MATH. SCAND. 12 (1963), 209–234

LENGTH FUNCTIONS IN GROUPS

ROGER C. LYNDON

1. Introduction.

Nielsen's proof of the Subgroup Theorem for free groups [2, p. 31] rests on an argument to the effect that a product of elements from a free group cannot reduce to the trivial element, provided that the amount of cancellation in forming the product of any three consecutive elements is not too great. We seek here to isolate certain ideas underlying this and similar cancellation arguments. To this end we consider a group G equipped with a "length function", assigning to each element g in G as length a non-negative integer $|g|$. A set of axioms is obtained, necessary and sufficient for the function $|g|$ to be the restriction to G of the usual length function on some free group F containing G, or alternatively, of the usual length function on some free product F (without amalgamation) containing G. Our main result concerns the structure of an arbitrary group G with a length function satisfying these axioms, and contains, separately, the Nielsen Subgroup Theorem and the Kurosh Subgroup Theorem [1, p. 17].

The core of our argument is an abstract reformulation of Nielsen's argument, adapted to the complications that arise from the possibility of elements g such that $|g^2| \leqq |g|$.

Alternative approaches to this question are possible. If x and y are words in a free group, there exist elements x_1, y_1 and z such that $x = x_1 z$, $y = y_1 z$, and $xy^{-1} = x_1 y_1^{-1}$, without cancellation, that is, with

$$|x| = |x_1| + |z|, \qquad |y| = |y_1| + |z|, \qquad |xy^{-1}| = |x_1| + |y_1^{-1}| .$$

The amount of cancellation, that is, the amount of agreement between x and y, is

$$|z| = d(x,y) = \tfrac{1}{2}[|x| + |y| - |xy^{-1}|] .$$

Here we deal entirely with the numerical function $d(x,y)$, and do not assume that, with every pair of elements x and y, G contains their greatest common right divisor z; in this connection we are led to introduce ideal divisors. An alternative approach would be to take as primitive the

Received May 18, 1962.
This work was supported in part by the U. S. National Science Foundation.

operation of forming greatest common right divisors; with this it might be possible to dispense with some of the metric properties of the length function.

We note also that the assumption that the values $|g|$ of the length function are non-negative integers plays a very limited role; it is used essentially only in establishing a well ordering of G with special properties that enables us to define a generalized Nielsen basis (Section 5). A modest illustration of this measure of flexibility is provided by the observation that the axioms A1–A5 (or A0–A5) below are preserved in passing from a function $|g|$ to a function $\|g\|$ defined by $\|1\|=0$ with $\|g\|=a|g|+b$ otherwise, for a and b positive real numbers.

2. The axioms.

We consider an arbitrary group G, equipped with a function assigning to each element x of G an integer $|x|$. We wish to reserve the notation x^m for upper indices. Hence we avoid exponents, adopting the notation x^- for the inverse of x, and write out xx for the square of x. Define

$$d(x,y) = \tfrac{1}{2}[|x|+|y|-|xy^-|];$$

note that $d(x,y)$ is an integer or a half integer.

We shall be interested only in functions $|x|$ satisfying the following axioms:

A1. $|x|=0$ *if and only if* $x=1$;

A2. $|x^-|=|x|$;

A3. $d(x,y)\geqq 0$;

A4. $d(x,y)<d(x,z)$ *implies that* $d(y,z)=d(x,y)$;

A5. $d(x,y)+d(x^-,y^-)>|x|=|y|$ *implies that* $x=y$.

The content of A1 and A2 is clear enough. In particular, they imply that $d(x,1)=0$ and that $d(x,y)=d(y,x)$. Axiom A3 is equivalent to the "triangle axiom": $|xy^-|\leqq|x|+|y|$. Axioms A1 and A3 imply that $|x|=d(x,x)\geqq 0$. Axiom A4 is a "triangle axiom" of a different nature: the two smaller of the three "measures of agreement" among three elements are equal; in practice it often takes the form that $d(x,y)\geqq m$, $d(x,z)\geqq m$ implies $d(y,z)\geqq m$. Axiom A5, relating agreement on the right with agreement on the left, will be discussed later.

We derive four immediate consequences of these axioms, using, in fact, only axioms A2 and A4.

(2.1) PROPOSITION. $d(xy,y)+d(x,y^-)=|y|$.

PROOF. By definition, $2d(xy,y)=|xy|+|y|-|x|$, and $2d(x,y^{-})=|x|+|y^{-}|-|xy|$. By A2, $|y^{-}|=|y|$.
Addition gives (2.1).

(2.2) PROPOSITION. $d(x,y^{-})+d(y,z^{-})\geqq|y|$,
implies that

$$|xyz| \leqq |x|-|y|+|z| .$$

PROOF. The hypothesis gives $d(y,z^{-})\geqq|y|-d(x,y^{-})$ while (2.1) gives $d(xy,y)=|y|-d(x,y^{-})$. By A4 it follows that $d(xy,z^{-})\geqq|y|-d(x,y^{-})$. Expanded, this last inequality becomes

$$|xy|+|z^{-}|-|xyz| \geqq 2|y|-|x|-|y^{-}|+|xy| ,$$

which, with $|y^{-}|=|y|$, $|z^{-}|=|z|$, gives (2.2).

(2.3) PROPOSITION. $d(x,y^{-})+d(y,z^{-})<|y|$
implies that

$$d(xy,z^{-}) = d(y,z^{-}) .$$

PROOF. The hypothesis gives $d(y,z^{-})<|y|-d(x,y^{-})$, while (2.1) gives $d(xy,y)=|y|-d(x,y^{-})$. By A4 it follows that $d(xy,z^{-})=d(y,z^{-})$.

(2.4) PROPOSITION. $d(x,y)+d(x^{-},y^{-})\geqq|x|=|y|$
implies that

$$|(xy^{-})(xy^{-})| \leqq |xy^{-}| .$$

PROOF. The hypothesis gives $d(x,y)+d(y^{-},x^{-})\geqq|y|$, whence, by (2.2),

$$|xy^{-}x| \leqq |x|-|y|+|x| = |x| .$$

Now $|xy^{-}x|\leqq|x|$ gives

$$2d(xy^{-},x^{-}) = |xy^{-}|+|x^{-}|-|xy^{-}x| \geqq |xy^{-}| .$$

Also, $2d(x,y)=|x|+|y|-|xy^{-}|$. Since $|x^{-}|=|x|$, addition gives

$$2d(xy^{-},x^{-})+2d(x,y) \geqq 2|x| .$$

Now (2.2), applied to xy^{-}, x, and y^{-}, gives

$$|xy^{-}xy^{-}| \leqq |xy^{-}|-|x|+|y^{-}| = |xy^{-}| .$$

The content of (2.4), which was obtained from A2 and A4 alone, is very close to that of Axiom A5. For this reason it seems worthwhile to show that A5 is nonetheless independent of A1–A4. For this purpose we take G to be any group containing a non-trivial subgroup H of index two. Let m and n be integers, with $0<m<n$. Define $|1|=0$; $|x|=m$ for

$x \in H$, $x \neq 1$; and $|x| = n$ for $x \notin H$. Clearly A1 and A2 hold. We find that $d(x,1)=0$, $d(x,x)=|x|$, and that, for 1, x, y all different, $d(x,y)=\frac{1}{2}m$ if either x or y is in H, while $d(x,y)=n-\frac{1}{2}m>\frac{1}{2}n$ otherwise. It follows that A3 and A4 hold. However, A5 fails, since, taking x, $y \notin H$ with $x \neq y$, we have $d(x,y)+d(x^-,y^-)=2n-m>n=|x|=|y|$. Here (2.4) tells us only that $|xy^-xy^-| \leqq |xy^-|$, that is, that xy^- is non-Archimedean in a sense defined below.

We call an element x such that $|x|<|xx|$ *Archimedean*, in view of the following proposition (where, exceptionally, superior numerals indicate powers).

(2.5) PROPOSITION. *The lengths* $|x^n|$ *are unbounded if and only if* x *is Archimedean.*

PROOF. Suppose that x is Archimedean. Then $d(x,x^-)=d<\frac{1}{2}|x|$, and, since $x \neq 1$, $|x| \geqq 1$. For $n \geqq 1$, assume inductively that $d(x^n,x^-)=d$ and $|x^n| \geqq n$. From $d(x^n,x^-)+d(x,x^-)=2d<|x|$ it follows by (2.3) that $d(x^{n+1},x^-)=d(x,x^-)=d$; moreover,

$$|x^{n+1}| = |x^n|+|x|-2d > |x^n| \geqq n ,$$

whence $|x^{n+1}| \geqq n+1$. This completes the induction. Suppose now that x is not Archimedean. If x has finite order, then the finite set of integers $|x^n|$ is bounded; we may suppose then that x has infinite order. Now $|x^2|<|x|$ would give

$$d(x,x^-) > \tfrac{1}{2}|x|, \qquad d(x,x^-)+d(x^-,x) > |x| = |x^-| ,$$

and, by A5, $x=x^-$, hence $x^2=1$, contrary to hypothesis. For $n \geqq 2$, assume inductively that $|x|=|x^2|=\ldots=|x^n|$. Then

$$d(x^{n-1},x^-)+d(x,x^-) = \tfrac{1}{2}|x|+\tfrac{1}{2}|x| = |x| ,$$

whence (2.2) gives $|x^{n-1}xx| \leqq |x^{n-1}|-|x|+|x|$, hence $|x^{n+1}| \leqq |x|$. But $|x^{n+1}|<|x|$ would give

$$d(x^n,x^-) = d(x,x^{-n}) = \tfrac{1}{2}[|x^n|+|x|-|x^{n+1}|] > \tfrac{1}{2}|x| ,$$

hence $d(x^n,x^-)+d(x,x^{n-}) > |x|=|x^n|$, and, by A5, $x^n=x^-$, $x^{n+1}=1$, contrary to hypothesis. Thus we conclude that $|x^{n+1}|=|x|$, completing the induction.

