ANNALS OF MATHEMATICS
Vol. 68, No. 1, July, 1958
Printed in Japan

FREE DIFFERENTIAL CALCULUS, IV. THE QUOTIENT GROUPS OF THE LOWER CENTRAL SERIES

BY K. T. CHEN, R. H. FOX[1] and R. C. LYNDON

(Received September 3, 1957)

The quotient groups $Q_n(G) = G_n/G_{n+1}$ of the lower central series $G=G_1 \supset G_2 \supset G_3 \supset \cdots$ of a finitely generated group G are finitely generated abelian groups. Our object is to develop an algorithm for the calculation of Q_n from any given finite presentation of G. As a preliminary step, the special case of a free group X is considered. It is known [2], [7] that, for a free group X of rank q, the group $Q_n(X)$ is a free abelian group whose rank is the Witt number $\psi_n(q)$, and a basis for $Q_n(X)$ has been exhibited by M. Hall [42]. Our approach is somewhat different in that we construct, by means of the free differential calculus, a basis for the dual group $Q_n^* = \text{Hom}\,[Q_n, J]$. The corresponding dual basis of Q_n is not the same as the Hall basis, although it bears a superficial resemblance to it.

In the course of this construction we re-prove Witt's result [7] that the elements of X_n are just those for which the non-constant terms of the Magnus expansion are all of degree at least n, in short, that the lower central groups coincide with the "dimension groups" of Magnus [2]. Further, we derive a complete set of finite identities for the coefficients in the Magnus expansion of an element of X. The algorithm for $Q_n(G)$ is to be found in the last section.

The authors wish to thank Julian Brody for his help in simplifying the arguments, and for selection of the example in §4.

1. Standard sequences

Our considerations are based on a given ordered set. The number q of elements in this ordered set may be either finite or infinite, although the algorithm in §4 is not necessarily effective unless q is finite. For simplicity we write $1, 2, \cdots, q$ for the ordered set although in fact it need not be well-ordered. The free semigroup generated by the given ordered set is ordered lexicographically and denoted by $\mathfrak{A}$. Thus each element a of $\mathfrak{A}$ is a sequence of finite positive length $n(a)$. The elements of given length n constitute a subset of $\mathfrak{A}$ denoted by $\mathfrak{A}_n$; the subset $\mathfrak{A}_1$ is identical with the originally given ordered set. For future reference we record

[1] Guggenheim Fellow associated with the University of Utrecht under a Fulbright Grant, 1951–52 when part of this paper was written.

several of the properties of lexicographic order:

(L1) $ab < ac$ if and only if $b < c$.

(L2) If $b < a < bc$ then $a = bd$ where $d < c$.

(L3) If $a < b$ but $n(a) \geqq n(b)$ then $ac < bd$.

A sequence $c = c_1c_2 \cdots c_{n(c)}$ will be called the *result* of an *infiltration* (or *generalized shuffle*) of two sequences $a = a_1a_2 \cdots a_{n(a)}$ and $b = b_1b_2 \cdots b_{n(b)}$ if there are $n(a)$ indices $\alpha(1), \alpha(2), \cdots, \alpha(n(a))$ and $n(b)$ indices $\beta(1), \beta(2), \cdots, \beta(n(b))$ such that

$$\text{(i)} \qquad \begin{cases} 1 \leqq \alpha(1) < \alpha(2) < \cdots < \alpha(n(a)) \leqq n(c) \\ 1 \leqq \beta(1) < \beta(2) < \cdots < \beta(n(b)) \leqq n(c) \end{cases}$$

$$\text{(ii)} \qquad \begin{cases} c_{\alpha(i)} = a_i, \ i = 1, 2, \cdots, n(a) \\ c_{\beta(j)} = b_j, \ j = 1, 2, \cdots, n(b) \end{cases}$$

(iii) each index $k = 1, 2, \cdots, n(c)$ is either an $\alpha(i)$ for some i or a $\beta(j)$ for some j or both.

The *infiltration* itself consists of the two indexings α and β. We shall denote the set of infiltrations of a and b by the symbol $I(a, b)$.

We note thot $n(c) \leqq n(a) + n(b)$ and that c may be the result of several different infiltrations of a and b. For example, the sequence 122343 results from infiltration of the sequences 123 and 1234 in two ways. In counting infiltrations, we count the number of distinct elements of $I(a, b)$; that is, we count the number $\mu(c)$ of distinct indexings α, β that yield the same c.

If $\alpha(i)$ is always distinct from $\beta(j)$ the infiltration will be called a *shuffle*. Thus in a shuffle

(iii′) each index $k = 1, 2, \ldots, n(c)$ is either an $\alpha(i)$ for some i or a $\beta(j)$ for some j but not both.

If c is a shuffle of a and b then, of course, $n(c) = n(a) + n(b)$. General infiltrations will not be used until §3; as there will be no occasion to count shuffles, we shall refer to c as itself a shuffle.

A proper terminal segment of a sequence c will be called an *end* of c. Thus the ends of $c_1c_2 \cdots c_{n(c)}$ are the sequences $c_2c_3 \cdots c_{n(c)}, c_3 \cdots c_{n(c)}, \cdots, c_{n(c)}$.

We define subsets $\mathfrak{A}', \mathfrak{A}'', \mathfrak{A}''', \mathfrak{A}''''$ (which will later be shown to coincide) as follows:

($\mathfrak{A}'$) $c \in \mathfrak{A}'$ if either $c \in \mathfrak{A}_1$ or $c = ab$ where $a \in \mathfrak{A}', b \in \mathfrak{A}'$ and $a < b$.

($\mathfrak{A}''$) $c \in \mathfrak{A}''$ if c is less than each of its ends (i.e., $c < e$ for each end e of c).

($\mathfrak{A}'''$) $c \in \mathfrak{A}'''$ if c is less than each of its (non-trivial) cyclic permutations.

($\mathfrak{A}''''$) $c \in \mathfrak{A}''''$ if, to each factorization $c = ab$, there is at least one shuffle d of a and b that is greater than c.

An element of $\mathfrak{A}''$ will be called a *standard sequence.* A sequence $c = c_1 c_2 \cdots c_{n(c)}$ of length $n(c) \geqq 2$ has at least one standard end, for example $c_{n(c)}$, hence a unique *longest standard end* b and a corresponding *standard factorization* $c=ab$. We denote $\mathfrak{A}_n \cap \mathfrak{A}'$ by $\mathfrak{A}_n'$ etc.

(1.1) LEMMA. *If $b \in \mathfrak{A}''$ and e is an end of ab such that $a < e$ then $ab < e$.*

PROOF. Suppose that some end e of ab were such that $e \leqq ab$. Then, by (L2), $e = ad$ where $d \leqq b$. Since $e = ad$ is an end of ab, d must be an end of b, and therefore b cannot belong to $\mathfrak{A}''$.

