ON NILPOTENT PRODUCTS OF CYCLIC GROUPS. II

RUTH REBEKKA STRUIK

Introduction. In a previous paper **(18)**,[1] $G = F/F_n$ was 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. In that paper the following cases were completely treated:

(a) F a free product of cyclic groups of order p^{α_i}, p a prime, α_i positive integers, and $n = 4, 5, \ldots, p + 1$.

(b) F a free product of cyclic groups of order 2^{α_i}, and $n = 4$.

In this paper, the following case is completely treated:

(c) F a free product of cyclic groups of order p^{α_i}, p a prime, α_i positive integers, and $n = \mathrm{p} + 2$.

(Note that $n = 2$ is well known, and $n = 3$ was studied by Golovin **(2)**.) By "completely treated" is meant: a unique representation of elements of the group is given, and the order of the group is indicated. In the case of $n = 4$, a multiplication table was given.

In view of the well-known decomposition of finite nilpotent groups into direct products of p-groups, cases (a), (b), and (c) can be summarized:

(d) F a free product of cyclic groups of order α_i where the prime factors of $\alpha_i \geqslant n - 2$.

Since the results, equations, and bibliography of **(18)** are used extensively in this paper, the numbering of theorems, equations, and bibliography will be a continuation of that of **(18)**. For example, (18) and (29) refer to equations (18) and (29) of **(18)**, and this paper starts with equation (31). The same notation will also be used.

Section 1 gives preliminary results. Lemma 4 may be of particular interest, as it is an application of P. Hall's collecting process, and may be of use in attacking other group-theoretic problems. Section 2 is an exposition of the "idea" of this paper; the device used in **(18)** to deal with case (b) can be applied to (c). In § 3, case (c) is handled.

1.

LEMMA 4. *Let a, b be any two elements of a nilpotent group, and r, s any two positive integers. Then*

$$(31) \qquad b^s a^r = a^r b^s (b, a)^{rs} ((b, a), a)^{\binom{r}{2} s} ((b, a), b)^{r \binom{s}{2}} \ldots u_i^{f_i} \ldots$$

Received June 17, 1960.

[1]Reference numbers refer to, or are continued from, this paper.

https://doi.org/10.4153/CJM-1961-045-2 Published online by Cambridge University Press

where if u_i is a standard commutator involving α a's and β b's, then

$$f_i = \sum_{\substack{j \leqslant \alpha \\ k \leqslant \beta}} n_{ijk} \binom{r}{j} \binom{s}{k},$$

n_{ijk} non-negative integers. In particular, if

$$u_i = (((b, \underbrace{a), a), \ldots, a}_{\alpha}),$$

then $f_i = \binom{r}{\alpha} s$, and if

$$u_j = ((((b, a), \underbrace{b), b), \ldots, b}_{\beta-1}),$$

then $f_j = r\binom{s}{\beta}$.

Proof. The proof is exactly the same as that given on pp. 179–181 of **(16)**. However, instead of (12.3.1) on p. 179, we have

$$b(1)b(2)\ldots b(s)a(1)a(2)\ldots a(r) \tag{32}$$

that is, the s b's and the r a's are each labelled. The precedence conditions at this first stage become

$$\begin{aligned} &b(\lambda) \text{ precedes } b(\mu) \text{ if } \lambda < \mu \\ &b(\lambda) \text{ precedes } a(\mu) \text{ if } \lambda < \mu \text{ or } \lambda = \mu \text{ or } \lambda > \mu \\ &a(\lambda) \text{ precedes } a(\mu) \text{ if } \lambda < \mu. \end{aligned} \tag{33}$$

After the a's have been collected (32) becomes an expression of the form

$$a^r b(b, a)(b, a)((b, a), a)\ldots b(b, a)(b, a)((b, a), a)\ldots \tag{34}$$

where each b and each a have the same label as before; each (b, a) has a label of the form (λ, μ); $1 \leqslant \lambda \leqslant s$; $1 \leqslant \mu \leqslant r$; it arose when $a(\mu)$ was collected: $b(\lambda)a(\mu) = a(\mu)b(\lambda)(b, a)(\lambda, \mu)$. In general, if u_j is being collected and $u_i > u_j$, and if u_i has the label $(\lambda_1, \ldots, \lambda_\sigma)$ and u_j has the label $(\mu_1, \ldots, \mu_\omega)$, then (u_i, u_j) will have the label $(\lambda_1, \ldots, \lambda_\sigma, \mu_1, \ldots, \mu_\omega)$. The existence and precedence conditions at each stage of the collecting process are all conditions (L) as described on p. 180 of **(16)**, and the induction proof given there goes through in exactly the same way to give Lemma 4. That

$$(((b, \underbrace{a), \ldots, a}_{\alpha})$$

will have the exponent

$$s\binom{r}{\alpha}$$

follows from the fact that all $(\lambda_1, \mu_1, \ldots, \mu_\alpha)$ which can be associated with such $(((b, a), \ldots, a)$ satisfy the conditions: $1 \leqslant \lambda_1 \leqslant s$; $1 \leqslant \mu_1 < \mu_2 < \ldots < \mu_\alpha \leqslant r$. A similar argument holds for $((((b, a), b) \ldots b)$.