Let *A*0 be the *Archimedean axiom*:

A0. $x \neq 1$ *implies that* $|x|<|xx|$.

Let A1′ be the following weakened form of Axiom A1:

A1′. $|1|=0$.

(2.6) PROPOSITION. *The set of axioms* A0, A1,... A5 *is equivalent to the set* A0, A1′, A2, A3, A4.

PROOF. Clearly the former set implies the latter. For the converse, assume A0, A1′, A2, A3, A4. To prove A1, we must show that $|x|=0$ implies $x=1$. If $|x|=0$, using A1′ we have $d(x,1)+d(x^-,1)=0+0=0=|x|=|1|$; by (2.4), which follows from A2 and A4, we have $|xx|\leqq|x|$. Then by A0 it follows that $x=1$. To establish A5, assume that $d(x,y)+d(x^-,y^-)>|x|=|y|$; by (2.4) again we have $|(xy^-)(xy^-)|\leqq|xy^-|$, which by A0 implies $xy^-=1$, hence $x=y$.

If F is the free group on a set X of free generators, then the *associated length function* $|x|$ assigns to each x in F the length of the unique reduced word, in the generators from the set X, representing x.

(2.7) PROPOSITION. *The length function associated with a set of free generators for a free group satisfies Axioms* A0, A1′, A2, A3, A4. *It also satisfies the following condition*:

C0: *$d(x,y)$ is always an integer.*

PROOF. A0 becomes obvious upon writing a word x as the conjugate of a cyclically reduced word. Then $d(x,y)$ is the length of the longest sequence of letters on the right ends of the (reduced) words where x and y agree. A1, A2, A3 and C0 are immediate. A4 follows from the observation that if both x and y agree with z in their last m letters, then they agree with each other in their last m letters.

If F is the free product of a family of pairwise disjoint subgroups F_a, then each element x in F has a unique representation as a product $x=x_1x_2\ldots x_n$, where each $x_i\neq 1$, each x_i is in some F_a, and where no consecutive x_i and x_{i+1} are in the same F_a; the *associated length function* assigns to x the value $|x|=n$.

(2.8) PROPOSITION. *The length function associated with a free decomposition (without amalgamation) of a group satisfies Axioms* A1, A2, A3, A4, A5. *It also satisfies the following two conditions*:

C1. *if $x\neq 1$ and $|xx|\leqq|x|$, then $|x|$ is odd*;

C2. *for no x is $|xx|=|x|+1$.*

PROOF. If elements x and y have normal representations $x=x_nx_{n-1}\ldots x_1$ and $y=y_my_{m-1}\ldots y_1$, let k be the greatest integer such that $x_1=y_1,\ldots,x_k=y_k$; if $n,m>k$ and x_{k+1} and y_{k+1} lie in the same free component (but are not equal) then $d(x,y)=k+\frac{1}{2}$; otherwise $d(x,y)=k$. With this, the verification of A1, A2, A3, A4 is routine. For A5, the hypothesis that $d(x,y)+d(x^-,y^-)>|x|=|y|$ implies (using $[m]$ for greatest integer in m) that $[d(x,y)]+[d(x^-,y^-)]\geqq|x|=|y|$, whence the number of letters in which x and y agree on the right end plus the number in which they agree on the left end add up to a number not smaller than the common length of x and y; it follows that x and y are identical.

For C1, we observe that the non-Archimedean elements x, satisfying $|xx|\leqq|x|$, are just the conjugates of elements from the free components F_a; thus, if $x\neq 1$, it has normal form

$$x = x_1x_2\ldots x_kx_{k+1}x_k^-\ldots x_2^-x_1^- ,$$

and length $|x|=2k+1$.

For C2, we may reduce consideration to the case that x is cyclically reduced, $x=x_nx_{n-1}\ldots x_1$. Then, according as x_n and x_1 lie in the same or different free components F_a, we have $|xx|=2n$ or $|xx|=2n-1$. In the second case, $|xx|=|x|+1$ implies $n=2$, whence $x=x_2x_1$ with x_2 and x_1 in the same component, so that $x=x_2x_1$ is not in normal form.

It is easy to see that C0 is not a consequence of A0–A4, and that neither of C1 and C2 is a consequence of A1–A5 together with the other. In this limited sense, these conditions (which we shall not refer to again until Section 8) are necessary. However, their rather superficial nature is indicated by the following observations. First, if any length function $|x|$ on G satisfies A1–A5, then the new length function $|x|_1=2|x|$ will also satisfy A1–A5, and C0 and C2 in addition. Second, if $|x|$ satisfies A1–A5, the new function defined by setting $|x|_2=2|x|+1$, except that $|1|_2=0$, will also satisfy A1–A5 and C1 and C2 in addition. Moreover, the set of Archimedean elements is the same under all three length functions.

3. Ideal divisors.

We define the length $|U|$ of any non-empty subset U of G to be the smallest value of $d(x,y)$ for elements x and y of U. Given any z in G, it follows by A4 that if $d(z,x)\geqq|U|$ for any single x in U, then the same is true for all x in U. We write (U) for the set of all z such that $d(z,x)\geqq|U|$ for some (and so all) x in U. A set U is an *ideal* if $(U)=U$.

Clearly every pair of elements, x and y, generate an ideal $U=(x,y)$, with $|U|=d(x,y)$; and, conversely, every ideal is generated by two of its elements (not necessarily distinct). The unit ideal is $(1)=G$, with length $|G|=0$.

In anticipation of Section 8, we note that a free group or free product is a "principal ideal group" in the sense that every ideal there is generated by a single element.

If two ideals, U and V, have non-empty intersection, then one is included in the other; in fact, $U \subset V$ if and only if $|V| < |U|$. To see this, taking x in $U \cap V$, we observe that U is characterized by the condition that $d(z,x) \geqq |U|$, while V is characterized by the weaker condition that $d(z,x) \geqq |V|$.

It follows that, if U is any proper ideal, $U \neq G$, there is a smallest ideal U' properly containing U. Since then $|U'| < |U|$, and the $|U|$ are non-negative integers, there is associated with U a unique chain of ideals $C(U)$: $U, U', U'', \ldots, U^{k(U)}$, ending, for some $k(U) \geqq 0$, with $U^{k(U)} = G$.

We start with any well ordering, $U \prec V$, of the set of all ideals, and derive from it a new well ordering, $U < V$, with certain special properties. First, we well order the chains $C(U)$ by the inverse lexicographical order based upon the order $U \prec V$. Then we define $U < V$ to hold just in case $C(U) < C(V)$ under this order. Thus $U < V$ if and only if some $U^p = V^q$, $0 \leqq p$, $q \leqq k(U)$, $k(V)$, and either $p = 0$, $q > 0$, or else p, $q > 0$ and $U^{p-1} \prec V^{q-1}$.

For each x in G, we define $U(x)$ to be the smallest ideal U such that $x \in U$ and $|U| \leqq \frac{1}{2}|x|$. The crucial property of the well ordering of ideals is then the following.

(3.1) PROPOSITION. *If* $|y| \leqq |x|$, $|y'| \leqq |x'|$, $|U(y)| = |U(y')|$, $U(y) < U(y')$, *and* $x \in U(y)$, $x' \in U(y')$, *then* $U(x) < U(x')$.

PROOF. $U(y)^p = U(y')^q$ for some $p,q \geqq 0$. Now $p = 0$ and $q > 0$ is impossible, since $|U(y)| = |U(y')|$. Thus p, $q > 0$, and $U(y)^{p-1} \prec U(y')^{q-1}$. Now $x \in U(y)$ and $|U(y)| \leqq \frac{1}{2}|y| \leqq \frac{1}{2}|x|$ implies that $U(y) \supseteqq U(x)$, hence $U(y) = U(x)^h$ for some $h \geqq 0$; similarly $U(y') = U(x')^k$ for some $k \geqq 0$. But now we have $U(x)^{h+p} = U(x')^{k+q}$, with $h+p$, $k+q > 0$, and $U(x)^{h+p-1} \prec U(x')^{k+q-1}$, whence $U(x) < U(x')$.

4. Non-Archimedean elements.

Let N be the set of non-Archimedean elements x, that is, elements x such that $|xx| \leqq |x|$. We define a relation $x \sim y$ between elements of N to hold if and only if $|xy^-| \leqq |x| = |y|$.

(4.1) PROPOSITION. *The relation* $x \sim y$ *is an equivalence relation on* N.

PROOF. It follows immediately from the definition that the relation is reflexive and symmetric. We note that, for elements of N, the relation $x \sim y$ is equivalent to the condition $d(x,y) \geqq \frac{1}{2}|x| = \frac{1}{2}|y|$. To establish transitivity, assume that $x \sim y$ and $y \sim z$, that is, that $d(x,y)$, $d(y,z) \geqq$

$\frac{1}{2}|x| = \frac{1}{2}|y| = \frac{1}{2}|z|$. By A4 it follows that $d(x,z) \geqq \frac{1}{2}|x| = \frac{1}{2}|z|$, that is, that $x \sim z$.

For each non-Archimedean element x in N, let $N(x)$ consist of the equivalence class of x under the relation $x \sim y$, together with the element 1.

(4.2) PROPOSITION. *If x is in N, then $N(x)$ is a group.*

PROOF. We observe first that x in N implies, by definition, that $|xx| \leqq |x| = |x^-|$, hence that $x \sim x^-$. It will now suffice to show that if $x,y \neq 1$, if $x \neq y$, and $x \sim y$, then $xy^- \sim y$. From $x \sim y$ we have $x^- \sim y^-$, that is, $d(x,y), d(x^-,y^-) \geqq \frac{1}{2}|x| = \frac{1}{2}|y|$. If either inequality were strict, addition would give $d(x,y) + d(x^-,y^-) > |x| = |y|$, whence by A5 we should have $x = y$, contrary to hypothesis. Thus both inequalities are in fact equalities, and addition gives $d(x,y) + d(x^-,y^-) = |x| = |y|$, which by (2.4), gives $|(xy^-)(xy^-)| \leqq |xy^-|$, hence xy^- in N. Finally, $d(x,y) = \frac{1}{2}|y|$ implies that $|xy^-| = |x| = |y|$, whence, by definition, $xy^- \sim y$.

