ON FREE GROUPS AND THEIR AUTOMORPHISMS

BY

ELVIRA STRASSER RAPAPORT

Stockbridge, Mass.

1. Introduction

The group A_n of automorphisms of a free group F_n on n free generators has been investigated by J. Nielsen [4]. Nielsen found generators and relations for A_n; it follows from his results that the elementary or t-transformations defined below generate A_n. Also, Nielsen found a recursive method to decide whether a given set of n elements of F_n generates the group. But for $n > 2$ it still remained an unsolved problem to decide whether a given element of F_n could appear in a set of free generators of F_n. This problem was solved by Whitehead [6]; in a subsequent paper, Whitehead [7] proved the following powerful theorem:

Given a set of words $W_0, \ldots, W_k$ in the generators of F_n, if the sum L of the lengths of these words can be diminished by applying automorphisms of F_n to the generators, then it can also be diminished by applying an automorphism of a pre-assigned finite set of automorphisms (the so-called T-transformations defined below).

The group A_n is of importance for Dehn's "isomorphism problem" of group theory (Dehn, [1]). Its most significant application is furnished by Grushko's theorem (see Kurosh [2] and B. H. Neumann [3]) which shows the following: given a minimal set of n generators of a group G which is a free product of a finite number of its subgroups $H_q\,(q = 1, \ldots, r)$. one can apply a transformation A of A_n to the generators a_j of G such that each of the resulting elements $A\,(a_j)$ belong to an H_q. The theorem of Whitehead and the theorem of Grushko have been used by Shenitzer [5] to devise tests for the free decomposability of groups with a single defining relation.

Whitehead uses difficult topological methods in proving his results. In the case where $n = 3$, a purely algebraic derivation of his theorems has been given by the author.(1) The present paper contains an algebraic proof of the full Whitehead theorem and of some extensions and applications.

2. Definitions and notation

G will denote the free group $F_n = F(a_1, \dots, a_n)$ on n generators.

$\overline{W}$ will denote the inverse of the element W of G.

Superscripts e and e' will denote $+1$ or -1.

$a \to ab$ will mean that under the automorphism in question the image of the element a of G is the element ab of G.

A permutation $a_i \to a_k^e$, $(i, k = 1, \dots, n)$ will be denoted by p.

A simple automorphism or t-transformation, t, is an automorphism of G of the form $a_i \to (a_i^e a_j^{e'})^e$, $a_k \to a_k$, $k \neq i$, $i \neq j$, i and j fixed but arbitrary.

A T-transformation is the following automorphism of G: let a, b, c, z denote fixed subsets of the generators of G and let d be a generator or the inverse of a generator, such that the sets a, b, c, d^e are disjoint and the set (a, b, c, z) contains every generator a_i of G just once. Then

$$T \begin{cases} a \to a\,d \\ b \to \bar{d}\,b \\ c \to \bar{d}\,c\,d \\ z \to z \end{cases}$$

is a T-transformation for every such subdivision of the generators.

The product $T_2 T_1$ of two T-transformations, with $T_1(a_i) = v_i(a_1, \dots, a_n) = v_i(a)$, $T_2(a_i) = w_i(a)$, $T_2 T_1(a_i) = v_i(w_1(a), \dots, w_n(a))$, will be given in the form

$$T_2 T_1 \begin{cases} a \to a\,d \\ b \to \bar{d}\,b \\ c \to \bar{d}\,c\,d \\ a' \to a'\,d' \\ b' \to \bar{d}'\,b' \\ c' \to \bar{d}'\,c'\,d' \end{cases}$$

with the appropriate subdivisions $(a, \dots)$ and $(a', \dots)$ of the generators of G, and with the statements $z \to z$, and $z' \to z'$ omitted.

(1) E. S. Rapaport, *On a theorem of J. H. C. Whitehead*, Ph. D. thesis, New York University, 1955 (unpublished), sponsored by Professor Wilhelm Magnus, whose valuable aid in preparing the present paper is gratefully acknowleged.

$L(w)$ will denote the length L of the element $w = w(a_1, \ldots a_n)$ of G, defined as the sum of the absolute values of the exponents of the generators appearing in w. $L(1) = 0$.

$L(w_1, \ldots, w_k)$ equals the sum of the lengths of the elements $w_1, \ldots, w_k$, by definition.

W is minimal t when $L(t(W)) = L(W)$ for every t.

A is a level transformation on w if $L(A(w)) = L(w)$.

A is a level transformation if $L(A(w)) = L(w)$ for all the elements w in G.

$A_1 = A_2$, if the automorphisms A_1 and A_2 of G map the generator a_i on the same element of G for every i.

$A_1 \sim A_2$ is defined in section 6.

The element, or word, w of G modulo inner automorphisms is called the cyclic word w.

The special symbols s, s_i, $z(xy)$, $\mathfrak{z}(xy)$, (xyz) are defined in section 4.1; $A(s)$ $T(s)$ in section 4.2.

An active generator under a T-transformation, T, is a generator of G whose image under T is not of length 1, hence is not that generator itself.

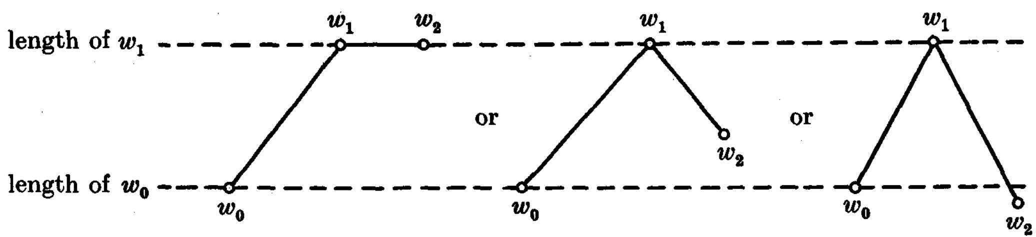
A multiplier under T is the generator by which the active generators or their inverses are multiplied under T.

3. Results

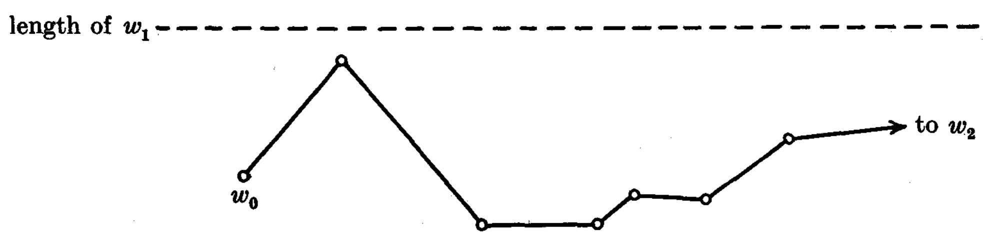
The key result is theorem 1 below, proved in sections 4–9. Section 10 contains some consequences of theorem 1. Section 11 contains some applications of the method of proof used in sections 4–9.

Before stating theorem 1, I shall put it in graphic form for easy survey. Let a line between two points

mean that the words w_1 and w_2 of G are connected by a T-transformation: $w_2 = T(w_1)$, where in the first diagram $L(w_2) = L(w_1)$, while in the second, $L(w_2) > L(w_1)$. Then the theorem asserts that if



then there exists a product $T_k T_{k-1} \ldots T_1 = B$ of T-transformations such that $B(w_0) = w_2$ and the diagram for B (below) never touches the line "length of w_1" except at w_2 in case $L(w_2) = L(w_1)$.



THEOREM 1. *Let* $A = T_2 T_1$, *or* $A = \bar{p} T$, *such that*

$$(1)\ L(T_1 w_0) > L(w_0),$$

$$(2)\ L(A w_0) \leqslant L(T_1 w_0),$$

where w_0 *is a cyclic word in* G. *Then there exists a factorization* $B = B_k \ldots B_1$ *of* A *such that for every intermediate word* $w'_h = B_h \ldots B_1(w_0)$, $h < k$, $L(w'_h) < L(T_1 w_0)$ — *"B is direct" — where the* B_i *are* T*-transformations or level transformations.*

COROLLARY: *If* w_0 *stands for a set of* m *words, the theorem is true.*

To prove theorem 1 a means is found to characterize (generic) words w_0 which satisfy the hypotheses above, in such a way that the properties required by the conclusion of the theorem are seen to be possessed by these words w_0. A properly chosen "syllable representation" of w_0, introduced in the sequel, leads to such a characterization.

