EQUIVALENCE OF ELEMENTS UNDER AUTOMORPHISMS OF A FREE GROUP

P. J. HIGGINS AND R. C. LYNDON

J. H. C. Whitehead [4, 5] proved by topological means a theorem that enables one to decide whether the elements of a free group represented by two given words are equivalent under an automorphism of the free group. E. S. Rapaport [3] gave a purely algebraic proof of this result. We present here a simplification of her argument. This paper originally appeared as a mimeographed note (Queen Mary College, London, 1962) but is no longer available in that form. We publish it here as an adjunct to J. McCool's paper [1] which immediately follows it.

Whitehead's theorem is essentially equivalent to the assertion that, if w is any word, and w' is an equivalent word of minimum length, then it is possible to pass from w to w' by a succession of automorphisms of an especially simple kind, and in such a way that the lengths of the successive words obtained decrease strictly until minimum length is attained, thereafter remaining constant. The set W of *Whitehead automorphisms* used in the successive steps comprises two sorts. For F the free group on the set X of free generators (which may be taken finite), let L be the set of all *letters*, that is, the set of all generators x in X together with their inverses $\bar{x} = x^{-1}$. Then W contains all those automorphisms which merely permute the letters, together with all automorphisms which, for fixed a in L, carry each generator x into one of x, xa, $\bar{a}x$, or $\bar{a}xa$. The assertion is a consequence of the analogous result for *cyclic words*, that is, cyclically ordered sets of letters with no pair of inverses adjacent, and is more easily proved for cyclic words. The length $|w|$ of a cyclic word w is the number of elements in the cyclically ordered set. The proof applies without change to finite sets of cyclic words, and the theorem follows with some effort for finite sets of ordinary words, the successive Whitehead automorphisms now reducing the *sum* of the lengths of the words until the minimum value is attained. (Lemma 2 of [1] leads easily to a proof of this result).

Whitehead's result follows by an obvious induction from the following

THEOREM. *If w and w' are cyclic words equivalent under an automorphism of the free group F, and if w' has minimum length for their equivalence class, then there exist $T_1, T_2, \ldots, T_n$ in W $(n \geqslant 0)$ such that, writing $w_i = wT_1 T_2 \ldots T_i$ $(0 \leqslant i \leqslant n)$, one has $w_n = w'$ and*

$$|w_1|, |w_2|, \ldots, |w_n| \leqslant |w| \tag{1}$$

with strict inequality unless w also has minimum length.

The hard part of the theorem is contained in the following lemma, whose proof we postpone.

LEMMA. *Let $u = wS$, $v = wT$, with $S, T \in W$, and let $|u| \leqslant |w|$, $|v| \leqslant |w|$, with either $|u| < |w|$ or $|v| < |w|$. Then $v = uS_1 S_2 \ldots S_n$ for some $S_1, S_2, \ldots, S_n \in W$*

Received 2 December, 1972.

[J. LONDON MATH. SOC. (2), 8 (1974), 254–258]

($n \geqslant 0$), such that, writing $u_i = uS_1 S_2 \dots S_i$ for all $0 \leqslant i \leqslant n$, one has $|u_i| < |w|$ for all $0 < i < n$.

To establish the theorem we observe that since W contains Nielsen's generators (see [2]) for the automorphism group, w can be connected to w' by some "path" as in the statement of the theorem except possibly not satisfying (1). If (1) is not satisfied, then $n \geqslant 2$, and the maximum value $m = |w_i|$ for $0 < i < n$ must be at least as large as $|w|$. Moreover, either $m > |w| = |w'|$ or $m \geqslant |w| > |w'|$. In either case, choosing i maximal for $|w_i| = m$, $0 < i < n$, one has $|w_{i-1}| \leqslant |w_i|$ and $|w_i| > |w_{i+1}|$. We may therefore use the lemma to obtain a new path by deleting w_i and passing from w_{i-1} to w_{i+1} by way of a succession of words of lengths less than m. The new path then has corresponding $m' \leqslant m$, and in any case contains one word fewer of length m. The conclusion now follows by induction first on m and second on the number of w_i of length m.