The group $N(1)$ clearly consists of the element 1 alone. It is also possible that some $N(x)$ consist of 1 together with a single other element x, of order two. In any case, from the definition of the groups $N(x)$, it is clear that distinct groups $N(x)$ and $N(y)$ have trivial intersection.

We note two corollaries of the above.

(4.3) COROLLARY. *If $x \sim y$ and $x \neq y$, then $d(x,y) = \frac{1}{2}|x|$, $U(x) = U(x^-)$, and $|U(x)| = \frac{1}{2}|x|$.*

(4.4) COROLLARY. *If $U(x) = U(x^-)$ and $|U(x)| = \frac{1}{2}|x|$, then x is in N.*

5. A generalized Nielsen basis.

We wish to impose on G a well ordering, $x < y$, that satisfies the following conditions:

(5.1) $|x| < |y|$ *implies that* $x < y$;

(5.2) $|x| = |y|$ *and* $U(x) < U(y)$ *implies that* $x < y$;

(5.3) $|x| = |y|$, $U(x) = U(y)$, *and* $U(x^-) < U(y^-)$ *implies that* $x < y$;

(5.4) *all the elements in an equivalence class of N under the relation $x \sim y$ occur consecutively, and, if $|x| = |y|$, $U(x) = U(x^-) = U(y) = U(y^-)$, while $x \in N$, $y \notin N$, then $x < y$.*

It is clear that one can realize the first three conditions; moreover, since $x \sim y$ implies $d(x,y) \geqq \frac{1}{2}|x| = \frac{1}{2}|y|$, we have $|x| = |y|$ and $U(x) = U(y)$, while $x \sim x^-$ and $y \sim y^-$ gives also $U(x^-) = U(x)$, $U(y^-) = U(y)$: the fourth condition is compatible with the first three. We suppose henceforth that G is well ordered by a fixed relation $x<y$ with these properties.

For each x in G define $G(x)$ to be the subgroup generated by all y in G such that $y<x$. Define X to be the set of those elements x in G such that $x \notin G(x)$. We note in particular that, since $1 \in G(x)$ for all x, as a matter of definition, it follows that $1 \notin X$.

(5.5) PROPOSITION. *The set X generates G.*

PROOF. Let H be the subgroup generated by X. If H is not all of G, let x be the first element of G not in H. Then $y \in H$ for every $y<x$, whence $G(x) \leqq H$. Since $x \notin H$, we have $x \notin G(x)$. But then $x \in X$, whence $x \in H$, contrary to the choice of x.

In the general case, under Axioms A1, A2, A3, A4, A5, but without the Archimedean Axiom A0, X will not be a free set of generators for G, and hence will not satisfy the condition on the amount of cancellation in a triple product upon which Nielsen's proof of the Subgroup Theorem rests. However, it will satisfy certain weaker conditions, from which we shall derive our main results.

Define Y to be the set consisting of all elements x and x^- for $x \in X-N$, together with all elements x such that $x \sim x'$ and $x \neq x'$ for some $x' \in X \cap N$.

For arbitrary $x \in G$, we shall write $\bar{x}$ for the earlier, in the order in G, of x and x^-; (or $\bar{x}=x$ in case $xx=1$).

(5.6) LEMMA. *If $x,y \in Y$ and $x \neq y^-$, then $|xy| \geqq |x|$, $|y|$.*

PROOF. If $x \sim y$, the conclusion follows from (4.3); we assume henceforth that $x \nsim y$. By symmetry we can suppose that $\bar{x} \leqq \bar{y}$. It follows by (5.1) that $|x| \leqq |y|$. Hence it suffices to show that $|xy| \geqq |y|$.

We may suppose that $\bar{x}<\bar{y}$. That $x=y^-$ is excluded by hypothesis, whence $\bar{x}=\bar{y}$ implies $x=y$. Unless $|y| \leqq |xy|$, as desired, we should have, from $x=y$, that $|xx|<|x|$, hence $x=y \in N$, and $x \sim y$, contrary to hypothesis.

If $y \in Y$, then either $\bar{y} \in X$ or else $y \sim y'$ for some $y' \in X$, $y' \neq y$.

Suppose first that $\bar{y} \in X$. Then $|xy|<|y|$, together with $\bar{x}<\bar{y}$, would imply that $xy, x \in G(\bar{y})$, hence $\bar{y} \in G(\bar{y})$, contrary to $\bar{y} \in X$. Thus, in this case, we have $|xy| \geqq |y|$.

The case remains that $y \sim y'$ for some $y' \in X$, $y' \neq y$. Since we have $x \nsim y$, while $y \sim y'$, it follows that $x \neq y'^-$, and, since $y' \in X$, we conclude from the previous case that $|xy'| \geqq |y'|=|y|$. If $|xy'|>|y|$, then $d(x,y'^-)<\frac{1}{2}|x|$, and since, by (4.3), $d(y^-,y'^-)=\frac{1}{2}|y| \geqq \frac{1}{2}|x|$, we conclude by A4 that $d(x,y^-)<\frac{1}{2}|x|$, that is, that $|xy|>|y|$. We may suppose then that

$|xy'| = |y|$. If $|x| < |y|$, then from $d(x,y'^-) = \frac{1}{2}|x|$ and $d(y^-,y'^-) = \frac{1}{2}|y| > \frac{1}{2}|x|$ we conclude by A4 that $d(x,y^-) = \frac{1}{2}|x|$, hence $|xy| = |y|$.

The case now remains that $|xy'| = |y'| = |x|$. Since $y' \in N$, by (4.3) we have $U(y') = U(y'^-)$ and $|U(y')| = \frac{1}{2}|y|$. Now $x \nsim y$, $y \sim y'$, $\bar{x} < \bar{y}$ implies by (5.4) that $\bar{x} < y'$. Since $|x| = |y|$ and $U(x) = U(y') = U(y'^-)$, this implies, by (5.1), (5.2), and (5.3), that $U(x^-) \leqq U(x)$. Now $U(x) = U(x^-)$, with $|U(x)| = |U(y')| = \frac{1}{2}|y'| = \frac{1}{2}|x|$ would, by (4.4), imply that $x \in N$; with $y' \in N$ and $|xy'| = |x| = |y'|$ this would imply that $x \sim y'$, hence $x \sim y$, contrary to hypothesis. We conclude that $U(x^-) < U(x)$.

Now
$$d(xy',y') = \tfrac{1}{2}[|xy'| + |y'| - |x|] = \tfrac{1}{2}|xy'| = \tfrac{1}{2}|x| ,$$
whence $U(xy') = U(y')$. Similarly,
$$d\big((xy')^-,x^-\big) = \tfrac{1}{2}[|xy'| + |x| - |y'|] = \tfrac{1}{2}|xy'| = \tfrac{1}{2}|x| ,$$
whence $U\big((xy')^-\big) = U(x^-) < U(y')$. Since $|xy'| = |y'|$, it follows from (5.1), (5.2), and (5.3) that $xy' < y'$. Since also $\bar{x} < y'$, we have xy', $x \in G(y')$, whence $y' \in G(y')$, contrary to $y' \in X$.

This completes the proof of Lemma (5.6).

(5.7) LEMMA. *If* $x,y \in Y$ *and* $|xy| = |x|$, *then* $U(y^-) \leqq U(y)$ *and* $|U(y^-)| = |U(y)| = \frac{1}{2}|y|$.

PROOF. If $\bar{x} \notin X$, then $x \sim x'$ for some $x' \in X$, $x' \neq x$. From $|xy| = |x|$ it follows that $d(x,y^-) = \frac{1}{2}|y|$, whence, by (5.6), $|y| \leqq |x|$. By (4.3), $d(x,x') = \frac{1}{2}|x| \geqq \frac{1}{2}|y|$. It follows by A4 that $d(x',y^-) \geqq \frac{1}{2}|y|$, whence $|x'y| \leqq |x|$, and, by (5.6), $|x'y| = |x'|$. Thus, replacing x by x' if necessary, we can suppose that $\bar{x} \in X$.

Now $|xy| = |x|$ gives
$$d(x,y^-) = \tfrac{1}{2}[|x| + |y| - |xy|] = \tfrac{1}{2}|y| ,$$
whence $|U(y^-)| = \frac{1}{2}|y|$ and $x \in U(y^-)$. Similarly, from
$$d(xy,y) = \tfrac{1}{2}[|xy| + |y| - |x|] = \tfrac{1}{2}|y|$$
it follows that $|U(y)| = \frac{1}{2}|y|$ and $xy \in U(y)$. We assume now that $U(y) < U(y^-)$ and derive a contradiction. By (3.1), since $|y| \leqq |x| = |xy|$, and $xy \in U(y)$, $x \in U(y^-)$, it follows that $U(xy) < U(x)$. On the other hand, from
$$d\big((xy)^-,x^-\big) = \tfrac{1}{2}[|xy| + |x| - |y|] = |x| - \tfrac{1}{2}|y| \geqq \tfrac{1}{2}|x| = \tfrac{1}{2}|xy| ,$$
we conclude that $U\big((xy)^-\big) = U(x^-)$. It now follows from (5.1), (5.2), and (5.3), that $(\overline{xy}) < \bar{x}$.

Now $y = x$, with $|xy| = |x|$, would imply that $y \in N$, which, by (4.3), contradicts $U(y) < U(y^-)$. Also, $y = x^-$ would give $|x| = |xy| = |1| = 0$ and $x = 1$, contrary to $x \in Y$. This establishes that $\bar{y} \neq \bar{x}$. Next, $\bar{y} < \bar{x}$, together with $(\overline{xy}) < \bar{x}$, would give $xy, y \in G(\bar{x})$, hence $\bar{x} \in G(\bar{x})$, contrary to $\bar{x} \in X$. Finally, $\bar{x} < \bar{y}$, together with $(xy) < \bar{x}$, would give $xy, x \in G(\bar{y})$, hence $\bar{y} \in G(\bar{y})$, contrary to $\bar{y} \in X$. This completes the proof that $U(y) < U(y^-)$ is contradictory, and establishes Lemma (5.7).

