right].
\end{aligned}$$

Therefore the generators have the form

$$\left[a_{j_1}^t, a_{j_2}, a_{j_3}, \ldots, a_{j_r}\right] \text{ where } j_1 \geq j_2 \geq \ldots \geq j_r.$$

If $j_1 = j_2$ then

$$\left[a_{j_1}^t, a_{j_2}\right] = \left[a_{j_1}^t, a_1\right],$$

$$\left[a_{j_1}^t, a_{j_2}, a_{j_3}\right] = \left[a_{j_1}^t, a_1, a_{j_3}\right] = \left[a_{j_1}^t, a_{j_3}, a_1\right] = \left[a_{j_1}^t, a_{j_3}\right]^2.$$

Thus G' is generated by:

$$\left[a_j^t, a_1\right] \quad (1 < j \leq k)$$

(in total of $k-1$, each of order dividing 2) and by

$$\left[a_{j_1}^t, a_{j_2}, a_{j_3}, \ldots, a_{j_r}\right] \text{ for all } j_1 > j_2 > \ldots > j_r > 1$$

(in total of $2^{k-1} - k$, each of order dividing 4). Hence, $\left|G'\right|$ divides 2^{k-1}. $4^{2^{k-1}-k} = 2^{k-1+2^k-2k} = 2^{2^k-k-1}$ and $|G|$ divides $2^{2^k-k-1}2^{2k} = 2^{2^k-1}2^k$. The nilpotency class of G is at most k and the commutator of highest weight is apparently $\left[a_k^t, a_{k-1}, a_{k-2}, \ldots, a_1\right]$.

Rather than effecting the final construction, we just remark that computations in GAP confirm the structural information obtained above for $k \leq 5$.

8.3 A transposition

Let $A = A_{2,k}$ and let f correspond to a transposition. Since $SL(k, 2)$ is 2-transitive on $A_{2,k}^{\#}$, any transposition of $A_{2,k}^{\#}$ is equivalent to f. Detailed analysis of $G\left(A_{2,k}; f\right)$ indicates that it has the same order as $\chi(A)$, but not isomorphic to the latter. Again, this is confirmed by computations in GAP.

Acknowledgments. The authors thank Alexander Hulpke for assistance with the double cosets package in GAP. The second author acknowledges support from the Brazilian agencies CNPq and FAPDF.

References

[1] M. Aschbacher, R. Guralnick and Y. Segev, *Elementary Abelian 2-subgroups of Sidki-Type in Finite Groups*. Groups Geom. Dyn., **1** (2007), 347–400.

[2] The GAP Group, GAP-Groups, Algorithms and Programming, Version 4.4.9 (2006). (http://www.gap-system.org).

[3] N. Gupta, N. Rocco and S. Sidki, *Diagonal Embeddings of Nilpotent Groups*. Illinois J. of Math., **30** (1986), 274–283.

[4] D. Quillen, *Homotopy properties of the poset of nontrivial p-subgroups*. Adv. Math., **28** (1978), 101–128.

[5] A.S. Rapinchuk, Y. Segev and G.M. Seitz, *Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable*. J. Amer. Math. Soc., **15** (2002), 929–978.

[6] S. Sidki, *Some Commutation Patterns between Involutions of a Finite Group II*. J. of Algebra, **39** (1976), 66–74.

[7] S. Sidki, *On Weak Permutability between Groups*. J. of Algebra, **63** (1980), 186–225.

[8] M. Vaughan-Lee, The Restricted Burnside Problem, Second edition, Oxford Science Publications (1993).

[9] M. Suzuki, Structure of a Group and the Structure of its Lattice of Subgroups, Ergebnisse der Math., Springer Verlag (1956).

Ricardo N. Oliveira
Departamento de Matemática
Universidade Federal de Goiás
Goiânia, GO
BRAZIL

E-mail: ricardo@mat.ufg.br

Said N. Sidki
Departamento de Matemática
Universidade de Brasília
70910-900 Brasília, DF
BRAZIL

E-mail: sidki@mat.unb.br