LEMMA 5.

$$\binom{\binom{r}{i}\binom{s}{j}}{k} = \sum_{\substack{\alpha \leqslant ik \\ \beta \leqslant jk}} n_{\alpha,\beta} \binom{r}{\alpha}\binom{s}{\beta},$$

$n_{\alpha,\beta}$ non-negative integers.

Proof. The following set, S, has order $\binom{r}{i}\binom{s}{j}$:

$$S = \left\{ (a_1, \ldots, a_i, b_1, \ldots, b_j)\ a_t, b_u \text{ integers } \begin{matrix} 1 \leqslant a_1 < \ldots < a_i \leqslant r \\ 1 \leqslant b_1 < \ldots < b_j \leqslant s \end{matrix} \right\}.$$

Let T consist of all subsets of order k taken from S;

$$T = \{(a_1^{(1)}, \ldots, a_i^{(1)}, b_1^{(1)}, \ldots, b_j^{(1)}), \ldots, (a_1^{(k)}, \ldots, a_i^{(k)}, b_1^{(k)}, \ldots, b_j^{(k)})\}.$$

T can be partitioned into disjoint subsets, depending on which of the $a_t^{(s)}$ or $b_u^{(v)}$ are equal to, greater than, or less than each other. Each such subset has order

$$\binom{r}{\alpha}\binom{s}{\beta}, \alpha \leqslant ik, \beta \leqslant jk.$$

This is sufficient to prove the lemma.

LEMMA 6. *Let A be any rational integer, p any prime and α any positive integer. Then*

$$\binom{A + p^\alpha}{p - 1} \equiv \binom{A}{p - 1} \pmod{p^\alpha}. \tag{35}$$

Proof. By definition

$$\binom{A + p^\alpha}{p - 1} = \frac{(A + p^\alpha)(A - 1 + p^\alpha) \ldots (A - p + 1 + p^\alpha)}{(p - 1)!}$$
$$= \binom{A}{p - 1} + \frac{p^\alpha u}{(p - 1)!}$$

where u is an integer. Since both

$$\binom{A + p^\alpha}{p - 1} \text{ and } \binom{A}{p - 1}$$

are integers, $p^\alpha u/(p - 1)!$ is an integer. Since $(p - 1)!$ and p^α are relatively prime, $(p - 1)!$ divides u. This is sufficient to prove Lemma 6.

LEMMA 7. *Let A, p, α be as in Lemma 6. Then*

$$\binom{A + p^\alpha}{p} \equiv \binom{A}{p} + p^{\alpha - 1} \pmod{p^\alpha} \tag{36}$$

Proof. Lemma 7 is true for $A = 0$, since $\binom{0}{p} = 0$, and

https://doi.org/10.4153/CJM-1961-045-2 Published online by Cambridge University Press

$$\binom{p^\alpha}{p} = p^{\alpha-1}\binom{p^\alpha - 1}{p-1} = p^{\alpha-1}(1+sp) \equiv p^{\alpha-1} \pmod{p^\alpha}. \tag{37}$$

$$\binom{p^\alpha - 1}{p-1} = 1 + sp, \tag{38}$$

where s is some integer, is justified with the use of Wilson's theorem (see p. 259 of **(17)**), that is, $(p-1)! = -1 \pmod p$. The numerator and denominator of the left-hand side of (38) consist of $p-1$ consecutive integers relatively prime to p, and the use of Wilson's theorem along with the fact that the integers modulo p form a field completes the proof of (37) and (38). This proves Lemma 7 for $A = 0$. Suppose true for A, then using induction and Lemma 6

$$\binom{A+1+p^\alpha}{p} = \binom{A+p^\alpha}{p} + \binom{A+p^\alpha}{p-1} \equiv \binom{A}{p} + p^{\alpha-1} + \binom{A}{p-1} \pmod{p^\alpha} \tag{39}$$

$$\binom{A+1}{p} = \binom{A}{p} + \binom{A}{p-1}. \tag{40}$$

Combining (39) and (40) gives the proof of Lemma 7 for A a positive integer. A similar argument proves Lemma 7 for A a negative integer.

