# FREE BASES FOR NORMAL SUBGROUPS OF FREE GROUPS

BY

D. E. COHEN AND R. C. LYNDON[1]

1. **Introduction.** The Main Theorem proved here was obtained independently by the two authors. It asserts that the normal subgroup of a free group defined by a single element of the free group is freely generated by a certain set of conjugates of that element.

The Identity Theorem [4] of the second author follows directly upon taking the quotient group of the normal subgroup by its derived group.

A further easy consequence of the Main Theorem, together with the Freiheitssatz of Dehn and Magnus [8], is an Elimination Theorem, which constitutes a combination and refinement of both the Identity Theorem and the Freiheitssatz. The Hauptform of the Freiheitssatz asserts, under certain circumstances, that if element $w$ is a consequence of a given set $S$ of relators it is in fact a consequence of a certain subset $S_0$ of $S$. The Elimination Theorem provides, under the same circumstances, a method of obtaining, from a given representation $w = p_1 \cdots p_n$ of $w$ as a product of conjugates of elements of $S$ and of their inverses, a similar representation $w = q_1 \cdots q_m$ of $w$ in terms of the elements of $S_0$. In fact, the second representation is obtainable from the first by a succession of Peiffer Transformations [12]: a pair of successive factors, $p_i$, $p_{i+1}$ may be deleted if $p_i p_{i+1} = 1$, or it may be replaced by either of the pairs $p_{i+1}$, $p_{i+1}^{-1} p_i p_{i+1}$ or $p_i p_{i+1} p_i^{-1}$, $p_i$.

The results of this paper admit extensions parallel to those of the Freiheitssatz obtained in [6]. A quite different hypothesis on a set $S$ of elements in a free group under which the normal subgroup defined by $S$ is freely generated by a set of conjugates of elements from $S$ is provided by Theorem (6.1) below.

The proof of the Main Theorem follows the same plan as the proof, by Dehn and Magnus, of the Freiheitssatz. We assume the Freiheitssatz, in a variant of the Hauptform stated in [6]. We do not assume the Identity Theorem, and thus provide here a new proof of that theorem. Our argument hinges on two lemmas concerning free products with amalgamation. The first of these, Lemma (2.1) below, may be regarded as a special case of a result of Hanna Neumann [10]; a topological proof has been given by the first author [1]. The second, Lemma (3.4), is obtained by a modification of Nielsen's proof [11] of the Subgroup Theorem; similar arguments are discussed in [2; 7].

Received by the editors August 1, 1962.

(1) Work of the second author was supported by National Science Foundation Grant G-24333.

We use the notation $\bar{x} = x^{-1}$, $x^y = \bar{y}xy$, $x^{-y} = \bar{x}^y$. By the normal subgroup $R$ of a group $G$ *defined* by a set $S$ of elements of $G$ we mean the smallest normal subgroup $R$ of $G$ containing $S$. By a *transversal* $T$ for a subgroup $H$ in a group $G$ we shall always mean a set of representatives for the cosets $Ht$ in $G$.

2. **Free products.** We are here concerned with drawing conclusions about a free product from assumptions on the free factors.

(2.1.) LEMMA. *Let a group $G$ be the free product of its subgroups $G_1$ and $G_2$, with intersection $G_0 = G_1 \cap G_2$. For $i = 1, 2$, let $R_i$ be a normal subgroup of $G_i$ such that $R_i \cap G_0 = 1$, and let $A_i$ be a transversal for the subgroup $G_0R_i$ in $G_i$, with $1 \in A_i$. Then the normal subgroup $R$ of $G$ defined by $R_1$ and $R_2$ is the free product of all groups $R_i^{a_1 \cdots a_n}$ for which: $i = 1, 2$; $n \geqq 0$; no $a_k = 1$; and all of $a_2, a_4, \cdots \in A_i$, while all of $a_1, a_3, \cdots \in A_j$, $j \neq i$.*

**Proof.** We first show that the subgroup $R'$ of $G$ generated by all these $R_i^{a_1 \cdots a_n}$ is in fact $R$. Clearly $R' \subseteq R$, and, for the opposite inclusion, it suffices to show that $r \in R_i$ and $w \in G$ implies $r^w \in R'$. The hypotheses imply (see, for example, Proposition (1.3) of [6]) that $G/R$ is the free product of its subgroups $G_iR/R \simeq G_i/R_i$ with intersection $G_0R/R \simeq G_0$. The normal form for the element $wR$ of the free product $G/R$ yields an expression for $w$ in the form $w = ua_1r_1 \cdots a_nr_n$, $n \geqq 0$, $u \in G_i$, and with all $a_k \in A_1 \cup A_2$ and all $r_k \in R_1 \cup R_2$. Let $b_k = a_{k+1} \cdots a_n$, $0 \leqq k \leqq n$. Let $r_0 = r^u$, in $R_i$. From the equation $r^w = (r_0^{b_0})^{r_1^{b_1} \cdots r_n^{b_n}}$ it follows by induction on $n$ that $r^w \in R'$.

It remains to show that $R = R'$ is the free product of the subgroups $R_i^{a_1 \cdots a_n}$. For this it will suffice to show that if $p = p_1 \cdots p_s$, $s > 1$, where each $p_i$ belongs to one of these groups and no two adjacent $p_i$, $p_{i+1}$ belong to the same group, then $p \neq 1$. We shall show that $p$ can be represented as an alternating product, $p = g_1 \cdots g_m$, $m \geqq 1$, with the $g_i$ alternately from $G_1$ and $G_2$, and no $g_i$ in $G_0$. By hypothesis, each $p_i$ is represented as an alternating product, $p_i = \bar{a}_n \cdots \bar{a}_1 r a_1 \cdots a_n$, with $r$ in $R_1$ or $R_2$. We obtain a representation for $p$ by putting together these representations for the $p_i$, and then successively deleting pairs of adjacent factors that are inverse to each other. If we now account as a single factor each part $\bar{a}b$ with $a$, $b$ in the same $A_h$, and each part $ar\bar{b}$ with $a$, $b$ in the same $A_h$ and $r$ in $R_h$, then we have a representation for $p$ with factors alternately from $G_1$ and $G_2$. It remains to verify that no factor lies in $G_0$. This is immediate for any factor that occured as a factor in some $p_i$. In the case of a factor $a\bar{b}$, with $a, b \in A_h$, we have $a \neq b$ by virtue of our preliminary deletions, whence $a\bar{b} \notin G_0$ follows from the fact thar $A_h$ is a transversal for the group $G_0R_h$, containing $G_0$. Finally, suppose that $ar\bar{b} \in G_0$, with $a, b \in A_h$ and $r \in R_h$. From $a \in G_0R_hb$ we should have $a = b$, hence $ar\bar{b} = ar\bar{a} \in R_h$. Since $R_h \cap G_0 = 1$, this implies $r = 1$, and thus some $p_i = 1$, contrary to hypothesis.

