ON NILPOTENT PRODUCTS OF CYCLIC GROUPS

RUTH REBEKKA STRUIK

Introduction. In this paper $G = F/F_n$ is studied for F a free product of a finite number of cyclic groups, and F_n the normal subgroup generated by commutators of weight n. The case of $n = 4$ is completely treated (F/F_2 is well known; F/F_3 is completely treated in **(2)**); special cases of $n > 4$ are studied; a partial conjecture is offered in regard to the unsolved cases. For $n = 4$ a multiplication table and other properties are given.

The problem arose from Golovin's work on nilpotent products (**(1)**, **(2)**, **(3)**) which are of interest because they are generalizations of the free and direct product of groups: all nilpotent groups are factor groups of nilpotent products in the same sense that all groups are factor groups of free products, and all Abelian groups are factor groups of direct products. In particular (as is well known) every finite Abelian group is a direct product of cyclic groups. Hence it becomes of interest to investigate nilpotent products of finite cyclic groups.

Golovin has done this (as well as other things) in **(2)** and **(3)**. In **(2)** there are results for the first nilpotent product (metabelian product) and in **(3)** there is a unique decomposition theorem for nilpotent products of finite cyclic groups.

It might be conjectured that all finite nilpotent groups are nilpotent products of cyclic groups. However, in **(2)** and **(3)** Golovin notes examples of non-Abelian groups with $((G, G), G) = 1$ which are not of this form. Here it is shown that the Burnside group with exponent 3 (with three or more generators) is not of this form.

To be more precise, and using Golovin's notation: Let

$$F = \prod\nolimits_{i=1}^{t}{}^{*} A_i$$

be the free product of the A_i. Let $(a, b) = a^{-1}b^{-1}ab$ and $(A, B) = \{(a, b)| a \in A, b \in B\}$ where A and B are subgroups of a group. Let $(A_i) = \{(A_i, A_j)| i \neq j\}$ where the A_i are considered as subgroups of F (the i in (A_i) is to indicate that it is formed from the A_i in F). Let ${}_0(A_i)_F$ be the normal subgroup generated by (A_i) in F, ${}_k(A_i)_F = ({}_{k-1}(A_i)_F, F)$. Then according to Golovin **(1)**, the kth nilpotent product of the A_i is

$$G = A_1(k)A_2(k)\ldots(k)A_t = F/{}_k(A_i)_F.$$

(If the A_i are cyclic, then $G = F/F_{k+2}$.)

From now on, Golovin's notation will be dropped.

Received October 17, 1958; in revised form January 21, 1960.

In **(6)** it is shown that if F is a free group with a finite number of generators, then every element of F/F_n can be uniquely expressed as a product of standard commutators. Here it is shown that if F is replaced by a free product of cyclic groups, then Hall's results hold "essentially" provided that all primes appearing in the orders of the factors are $\geqslant n-1$. If the primes are $< n-1$, then the situation is complicated. The case $n = 4$ is completely treated here (that is, $p = 2, n = 4$); partial results and conjectures are offered for $n > 4$ and $p < n - 1$.

Section 1 gives preliminary results. In § 2, the "well-behaved" case ($p \geqslant n-1$) is handled, and in § 3, the other cases are discussed.

The author would like to thank W. Magnus for encouragement while preparing this paper, and R. Ree for reading the manuscript and for helpful criticisms. The author is also indebted to the referee for many improvements.

1. Preliminaries. Let G be an arbitrary group. As usual, $(a, b) = a^{-1}b^{-1}ab$ for $a, b \in G$ and if A, B are subgroups of G, then $(A, B) = \{(a, b)|a \in A, b \in B\}$. The lower central series of G is an infinite sequence of subgroups, $G_1, G_2, \ldots,$ where $G_1 = G$, $G_2 = (G, G), \ldots, G_{n+1} = (G_n, G)$. $(((a_1, a_2), a_3), \ldots, a_n)$ will often be abbreviated $(a_1, \ldots, a_n)$. An element of the form $(((a_1, a_2), (a_3, a_4)), \ldots, a_n)$ (that is, with arbitrary arrangement of parentheses) will often be referred to as a commutator (of weight n), as opposed to a member of G_n which is (in general) a product of commutators (of weight n or greater). In this paper, F will stand for a free product of a finite number of cyclic groups: $F = \prod^* A_i$, A_i cyclic. (A_i may be finite or infinite). The following identities are often useful:

$$(1) \qquad \begin{aligned} (xy, z) &= (x, z)((x, z), y)(y, z) \\ (x, yz) &= (x, z)(z, (y, x))(x, y) \end{aligned}$$

In **(6)**, the following theorem is proved:

THEOREM H1. *Let F be a free group with t generators, $u_1, u_2, \ldots, u_t$. Let $u_1, \ldots, u_s$ be a sequence of standard commutators of weight $< n$ (See* **(7)**.) *of non-decreasing weight. Then every element, g, of $F/F_n = G$ (free nilpotent group) can be uniquely expressed as*

$$g = \prod{}_{i=1}^{s} u_i^{c_i}$$

where the c_i are rational integers. If

$$h = \prod u_i^{d_i} \in G,$$

then

$$gh = \prod u_i^{e_i},$$

where $e_i = f_i(c_j, d_k)$ are polynomials with integer coefficients in the c_j and the d_k (for example, $e_i = c_i + d_i$; $1 \leqslant i \leqslant t$). If s-tuples of the form $(c_1, \ldots, c_s)$,

https://doi.org/10.4153/CJM-1960-039-x Published online by Cambridge University Press

c_i rational integers are taken with multiplication given by $(c_1, \ldots, c_s) \times (d_1, \ldots, d_s) = (f_1(c_j, d_k), \ldots, f_s(c_j, d_k))$, the set of these s-tuples forms a nilpotent group isomorphic to F/F_n.