LEMMA 8. *Let A, B, C, D be rational integers, p a prime, and α a positive integer. If*

$$A \equiv C \pmod{p^\alpha}$$

and

$$B \equiv D \pmod{p^\alpha},$$

then

$$AB - p\binom{A}{p}B - p\binom{B}{p}A \equiv CD - p\binom{C}{p}D - p\binom{D}{p}C \pmod{p^{\alpha+1}}. \tag{41}$$

Proof. It is sufficient to prove (41) for the cass $C = A + p^\alpha$ and $B = D$ in view of the symmetry of (41). Then (41) becomes

$$\begin{aligned} AB - p\binom{A}{p}B - p\binom{B}{p}A \\ \equiv (A+p^\alpha)B - p\binom{A+p^\alpha}{p}B - p\binom{B}{p}(A+p^\alpha) \pmod{p^{\alpha+1}}. \end{aligned} \tag{42}$$

If one expands the right-hand side of (42) and makes use of Lemma 7, one obtains the left-hand side of (42) modulo $p^{\alpha+1}$. Note that since

$$\binom{A+p^\alpha}{p} \equiv \binom{A}{p} + p^{\alpha-1} \pmod{p^\alpha},$$

$$p\binom{A+p^\alpha}{p} \equiv p\binom{A}{p} + p^\alpha \pmod{p^{\alpha+1}}.$$

2. In this section, the "idea" of the proof will be explained. Details will be carried out in § 3.

In § 2 of **(18)**, the "well-behaved" case was studied. In F, a free group or a free product of cyclic groups, a sequence of standard commutators $u_1, \ldots$ was selected and it was shown that every element of F/F_n could be written uniquely as $\prod u_k^{c_k}$. In the case of F/F_4 (18) gives the multiplication table for two such elements. One reason for the failure of the proof for the case $p = 2$ with F/F_4 is that in (18), terms such as $\binom{d_i}{2}$ appear which are not unique modulo the appropriate powers of 2. To get around this difficulty, another set of basis elements was chosen in § 3 to handle the case of $p = 2$. When the new basis is used (29) is the multiplication table of two elements of F/F_4. Actually, (29) can be considered a modification of (18) in the following sense: Let $F = \{a, b\}$ be a free group on two generators. Then every element g of F/F_4 can be expressed (uniquely) as

$$a^{c_1}b^{c_2}(a, b)^{c_{12}}((a, b), a)^{c_{121}}((a, b), b)^{c_{122}} \tag{43}$$

where c_i, c_{12}, c_{ijk} are rational integers. When (28) is used every element of F/F_4 can be expressed uniquely as

$$a^{\gamma_1}b^{\gamma_2}(a, b)^{\gamma_{12}}(a^2, b)^{\gamma_{121}}(a, b^2)^{\gamma_{122}} \tag{44}$$

where γ_i, γ_{12}, γ_{ijk} are rational integers. Since

$$\begin{aligned}
&a^{c_1}b^{c_2}(a, b)^{c_{12}}((a, b), a)^{c_{121}}((a, b), b)^{c_{122}} \\
&\qquad = a^{c_1}b^{c_2}(a, b)^{c_{12}}((a^2, b)^{c_{121}}(a, b)^{-2c_{121}}(a, b^2)^{c_{122}}(a, b)^{-2c_{122}} \\
&\qquad = a^{c_1}b^{c_2}(a, b)^{c_{12}-2c_{121}-2c_{122}}(a^2, b)^{c_{121}}(a, b^2)^{c_{122}},
\end{aligned}$$

$$\begin{array}{llll}
 & \gamma_i = c_i & & c_i = \gamma_i \\
(45) & \gamma_{12} = c_{12} - 2c_{121} - 2c_{122} & & c_{12} = \gamma_{12} + 2\gamma_{121} + 2\gamma_{122} = \alpha(\gamma_{12}) \\
 & \gamma_{121} = c_{121} & & c_{121} = \gamma_{121} \\
 & \gamma_{122} = c_{122} & & c_{122} = \gamma_{122}.
\end{array}$$