We now introduce notation to be used in the proof of the lemma. If S is a Whitehead automorphism carrying each generator x into one of x, xa, $\bar{a}x$, $\bar{a}xa$, we denote S by the symbol (A, a), where A consists of a together with all those *letters* $y \neq a, \bar{a}$ that are carried into either ya or $\bar{a}ya$. (Thus, if $x \to \bar{a}x$, then $\bar{x} \in A$, while if $x \to \bar{a}xa$, then $x, \bar{x} \in A$). It is clear that

$$(A, a)^{-1} = (A - a + \bar{a}, \bar{a}). \tag{i}$$

It is also clear that, if A' is the complement of A in L, then

$$(A, a)(A', \bar{a})^{-1} = (A, a)(A' - \bar{a} + a, a)$$

is the inner automorphism $(L - \bar{a}, a)$ carrying each element w of F into $\bar{a}wa$. Since inner automorphisms leave cyclic words unchanged, this implies that

$$w(A, a) = w(A', \bar{a}) \text{ for any cyclic word } w. \tag{ii}$$

For $A, B \subseteq L$, and any cyclic word w, we denote by $(A.B)_w$ the number of consecutive pairs of letters in w of either of the forms $x\bar{y}$ or $y\bar{x}$, where $x \in A$ and $y \in B$. (If $w = x$ has length 1, we count xx as a consecutive pair.) We shall ordinarily suppress reference to w in this symbol. We write $A + B$ for $A \cup B$ only if $A \cap B = \varnothing$, and $A - B$ for $A \cap B'$ only if $B \subseteq A$. Then it is clear that

$$\left.\begin{aligned} &A.B \geqslant 0, \quad A.B = B.A, \quad (A+B).C = A.C + B.C, \\ &(A-B).C = A.C - B.C, \quad a.a = 0; \\ &\text{also } a.L = \bar{a}.L \text{ is the total number of letters } a \text{ and } \bar{a} \text{ in } w. \end{aligned}\right\} \tag{iii}$$

If $S = (A, a)$, we write $\Delta_w(S)$, or, more simply, $\Delta(S)$ for $|wS| - |w|$. We shall show that

$$\Delta(S) = A.A' - a.L. \tag{iv}$$

First, we let w' be the unreduced cyclic word obtained from w be replacing each letter x by xS, and let w'' be the result of deleting all parts $a\bar{a}$ from w'. We shall show that w'' is reduced, whence it follows that $w'' = wS$. Since w is reduced, and w' is obtained from w by inserting letters a and $\bar{a}$, w' can contain parts $x\bar{x}$ only of the form $a\bar{a}$ or $\bar{a}a$, where at least one of the letters is newly inserted. Now a new a can arise only following an old x, with x in $A - a$, hence never following an $\bar{a}$;

similarly a new $\bar{a}$ can arise only preceding an old $\bar{x}$, with x in $A-a$. It follows that w' contains no part $\bar{a}a$. To prove that w'' is reduced, it remains to show that w' contains no part $xa\bar{a}\bar{x}$. Since one of $a, \bar{a}$ must be new, we can suppose, by symmetry, that a is new, and so follows an old x, with x in $A-a$. If $\bar{a}$ is old, then it occurs in w in a context $x\bar{a}\bar{y}$, giving rise in w' to a part $xa\bar{a}\bar{y}$ or $xa\bar{a}\bar{a}\bar{y}$, the latter if $y \in A-a$; in particular, since $x \in A-a$, $xa\bar{a}\bar{y}$ does not arise if $y = x$. If $\bar{a}$ is new, then w contains $x\bar{y}$, where $y \in A-a$ but $y \neq x$, giving rise to $xa\bar{a}\bar{y}$ with $y \neq x$. It follows that w'' is reduced, and $w'' = wS$.

It is now clear that $\Delta(S) = \Delta_1 - \Delta_2$, where Δ_1 is the number of new a or $\bar{a}$ in w' that do not cancel in passing to w'', while Δ_2 is the number of new a or $\bar{a}$ that cancel against an old $\bar{a}$ or a already present in w. We have seen above that a new a, introduced following $x \in A-a$, will *not* be followed in w' by an $\bar{a}$ if and only if x occurs in w in a context $x\bar{y}$ for some $y \in A'$; similarly, a new $\bar{a}$ preceding $\bar{x}$ will not be preceded by an a if and only if $\bar{x}$ occurs in w in a context $y\bar{x}$ for some $y \in A'$. Thus $\Delta_1 = (A-a).A'$, the number of such parts $x\bar{y}$ and $y\bar{x}$ in w. It was also seen that a new a, introduced following $x \in A-a$, if followed by an old $\bar{a}$ if and only if w contained $x\bar{a}$; similarly, a new $\bar{a}$ is preceded by an old a if and only if w contained $a\bar{x}$. Thus $\Delta_2 = (A-a).a$. It follows that

$$\Delta(S) = (A-a).A' - (A-a).a = A.A' - a.(A+A') + a.a.$$

Since $A+A' = L$ and $a.a = 0$, this gives (iv).

To prove the lemma, consider a fixed cyclic word w. Let $u = wS$ and $v = wT$, where $S, T \in W$, and suppose that

$$|u| \leqslant |w|, |v| \leqslant |w| \text{ with either } |u| < |w| \text{ or } |v| < |w|. \tag{2}$$

It follows that

$$|w| > \tfrac{1}{2}(|u| + |v|). \tag{3}$$

It will be shown that there exist $S_1, S_2, \ldots, S_n$ in W (in fact with $n \leqslant 4$) such that $uS_1 S_2 \ldots S_n = v$ and

$$|uS_1 S_2 \ldots S_i| < |w| \text{ for all } i,\ 0 < i < n. \tag{4}$$

We first dispose of some special cases.