4. Syllables and syllable representation

4.1. The word syllable will stand for a string of letters, but never a single letter, and a rule (or restriction) as to what letters may not precede or succeed it. To give a preliminary example, $(xyz)\mathfrak{u}$ designates the string of letters xyz — *but* *not* u *also* — whenever xyz is not followed by u in a given sequence of letters $cab \dots xyz \dots d$; (xyz) designates the string of letters xyz regardless of what follows it. In these examples, the fact that no symbol stands in front of the parentheses means that any symbol is allowed to precede the syllable.

Let $w = xyz$ be a cyclic word in G, so that x is successor to z. Then I shall say that the symbol $(xyz)(zx)$ is a product of the (overlapping) syllables (xyz) and (zx) and represents w. The product $(xy)(yz)(zx)$ also represents w.

The product $s_1 s_2$ of the syllables s_1 and s_2 is defined when s_1 ends with the first symbol in s_2 read from left to right, and multiplication is juxtaposition. (The word represented by $s_1 s_2$ contains this joining symbol of s_1 and s_2 just once.)

A word may have several such representations, but any representation in terms of a given set of syllables must conform to the given restrictions on the elements s_i of the set. If, for example, one has the syllables $s_1 = (xy)\mathfrak{z}$, $s_2 = (xyz)$, $s_3 = (zx)$, and $s_4 = (yz)$, then $w = xyz$ is represented by $s_2 s_3$ but not by $s_1 s_4 s_3$.

The reason for introducing a syllable representation is briefly as follows:

first, it turns out that it is possible to represent the (generic) word w_0 uniquely in terms of a certain set S of syllables in such a way that the change of length of w_0 under given T_1 or $A = T_2 T_1$ equal the sum of the changes of length of the constituent syllables of w_0 — with "change of length of s_i" suitably defined and computable;

secondly, the two hypotheses of the theorem become conditions, in the form of inequalities, on the number of times certain of the syllables must occur in w_0;

finally, these inequalities can be used to find a set of automorphisms containing B of the theorem.

At this point the following, rather trivial, yet necessarily sketchy example can be given. Let a, c, d be fixed generators of G, w_0 an element of G, and $A = T_2 T_1$ the automorphism given by $T_1 : a \to ac$, $T_2 : a \to da$ (all other generators remaining unchanged under A). Then, $A' = T_1 T_2$ clearly equals A. Let

$$s_1 = (a\bar{c})^{\pm 1},\ s_2 = (az)^{\pm 1},\ s_3 = (uv),\ s_4 = (\bar{d}a)^{\pm 1},\ s_5 = (ya)^{\pm 1},$$

where y, u, v, z run through all generators and their inverses except that $s_i \neq s_j$ for $i \neq j$ and that $s_i \neq 1$, every i.

Let N_i be the number of times s_i occurs in w_0, and M_i the number of times s_i occurs in $T_1(w_0) = w_1$, when w_0 and w_1 are reduced (do not contain segments $g\bar{g}$). Suppose that

$$\text{(i)} \quad L(T_1 w_0) - L(w_0) = N_2 - N_1,$$
$$\text{(ii)} \quad L(A w_0) - L(w_1) = -M_4 + M_5.$$

If now the hypotheses (1) and (2) of theorem 1 hold for w_0 and A, then

$$(1) \qquad N_2 - N_1 > 0,$$
$$(2) \quad -M_4 + M_5 \leqslant 0.$$

It can be shown that under (i) and (ii), $N_4 = M_4$, $M_5 = N_5$ and $L(T_2 w_0) - L(w_0) = N_5 - N_4$. But then the last difference is equal or less than 0, so that $T_2(w_0)$ is not longer than w_0; consequently A' is direct, that is, A' is a solution B of the theorem.

4.2. Next, the change of length of a syllable under an automorphism has to be defined. Let s be a syllable, $s = a_1 a_2 \ldots a_j$, where the symbols stand for, not necessarily distinct, generators or their inverses; let s be reduced. Let T be a T-transformation. The image under T of every generator a is of the form $U a V$, reduced. The words U, V may have lengths 0. Then the image of s under T can be written as $U_1 a_1 V_1 U_2 a_2 V_2 \ldots U_j a_j V_j$, unreduced. Define $T(s)$ by

$$T(s) = T(a_1 \ldots a_j) = a_1 V_1 U_2 a_2 V_2 \ldots U_j a_j \ (\mathrm{mod}\ 1) = W_s \ (\mathrm{mod}\ 1), \qquad (^*)$$

so that $T(s)$ is given by the word W_s on the right hand side after it has been reduced. This word is the image of s under T with U_1 and V_j left off. For example, if $s = ab$, $T: b \to bc$, then $T(s) = ab$. If $T(s)$ is a syllable, then $T'(T(s))$ is defined.

Syllables will be used as the building blocks of a cyclic word; in the latter every symbol has predecessors and successors; thus s will have a predecessor in w_0, hence U_1 will have one in $T(w_0)$ unreduced; these predecessors will end respectively with a_1 and $U_1 a_1$. Therefore, U_1 will appear just once in the product of the $T(s_i)$ intended to represent $T(w_0)$. Similarly for V_j. This shows that if w_0 is represented by the product $\prod_{s_i \subset w_0} s_i$ of a subset of a set S of syllables s_i, then, with this definition of $T(s_i)$, the product $\prod_{s \subset w_0} W_s$ is defined and represents a (generally unreduced) form of $T(w_0)$.

4.3. Next, a set S of syllables must be found which is capable to represent every group element uniquely and satisfies requirements that will justify the use the set is put to. This use will consist in replacing w_0 by its representation $\prod s_i$ in calculations of length and changes of length under certain products $T_2 T_1$. The requirements can be read off the wording of the theorem as follows:

Suppose $A = T_2 T_1$ and $A' = \prod_1^k T_i'$ given and that $T_i' = B_i$ is claimed for each $i \leqslant k$ (section 3). If for the moment X stands for any one of the automorphisms T_1, A, $\prod_1^r T_i'$, $r = 1, 2$, then $\prod s_i$ can replace w_0 in calculations of changes of length $L(X w_0) - L(w_0)$ if the condition (assuming $X(s_i)$ defined)

$$L(X w_0) - L(w_0) = L(X(\prod_{s_i \subset w_0} s_i)) - L(\prod_{s_i \subset w_0} s_i) = \sum_{s_i \subset w_0} L(X(s_i)) - \sum_{s_i \subset w_0} L(s_i) \qquad \text{(C)}$$

is satisfied. A method of constructing such a set is given in my doctoral dissertation (see section 1 of the present paper) for $G = F_3$; the method takes its departure from the 15 pairs of symbols $xy \neq 1$ that can be built out of generators and their inverses. It is seen there that the construction can be carried out for any $G = F_n$ provided only that the set of all such pairs can be written down explicitly. In order to utilize this fact, I shall, in sections 5 and 6, "standardize" the generators and the automorphisms $T_2 T_1$ in a way that will allow writing down the complete set of pairs needed for (indeterminate) $n \leqslant \infty$ as well as the construction of a single set S of syllables usable for each of the suitably chosen representatives of the equivalence classes of section 6.

4.4. Suppose that a set S of syllables has the property of affording unique syllable representation for every element of G and that for a certain set (T_k) of T-transformations

$$\left.\begin{array}{l}\text{every } T_k(s_i) \text{ in the set } T_k(S) \text{ has the same terminal symbols as does } s_i;\\ \text{that is } s_i = (x \alpha y) \text{ implies } T_k(s_i) = (x \beta y) \text{ reduced.}\end{array}\right\} \quad \text{(C}'\text{)}$$

By means of the lemma below I shall show that (C′) implies (C), for $X = T$ or $T T_k$, where T is any T-transformation. Then if such a set S is given, together with (T_k), (C') is a means of verifying (C).

Syllable representation by means of a set S is unique if every combination of symbols, that is, every word w, can be written in just one way as a product of syllables from S; this will hold if every pair of consecutive symbols xy that can be formed in $F_n = G$, $xy \neq 1$, occurs in the set either just once with no restriction on predecessors or successors, or else just once for each possible choice of the latter symbols.

The set S given in section 7 affords unique representation and satisfies (C′) with respect to every automorphism actually used in computations of length in section 8.

The verification of this is left to the reader; it is greatly simplified by the lemma below and the standardization in section 5.

LEMMA. *Any set S of syllables which can represent all elements of G uniquely has the property (C) with respect to a single T-transformation, T.*

In other words, changes of length in w_0 under T are just those occurring in the syllables s_i of S, contained in w_0, transformed as separate words, albeit by the rule (*) of section 4.2.

