GROUPS OF ORDER 1
SOME PROPERTIES OF PRESENTATIONS

BY

ELVIRA STRASSER RAPAPORT

State University of New York at Stony Brook, Stony Brook, N.Y., U.S.A.[1]

Section 1

A presentation of deficiency zero (on n symbols and n defining relations) of a group G may define the trivial group, $G=1$.

The present work is a contribution to the decision problem: when does the presentation

$$P\colon (a_1, ..., a_n; r_1(a), ..., r_n(a))$$

of G give the trivial group?

It can be decided at once whether the r_i freely generate the free group $F_n = F(a)$ (see [12]). The question is how to reduce P to this case if $G=1$.

The next simplest case is that all but one of the r_i form a set of associated generators (one that can be completed to a free generating set of F_n) [8]. The simple fact that the consequence of such a set $(r_1, ..., r_{n-1})$ contains the commutator subgroup F' of F_n motivates the introduction of what I will call root-extraction. For example if $(a_1, a_2; a_1, r_2) = 1$ then there is a word s_2 such that a_1 and s_2 generate $F_2 = F(a)$ and $r_2 \equiv a_2$ modulo a_1 and $r_2 \equiv s_2$ modulo s_2. (See Sections 4 and 5.)

The introduction of Nielsen transformations (automorphisms of free groups) combined with conjugations—I will call these Q-transformations—hardly needs motivating in this context. Root-extraction on t-tuples $r = (r_1(a), ..., r_t(a))$ in $F_n = F(a)$ will consist of replacing a proper subset of r by another set without changing normal closure and deficiency of presentation.

For n-tuples r for which the presentation P above is that of the trivial group, the fol-

[1] The support of the National Science Foundation under GP-3204 and GP-6497 is gratefully acknowledged.

lowing facts will emerge. Q-transformations form the largest group of mappings that can transform two such n-tuples into each other. Modulo this group a single root-extraction R can be found that takes a given r into a given r^*. While certain of these pairs of n-tuples are Q-transforms of each other, $r^* = Q(r)$, it may happen that also $r^* \equiv R(r)$ modulo Q-transformations and R is not a Q-transformation. Examples will be given for which Q-equivalence seems to be an open question. Thus, it remains to be decided whether any two n-tuples rendering P a presentation of the trivial group are equal modulo Q. The remaining results of this paper, properties of presentations of $G = 1$ of deficiency zero, were found during my study of this problem.

The first five sections set up the machinery for the study and give some labor-saving devices.

Section 6 gives a set of generators of the mappings between any two presentations on n generators (and so on n defining relations) and gives two basic properties. These lead—naturally, as it were—to remarks on unsolvable problems in group theory (Section 7) and, via examples, to algorithmic posers (Section 11).

Sections 8 and 10 lead off with examples, to illustrate what had gone before and to motivate the next step.

Section 9 draws on the literature for devices to change or manufacture presentations for study.

All the examples are contained in Sections 8, 10, and 11.

Theorems comparing two presentations which share some defining relations are akin to a problem posed by Magnus: if the consequence in F_n of $(r_1, ..., r_n)$ is F_n, can r_1 be replaced by some free generator of F_n without loss of the property?

Numbers in brackets refer to the reference list.

I am indebted to Tekla Taylor for helpful critical remarks. Above all it is hoped that the work done here suggests methods of attacking this difficult problem.

Section 2

A presentation of a group G consists of two sets of elements written as $(a_1, ...; r_1, ...)$, of which the first is a set of symbols $a = (a_1, ...)$ that freely generate the free group $F = F(a)$, the second a set r of elements (words) in F, given in terms of the a-symbols. The presentation is finite if both sets are. G is the factor group F/r of F by the normal closure $\{r\}$ of r in F.

$F_n \quad = F(a)$ is the free group generated by the n-tuple $a = (a_1, ..., a_n)$.

$\bar{w} \quad =$ abbreviates w^{-1}.

w^z $= \bar{z}wz$; for example $\bar{w}^z = w^{-z}$, $w^{-z+\bar{x}} \neq w^{\bar{x}-z} \neq \bar{w}^{z+\bar{x}} = (\bar{w})^{z+\bar{x}} = w^{-z-\bar{x}}$, and $(w^x)^y = w^{xy}$. Here x, y, z are elements of F_n.

$|w|$ is the length of $w \subset F(a)$; that is, the number of a-symbols in w.