(5.8) LEMMA. *If* $x,y,z \in Y$ *and* $|xy| = |x|$, $|yz| = |z|$, *then* $y \in N$.

PROOF. From (5.7) and its symmetric counterpart we have $U(y^-) \leqq U(y)$, $U(y) \leqq U(y^-)$, whence $U(y) = U(y^-)$, and also $|U(y)| = \frac{1}{2}|y|$. It follows by (4.4) that $y \in N$.

(5.9) LEMMA. *Let* $x,y,z \in Y$, *with* $y \nsim x$, $y \nsim z$, *and with* $|xy| = |x|$, $|yz| = |z|$. *Then* $|xyz| = |x| - |y| + |z|$.

PROOF. The hypotheses $|xy| = |x|$ and $|yz| = |z|$ are equivalent to the equations $d(x,y^-) = d(y,z^-) = \frac{1}{2}|y|$. Using (5.6) we conclude that $|y| \leqq |x|, |z|$. Using (2.2), from $d(x,y^-) + d(y,z^-) = |y|$ we conclude that $|xyz| \leqq |x| - |y| + |z|$. We assume henceforth that $|xyz| < |x| - |y| + |z|$, and it will suffice to derive from this assumption a contradiction.

Using (5.8) we conclude that $y \in N$.

We next justify the assumption that $\bar{x} \in X$, where $\bar{x}$ is the earlier, in the well ordering of G, of x and x^-. If, in fact, $\bar{x} \notin X$, then $x \sim x'$ for some $x' \in X$, $x' \neq x$. Now $|y| \neq |x|$, for if $|y| = |x|$, then $x,y \in N$ with $|xy| = |x| = |y|$ would imply $y \sim x$, contrary to hypothesis. Since we had $|y| \leqq |x|$, we conclude that $|y| < |x|$. Now $d(x,y^-) = \frac{1}{2}|y|$, while $x \sim x'$ implies that $d(x,x') \geqq \frac{1}{2}|x| > \frac{1}{2}|y|$; by A4 we conclude that $d(x',y^-) = \frac{1}{2}|y|$, that is, that $|x'y| = |x'|$. The assumption that $|xyz| < |x| - |y| + |z|$ implies that

$$d(x,(yz)^-) = \tfrac{1}{2}[|x| + |yz| - |xyz|] = \tfrac{1}{2}[|x| + |z| - |xyz|] > \tfrac{1}{2}y .$$

From this with $d(x,x') > \frac{1}{2}|y|$ we conclude by A4 that $d(x',(yz)^-) > \frac{1}{2}|y|$, hence that $|x'yz| < |x'| - |y| + |z|$. Further, $y \nsim x$ together with $x \sim x'$ implies that $y \nsim x'$. Thus x', in X, satisfies all the original hypotheses on x, and, replacing x by x' if necessary, we can assume henceforth that $\bar{x} \in X$.

The hypotheses and conclusion of the lemma are unaltered if we replace x,y, and z by z^-, y^-, and x^-. Thus we may conclude that $\bar{z} \in X$ as well as $\bar{x} \in X$. Moreover, by symmetry, we can suppose that $\bar{z} \leqq \bar{x}$.

We now treat the case that $z = x^-$. The assumption that $|xyx^-| < |x| - |y| + |x|$ implies as before that $d(x,(yx^-)^-) > \frac{1}{2}|y|$. Since also

$$\begin{aligned} d(x^-,yx^-) &= \tfrac{1}{2}[|x| + |yx^-| - |x^-xy^-|] \\ &= \tfrac{1}{2}[|x| + |x| - |y|] \\ &= |x| - \tfrac{1}{2}|y| , \end{aligned}$$

we have
$$d(x^-,yx^-)+d(x,(yx^-)^-) > |x| = |x^-| = |yx^-| ,$$

and from A5 we conclude that $x^- = yx^-$, whence $y=1$, contrary to the hypothesis that $y \in Y$. This completes this case, showing that $\bar{x} \in X$, $y \in Y$, $y \nsim x$, and $|xy| = |yx^-| = |x|$, implies that $|xyx^{-1}| = |x| - |y| + |x|$.

We turn now to the case that $z = x$. From the assumptions that $\bar{x} \in X$, $y \in Y$, $y \nsim x$, $|xy| = |yx| = |x|$ and $|xyx| < |x| - |y| + |x|$, we must derive a contradiction. Observe that these assumptions remain unaltered if we replace x by x^- and y by y^-. From $d(x,y^-) = \frac{1}{2}|y|$, $d(y,y^-) \geqq \frac{1}{2}|y|$ we conclude that $d(y,x) = \frac{1}{2}|y|$, hence $|yx^-| = |x|$, so that we may infer, from the case $z = x^-$ treated above, that $|xyx^-| = |x| - |y| + |x|$, whence $d(xy,x) = \frac{1}{2}|y|$. The assumption that $|xyx| < |x| - |y| + |x|$ gives $d(xy,x^-) > \frac{1}{2}|y|$. By A4, it follows that $d(x,x^-) = \frac{1}{2}|y|$. Now $|y| = |x|$ would give $d(x,x^-) = \frac{1}{2}|x|$, hence $|xx| = |x|$, $x \in N$, and, with $y \in N$ and $|xy| = |x| = |y|$, would give $y \sim x$, contrary to hypothesis. Thus we may assume that $|y| < |x|$.

Continuing the case $z = x$, we next show that the assumption $d(xy,x^-) > \frac{1}{2}|x|$ implies $U(x) < U(x^-)$. From this assumption, together with the equation
$$\begin{aligned} d((xy)^-,x^-) &= \tfrac{1}{2}[|xy| + |x| - |y^-x^-x|] \\ &= \tfrac{1}{2}[|x| + |x| - |y|] \\ &= |x| - \tfrac{1}{2}|y| > \tfrac{1}{2}|x| , \end{aligned}$$

we conclude by A4 that $d(xy,(xy)^-) > \frac{1}{2}|x| = \frac{1}{2}|xy|$, whence $|xyxy| < |xy|$ and $xy \in N$. (In fact, by A5, it follows that $xyxy = 1$.) The inequalities above now give $U(xy) = U((xy)^-) = U(x^-)$. Now $U(x^-) < U(x)$ would give $xy < \bar{x}$, hence $y, xy \in G(\bar{x})$ and so $\bar{x} \in G(\bar{x})$, contrary to $\bar{x} \in X$. Also $U(x^-) = U(x)$ proves impossible. First, $x \in N$ together with $xy \in N$ and $d(xy,x^-) > \frac{1}{2}|x| = \frac{1}{2}|xy|$ implies $|xyx| < |xy| = |x|$, whence $xy \sim x$ and so $y \sim x$, contrary to hypothesis. Therefore $x \notin N$, while $xy \in N$. But $U(xy) = U((xy)^-) = U(x) = U(x^-)$, whence it follows by (5.4) that $xy < \bar{x}$, leading to a contradiction as before. We must conclude that $U(x) < U(x^-)$.

We now show that the alternative assumption, $d(xy,x^-) \leqq \frac{1}{2}|x|$ also implies $U(x) < U(x^-)$. Write $d(xy,x^-) = d > \frac{1}{2}|y|$. We have, as before, $d(xy,x) = d(x,x^-) = \frac{1}{2}|y|$, and also $U(x^-) = U((xy)^-)$. Now $U(xy) < U(x)$ would imply $y, xy \in G(\bar{x})$, hence $\bar{x} \in G(\bar{x})$, contrary to $\bar{x} \in X$. Moreover $U(xy) = U(x)$ is impossible, since $d(xy,x) = \frac{1}{2}|y| < d$, while xy belongs to the ideal $U_d = (xy,x^-)$ of length $d \leqq \frac{1}{2}|xy|$. Therefore we have $U(xy) > U(x)$. Now the chains of ideals $C(x)$, $C(x^-)$, $C(xy)$ all agree, reading from right to left, up through a common ideal V with $|V| = \frac{1}{2}|y|$, and $C(x^-)$ and $C(xy)$ agree further up through the ideal U_d. That $U(x) < U(xy)$

means either that the chain $C(x)$ has no further members to the left of V (while $C(xy)$ does), or else that the next member W of the chain $C(x)$ to the left of V stands in the relation $W \prec Z$ to the next member Z of $C(xy)$ to the left of V. Since Z is also the next member of $C(x^-)$ to the left of V, this implies that $U(x) < U(x^-)$.

We have now proved, under the assumptions for the case $z = x$, that $U(x) < U(x^-)$. But it was noted that the assumptions hold equally with x replaced by x^- and y by y^-. Thus we may conclude equally that $U(x^-) < U(x)$, providing a contradiction.

We next examine the case that $\bar{z} < y$. Since we had $|y| \leqq |z|$, this implies $|y| = |z|$. If $\bar{y} \notin X$, then $y \sim y'$ for some $y' \in X$, $y' \neq y$. From $y \nsim x$, $y \nsim z$, it follows that $y' \nsim x$, $y' \nsim z$. From $|xy| = |x|$ we have $d(x,y^-) = \frac{1}{2}|y|$. Since $y' \sim y$, $y' \neq y$, gives $d(y,y'^-) = \frac{1}{2}|y| = \frac{1}{2}|y'|$, we conclude, using A4, that $d(x,y'^-) \geqq |y'|$ and hence $|xy'| \leqq |x|$. Since $y' \nsim x$, it follows by (5.6) that $|xy'| = |x|$. We have symmetrically that $|y'z| = |z|$. Thus y' satisfies all the same hypotheses as y, and, replacing y by y' if necessary, we can suppose that $\bar{y} \in X$. From $d(y,z^-) = \frac{1}{2}|y| = \frac{1}{2}|z|$ and $y \in N$ we conclude that $U(y) = U(y^-) = U(z^-)$, while $y \nsim z$ implies that $U(z) \neq U(z^-)$. From $\bar{z} < y$ we infer that $U(z) < U(z^-)$. Now

$$d(yz,z) \;=\; \tfrac{1}{2}[|z| + |z| - |y|] \;=\; \tfrac{1}{2}|z| \;=\; \tfrac{1}{2}|y|$$

gives $U(yz) = U(z)$, and $d\big((yz)^-,y^-\big) = \frac{1}{2}|y| = \frac{1}{2}|yz|$ gives $U\big((yz)^-\big) = U(y^-)$. But $U\big((yz)^-\big) = U(y^-)$ together with $U(yz) = U(z) < U(y)$ implies that $yz < y$. Thus $\bar{z}, yz \in G(\bar{y})$, whence $\bar{y} \in G(\bar{y})$, contrary to $\bar{y} \in X$.