(1.2) LEMMA. *If ab is the standard factorization of an element of $\mathfrak{A}''$ then $a \in \mathfrak{A}''$.*

PROOF. We may assume that $n(a) > 1$, since $\mathfrak{A}_1 \subset \mathfrak{A}''$, hence that a has at least one end. Consider any end d of a. Since b is the longest standard end of ab the end db of ab cannot belong to $\mathfrak{A}''$. Therefore there must be an end e of db such that $db \geqq e$. By Lemma 1.1 $d \geqq e$. Since e is also an end of ab and $ab \in \mathfrak{A}''$ we must have $ab < e$. Hence $a < ab < e \leqq d$.

(1.3) LEMMA. *If ab is less than or equal to each of its cyclic permutations then ba is maximal among the shuffles of a and b.*

PROOF. We proceed by induction on the length $n(ab) = n(a) + n(b)$ of ab. The statement is trivially true for $n(ab) = 2$. Suppose, inductively that $n(ab) \geqq 3$. Let $a = a_1 \cdots a_{n(a)}$, $b = b_1 \cdots b_{n(b)}$ and let $c = c_1 \cdots c_{n(c)}$ be any shuffle of a and b such that $c \geqq ba$. Then $n(c) = n(a) + n(b)$ and there are indices $\alpha(1), \cdots, \alpha(n(a))$; $\beta(1), \cdots, \beta(n(b))$ satisfying (i), (ii) and (iii′). We have to show that $c = ba$. It is no loss of generality to assume that the symbol 1 occurs at least once as a c_k. Then, writing 1^2 for 11, 1^3 for 111, etc., we have $a = 1^r\, a_{r+1} \cdots a_{n(a)}$, $b = 1^s\, b_{s+1} \cdots b_{n(b)}$, $c = 1^t\, c_{t+1} \cdots c_{n(c)}$, where $a_{r+1} > 1$, $b_{s+1} > 1$, $c_{t+1} > 1$, and $0 \leqq r \leqq n(a)$, $0 \leqq s \leqq n(b)$, $0 \leqq t \leqq n(c)$.

Since ab is less than or equal to each of its cyclic permutations we must have $a_1 = 1$, hence $r \geqq 1$. On the other hand if $r = n(a)$, that is, if $a = 1^{n(a)}$, the conclusion of the lemma is immediate, so we may assume $r < n(a)$. Then $1^r\, a_{r+1} \cdots b_{n(r)} = ab \leqq ba = 1^s \cdots a_{n(a)}$, and hence $s \leqq r$. If $s = n(b)$, i.e., if $b = 1^{n(b)}$, we would have $1^r a_{r+1} \cdots b_{n(b)} = ab \leqq ba = 1^{r+n(b)}\, a_{r+1} \cdots a_{n(a)}$, which is impossible; hence $s < n(b)$. Since $1^s\, b_{s+1} \cdots a_{n(a)} = ba \leqq c = 1^t\, c_{t+1} \cdots c_{n(c)}$, it follows that $t \leqq s$. We have to consider two cases: $\alpha(1) = 1$ or $\beta(1) = 1$.

CASE I. Suppose $\alpha(1) = 1$. Then $c_1 = a_1$. If $\beta(j) = t + 1$ for some j, hence $b_j = c_{t+1} > 1$, than j would have to be larger than s, so that t would have to be larger than s, because $c_1 \cdots c_t$ would have to include a_1 as well as $b_1 \cdots b_s$. Therefore $\alpha(i) = t + 1$ for some i, hence $a_i = c_{t+1}$. It follows that i must be larger than r, and hence $r \leqq t$ because $c_1 \cdots c_t$ must include $a_1 \cdots a_r$. We now have $r \leqq t \leqq s \leqq r$, hence $r = s = t$. Since by hypothesis $ab \leqq a_{n(a)}\, b_1 \cdots b_{n(b)}\, a_1 \cdots a_{n(a)-1}$ and $ab \leqq b_{n(b)}\, a_1 \cdots a_m\, b_1 \cdots b_{n(b)-1}$, we must have $a_{n(a)} > 1$ and $b_{n(a)} > 1$. Since $r = s \geqq 1$, we have $a_1 = 1$ and $b_1 = 1$.

Now we introduce a new semigroup $\mathfrak{B}$, freely generated by the symbols $2_i, 3_i, \cdots, q_i$ for $i = 0, 1, \cdots, r$. A homomorphism η of $\mathfrak{B}$ into $\mathfrak{A}$ is defined by taking $\eta(k_0) = k$ and, for $i > 0$, $\eta(k_i) = 1^i k$. Evidently η maps $\mathfrak{B}$ isomorphically upon the subset of $\mathfrak{A}$ that consists of those elements whose last letter is not 1 and which contain no block of the form 1^m with $m > r$; for such an element e we write $\bar{e}$ for its inverse image $\eta^{-1}(e)$ in $\mathfrak{B}$. Moreover the induced order on $\mathfrak{B}$ is precisely the lexicographical order determined by the induced order on its generators.

Now if any block $1^i k$ of a or b does not occur consecutively in c, then by moving the i symbols 1 to the right in c until they immediately precede the symbol k we obtain a new shuffle c'' of a and b such that $c'' \geqq c$. Successively modifying c in this way a finite number of times, we arrive at a new shuffle $c' \geqq c$ in which each block $1^i k$ of a or b occurs consecutively. Observe that $\bar{a}$ and $\bar{b}$, and hence $\bar{c}'$, are defined; this follows from the third paragraph of the proof and the assumption that no cyclic permutation of ab is less than ab; moreover $\bar{c}'$ is a shuffle of $\bar{a}$ and $\bar{b}$.

Since $c' \geqq c \geqq ba$, we have $\bar{c}' \geqq \overline{ba}$; since ab is not larger than any of its cyclic permutations, $\overline{ab}$ is not larger than any of its cyclic permutations. Since $\overline{ab}$ is a shorter word than ab, it follows from the inductive hypothesis that $\bar{c}' = \overline{ba}$, hence that $c' = ba$. Therefore $ba \leqq c \leqq c' = ba$, so that $c = ba$ as required.

CASE II. Suppose $\beta(1) = 1$, so that $c_1 = b_1$. In this case $c = ef$ where $b = eb'$ and f is a shuffle of a and b' whose first symbol is a_1. Clearly $c' = fe$ is a shuffle of $a' = ae$ and b'. Since $ef = c \geqq ba = eb'a$, we have $f \geqq b'a$ by (L1). Hence $c' = fe \geqq b'ae = b'a'$ by (L3). Since c' begins with the symbol 1 we have, by Case I, that $fe = c' = b'a' = b'ae$, hence $f = b'a$ and $c = ef = eb'a = ba$. This completes the proof.