Proof. Take $T(w_0)$ unreduced; if a symbol introduced by T into w_0 does not cancel out as $T(w_0)$ is reduced, it will appear in just one $T(s_i)$; this follows from the definition of $T(s_i)$. Thus, all that needs proving is that if the symbol cancels in $T(w_0)$, it cancels in just one $T(s_i)$. Let $W = T(w_0)$ unreduced; let w_0 be reduced.

I. If x is a generator, then W contains no segment $x\bar{x}x$. For suppose the contrary:

$$W = \cdots y x \bar{x}^k x z \cdots .$$

Then the portions $x\bar{x}$ and $\bar{x}x$ of $x\bar{x}^k x$ were not in w_0, and as $T(x^e) = x x^e$ is impossible, the symbols x were not in w_0. Then $T(y) = \cdots yx$ and $T(z) = xz \cdots$, which is impossible. It follows from this that if $s_1 = (\cdots \bar{x})$, $s_2 = (\bar{x} \cdots)$ and $\bar{x}$ cancels in s_1, it cannot cancel in s_2.

II. To show that *some* symbol in s_2 above cannot cancel *some* symbol in s_1, one needs to show that in $W = \cdots E \cdots E \cdots$, where E reduces to the empty word, $L(E) = 2$ is always true. Suppose

$$W = \cdots y \bar{x} x z \cdots u \bar{u} \cdots$$

so that $\bar{x}x$ is not in w_0, hence $\bar{x}$, say, is not in w_0. Then $T(y) = \cdots y\bar{x}$, and so $\bar{x}$ is the multiplier in T, y is active in T, and so $u\bar{u} = x^e \bar{x}^e$. If now $E \neq \bar{x}x$, drop all pairs $x\bar{x}$, $\bar{x}x$ in E and call the result E'. Then E' is of the form $\ldots z\bar{z} \ldots$ since $E' = 1$. If $z\bar{z}$ was in E, then $z\bar{z} = x\bar{x}$ or $\bar{x}x$, and so cannot be in E', hence $z\bar{z} \not\subset E$. But then

$$E = \cdots z (\bar{x}x)^k \bar{z} \cdots ,$$

and because of I. above, $k = 1$, with

$$W = \cdots z \bar{x} x \bar{z} \cdots$$

and $\bar{x}x \not\subset w_0$. Suppose $\bar{x} \not\subset w_0$; then $T(z) = \cdots z\bar{x}$, $T(\bar{z}) = x\bar{z} \cdots$, so $w_0 = \cdots z\bar{z} \cdots$, contrary to the assumption that w_0 is reduced. This concludes the proof of the lemma.

Now let S be a set of syllables satisfying the condition of the lemma and the condition (C′) with respect to a given T_1. Then $\prod_{s_i \subset w_0} T_1(s_i)$ is defined and represents $T_1(w_0)$, by virtue of the definition of $T(s_i)$ for arbitrary T; moreover it represents the reduced word $T_1(w_0)$, by virtue of (C′), with $L(T_1(s_i)) \geqslant 2$. Hence the set $(T_1(s_i))$ is a set of syllables to which the lemma is applicable with respect to any T-transformation T_2; hence S satisfies (C) with respect to $T_2 T_1$.

5. Standardization [1]

Let T_1 be given by

$$\begin{array}{ll} a_1 \to a_1 c & a_{j_1} \to \bar{c}\, a_{j_1} c \\ a_2 \to a_2 c & \vdots \\ \vdots & a_{k_1} \to a_{k_1} \\ a_{i_1} \to \bar{c}\, a_{i_1} & \vdots \\ a_{i_2} \to \bar{c}\, a_{i_2} & d \to T_1(d) \\ \vdots & \end{array}$$

in $F_n = F(a_1, \ldots; a_{i_1}, \ldots; a_{k_1}, \ldots; c, d)$ with c and d^e not necessarily distinct. Represent a_m symbolically by $\bar{X}_m Y_m = a_m$, for every generator excepting c and d. Then under T_1, $a_1 = \bar{X}_1 Y_1 \to \bar{X}_1 Y_1 c$, which will be written symbolically as $\{\bar{X}_1 \to \bar{X}_1,\ Y_1 \to Y_1 c\}$, or equivalently, as $\{X_1 \to X_1,\ Y_1 \to Y_1 c\}$. For example, $a_{j_1} = \bar{X}_{j_1} Y_{j_1}$ gives $\{X_{j_1} \to X_{j_1} c,\ Y_{j_1} \to Y_{j_1} c\}$.

Let α range over the set of symbols X_r, Y_s for which $X_r \to X_r c$, $Y_s \to Y_s c$. Then $\alpha = (Y_1, Y_2, \ldots; X_{i_1}, X_{i_2}, \ldots; X_{j_1}, \ldots; Y_{j_1}, \ldots)$. Let β range over all other symbols X_r, Y_s. Then T_1 is given by

$$T_1 \begin{cases} \alpha \to \alpha c \\ \beta \to \beta \\ d \to T_1(d). \end{cases}$$

Similarly, an automorphism T_2 with multiplier d^e is given by

$$T_2 \begin{cases} \alpha' \to \alpha' d^e \\ \beta' \to \beta' \\ c \to T_2(c) \end{cases}$$

where c is the multiplier in T_1 and $\alpha \cup \beta = \alpha' \cup \beta'$.

[1] The procedure of this section may be interpreted as an embedding of F_n in F_{2n-2}.

Set

$$x = \alpha \cap \alpha', \qquad y = \text{complement of } x \text{ in } \alpha.$$
$$z = \beta \cap \beta', \qquad u = \text{complement of } x \text{ in } \alpha'.$$

Then $x \cup y \cup z \cup u = \alpha \cup \beta$, and the sets x, y. u, z, (c, d) are disjoint pairwise. In their terms

$$T_1 = t_1\, t_{12}\, t_{11} \begin{cases} t_{11} : x \to x\, c \\ t_{12} : y \to y\, c \\ t_1 \ : d \to T_1(d) \end{cases} \qquad T_2 = t_2\, t_{22}\, t_{21} \begin{cases} t_{21} : x \to x\, d^e \\ t_{22} : u \to u\, d^e \\ t_2 \ : c \to T_2(c) \end{cases}$$

where the statement $z \to z$ is omitted for brevity. Any pair $T_2 T_1$ can be so written, with the proper choice of the sets x, y, z, u, (c, d).

The images $T_1(d)$ may be dc, $\bar{c}d$, or "both": $\bar{c}dc$; accordingly let

$$t_{13} : d \to d\, c$$
$$t_{14} : d \to \bar{c}\, d,$$

so that t_1 may equal t_{13}, t_{14}, or $t_{14}\, t_{13}$, or 1. Similarly for $T_2(c)$, with

$$t_{23} : c \to c\, d^e$$
$$t_{24} : c \to \bar{d}^e\, c.$$

This result has two consequences. There are now only twelve symbols in F_n, namely x, y, z, u, c, d and their inverses, and hence a fixed number of syllables of length 2.(¹) Thus a fixed set S can be found (section 4.3) for all F_n. Furthermore, the sets x, y, u, z, $(c\ d)$ may be taken to stand for an arbitrary fixed partition of the symbols X_j, Y_i, c, d; then every $T_2 T_1$ is a product of certain of the t_{ij}, $j = 1, \dots, 4$, $i = 1, 2$, provided only that T_i stands for a T-transformation.

6. Equivalence classes

Before defining equivalence between automorphisms, it will be convenient to settle the case (section 3) when $A = \bar{p}\, T$, where p is a permutation of the generators and their inverses.

(¹) Among all pairs one may form here, the 8 pairs $a\bar{a}$ stay invariant under all $T_2 T_1$, or else $a\bar{a} = 1$; the 16 pairs ab, where a and b range over x, y, z, u, never occur; similarly for the following: 16 pairs $\bar{a}\bar{b}$, 16 pairs $c^{e'} a$ or $d^{e'} a$, 16 pairs $\bar{a} c^{e'}$ or $\bar{a} d^{e'}$. Finally, the 16 pairs $\bar{a} b$ are generators, hence not syllables. The remaining pairs are the following and their inverses: $x\bar{y}$, $x\bar{u}$, $y\bar{u}$, $x\bar{z}$, $y\bar{z}$, $u\bar{z}$, xc^e, yc^e, uc^e, zc^e, cc, dd, xd^e, yd^e, ud^e, zd^e, cd^e, $\bar{c}d^e$; $e = \pm 1$.