Let

$$\begin{aligned}
h &= a^{d_1}b^{d_2}(a, b)^{d_{12}}((a, b), a)^{d_{121}}((a, b), b)^{d_{122}} \\
&= a^{\delta_1}b^{\delta_2}(a, b)^{\delta_{12}}(a^2, b)^{\delta_{121}}(a, b^2)^{\delta_{122}}
\end{aligned}$$

and

$$\begin{aligned}
g\cdot h &= a^{e_1}b^{e_2}(a, b)^{e_{12}}((a, b), a)^{e_{121}}((a, b), b)^{e_{122}} \\
&= a^{\epsilon_1}b^{\epsilon_2}(a, b)^{\epsilon_{12}}(a^2, b)^{\epsilon_{121}}(a, b^2)^{\epsilon_{122}}.
\end{aligned}$$

One can now take ϵ_{12} (or ϵ_{121} or ϵ_{122}), express it in terms of e_{12}, e_{121}, e_{122} using (45), then in terms of c_{12}, d_{12}, c_{121}, d_{121}, c_{122}, d_{122} using (18) with $i = 1$ and $j = 2$, and then in terms of γ_{12}, δ_{12}, γ_{121}, δ_{121}, γ_{122}, δ_{122} using (45). This gives the ϵ's in terms of the γ's and the δ's. If one now substitutes e_{12}, c_{12}, d_{12} for ϵ_{12}, γ_{12}, δ_{12} and $e_{12}^{(2)}$, $c_{12}^{(2)}$, $d_{12}^{(2)}$ for ϵ_{121}, γ_{121}, δ_{121} and $e_{12}^{(3)}$, $c_{12}^{(3)}$, $d_{12}^{(3)}$ for

$\epsilon_{122}, \gamma_{122}, \delta_{122}$ respectively, one obtains (29) for $i = 1,\ j = 2$. Hence (29) is a modification of (18) in the sense that one set of basic commutators has been substituted for another, but the same multiplication table has been used. Hence it is not necessary to check the group axioms for the group H, as indicated after (29); all that needs to be done is to ascertain whether (29) is unambiguous modulo appropriate powers of 2. The author did not realize this until after writing paper **(18)**.

This same idea will be used to study F/F_{p+2} where F is a free product of cyclic groups of order p^{α_i}, p a fixed prime. The over-all strategy is:

I. Investigations of the terms appearing in the multiplication table analogous to (18) for F/F_{p+2}. In particular, it will be shown that p appears in the denominator of a term only when the corresponding u_i is

$$((\underbrace{(b, a), \ldots , a}_{p})$$

or

$$(((\underbrace{(b, a), b), \ldots , b}_{p-1}).$$

Call these terms u_p' and u_p'' respectively.

II. u_p' and u_p'' will be replaced by (b, a^p) and (b^p, a) respectively, and the multiplication table of F/F_{p+2} analogous to (29) will be investigated to ascertain whether the terms are unambiguous modulo appropriate powers of p.

It will be assumed that F is a free group until near the end. The proof of the unambiguity of the multiplication table modulo appropriate powers of p will be sufficient to prove the desired theorem for F a free product of cyclic p-groups.

3.

I. *Investigation of the multiplication table of $G = F/F_{p+2}$ where each element of G is expressed as a product of standard commutators.*

Let $F\{a, b\}$ be a free group with two generators, and let $g \in F/F_n$. Then g can be uniquely expressed as

$$g = a^{c_1}b^{c_2}(b, a)^{c_3}((b, a), a)^{c_4}((b, a), b)^{c_5} \ldots = \prod u_i^{c_i}$$

where u_i are a sequence of standard commutators (see **(7)**) and c_i are rational integers. Let $h \in F/F_n$ and

$$h = a^{d_1}b^{d_2}(b, a)^{d_3} \ldots = \prod u_i^{d_i} .$$

Then to compute a multiplication table of F/F_n analogous to (18), we put

$$a^{e_1}b^{e_2} \ldots = \prod u_i^{e_i} = a^{c_1}b^{c_2} \ldots a^{d_1}b^{d_2} \ldots = g \cdot h$$

and we first collect a^{d_1}, then b^{d_2} and so on. A typical step consists in

$$(46) \qquad u_i^{c_i}u_j^{d_j} = u_j^{d_j}u_i^{c_i}(u_i, u_j)^{c_i d_j}((u_i, u_j), u_j)^{c_i \binom{d_j}{2}} \ldots$$

where Lemma 4 (that is (31)) is used. Since the commutators appearing on the right-hand side of (46) may not be standard commutators, they should be expressed as products of standard commutators and (4) used. Using Lemma 5, and repeating until the right-hand side of (46) is a product of the original standard commutators, one obtains

$$u_i^{c_i} u_j^{d_j} = u_j^{d_j} u_i^{c_i} \prod u_k^{n_k \binom{c_i}{\alpha_k}\binom{d_j}{\beta_k}} \tag{47}$$

where n_k are non-negative integers. Note that if σ_k is the weight of u_k in a's and b's (that is, $u_k \in F_{\sigma_k}, \notin F_{\sigma_k+1}$), then $\alpha_k + \beta_k \leqslant \sigma_k$. The only time $\binom{c_i}{p}$ or $\binom{d_j}{p}$ appears is if $u_k = (((b, a), a, \ldots, a)$ $(p-1$ a's) or $((((b, a), b), b), \ldots, b)$ $(p-1$, b's).