P is a polynomial in the "integral group ring" of F with neither operation commutative. Thus, $w^{-z+\bar{x}} = w^P$, with x, z, w in F, $P = -z + \bar{x} \neq \bar{x} - z$.

w is said here to be cyclically reduced if w is *both* freely reduced and cyclically reduced.

G' is the commutator subgroup of G.

A is an automorphism of F acting on the given generating symbols $(a_1, \ldots,)$; thus $Aw(a) = w(Aa_1, \ldots, Aa_k, \ldots)$.

The Aa_k are a-words $s_k = s_k(a)$, abbreviated to s_k where no misunderstanding arises from doing so.

Small Greek letters are units; thus

ε $= \pm 1$.

$\{r\}$ $= \{r_1, \ldots\}$ is the normal closure of the elements $r = (r_1, \ldots)$ in $F(a)$.

$N(t) = N$ is a Nielsen transformation acting on a t-tuple of elements (t fixed) regarded as symbols.

The generators of choice for the group of Nielsen transformations will be the set of mappings

$$N_{kh}(w_1, \ldots, w_t) = (w_1, \ldots, w_{k-1}, v, w_{k+1}, \ldots, w_t) \text{ with } \quad v = w_k w_h^{\varepsilon} \text{ or } \quad w_h^{\varepsilon} w_k; \quad k \neq h.$$

In $N_{ij}N_{kh}$, N_{ij} acts on the t-tuple $N_{kh}(w)$ (cf. [8], p. 125 ff.). While $N(t)$ is isomorphic to the automorphism group of F_t, the manner of action just defined will not be referred to as an automorphism but as a Nielsen transformation, even if $w(a)$ freely generates $F_t(a)$. My reason for defining A and N differently will appear later. A is so defined that direct length-reductions be possible for "reducible" words (words whose length can be reduced by some automorphism of the group) [12]. The distinction is indispensable (cf. Section 11). [$T_2 T_1(w) = v$ is a direct reduction if $T_1(w)$ has fewer a-symbols than w, and v fewer than $T_1(w)$.]

Section 3

For the purpose at hand a combinatorial definition of invertibility is needed. It is given below. Invertible transformations, $Q = Q(t)$, acting on a t-tuple in F_n, form a group, with Nielsen transformations a subgroup. A set of generators is found in Section 5. The other transformation I need, root-extraction, $R=R(t)$, is not going to be invertible, but A, N, $Q(n)$, $R(n)$ share the property of taking an n-tuple in F_n whose normal closure is F_n into another such.

Let r be a t-tuple of elements $r_i=r_i(a)$ in $F_n=F(a)$, x_1 some one of the r_i, x_2 some one of the r_i, possibly the same as x_1, and so on. Finally let $K_1=x_1^{P_1}x_2^{P_2} \dots x_m^{P_m}$, so that K_1 is consequence of r written in fixed fashion in terms of r-conjugates in F_n.

That is, K_1 designates not just that word in F_n which it represents but also the particular way here given of writing it as an r-consequence.

If $K_2, \dots, K_t$ are similarly defined, let K be the t-tuple $(K_1, \dots, K_t)$. Furthermore, let K^* be a t-tuple defined exactly like K except that the symbols x_i signify elements $K_{i'}$ of K rather than elements $r_{i'}$ of r.

Suppose that for a given t-tuple $K=(K_1, \dots, K_t)$ there is a t-tuple K^* of consequences of K in F_n such that upon cancelling segments $r^x\bar{r}^x$ formally, each K_i^* reduced to r_i. Then the mapping that takes r into K is *invertible*.

For integral exponents P this defines K as a Nielsen transform of r; if then the set r freely generates F_n, the mapping that takes r into K is an automorphism of F_n. Else K merely generates the same normal subgroup in F as r does.

Let $t=n$, and $\{r\}=F_n$. Then there are endless ways of writing the r_i as power-products of the a-symbols; r will be an invertible transform of the latter if at least one such is invertible. For example, the pair $r_1=\bar{a}^2\bar{b}ab$, $r_2=\bar{b}^2\bar{a}ba$ is not invertible consequence of the pair (a, b) in $F_2=F(a, b)$ under Nielsen transformations, or automorphisms of F_2; but there is a K, and a K^* that inverts it, such that $K(r(a, b))=(a, b)$ in F_2 (Example 3).