Case 1. *Suppose that T effects a permutation of the letters.*

Then $|v| = |w|$. Clearly $S^* = T^{-1} S^{-1} T$ is in W since S is in W. Setting $n = 2$, $S_1 = T$ and $S_2 = S^*$, we have $uS_1 S_2 = uS^{-1} T = v$, and (4) holds since $|uS_1| = |uT| = |u| < |w|$.

In view of this case, we may suppose that neither S nor T is a permutation. Accordingly, we now write $S = (A, a)$ and $T = (B, b)$.

Case 2. *Suppose that $A \cap B = \varnothing$, and $b = \bar{a}$.* Then $uS_1 = v$, where $S_1 = S^{-1} T = (A-a+\bar{a}, \bar{a})(B, \bar{a}) = (A+B-a, \bar{a})$ is in W, and (4) holds vacuously with $n = 1$.

Case 3. *Suppose that $A \cap B = \varnothing$, and $\bar{a} \in B'$.* We shall first show that $|uT| < |w|$. Let w', u' be the unreduced cyclic words obtained from w, u by replacing each letter x by xT. Since $u = wS$, and $a, \bar{a} \notin B$, all letters x or $\bar{x}$ in w with $x \in B-b$ are preserved in u, and no new ones are introduced. It follows that $|u'|-|u| = |w'|-|w|$. We have

seen that w', u' contain no parts $\bar{b}b$, and that wT, uT are obtained from them by deleting all parts $b\bar{b}$. Now, a part $b\bar{b}$ in w' must occur in one of the contexts $xb\bar{b}$, $b\bar{b}y$ or $xb\bar{b}\bar{y}$ arising from parts $x\bar{b}$, $b\bar{y}$ or $x\bar{y}$ in w, where $x, y \in B-b$. Since $x, y, b \notin A$, and $x, y, b \neq \bar{a}$, any such part in w is preserved in $u = wS$, and so gives rise to a part $b\bar{b}$ in u'. Thus, at least as many cancellations are possible in u' as in w', and we conclude that $|uT|-|u| \leqslant |wT|-|w|$. (In fact equality holds, but we do not need this.) Since $wT = v$, and $|u|+|v| < 2|w|$ by (2), we have $|uT| \leqslant |u|+|v|-|w| < |w|$, as asserted.

Now $v = uS^{-1}T = uTS^{*-1}$, where $S^* = T^{-1}ST$. It is easy to verify that $S^* = S$ if $\bar{b} \in A'$, while $S^* = (A+b-\bar{b}, a)$ if $\bar{b} \in A$. In either case S^* is in W, and the conclusion follows with $n = 2$, $S_1 = T$ and $S_2 = S^{*-1}$.

Case 4. *Suppose that* $A \cap B = \varnothing$. Since $a \in A$, $b \in B$, this implies $a \neq b$. In view of Case 2 we can assume also that $a \neq \bar{b}$. Further, in view of Case 3, we can assume that $\bar{a} \in B$, and, symmetrically, that $\bar{b} \in A$. If we define $S' = (A, \bar{b})$, $T' = (B, \bar{a})$, and write Δ for Δ_w, we find, using the fact that $\bar{a}.L = a.L$ and $\bar{b}.L = b.L$, that $\Delta(S')+\Delta(T') = \Delta(S)+\Delta(T)$. Since, by (3), $\Delta(S)+\Delta(T) = |u|+|v|-2|w| < 0$, one of $\Delta(S')$, $\Delta(T')$ must be negative. By symmetry, we may suppose that $\Delta(T') < 0$. Setting $w_1 = wT'$, we therefore have $|w_1| < |w|$. Also, $w_1 = uS_1$, where

$$S_1 = S^{-1}T' = (A-a+\bar{a}, \bar{a})(B, \bar{a}) = (A+B-a, \bar{a})$$

is in W. Now $v = wT = w_1 T'^{-1} T$, and

$$T'^{-1}T = (B-\bar{a}+a, a)(B, b) = S_2(B-\bar{a}+a-b+\bar{b}, a) = S_2 S_3,$$

where S_2 is the permutation carrying a into b, b into $\bar{a}$, and leaving fixed all letters other than $a, \bar{a}, b, \bar{b}$. Thus $v = uS_1 S_2 S_3$ with S_1, S_2, S_3 in W, and, since S_2 is a permutation, $|uS_1 S_2| = |uS_1| = |w_1| < |w|$, as required.