Throughout this paper, Hall's collection process will be frequently used. Several of its important theorems will now be summarized:

THEOREM H2: *Let R, S be any two elements of a group; let $u_1, u_2, \ldots,$ be a fixed sequence of commutators in R and S of non-decreasing weight, that is, $u_1 = (R, S)$, $u_2 = ((R, S), R)$, $u_3 = ((R, S), S)$, etc. Then*

$$(RS)^n = R^n S^n u_1^{f_1(n)} u_2^{f_2(n)} \ldots u_i^{f_i(n)} \ldots \tag{2}$$

where

$$f_i(n) = a_1\binom{n}{1} + a_2\binom{n}{2} + \ldots + a_{w_i}\binom{n}{w_i} \tag{3}$$

a_i are rational integers and w_i is the weight of u_i as a commutator in R and S. (2) is an identity if the group is nilpotent; otherwise (2) can be considered as giving a series of "approximations" to $(RS)^n$ modulo successive members of the lower central series.

The proof of Theorem H1 also gives

THEOREM H3. *Let $R_1, R_2, \ldots, R_s$ be any s elements of a group. Let $u_1, u_2, \ldots,$ be a fixed sequence of commutators in the R_i of non-decreasing weight (weight $\geqslant 2$). Let $i_1, i_2, \ldots, i_s$ be any fixed permutation of $1, 2, \ldots, s$. Then*

$$(R_1R_2 \ldots R_s)^n = R_{i_1}^n R_{i_2}^n \ldots R_{i_s}^n u_1^{f_1(n)} u_2^{f_2(n)} \ldots u_i^{f_i(n)} \ldots \tag{4}$$

where $f_i(n)$ are of form (3) with w_i the weight of u_i in the R_j.

From Theorem H1 we can obtain

LEMMA H1. *Let X, Y be any elements of a group, and let $u_1, u_2, \ldots,$ be any fixed sequence of commutators in X and (X, Y) of non-decreasing weight; then*

$$(X^n, Y) = (X, Y)^n u_1^{f_1(n)} u_2^{f_2(n)} \ldots u_i^{f_i(n)} \ldots \tag{5}$$

where the $f_i(n)$ are like (3) with w_i as the weight of u_i in X and (X, Y).

Proof of Lemma H1. (5) follows from (2) in view of

$$(X^n, Y) = X^{-n}Y^{-1}X^nY = X^{-n}[Y^{-1}XY]^n = X^{-n}[X(X, Y)]^n$$
$$= X^{-n}X^n(X, Y)^n u_1^{f_1(n)} \ldots = (X, Y)^n u_1^{f_1(n)} \ldots .$$

LEMMA H2. *Let α be a fixed integer and G a group such that $G_n = 1$. Then if $b_j \in G$ and $r < n$,*

$$(b_1, \ldots, b_{i-1}, b_i^{\alpha}, b_{i+1}, \ldots, b_r) = (b_1, \ldots, b_r)^{\alpha} v_1^{f_1(\alpha)} v_2^{f_2(\alpha)} \ldots \tag{6}$$

where the v_k are commutators in $b_1, \ldots, b_r$ of weight $> r$, and every b_j, $1 \leqslant j \leqslant r$ appears in each commutator v_k. The f_i are of form (3) where w_i is the weight of v_i minus $(r - 1)$.

Proof. (6) is (5) with $r = 2$, $i = 1$, and $\alpha = n$. For $r = 2$, $i = 2$, and $\alpha = n$, take inverses on each side of (5).

$$(Y, X^{\alpha}) = u_s^{-f_s(\alpha)} \ldots u_1^{-f_1(\alpha)}(Y, X)^{\alpha} \tag{7}$$

where $u_s \in G_{n-1}$. Since $G_n = 1$, s is finite. Now apply (4):

$$(Y, X^{\alpha}) = u_s^{-f_s(\alpha)} \ldots u_1^{-f_1(\alpha)}(Y, X)^{\alpha} \qquad [R_i = (Y, X) \text{ or } u_j^{-f_j(\alpha)}] \tag{8}$$
$$= [(Y, X)^{\alpha} u_1^{-f_1(\alpha)} \ldots u_s^{-f_s(\alpha)}] w_1^{f_1(1)} w_2^{f_2(1)} \ldots$$

where w_i are commutators in $(Y, X)^{\alpha}$ and $u_j^{-f_j(\alpha)}$. Use induction starting with $(Y, X) \in G_{n-1}$. For $(Y, X) \in G_{n-s}$, assume the theorem (that is, (6)) is true for commutators $\in G_{n-s+1}$, and use this and (1) to express w_j in desired form. One will obtain as exponents in the expansions, expressions of the form

$$\binom{\binom{\alpha}{i}}{j}. \tag{9}$$

From its meaning in terms of the number of subsets of a set, (9) is an integral-valued function of α (of degree $i \times j$). By (3.21) p. 64 of **(5)**, this can be expressed in the form

$$a_1\binom{\alpha}{1} + \ldots + a_{i \times j}\binom{\alpha}{i \times j}$$

a_i rational integers. This is sufficient to show

$$(Y, X^{\alpha}) = (Y, X)^{\alpha} \prod v_k^{f_k(\alpha)} \tag{10}$$

which completes the proof for $r = 2$.

Suppose true for r, then for

$$(c_1, c_2, \ldots, c_{i-1}, c_i^{\alpha}, c_{i+1}, \ldots, c_{r+1}) \qquad i > 2 \tag{11}$$

put $b_1 = (c_1, c_2)$, $b_i = c_{i+1}$, $i = 2, \ldots, r$ in (6) and use induction hypothesis. For

$$(c_1^{\alpha}, c_2, \ldots, c_{r+1}) \tag{12}$$

put

$$X = (c_1^{\alpha}, c_2, \ldots, c_r),\ Y = c_{r+1}.$$

By induction

$$X = (c_1, \ldots, c_r)^{\alpha} \prod w_k^{f_k(\alpha)}.$$

Now use (1) an appropriate number of times with

$$x, y, z = (c_1, \ldots, c_r)^{\alpha},\ w_k^{\binom{\alpha}{i}} \qquad \text{or} \qquad c_{r+1}$$

and the induction hypothesis to put

$$(X, Y) = ((c_1, \ldots, c_r)^{\alpha} \prod w_k^{f_k(\alpha)}, c_{r+1}) \tag{13}$$

in the form of (6).