For every $\bar{p}\,T$ there is a T-transformation T' such that $\bar{p}\,T = T'\,\bar{p}$. To show this, designate by c the multiplier in $T_1 = T$, say $c = a_i^e$ and let $(a_i^{e'}, c)$ denote the image of $a_i^{e'}$ under T. Then $(c, c) = c$ and the set $(a_i^{e'}, c)$, $i = i, \dots, n$, defines T. Let p be given by $a_j^e \to a_i^{e'}$, $i, j = 1, \dots n$; in particular let $a_r^{e''} = d$ and $d \to c$. Then

$$a_j^e \xrightarrow{p} a_i^{e'} \xrightarrow{T} (a_i^{e'}, c) \xrightarrow{\bar{p}} (a_j^e, d)$$

$$d \xrightarrow{p} c \xrightarrow{T} c \xrightarrow{\bar{p}} d.$$

Thus, $\bar{p}\,T\,p : a_j^e \to (a_j^e, d)$, with $a_r^{e''} = d \to (d, d)$. The set (a_j^e, d) defines a single T-transformation $T' = \bar{p}\,T\,p$; hence $\bar{p}\,T = T'\,\bar{p}$.

A permutation is a level transformation, so that $T'\,\bar{p}$ is direct (section 3).

It follows also that $\bar{p}\,T_2\,T_1\,p = (\bar{p}\,T_2\,p)\,(\bar{p}\,T_1\,p) = T_2'\,T_1'$, which can be expressed by saying that $T_2\,T_1$ and $T_2'\,T_1'$ differ by nomenclature. The rest of the discussion of theorem 1 will concern forms $T_2\,T_1 \neq \bar{p}\,T$.

Two automorphisms A_1, A_2, will be called equivalent, $A_1 \sim A_2$, if for $A_1 = T_k\,T_{k-1} \dots T_1$

$$A_2 = \bar{p}\,C_k\,T_k\,C_{k-1}\,T_{k-1} \dots T_1\,C_0\,p$$

where p is a permutation and the C_i are inner automorphisms.

Since on cyclic words inner automorphisms are the identity transformation, the proof of theorem 1 is identical for automorphisms differing only by these. Conjugation of A_1 by a permutation amounts to a change of nomenclature: if B is direct (section 3) for A_1 then $\bar{p}\,B\,p = B'$ is direct for $A_2 = \bar{p}\,A_1\,p$. Thus it suffices to carry the proof for one element of an equivalence class.

The following shows that every equivalence class of the forms $T_2\,T_1$ is already generated by t_{11}, t_{12}, t_{13}, t_{21}, t_{22}, t_{23} of section 5.

Suppose T_1 contained $t_{14} : t \to \bar{c}\,d$, and $A = T_2\,T_1$. Then $T_1(d) = \bar{c}\,d$ or $\bar{c}\,d\,c$. Let $C : a_i \to c\,a_i\,\bar{c}$ for every generator a_i, so that $A \sim C\,A = T_2'\,T_1'$, where under T_1' either $d \to d\,\bar{c}$ or $d \to d$. If the latter holds, then $C\,A$ does not contain t_{14}; if the former holds, then let p be the permutation $c \to \bar{c} \to c$, and let $A'' = \bar{p}\,C\,A\,p = T_2''\,T_1''$. Then $A \sim A''$ and under T_1'' the image of d is $d\,c$. Hence A is equivalent to a product of two T-transformations in which t_{14} does not occur.

Suppose in $A = T_2\,T_1$ t_{14} does not occur but t_{24}: $c \to \bar{d}^e\,c$ does. Then $T_2(c) = \bar{d}^e\,c$ or $\bar{d}^e\,c\,d^e$. Let C: $a_i \to d^e\,a_i\,\bar{d}^e$ for every generator a_i. As before, $A \sim C\,A = T_2'\,T_1'$ and $T_2'(c) = c\,d^e$ or c. Since C leaves d fixed and since $C\,A = C\,T_2\,T_1 = (C\,T_2)\,T_1$, we have

$T_1' = T_1$, $T_2' = C\,T_2$, so that t_{24} does not occur in CA. Hence A is equivalent to a product of two T-transformations in which t_{14} and t_{24} do not occur.

It follows that the theorem needs proving only for forms $T_2\,T_1$ generated by t_{ij}, $i = 1, 2$; $j = 1, 2, 3$. This is done in section 8.

7. The set S

The symbol $(l\,m)$ will stand for the pairs $(l\,m)$ and $(l\,m)^{-1}$, that is $(l\,m) = (l\,m)^{\pm 1}$.

The symbol $(l\,m)\,\bar{\mathfrak{a}}$ will abbreviate the collection of all pairs $(l\,m)$ not followed by the symbols $\bar{x}$, $\bar{y}$, d, or $\bar{d}$, that is $(l\,m)\,\bar{\mathfrak{a}} = ((l\,m)\,\bar{\mathfrak{x}},\ (l\,m)\,\bar{\mathfrak{y}},\ (l\,m)\,\mathfrak{d}^e)$.

Since x (or y, etc.) is a set of symbols X_i, Y_j (section 5), the statement "x is void" is clear. In a set of syllables containing the symbol x, whenever in the automorphism under discussion the set x is void, one merely drops all syllables containing x. Similarly, if in the automorphism under discussion $c = d$ or $c = \bar{d}$, one drops all syllables containing, say, d; for then d is void.

With these conventions, the following is a set S usable in all computations necessary to prove theorem 1.

Pairs of the form $(\bar{h}\,k)^e$ and $(h\,h^e)$, h, k: x, y, z, u, do not appear in S (section 5), and will, when necessary, be referred to as s_0.

$s_1 = (d\,d)$	$s_{14} = (x\,\bar{c}\,\bar{u})$	$s_{27} = (y\,c\,\bar{d})$	$s_{40} = (u\,c)\,\bar{\mathfrak{a}}$
$s_2 = (x\,\bar{z})$	$s_{15} = (x\,\bar{c}\,\bar{d})$	$s_{28} = (y\,c\,\bar{y})$	$s_{41} = (u\,d)$
$s_3 = (x\,c\,\bar{d})$	$s_{16} = (x\,d)$	$s_{29} = (y\,c)\,\bar{\mathfrak{a}}$	$s_{42} = (u\,\bar{c})$
$s_4 = (x\,c\,d)$	$s_{17} = (y\,\bar{z})$	$s_{30} = (y\,c\,d)$	$s_{43} = (u\,\bar{d})$
$s_5 = (x\,c\,\bar{y})$	$s_{18} = (u\,\bar{z})$	$s_{31} = (y\,d)$	$s_{44} = (c\,c\,\bar{d})$
$s_6 = (x\,c\,\bar{x})$	$s_{19} = (z\,c\,\bar{\mathfrak{a}})$	$s_{32} = (y\,\bar{u})$	$s_{45} = (c\,c\,d)$
$s_7 = (x\,c)\,\bar{\mathfrak{a}}$	$s_{20} = (z\,c\,d)$	$s_{33} = (y\,\bar{c}\,d)$	$s_{46} = (c\,c)\,\bar{\mathfrak{a}}$
$s_8 = (x\,\bar{d})$	$s_{21} = (z\,c\,\bar{d})$	$s_{34} = (y\,\bar{c}\,\bar{c})$	$s_{47} = (d\,c\,d)$
$s_9 = (x\ \bar{y})$	$s_{22} = (z\,c\,\bar{y})$	$s_{35} = (y\,\bar{c}\,\bar{u})$	$s_{48} = (\bar{d}\,c\,d)$
$s_{10} = (x\,\bar{u})$	$s_{23} = (z\,c\,\bar{x})$	$s_{36} = (y\,\bar{c}\,\bar{d})$	$s_{49} = (d\,c\,\bar{d})$
$s_{11} = (x\,\bar{c}\,d)$	$s_{24} = (z\,d)$	$s_{37} = (y\,\bar{d})$	$s_{50} = (\bar{d}\,c\,\bar{d})$
$s_{12} = (x\,\bar{c}\bar{y})$	$s_{25} = (z\,\bar{c})$	$s_{38} = (u\,c\,\bar{d})$	$s_{51} = (\bar{d}\,c)\,\bar{\mathfrak{a}}$
$s_{13} = (x\,\bar{c}\,\bar{c})$	$s_{26} = (z\,\bar{d})$	$s_{39} = (u\,cd)$	$s_{52} = (d\,c)\,\bar{\mathfrak{a}}$.