(2.2) COROLLARY. *Let $F$ be freely generated by a set $X$, where $X$ is the*

*disjoint union of a set $Y$ together with a family of sets $X_h$ indexed by the integers. Let $m$ be an integer such that $m \geqq 0$. For each integer $h$, denote by $F_h$ the subgroup of $F$ generated by $Y \cup X_h \cup \cdots \cup X_{h+m}$. For each $h$, let $R_h$ be a normal subgroup of $F_h$ such that $R_h \cap F_k = 1$ for all $k \neq h$, and let $R$ be the normal subgroup of $F$ defined by all the $R_h$ together. Then there exist for all $h$ transversals $U_h$ for $F_h R$ in $F$, with $1 \in U_h$, such that $R$ is the free product of all the groups $R_h^u$ for which $u \in U_h$.*

**Proof.** For integers $p$ and $q$, let $F_{p,q}$ be the group generated by all the $F_h$ with $p \leqq h \leqq q$. By Corollary (1.8) of [6], the group $R_{p,q} = R \cap F_{p,q}$ is defined by all the $R_h$ with $p \leqq h \leqq q$. Suppose that, for each $h$, $p \leqq h \leqq q$, there exists a transversal $U_h^{p,q}$ for $F_h R_{p,q}$ in $F_{p,q}$, with $1 \in U_h^{p,q}$, and such that $R_{p,q}$ is the free product of all the groups $R_h^u$ for $p \leqq h \leqq q$ and $u \in U_h^{p,q}$. We shall show that the same holds for $F_{p,q+1}$, and with $U_h^{p,q} \subseteq U_h^{p,q+1}$ for each $h$, $p \leqq h \leqq q$.

By Corollary (1.8) of [6], the group $F_{p,q+1}$, as free product of $F_{p,q}$ and $F_{q+1}$, with normal subgroups $R_{p,q+1}$, $R_{p,q}$, and $R_{q+1}$, satisfies the hypotheses of Lemma (2.1). Therefore there are transversals $A_{p,q}$ and $A_{q+1}$, each containing 1, such that $R_{p,q+1}$ is the product of groups of the form $R_h^{ua_1 \cdots a_n}$, $p \leqq h \leqq q$, $n \geqq 0$, $u \in U_h^{p,q}$, $a_2, a_4, \cdots \in A_{p,q}$, $a_1, a_3, \cdots \in A_{q+1}$, or of the form $R_{q+1}^{a_1 \cdots a_n}$, $n \geqq 0$, $a_2, a_4, \cdots \in A_{q+1}$, $a_1, a_3, \cdots \in A_{p,q}$. It is clear from the normal form in $F_{p,q+1}/R_{p,q+1}$, as free product of $F_{p,q}R_{p,q+1}/R_{p,q+1} \simeq F_{p,q}/R_{p,q}$ and $F_{q+1}R_{p,q+1}/R_{p,q+1} \simeq F_{q+1}/R_{q+1}$, that the set $U_{q+1}^{p,q+1}$ of all $a_1 \cdots a_n$ with the $a_i \neq 1$ alternately from $A_{p,q}$ and $A_{q+1}$, beginning with $a_1 \in A_{p,q}$ is a transversal for $F_{q+1}R_{p,q+1}$ in $F_{p,q+1}$. It is clear on the same grounds that, for $p \leqq h \leqq q$, the set $U_h^{p,q+1}$ of all $ua_1 \cdots a_n$, with $u \in U_h^{p,q}$ and the $a_i \neq 1$ alternately from $A_{q+1}$ and $A_{p,q}$, beginning with $a_1 \in A_{q+1}$, contains a transversal for $F_h R_{p,q+1}$ in $F_{p,q+1}$. Also, $U_h^{p,q} \subseteq U_h^{p,q+1}$. To show that $U_h^{p,q+1}$ is a transversal, we note that, from the normal form, $u' a_1' \cdots a_{n'}' \in F_h R_{p,q+1} u a_1 \cdots a_n$ implies $n = n'$ and $a_1 = a_1', \cdots, a_n = a_n'$; it also implies that $u' \in F_h R_{p,q+1} u$, whence, by the Freiheitssatz, $u' \in F_h R_{p,q} u$ and since $u, u' \in U_h^{p,q}$, a transversal for $F_h R_{p,q}$, that $u' = u$.

For $p = q = 0$ the hypothesis on $F_{p,q}$ is trivial. Applying the result just established successively to $F_{0,0}$, $F_{0,1}$, $F_{-1,1}$, $F_{-1,2}$, $F_{-2,2}$, $\cdots$ we obtain for each $h$ a chain of transversals $U_h^{-q,q}$, $q = h, h+1, \cdots$. It is now immediate that the sets $U_h = \bigcup_{q \geqq h} U_h^{-q,q}$ are transversals for $F_h R$ in $F$ with the required property.

3. **Free products, continued.** We now seek to gain information about a free factor from assumptions on a free product.