A similar proof holds for

$$(c_1, c_2^{\alpha}, c_3, \ldots, c_{r+1}).$$

Throughout this proof, we have implicitly used the fact that an arbitrary commutator can be expressed as a product of commutators of the form $(b_1, \ldots, b_r)$. Or to express the same idea in a different way, (6) can be proved in the same way, if $(b_1, \ldots, b_{i-1}, b_i^{\alpha}, b_{i+1}, \ldots, b_r)$ and $(b_1, \ldots, b_r)$ are replaced by arbitrary commutators (that is, monomial commutators with parentheses arranged arbitrarily).

Let gcd stand for greatest common divisor and $\gcd(\alpha_1, \ldots, \alpha_k)$ stand for the gcd of the rational integers $\alpha_1, \ldots, \alpha_k$. The $\gcd(\alpha_1, \ldots, \alpha_k, 0) = \gcd(\alpha_1, \ldots, \alpha_k)$. This should not be confused with $(a_1, \ldots, a_k)$, a member of G_k, G a group, since $a_i \in$ a group, and will not be rational integers (in this paper). A cyclic group of order 0 will be understood to be infinite cyclic.

LEMMA 1. *Let*

$$F = \prod\nolimits_{i=1}^{t*} A_i,$$

A_i cyclic of order α_i. Let a_i generate A_i. Let $n \geqslant 3$ be a fixed positive integer, and let all primes appearing in the factorizations of the $\alpha_i \geqslant n - 1$. Let $G = F/F_n$. If $v \in G$, and

$$v = (a_{i_1}, \ldots, a_{i_k}),$$

then $v^N = 1$, where

$$N = \gcd(\alpha_{i_1}, \ldots, \alpha_{i_k}), \quad k \geqslant 2$$

(some of the α_{i_j} (or a_{i_j}) may equal each other). If w is a product of commutators like v in which every commutator contains all the distinct a_i appearing in v, then $w^N = 1$. Hence $w^N = 1$ where w is an arbitrary commutator.

Proof. Let

$$v = (a_{i_1}, \ldots, a_{i_{n-1}}) \in G_{n-1}.$$

By (6)

$$(14) \quad 1 = (a_{i_1}, \ldots, a_{i_j}^{\alpha_{i_j}}, \ldots, a_{i_{n-1}}) = (a_{i_1}, \ldots, a_{i_{n-1}})^{\alpha_{i_j}} \prod v_m^{\alpha_{i_j}}$$

$$1 \leqslant j \leqslant n - 1$$

where all $v_m = 1$ since $G_n = 1$. Hence the Lemma holds for $k = n - 1$. Since G_{n-1} is Abelian, $w^N = 1$ if w is a product of commutators of weight $n - 1$ in which the same a_i appear in each commutator.

Suppose true for $k + 1$, that is, if

$$v = (a_{i_1}, \ldots, a_{i_{k+1}}),$$

then $v^N = 1$ where

$$N = \gcd(\alpha_{i_1}, \ldots, \alpha_{i_{k+1}}),$$

https://doi.org/10.4153/CJM-1960-039-x Published online by Cambridge University Press

and if w is a product of commutators of weight $k+1$ or greater in

$$a_{i1}, \ldots, a_{ik+1},$$

then $w^N = 1$. Consider $(a_{i1}, \ldots, a_{ik})$. By (6)

$$(15) \quad 1 = (a_{i1}, \ldots, a_i^{\alpha_{ij}}, \ldots, a_{ik}) = (a_{i1}, \ldots, a_{ik})^{\alpha_{ij}} \prod v_m^{f_m(\alpha_{ij})} \quad 1 \leqslant j \leqslant k.$$

$$\prod v_m^{f_k(\alpha_{ij})} = 1$$

by the induction hypothesis, and the assumption on the primes; hence

$$(a_{i1}, \ldots, a_{ik})^{\alpha_{ij}} = 1.$$

Hence

$$(a_{i1}, \ldots, a_{ik})^N = 1 \text{ where } N = \gcd(\alpha_{i1}, \ldots, \alpha_{ik}).$$

Making use of (4), one obtains that if w is the product of commutators of weight k or greater in $a_{i1}, \ldots, a_{ik}$, then $w^N = 1$. Note that every factor of w must contain all the distinct a_{ij}, and that in a nilpotent group, every commutator can be expressed a product of commutators of the form $(a_{i1}, \ldots, a_{ik})$.

For the case $n = 4$, (5) becomes:

Lemma 2. *If G is any group and $a, b \in G$, then*

$$(16) \quad (a^r, b^s) = (a, b)^{rs}((a, b), a)^{s\binom{r}{2}}((a, b), b)^{r\binom{s}{2}} \quad \text{mod } G_4,$$

$$(b^r, a^s) = (a, b)^{-rs}((a, b), a)^{-r\binom{s}{2}}((a, b), b)^{-s\binom{r}{2}} \quad \text{mod } G_4,$$

$$\text{where} \quad \binom{r}{2} = \frac{r(r-1)}{2}.$$

Lemma 2 is proved in **(14)** and is a particular case of (5) in which the $f_i(n)$ have been computed. The proof of (16) is based on the work of Magnus **(11)**.

2. The "well-behaved" case.

Theorem 1. *Let A_1, A_2, A_3 be cyclic groups of orders $\alpha_1, \alpha_2, \alpha_3$ respectively, α_i odd integers. Let a_i generate A_i. Let*

$$F = \prod_{i=1}^{t} {}^* A_i.$$

Let $u_1, \ldots, u_{14}$ be a sequence of standard monomial commutators of non-decreasing weight in a_1, a_2, a_3 of weight $\leqslant 3$. (See **(7)**.*) Let $N_i = \alpha_i$ if u_i is of weight 1; let $N_i = \gcd(\alpha_i, \alpha_j)$ if $u_i = (a_i, a_j)$, and let $N_i = \gcd(\alpha_i, \alpha_j, \alpha_k)$ if a_i, a_j, a_k appear in u_i of weight 3. Then every element of g of F/F_4 can be uniquely expressed as*

$$(17) \quad g = \prod u_i^{c_i}$$

where the c_i are integers modulo N_i. If

$$h = \prod u_i^{d_i}$$

https://doi.org/10.4153/CJM-1960-039-x Published online by Cambridge University Press

is another element of F/F_4, *then*

$$gh = \prod u_i^{e_i}$$

where $e_i = f_i(c_j, d_k)$ *are the polynomials with integral coefficients of Theorem* H1.