We now prove the general result, for $S = (A, a)$, $T = (B, b)$, by reduction to the case $A \cap B = \varnothing$. We first observe that (3) can be written $\Delta(S)+\Delta(T) < 0$, which, according to (iv), gives

$$A.A'+B.B'-a.L-b.L < 0. \tag{3*}$$

For convenience, we now write $A_1 = A$, $A_2 = A'$, $B_1 = B$, $B_2 = B'$ and $P_{ij} = A_i \cap B_j$. It is easily verified that

$$A_1.A_2+B_1.B_2 = P_{11}.P_{11}'+P_{22}.P_{22}'+2P_{12}.P_{21} \geqslant P_{11}.P_{11}'+P_{22}.P_{22}',$$

and, interchanging B_1 and B_2, that $A_1.A_2+B_1.B_2 \geqslant P_{12}.P_{12}'+P_{21}.P_{21}'$. Since, by (3*), $A_1.A_2+B_1.B_2-a.L-b.L < 0$, we have

$$\left.\begin{aligned} P_{11}.P_{11}'+P_{22}.P_{22}'-a.L-b.L < 0, \\ P_{12}.P_{12}'+P_{21}.P_{21}'-a.L-b.L < 0. \end{aligned}\right\} \tag{5}$$

Let x stand for any one of the letters a, $\bar{a}$, b, $\bar{b}$, which need not all be distinct, and denote by $P(x)$ the set P_{ij} to which x belongs; clearly $\bar{x} \notin P(x)$. We shall deduce from (5) that at least one of the Whitehead automorphisms $(P(x), x)$ decreases the

length of w. First, if each of the four sets P_{ij} contains one of the letters a, $\bar{a}$, b, $\bar{b}$, then

$$\begin{aligned}\sum\Delta(P(x), x) &= \sum P(x).P(x)' - \sum x.L \\ &= \sum P_{ij}.P_{ij}' - 2(a.L + b.L) \\ &< 0 \text{ by (5)},\end{aligned}$$

and it follows that some $\Delta(P(x), x) < 0$. Second, if P_{ij}, say, contains none of these letters, then, writing $a_1 = a$, $a_2 = \bar{a}$, $b_1 = b$, $b_2 = \bar{b}$, we have $a_i \in A_i = P_{i1} + P_{i2}$, $b_j \in B_j = P_{1j} + P_{2j}$, whence $a_i \in P_{ik}$ $(k \neq j)$ and $b_j \in P_{hj}$ $(h \neq i)$. Thus

$$\Delta(P(a_i), a_i) + \Delta(P(b_j), b_j) = P_{ik}.P_{ik}' + P_{hj}.P_{hj}' - a.L - b.L < 0$$

by (5), and again some $\Delta(P(x), x) < 0$.

Interchanging S and T if necessary, we can assume that $\Delta(P(x), x) < 0$ for $x = a$ or $\bar{a}$. Since, by (ii), S can be replaced by $(A', \bar{a})$, we can even assume that $x = a$. Then $P(x)$ must be either P_{11} or P_{12}, and, replacing T by $(B', \bar{b})$ if necessary, we can assume that $P(x) = P_{12}$. Thus we may suppose that $a \in B'$ and $\Delta(A \cap B', a) < 0$. Setting $U = (A \cap B', a)$ and $w_1 = wU$, we have $|w_1| < |w|$. Now $w = u(A', \bar{a})^{-1} = u(A' - \bar{a} + a, a)$. Hence $w_1 = uS_1$, where

$$S_1 = (A' - \bar{a} + a, a)(A \cap B', a) = (A' \cup B' - \bar{a}, a)$$

is in W. Moreover, $w_1 = w(A \cap B', a)$, $v = w(B, b)$, and $(A \cap B') \cap B = \varnothing$. Since $|w_1| < |w|$ and $|v| \leqslant |w|$, Case 4 provides a path from w_1 to v with at most three steps, and with all intermediate words shorter than w. This completes the proof of the lemma, and with it the theorem.

References

1. J. McCool, " A presentation for the automorphism group of a free group of finite rank ", *J. London Math. Soc.*, 8 (1974), 259–266.
2. J. Nielsen, " Die Isomorphismengruppe der freien Gruppen ", *Math. Ann.*, 91 (1924), 169–209.
3. E. S. Rapaport, " On free groups and their automorphisms ", *Acta. Math.*, 99 (1958), 139–163.
4. J. H. C. Whitehead, " On certain sets of elements in a free group ", *Proc. London Math. Soc.*, 41 (1936), 48–56.
5. J. H. C. Whitehead, " On equivalent sets of elements in a free group ", *Ann. of Math.*, 37 (1936), 782–800.

King's College,
Strand,
London, WC2R 2LS

University of Michigan,
Ann Arbor,
Michigan 48104,
U.S.A.