We begin with some general considerations. Let $G$ be any group, equipped with two functions, $\rho$ one-to-one from $G$ into some well-ordered set, and $L$ from $G$ into the non-negative integers, such that $L(g) < L(h)$ implies $\rho(g) < \rho(h)$. With each subset $C$ of $G$ we associate a set $C'$, obtained from $C$ by replacing each $c$ in $C$ by $c'$, where $c'$ is that element $c^h$, for $h \in gp(d : d \in C, L(d) < L(c))$, for

which $\rho(c^h)$ is a minimum. We define the *reduct* $C^x$ of $C$, with respect to $r$ and $L$, to be the set $C^x = \bigcup_{n \geqq 0} \bigcap_{m \geqq n} C^{(m)}$, consisting of all elements $c$ that belong to every member of the sequence $C$, $C'$, $C''$, $\cdots$ from some member $C^{(n)}$ on. Each element $c$ in $C$ has a conjugate $c^u$ *in* $C^x$, with $u \in gp\, C$. For $c$ has such a conjugate in each $C^{(n)}$, and, if none of these were in $C^x$, we should have an infinite decreasing sequence of elements.

(3.1) PROPOSITION. $C^{x'} = C^x$; *that is, if* $c \in C^x$ *and* $h \in gp(d : d \in C^x, L(d) < L(c))$, *then* $\rho(c^h) \geqq \rho(c)$.

**Proof.** Suppose the assertion false. Then there exist $c \in C^x$ and $d_1, \cdots, d_k \in C^x$ for some $k$, with $L(d_1), \cdots, L(d_k) < L(c)$, and $h \in gp(d_1, \cdots, d_k)$, such that $\rho(c^h) < \rho(c)$. From the definition of $C^x$ there must exist some $n$ such that $c, d_1, \cdots, d_k \in C^{(m)}$ for all $m \geqq n$. In the passage from $C^{(n)}$ to $C^{(n+1)}$, $c$ is replaced by some $c' = c^g$ with $\rho(c^g) = \rho(c^h) < \rho(c)$; and, in view of these inequalities, $c$ cannot be introduced into $C^{(n+1)}$ as $d'$ for any $d \in C^{(n)}$. But this implies that $c \notin C^{(n+1)}$, a contradiction.

(3.2) PROPOSITION. $gp\, C^x = gp\, C$.

**Proof.** It is clear that $gp\, C^x \subseteq gp\, C$. For the converse, we show by induction on $\rho(c)$ that $c \in C^{(n)}$, $n \geqq 0$, implies $c \in gpC^x$. In the initial case, where $\rho(c)$ is a minimum, $\rho(c^h) \leqq \rho(c)$ implies $c^h = c$, whence $c \in C^{(m)}$ for all $m \geqq n$. For the induction, we assume the conclusion for all $d$ with $\rho(d) < \rho(c)$. If $c \in C^{(n)}$ but not $c \in gpC^x$, then, for some $m$, $c \in C^{(m)}$ but not $c \in C^{(m+1)}$. This implies that there exist $d_1, \cdots, d_k \in C^{(m)}$ with $L(d_1), \cdots, L(d_k) < L(c)$, and $h \in gp(d_1, \cdots, d_k)$, such that $c^h \in C^{(m+1)}$ and $\rho(c^h) < \rho(c)$. Now $\rho(d_1), \cdots, \rho(d_k) < \rho(c)$, whence, by the induction hypothesis, $d_1, \cdots, d_k \in gp\, C^x$, and $h \in gp\, C^x$. Likewise, $c^h \in gp\, C^x$. Now it follows that $c \in gp\, C^x$, a contradiction.

(3.3) PROPOSITION. *If* $C$ *freely generates* $gpC$, *then* $C^x$ *freely generates* $gp\, C$.

**Proof.** Assume that $C$ is free, that is, freely generates $gp\, C$. Every finite set of elements from $C^x$ lies in some $C^{(m)}$. Therefore it suffices to show that each $C^{(m)}$ is free, and, by induction, it suffices to show that $C'$ is free. Finally, it is enough to show that every finite subset $D'$ of $C'$ is free.

The set $D'$ consists of all replacements $c'$ for elements $c$ in some finite subset $D$ of $C$. Let $E$ be a minimal set with the property that $D \subseteq E$ and that whenever $c \in E$ is replaced by $c' = c^h$ in $C'$, then $E$ contains elements $d_1, \cdots, d_k \in C$ with $L(d_1), \cdots, L(d_k) < L(c)$, such that $h \in gp(d_1, \cdots, d_k)$. It follows, by a well-known theorem on graphs, that $E$ is finite; we suppose its elements $c_1, \cdots, c_n$ ordered in such a way that $L(c_1) \leqq L(c_2) \leqq \cdots \leqq L(c_n)$. Then each $c_k' = c_k^h$ for some $h \in gp(c_1, \cdots, c_{k-1})$, so that, successively replacing $c_n$ by $c_n', \cdots, c_1$ by $c_1'$, we pass from $E$, which is free as a subset of $C$, to a free set $E'$ containing $D'$.

(3.4) LEMMA. *Let a group* $G$ *be the free product of its subgroups* $G_1$ *and* $G_2$,

*with intersection $G_0 = G_1 \cap G_2$. Let $R_1$ be a normal subgroup of $G_1$ such that $R_1 \cap G_0 = 1$, and let $R$ be the normal subgroup of $G$ defined by $R_1$. Then there exist functions $\rho$ and $L$ on $G$ such that, if $C$ is any set of conjugates of elements from $R_1$ that generates $R$, then the reduct $C^x$ of $C$ generates $R$ and $C^x \cap R_1$ generates $R_1$.*

**Proof.** We first define the functions $\rho$ and $L$. Each element $g \in G$ can be written in the form $g = a_0 b_1 a_1 \cdots b_n a_n$ where all $a_i \in G_1$, all $b_i \in G_2$, and $b_1, a_1, \cdots, b_n \notin G_0$. The number $n$ is independent of the representation, and we define $L(g) = n$. Let $W$ be the set of all finite sequences $w = (b_1, a_1, \cdots, b_n, a_n)$, $n \geqq 0$, where all $a_i \in G_1$, all $b_i \in G_2$, and $b_1, a_1, \cdots, b_n \notin G_0$. Let $G$ be well ordered, and well order $W$, first, according to $n$, and, for fixed $n$, by inverse lexical order induced by the order on $G$. Let $K$ be the set of all conjugates of elements of $R_1$. For $q$ in $K$ we define $\rho(q) = w = (b_1, a_1, \cdots, b_n, a_n)$ for that $w$ of lowest order such that $q = r^{b_1 a_1 \cdots a_n}$ for some $r \in R_1$. The condition $R_1 \cap G_0 = 1$ implies that $L(q) = 2n$, whence, for $q, q' \in K$, we have that $L(q) < L(q')$ implies $\rho(q) < \rho(q')$. Clearly we may extend $\rho$ to the remaining elements of $G$ in such a way that, for all $g$, $h \in G$, $L(g) < L(h)$ implies $\rho(g) < \rho(h)$.