We have shown that $\bar{z} < y$ is impossible; since we have also that $y \nsim z$, we may conclude that $y < \bar{z}$. Write

$$d \;=\; d\big(x,(yz)^-\big) \;=\; d(xy,z^-) \;=\; \tfrac{1}{2}[|x| + |z| - |xyz|] \;>\; \tfrac{1}{2}|y| \;.$$

If $d > \frac{1}{2}|z|$, that is, $|x| + |z| - |xyz| > |z|$, then $|xyz| < |x|$. Since $y < \bar{z} < \bar{x}$, this gives $y, \bar{z}, xyz \in G(\bar{x})$, hence $\bar{x} \in G(\bar{x})$, contrary to $\bar{x} \in X$. We may suppose henceforth that $d \leqq \frac{1}{2}|z| \leqq \frac{1}{2}|x|$. The two ideals $U_1 = (x,(yz)^-)$ and $U_2 = (xy, z^-)$ have the same length, $|U_1| = |U_2| = d$.

We show that $U_1 = U_2$ is impossible. This equation would imply that $d(x,xy) \geqq |U_1| = d > \frac{1}{2}|y|$. Together with

$$d\big(x^-,(xy)^-\big) \;=\; \tfrac{1}{2}[|x| + |x| - |y|] \;=\; |x| - \tfrac{1}{2}|y| \;,$$

this would give

$$d(x,xy) + d\big(x^-,(xy)^-\big) \;>\; |x| \;=\; |xy| \;,$$

whence, by A5, $x = xy$ and $y = 1$, contrary to $y \in Y$.

If $U_2 < U_1$, by (3.1) we should have $U(xy) < U(x)$. It was seen that

$d(x^-,(xy)^-) = |x| - \frac{1}{2}|y| \geqq \frac{1}{2}|x|$, whence $U(x^-) = U((xy)^-)$. It follows that $xy < \bar{x}$. But then $y, xy \in G(\bar{x})$, whence $\bar{x} \in G(\bar{x})$, contrary to $\bar{x} \in X$.

Finally, if $U_1 < U_2$, it follows that $U((yz)^-) < U(z^-)$, while $d(yz,z) = |z| - \frac{1}{2}|y| \geqq \frac{1}{2}|z|$ implies that $U(yz) = U(z)$. Therefore one has $yz < \bar{z}$, hence $y, yz \in G(\bar{z})$ and $\bar{z} \in G(\bar{z})$, contrary to $\bar{z} \in X$.

This completes the proof of (5.9).

6. The cancellation theorem.

An essential element in the proof of the Nielsen Subgroup Theorem is that if, in forming the product of a sequence of one or more non-trivial elements of a free group, no factor cancels entirely into the two adjacent factors, then the product cannot be trivial. We paraphrase this in the following lemma and corollary.

(6.1) LEMMA. *Let $x_1, x_2, \ldots, x_n$ be elements of a group G satisfying Axioms* A1–A5. *Assume that*

(6.1a) $$d(x_{i-1}, x_i^-) + d(x_i, x_{i+1}^-) < |x_i|, \quad \text{all } i \text{ with } 1 < i < n .$$

Then it follows that

(6.1b) $$|x_1 x_2 \ldots x_n| = \sum_{i=1}^{n} |x_i| - 2 \sum_{i=1}^{n-1} d(x_i, x_{i+1}^-) .$$

PROOF. The assertion (6.1b) is trivial for $n = 0, 1, 2$; assume $n \geqq 3$. Define $p_i = x_1 x_2 \ldots x_i$ for $1 \leqq i \leqq n$. For $i = 1$ the equation

(6.1c) $$d(p_i, x_{i+1}^-) = d(x_i, x_{i+1}^-)$$

is trivial. Inductively, assume (6.1c) for some i, $1 \leqq i < n-1$. From (6.1a), with indices increased by 1, we have

$$d(p_i, x_{i+1}^-) + d(x_{i+1}, x_{i+2}^-) < |x_{i+1}| .$$

By (2.3) it follows that $d(p_i x_{i+1}, x_{i+2}^-) = d(x_{i+1}, x_{i+2}^-)$, that is, that (6.1c) holds for $i+1$ in place of i. It follows that (6.1c) holds for all i, $1 \leqq i \leqq n-1$. Summing over this range, and multiplying by 2, gives

$$\sum_{i=1}^{n-1} (|p_i| + |x_{i+1}| - |p_{i+1}|) = 2 \sum_{i=1}^{n-1} d(x_i, x_{i+1}^-) .$$

Since the left member reduces to

$$|p_1| + \sum_{i=2}^{n} |x_i| - |p_n| = |x_1| + \sum_{i=2}^{n} |x_i| - |p_n| ,$$

the equation (6.1b) results after transposition.

(6.2) Corollary. *Under the hypotheses of Lemma* (6.1), *if* $n \geqq 3$, *then* $x_1 x_2 \ldots x_n \neq 1$.

Proof. Write $d_i = d(x_i, x_{i+1}^-)$, $1 \leqq i < n$. From (6.1a) we have

$$\sum_{i=2}^{n-1} |x_i| > d_1 + 2\sum_{i=2}^{n-2} d_i + d_{n-1} .$$

By (6.1b) this gives

$$|p_n| > |x_1| + |x_n| - d_1 - d_{n-1} .$$

Now (2.1) with A3 implies that, for any $z = xy$, $d(z, y) \leqq |y|$; since $d(u, v) = d(v, u)$ and $|u^-| = |u|$, this gives $d_1 \leqq |x_1|$ and $d_{n-1} \leqq |x_n|$, hence $|p_n| > 0$.

Roughly speaking, the condition (6.1a) ensures that, after all cancellation between adjacent factors has been carried out, there will remain some part of each x_i, $1 < i < n$ to act as a barrier against further cancellation between x_{i-1} and x_{i+1}, and hence against any further cancellation whatsoever. In fact, (6.1a) is equivalent to the condition that

$$|x_{i-1} x_i x_{i+1}| > |x_{i-1}| - |x_i| + |x_{i+1}| .$$

In the situations with which we shall deal, we have only the weaker condition (see Lemma (5.9)) that

$$\text{(6.3a)} \qquad |x_{i-1} x_i x_{i+1}| \geqq |x_{i-1}| - |x_i| + |x_{i+1}| \qquad \text{for } 1 < i < n .$$

This condition, although not ensuring that any barrier remains from x_i to provide against cancellation between x_{i-1} and x_{i+1}, does assert that no such cancellation takes place; however, (6.3a) in itself fails to prevent cancellation between more remote factors, and to secure (6.2); this is illustrated by the product $(p^- q)\,(q^- r)\,(r^- s)\,(s^- p)$, in the free group on generators p, q, r, and s.

In the situations to be considered here, as with the Nielsen Theorem, one has the additional condition on consecutive factors, that

$$\text{(6.3b)} \qquad |x_i x_{i+1}| \geqq |x_i|, |x_{i+1}| \qquad \text{for } 1 \leqq i < n;$$

but the example just cited shows that even (6.3a) and (6.3b) together do not suffice for the desired conclusions.

In fact, we have yet a further condition (6.3c), that equality in (6.3a) cannot occur for two consecutive x_i, x_{i+1}. That (6.3a) and (6.3c) do not suffice to secure $x_1 x_2 \ldots x_n \neq 1$ is shown by the product $(pqr)\,(r^- s)\,(s^- q^- t)\,(t^- p^-)$, in the free group on generators p, q, r, s, and t. But the conditions (6.3a), (6.3b) and (6.3c) together do suffice for our purpose. We turn to the proof of this fact.

(6.4) THEOREM. *Let* $x_1, x_2, \ldots, x_n$ *be non-trivial elements of a group* G *satisfying Axioms* A1–A5. *Assume that*

(6.4a) $$d(x_i, x_{i+1}^-) \leqq \tfrac{1}{2}|x_i|,\ \tfrac{1}{2}|x_{i+1}| \quad \text{for } 1 \leqq i < n;$$

(6.4b) $d(x_{i-1}, x_i^-) = d(x_i, x_{i+1}^-) = \frac{1}{2}|x_i|$ *does not hold for any two consecutive factors* x_i;

(6.4c) *the equation of* (6.4b) *implies* $|x_{i-1}x_ix_{i+1}| = |x_{i-1}| - |x_i| + |x_{i+1}|$.

Then (6.1b) *holds, and* $x_1x_2\ldots x_n \neq 1$ *if* $n \geqq 1$.