In general, instead of $u_i^{c_i}$ (or $u_j^{d_j}$) in (46), one may have an element of the form

$$u_i^{\binom{c_{i_1}}{\alpha_1}\cdots\binom{c_{i_s}}{\alpha_s}\binom{d_{i_1}}{\beta_1}\cdots\binom{d_{i_t}}{\beta_t}}$$

in which case the exponent of u_k on the right-hand side of (47) will be of the form

$$n_k\binom{c_{j_1}}{\alpha_1}\cdots\binom{c_{j_s}}{\alpha_s}\binom{d_{j_1}}{\beta_1}\cdots\binom{d_{j_t}}{\beta_t},$$

where n_k are non-negative integers, and

$$\sum \alpha_i + \sum \beta_j \leqslant \sigma_k$$

where u_k has weight σ_k in the a's and b's.

We now investigate under what conditions u_p' and u_p'' occur. Let $u_0' = b$, $u_1' = (b, a)$, $u_{s+1}' = (u_s', a)$ for s a positive integer. Similarly, let

$$u_1'' = (b, a), u_{s+1}'' = (u_s'', b).$$

Note that in (47), each u_k will have at least as many a's and b's as (u_i, u_j). Hence u_s' can occur in (46) and (47) only when a^{d_1} is being collected, for example

$$u_t'^{c_t'} a^{d_1} = a^{d_1} u_t'^{c_t'} \ldots u_s'^{\binom{d_1}{s-t} c_t'} \ldots t < s \tag{48}$$

(where c_t' is the exponent of u_t' in g). Here Lemma 4 is used. Hence, when u_s' is collected, its exponent will be

$$c_s' + d_s' + \sum_{t=0}^{s-1} c_t' \binom{d_1}{s-t} \tag{49}$$

(where d_s' is the exponent of u_s' in h). When a^{d_1} is collected u_s'' occurs:

$$b^{c_2} a^{d_1} = a^{d_1} b^{c_2} u_1''^{c_2 d_1} \ldots u_s''^{d_1 \binom{c_2}{s}} \ldots \tag{50}$$

and hence when b^{d_2} is collected, u_t'' appears twice, once with exponent c_t''

https://doi.org/10.4153/CJM-1961-045-2 Published online by Cambridge University Press

(its exponent from g at the beginning) and also with exponent $d_1\binom{c_2}{t}$ from (50). Hence

$$u_t''^{\alpha}b^{d_2} = b^{d_2}u_t''^{\alpha} \dots u_s''^{\alpha\binom{d_2}{s-t}}.$$

After b^{d_2} is collected, u_s'' will not arise again in the subsequent collectings, so that when it is collected, its exponent will be

$$c_s'' + d_s'' + \sum_{t=1}^{s-1}\left[c_t'' + d_1\binom{c_2}{t}\right]\binom{d_2}{s-t} + d_1\binom{c_2}{s}. \tag{51}$$

The following theorem and corollaries have been proved:

THEOREM 5. *Let $F = \{a, b\}$ be the free group on two generators. Let $G = F/F_n$. Let $u_1, u_2, \dots$ be the sequence of standard monomial commutators of non-decreasing weight $\leqslant n-1$ (see (7)) in a and b. Let $g, h \in G$,*

$$g = a^{c_1}b^{c_2}(b, a)^{c_3} \dots u_i^{c_i} \dots = \prod u_i^{c_i}$$

$$h = a^{d_1}b^{d_2}(b, a)^{d_3} \dots u_i^{d_i} \dots = \prod u_i^{d_i}$$

where c_i, d_i are rational integers. If

$$g\cdot h = \prod u_i^{e_i},$$

then

$$e_i = c_i + d_i + \sum n_k\binom{c_{i_1}}{\alpha_1}\dots\binom{c_{i_s}}{\alpha_s}\binom{d_{i_1}}{\beta_1}\dots\binom{d_{i_t}}{\beta_t} \tag{52}$$

where if $u_i \in F_s$, $u_i \notin F_{s+1}$ (that is, u_i is a commutator of weight s in a and b),

$$\sum \alpha_j + \sum \beta_j \leqslant s.$$

In particular, let $(b, a) = u_1'$, $(u_s', a) = u_{s+1}'$ and c_s', d_s', e_s' be the exponents of u_s' in g, h, and $g\cdot h$ respectively, then

$$e_s' = c_s' + d_s' + \sum_{t=1}^{s-1} c_t'\binom{d_1}{s-t} + c_2\binom{d_1}{s}. \tag{49}$$