From the fact that $C \subseteq K$ it follows by the definition of $C^x$ that $C^x \subseteq K$. From the fact that $C$ generates $R$ it follows by Proposition (3.2) that $C^x$ generates $R$. It remains to show that $C^x \cap R_1$ generates $R_1$.

For each $g \in G$, define $Q_g = gp(R_1^g \cap C^x)$; we must show that $R_1 \subseteq Q_1$. Since $R$ is generated by $C^x$, and $C^x$ is contained in the union of the $Q_g$, each element of $R$ can be written as a product $r = q_1 \cdots q_m$, $m \geqq 0$, with each $q_i$ in some $Q_g$. Supposing now that there exists some $r$ in $R_1$ but not in $Q_1$, we choose such an $r = q_1 \cdots q_m$ with $m$ as small as possible. Then it is clear that $m \geqq 1$, that no adjacent $q_i$ and $q_{i+1}$ come from the same $Q_g$, and that $q_1, q_m \notin Q_1$. We may suppose each $q_i = s_i^{g_i}$ for some $s_i \neq 1$ in $R_1$ and for $g_i = b_{i1} a_{i1} \cdots b_{in_i} a_{in_i}$ where $\rho(q_i) = (b_{i1}, \cdots, a_{in_i})$.

We shall show that each $g_i \bar{g}_{i+1}$, for $1 \leqq i \leqq m-1$, has a representation $u_n$ as a product of factors alternately from $G_1$ and $G_2$, with none in $G_0$, and such that the representation

$$r = \bar{g}_1 s_1 u_1 s_2 u_2 \cdots u_{m-1} s_m g_m$$

yields such an alternating product after grouping together successive factors from the same group $G_1$ or $G_2$. From this it will follow that $L(r) \geqq L(\bar{g}_1) > 0$, contradicting the assumption that $r$ is in $R_1$.

First, suppose that the terminal string of factors common to $g_i$ and $g_{i+1}$ exhausts neither. Then, after cancelling such factors, $g_i \bar{g}_{i+1}$ either has the form $b_{i1} \cdots b_{ih} b_{i+1,k} \cdots b_{i+1,1}$ or $b_{i1} \cdots a_{i,h} a_{i+1,k} \cdots b_{i+1,1}$ for some $h, k \geqq 1$. Now $b_{i,h} b_{i+1,k} \in G_0$ or $a_{i,h} a_{i+1,k} \in G_0$ would contradict the minimality of $\rho(q_i)$ and $\rho(q_{i+1})$. Therefore, after combining these two factors, we have an alternating product

$$q_iq_{i+1} = \bar{g}_is_iu_is_{i+1}g_{i+1}.$$

Second, we observe that $g_ig_{i+1} \in G_1$ is impossible, since this would imply that both $q_i$ and $q_{i+1}$ belonged to the same group $Q_{g_i} = Q_{g_{i+1}}$.

Third, suppose that $g_{i+1} = b_{i+1,1} \cdots a_{i+1,k}g_i$ for some $k \geqq 1$. Then $q_i\bar{g}_{i+1} = \bar{g}_is_i\bar{a}_{i+1,k} \cdots \bar{b}_{i+1,1}$. If $s_i\bar{a}_{i+1} \in G_0$, we should have $L(q_i\bar{g}_{i+1}) < L(\bar{g}_{i+1})$ and thus $L(q_iq_{i+1}\bar{q}_i) < L(q_{i+1})$. The same inequality would hold if we replace $q_{i+1}$ by $q'_{i+1} \in R_1^{g_1} \cap C^x$, and, since $\bar{q}_i$ is in the group $Q_{gi}$ generated by all $d \in R_1^{g_i} \cap C^x$, for which $L(d) = L(q_i) < L(q'_{i+1})$, this would contradict Proposition (3.1). Thus, in this case as well, the product $\bar{g}_is_iu_is_{i+1}g_{i+1}$ becomes alternating after combining adjacent parts from the same group $G_1$.

To complete the proof, it will suffice to show that, for three consecutive factors, the product $q_{i-1}q_iq_{i+1}$ has a representation $\bar{g}_{i-1}s_{i-1}u_{i-1}s_iu_is_{i+1}g_{i+1}$ with the required property. This follows directly from what has been established above except possibly in the case that $g_i$ ends both $g_{i-1}$ and $g_{i+1}$. Suppose, then, that $g_{i-1} = b_{i-1,1} \cdots a_{i-1,h}g_i$ and $g_{i+1} = b_{i+1} \cdots a_{i+1,k}g_i$, where $h, k \geqq 1$. Then

$$q_{i-1}q_iq_{i+1} = \bar{g}_{i-1}s_{i-1}b_{i-1,1} \cdots a_{i-1,h}s_i\bar{a}_{i+1,k} \cdots \bar{b}_{i+1,1}s_{i+1}g_{i+1},$$

and we show that $a = a_{i-1,h}s_i\bar{a}_{i+1,k} \notin G_0$. If we had $a \in G_0$, then we should have $q_{i-1}^{q_i} = s_{i-1}^{g'_{i-1}}$ where $g'_{i-1} = b_{i-1,1} \cdots a_{i-1,h-1}b'_{i-1,h}a_{i+1,k}g_i$, with $b'_{i-1,h} = b_{i-1,h}a$. By Proposition (3.1), $\rho(q_{i-1}^{q_i}) \geqq \rho(q_{i-1})$, whence, first, $L(q_{i-1}^{q_i}) = L(q_{i-1})$ and, second, comparing the sequences of factors of $g_{i-1}$ and of $g'_{i-1}$ in inverse lexical order, we conclude that $a_{i+1,k} \geqq a_{i-1,h}$. A symmetric argument gives $a_{i-1,h} \geqq a_{i+1,k}$, whence $a_{i-1,h} = a_{i+1,k}$. But this implies that $a = s_i^{\bar{a}_{i-1,h}} \in R_1$, and, since also $a \in G_0$, while $R_1 \cap G_0 = 1$, we conclude that $a = 1$, whence $s_i = 1$ and $q_i = 1$, contrary to fact that $q_{i-1}$ and $q_i$ do not belong to the same group $Q_g$. This completes the proof of Lemma (3.4).