(1.4) THEOREM. *The subsets* $\mathfrak{A}'$, $\mathfrak{A}''$, $\mathfrak{A}'''$ and $\mathfrak{A}''''$ *of* $\mathfrak{A}$ *are identical.*

PROOF. Since $\mathfrak{A}_1' = \mathfrak{A}_1'' = \mathfrak{A}_1''' = \mathfrak{A}_1'''' = \mathfrak{A}_1$, we have to prove that $\mathfrak{A}_n' = \mathfrak{A}_n'' = \mathfrak{A}_n''' = \mathfrak{A}''''$ for $n \geqq 2$.

$\mathfrak{A}_n' \subset \mathfrak{A}_n''$: If $c \in \mathfrak{A}_n'$ then $c = ab$ where $a \in \mathfrak{A}_r'$, $b \in \mathfrak{A}_s'$ $r + s = n$, $a < b$. By the induction hypothesis, $a \in \mathfrak{A}_r''$, $b \in \mathfrak{A}_s''$. It must be shown that, given any end e of ab, we have $ab < e$. By Lemma 1.1 it is sufficient to show that $a < e$. An end e of ab is one of three types, either e is an end of b, or $e = b$, or $e = db$ where d is an end of a. If e is an end of b then $b < e$ because $b \in \mathfrak{A}''$, hence $a < b < e$. If $e = b$ then $a < b = e$. If $e = db$ then $a < d$, because $a \in \mathfrak{A}''$, and hence $a < d < db = e$.

$\mathfrak{A}_n'' \subset \mathfrak{A}_n'$: If $c \in \mathfrak{A}_n''$ we consider its standard factorization $c = ab$. By definition $b \in \mathfrak{A}''$, and $a \in \mathfrak{A}''$ by Lemma 1.2. Hence by the induction hypothesis $a \in \mathfrak{A}'$ and $b \in \mathfrak{A}'$. Furthermore, $a < ab < b$ since $ab \in \mathfrak{A}_n''$. Thus $c \in \mathfrak{A}_n'$

$\mathfrak{A}_n'' \subset \mathfrak{A}_n'''$: If $c \in \mathfrak{A}_n''$ and c' is a cyclic permutation of c then $c = ab$ and $c' = ba$. Since $c \in \mathfrak{A}_n''$ we have $c < b < ba = c'$.

$\mathfrak{A}_n''' \subset \mathfrak{A}_n''$: If $c \in \mathfrak{A}_n'''$ and b is any end of c, so that $c = ab$ then $c < ba$. Suppose $b \leqq c$. Since $c \neq b$ we must have $b < c$. By L2 we have $c = bd$ where $d < a$. Since $c \in \mathfrak{A}_n'''$ we have $c < db$, hence $d < a < ab < db$. By L2 again, $a = de$ where $e < b$. Hence $ba = bde = ce = abe$, which is impossible because ba is necessarily shorter than abe.

$\mathfrak{A}_n''' \subset \mathfrak{A}_n''''$: If $c \in \mathfrak{A}_n'''$ and $c = ab$, then $c = ba$. Since ba is a shuffle of a and b it follows that $c \in \mathfrak{A}_n''''$.

$\mathfrak{A}_n'''' \subset \mathfrak{A}_n'''$: If $c \in \mathfrak{A}_n''''$ and c' is any cyclic permutation of c then $c = ba$ and $c' = ab$. Since $c \in \mathfrak{A}_n''''$, ba cannot be maximal among the shuffles of a and b. Hence by Lemma 1.3, c' must be larger than at least one of its cyclic permutations. Since no proper cyclic permutation c' of c can be minimal among all the cyclic permutations of c, it follows that c itself must be minimal, and hence $c \in \mathfrak{A}_n'''$.

(1.5) THEOREM [7]. *The number of standard sequences of length n on $q < \infty$ letters is*

$$\psi_q(n) = \frac{1}{n}\sum_{d|n} \mu(n/d)q^d$$

where μ denotes the Möbius function.

PROOF. Let us call an element of $\mathfrak{A}$ *acyclic* if it is not equal to any of its cyclic permutations. Writing a^2 for aa, a^3 for aaa, etc., we see that each element c of $\mathfrak{A}_n$ can be written uniquely in the form $c = a^{n/d}$, where d is a divisor of n and a is an acyclic element of $\mathfrak{A}_d$. Thus $q^n = \sum_{d|n}\theta_q(d)$, where $\theta_q(d)$ denotes the number of acyclic elements of $\mathfrak{A}_d$.

Clearly an element of $\mathfrak{A}_d'''$ is acyclic, and each of its acyclic permutations must also be acyclic. Under acyclic permutation the acyclic elements of $\mathfrak{A}_d$ fall into sets of d elements each, and each such set contains exactly one element from $\mathfrak{A}_d'''$. Hence, if $\psi_q(d)$ is the number of elements in $\mathfrak{A}_d'''$, then $\theta_q(d) = d \cdot \psi_q(d)$.

From the resulting relation

$$q^n = \sum_{d \mid n} d\psi_q(d)$$

the required result follows by an application of the Möbius inversion formula.

We conclude this section with a lemma which will be required in §2.

(1.6) LEMMA. *Let $c = ab$ be a standard factorization and let d be any standard sequence such that $d \leqq b$. Then cd is a standard factorizatian.*

PROOF. Let e be any end of cd that is longer than d. Either $e = fd$ where f is an end of b or $e = bd$ or $e = gbd$ where g is an end of a. If $e = fd$ we have $b < f$, since b is standard, and hence $d \leqq b < f < fd$ so that e is not standard. Similarly if $e = bd$ we have $d \leqq b < bd$ so that again e is not standard. In the case $e = gbd$ we may assume that e is standard and that g is the shortest end of a which is such that gbd is standard. Referring to the first two cases, we see that d must be the longest standard end of gbd. By Lemma 1.2 it follows that gb must be standard. But this contradicts the assumption that b is the longest standard end of ab. Thus we have proved that d is the longest standard end of cd.

2. Standard commutators

We consider the free group X generated by symbols $x_1, \cdots, x_q$, and the abelian groups $Q_n = X_n/X_{n+1}$, $n = 1, 2, \cdots$. The object of this section is to show that Q_n is generated by certain "standard commutators"; in the next section it will be shown that Q_n is a free abelian group and the standard commutators constitute a basis of it.