Let $(b, a) = u_1''$, $(u_s'', b) = u_{s+1}''$ with c_s'', d_s'', e_s'' the exponents of u_s'' in g, h, $g\cdot h$ respectively, then

$$e_s'' = c_s'' + d_s'' + \sum_{t=1}^{s-1}\left[c_t'' + d_1\binom{c_2}{t}\right]\binom{d_2}{s-t} + d_1\binom{c_2}{s}. \tag{51}$$

COROLLARY 1. *Let $n = p + 2$, p a prime in Theorem 5. Then*

$$e_p' = c_p' + d_p' + \sum_{t=1}^{p-1} c_t'\binom{d_1}{p-t} + c_2\binom{d_1}{p}, \tag{53}$$

$$e_p'' = c_p'' + d_p'' + \sum_{t=1}^{p-1}\left[c_t'' + d_1\binom{c_1}{t}\right]\binom{d_2}{p-t} + d_1\binom{c_2}{p}, \tag{54}$$

and these are the only places where p appears in the denominator of a term of an e_i.

COROLLARY 2. *Let F be a free group on 3 or more generators, p a fixed prime, $u_1, \ldots,$ a sequence of standard commutators in the generators of F,*

$$g = \prod u_i^{ci}, h = \prod u_i^{di}, g \cdot h = \prod u_i^{ei}.$$

Then for $n = p + 2$,

$$e_i = c_i + d_i + \sum n_k \binom{c_{i_1}}{\alpha_1} \cdots \binom{c_{i_s}}{\alpha_s} \binom{d_{i_1}}{\beta_1} \cdots \binom{d_{i_t}}{\beta_t}$$

as in Theorem 5, and if u_i contains at least 3 generators of F, then $\alpha_j < p$, $\beta_j < p$.

Comment. For $u_3 = (b, a)$ $(u_1 = a, u_2 = b)$, (49) becomes

(55) $$e_3 = c_3 + d_3 + c_2 d_1.$$

In (18) the corresponding formula is

$$c_3 + d_3 - c_2 d_1$$

(c_{ij}, d_{ij}, e_{ij} of (18) become c_3, d_3, e_3 here, and $j = 2$ and $i = 1$). The reason for $- c_2 d_1$ in (18) is that (a, b) is used instead of (b, a). Similar comments apply to the other equations of (18).

II. u_p' and u_p'' are replaced by (b, a^p) and (b^p, a) respectively, and the corresponding multiplication table for F/F_{p+2} is investigated.

As before, let F be a free group on two generators, $g, h \in F/F_{p+2}$. Let $u_1 = a$, $u_2 = b$, $u_3 = (b, a), \ldots, u_s'$ and u_s'' as in Theorem 5; similarly for g, h and $g \cdot h$. Let $v_i = u_i$ except that u_p' is replaced by $(b, a^p) = v_p'$, and u_p'' is replaced by $(b^p, a) = v_p''$. If one puts $s = 1$ and $r = p$ in (31), and brings $a^p b$ over to the left-hand side, one obtains

(56) $$(b, a^p) = b^{-1} a^{-p} b a^p = (b, a)^p \prod u_i^{pf_i} u_p' \qquad (\text{mod } F_{p+2})$$

where f_i are positive integers, that is,

(57) $$v_p' = (b, a)^p \prod u_i^{pf_i} u_p' \qquad (\text{mod } F_{p+2}).$$

Similarly

(58) $$v_p'' = (b, a)^p \prod u_i^{pg_i} u_p'' \qquad (\text{mod } F_{p+2})$$

where g_i are positive integers. Using (57) and (58), we can take any $g \in F/F_{p+2}$ and express it either in terms of u_i or v_i. If

$$g = \prod u_i^{ci} = \prod v_i^{\gamma_i}$$

and the v_i are expressed in terms of the u_i, and terms collected, one obtains

(59) $$\begin{aligned} c_1 &= \gamma_1 \\ c_2 &= \gamma_2 \\ c_3 &= \gamma_3 + p\gamma_p' + p\gamma_p'' \\ c_i &= \gamma_i + ph_i \qquad\qquad h_i \text{ function of the } \gamma_j \\ c_p' &= \gamma_p' \\ c_p'' &= \gamma_p'' \end{aligned}$$

https://doi.org/10.4153/CJM-1961-045-2 Published online by Cambridge University Press

where γ_p', γ_p'' are exponents associated with v_p' and v_p'' respectively. In order to compute the h_i, Lemma 4 and (4) must be extensively used. Equations similar to (59) can be formed for d_i and δ_i, e_i and ϵ_i where

$$h = \prod u_i^{d_i} = \prod v_i^{\delta_i} \quad \text{and} \quad g\cdot h = \prod u_i^{e_i} = \prod v_i^{\epsilon_i}.$$