## 4. The Main Theorem.

(4.1) MAIN THEOREM. *Let $F$ be a free group, $R$ the normal subgroup of $F$ defined by an element $r \neq 1$ of $F$, and $Q$ the centralizer of $r$ in $F$. Then there exists a transversal $U$ for $QR$ in $F$ such that $R$ is freely generated by the set of all elements $r^u$ for $u$ in $U$.*

Before proceeding to the proof, by induction on the length of $r$, we assemble some lemmas.

(4.2) LEMMA. *Let $r = x^n$, $n \neq 0$, where $x$ belongs to a free set $X$ of generators for $F$. Then the conclusion of the Main Theorem holds.*

**Proof.** The group $F$ is the free product of its subgroups $F_1$, generated by $x$, and $F_2$, generated by $X - \{x\}$; and $F_0 = F_1 \cap F_2 = 1$. Let $R_1 = gp(r)$ and $R_2 = 1$. By Lemma (2.1), $R$ is the free product of groups $R_1^u$, where $u$ runs through

a transversal $U$ for $F_1R$ in $F$. Thus $R$ is freely generated by the set of $r^u$ for $u$ in $U$, and, since $F_1 = Q$, the centralizer of $r$ in $F$, the conclusion holds.

(4.3) LEMMA. *Let $X$ be a free set of generators for $F$, let $x \in X$, let $m$ be an integer, and let $F'$ be the subgroup of $F$ generated by $x^m$ together with $X - \{x\}$. Let $R'$ be the normal subgroup of $F'$ defined by an element $r$ in $F'$, and let $R$ be the normal subgroup of $F$ defined by $r$. If the conclusion of the Main Theorem holds for $r$ in $F$, then it holds for $r$ in $F'$.*

**Proof.** The group $F$ is the free product of its subgroups $F_1$, generated by $x$, and $F_2 = F'$; and $F_0 = F_1 \cap F_2 = gp(x^m)$. In view of Lemma (4.2), we may assume that $r$ is not a power of $x$; then it follows by the Freiheitssatz that $R \cap F_0 = 1$. Let $R_1 = 1$ and $R_2 = R'$. Since the centralizer $Q$ of $r$ in $F$ is generated by some $q$ such that $r = q^e$, $e > 0$, and $r \in F'$, it follows that $q \in F'$ and $Q$ is also the centralizer of $r$ in $F'$. Assume now that $U$ is a transversal for $QR$ in $F$ such that $R$ is freely generated by the set $C = r^U = \{r^u : u \in U\}$. The hypotheses of Lemma (3.4) are satisfied (with subscripts 1 and 2 exchanged), and it follows that that $R'$ is freely generated by $C^x \cap R'$ where $C^x$ is a reduct of $C$. From the definition of a reduct, together with the hypothesis on $C$, it follows that $C^x = r^V$, where $V$ is a transversal for $QR$ in $F$. Let $u \in F'$; then $u \in QRv$ for some $v \in V$, hence $u = q^f vs$ for some integer $f$ and some $s \in R$. Since $C^x$ generates $R$, $s = \prod_1^n c_i^{e_i}$ for some $n \geqq 0$, $c_i \in C^x$, and $e_i = \pm 1$. Since $C^x \cap R'$ generates $R'$, and $r^u \in R'$, we have similarly $r^u = \prod_1^m c_j^{f_j}$ for some $m \geqq 0$, $c_j \in C^x \cap R'$, and $f_j = \pm 1$. If $v \notin F'$, then the factor $c = r^v$ occurs, with exponent $\pm 1$, an odd number of times in two members of the equation $r^u = \bar{s} r^v s$, when written in terms of the elements of $C^x$, as $\prod_1^m c_j^{f_j} = (\prod_1^n c_i^{e_i})^{-1} c (\prod_1^n c_i^{e_i})$; and this contradicts the fact that $C^x$ freely generates $R$. It follows that $V \cap F'$ contains a transversal $V'$ for $QR'$ in $F'$, hence that $V \cap F' = V'$, and that $R'$ is freely generated by $C^x \cap R' = r^{V'}$, as required.

(4.4) LEMMA. *Let $X$ be a free set of generators for $F$, and let a certain $x \in X$ occur in $r$ with exponent sum 0. Let $n$ be the number of occurrences in $r$ of letters other then $x$ and $\bar{x}$ and assume that the Main Theorem holds for every element $r'$ of a free group $F'$ that has length no greater than $n$ with respect to some free set of generators for $F'$. Then the Main Theorem holds for $r$.*

**Proof.** Let $F^x$ be the subgroup of $F$ comprising all elements in which $x$ has exponent sum 0. Then $F^x$ is freely generated by the set of all elements $y_k = y^{x^k}$ for $y \in X$, $y \neq x$, and $k$ an integer. Moreover, $R$ is contained in $F^x$ and is the normal subgroup of $F^x$ defined by all the elements $r_k = r^{x^k}$. Let $a$ be the least index $k$ such that some $y_k$ occurs in $r$, when written as a word in the $y_k$, and let $b$ be the greatest such index. Then $r$ is in the group $F_a$ generated by all $y_k$ such that $a \leqq k \leqq b$. Let $R_a$ be the normal subgroup of $F_a$ defined by $r$, and, for all

integers $p$, let $F_{a+p} = F_a^{x^p}$ and $R_{a+p} = R_a^{x^p}$. It follows by the Hauptform of the Freiheitssatz that $F^x$ with its subgroups $F_h$ and $R_h$ satisfies the hypothesis of Corollary (2.2), and we conclude that there exist transversals $U_h$ for the groups $F_hR$ in $F^x$, such that $R$ is the free product of all the groups $R_h^u$ with $u \in U_h$.