Section 4

Though it is not essential to take $t=n$, let $r=r(a)$ be an n-tuple in F_n, and $\{r\}=F_n$. Then there is at least one n-tuple of consequences, K', of the a-words r that freely reduces to $(a_1, \dots, a_n)$, so that $\bar{a}_iK_i'(r(a))=1$ for i: $1, \dots, n$.

Turning this process around, pick an n-tuple $E(a)$ of (unreduced) words in F_n such that each $E_i(a)$ reduces to the empty word. Form the (unreduced) words E_ia_i and mark out each into segments. Let $v_1', \dots$ be those segments, and $v_1, \dots$ the result of reducing them. If the v_i are conjugates or inverses of conjugates of just n distinct ones among them, say $r_1, \dots, r_n$, then $K_i(r)=a_i$ for certain consequences K_i of the set. If one calls $r=(r_1, \dots, r_n)$ a set of roots of $a=(a_1, \dots, a_n)$, though trivial, it is true that $\{r\}=F_n$ if and only if (the n-tuple) r is a set of roots of the n-tuple a. Similarly, if $\{r\}=F_n$ and $r_i\subseteq\{r_i'\}$, then $\{r'\}=F_n$. The following definition suggests itself:

If r is a t-tuple, $\{r_1, ..., r_k\} \subseteq \{r_1', ..., r_k'\}$, and either $k=t=1$ or $0<k<t$, then the set $r'=(r_1', ..., r_k', r_{k+1}, ..., r_t)$ is a *root* of r. In symbols: $r'=R(r)$. It will be convenient to assume that a conjugate, or inverse of a conjugate, is not a root of a word. With this restriction and for arbitrary t, R_t will be called a *root-extraction* in a t-tuple. If $t=n$, the subscript will be omitted.

Section 5

Let $r=(r_1, ..., r_t)$ be a set of fixed cyclically reduced words $r_i(a)$ in $F_n=F(a)$, x or $-x$, y or $-y$, ... reduced words ranging over F_n, $x=x(a)$, $y=y(a)$, $\varepsilon=\pm 1$. Let $r_1 r_2^{\bar{x}}=yv\bar{y}$, with $v=v(a)$ cyclically reduced. Then v and y may be chosen in more than one way; let $(r_1 r_2^{\bar{x}})^y = r_1^*$ stand for a fixed choice of y (and v) for given r_i and x. For example, $u\bar{z}w\bar{u}=(\bar{z}w)^{\bar{u}}= u\bar{z}\cdot w\bar{z}\cdot z\bar{u}=(w\bar{z})^{z\bar{u}}$ and so y may be chosen as u or as $u\bar{z}$ depending on which cyclically reduced conjugate of $\bar{z}w$ is to be r_1^*: $w\bar{z}$ or $\bar{z}w$.

The proof of Theorem 1 hinges on the formalism embodied in this definition. For example, $r_2 r_1 = r_1(\bar{r}_1 r_2 r_1)$ in a group, but $r_1(\bar{r}_1 r_2 r_1)$ will not be taken as $r_1 r_2^{\bar{x}}$ even if $x=x(a)$ *is* $r_1(a)$. The point and the reason for it should become clear from the context in which, later on, n new symbols will be introduced as new generators to replace $a_1, ..., a_n$ in the exponents (and *only* there).

If x or $-x$ is an element of F_n, and the same holds for y, let $Q_{12}(r_1)=(r_1 r_2^{\bar{x}})^y$, and $Q_{12}(r_i)=r_i$ for $i>1$. Let Q_{ij} be similarly defined for each pair (i, j) with $i \neq j$ and given t-tuple $r=(r_1, ..., r_t)$ in $F_n=F(a)$. If $t=1$, write $Q(r)=r^y$. These mappings will be multiplied as follows.

If $Q_{ij}(r)=r^*$, then

$$Q_{hk}Q_{ij}(r)=Q_{hk}(r^*)=(r_1^*, \dots\ r_{h-1}^*, [r_h^*(r_k^*)^{x*}]^{y*}, r_{h+1}^*, \dots, r_t^*).$$

For fixed t-tuple r and F_n, the set of these mappings as the exponents vary generates a group, $Q=Q(t)$. Q will also mean any element of the group when the meaning is clear from the context.