(Theorem 1 is a generalization of a lemma appearing in **(15)**.)

Proof. By Lemma 1, $u_i^{N_i} = 1$. Hence every element of G can be expressed in the form of (17) where the c_i are integers modulo N_i. The problem is to show that this expression is unique.

Let $u_1, \ldots, u_{14}$ be $a_1, a_2, a_3, (a_1, a_2), (a_1, a_3), (a_2, a_3), (a_1, a_2, a_1), (a_1, a_3, a_1), (a_2, a_3, a_2), (a_1, a_2, a_2), (a_1, a_3, a_3), (a_2, a_3, a_3), (a_1, a_2, a_3), (a_2, a_3, a_1)$, respectively. If another sequence of standard commutators is chosen, a similar proof will hold. Since (a_i, a_j), $i \neq j$ generate (G, G) modulo G_3 and since

$$((a, b), c)((b, c), a)((c, a), b) = 1 \text{ modulo } G_4 \quad \text{(see } \mathbf{(11)}\text{)}$$

and (a_i, a_j, a_k) generate G_3 modulo G_4, the u_i specified above do form a basis for G. The following change of notation will be made:

let $u_{ij} = (a_i, a_j)$ and designate the corresponding c_i, d_i, e_i by c_{ij}, d_{ij}, e_{ij} respectively;

Let $u_{iji} = (a_i, a_j, a_i)$ and designate the corresponding c_i, d_i, e_i by c_{iji}, d_{iji}, e_{iji} where $i < j$;

let $u_{ijj} = (a_i, a_j, a_j)$ and designate the corresponding c_i, d_i, e_i by c_{ijj}, d_{ijj}, e_{ijj} where $i < j$;

let $u_{ijk} = (a_i, a_j, a_k)$ and designate the corresponding c_i, d_i, e_i by c_{ijk}, d_{ijk}, e_{ijk} where $i < j < k$;

let $u_{jki} = (a_j, a_k, a_i)$ and designate the corresponding c_i, d_i, e_i by c_{jki}, d_{jki}, e_{jki} where $i < j < k$.

For Theorem 1, u_{jki} and u_{ijk} are u_{231} and u_{123} respectively, but the more general notation is used here for the sake of Theorem 2.

Then a somewhat laborious computation gives

$$\begin{aligned}
&e_i = c_i + d_i \\
&e_{ij} = c_{ij} + d_{ij} - c_j d_i \\
&e_{iji} = c_{iji} + d_{iji} - c_j\binom{d_i}{2} + c_{ij} d_i \\
(18)\qquad &e_{ijj} = c_{ijj} + d_{ijj} - d_i\binom{c_j}{2} + c_{ij} d_j - d_i d_j c_j \\
&e_{ijk} = c_{ijk} + d_{ijk} + c_{ik} d_j + c_{ij} d_k - d_i c_j c_k - c_k d_i d_j - c_j d_i d_k \\
&e_{jki} = c_{jki} + d_{jki} + c_{jk} d_i + c_{ik} d_j - c_k d_i d_j.
\end{aligned}$$

https://doi.org/10.4153/CJM-1960-039-x Published online by Cambridge University Press

Note that these are the $f_i(c_j, d_k)$ of Theorem H1 for $n = 4$, and the particular sequence of u_i chosen here. Also note that they apply unambiguously if they are interpreted as integers modulo the appropriate gcd. For example, e_{121} is an integer modulo $\gcd(\alpha_1, \alpha_2)$; c_2, d_1, and c_{12} appear in its formula, but since c_2, d_1, and c_{12} are integers modulo α_2, α_1, and $\gcd(\alpha_1, \alpha_2)$ respectively, no ambiguity arises in the computation of a particular e_{121}. By Theorem H1, if one takes 14-tuples, $(c_1, \ldots, c_{14})$, $(d_1, \ldots, d_{14})$, c_i, d_j rational integers and lets (18) define a multiplication, a group isomorphic to F/F_4 (free nilpotent group) (F a free group) is obtained. The same proof will go through if the c_i, d_j are integers modulo the appropriate gcd. (One can also check the group axioms directly, a tedious verification.) Note that α_i odd is essential here, since (18) involves

$$\binom{c_i}{2}, \quad \binom{d_i}{2},$$

and this will give difficulty if one is dealing with integers modulo an even integer.

THEOREM 2. *Let $A_1, \ldots, A_t$ be cyclic groups of order $\alpha_1, \ldots, \alpha_t$ respectively, α_i odd integers or* 0. *Let a_i generate A_i. Let*

$$F = \prod_{i=1}^{t} {}^* A_i.$$

Let $u_1, u_2, \ldots,$ be a sequence of standard (monomial) commutators of non-decreasing weight in the a_i of weight $\leqslant 3$ (see (7)*). Let $N_i = \alpha_i$ if u_i is of weight* 1; *$N_i = \gcd(\alpha_i, \alpha_j)$ if $u_i = (a_i, a_j)$ and $N_i = \gcd(\alpha_i, \alpha_j, \alpha_k)$ if a_i, a_j, a_k appear in u_i (of weight* 3). *Then every element of F/F_4 can be uniquely expressed as*

$$g = \prod u_i^{c_i}$$

where c_i are integers modulo N_i. (If $N_i = 0$, then c_i is a rational integer.) If

$$h = \prod u_i^{d_i}$$

is another element of F/F_4, then

$$gh = \prod u_i^{e_i}$$

where $e_i = f_i(c_j, d_k)$ are the polynomials with integral coefficients of Theorem H1.