Now $r$, as a word in the generators $y_k$ for $F_a$, has length $n$. By hypothesis, $R_a$ is freely generated by a transversal $V_a$ for $Q_aR_a$ in $F_a$, where $Q = Q_a$ is the centralizer of $r$ in $F$ and in $F_a$. It follows that $R$ is freely generated by the $r^w$ for all $w$ in $W$, the union of the sets $x^pV_{a+p}U_{a+p}$, where $V_{a+p} = V_a^{x^p}$. To show that $W$ is a transversal for $QR$ in $F$, consider arbitrary $g \in F$. For some integer $p$, $g = x^ph$, with $h \in F^x$. Now $h \in Rfu$ for some $f \in F_{a+p}$ and $u \in U_{a+p}$. Moreover, $f \in R_{a+p}qv$ for some $q \in Q_{a+p} = Q^{x^p}$ and $v \in V_{a+p}$. Therefore, $g \in x^pRqvu = Rq^{x^{-p}}x^pvu \subseteq RQx^pvu = QRw$ with $w = x^pvu$. This shows that each $g \in QRw$ for some $w \in W$; since $w$ is clearly uniquely determined by $g$, it follows that $W$ is a transversal for $QR$ in $F$, as required.

We now carry out the proof of the Main Theorem, by induction on the length of $r$ with respect to a free set $X$ of generators for $F$. Lemma (4.2) contains the initial case, that $r$ has length 1. We may assume then that $r$ has length $n > 1$ with respect to some free set $X$ of generators for $F$, and that the Main Theorem holds for all $r'$ in $F'$ with length less than $n$ with respect to some free set of generators for $F'$. In view of Lemma (4.2) we may also assume that two distinct generators $x$ and $y$ from the set $X$ actually occur in $r$. If either $x$ or $y$ occurs in $r$ with exponent sum 0, the conclusion follows by Lemma (4.4). Therefore we may assume that $x$ occurs in $r$ with exponent sum $a \neq 0$, and that $y$ occurs in $r$ with exponent sum $b \neq 0$. We can embed $F$ in a group $F'$, freely generated by $X - \{x\}$ together with an element $x_1$ such that $x_1^b = x$. Now $F'$ is also freely generated by the set $X'$ consisting of $X - \{x,y\}$ together with $x_1$ and $y_1 = yx_1^a$. Now $r$, written as a word in the elements of $X'$, contains $x_1$ with exponent sum 0; moreover, the total number of occurrences of letters other than $x_1$ and $\bar{x}_1$ in $r$, thus written, is the same as the total number of occurrences of letters other than $x$ and $\bar{x}$ in $r$, written as a word in the elements of $X$, and is therefore less than $n$. By Lemma (4.4) and the induction hypothesis, it follows that the Main Theorem holds for $r$ as an element of $F'$. By Lemma (4.3), it follows that the Main Theorem holds for $r$ as an element of $F$. This completes the proof of the Main Theorem.

REMARK. The proof of the Main Theorem provides an effective construction for $C$. Indeed, it determines a particular $C$ together with a method for deciding, for arbitrary $w$ in $F$, whether $w$ is in $C$. We have to consider the effectiveness of the inductive procedure of Corollary (2.2) and of the reduction procedure of §3. The former is immediate once we have an effective construction for the transversals occuring and this is provided by Magnus's solution in [9] for the generalised word problem. The reduction process, leading to $C^x$ from $C$, is not effective. But it is possible to modify the procedure (in the case when $F$ is finitely generated, to which the general case can be reduced) so that $C^{(n+1)}$ is obtained by

altering only a finite number of elements of $C^{(n)}$ in a way which can be effectively determined. $C^x$ will still not be effective, or even effectively enumerated. However, the set $D$ of elements of zero length occurring in $C^x$ is effectively enumerated, since it consists of those elements of zero length occurring in $C^{(n)}$ for some $n$. We can determine effectively whether a given conjugate $r^v$ of $r$ occurs in $D$ by enumerating the elements $r^u$ of $D$, checking for each such element whether $u$ and $v$ are in the same coset mod $QR$. Since $D$ contains exactly one element $r^u$ for each coset, we will ultimately discover the element $r^u$ in $D$ for which $u$ and $v$ are in the same coset and so will determine whether or not $r^v$ is in $D$.

It should be noticed, however, that in the proof of Corollary (2.2) the transversals $U_h$ were obtained as unions of ascending chains of sets $U_h^{p,q}$, and the choice of the particular chains, and of the sets $U_h^{p,q}$, used there was to some extent arbitrary; in consequence we do not have any simple and natural description of the sets $U_h$. Also the well-ordering used in Lemma (3.4) is not uniquely defined. In connection with the Main Theorem, these ambiguities are reflected by the fact that we do not have any satisfactory criterion, such as, possibly, the Schreier condition, ensuring that a transversal $U$ for $QR$ in $F$ have the property that $r^U$ freely generate $R$.

The Identity Theorem is an immediate consequence of the Main Theorem.

(4.5) COROLLARY (IDENTITY THEOREM). *Let $R$ be the normal subgroup of a free group $F$ defined by an element $r \in F$, $r \neq 1$; let $R'$ be the derived group of $R$, and $Q$ the centralizer of $r$ in $F$. If $\prod_1^n r^{e_i w_i} \in R'$ for some $n \geqq 0$, $e_i = \pm 1$, and $w_i \in F$, then the factors fall into pairs such that $e_i = -e_j$ and $w_i \in QRw_j$.*

**Proof.** By the Main Theorem, $R$ is freely generated by a set $C = r^U$, for $U$ a transversal for $QR$ in $F$. Thus each $w_i = q_i u_i s_i$ for some $q_i \in Q$, $s_i \in R$, and $u_i \in U$. It follows that $\prod_1^n r^{e_i u_i} \in R'$. The conclusion now follows from the fact that the $r^{u_i}$ belong to a free set of generators for $R$.

We show next that the only sets $C$ of conjugates of $r$ that freely generate $R$ are those of the form $C = r^U$, for $U$ a transversal for $QR$ in $F$, as provided by the Main Theorem.