It may be noted that images under Q are taken cyclically reduced, so that conjugation alone, to be effected by Q, is limited to cyclically reduced images. This is done to avoid clutter and trivia. Merely dropping the requirement that $Q_{ij}(r_i)$ be a cyclically reduced word allows one to generate any conjugation. Thus one gets $ba\bar{b}$ by letting $a \to a\bar{b}$ be followed by $(a\bar{b}) \to [(a\bar{b})b]^{\bar{b}}$. All conjugations yielding cyclically reduced words can be effected in this way by the Q_{ij}.

THEOREM 1. *$Q(t)$ is the set of all invertible transformations of the t-tuple $r=r(a)$ in $F_n=F(a)$ into t-tuples of cyclically reduced words.*

8*† – 682903 *Acta mathematica*. 121. Imprimé le 18 septembre 1968.

Proof. Let Q be an element of $Q(t)$. To prove Q invertible it suffices to find $\overline{Q}$ for $Q=Q_{12}$ when $t=2$. Let $Q(r)=p$ with $Q(r_1)=(r_1 r_2^x)^y$, $Q(r_2)=r_2$; then $Q^*(p_1)=(p_1\bar{p}_2^{xy})^{\bar{y}}$, $Q^*(p_2)=p_2$ gives

$$Q^*Q(r_1)=[(r_1 r_2^x)^y\bar{r}_2^{xy}]^{\bar{y}}=r_1 r_2^x \bar{r}_2^x=r_1,$$

$$Q^*Q(r_2)=r_2$$

identically in the r-conjugates: that is, regardless of the expression of the r_i as a-words. Thus $Q^*=\overline{Q}$.

Note that in this necessarily formal definition of "identical", r^w is not identically r for $w=r$; rather, $r^w\bar{r}=r^{w-1}$ and this is 1 only for $w=1$.

To prove the converse, let r and p be t-tuples in $F_n=F(a)$, with p invertible consequence of r.

To show that $p=Q(r)$, I will introduce a set $b=(b_1, ..., b_n)$ of new symbols and convert the $(n+t)$-tuple $(p_1, ..., p_t, b_1, ..., b_n)$ into a Nielsen transform $N(r, b)$ of the $(n+t)$-tuple $(r_1, ..., r_t, b_1, ..., b_n)$ in $F_{n+t}=F(r_1, ..., r_t, b_1, ..., b_n)$. This N will become a Q-transformation on the t-tuple $r(a)$ when the b-symbols are eliminated.

Since p is invertible consequence of r, the following holds.

(1). $p_1=r_{i_1}(a)^{x_1(a)}r_{i_2}(a)^{x_2(a)}\ldots r_{i_k}(a)^{x_k(a)}$ with similar expressions for $p_2, \ldots, p_t$;

(2). $r_1=p_{j_1}^{y_1(a)}\,p_{j_2}^{y_2(a)}\ldots p_{j_h}^{y_h(a)}$,with similar expressions for $r_2, \ldots r_t$;

(3). If (1) is substituted in (2) then r-conjugates cancel in pairs to yield identities $r_i=r_i$ for each i.

Now replace in (1) the exponents $x(a)$ by the corresponding words $x(b)$ and replace each a-word $r_i(a)$ by the symbol r_i, i: $1, \ldots, t$. Call the resulting words (1′) $q_1, \ldots, q_t$. Replace the a-words $y(a)$ in (2) by the b-words $y(b)$ and call the result (2′) $s_1, \ldots, s_t$. Thus, in $F_{n+t}=F(r_1, \ldots, r_t, b_1, \ldots, b_n)$,

(1′). $q_1=q_1(r, b)=r_{i_1}^{x_1(b)}r_{i_2}^{x_2(b)}\ldots r_{i_k}^{x_k(b)}=\varepsilon\bar{x}_1(b)r_{i_1}^{\varepsilon}\,\varepsilon x_1(b)\ldots,$

(2′). $r_1=s_1(q, b)=q_{j_1}^{y_1(b)}\ldots,$ etc.

Because x may be $-w$ for an element w of the group, so that $-x\subset F$ but $x\not\subset F$, the three ε-symbols take on the value -1 if this is the case, and $+1$ otherwise.

If follows from the definition of invertibility that $(q_1, ..., q_t, b_1, ..., b_n)$ freely generate $(r_1, ..., r_t, b_1, ..., b_n)$, i.e. the free group $F_{n+t}=F(r, b)$.