By a *monomial of weight* 1 we mean an element of $\mathfrak{A}_1$. For $n > 1$ a *monomial of weight* n is a symbol (a, b) where a is a monomial of weight r and b is a monomial of weight s, $r + s = n$ and, in case $r = s$, $a \neq b$. We denote by $\mathfrak{M}_n$ the collection of monomials of weight n, and by Y_n the free group generated by this collection $\mathfrak{M}_n$. A homomorphism λ_n of Y_n into X_n is defined inductively by

$$k^{\lambda_1} = x_k, \qquad k \in \mathfrak{M}_1 = \mathfrak{A}_1,$$

$$(a, b)^{\lambda_n} = [a^{\lambda_r}, b^{\lambda_s}], \quad a \in \mathfrak{M}_r, b \in \mathfrak{M}_s, r + s = n.$$

Since $[\prod_i u_i^{\varepsilon_i}, \prod_j v_j^{\eta_j}] \equiv \prod_{i,j}[u_i, v_j]^{\varepsilon_i\eta_j} \pmod{X_{n+1}}$, where $u_i \in X_r$, $v_j \in X_s$, $r+s=n$, $\varepsilon_i = \pm 1$, $\eta_j = \pm 1$, and $[u, u] = [u, 1] = [1, u] = 1$, it is easily shown that Q_n is generated by the cosets $u^{\lambda_n}X_{n+1}$, $u \in \mathfrak{M}_n$.

We denote by S_n the consequence in y_n of the following elements:

(S1) $(a, b)(b, a)$, $\quad a \in \mathfrak{M}_r,\ b \in \mathfrak{M}_s,\ a \neq b,\ r+s=n \geqq 2$,

(S2°) $((a, (a, b)), b)((b, (b, a)), a)$, $\quad a \in \mathfrak{M}_r,\ b \in \mathfrak{M}_s,\ a \neq b,\ 2r+2s=n \geqq 4$,

(S2) $((a, b), c)((b, c), a)((c, a), b)$, $\quad a \in \mathfrak{M}_r,\ b \in \mathfrak{M}_s,\ c \in \mathfrak{M}_t$, $c \neq a, b, (a, b), (b, a), a \neq b, c, (b, c), (c, b)$, $b \neq c, a, (c, a), (a, c)$ $r+s+t=n \geqq 3$,

(S3) $\prod_{j \mid b_j \neq a}(a, b_j)^{\varepsilon_j}$, $\quad a \in \mathfrak{M}_r,\ b_j \in \mathfrak{M}_s,\ r+s=n \geqq 2,\ \varepsilon_j = \pm 1$, whenever $\prod_j b_j^{\varepsilon_j} \in S_s$.

It is easily checked that $S_n^{\lambda_n} \subset X_{n+1}$; hence that λ_n induces a homomorphism $\bar{\lambda}_n$ of Y_n/S_n upon $X_n/X_{n+1} = Q_n$.

To each monomial $a \in \mathfrak{M}_n$ we associate a sequence $|a| \in \mathfrak{A}_n$ as follows;

$$|k| = k \qquad \text{for } k \in \mathfrak{M}_1 = \mathfrak{A}_1$$

$$|(a, b)| = |a||b| \quad \text{for } a \in \mathfrak{M}_r,\ b \in \mathfrak{M}_s,\ r+s=n \geqq 2.$$

Conversely to each sequence $a \in \mathfrak{A}'_n$ we associate a monomial $a^\times \in \mathfrak{M}_n$ as follows:

$$k^\times = k \qquad \text{for } k \in \mathfrak{A}'_1 = \mathfrak{M}_1$$

$$c^\times = (a^\times, b^\times) \quad \text{for } a \in \mathfrak{A}'_r,\ b \in \mathfrak{A}'_s,\ c \in \mathfrak{A}'_n,\ r+s=n \geqq 2$$

where ab is the standard factorization of c. It should be observed that, for any $a \in \mathfrak{A}'_n$,

$$|a^\times| = a\ ,$$

but that for $a \in \mathfrak{M}_n$, $|a|^\times$ is not generally defined and when defined is not generally the same as a. For example $|((1, 2), 3)|^\times = (123)^\times = (1, (2, 3))$. Those monomials $a \in \mathfrak{M}_n$ for which $|a|^\times = a$ will be called *standard monomials*[2], and the collection of standard monomials of weight n will be denoted by $\mathfrak{M}'_n$. Obviously $\mathfrak{M}'_1 = \mathfrak{M}_1$, and $\mathfrak{M}'_n \subset \mathfrak{M}_n$ for $n = 2, 3, \cdots$. If $a \in \mathfrak{M}'_n$ then $|a| \in \mathfrak{A}'_n$. The λ_n-image of a standard monomial of weight n will be called a *standard commutator*[2] of weight n. Thus the object of this section has been reduced to that of showing that Y_n/S_n is generated by the cosets uS_n, $u \in \mathfrak{M}'_n$.

(2.1) THEOREM. *If $d \in \mathfrak{M}'_u$ and $c \in \mathfrak{M}'_t$, $u+t=n \geqq 2$, and $(d, c) \notin S_n$,*

[2] This terminology differs from that in [42].

then there exist sequences c_i and d_i such that

$$(d, c) \equiv \prod_{i=1}^{l} (d_i, c_i)^{\varepsilon_i} \pmod{S_n} ,$$

where $(d_i, c_i) \in \mathfrak{M}'_n$, $\varepsilon_i = \pm 1$, $l \geqq 1$ and, for each i, either $|d_i||c_i| > |d||c|$ or $|d_i||c_i| = |d||c|$ and $|d_i| \leqq |d|$.

PROOF. Because of (S1) we may assume that $|d| \leqq |c|$. Since $d \in \mathfrak{M}'_u$ and $c \in \mathfrak{M}'_t$, $|d| = |c|$ would imply that $d = |d|^\times = |c|^\times = c$, which is impossible. Thus we may assume that $|d| < |c|$. We shall prove the theorem by triple induction, firstly on $n = 2, 3, \cdots$, secondly on $|(d, c)|$, and thirdly on $|d|$. To start the induction we note that the conclusion is trivially true for $n = 2$. To prove the inductive step we assume that the theorem holds for all $(\bar{d}, \bar{c})$, $\bar{d} \in \mathfrak{M}'_{\bar{u}}$, $\bar{c} \in \mathfrak{M}'_{\bar{t}}$, $\bar{u} + \bar{t} = \bar{n}$, $(\bar{d}, \bar{c}) \notin S_{\bar{n}}$ whenever either $\bar{n} < n$, or $\bar{n} = n$ and $|(\bar{d}, \bar{c})| > |(d, c)|$, or $\bar{n} = n$, $|(\bar{d}, \bar{c})| = |(d, c)|$ and $|\bar{d}| < |d|$.