We now compute ϵ_i in terms of γ_i and δ_i. Obviously

$$\begin{aligned}\epsilon_1 &= \gamma_1 + \delta_1 \\ \epsilon_2 &= \gamma_2 + \delta_2.\end{aligned} \tag{60}$$

To find ϵ_3, we first use (59)

$$e_3 = \epsilon_3 + p\epsilon_p' + p\epsilon_p''$$

or

$$\epsilon_3 = e_3 - p\epsilon_p' - p\epsilon_p''.$$

Using (55) and (59)

$$\epsilon_3 = c_3 + d_3 + c_2 d_1 - pe_p' - pe_p'',$$

Using (53) and (54)

$$\epsilon_3 = c_3 + d_3 + c_2 d_1 - p\Big\{c_p' + d_p' + \sum_{t=1}^{p-1} c_t'\binom{d_1}{p-t} + c_2\binom{d_1}{p}$$
$$+ c_p'' + d_p'' + \sum_{t=1}^{p-1}\Big[c_t'' + d_1\binom{c_1}{t}\Big]\binom{d_2}{p-t} + d_1\binom{c_2}{p}\Big\}.$$

Using (59) again, and collecting terms

$$\epsilon_3 = \gamma_3 + \delta_3 + \gamma_2\delta_1 - p\gamma_2\binom{\delta_1}{p} - p\delta_1\binom{\gamma_2}{p} \tag{61}$$
$$+ p\Big\{\sum_{t=1}^{p-1}(\gamma_i' + ph_i)\binom{\delta_1}{p-t} + \sum_{t=1}^{p-1}\Big[\gamma_i'' + ph_i + \delta_1\binom{\gamma_1}{t}\Big]\binom{\delta_2}{p-t}\Big\}$$

A similar computation gives (using (52), (53), (54))

$$\epsilon_i = \gamma_i + \delta_i + \sum n_k\binom{\gamma_{i_1} + ph_i}{\alpha_1}\dots\binom{\delta_{j_s} + ph_j}{\beta_s} - ph_i(\gamma_j, \delta_k) \tag{62}$$

$$\alpha_i, \beta_j < p$$

$$\epsilon_p' = \gamma_p' + \delta_p' + \sum\,[\gamma_t' + ph_t]\binom{\delta_1}{p-t} + \gamma_2\binom{\delta_1}{p} \tag{63}$$

$$\epsilon_p'' = \gamma_p'' + \delta_p'' + \sum\Big[\gamma_t'' + ph_t + \delta_1\binom{\gamma_1}{t}\Big]\binom{\delta_2}{p-t} + \delta_1\binom{\gamma_2}{p}. \tag{64}$$

Equations (60) through (64) are analogous to (29). We now assume that

$$a^{p^\alpha} = b^{p^\beta} = 1 \qquad \alpha \leqslant \beta,$$

and we investigate (60) through (64) with γ_i, δ_i, ϵ_i considered as integers modulo powers of p. The proof of Lemma 1 in § 1 of **(18)** shows that

$$(65) \qquad v_i^{p^\alpha} = 1$$

except if $v_i = b$, (b, a), v_p' or v_p''. Similarly

$$(66) \qquad u_i^{p^\alpha} = 1$$

except if $u_i = b$ or (b, a).

In (31), put $s = 1$, $r = p^\alpha$. This gives

$$(67) \qquad 1 = (b, a^{p^\alpha}) = (b, a)^{p^\alpha} \prod u_k^{p^\alpha} u_p'^{\binom{p^\alpha}{p}} = (b, a)^{p^\alpha} u_p'^{p^{\alpha-1}}$$

where Lemma 7 (that is (36)) has been used with $A = 0$. Similarly

$$(68) \qquad 1 = (b, a^{p^{\alpha+1}}) = (b, a)^{p^{\alpha+1}} u_p'^{p^\alpha} = (b, a)^{p^{\alpha+1}}.$$