Proof. The proof is the same as that of Theorem 1. (18) is a multiplication table for G provided the standard commutators are arranged in the order: a_i, (a_i, a_j), (a_i, a_j, a_i), (a_i, a_j, a_j), (a_i, a_j, a_k), (a_j, a_k, a_i) with $i < j < k$.

Comment. Since every finite nilpotent group is a direct product of prime power groups, the α_i may be assumed to be prime powers or 0.

COROLLARY 1. *Let*

$$g = \prod u_i^{c_i}$$

be a particular element of G. Then $g^N = 1$ *where* N *is the least common multiple of the orders of the* $u_i^{c_i}$ *appearing in* g *unless* $g \notin (G, G)$ *and* $3|N$. *In the latter case,* $g^{3N} = 1$, *and* g *may be of order* $3N$. *If any of the* u_i *appearing in* g *are infinite cyclic, then* g *is of infinite order.*

The author is indebted to the referee for a simplification of the statement and proof of this corollary.

Proof. If $g \in (G, G)$, then since (G, G) is Abelian, the Corollary follows. If g contains a u_i which is infinite cyclic, then by (4) and the unique representation of g, g must be infinite cyclic. If $g \notin (G, G)$, and all the factors are of finite order, then at least one of the u_i is equal to an a_j. Looking at (4) with the n of (4) put equal to N, it is obvious that $g^N = 1$ (Lemma 1 is used here) provided $3 \nmid N$, since the $f_i(N)$ will involve N,

$$\binom{N}{2}, \text{ and } \binom{N}{3}.$$

(All commutators are of weight $\leqslant 3$).

If $3|N$, i.e., $3|\alpha_j$ for an a_j appearing in g, then the above reasoning indicates that $g^{3N} = 1$. g can actually be of order $3N$; for example, if

$$G = \{a, b \mid a^3 = b^3 = 1, \quad G_4 = 1\} \tag{19}$$

an actual computation shows that ab, ab^2, a^2b, and a^2b^2 are of order 9; in this case

$$(a^ib^j)^3 \in G_3. \tag{20}$$

Another way of seeing this is to consider equation (7) of **(14)** (due to Sanov) that is,

$$((a, b), b)^{\frac{1}{3}N} \in F(N)F_4 \tag{21}$$

where F can be any group generated by a and b and $F(N)$ is the normal subgroup generated by all $N = 3N'$ powers of elements of F. If a and b are of order N and if all elements of F/F_4 were of order N (or less), then $((a, b), b)$ would be of order $\leqslant \frac{1}{3}N$ and not N as Theorem 2 indicates (that is, $t = 2$, $\alpha_1 = \alpha_2 = N$).

Comment. The group G given by (19) is a kind of curiosity, for p-groups, since it is *not* regular in the sense of Hall **(5**, p. 73**)**. However all groups of the form

$$G = \{a, b | a^{p^\alpha} = b^{p^\alpha} = 1, G_4 = 1\} \tag{22}$$

with $p \geqslant 5$, p a prime, are regular groups in the sense of Hall.

A similar comment can be made in connection with

$$G = \{a, b \mid a^2 = b^2 = 1, G_3 = 1\}, \tag{23}$$

a group of order 8.

COROLLARY 2. *The group* $S_t = \{a_i | 1 \leqslant i \leqslant t, s^3 = 1, s \in S_t\}$ *is not a nilpotent product of cyclic groups of order three, except for* $t = 2$ *when* $S_2 = F/F_3$, $F = \{a_1\}^*\{a_2\}$. *However,* S_t *is a fully regular product* (see [1]) *of the* $\{a_i\}$, *and, in particular, it is the third Burnside product of the* $\{a_i\}$ **(12)**.

Proof. The only candidates for S_t to be a nilpotent product are the first (F/F_3) and second (F/F_4) nilpotent products. (F a free product of cyclic groups of order three.) Since $((a_1, a_2), a_1) \neq 1$ in F/F_4 while $((a_1, a_2), a_1) = 1$ in S_t (cf. **(9)**), S_t cannot be a second nilpotent product. As for the first nilpotent product (that is, F/F_3), $(a_1, a_2, a_3) = 1$ in this case, while $(a_1, a_2, a_3) \neq 1$ in S_t. However, if $t = 2$, $S_2 = F/F_3$ where F is the free product of two cyclic groups of order three, and $S_2 =$ first nilpotent product of $\{a_1\}$ and $\{a_2\}$ **(2, 9)**.

THEOREM 3. *Let* $A_1, \ldots, A_t$ *be cyclic groups of order* $\alpha_1, \ldots, \alpha_t$ *respectively. If* A_i *is infinite cyclic, let* $\alpha_i = 0$. *Let* a_i *generate* A_i; *let* $F = \prod^t{}_{i=1}{}^* A_i$. *Let* $n \geqslant 3$ *be a fixed positive integer and let all the primes appearing in the factorizations of the* $\alpha_i \geqslant n - 1$. *Let* $u_1, \ldots,$ *be a sequence of standard monomial commutators of non-decreasing weight in the* a_i *of weight* $\leqslant n - 1$. *Let* $N_i = \alpha_i$ *if* u_i *of weight* 1, *and*

$$N_i = \gcd(\alpha_{i1}, \ldots, \alpha_{ik}) \text{ if } a_{ij},\ 1 \leqslant j \leqslant k,$$

appears in u_i. *Then every element* g, *of* $G = F/F_n$ *can be uniquely expressed as*

$$g = \prod u_i^{c_i}$$

where the c_i *are integers modulo* N_i. (*If* $N_i ;=0$, c_i *is a rational integer.*) *If*

$$h = \prod u_i^{d_i}$$

is another element of F/F_n, *then*

$$gh = \prod u_i^{e_i}$$

where $e_i = f_i(c_j, d_k)$ *are the polynomials with integer coefficients of Theorem* H1.

We note that if F were free, the u_i of weight k would form a basis for F_k/F_{k+1}, see **(7)**.