The following observation will be used in section 8. Let each symbol in the set (x, y, u, z, c, d) stand for a fixed subset of the symbols X_i, Y_i (section 5) and define the form $T_2'\,T_1'$. Let $T_2\,T_1$ be given by

$$T_1 \begin{cases} y \to y\,c \\ x \to x\,c \end{cases};\; T_2 : u \to u\,d.$$

Then no symbol X_i or Y_j is active in *both* T_i, hence one can write $y'' = x \cup y$ and $T_1'' : y'' \to y''\,c$, $T_2'' : u \to u\,d$, with $T_i'' = T_i$, so that $T_2 T_1 = T_2'' T_1''$ identically. This can be expressed by saying: $T_2 T_1$ is of the form $T_2'' T_1''$.

The results gotten so far may be summed up so: if T_i is a product of a subset of the automorphisms t_{i1}, t_{i2}, t_{i3}, $i = 1, 2$, with x, y, z, u, c, d fixed but arbitrary sets of symbols X_i, Y_j (section 5), it suffices to prove theorem 1 for $T_2 T_1$ acting on any word w_0 satisfying the hypotheses (1) and (2) of the theorem. It is permissible to replace w_0 by its representation $\prod\limits_{s_i \subset w_0} s_i$, $s_i \subset S$ above, in computations of changes of length under such T_i and $T_2 T_1$.

8. Computations

The following device is the key to demonstrating that if A and w_0 satisfy the hypotheses (1) and (2) of theorem 1, then a proposed A' has the properties of B in the theorem.

If T: $x \to x\,c$, then T and the (cyclic) word $x\,\bar{c}\,\bar{z} = w = \Pi\, s_i = (x\,\bar{c}\,\bar{z})\,(\bar{z}\,x) = s_{23}\,s_0$ cannot satisfy hypothesis (1), for $T\,(x\,\bar{c}\,\bar{z}) = x\,\bar{z} = T\,(w)$ is shorter than w. For this T, s_{23} is a reduction syllable, that is $L\,(T\,s_{23}) - L\,(s_{23}) = -1 < 0$, and the word w contains reduction syllables in excess of increase syllables under T.

In general, if $L\,(T\,s_i) - L\,(s_i) = k_i$, and x_i stands for the (indeterminate) number of times s_i occurs in w_0, then $L\,(T\,w_0) - L\,(w_0) = \sum\limits_i k_i\,x_i = I - R$, where I sums the positive, $-R$ the negative terms. If $A = T_2 T_1$ and w_0 satisfy (1) and (2), then $I - R = r > 0$ for T_1 and $I - R \leqslant r$ for A.

Suppose now that S is usable for $T_2' T_1' = A'$, that $A' \sim A$, and $T_1'\,(w_0) = W$ is at least as long as $T_1\,(w_0)$. Then $I - R \geqslant r$ for T_1' is a third inequality, with known coefficients, in the x_i. If adding these three inequalities gives a contradiction, then W is shorter than $T_1\,(w_0)$ and so A' is direct.

For convenience, in the sequel x_i will be abbreviated to i.

0.1. Products of t_{12}, t_{22}.

$$A \begin{cases} y \to y\,c \\ u \to u\,d \end{cases} = A' \begin{cases} u \to u\,d \\ y \to y\,c \end{cases};\; A' = T_2' T_1'.$$

If y, or u, or both be void, there is nothing to prove. The following shows that the assumption $T_1'(w_0)$ is longer than w_0 gives a contradiction. The result holds whether d is void or not (section 7), that is whether $c=d^e$ or not.

By hypothesis (1), for T_1, $I-R=r>0$, or $I=R+r$:

$$17+27+29+30+31+32+37=22+33+34+35+36+r. \tag{1}$$

By hypothesis (2), for A, $R+r\geqslant I$:

$$\begin{aligned}&22+33+34+36+43+r\geqslant\\&\qquad\geqslant 17+18+27+29+30+31+37+38+39+40+41+42+2\,(32).\end{aligned} \tag{2}$$

For T_1', $I>R$:

$$18+32+35+38+39+40+41+42>43. \tag{3}$$

Adding these three inequalities gives $0>0$, a contradiction.

0.2. Products of t_{11}, t_{12}, t_{21}.

$$A\begin{cases}x\to x\,c\\ y\to y\,c\,;\quad A=t_{21}\,t_{12}\,t_{11}.\\ x\leftarrow x\,d\end{cases}$$

If x is void there is nothing to prove; if y or d is void the result below still holds. If the assumption (3) below that $t_{11}(w_0)$ is longer than w_0 gives a contradiction, then $t_{21}\,t_{12}$ is left to investigate, which is of the form 0.1. (section 7) and can be made direct.

$$2+3+4+7+8+16+17+27+29+30+31+37=11+13+15+22+23+33+34+36+r \tag{1}$$

$$2\,(15)+22+33+34+36+r\geqslant\begin{Bmatrix}2\,(2+3+4+6+7+8+16)+\\ 5+9+12+17+27+29+30+31+37\end{Bmatrix} \tag{2}$$

$$2+3+4+5+7+8+9+16>11+12+13+14+15. \tag{3}$$

Adding these three inequalities gives $0>2\,(11+13)+12+23$, which contradicts the fact that $x_i\geqslant 0$ for every i.

0.3. Products of t_{11}, t_{12}, t_{21}, t_{22}.

$$A\begin{cases}x\to x\,c\\ y\to y\,c\\ x\to x\,d\\ u\to u\,d\end{cases}=A'\begin{cases}u\to u\,d\\ x\to x\,c\\ y\to y\,c\\ x\to x\,d\end{cases}.$$

If x (or u) is void, A is of the form 0.1 (or 0.2). Whether or not y is void, the result below holds.

If t_{11}: $x \to x c$ does not lengthen w_0, then $A t_{11}$ is left to investigate and this is of the form 0.1; thus one may assume the contrary; this is done under (3) below. If t_{11}': $u \to u d$ does not lengthen w_0, then $A' t_{11}'$ is left, which is of the form 0.2; the contrary is assumed under (4) below.

$$\left.\begin{matrix} 2+3+4+7+8+10+16+17 \\ +27+29+30+31+32+37 \end{matrix}\right\} = \left\{\begin{matrix} 11+13+14+15+22+ \\ 23+33+34+35+36+r \end{matrix}\right\} \tag{1}$$

$$\left.\begin{matrix} 2\,(15)+14+22+33+ \\ +34+36+43+r \end{matrix}\right\} \geqslant$$
$$\geqslant \left\{\begin{matrix} 2\,(2+3+4+6+7+8+10+16+32)+5+9+10+12+17+ \\ 18+27+29+30+31+37+38+39+40+41+42 \end{matrix}\right\} \tag{2}$$

$$2+3+4+5+7+8+9+10+16 > 11+12+13+14+15 \tag{3}$$

$$10+14+18+32+35+38+39+40+41+42 > 43 \tag{4}$$

Adding these inequalities gives $0 > 2\,(11+12+13)+23$, a contradiction.

In the rest of the computations, if d is void, then every automorphism under discussion is of a form already treated. Hence it is now assumed that $c \neq d^e$.

1.1. Products of t_{12}, t_{22}, t_{23}.

$$A \begin{cases} y \to y c \\ c \to c d \\ u \to u d \end{cases} = A' \begin{cases} c \to c d \\ u \to u d \\ y \to y d \\ y \to y c \end{cases};\quad A' = T_2' T_1'.$$

If c is not active, A is of the form 0.1. If y, or u, or both be void, then either there is nothing to prove, or the results below still hold. Assume neither void. If T_1' does not lengthen w_0, A' is direct. In (3) below the contrary is assumed.

$$17+27+29+30+31+32+37 = 22+33+34+35+36+r \tag{1}$$

$$21+22+33+36+43+49+50+r \geqslant$$
$$\geqslant \left\{\begin{matrix} 2\,(17+29+30+31+39+45)+18+20 \\ +25+27+28+30+32+40+41+46+47+48 \end{matrix}\right. \tag{2}$$

$$\left.\begin{array}{l}17+18+20+25+28+29+31+34+35+\\ 40+41+46+47+48+2\,(30+39+45)\end{array}\right\}>21+37+43+49+50 \tag{3}$$

Adding these gives $0>0$, a contradiction.