CASE A. If $u = 1$ then $|c|$ is necessarily the longest standard end of $|d|\,|c|$. Hence $|(d, c)|^\times = (|d|\,|c|)^\times = (d, c)$, so that $(d, c) \in \mathfrak{M}'_n$. The conclusion holds with $l = 1$

CASE B. If $u > 1$ then $d = (a, b)$ where $a \in \mathfrak{M}'_r$, $b \in \mathfrak{M}'_s$, $r + s + t = n \geqq 3$, $|a| < |b|$. We have three subcases.

SUBCASE BA. If $|c| \leqq |b|$ then, since $|a|\,|b|$ is a standard factorization, $|c|$ is a standard sequence and $|c| \leqq |b|$ it follows by Lemma 1.6 that $|d|\,|c|$ is a standard factorization, and hence that $(d, c) \in \mathfrak{M}'_n$. Again the conclusion holds with $l = 1$.

SUBCASE BB. If $|b| < |c|$ and $(a, c) = b$ we write, using (S2°), $((a, b), c) = ((a, (a, c)), c) \equiv (a, ((a, c), c)) = (a, (b, c)) \pmod{S_n}$. Since $s + t < n$ it follows from the inductive hypothesis that

$$(b, c) \equiv \prod_j (b_j, c_j)^{\pm 1} \pmod{S_{s+t}} ,$$

where $(b_j, c_j) \in \mathfrak{M}'_{s+t}$ and, for each j, either $|b_j|\,|c_j| > |b|\,|c|$ or $|b_j|\,|c_j| = |b|\,|c|$ and $|b_j| \leqq |b|$. Consequently, by (S3),

$$(a, (b, c)) \equiv \prod_j (a, (b_j, c_j))^{\pm 1} \pmod{S_n} ,$$

the product extended over those indices j for which $(b_j, c_j) \neq a$. But for each j, $a \in \mathfrak{M}'_r$, $(b_j, c_j) \in \mathfrak{M}'_{s+t}$, and either

$$|(a, (b_j, c_j))| = |a|\,|b_j|\,|c_j| > |a|\,|b|\,|c| = |((a, b), c)|$$

or

$$|(a, (b_j, c_j))| = |a|\,|b_j|\,|c_j| = |a|\,|b|\,|c| = |((a, b), c)|$$

and $$|(a, b)| = |a|\,|b| > |a|$$

Therefore, by the inductive hypothesis,

$$(a, (b_j, c_j)) \equiv \prod_k (a_{jk}, e_{jk})^{\pm 1} \pmod{S_n} ,$$

where $(a_{jk}, e_{jk}) \in \mathfrak{M}'_n$ and, for each k, either $|a_{jk}|\,|e_{jk}| > |a|\,|(b_j, c_j)|$ or $|a_{jk}|\,|e_{jk}| = |a|\,|(b_j, c_j)|$ and $|a_{jk}| \leqq |a|$. Hence

$$(a, (b, c)) \equiv \prod_{j,k} (a_{jk}, e_{jk})^{\pm 1} \pmod{S_n} ,$$

where $|a_{jk}|\,|e_{jk}| \geqq |(a, (b, c))|$, and $|a_{jk}| \leqq |a|$ if equality holds. Thus the conclusion holds in this subcase.

SUBCASE BC. If $|b| < |c|$ and $(a, c) \neq b$ we use (S2) to write

$$((a, b), c) \equiv (a, (b, c))((a, c), b)) \pmod{\mathrm{S}_n} .$$

The term $(a, (b, c))$ is dealt with as in the preceding subcase.

For the term $((a, c), b)$ we have a similar argument. Since $r + t < n$ it follows from the inductive hypothesis that

$$(a, c) \equiv \prod_i (a_i, c_i)^{\pm 1} \pmod{S_{r+t}} ,$$

where $(a_i, c_i) \in \mathfrak{M}'_{r+t}$ and, for each i, either $|a_i|\,|c_i| > |a|\,|c|$ or $|a_i|\,|c_i| = |a|\,|c|$ and $|a_i| \leqq |a|$. Consequently, by (S3),

$$((a, c), b) = \prod_i ((a_i, c_i), b)^{\pm 1} \pmod{S_n} ,$$

the product extended over those indices i for which $(a_i, c_i) \neq b$. But, for each i, $(a_i, c_i) \in \mathfrak{M}'_{r+t}$, $b \in \mathfrak{M}'_s$, and

$$|(b, (a_i, c_i))| = |b|\,|a_i|\,|c_i| \geqq |b|\,|a|\,|c| > |a|\,|b|\,|c| = |((a, b), c)| ,$$

because $|a|\,|b| \in \mathfrak{A}'''_u$. Therefore, by the inductive hypothesis,

$$(b, (a_i, c_i)) \equiv \prod_h (b_{ih}, f_{ih})^{\pm 1} \pmod{S_n} ,$$

where $(b_{ih}, f_{ih}) \in \mathfrak{M}'_n$ and, for each h,

$$|b_{ih}|\,|f_{ih}| \geqq |b|\,|(a_i, c_i)| > |((a, b), c))| .$$

Thus

$$((a, c), b)) \equiv \prod_{i,h} (b_{ih}, f_{ih})^{\pm 1} \pmod{S_n} ,$$

and the conclusion is seen to hold in this case also. This completes the proof.

(2.2) COROLLARY. *For each* $n \geqq 1$, *the group* Y_n/S_n *is generated by the cosets* uS_n, $u \in \mathfrak{M}'_n$.

(2.3) COROLLARY. *For each* $n > 1$, *the group* Q_n *is generated by the cosets that contain the standard commutators of weight* n.

3. Bases for Q_n and Q_n^*

For any element w of X and any element $a = a_1 a_2 \cdots a_n$ of $\mathfrak{A}$ we denote

$(\partial^n w/\partial x_{a_1}\partial x_{a_2}\cdots\partial x_{a_n})^0$ by $D_a^0 w$, or, more simply, by w_a^0. Since [FDC I, (3.2)]

$$(uv)_a^0 = u^0_{a_1\cdots a_n} + u^0_{a_1\cdots a_{n-1}}v^0_{a_n} + \cdots + u^0_{a_1}v^0_{a_2\cdots a_n} + v^0_{a_1\cdots a_n} ,$$

we conclude easily, by induction on $n = n(a)$, that

(3.1) $w_a^0 = 0$ if $w \in X_{n+1}$;

(3.2) $(uv)_a^0 = u_a^0 + v_a^0$ if $u, v \in X_n$; and hence that

(3.3) $[u, v]_a^0 = u^0_{a_1\cdots a_r}v^0_{a_{r+1}\cdots a_n} - v^0_{a_1\cdots a_s}u^0_{a_{s+1}\cdots a_n}$ if $u \in X_r$, $v \in X_s$ and $r + s = n$.