(4.6) COROLLARY. *Let $R$ be the normal subgroup of a free group $F$ defined by an element $r$ of $F$, and let $Q$ be the centralizer of $r$ in $F$. If a set $C$ of conjugates of $r$ generates $R$, then $C$ contains $r^U$ for some transversal $U$ for $QR$ in $F$.*

**Proof.** Let $v$ be any element of $F$. Since $C$ generates $R$, we have $r^v = \prod r^{e_i u_i}$ for some $e_i = \pm 1$ and some $u_i \in F$ such that $r^{u_i} \in C$. By the Identity Theorem, some $u_i \in QRv$. It follows that the set of $u$ such that $r^u \in C$ contains a transversal for $QR$ in $F$.

(4.7) COROLLARY. *If $C$, as above freely generates $R$, then $C = r^U$ for some transversal $U$ for $QR$ in $F$.*

**Proof.** By Corollary (4.6), $C$ contains $r^U$ for some transversal $U$. Suppose that $C$ contained distinct elements $r^u$ and $r^v$ such that $u \in QRv$. Then $u = qvs$ for some $q \in Q$ and $s \in R$. Since $C$ generates $R$, we have $s = \prod c_i^{e_i}$ for some $c_i \in C$ and $e_i = \pm 1$. It follows that $r^u = (\prod c_i^{e_i})^{-1} r^v (\prod c_i^{e_i})$, a relation among the elements $r^u$, $c_i$, $r^v$ of $C$ that is not trivial, since $r^u$ enters an odd number of times. This contradicts the assumption that $C$ freely generates $R$.

It is not true that $C = r^U$ generates $R$ for every transversal $U$ for $QR$ in $F$. To illustrate this, let $F$ have two free generators $x$ and $y$, and take $r = x$. The set $U$ consisting of $\bar{y}\bar{x}yx$ together with all $y^n$ for $n \neq 0$ is a transversal. From the fact that less than half of each factor can cancel in forming the product of $r^{eu}$ and $r^{fv}$ for $e, f = \pm 1$, $u, v \in U$ and $r^{eu} r^{fv} \neq 1$, it follows that $r = x$ is not in the subgroup generated by $r^U$.

On the other hand, for every transversal $U$ for $QR$ in $F$, the set $C = r^U$ freely generates some subgroup of $R$. This follows from the more general observation that, if $X$ is a free set of generators for a group $F$, and $X'$ is a set containing exactly one conjugate of each element in $X$, then $X'$ freely generates a subgroup $F'$ of $F$. To see this, it suffices to show that every finite subset $X''$ of $X'$ freely generates a subgroup $F''$ of $F$. The canonical map of $F$ into its commutator quotient group maps $F''$ onto a free abelian group of rank $n$, the number of elements in $X''$. It follows that $F''$, which, as a subgroup of $F$, is a free group, has rank at least $n$; since the set $X''$ of $n$ elements generates $F''$, it follows that $X''$ generates $F''$ freely(2).

Finally, we remark that for the set $r^U$ to freely generate a subgroup $R'$ of $R$ does not imply that $U$ is contained in a transversal. To illustrate this, let $F$ be freely generated by two elements $x$ and $y$, let $r = x$, and let $U$ consist of the two elements $yx$ and $yx^2$.

5. **An Elimination Theorem.** We prove a theorem that contains a refinement of both the Hauptform of the Freiheitssatz and the Identity Theorem.

Let $p_1, \cdots, p_n$, $n \geqq 0$, be a sequence of elements from a group $F$. A second sequence $q_1, \cdots, q_m$, $m \geqq 0$ is obtained from the first by a *Peiffer transformation* if it is obtained by deleting a pair $p_i$, $p_{i+1}$ in case that $p_i p_{i+1} = 1$, or by replacing a pair $p_i$, $p_{i+1}$ by the pair $p_{i+1}$, $\bar{p}_{i+1} p_i p_{i+1}$ or by the pair $p_i p_{i+1} \bar{p}_i$, $p_i$.

(5.1) ELIMINATION THEOREM. *Let $F$ be freely generated by set a $X$ together with distinct elements $x_a$, $x_{a+1}, \cdots, x_{b+l}$, where $a$, $b$, and $m$ are integers such that $a \leqq b$ and $l \geqq 0$. For each integer $k$ such that $a \leqq k \leqq b$, let there be given a cyclically reduced word $r_k$ such that $k$ is the least, and $k+l$ the greatest, of the indices $h$ appearing on letters $x_h$, $\bar{x}_h$ that occur in $r_k$. Let $p = p_1 \cdots p_n$, $n \geqq 0$, where each $p_i$ is a conjugate of some $r_k$ or $\bar{r}_k$. Suppose that $c$ is the least, and $d + l$ the greatest, of the indices $h$ appearing on letters that occur in $p$. Then*

(2) The authors thank the referee for this simplified argument.

*$p = q_1 \cdots q_m$, $m \geqq 0$, where each $q_i$ is a conjugate of some $r_k$ or $\bar{r}_k$ for $c \leqq k \leqq d$, and where the sequence $q_1, \cdots, q_m$ is obtained from $p_1, \cdots, p_n$ by a succession of Peiffer transformations.*

**Proof.** The group $F$ is the free product of its subgroups $F_1$, generated by $X$ together with all the $x_h$ for $c \leqq h \leqq d + l$, and $F_2$, generated by $X$ together with the remaining $x_h$; and $F_0 = F_1 \cap F_2$ is generated by $X$. By the Hauptform of the Freiheitssatz, $R_1 = R \cap F_1$ is the normal subgroup of $F_1$ defined by all the $r_h \in F_1$, $R_2 = R \cap F_2$ is the normal subgroup of $F_2$ defined by all the $r_h$ in $F_2$, and $R \cap F_0 = 1$. By Lemma (2.2), and the Main Theorem, $R$ is freely generated by a set $C$ of conjugates of $r_h$ such that $C \cap R_1$ freely generates $R_1$.

Let $p_i = r_h^{eu}$, $e = \pm 1$, $u \in F$; since $p_i$ is equal to a word in the elements of $C$, it follows by the Identity Theorem that $r^u = r^{vs}$ for some $v$ such that $r_h^v \in C$ and some $s \in R$. Writing $s$ as a word in the elements of $C$, we obtain for $p_i = \bar{s}(r_h^v)^e s$ an expression as a word in the elements of $C$. We apply successively to the sequence $p_1, \cdots, p_n$ Peiffer transformations decreasing the sum of the lengths of the $p_i$, as reduced words in the elementof $C$, until we arrive at a sequence $q_1, \cdots, q_m$ to which no further transformation of this sort is possible.