1.2. Products of all $t_{ij} \neq t_{13}$.

$$A\left\{\begin{array}{l}x\to x\,c\\ y\to y\,c\\ x\to x\,d\\ u\to u\,d\\ c\to c\,d\end{array}\right. = t_{21}\,(\bar{t}_{21}\,A)=t_{21}\,A';\ t_{21}\colon x\to x\,d.$$

If x is void, A is of the form 1.1. If c is not active, A is of the form 0.3. If u or y or both be void, the results below still hold. Assume neither void. Now, A' is of the form 1.1 and is not direct by hypothesis; if $A'(w_0)$ is not longer than $T_1(w_0)$, then (on the pattern of 1.1, and by section 7) $A'=A''$, where

$$A''\left\{\begin{array}{l}c\to c\,d\\ u\to u\,d\\ x\to x\,d\\ y\to y\,d\\ x\to x\,c\\ y\to y\,c\end{array}\right.;\ A''=T_2''\,T_1'',$$

and A'' is direct, so that $T_1''(w_0)$ is not longer than w_0. Then $t_{21}\,T_2''$ is left to investigate, which is of the form 0.2. Under (3) below the contrary is assumed: $A'(w_0)$ is longer than $w_1=T_1(w_0)$.

If for t_{11}: $x\to x\,c$, $t_{11}(w_0)$ is not longer than w_0, then $A\,\bar{t}_{11}$ is left to investigate, which is of the form 1.1; under (4) below the contrary is assumed.

$$\left.\begin{array}{l}2+3+4+7+8+10+16+17+\\ 27+29+30+31+32+37\end{array}\right\}=\left\{\begin{array}{l}11+13+14+15+22+23+\\ 33+34+35+36+r\end{array}\right. \tag{1}$$

$$\left.\begin{array}{l}13+14+2\,(15)+21+22+\\ 33+36+43+49+50+r\end{array}\right\}\geqslant\left\{\begin{array}{l}3\,(2+7+16+30)+4\,(4)+2\,(3+5+10+17+29+\\ 31+39+45)+6+8+9+18+20+25+27+28+\\ 32+40+41+46+47+48\end{array}\right. \tag{2}$$

$$\left.\begin{array}{l}3\,(4+30)+2\,(2+7+16+17+\\ 29+31+39+45)+3+5+6+10+\\ 12+18+20+25+27+28+32+\\ 40+41+46+47+48\end{array}\right\}>\left\{\begin{array}{l}11+15+21+22+23+33+36+\\ 43+49+50+r\end{array}\right. \tag{3}$$

$$2+3+4+5+7+8+9+10+16>11+12+13+14+15+23 \tag{4}$$

Adding the last three inequalities gives $0>2(11)$, a contradiction.

2. Products of all $t_{ij} \neq t_{23}$.

$$A\begin{cases} x\to x\,c \\ y\to y\,c \\ d\to dc \\ x\to x\,d \\ u\to u\,d \end{cases} = A'\begin{cases} x\to x\,d \\ y\to y\,c \\ d\to d\,c \\ u\to u\,d \end{cases} = A''\begin{cases} u\to u\,\bar{c} \\ u\to u\,d \\ x\to x\,d \\ d\to d\,c \\ y\to y\,c \end{cases}$$

where $A' = T_3'\,T_2'\,T_1'$ and $A'' = T_3''\,T_2''\,T_1''$.

If u is void, A'' is of the form 1.1. (As soon as the symbols d and c are exchanged and section 7 is considered this becomes apparent.) Since 1.1. can be made direct in such a way that no intermediate word is longer than w_0, this case is already taken care of. Similarly for the other symbols. Thus, one may assume that u, etc. are not void. By the same token, $T_1''(w_0)$ may be assumed longer than w_0; this is done under (3) below; also $T_1'(w_0)$ may be assumed not shorter than w_0; this is done under (4) below.

$$\left.\begin{array}{l} 1+2+4+7+10+16+17+26+ \\ 29+30+31+32+43+47+52 \end{array}\right\} = \left\{\begin{array}{l} 11+13+14+21+22+23+33+34+ \\ 35+38+44+50+r \end{array}\right. \tag{1}$$

$$\left.\begin{array}{l} 8+14+21+22+33+34+ \\ 2(38)+44+50+r \end{array}\right\} \geqslant \left\{\begin{array}{l} 3(10)+2(2+4+6+7+16+32+43)+ \\ 1+3+5+9+12+15+17+18+26+29+ \\ 30+31+39+40+41+42+47+52 \end{array}\right. \tag{2}$$

$$10+18+32+35+41+42+43>14+38+39+40 \tag{3}$$

$$2+3+4+5+2(6)+7+9+10+11+12+13+14+15+16+23\geqslant 8 \tag{4}$$

Adding these gives $0>2(39+40)$, a contradiction.

This takes care of all categories save 3: products of all t_{ij}. The fact that in every case a direct automorphism B was found with the property that no intermediate word is longer than w_0 will be used in 3. below.

Because the cases 3. require a great many inequalities, the following simplifying device is used. The set S so far used is large because it is usable for every case; but smaller sets suffice for just one category. A set usable for 3. alone, of fewest possible syllables, will be given. They will be devided into subsets as indicated by the numbering, and in the computations the number of times s_{ij} occurs in w_0 will be designated by $i\,j$.

The symbol a stands for each symbol in the set $(\bar{x},\ \bar{y},\ d^e)$; the symbol b for each in $(\bar{x},\ \bar{d})$.

$$s_0 = (s_{0i}) = ((x\,c\,\bar{d}),\ (y\,c\,\bar{x}),\ (d\,c\,\bar{x}),\ (\bar{d}\,c)\,\mathfrak{b},\ (y\,\bar{d}),\ (u\,\bar{c}),\ (z\,d))$$

$$s_1 = (s_{1i}) = ((x\,d),\ (x\,\bar{z}),\ (x\,c)\,\mathfrak{a})$$

$$s_2 = (s_{2i}) = ((y\,d),\ (d\,d),\ (y\,\bar{z}),\ (d\,\bar{z}),\ (x\,\bar{u}),\ (y\,c)\,\mathfrak{a},\ (d\,c)\,\mathfrak{a})$$

$$s_3 = (s_{3i}) = ((x\,c\,\bar{x}),\ (y\,c\,\bar{y})\ (d\,c\,\bar{y}),\ (u\,c)\,\mathfrak{a},\ (c\,d),\ (c\,\bar{z}),\ (x\,\bar{y}),\ (u\,d),\ (u\,\bar{z}),\ (c\,c)\,\mathfrak{a})$$

$$s_4 = (x\,c\,\bar{y})$$

$$s_5 = (s_{5i}) = ((u\,\bar{y}),\ (u\,\bar{d}))$$

$$s_6 = (s_{6i}) = ((c\,c\,\bar{d}),\ (u\,c\,\bar{d}))$$

$$s_7 = (s_{7i}) = ((d\,\bar{c}\,d),\ (d\,\bar{c}\,\bar{z}),\ (c\,c\,\bar{x}),\ (u\,c\,\bar{x}),\ (z\,c\,\bar{y}),\ (y\,\bar{c}\,d))$$

$$s_8 = (s_{8i}) = ((x\,\bar{c}\,d),\ (x\,\bar{c}\,\bar{z}),\ (c\,c\,\bar{y}),\ (u\,c\,\bar{y}))$$

$$s_9 = (s_{9i}) = ((y\,c\,\bar{d}),\ (d\,c\,\bar{d}),\ (x\,\bar{d})).$$

3.1. Products containing t_{13} and t_{23}, with $e = +1$.

$$A \begin{cases} x \to xc \\ y \to yc \\ d \to dc \\ c \to cd \\ x \to xd \\ u \to ud \end{cases} \sim A' \begin{cases} x \to xc \\ y \to yc \\ d \to dc \\ c \to cd \\ x \to xd \\ u \to ud \\ g \to dg\bar{d} \end{cases} = \begin{cases} x \to xc \\ y \to yc \\ d \to dc \\ x \to xd \\ x \to x\bar{d} \\ c \to dc \\ y \to y\bar{d} \\ z \to z\bar{d} \end{cases} = A^* \begin{cases} x \to xc \\ y \to yc \\ d \to dc \\ z \to z\bar{d} \\ c \to dc \\ y \to y\bar{d} \end{cases}$$

where g runs through x, y, u, z, c. Moreover, A equals

$$A'' \begin{cases} u \to uc \\ d \to dc \\ x \to xc \\ y \to yc \\ c \to cd \\ x \to xd \\ u \to u\bar{c} \end{cases} ;\ A'' = T_3''\,T_2''\,T_1''.$$

Set $A' = T_3' T_2' T_1'$ and $A^* = T_3^* T_2^* T_1^*$, where $T_1^* = T_1$, $T_2^* = t$: $z \to z\bar{d}$; also $T_1' = T_1$, $T_2' = t' : x \to x d$.