PROOF. We first remark that (6.4a) implies that

(6.4d) $$d(x_{i-1}, x_i^-) + d(x_i, x_{i+1}^-) \leqq |x_i| \quad \text{for } 1 < i < n .$$

An element x_i will be called *singular* (relative to its position in the product) if, in (6.4d), equality holds. Then (6.4b) says that no two consecutive factors x_i and x_{i+1} are singular. We observe that the theorem is trivial for $n < 3$, whence we may assume $n \geqq 3$. As a consequence of the definition, neither x_1 nor x_n can be singular. If $z_1, z_2, \ldots, z_m$ are the non-singular x_i, in order, then $m \geqq 2$. If some $z_j = x_i$, and x_{i+1} is non-singular, or $i = n$, then we define $u_j = z_j = x_i$; if $i < n$ and x_{i+1} is singular, then we define $u_j = x_ix_{i+1}$. Evidently $p = x_1x_2\ldots x_n = u_1u_2\ldots u_m$. If $m = 2$, we have $p = x_1x_2x_3$, where x_2 is singular, and, by (6.4c),

$$\begin{aligned} |p| &= |x_1| - |x_2| + |x_3| = |x_1| + |x_2| + |x_3| - 2|x_2| \\ &= |x_1| + |x_2| + |x_3| - 2d(x_1, x_2^-) - 2d(x_2, x_3^-) , \end{aligned}$$

so that (6.1b) holds. Since (6.4a) gives $|x_2| = d(x_1, x_2^-) \leqq |x_1|$, while $x_3 \neq 1$ gives $|x_3| > 0$, we have $|p| = |x_1| - |x_2| + |x_3| > 0$, and it follows that $p \neq 1$. Thus we may assume $m \geqq 3$.

Our aim is to establish (6.1a) for the product of $u_1, u_2, \ldots, u_m$. For this we shall show that, writing $d_i = d(u_i, u_{i+1}^-)$, we have always $d_i \leqq \frac{1}{2}|u_i|$, $\frac{1}{2}|u_{i+1}|$, and that $d_i = d_{i+1} = \frac{1}{2}|u_{i+1}|$ is impossible. To simplify notation, we write $u_i = xy$, $u_{i+1} = zw$, $u_{i+2} = st$, where x, z, s are non-singular and where y, w, t are either singular or trivial. From (2.3), since z and s are non-singular and $d(xy, z^-) = d(y, z^-)$ for singular y, as a consequence of the assumptions, $d_i = d(xy, z^-)$ and $d_{i+1} = d(zw, s^-)$. Singularity or triviality of y and w implies that $|xy| = |x|$ and $|yz| = |z| = |zw| = |u_{i+1}|$. In case $y = 1$, (6.4a) gives $d_i = d(x, z^-) \leqq \frac{1}{2}|z| = \frac{1}{2}|u_{i+1}|$. If $y \neq 1$, whence y is singular, from (6.4c) and (6.4a) we have

$$\begin{aligned} d_i = d(xy, z^-) &= \tfrac{1}{2}[|xy| + |z| - (|x| - |y| + |z|)] \\ &= \tfrac{1}{2}|y| \leqq \tfrac{1}{2}|yz| = \tfrac{1}{2}|z| = \tfrac{1}{2}|u_{i+1}| . \end{aligned}$$

Thus $d_i \leqq \frac{1}{2}|u_{i+1}|$, and, since $d(xy,z^-) = d(x,(yz)^-)$, a symmetric argument shows that $d_i \leqq \frac{1}{2}|u_i|$.

If $y=1$, the equality $d_i = \frac{1}{2}|u_{i+1}| = \frac{1}{2}|z|$ becomes $d(x,z^-) = \frac{1}{2}|z|$ where x is now the member of the sequence $x_1,\ldots,x_n$ immediately preceding z. If $y \neq 1$, $d_i = \frac{1}{2}|u_{i+1}|$ implies by the chain of inequalities above, that $|yz| = |y|$ and hence $d(y,z^-) = \frac{1}{2}|z|$, where y is now the member of the sequence $x_1,\ldots,x_n$ immediately preceding z. Thus, if $z = x_h$, $d_i = \frac{1}{2}|u_{i+1}|$ implies that $d(x_{h-1},x_h^-) = \frac{1}{2}|x_h|$. Symmetrically, $d_{i+1} = \frac{1}{2}|u_{i+1}|$ implies that $d(x_h,x_{h+1}^-) = \frac{1}{2}|x_h|$. In view of the fact that $z = x_h$ is non-singular, $d(x_{h-1},x_h^{-1}) = d(x_h,x_{h+1}^-) = \frac{1}{2}|x_h|$ is impossible, whence $d_i + d_{i+1} < |u_{i+1}|$. By Lemma (6.1) and Corollary (6.2) it follows that $p \neq 1$ and then

$$|p| = \sum_{i=1}^{m} |u_i| - 2\sum_{i=1}^{m-1} d_i .$$

From this equation we must obtain (6.1b). From the fact that $d_i = d(u_i,u_{i+1}^-) = d(xy,z^-)$, it follows, if $y=1$, that $|u_i| - 2d_i = |x| - 2d(x,z^-)$. It remains to show that, if $y \neq 1$, whence y is singular, that

$$|u_i| - 2d_i = |x| + |y| - 2d(x,y^-) - 2d(y,z^-) .$$

Now $|u_i| = |xy| = |x|$, and

$$2d_i = (|xy| + |z| - |xyz|) = [|x| + |z| - (|x| - |y| + |z|)] = |y| ,$$

whence $|u_i| - 2d_i = |x| - |y|$. On the other hand, $d(x,y^-) = d(y,z^-) = \frac{1}{2}|y|$ implies that

$$|x| + |y| - 2d(x,y^-) - 2d(y,z^-) = |x| + |y| - |y| - |y| = |x| - |y| .$$

This completes the proof of the theorem.

7. The theorems of Nielsen and Kurosh.

Let $\mathcal{N}$ be the family of all those non-Archimedean subgroups M of G that meet X, that is, of all $M = N(x)$ for some $x \in X \cap N$. Let $\mathcal{A}$ be the family of all the cyclic groups $Z = Z(x)$ generated by an Archimedean element of X, that is, for $x \in X - N$. Let $\mathcal{G}$ be the union of these two families: $\mathcal{G} = \mathcal{N} \cup \mathcal{A}$.

(7.1) Main Theorem. *The groups of the family $\mathcal{G}$ have pairwise trivial intersection. The cyclic groups $Z(x) \in \mathcal{A}$ are infinite cyclic groups. The group G is the free product of the family $\mathcal{G}$ of subgroups.*

Proof. It clearly suffices to establish that, for $n \geqq 1$, a product $p = x_1x_2\ldots x_n$ is not trivial, $p \neq 1$, provided the factors $x_1,x_2,\ldots,x_n$ satisfy the following conditions. None of the $x_i = 1$, and each x_i either belongs to some $M=N(x)$ from $\mathscr{N}$, or else is the generator x of some $Z=Z(x)$ in $\mathscr{A}$, or the inverse x^- of such a generator x. Moreover, no adjacent factors x_i and x_{i+1} belong to the same subgroup M in $\mathscr{N}$, nor are they, in one order or the other, the generator x of some $Z=Z(x)$ in $\mathscr{A}$ and its inverse x^-. More simply, this requires that all the $x_i \in Y$, and that, for all i, $1 \leqq i < n$, $x_i \nsim x_{i+1}$ and $x_i \neq x_{i+1}^-$.

Let p then be the product of elements $x_1, x_2, \ldots, x_n$, for $n \geqq 1$ satisfying these conditions.

From these conditions it follows first by (5.6) that condition (6.4a) holds:

$$d(x_i, x_{i+1}^-) \leqq \tfrac{1}{2}|x_i|,\ \tfrac{1}{2}|x_{i+1}| \qquad \text{for all } i,\ 1 \leqq i < n\,.$$

Suppose next that some x_i is singular, in the sense that $d(x_{i-1}, x_i^-) = d(x_i, x_{i+1}^-) = \frac{1}{2}|x_i|$, or, equivalently, that $|x_{i-1}x_i| = |x_{i-1}|$ and $|x_i x_{i+1}| = |x_{i+1}|$. Then, by (5.8), $x_i \in N$. Suppose now that successive x_i and x_{i+1} are singular; then $x_i, x_{i+1} \in N$ and $|x_i x_{i+1}| = |x_{i+1}|$ with $|x_i x_{i+1}| = |x_i|$; then, by definition, $x_i \sim x_{i+1}$. Since this is contrary to our hypothesis on the x_i, we have established (6.4b), that no successive x_i and x_{i+1} both can be singular. Finally, (5.9), with x, y, and z replaced by x_{i-1}, x_i, and x_{i+1} establishes (6.4c), that, if x_i is singular, then

$$|x_{i-1}x_i x_{i+1}| = |x_{i+1}| - |x_i| + |x_{i+1}|\,.$$

Thus all the hypotheses of (6.4) are fulfilled, and we may conclude, by (6.4), that $p \neq 1$, as required.

The additional conclusion, that $|p|$ is given by (6.1b), which also follows, will be used later.

An immediate corollary of this result is the following.

(7.2) Corollary. *If G is a group with an Archimedean length function, that is, satisfying* A0–A4, *then G is freely generated by the set X.*

Suppose now that F is any free group, freely generated by a set W of generators, and with $|x|$ the length function on F relative to the set W of generators. Then, by (2.7), $|x|$ is an Archimedean length function, and so, a fortiori, is its restriction to any subgroup G of F. We now appeal to (7.2).

(7.3) Nielsen Subgroup Theorem. *Every subgroup of a free group is free.*

We want to reiterate here that the full argument of this paper, cut down to the case at hand, is essentially the original argument of Nielsen, and that our full argument seems to be the obvious and natural, albeit laborious, adaptation of Nielsen's argument to a situation in which we have admitted two new difficulties: first, the length function on G is given axiomatically without reference to any containing group F; and, second, we have admitted the possibility of non-trivial non-Archimedean elements.

Suppose alternatively that F is any free product of a family $\mathscr{F}$ of subgroups F_a, a ranging over an index set A, and with pairwise trivial intersection. Then, by (2.8), the length function $|x|$ on F naturally associated with this free decomposition satisfies Axioms A1–5, and the same is true of the restriction of the function $|x|$ to any subgroup G of F. Moreover, it is easily seen that the non-Archimedean elements of F are precisely the elements of the groups F_a, $a \in A$, together with their conjugates. Application of (7.1) to G now provides a version of the Kurosh Subgroup Theorem.