(To prove (3.3), write $w = [u, v]$ and apply (3.1) and (3.2) to the identity $(wvu)_a^0 = (uv)_a^0$.)

The operators D_a^0: $JX \to J$ are added and multiplied according to the following definitions :

$$(D_a^0 + D_b^0)w = D_a^0 w + D_b^0 w$$
$$(kD_a^0)w = k(D_a^0 w)$$
$$(D_a^0 \cdot D_b^0)w = (D_a^0 w)(D_b^0 w)$$

For each pair of sequences, $a, b \in \mathfrak{A}$, we define the operator

$$E_{a,b} = D_a^0 \cdot D_b^0 - \textstyle\sum_{I(a,b)} D_c^0 = D_a^0 \cdot D_b^0 - \sum_c \mu(c) D_c^0 ,$$

where $\mu(c)$ is the number defined in §1, the summations extended over the infiltrations of a and b and over the result c of infiltrating a and b.

(3.3) LEMMA. *For every $w \in X$ and every $a, b \in \mathfrak{A}$, we have*

$$E_{a,b}w = 0 .$$

EXAMPLES.

$$(w_1^0)^2 = 2w_{11}^0 + w_1^0 \qquad \text{[FDC I (3.9), } n = 2]$$
$$w_1^0 w_2^0 = w_{12}^0 + w_{21}^0 \qquad \text{[FDC I (3.10)]}$$
$$w_1^0 w_{11}^0 = 3w_{111}^0 + 2w_{11}^0 \qquad \text{cf. [FDC I (3.9), } n = 3] .$$

PROOF. We proceed, by induction on the length of the word w, to prove that $w_a^0 w_b^0 = \sum_{I(a,b)} w_c^0$.

Consider first the case $w = x_j$. The left-hand side is equal to zero unless $a = j$ and $b = j$, and the same is true of the right-hand side. If $a = j$ and $b = j$ we have $(x_j)_j^0(x_j)_j^0 = 2(x_j)_{jj}^0 + (x_j)_j^0$ or $1 \cdot 1 = 2 \cdot 0 + 1$.

Next we consider the case $w = x_j^{-1}$. Both sides are equal to zero unless $a = j^r$, $b = j^s$. The left hand side is then equal to $(x_j^{-1})^0_{j^r}(x_j^{-1})^0_{j^s} = (-1)^{r+s}$. Denote by $(r, s)_\tau = (s, r)_\tau$ the number of infiltrations of j^r and j^s that yield j^τ. We have to prove that

$$(*_{r,s}) \qquad \sum_{\tau=\max(r,s)}^{r+s} (-1)^\tau (r,s)_\tau = (-1)^{r+s} .$$

we prove this by induction on s. We have $(r,1)_r = r$ and $(r,1)_{r+1} = r+1$, hence $(-1)^r r + (-1)^{r+1}(r+1) = (-1)^{r+1}$, so that $(*_{r,1})$ is true. For the inductive step we assume $s > 1$ and the truth of $(*_{r,s})$ for any r. Since $I(j^r, I(j, j^s)) = I(I(j^r, j), j^s)$, we have

$$\begin{aligned} s(-1)^{r+s} &+ (s+1)\sum_{\tau=\max(r,s+1)}^{r+s+1}(-1)^\tau(r, s+1)_\tau \\ &= \sum_{\sigma=s}^{s+1}\sum_{\tau=\max(r,\sigma)}^{r+\sigma}(-1)^\tau(r,\sigma)_\tau(1,s)_\sigma \\ &= \sum_{\rho=r}^{r+1}\sum_{\tau=\max(\rho,s)}^{\rho+s}(-1)^\tau(r,1)_\rho(\rho,s)_\tau \\ &= \sum_{\rho=r}^{r+1}(-1)^{\rho+s}(r,1)_\rho \text{ by inductive hypothesis} \\ &= (-1)^{r+s+1} \text{ by inductive hypothesis} \end{aligned}$$

Hence

$$\begin{aligned} \sum_{\tau=\max(r,s+1)}^{r+s+1}(-1)^\tau(r,s+1)_\tau &= \frac{1}{s+1}((-1)^{r+s+1} - s(-1)^{r+s}) \\ &= (-1)^{r+s+1} \end{aligned}$$

completing the induction. This completes the proof for words of length 1.

If w is of length greater than 1 then $w = uv$. Suppose, inductively that $u_a^0 u_b^0 = \sum u_c^0$ and $v_a^0 v_b^0 = \sum v_c^0$. Then

$$\begin{aligned} w_a^0 w_b^0 &= \left(\sum_{r=0}^{n(a)} u^0_{a_1\cdots a_r} v^0_{a_{r+1}\cdots a_{n(a)}}\right)\left(\sum_{s=0}^{n(b)} u^0_{b_1\cdots b_s} v^0_{b_{s+1}\cdots b_{n(b)}}\right) \\ &= \sum_{r,s} u^0_{a_1\cdots a_r} u^0_{b_1\cdots b_s} v^0_{a_{r+1}\cdots a_{n(a)}} v^0_{b_{s+1}\cdots b_{n(b)}} \\ &= \sum_{r,s}\sum u^0_{c(a_1\cdots a_r,\, b_1\cdots b_s)} v^0_{c(a_{r+1}\cdots a_{n(a)},\, b_{s+1}\cdots b_{n(b)})} \end{aligned}$$

where $\sum$ ranges over the infiltrations of $a_1\cdots a_r$ and $b_1\cdots b_s$, and over the infiltrations of $a_{r+1}\cdots a_{n(a)}$ and $b_{s+1}\cdots b_{n(b)}$,

$$= \sum_c \mu(c) \sum_{t=0}^{n(c)} u^0_{c_1\cdots c_t} v^0_{c_{t+1}\cdots c_{n(c)}}) ,$$

where $c = c_1\cdots c_{n(c)}$ ranges over the result of the infiltrations of a and b. Note that at the extremes $r = 0$, $r = n(a)$, $s = 0$, $s = n(b)$, $t = 0$, $t = n(c)$ we have derivatives of zero order $u^0, v^0, u^0, v^0, u^0, v^0$; we use the natural convention that the only infiltration of a sequence a with an empty sequence is the sequence a itself;

$$= \sum_c \mu(c) w_c^0 .$$

This completes the induction.

(3.4) LEMMA. *If* $c \in \mathfrak{A}'_n$ *and* w *denotes the standard commutator* $(c^\times)^{\lambda_n}$ *then* (i) $w^0_e = 0$ *for every* $e \in \mathfrak{A}_n$ *such that* $e < c$, *and* (ii) $w^0_c = 1$.