The computation below gives the same result if any subset of (x, y, u, z) is void. If c or d is void, A reverts to a form discussed before. Similarly for 3.2, where $e = -1$. Assume therefore that none of the sets are void.

The product $T_3'' T_2''$ is equivalent to the form 2. (exchanging the letters c and d, and setting x and y void in 2. makes this apparent), which can be made direct in such a way that no intermediate word is longer than the first word. Thus if $T_1''(w_0)$ is shorter than $w_1 = T_1(w_0)$, then A'' either is direct or can be made direct. Under (3) below the contrary is assumed.

The product $T_2' T_1'$ is of the form 2. (with u made void in 2.), so it can be made direct in same manner. Thus if $T_2' T_1'(w_0)$ is shorter than w_1, then A' either is direct or can be made so. Under (4) below the contrary is assumed. The same holds for $T_2^* T_1^*$, so it is assumed under (5) below that $T_2^* T_1^*(w_0)$ is not shorter than w_1.

Set T^0: $x \to xc$, $d \to dc$. If $T^0(w_0)$ is shorter than w_1, then $A\bar{T}^0$ is left to investigate, which is of the form 1.1. Under (6) below the contrary is assumed.

Let C be a conjugation of every symbol, except d, by d, and C' a conjugation of every symbol, except c, by c. Since conjugations are the identity transformation on cyclic words, $I = R$ (see beginning of section 8) for C and C'. This is what the equalities (7) and (8) below state.

$$1+2+5=6+7+8+r \tag{1}$$

$$2(6+7+8+r)=2(1+2+5) \tag{1'}$$

$$3(6+7+8+r)=3(1+2+5) \tag{1''}$$

$$2(6)+7+9+r \geqslant 3(1)+2(2+4)+3+5 \tag{2}$$

Combining (1′) and (2) gives

$$5+9 \geqslant 1+3+7+r+2(4+8), \text{ or} \tag{2'}$$

$$6+9 \geqslant 2+3+8+2(1+4) \tag{2''}$$

$$1+(2-25)+34+38+39 \geqslant 07+61+(7-74)+(8-84)+r \tag{3}$$

$$\left.\begin{matrix} 01+02+03+2+25+37+4+ \\ 5+2(1+31) \end{matrix}\right\} \geqslant 6+71+72+75+76+83+84+93+r \tag{4}$$

$$\left.\begin{matrix} 05+1+12+2+23+24+36+ \\ 39+5+82 \end{matrix}\right\} \geqslant 09+6+71+73+74+76+8+r \tag{5}$$

$$\left.\begin{matrix}06+1+22+24+25+27+33+\\ 37+4+52+75+76\end{matrix}\right\}\geqslant 02+6+7+81+82+91+r \tag{6}$$

$$\left.\begin{matrix}01+03+06+24+27+33+52+\\ 6+72+9+92\end{matrix}\right\}=04+09+11+21+35+38+76+81 \tag{7}$$

$$07+35+36+61+73+83=04+05+13+26+27+34. \tag{8}$$

Adding (1″), (2′), (2″) and (3) to (8) gives $0\geqslant 2r+\cdots$, where the right hand side is at least as large as r, contrary to the definition of r. Thus, one of the automorphisms above is direct or can be made direct by previous results.

3.2. Products containing t_{13} and t_{23}, with $e=-1$.

$$A\begin{cases} x\to xc\\ y\to yc\\ d\to dc\\ x\to x\bar{d}\\ u\to u\bar{d}\\ c\to c\bar{d}\end{cases}\sim A'\begin{cases} x\to xc\\ y\to yc\\ d\to dc\\ x\to x\bar{d}\\ u\to u\bar{d}\\ c\to c\bar{d}\\ g\to \bar{d}gd\end{cases}=A^*\begin{cases} x\to xc\\ c\to \bar{d}\to \bar{c}\\ d\to \bar{c}d\\ y\to yc\\ z\to zd\end{cases}$$

where g runs through x, y, z, u, c.

Set $A^*=T_3^*T_2^*P^*T_1^*$, $t:x\to xc$, and $t':x\to x\bar{d}$. Then $T_3^*T_2^*$ is equivalent to the form 2. and can be made direct; thus if x is void A^* can be made direct. If x is not void but $t(w_0)$ is shorter than $w_1=T_1(w_0)$, then $\bar{t}A$ is left to investigate, which is equivalent to having x void. Assume then that $t(w_0)$ is not shorter than w_1; this gives the inequality (3) below.

Similarly, if $\bar{t}'A(w_0)$ is shorter than w_1, $\bar{t}'A$ is left to investigate, in which x is void. Assuming the contrary gives the inequality (4) below.

The results below remain the same if any subset of (u, y, z) is void.

$$1+2+5=6+7+8+r \tag{1}$$

$$35+38+7+2(81)+r\geqslant\begin{cases}2(01)+1+2(12+13+2-21-22+3-35-38)+\\ 2(4)+5+9\end{cases} \tag{2}$$

$$01+1+25+37+4+93\geqslant 02+03+73+74+81+82+r \tag{3}$$

$$\left.\begin{matrix}01+02+03+2(12+13+23+24+26+27)+\\ 25+3-35-37-38+4+5+91+92\end{matrix}\right\}\geqslant\begin{cases}35+38+71+72+75+76+\\ 81+82+r\end{cases} \tag{4}$$

Adding (2), (3) and (4) gives $0\geqslant r+26+27+2(82)$, contrary to the definition of r. Thus A^* is or can be made direct by previous results.

9. Corollary

The corollary to theorem 1 states (section 3) that w_0 may stand for a set of words $(w_{01}, w_{02}, \ldots, w_{0m})$. This is seen as follows.

Let a_i denote a generator of $F_n = G'$ and let g denote a new symbol. Let w_0 stand for the set of words above from a free group on any number of generators, finite or not, and suppose that n of these generators occur in w_0; denote them by a_i, $i = 1, \ldots, n$, and let g be a_{1+n} in the group. It is no loss of generality in what follows to consider only the free subgroup $G = F(a_1, \ldots, a_n, g)$.

Form the cyclic word

$$W_0 = w_{01}\, g\, w_{02}\, g\, w_{03}\, g \ldots w_{0n}\, g$$

in G. Then the theorem holds for W_0 in G. It will be seen to hold for w_0 in $F_n = G'$, and hence in any free group.

The direct automorphism B that takes W_0 into $A(W_0) = A(w_{01}\, g \ldots w_{0n}\, g) = (A\, w_{01} \cdot g \cdot A\, w_{02} \cdot g \cdot \ldots)$ has the following property: the image under B of an active generator differs from its image under A at most by a conjugation by a word w composed of multipliers in A. In particular, $B(g) = w g \bar{w}$, and for any T'_k in B, $T'_k(g) = w_k\, g\, \bar{w}_k$.

If w is the empty word, $w = 1$, then B is an automorphism of G', and the corollary is true, provided that also $w_k = 1$ for every k. Otherwise there is a smallest number k, with $w_k \neq 1$, and hence of length 1: $T'_k(g) = w_k\, g\, \bar{w}_k$, and w_k^e is a generator. Set T^*: $g \to \bar{w}_k\, g\, w_k$, $a_i \to \bar{w}_k\, a_i\, w_k$, $i = 1, \ldots, n$; the product $T^* T'_k = T_k$ is a single T-transformation. Replacing T'_k by T_k in B gives another direct transformation of W_0 into $A(W_0)$ but one with fewer factors that act on g. As B is a finite product of T-transformations, repetition of this procedure yields a direct transformation equivalent to B and with $w_k = 1$. This transformation will be an element of the automorphism group of G', hence the corollary.

10. Some consequences of theorem 1

THEOREM 2. *If w_0 is a set of elements and A is an automorphism of the free group G, $A(w_0) = w$, then there exist T-transformations B_i, $i = 1, \ldots, k$, $\prod_1^k B_i = A$, such that every set of words $\prod_1^r B_i(w_0)$, $r \leqslant k$, is at most as long as* $\max(L(w_0), L(w))$.

Proof. Suppose, for definiteness, that $L(w) \leqslant L(w_0)$. Let $T_h \ldots T_1$ be a representation of A in terms of T-transformations, with intermediate words $\prod_1^g T_i(w_0) = w_g$.