(7.4) KUROSH SUBGROUP THEOREM. *Let a group F be the free product of a family $\mathscr{F}$ of subgroups F_a, $a \in A$, with pairwise trivial intersections. If G is any subgroup of F, then G is the free product of a family $\mathscr{G}$ of subgroups G_b, $b \in B$, with pairwise trivial intersection. One member G_b of the family G is a free group* (possibly trivial), *while each of the remaining groups G_b is conjugate in F to some subgroup of one of the F_a.*

We eludicate now the word "separately" in the final sentence of the first paragraph of the introduction. Although the Nielsen Theorem is indeed contained as a special case in the Kurosh Theorem, by viewing the free group F as the free product of the family $\mathscr{F}$ of infinite cyclic groups F_a generated by the elements w of a free set W of generators for F, our proof of the Kurosh Theorem does not reduce, under these special circumstances, to our proof of the Nielsen Theorem. For the Archimedean length function on F, viewed as the free group on W as free set of generators, does not coincide with the length function (which is non-Archimedean unless F is trivial) on F, viewed as the free product of the family $\mathscr{F}$ of groups F_a.

8. Embedding theorems.

The axiom sets A1–A5 and A0–A4 were chosen (as ordinarily with representation theorems) to be sufficient to carry out a proof that a group G with a length function satisfying them would be a free group, or a free product of subgroups with pairwise trivial intersection. In view of (2.7) and (2.8), every subgroup of a free group or free product F must possess a length function satisfying the axioms. In this sense, apart from the question of possible dependence, which seems most unlikely and of little interest, the axioms are best possible; that is, necessary as well as sufficient for the conclusions that we have drawn from them.

We have shown that if G is equipped with a length function $|x|$ satisfying the properties it would have to satisfy if it were derived from the natural length function on a containing group F, free group or free product, then G indeed possesses the structure it would have to possess, by virtue of the theorems of Nielsen and Kurosh, if it were in fact a subgroup of such a containing group F. One can even remark, rather vacuously, that G is in fact a subgroup of a group F of the prescribed structure, namely, of G itself. But a more serious question in this direction considers not only the structure of groups, but of ordered couples consisting of groups equipped with length functions. We ask whether G with its length function, satisfying one or the other of the two sets of axioms, can be embedded in a group F, of the expected sort, whose natural length function is an extension of that given on G. We can show that, with certain minor reservations, this is in fact always the case.

It will appear from our construction that, given G and its length function, the extension to F with its natural length function is minimal and essentially unique. However, there remains a reasonable sense, suggested by a remark of Hanna Neumann, in which the extension F is needlessly large. It is characteristic of free groups or free products F, with their natural length functions, that every ideal is principal: in explicit terms, if x and y are elements of F and $d(x,y)=m$, then there exists in F an element z such that $|z|=m$ and $d(x,z)=d(y,z)=m$. There will lie between G and F, an essentially unique minimal "principal ideal group" F^*, that is, a group on which the length function derived from the containing group F has the property just enunciated. The length function on F^* will not ordinarily be the natural length function associated with F^* under any interpretation of it as a free group or free product, but will depart from such a function only in that the lengths $|w|$ attached to the elements w of a free set W of generators, or the lengths l_a attached to all the nontrivial elements of a free factor F_a (in the case of a free product), will not necessarily all be equal to 1, nor, indeed, equal among themselves.

We feel strongly that the restriction to length functions whose values are integers, rather than real numbers, elements of an ordered abelian group, or even of algebraic structures of a more unfamiliar nature, is regrettable; both the consideration of the various groups of paths (or rather of disconnected finite sequences of paths) in topology, as well as the occurrence in group theory of groups admitting exponents x^n for n in some domain more general than the integers, appear to support this feeling. From this point of view, we are inclined to attach more interest to the "splitting group" F^* of G than to the larger group F. However, we have not wanted to obscure the main ideas here by dealing with length functions into domains any more abstract and unfamiliar than the integers. For this reason we abandon for the present any further consideration of F^* (whose nature will in any case be apparent from the construction that follows), and return to the construction of F.

(8.1) THEOREM. *Let G be any group with an Archimedean length function, that is, whose length function satisfies Axioms* A0–A4 *together with Condition* C0. *Then G is a subgroup of a free group F, free on a set W of free generators, such that the length function on G is the restriction of the natural length function on F relative to the set W of generators.*

(8.2) THEOREM. *Let G be any group with a length function satisfying Axioms* A1–A5, *and also Conditions* C1 *and* C2. *Then G is a subgroup of a group F, which is a free product of a family $\mathscr{F}$ of its subgroups, and in such a way that the length function on G is the restriction of the natural length function on F relative to the given free decomposition.*

Although neither (8.1) nor its proof is a special case of (8.2) or its proof, the ideas employed in the proof of (8.1) are the same as those in that of (8.2), adapted to a simpler situation. Therefore we give a proof of (8.2) only, omitting that of (8.1).

The idea of the proof is as follows. Starting with G and its length function, assumed to satisfy A1–A5 and C1, C2, we associate with each $x \in Y$ a sequence of symbols x^m (here m is an upper index, and not an exponent) and x^{-m} of length equal to $|x|$, which are intended to represent the "syllables" of x, written, in F, as a product of non-trivial factors from the F_a, with successive factors in different F_a. The group F will be generated by these symbols x^m, x^{-m}, upon which we must impose certain relations. These relations arise on two accounts. First, that if $d(x,y) \geqq m$, then x^m and y^m must be counted as the same element of F; second, the subgroups $N(x)$ of G are not necessarily free, whence relations must be imposed on their intended images in F. With this done properly, we have a map from Y into F, carrying each x in Y into its expression as a product of syllables x^m in F, which induces a homomorphism and, indeed, a monomorphism, φ from G into F.

There remains the matter of specifying the family $\mathscr{F}$ of subgroups F_a of F, of showing that F is their free product, and that they have pairwise trivial intersection. This defines a natural length function $|u|$ on F, and it remains further to show that $|\varphi x| = |x|$ for all x in G.

We turn now to the details. Let K_1 be the set of all ordered couples (x,m) for $x \in Y$ and $m \leqq \frac{1}{2}|x|$. If $x \in X - N$ and x has odd length, $|x| =$

$2k+1$, we introduce a further ordered couple $(x,k+1)$; the set of all these we denote by K_2. Finally, if $M \in \mathscr{N}$, then all non-trivial elements of M have the same length which, by C1, is odd, say $2k+1$. Let K_3 be the set of all elements $(x,k+1)$, $x \in M \in \mathscr{N}$, $|x| = 2k+1$. Define $K = K_1 \cup K_2 \cup K_3$.

Define a relation $(x,m) \equiv (y,m)$ on K to hold if and only if $d(x,y) \geqq m$. By A4, this is an equivalence relation. We write x^m for the equivalence class of (x,m), and L for the set of all equivalence classes. We observe that, from the definition, $(x,m) \equiv (y,n)$ implies $m=n$, whence $x^m = y^n$ implies $m=n$. Further, if $|x| = |y| = 2k+1$, odd, then $x^{k+1} = y^{k+1}$ implies that $d(x,y) \geqq k+1 > \frac{1}{2}|x|$, whence, by (5.6), $x=y$. In particular, for each $M \in \mathscr{N}$, the map θ_M from M into $L \cup \{1\}$ defined by $\bar{\theta}_M x = x^{k+1}$ and $\theta_M 1 = 1$ is one to one, and we may use it to equip the image $\theta_M M$ with the structure of a group isomorphic to M under θ_M. Moreover, the $\theta_M M$ have pairwise trivial intersection, hence together generate in $L \cup \{1\}$ a subgroup F_N which is their free product. We now define F_A to be the free group on the set $L - F_N$ as free generators. Finally, we define F to be the free product of F_N and F_A. Evidently F contains L, and is the free product of the family F' of subgroups consisting of all the $\theta_M M$ for $M \in \mathscr{N}$, together with the infinite cyclic groups $Z(x^m)$ generated by the $x^m \in L - F_N$; and the groups of this family have pairwise trivial intersection.

We next define a map φ from Y into F. Let x, in Y, have length $2k$ or $2k+1$. Then we set

$$\varphi x = x^{-1-}x^{-2-} \ldots x^{-k-}x^{k+1}x^k \ldots x^2 x^1;$$

here x^{-m-} means the inverse $((x^-)^m)^-$ of the m-th syllable $(x^-)^m$ of x^-, that is, of the equivalence class of (x^-,m); if $|x| = 2k$ it is to be understood that the symbol x^{k+1} is omitted; further, if $x^- \in X-N$ and $|x| = 2k+1$, so that x^{k+1} has not been defined, we now define $x^{k+1} = x^{-(k+1)-}$. With this definition it is easily seen that the x in $X-N$ and their inverses are on an equal footing, and we have, in particular, for all $x,y \in Y$, that $x^m = y^n$ if and only if $m=n$ and $d(x,y) \geqq m = n$.

The last mentioned convention ensures that, for $x \in X-N$, $\varphi(x^-) = (\varphi x)^-$. It follows that the correspondence from x into φx extends uniquely to a homomorphism φ_Z from the infinite cyclic subgroup $Z = Z(x)$ of G, generated by x, into F. (In fact, as is easily seen, and will be shown later, φ_Z is a monomorphism.)

We next show that, for each $M \in \mathscr{N}$, the restriction of φ to $M \cap Y = M - \{1\}$ determines a monomorphism from M into F. All elements of $M - \{1\}$ have common odd length $2k+1$; if x and y are such elements, then $d(x,y)=k+\frac{1}{2}>k$, which implies that $x^1=y^1$, $x^2=y^2,\ldots$, $x^k=y^k$, whence we may unambiguously associate with M an element $u_M=x^kx^{k-1}\ldots x^2x^1$. Then $\varphi x=u_M{}^- x^{k+1}u_M$ for all $x\in M$, $x\neq 1$. Since the map θ_M carrying x into x^{k+1} was a monomorphism, it follows that the restriction of φ to $M-\{1\}$ defines a monomorphism φ_M from M into F.