Proof. The proof is exactly the same as that of Theorems 1 and 2. Lemma 1 shows that the orders of the u_i are as stated in the theorem, so that every element of g is of the form stated, and the only problem is uniqueness. As in Theorem 1, one can theoretically compute a multiplication table similar to (18). This is computed by multiplying

$$u_1^{c_1} \ldots u_s^{c_s} . u_1^{d_1} \ldots u_s^{d_s} = u_1^{c_1} \ldots u_{s-1}^{c_s-1} u_1^{d_1} u_s^{c_s} (u_s^{c_s}, u_1^{d_1}) u_1^{d_2} \ldots$$

etc., and using (5), (6), or (10), or a suitable modification of them. The coefficients of the multiplication table will involve

$$c_i, d_j, \binom{c_i}{2}, \binom{d_j}{2}, \ldots, \binom{c_i}{n-2}, \binom{d_j}{n-2}.$$

https://doi.org/10.4153/CJM-1960-039-x Published online by Cambridge University Press

Note that the $f_k(n)$ of largest order will come from applying (5) and (10) to

$$(u_s^{c_s}, u_1^{d_1}) \quad \text{or} \quad (u_j^{c_j}, u_i^{d_i},)\ i < j$$

and since in (5) one is dealing with commutators in X and (X, Y), the corresponding coefficients of the $f_i(c_j, d_k)$ will involve at most

$$\binom{c_i}{n-2}, \binom{d_j}{n-2} \quad \text{not} \quad \binom{c_i}{n-1}, \binom{d_j}{n-1}.$$

Hence, since all the primes of the $\alpha_j \geqslant n - 1$, no ambiguity will occur because the c_i and d_j are taken modulo the appropriate gcds. Hence Theorem H1 can be used with the $f_i(c_j, d_k)$ considered as integers modulo the appropriate gcds, and this is sufficient to prove the theorem.

COROLLARY. *Let*

$$g = \prod u_i^{c_i}$$

be the unique representation of an element of G. Let N be the least common multiple of the orders of the $u_i^{c_i}$ *appearing in g.*

Case I. *If one of the* u_i *is infinite cyclic, then g is infinite cyclic.*

Case II. *All the primes appearing in the orders of the* u_i *are greater than* $n - 1$ OR $g \in (G, G)$. *(g is assumed to have factors which are all of finite order.) Then* $g^N = 1$.

Case III. $g \notin (G, G)$ *and* p *(a prime)* $= n - 1$ *and p appears in the factorization of one of the* α_j *where* a_j *is a factor of g. Then* $g^{pN} = 1$, *and there are cases where* $g^N \neq 1$.

Proof. Case I follows from (4) and the uniqueness of the representation of g. (Consider what happens in (4) to the infinite cyclic u_i of least weight.) For Case II, consider (4) where $R_i = u_i^{c_i}$ (of g). If every u_i (of g) $\in G_{n-1}$, then (4) gives $g^N = 1$. If $g \in G_{n-s}$, use induction on s, (4), (6) Lemma 1, and the fact that the u_i of (4) can be expressed as products of commutators of the form

$$(a_{i_1}, \ldots, a_{i_k}).$$

If all the primes appearing in the α_j of u_i (of g) are greater than $n - 1$, the $f_i(N)$ of (4) will involve

$$\binom{N}{2}, \ldots, \binom{N}{n-1},$$

and $N \mid f_i(N)$, hence

$$u_i^{f_i(N)} = 1$$

and $g^N = 1$. If $g \in (G, G)$, then the same proof holds except that the $f_i(N)$ involve

$$\binom{N}{2}, \ldots, \binom{N}{n-2}.$$

For Case III, if $p = n - 1$, p a prime, and for some a_j (appearing in g, $p|\alpha_j$ (hence $p|N$), then

$$\binom{N}{n-1} = \binom{N}{p}$$

may cause difficulty, but in any case,

$$pN \Big| \binom{pN}{p}$$

and hence $g^{pN} = 1$. If $\alpha_1 = \alpha_2 = \ldots = \alpha_t = p^\lambda = N$ where $p = n - 1$, then according to Sanov **(13)**,

$$(a_1, \underbrace{a_2, \ldots, a_2}_{p-1 \text{ times}})^{p^{\lambda-1}} \in F(p^\lambda)F_{p+1} = F(p^\lambda)F_n \qquad (p = n-1)$$

where

$$F(p^\lambda) = \{x^{p^\lambda}|x \in F\} .$$

If $g^{p^\lambda} = 1$ for every element of F/F_n,

$$(a_1, \underbrace{a_2, \ldots, a_2}_{p-1 \text{ times}})$$

would have order $p^{\lambda-1}$ or less which contradicts Theorem 3 (according to which $(a_1, a_2, \ldots, a_2)$ has order p^λ). Hence there exist elements which have order $p^{\lambda+1} = pN$. In view of the Corollary to Theorem 2, probably

$$(a_1a_2)^{p^\lambda} \neq 1.$$

Comment. If $a_i^p = 1$, $1 \leqslant i \leqslant t$, $n \leqslant p$, p a prime, all elements of G are of order p, and hence G is a factor group of the Burnside group B with exponent p in t generators. In **(10)** and **(13)** it is shown that B_s/B_{s+1} has the same rank as F_s/F_{s+1} (F the free group with t generators) for $s = 1, 2, \ldots,$ $p - 1$. This provides a partial verification of Theorem 3.

Comment. In **(4)** Gruenberg states and proves "Hall's Second Basis Theorem." It is essentially Theorem 3 for the case $\alpha_1 = \alpha_2 = \alpha_3 = \ldots$ $= \alpha_t = p^\lambda$ and $n \leqslant p$. Theorem 3 shows that Hall's Second Basis Theorem holds "one step further" for $n = p + 1$.