PROOF. We proceed by induction on $n = n(c)$, the case $n = 1$ being trivial. If $n > 1$, then $w = [u, v]$ where $u = (a^\times)^{\lambda_n}$ and $v = (b^\times)^{\lambda_n}$, $a \in \mathfrak{A}'_r$, $b \in \mathfrak{A}'_s$, $r + s = n$, and $c = ab$ is the standard factorization. By (3.3)

$$w^0_e = u^0_f v^0_g - v^0_{f'} u^0_{g'} ,$$

where $e = fg = f'g'$, $n(f) = n(g') = n(a)$, $n(g) = n(f') = n(b)$. If we assume that $e \leqq c$, it follows that $f' < f'g' = e \leqq c = ab < b$. By the inductive hypothesis it follows that $v^0_{f'} = 0$, hence $w^0_e = u^0_f v^0_g$.

If $e < c$ either $f < a$ or $f = a$ and $g < b$. In the first case $u^0_f = 0$ by the inductive hypothesis, and in the second $v^0_g = 0$.

If $e = c$ then $f = a$ and $g = b$, whence, by the inductive hypothesis $u^0_f = 1$, $v^0_g = 1$.

(3.5) THEOREM. *The cosets* wX_{n+1} *determined by the standard commutators* w *form a basis for the free abelian group* Q_n. *If* g *is finite, the operators* D^0_c, $c \in \mathfrak{A}'_n$, *form a basis for* Q^*_n, *the additive group of homomorphisms of the multiplicative group* Q_n *into the additive group* J *of the integers.*

PROOF. That the cosets wX_{n+1} generate Q_n was proved in Corollary (2.3). By Lemma (3.4), we can construct linear combinations of the operators D^0_c, $c \in \mathfrak{A}'_n$, assuming arbitrarily prescribed integer values on the standard commutators of weight n. Hence the D^0_c, $c \in \mathfrak{A}'_n$, generate Q^*_n.

Now suppose that $\prod w^{k(w)} \in X_{n+1}$, where $k(w) \in J$ and the product is extended over the standard commutators w of weight n. Among those w for which $k(w) \neq 0$ let w^+ be the one for which $c = |\lambda_n^{-1}(w)|$ is the smallest; let $e^+ = |\lambda_n^{-1}(w^+)|$. Then, by Lemma (3.4), $0 \neq k(w^+) = \sum k(w) w^0_{c^+} = (\prod w^{k(w)})^0_{c^+} = 0$. Hence there can be no w for which $k(w) \neq 0$, that is, $\prod w^{k(w)} = 1$.

If $\sum k(c) D^0_c = 0$, where $k(c) \in J$ and the summation is extended over the standard sequences of length n, we can show in an entirely analogous way that all the coefficients $k(c)$ are equal to 0.

(3.6) COROLLARY (Witt [7]). *An element* w *of* X *lies in* X_n *if and only if* $D^0_c(w) = 0$ *for all* c *of length less than* n.

(3.7) LEMMA. *If* q *is finite, and for each sequence* $e \in \mathfrak{A}'_1 \cup \cdots \cup \mathfrak{A}'_n$. *there is selected an integer* σ_e *then there can be found an element* w *of* X *such that* $w^0_e = \sigma_e$ *for every* $e \in \mathfrak{A}'_1 \cup \cdots \cup \mathfrak{A}'_n$.

PROOF. For $n = 1$ this is trivial; assume inductively that $n > 1$. By the induction hypothesis there is an element u of X such that $u_e^0 = \sigma_e$ for every $e \in \mathfrak{A}_1' \cup \cdots \cup \mathfrak{A}_{n-1}'$. By Theorem 3.5, there is an element v of X_n such that $v_e^0 = \sigma_e - u_e^0$ for every $e \in \mathfrak{A}_n'$. Let $w = uv$. Then, by (3.1), $w_e^0 = \sigma_e$ for every $e \in \mathfrak{A}_1' \cup \cdots \cup \mathfrak{A}_n'$.

(3.8) LEMMA. *Every operator D_c^0, $c \in \mathfrak{A}_1 \cup \cdots \cup \mathfrak{A}_n$ can be expressed as a rational polynomial in the operators $E_{a,b}$, $a \in \mathfrak{A}_r$, $b \in \mathfrak{A}_s$, $r + s \leqq n$, and the operators D_e^0, $e \in \mathfrak{A}_1' \cup \cdots \cup \mathfrak{A}_n'$.*

PROOF. The lemma is trivial for $n = 1$, because $\mathfrak{A}_1 = \mathfrak{A}_1'$, and, of course, for $c \in \mathfrak{A}_1' \cup \cdots \cup \mathfrak{A}_n'$. We proceed by double induction on the length n of c and on the size of c in the ordered set $\mathfrak{A}_n$. Suppose $n > 1$ and $c \notin \mathfrak{A}'$. Since $c \notin \mathfrak{A}' = \mathfrak{A}''''$, there must be a factorization $c = ab$ such that c is not smaller than any shuffle of a and b. Then, for some positive integer k,

$$E_{a,b} = -kD_c^0 + D_a^0 \cdot D_b^0 - \sum_c \mu(c')D_{c'}^0 ,$$

c' ranging over certain sequences $\in \mathfrak{A}_1 \cup \cdots \cup \mathfrak{A}_n$ for which $c' < c$. By the inductive hypothesis it follows that D_c^0 can be expressed as a polynomial of the required type.

In order to discuss the converse of Lemma (3.3), we consider the ring $\mathfrak{P}$ of formal integral power series in the non-commuting variables $x_1-1, \cdots, x_q - 1$. Define the *norm* of a non-trivial power series to be $1/n$ where n is the smallest integer for which there is a term of degree n with non-vanishing coefficient, (and the norm of the trivial power series is defined to be 0). Then, defining the *distance* between two power series to be the norm of their difference, $\mathfrak{P}$ is a metric, and hence a topological, ring. Let us denote by μ the Magnus homomorphism

$$w \to w^0 + \sum_c w_{c_1 \cdots c_n}^0 (x_{c_1} - 1) \cdots (x_{c_n} - 1)$$

of the group ring JX into the ring $\mathfrak{P}$. Lemma (3.3) states that a power series can belong to $\mu(X)$ only if the coefficients satisfy certain identities indicated there. But, it is easy to see that these identities are in fact satisfied by any power series that belongs to the closure of $\mu(X)$ in the topology. Now we shall show that the converse holds.