Each $q_i$ has reduced form $q_i = \bar{w}_i t_i w_i$ where $t_1$ or $\bar{t}_i \in C$, written as a word in the elements of $C$. We argue that neither $t_i$ or $t_{i+1}$ can cancel in forming the reduced word for $q_i q_{i+1}$. If $L(q_i) = L(q_{i+1})$, such cancellation would imply $q_i q_{i+1} = 1$, contrary to the hypothesis on the sequence of $q_i$. If, say $L(q_i) < L(q_{i+1})$, then the part $t_i w_i$ of $q_i$ would have to cancel into $\bar{w}_{i+1}$, giving $L(q_i \bar{w}_{i+1}) < L(\bar{w}_{i+1})$ and hence $L(q_{i+1}) < L(q_{i+1}^{q_i})$, again contrary to hypothesis. Thus the reduced word for $p = q_1 \cdots q_m$ in terms of the elements of $C$ contains all the $t_i^{\pm 1}$. But $p$, by hypothesis, is in $R_1$, generated by $C \cap R_1$. It follows that all the $t_i^{\pm 1} \in C \cap R_1$, whence all the $t_i$ and thus all the $q_i$ are conjugates of elements $r_h$ or $\bar{r}_h$ for $c \leqq h \leqq d$.

The following Corollary contains the Identity Theorem.

(5.2) COROLLARY. *Under the hypothesis of Theorem* (5.1), *those factors $p_i$ that are conjugates of $r_h^{\pm 1}$, for $h$ not in the interval $c \leqq h \leqq d$, fall into pairs $p_i$, $p_j$ of the form $p_i = r_h^u$, $p_j = r_h^{-v}$ where $u$ and $v$ are congruent modulo $R$.*

REMARK. Theorem (5.1) does not provide, without a knowledge of $C$, a practical method for obtaining the sequence $q_1, \cdots, q_m$ from $p_1, \cdots, p_n$. However, it is easily seen that this can be accomplished by a succession of Peiffer transformations, each of which diminishes the total number of occurrences of letters $x_h$, for $h$ not in the interval $c \leqq h \leqq d + m$, in the factors $p_i$, written as words in the original set of free generators for $F$.

6. **A related theorem.** Greendlinger [3] has given a condition, which is effective if $S$ is finite, on a set $S$ of elements in the group $F$ freely generated by a set $X$, which implies the following condition:

(*) Every element $r \neq 1$ of the normal subgroup $R$ of $F$ defined by $S$ when

written as a reduced word in the elements of $X$, contains more than half of the reduced word for some element of $S$.

(6.1) THEOREM. *If $S$ satisfies condition (*), then $R$ is freely generated by a set of conjugates of elements of $S$.*

**Proof.** Federer and Jónsson [2] have shown that $R$ has a basis $U$, well-ordered by a relation $u < v$, with the property that, if $r \in R$ and $u \in U$ and $r$ has length $L(r) < L(u)$, then $r$ lies in the subgroup $R_u = gp(v : v \in U, v < u)$. It will suffice to construct an ascending chain of sets $C_u$ of conjugates of elements of $S$ such that, for each $u \in U$, $C_u$ freely generates $R_u$. Supposing, then, that for some $u \in U$, such a set $C_u$ freely generates $R_u$, we must find a conjugate $c$ of an element of $S$ such that $C_u$ together with $c$ freely generates the group $R'_u = gp(v : v \in U, v \leqq u)$. By the hypothesis (*), $u$ has reduced form $u = aqb$ where some cyclic conjugate $s$ of an element in $S$ has reduced form $s = pq$, with $L(p) < L(q)$. It follows that $v = us^{\bar{b}} = a\bar{p}b$ is shorter than $u$, whence $v \in R_u$ and $c = s^{\bar{b}} \in R'_u$. Since it is clear that $C_u$ together with $u$ freely generates $R'_u$, it follows that $C_u$ together with $c$ freely generates $R'_u$.

We remark that, if $S$ is finite, this construction can be used to provide a basis $C$ for which it is decidable, for arbitrary $w$ in $F$, whether $w$ belongs to $C$.

## BIBLIOGRAPHY

1. D. E. Cohen, *A topological proof in group theory*, Proc. Cambridge Philos. Soc. **59** (1963), 277–282.

2. H. Federer and B. Jónsson, *Some properties of free groups*, Trans. Amer. Math. Soc. **68** (1950), 1–27.

3. M. Greendlinger, *Dehn's algorithm for the word problem*, Comm. Pure Appl. Math. **13** (1960), 67–83.

4. R. C. Lyndon, *Cohomology theory of groups with a single defining relation*, Ann. of Math. (2) **52** (1950), 650–665.

5. ———, *Metamathematics and algebra: an example*, Proc. Internat. Congress of Logic, Methodology, and Philosophy of Science, pp. 143–150, Stanford Univ. Press, Stanford, Calif., 1962.

6. ———, *Dependence and independence in free groups*, Crelles J. **210** (1962), 148.

7. ———, *Length functions in groups*, Math. Scand. (to appear).

8. W. Magnus, *Über diskontinuerliche Gruppen mit einer definierenden Relation. (Der Freiheitssatz)*, Crelles J. **103** (1930), 141–165.

9. ———, *Das Identitätsproblem für Gruppen mit einer definierenden Relation*, Math. Ann. **106** (1932), 295–301.

10. H. Neumann, *Generalised free products with amalgamated subgroups*. II, Amer. J. Math. **71** (1949), 491–540.

11. J. Nielsen, *A basis for subgroups of free groups*, Math. Scand. **3** (1955), 31–43.

12. R. Peiffer, *Über Identitäten zwischen Relationen*, Math. Ann. **121** (1949), 67–99.

13. K. Reidemeister, *Über Identitäten von Relationen*, Abh. Math. Sem. Univ. Hamburg **16** (1949), nos. 3–4, 114–118.

BIRKBECK COLLEGE,
LONDON, ENGLAND
UNIVERSITY OF MICHIGAN,
ANN ARBOR, MICHIGAN