Hence, u_3 (or v_3) has order at most $p^{\alpha+1}$. Now using (57), (4), and (67),

$$v_p'^{p^{\alpha-1}} = (b, a^p)^{p^{\alpha-1}} = [(b, a)^p \prod u_i^{pf_i} u_p']^{p^{\alpha-1}} = (b, a)^{p^\alpha} u_p'^{p^{\alpha-1}} = 1.$$

If $\alpha = \beta$, then

$$v_p''^{p^{\alpha-1}} = 1$$

otherwise (that is, $\alpha < \beta$)

$$v_p''^{p^\alpha} = 1.$$

We now show that (60) through (64) are unambiguous if

$$(69) \qquad \begin{array}{l} \gamma_1, \delta_1, \epsilon_1 \text{ are integers modulo } p^\alpha \\ \gamma_2, \delta_2, \epsilon_2 \text{ are integers modulo } p^\beta \\ \gamma_3, \delta_3, \epsilon_3 \text{ are integers modulo } p^{\alpha+1} \\ \gamma_i, \delta_i, \epsilon_i \text{ are integers modulo } p^\alpha \text{ if } i > 3, \text{ except} \\ \gamma_p', \delta_p', \epsilon_p' \text{ are integers modulo } p^{\alpha-1} \\ \gamma_p'', \delta_p'', \epsilon_p'' \text{ are integers modulo } \begin{cases} p^{\alpha-1} & \text{if } \alpha = \beta \\ p^\alpha & \text{if } \alpha < \beta \end{cases}. \end{array}$$

(60) is obviously unambiguous. As for (61), consider its three parts

$$\begin{aligned} E &= \gamma_3 + \delta_3 \\ F &= \gamma_2\delta_1 - p\gamma_2\binom{\delta_1}{p} - p\binom{\gamma_2}{p}\delta_1 \\ G &= \epsilon_3 - E - F \end{aligned}$$

E gives no trouble. F is taken care of by Lemma 8. G will cause no difficulties because it has a factor of p. γ_p' or δ_p' (modulo $p^{\alpha-1}$) if they appear at all in G are in the h_i which are multiplied by p^2, and hence G is unambiguous modulo $p^{\alpha+1}$. For reasons similar to G (62) causes no trouble. The factor $\binom{\delta_1}{p}$ in

https://doi.org/10.4153/CJM-1961-045-2 Published online by Cambridge University Press

(63) is covered by Lemma 7. If $\alpha = \beta$, the factor $\binom{\gamma_2}{p}$ is covered by Lemma 7; if $\alpha < \beta$, then γ_2 is an integer modulo p^β and a similar argument applies.

We have now proved the following theorem:

THEOREM 6. *Let $A_1, A_2, \ldots, A_t$ be cyclic groups of order $p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_t}$, respectively, α_i positive integers, p a fixed prime, $\alpha_1 \leqslant \alpha_2 \leqslant \ldots \leqslant \alpha_t$. Let a_i generate A_i. Let $v_1, v_2, \ldots$ be the sequence of standard commutators of non-decreasing weight in the a_i of weight $\leqslant p+1$ (see* **(7)**), *except that*

$$(((a_i, \underbrace{a_j), a_j), \ldots, a_j)}_{p} \quad \textit{and} \quad (((a_i, a_j), \underbrace{a_i), \ldots, a_i)}_{p-1}$$

are replaced by

$$v'_{ij,p} = (a_i, a_j^p) \quad \textit{and} \quad v''_{ij,p} = (a_i^p, a_j)$$

respectively. Let

$$N_i = p^{\alpha_i} \textit{ if } v_i \textit{ is of weight } 1,$$
$$N_i = \gcd(p^{\alpha_j}) \textit{ if } a_j \textit{ appears in } v_i,$$

except that for

$$v_i = v'_{ij,p}, N_i = \gcd(p^{\alpha_i - 1}, p^{\alpha_j - 1})$$

and for

$$v_i = v''_{ij,p}, N_i = \begin{cases} p^{\alpha_i - 1} & \text{if } \alpha_i = \alpha_j \\ \gcd(p^{\alpha_i}, p^{\alpha_j}) & \text{if } \alpha_i \neq \alpha_j. \end{cases}$$

Then every element g, of F/F_{p+2} can be uniquely expressed as

$$\prod v_i^{\gamma_i}$$

where γ_i are integers modulo N_i.

REFERENCES

16. Marshall Hall, *The theory of groups*, Macmillan Co. (New York, 1959).
17. Oystein Ore, *Number theory and its history*, McGraw-Hill Book Co., Inc. (New York, 1948).
18. R. R. Struik, *On nilpotent products of cyclic groups*, Can. J. Math., *12* (1960), 447–462.

University of British Columbia