(3.9) THEOREM. *An integral power series*

$$p(x) = 1 + \sum_c \sigma_{c_1 \cdots c_n} (x_{c_1} - 1) \cdots (x_{c_n} - 1) \in \mathfrak{P}$$

belongs to the closure of $u(X)$ if and only if, for every pair of sequences $a, b \in \mathfrak{A}$,

$$\sigma_a\sigma_b = \sum_c \mu(c)\sigma_c ,$$

c ranging over the results of infiltrating a and b.

PROOF. Given integers σ_c satisfying these identities, we can, by Lemma (3.7) find for each n an element $w = w^{(n)}$ of X such that $w_e^0 = \sigma_e$ for every $e \in \mathfrak{A}_1' \cup \cdots \cup \mathfrak{A}_n'$. We have to show that $w_c^0 = \sigma_c$ for every $c \in \mathfrak{A}_1 \cup \cdots \cup \mathfrak{A}_n$.

This last statement is trivial for $n = 1$, because $\mathfrak{A}_1 = \mathfrak{A}_1'$, and of course, for $c \in \mathfrak{A}_1' \cup \cdots \cup \mathfrak{A}_n'$. We proceed by double induction as in the proof of Lemma (3.8). If $n > 1$ and $c \notin \mathfrak{A}'$ there is a factorization $c = ab$ such that c is not smaller than any shuffle of a and b. Since $kw_c^0 + \cdots = w_a^0 w_b^0 = \sigma_a\sigma_b = k\sigma_c + \cdots$, where $k \geqq 1$, it follows from the inductive hypothesis that $w_c^0 = \sigma_c$.

4. The Âlgorithm

Let $G = \{x_1, \cdots, x_q : r_1, r_2, \cdots\}$ be a finitely generated group and let ϕ denote the canonical homomorphism of $X_1 = X$ upon $G_1 = G$; its kernel is the consequence $R_1 = R$ of the elements $r_1, r_2, \cdots$ in X. Since $\overline{\phi}_n(X_n) = G_n$, $n = 1, 2, \cdots$, there is induced a homomorphism $\overline{\phi}_n$ of $Q_n = X_n/X_{n+1}$ upon G_n/G_{n+1}. The kernel of $\phi_n = \phi \mid X_n$ is $R_n = R \cap X_n$ and the kernel of $\overline{\phi}_n$ is $\overline{R}_n = R_n X_{n+1}/X_{n+1}$.

Let $r_{n1}, r_{n2}, \cdots$ be any set of elements of X such that the consequence in X of $r_{n1}, r_{n2}, \cdots$ and X_{n+1} is R_n. Then R_n is the consequence in X_n of the elements $wr_{ni}w^{-1}$, $w \in X$. But $wr_{ni}w^{-1} \equiv r_{ni} \pmod{X_{n+1}}$. Hence $\overline{R}_n$ is the consequence in Q_n of the cosets $\overline{r}_{ni} = r_{ni}X_{n+1}$. If $\xi_1, \xi_2, \cdots$ is a basis for Q_n then

$$G_n/G_{n+1} = Q_n/\overline{R}_n = \{\xi_1, \xi_2, \cdots : \overline{r}_{n1}, \overline{r}_{n2}, \cdots\} .$$

Hence if $\xi_1^*, \xi_2^*, \cdots$ is a dual basis for Q_n^*, i.e. $\xi_k^*\xi_j = \delta_{jk}$, then a simple calculation shows that $\overline{r}_{ni} = \prod \xi_j^{\xi_j^* \overline{r}_{ni}}$, so that $\| \xi_j^* \overline{r}_{ni} \|$ is a relation matrix for G_n/G_{n+1}.

By Theorem (3.5), the operators D_c^0, $c \in \mathfrak{A}_n'$ form a basis for Q_n^*. Let $\xi_1, \xi_2, \cdots$ be a dual basis for Q_n. (Such a dual basis can be computed by means of Lemma (3.4), but does not seem to have any simple direct description.) Thus $\| D_c^0 r_{ni} \|$ is a relation matrix for G_n/G_{n+1}.

It remains to determine, for each n, a set of elements r_{ni} whose consequence in X is R_n. For $n = 1$, such a set is obviously $r_1, r_2, \cdots$. Assume inductively that such a set has been determined for $n \geqq 1$. The row space of the matrix $||D_c^0 r_{ni}||$ is generated by some linearly independent set of vectors $\{D_c^0 s_k\} k = 1, 2, \cdots, l_n$. Hence every r_{ni} is congruent modulo X_{n+1} to $\prod_k s_k^{\beta_{ik}}$, $\beta_{ik} \in J$. Thus the elements s_k, $r_{ni} \cdot (\prod_k s_k^{\beta_{ik}})^{-1}$ have the same consequence R_n as the r_n. Therefore [19, Lemma A5] R_{n+1} is the consequence in X of the elements $[s_k, x_j]$, $k = 1, \cdots, l_n, j = 1, \cdots, q$ an the elements $r_{ni} \cdot (\prod_k s_k^{\beta_{ik}})^{-1}$

We illustrate the algorithm with an example.

EXAMPLE[3]. $G = \{x, y : r_1 = [[x, y], y], r_2 = [x, [x, [x, y]]]^n\}$. We have $r_1 \in X_3$, $r_2 \in X_4$. $G_1/G_2 \approx X_1/X_2$ is free abelian of rank 2, $G_2/G_3 \approx X_2/X_3$ is free cyclic. For G_3/G_4 we have the relation matric

	D^0_{xxy}	D^0_{xyy}
r_1	0	1
r_2	0	0

Hence G_3/G_4 is free cyclic. For G_4/G_5 we have the relation matrix

	D^0_{xxxy}	D^0_{xxyy}	D^0_{xyyy}
$[r_1, x]$	0	-1	0
$[r_1, y]$	0	0	1
r_2	n	0	0

Thus G_4/G_5 is cyclic of order n. Similarly, G_5/G_6 and G_6/G_7 are also cyclic of order n.

UNIVERSITY OF HONG KONG
UNIVERSITY OF MICHIGAN
PRINCETON UNIVERSITY

BIBLIOGRAPHY
(continued from FDC III)

FDC I, II, III. R. H. FOX, *Free differential calculus* [I], Ann. of Math. 57 (1953), 547–560; [II] ibid. 59 (1954), 196–210; III ibid. 64 (1956), 407–419.

42. M. HALL, *A basis for free Lie rings and higher commutators in free groups*, Proc. Am. Math. Soc. 1 (1950), 575–581.

43 R. C. LYNDON, *On Burnside's problem*. I, Trans. Amer. Math. Soc. 77 (1954), 202–215; II, ibid. 78 (1955), 329–332.

[3] This algorithm was used in [43] to obtain results on the Burnside problem. It should be noted that what we have denoted by D_c^0 is written there as just D_c, and what we have called *infiltrations* or *generalized shuffles* are called just *shuffles*.