3. The "ill-behaved" case. If $p < n - 1$, the proofs above break down The case of $A = \{a\}$, $B = \{b\}$, $a^2 = b^2 = 1$ is of interest. In $F = A*B$ (the free product of A and B), (A, B) is infinite cyclic and generated by (a, b). Since

https://doi.org/10.4153/CJM-1960-039-x Published online by Cambridge University Press

$$1 = (a, b^2) = (a, b)^2((a, b), b), \tag{24}$$

$(a, b)^2 \in F_3$. Similarly

$$1 = ((a, b), b^2) = ((a, b), b)^2(((a, b), b), b) = (a, b)^{-4}(((a, b), b), b).$$

By induction,

$$(a, b)^{2n-2} \in F_n;$$

hence in F/F_n,

$$(a, b)^{2n-2} = 1.$$

By **(8)**, the F_n, $n = 1, 2, \ldots$, are all distinct and hence (A, B) in F/F_n is exactly of order 2^{n-1} and F/F_n is of order 2^n.

That this is not a freak case can be seen from Theorem 4 below. Since finite nilpotent groups are direct products of prime power groups, it is sufficient for $n = 4$ to discuss the case of $p = 2$.

THEOREM 4. *Let $A_i = \{a_i\}$, $1 \leqslant i \leqslant t$ be cyclic groups of order 2^{r_i}. Let $r_1 \leqslant r_2 \leqslant \ldots \leqslant r_t$. Let $F = \prod^t{}_{t=1}^* A_i$. Let $G = F/F_4$. Then every element of G can be expressed uniquely in the form*

$$a_1^{c_1}a_2^{c_2}\ldots a_t^{c_t}\prod_{i<j}(a_i, a_j)^{c_{ij}}(a_i^2, a_j)^{c_{ij}^{(2)}}(a_i, a_j^2)^{c_{ij}^{(3)}}\cdot \tag{25}$$

$$\prod_{i<j<k}((a_i, a_j), a_k)^{c_{ijk}}((a_j, a_k), a_i)^{c_{jki}}$$

where the c_i, c_{ij}, $c_{ij}^{(2)}$, c_{ijk}, c_{jki} are integers modulo

$$2^{r_i}, 2^{r_i+1}, 2^{r_i-1}, 2^{r_i}, 2^{r_i}$$

respectively while $c_{ij}^{(3)}$ are integers modulo 2^{r_i-1}, if $r_i = r_j$, and 2^{r_i} if $r_i \neq r_j$. In particular, (a_i, a_j) is of order 2^{r_i+1} for $i \neq j$.

Formulas for multiplying two elements of G are given below.

Proof. Let a, b, c be three of the a_i of orders n_a, n_b, n_c, respectively, $n_a \leqslant n_b \leqslant n_c$. By (16)

$$1 = (a^{n_a}, b) = (a, b)^{n_a}(a, b, a)^{\binom{n_a}{2}}, a, b \in G.$$

From the work of Magnus **(11)**, it follows that

$$1 = (a, b, a)^{n_a} = (a, b, b)^{n_a} = (a, b, c)^{n_a} = (b, c, a)^{n_a} \qquad \text{in } G.$$

Since (G, G) is Abelian, and $\binom{n_a}{2} \equiv n_a/2 \pmod{n_a}$

$$(a, b)^{2n_a} = 1 \tag{26}$$

and

$$(a, b)^{-n_a} = (a, b)^{n_a} = ((a, b), a)^{\frac{1}{2}n_a}. \tag{27}$$

If $n_a = n_b$, the same reasoning gives

$$(a, b)^{n_a} = ((a, b), b)^{\frac{1}{2}n_a}.$$

However, if $n_a < n_b$, all that can be said is $((a, b), b)^{n_a} = 1$. In view of (26) and (27), computing a multiplication table using a representation such as (18) would be somewhat complicated; to avoid this difficulty, note that in G

$$(28) \qquad \begin{aligned}(a^2, b) &= (a, b)^2((a, b), a)\\ (a, b^2) &= (a, b)^2((a, b), b)\end{aligned}$$

and hence $\{(a, b), ((a, b), a), ((a, b), b)\} = \{(a, b), (a, b^2), (a^2, b)\}$. Now, using (27) and the fact that (G, G) is Abelian,

$$(a^2, b)^{\frac{1}{2}n_a} = (a, b)^{n_a}((a, b), a)^{\frac{1}{2}n_a} = 1.$$

If $n_a = n_b$, then $(a, b^2)^{\frac{1}{2}n_a} = 1$, while if $n_a < n_b$,

$$(a, b^2)^{n_a} = (a, b)^{2n_a}((a, b), b)^{n_a} = 1.$$

Hence every element of G can be expressed in the form of (25). If one multiplies two elements like (25), that is, let

$$\begin{array}{lll} c = a_1^{c_1}a_2^{c_2}\ldots & (a_i, a_j)^{c_{ij}}\ldots & ((a_i, a_j), a_k)^{c_{ijk}}\ldots \\ d = a_1^{d_1}a_2^{d_2}\ldots & (a_i, a_j)^{d_{ij}}\ldots & ((a_i, a_j), a_k)^{d_{ijk}}\ldots \\ e = a_1^{e_1}a_2^{e_2}\ldots & (a_i, a_j)^{e_{ij}}\ldots & ((a_i, a_j), a_k)^{e_{ijk}}\ldots \end{array}$$

with $e = c\cdot d$, then

$$e_i = c_i + d_i$$

$$e_{ij} = c_{ij} + d_{ij} - 2\alpha(c_{ij})d_i - 2\alpha(c_{ij})d_j - c_jd_i + 2c_j\binom{d_i}{2} + 2d_i\binom{c_j}{2} + 2\,c_jd_id_j$$

$$(29) \qquad e_{ij}^{(2)} = c_{ij}^{(2)} + d_{ij}^{(2)} + \alpha(c_{ij})d_i - c_j\binom{d_i}{2}$$

$$e_{ij}^{(3)} = c_{ij}^{(3)} + d_{ij}^{(3)} - d_i\binom{c_j}{2} + \alpha(c_{ij})d_j - c_jd_id_j$$

$$e_{ijk} = c_{ijk} + d_{ijk} + \alpha(c_{ik})d_j - c_kd_id_j - d_ic_jc_k + \alpha(c_{ij})d_k - c_jd_id_k$$

$$e_{jki} = c_{jki} + d_{jki} + \alpha(c_{jk})d_i + \alpha(c_{ik})d_j - c_kd_id_j$$

where

$$\alpha(c_{ij}) = c_{ij} + 2c_{ij}^{(2)} + 2c_{ij}^{(3)}.$$

Here there appear to be a few problems as to ambiguities, since, for example, d_i is an integer modulo 2^{r_i} and appears in the computation of e_{ij} which is an integer modulo 2^{r_i+1}. However, if d_i is replaced by $d_i + 2^{r_i}$, then

$$-\,c_jd_i + 2\,c_j\binom{d_i}{2} + 2d_i\binom{c_j}{2}$$

remains unchanged modulo 2^{r_i+1}. Similar reasoning applies to other cases of apparent ambiguity.