Let $w_{g'}$ be a longest intermediate word such that $L(w_{g'-1}) < L(w_{g'})$ or $L(w_{g'+1}) < L(w_{g'})$; $L(w_{g'}) = L$. Applying the corollary to $w_{g'-1}$, $w_{g'}$, $w_{g'+1}$ and using the direct transformation B so obtained to replace $T_{g'+1} T_{g'}$ in A yields $T_h \dots B \dots T_1 = A$, with intermediate (sets of) words of length at most L, but fewer longest ones than before. A finite number of these steps leads to the goal.

In particular, an automorphism B can be found for which there exist numbers $h'' \leqslant h' \leqslant k$, such that the lengths of the intermediate words W_g under B are monotone decreasing from 1 to h'', are unchanged from h'' to h', and are monotone increasing from h' to k. This result implies theorem 3 of Whitehead [7], which states that if w_0 and $A(w_0)$ are minimal T then they can be transformed into each other by level T-transformations.

THEOREM 3. *Words minimal relative to all single T-transformations are minimal relative to any automorphism.*

Otherwise the automorphism B of theorem 1 would fail to exist for some factor $T_2 T_1$ of such an automorphism.

THEOREM 4. *If w_1 and w_2 are minimal and are connected by an automorphism, then they contain the same number of distinct generators; moreover, if k_{ij} is the number of times a_i^e occurs in w_j, $i = 1, \dots, n$, $j = 1, 2$, then the sets of numbers (k_{i1}) and (k_{i2}) differ by a permutation of the subscripts i.*

Proof. By theorems 2 and 3 the (sets of) words w_j are connected by level T-transformations, T', and possibly permutations. The effect of such T' is to move the multiplier in T' from some places of occurrence to others with a change of sign. This, as well as a permutation, leaves the set of numbers (k_{ij}) unchanged.

THEOREM 5. *If $w_2 = A(w_1)$ is minimal, then the number of distinct generators in w_1 can be diminished by applying a transformation if and only if w_2 has fewer distinct generators than does w_1.*

This follows from the two preceding results.

THEOREM 6. *If w contains a_i or $\bar{a}_i$ for every i, $w \subset G = F(a_1, \dots)$ and is minimal, then $A(w)$ contains, for arbitrary A, a_i or $\bar{a}_i$ for every i.*

For suppose $w_1 = A(w)$ did not contain a_1^e; then $w = \bar{A}(w_1)$ would contain more distinct generators than w_1; this would contradict theorem 5.

11. Some applications of the syllable method

Let $(b_1, \ldots, b_k, a') = (b, a')$, $a' \neq b_i^e$, denote any non-empty subset of the symbols $a_1, \bar{a}_1, a_2, \bar{a}_2, \ldots, a_n, \bar{a}_n$; let z run through all those a_j^e not equal to $\bar{b}_i$ or $\bar{a}'$, $i = 1, \ldots, k$, as well as the identity element 1. Let $w \subset G = F(a_1, \ldots, a_n)$; denote by $(b_i \bar{a}')$ the number of times the symbol b_i is followed by $\bar{a}'$ in w plus the number of times $\bar{b}_i$ is preceded by a' in w; denote by $(b_i z)$ the corresponding number summed over all values of z. (A symbol is followed by 1 in w if it is the terminal symbol, and is preceded by 1 if it is the initial symbol there.)

THEOREM 7. *The word w is minimal if and only if the relation*

$$\sum_i (b_i \bar{a}') \leqslant \sum_i (b_i z) \tag{*}$$

holds for every set (b, a') in G.

Proof. The automorphism $b \to b a'$ is a T-transformation whose effect is to replace each element b_i of the set (b) by $b_i a'$. When $b_i \bar{a}'$ occurs in w, the symbol a' introduced by this T into $b_i \bar{a}'$ cancels against $\bar{a}'$; for an occurrence of $b_i z$ there is no cancellation. The excluded values for z yield the combinations $b_i \bar{b}_k$ and $b_i \bar{a}'$; in the latter there is cancellation, in the former there is no change under T. Thus the condition (*) states that the number of cancellations must not exceed the number of new symbols introduced by T. This condition is clearly necessary. Its sufficiency to make w minimal T, for any T-transformation, T follows from the lemma of section 4.4. It follows now from theorem 3 that under the hypotheses above w is minimal.

THEOREM 8. *"T-transformation" cannot be replaced by "simple, or, t-transformation" in theorem* 1.

Proof. The relation (*) of theorem 7, stated for simple automorphisms t, for $G = F(a_1, a_2, a_3)$ is of the form

$$(x y) \leqslant (x z) \tag{**}$$

since now $(b_1, \ldots, b_k, a') = (b, a') = (b_1, a')$, or, briefly, $(x y)$.

A word in G satisfying this condition for every pair (x, y), where x^e, $y^{e'}$ are generators, is minimal t.

Let v and u run through every symbol in G having exponent $+1$, and set $a = a_1$, $b = a_2$, $c = a_3$ in G. Then G has an element which satisfies (**) for every pair (x, y) as well as the condition

$$(a \bar{c}) + (b \bar{c}) > (a v) + (b u)$$

(for notation see the introduction to this section), which contradicts one of the relations (*).

This element is

$$w = b\,\bar{a}\,b\,\bar{c}\,a\,c\,\bar{b}\,c\,c\,\bar{b}\,c\,\bar{a}\,\bar{c}\,b\,b\,\bar{a}\,b\,b\,c\,\bar{a}\,c\,\bar{a}\,b\,\bar{c}$$

of length 24 and is minimal t but is reducible under the T-transformation T: $a \to a\,c$, $b \to b\,c$.

It may be noted that in F_2 every T-transformation is a t-transformation, and since $w\,(a, b, c)$ above is the shortest word in F_3 having this property, it is also shortest possible in any free group.

THEOREM 9. *If the word $T\,(w)$ is longer then w, then $T\,T\,(w)$ is longer than $T\,(w)$. More precisely, $L\,(T\,w) - L\,(w) = r > 0$ implies $L\,(T^2\,w) - L\,(T\,w) \geqslant r$.*

Proof. Let the inequality sign in the relation (*) of theorem 7 be replaced by a true inequality for a fixed set (b, a'):

$$\sum_i (b_i\,\bar{a}') < \sum_i (b_i\,z)$$

and let it hold for the word $w \subset G\,(a_1, \ldots, a_n)$. Then under the T-transformation T: $b_i \to b_i\,a'$, $i = 1, \ldots, k$, $T\,(w)$ is longer than w.

In $T\,(w) = w_1$, $b_i\,a'$ and its inverse occur more often than $b_i\,v = b_i\,\mathfrak{a}'$ and its inverse, for all b_i combined, so

$$\sum_i (b\;\mathfrak{a}') < \sum_i (b_i\,a') \text{ in } T\,(w).$$

Clearly, the set $(b_i\,\mathfrak{a}')$ contains the set $(b_i\,\bar{a}')$ of consecutive symbols, and so for the number of their respective occurrences, also written as $(b_i\,\mathfrak{a}')$ and $(b_i\,\bar{a})$: $(b_i\,\bar{a}') \leqslant (b_i\,\mathfrak{a}')$; since z was to take on the value a' too, $(b_i\,a') \leqslant (b_i\,z)$; hence

$$\sum_i (b_i\,\bar{a}') \leqslant \sum_i (b_i\,\mathfrak{a}') < \sum_i (b_i\,a') \leqslant \sum_i (b_i\,z) \text{ in } T\,(w).$$

Moreover, the difference between the two extremal sums in the last inequality is seen to be at least as great as that derivable from the first inequality above; hence if the latter be $r > 0$, the former is at least equal to r.

References

[1]. M. DEHN, Ueber unendliche diskontinuierliche Gruppen. *Math. Ann.*, 71 (1911), 116–144.
[2]. A. G. KUROSH, *The theory of groups*. 2nd ed. Translated from the Russian by K. Hirsch. Chelsea, New York, 1955/56.

[3]. B. H. NEUMANN, On the number of generators of a free product. *J. London Math. Soc.*, 18 (1943), 12–20.

[4]. J. NIELSEN, Die Isomorphismengruppe der freien Gruppen. *Math. Ann.*, 91 (1924), 169–209.

[5]. A. SHENITZER, Decomposition of a group with a single defining relation into a free product. *Proc. Amer. Math. Soc.*, 6 (1955), 73–79.

[6]. J. H. C. WHITEHEAD, On certain sets of elements in a free group. *Proc. London Math. Soc.*, 41 (1936), 48–56.

[7]. ——, On equivalent sets of elements in a free group. *Ann. of Math.*, 37 (1936), 782–800.