Since G is the free product of the family of its subgroups Z and M of the types just considered, and these have pairwise trivial intersection, it follows that all the φ_Z and φ_M have a common extension φ_G to a homomorphism from G into F. Since φ_G is in fact the unique extension of the map φ defined on the set Y of generators for G, we shall drop the subscript, and write simply φ in place of φ_G.

Returning to the set K of couples (x,m), we define a new relation $(x,m)\leftrightarrow(y,m)$ to hold if $d(x,y)\geqq m-\frac{1}{2}$. By A4, this is an equivalence relation. It is immediate that $(x,m)\equiv(y,m)$ implies $(x,m)\leftrightarrow(y,m)$, so that we may carry the new relation over to the set L, writing $x^m\leftrightarrow y^m$. Let x and y be two elements of N, of the same length $2k+1$; then $x^{k+1}\leftrightarrow y^{k+1}$ is equivalent to $d(x,y)>k+\frac{1}{2}=\frac{1}{2}(2k+1)$, hence to $x\sim y$. Thus each equivalence class C_a of L under the relation $x^m\leftrightarrow y^m$ contains $\theta_M M-\{1\}$ for at most one $M\in\mathcal{N}$. In addition, C_a may contain certain elements from $L-F_N$. The subgroup F_a of F generated by C_a will therefore contain at most one $\theta_M M$ together with groups $Z(x^m)$ for all $x^m\in C_a-F_N$. In view of the structure of F as the free product of the $\theta_M M$ together with the $Z(x^m)$ for $x^m\in L-F_N$, it follows that each F_a is the free product of the groups it was just mentioned to contain, that F is the free product of the F_a, and that the F_a have pairwise trivial intersection.

A natural length function $|u|$ on F is now determined by the family $\mathscr{F}$ of subgroups F_a, and we want to show that $|\varphi x|=|x|$ for all $x\in G$. From this it will follows that the homomorphism φ is a monomorphism, since $\varphi x=1$ would imply that $|\varphi x|=|x|=0$, hence $x=1$.

(8.3) LEMMA. *If x is in Y, then* $|\varphi x|=|x|$.

PROOF. Since y^m and z^n can belong to the same F_a only if $m=n$, inspection of the definition of φx requires us only to consider the case that $|x|=2k$, when the two syllables x^{-k-} and x^k, with same superscript, are adjacent. But $x^{-k}\leftrightarrow x^k$ requires that $d(x,x^-)\geqq k-\frac{1}{2}$, and this implies that

$$|xx|-|x| \;=\; |x|-2d(x,x^-) \;\leqq\; 2k-2(k-\tfrac{1}{2}) \;=\; 2k-2k+1 \;=\; 1\ .$$

Now $|xx|-|x|=0$ implies that $x\in N$, which, by C1, contradicts $|x|=2k>0$, while $|xx|-|x|=1$ is excluded directly by C2. Therefore the expression for φx as given (with the convention to omit x^{k+1} if $|x|=2k$)

is in normal form relative to the free decomposition, and $|\varphi x|$ is precisely the number of syllables displayed, that is, $|\varphi x| = |x|$.

(8.4) LEMMA. *If x and y are in Y, then $d(\varphi x, \varphi y) = d(x,y)$.*

PROOF. We may put aside as trivial the cases that $x = 1$, $y = 1$, $x = y$, or $x \sim y$. We may assume by symmetry that $|x| \leqq |y|$. Then φy has the form

$$\varphi y = y^{-1-}y^{-2-}\dots y^{h+1}y^{h}\dots y^{2}y^{1} \quad \text{with} \quad k \leqq h .$$

By (5.6),

$$d(x,y) \leqq \tfrac{1}{2}|x|, \quad \text{whence } n = [d(x,y)] \leqq k ,$$

and it will result from the definition of the relation $(x,m) \equiv (y,m)$ that the last n syllables of φx and φy will agree; unless the last remaining syllable of φx is x^{-k-}, it follows also that the last remaining syllables of φx and φy do not agree. Excepting the case noted, using also the definition of the relation $x^m \leftrightarrow y^m$ to decide whether or not the two last remaining syllables lie in the same component F_a, it follows routinely from the definitions that $d(\varphi x, \varphi y) = d(x,y)$.

The case remains that the last remaining syllable of $\varphi\ x$ is x^{-k-}; here necessarily $|x| = 2k$ and, by (5.6), $d(x,y) = k$. If $|x| < |y|$, so that the last remaining syllable of φy is y^{k+1}, then, since $x^{-k} \leftrightarrow y^{k+1}$ is impossible for elements with different superscripts k and $k+1$, it follows that x^{-k-} and y^{k+1} are in different F_a, whence $d(\varphi x, \varphi y) = k = d(x,y)$ as required.

We are left with the possibility that the last remaining syllables of φx and φy are x^{-k-} and y^{-k-}; here necessarily $|x| = |y| = 2k$ and, using (5.6), $d(x,y) = k$. If x^{-k-} and y^{-k-} lie in different F_a, then $d(\varphi x, \varphi y) = k$ and all is well. We must show that the assumption that $x^{-k-} \leftrightarrow y^{-k-}$ is contradictory. This implies, again using (5.6), that $d(x^-, y^-) = k - \varepsilon$, where ε can be either 0 or $\frac{1}{2}$. Formula (6.1b) is applicable to each of the products xy^- and xy^-xy^- to give

$$|xy^-| = |x| + |y| - 2d(x,y) = 2k + 2k - 2k = 2k ,$$

and

$$|xy^-xy^-| = 2|x| + 2|y| - 4d(x,y) - 2d(y^-, x^-)$$

thus

$$|(xy^-)(xy^-)| = 4k + 4k - 4k - 2(k - \varepsilon) = 2k + 2\varepsilon = |xy^-| + 2\varepsilon .$$

Now 2ε is either 0 or 1. If $2\varepsilon = 0$, we have $|(xy^-)(xy^-)| = |xy^-|$, whence $xy^- \in N$, $xy^- \neq 1$, which, since, $|xy^-| = 2k$, even, contradicts C1. If $2\varepsilon = 1$, we have $|(xy^-)(xy^-)| = |xy^-| + 1$, in direct contradiction of C2. This completes the proof of (8.4).

(8.5) LEMMA. *Let x, y and $z \in Y$, with $y \nsim x$, $y \nsim z$, and $|xy| = |x|$, $|yz| = |z|$. Then $|\varphi(xyz)| = |xyz|$.*

PROOF. We use freely the results (5.7), (5.8), (5.9), and also (8.3) and (8.4). It then follows directly that $y \in N$ has odd length $2k+1$ and that

$$\varphi(xyz) = x^{-1-}x^{-2-} \dots x^{k+1}y^{k+1}z^{-(k+1)-} \dots z^2z^1 ,$$

a product consisting of an initial segment of the normal form for φx followed by y^{k+1} and then by a final segment of the normal form for φz. And all pairs of adjacent factors lie in different components F_a with the possible exception of the pairs x^{k+1}, y^{k+1} and y^{k+1}, $z^{-(k+1)-}$. But, in fact, $d(x,y^-) = \frac{1}{2}|y| = k+\frac{1}{2}$ implies that $x^{k+1} \leftrightarrow y^{k+1}$, and similarly, $y^{k+1} \leftrightarrow z^{k+1}$, so that the triple product $x^{k+1}y^{k+1}z^{-(k+1)-}$ reduces to a single syllable u, lying in some F_a. From the structure of F_a, which can contain only a single group $\theta_M M$, containing the element y^{k+1}, and is the free product of this with infinite cyclic groups generated by elements not lying in $\theta_M M$, it follows that $u \neq 1$. Thus the normal form for $\varphi(xyz)$ is obtained from that given above by replacing the product $x^{k+1}y^{k+1}z^{-(k+1)-}$ by a single factor u. Thus, starting from the normal words for φx, φy, φz, written down one after the other, and containing in all $|x|+|y|+|z|$ syllables, we have cancelled k syllables of x against k from y, and another k from y against k from z, removing thus $4k$ syllables; we have further decreased the number of syllables by two, in replacing a triple product by a single syllable u. In all, this gives $|\varphi(xyz)| = |x|+|y|+|z|-4k-2$; since $|y| = 2k+1$ this gives $|\varphi(xyz)| = |x|-|y|+|z| = |xyz|$, as required.

To complete the proof of (8.2) we must show that $|\varphi p| = |p|$ for all $p \in G$. We may suppose p written in the form $p = x_1x_2 \dots x_n$ where the x_i satisfy the conditions established in the proof of (7.1). We shall apply Theorem (6.4).

From (8.3) and (8.4), and the result (5.6) that the x_i satisfy (6.4a), it follows that the φx_i satisfy the analogous condition (6.4a)′. Next, it was shown in the proof of (7.1) that (6.4b) holds, whence it again follows that the analogous condition (6.4b)′ holds with the φx_i in place of the x_i. The analog, (6.4c)′, of (6.4c), was established directly, under the given hypotheses, as (8.5) above. Thus the sequence of elements φx_1, $\varphi x_2, \dots, \varphi x_n$ of the group F, satisfying Axioms A1–A5, fulfils conditions (6.4a), (6.4b), and (6.4c). By (6.4) we are permitted to conclude that $|\varphi p|$ is given, in accordance with (6.1b), by the formula

$$|\varphi p| = \sum_{i=1}^{n} |\varphi x_i| - 2\sum_{i=1}^{n-1} d(\varphi x_i, \varphi x_{i+1}^{-}) .$$

Comparing this with the original form of (6.1b),

$$|p| = \sum_{i=1}^{n} |x_i| - 2\sum_{i=1}^{n-1} d(x_i, x_{i+1}^{-}),$$

and appealing to (8.3) and (8.4), we conclude that $|\varphi p| = |p|$. This completes the proof of the embedding theorem, (8.2).

REFERENCES

1. A. G. Kurosh, *The theory of groups* II, New York, 1956.
2. J. Nielsen, *A basis for subgroups of free groups*, Math. Scand. 3 (1955), 31–43.

UNIVERSITY OF MICHIGAN, ANN ARBOR, MICHIGAN, U.S.A.