We can now proceed as in the proof of Theorem 1 and construct a group H made of

$$t + 3\binom{t}{2} + 2\binom{t}{3} - \text{tples}$$

with multiplication as indicated by (29). The verification of the group axioms is straightforward, but tedious.

It might be asked whether or not a modification of (18) could not be used instead of (29). There are several difficulties: in the case of $p = 2$, the e_{ij} are integers modulo 2^{r_i+1}, but c_j, d_i which appear in the formula for e_{ij} are integers modulo 2^{r_i} (assuming $r_i = r_j$). Similarly if $r_i = r_j$, e_{iji} is an integer modulo 2^{r_i} and $\binom{d_i}{2}$ will cause difficulties, since it is not unambiguously defined modulo 2^{r_i}. If one decides to let c_{ij} be integers modulo 2^{r_i}, then the fact that

$$(a_i, a_j)^{2^{r_i}} = (a_i, a_j, a_i)^{2^{r_i - 1}} \qquad \text{(see (27))}$$

means that the multiplication formulas would have to take into account in some way the fact that the order of (a_i, a_j) is 2^{r_i+1}. The author tried to think of a device to get around these difficulties, but was unable to do so.

If one attempts to carry out computations for the general case, with $p < n - 1$, then by using (5) and (6) one readily obtains Lemma 3 below. Since nilpotent groups of finite order are direct products of p-groups, we consider only the case of p-groups here.

LEMMA 3. *Let $A_1, \ldots, A_t$ be cyclic groups of order*

$$p^{\alpha_1}, \ldots, p^{\alpha_t}$$

respectively. Let a_i generate A_i. Let $F = \prod{}^{t}_{i=1}{}^{*} A_i$. Let $G = F/F_n$; let

$$v = (a_{i_1}, a_{i_2}, \ldots, a_{i_r}) \in G_r.$$

Let

$$\alpha = \min (\alpha_{i_1}, \ldots, \alpha_{i_r}).$$

Then

$$v^{p^\alpha} \in G_{r+(p-1)} \tag{30}$$

$$v^{p^{\alpha+j}} \in G_{r+(j+1)(p-1)} \qquad j = 0, 1, 2 \ldots.$$

If $w \in G_r$, then w can be substituted for v in (30).

Proof. The proof follows by induction ($r = n - 1, n - 2, \ldots,$) and uses (6) and (4).

Note that (20) is a special case of (30) with $w = a^i b^j$, $r = 1$, $p = 3$, $\alpha = 1$, $j = 0$, $n = 4$. Similarly, using group (23), one obtains another special case of Lemma 3, with $w = ab$, $r = 1$, $p = 2$, $n = 3$, $\alpha = 1$, $j = 0$. This gives rise to the conjecture that these may be the best possible results in the following sense:

Conjecture. In the notation of Lemma 3, the order of v is $p^{\alpha+j}$, where j is the least integer such that

$$r + (j + 1)(p - 1) \geqslant n.$$

However, the author was unable to think of a way to prove that the order of v is exactly $p^{\alpha+j}$ and not something less, nor of a manageable method to solve the general case of $p < n - 1$.

References

1. O. N. Golovin, *Nilpotent products of groups*, Mat. Sbornik N.D., *27* (*69*) (1950), 427–454. Amer. Math. Soc. Translations, 2, *2* (1956), 89–115.

2. ——— *Metabelian products of groups*, Mat. Sbornik N.S., *28* (*70*) (1951), 431–444. Amer. Math. Soc. Translations, 2, *2* (1956), 117–132.

3. ——— *On the isomorphism of nilpotent decompositions of groups*, Mat. Sbornik N.S., *28* (*70*) (1951), 445–452. Amer. Math. Soc. Translations, 2, *2* (1956), 133–140.

4. K. W. Gruenberg, *Residual properties of infinite soluble groups*, Proc. London Math. Soc., Series 3, *7* (1957), 29–62.

5. Philip Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc., *36* (1934), 29–95.

6. ——— *Nilpotent groups*, Lecture Notes of Summer Seminar, Canadian Mathematical Congress (University of Alberta, August, 1957).

7. Marshall Hall, *A basis for free Lie rings and higher commutators in free groups*, Proc. Amer. Math. Soc., *1* (1950), 575–581.

8. A. Karass and D. Solitar, *On free products of groups*, Bull. Amer. Math. Soc., *63* (1957), 407

9. Friedrich Levi and B. L. van der Waerden, *Ueber eine Besondere Klasse von Gruppen*, Abhandlungen aus dem Hamburg Universität., *9* (1932), 154–158.

10. R C Lyndon, *On Burnside's problem, I.* Trans. Amer. Math. Soc., *77* (1954), 202–215.

11. W. Magnus, *Ueber Beziehungen zwischen höheren Kommutatoren*, J. Reine Angew. Math., *177* (1937), 105–115.

12. S. Moran, *Associative operations on groups* I. Proc. London Math. Soc., *6* (1956), 581–596.

13. I. N. Sanov, *Establishment of a connection between periodic groups with prime power periods and Lie rings.* Izvestiya Akad Nauk SSSR Ser Mat., *16* (1952), 23–58.

14. R. R. Struik, *Notes on a paper by sanov*, Proc. Amer. Math. Soc., *8* (1957), 638–641.

15. ——— *A note on prime power groups*, Can. Math. Bull., *3* (1960), 27–30.

University of British Columbia