Finally set $q_{t+1}=b_1, \ldots, q_{t+n}=b_n$, $q=(q_1, \ldots, q_{t+n})$ and $s_{t+1}=b_1, \ldots, s_{t+n}=b_n$, $s=(s_1, \ldots, s_{t+n})$. Then both $(n+t)$-tuples generate F_{n+t} and if the right sides in (1′) are substituted in (2′) for the q_i, $i:1, \ldots, t$, the result freely reduces to identities. Therefore, $q=\bar{N}(r, b)$, $s=N(r, b)$ for some N of F_{n+t}.

I will show that N can be expressed as a product $N_m^* \ldots N_1^*$ of Nielsen transformations N_j^* each of which leaves the b-symbols fixed and for the rest turns into a product of some $Q_{hk}(r)$ when the $x(b)$ are replaced by the $x(a)$, the $y(b)$ by the $y(a)$, and the r_i by the $r_i(a)$. Then the same will be true of $\bar{N}$ so that $q=Q(r)$ will result.

If $w=(w_1, w_2)$, denote $|w_1|+|w_2|$ by $|w|$.

It is well known (see e.g., [2]) that if $|N(w)| \leqslant |w|$ for a finite set of elements $w=w(z)$ in $F(z)$, then N can be written as a product of generators N_{ij} none of which increases z-length. Since in terms of (r, b)-length $|r|+|b| \leqslant |q|$ and $N(q)=(r, b)$, N has such a representation: $N=N_c \ldots N_1$. This will now be changed into the $N_m^* \ldots N_1^*$ described above.

N_1 leaves all but a single q_i fixed, and $i \leqslant t$ since otherwise N_1 would increase (r, b)-length. Suppose $N_1(q_1) \neq q_1$. Then N_1 multiplies q_1 by q_j^ε on the left, or else on the right. It may be assumed that $N_1(q_1)=q_1 q_j$. Similarly, each N_j multiplies some (r, b)-word by another or by some b-symbol (or its inverse). I will express N as a product

$$N=N_h' \ldots N_1'$$

of generators N_{ij} such that if N_i' multiplies a word by some b_k^ε, say $N_i'(w_1)=b_1 w_1$, then $N_{i+1}' N_i'(w_1)=b_1 w_1 \bar{b}_1$ or $w_1=\tilde{w}_1 \bar{b}=N_{i-1}'(\tilde{w}_1)$. Setting $N^*=N_{i+1}' N_i'$ in the first case and $N^*=N_i' N_{i-1}'$ in the second, and assigning a suitable subscript to N^* will then result in the desired expression.

It remains then to show that $N=N_h' \ldots N_1'$ exists. If N_j, acting on the $(n+t)$-tuple w, changes $w_{j'}$, it may be assumed that $N_j(w_{j'})=w_{j'} w_{j''}$. Then $j' \leqslant t$, as $w_{t+1}=b_1, \ldots, w_{t+n}=b_n$ for each N_j.

For transformations of the type $N=N_c \ldots N_1$ under consideration here, let k be the number of factors N_j for which $j'' \leqslant t$. If $k=0$ then the effect of N is the removal of the b-symbols from $(q_1, \ldots, q_t)$. Since $N(q_i)=r_i$ contains no b-symbol for $i \leqslant t$ and the q_i are conjugates of the r_i, it is easy to see that in this case $N=N_h' \ldots N_1'=N_c \ldots N_1$ with each N_i' an N_j. (See the remark before Theorem 1.)

Suppose now that the value of k is $k_0>0$. The proof will be completed by reducing the case to one with $k=k_0-1$.

Let j be the least subscript in $N=N_c \ldots N_1$ for which $N_j(w_{j'})=w_{j'} w_{j''}$ has $j'' \leqslant t$. If $j=1$ there is nothing to prove since N_1 is a Q-transformation and so only $N_c \ldots N_2$, with $k=k_0-1$, remains.

If $j>1$, I will express N in a form $N_c \dots N_{j+1}N^{**}N_jN^*N_{j-1}\dots N_1$ with the following property: $N_jN^*N_{j-1}\dots N_1$ can be rewritten as a product $N' = N'_h \dots N'_1$, while for $N_c \dots N_{j+1}N^{**}$ the value of k is $k_0 - 1$.

Let $N_{j-1}\dots N_1(q) = w$, so that $N(q) = N_c \dots N_j(w)$. Let $N_j(w_1) = w_1w_2$, and suppose that w arose from q by the removal of some b-symbols from $(q_1, \dots, q_t)$. It is no loss of generality to assume further that only q_1 and q_2 were changed by $N_{j-1}\dots N_1$, since any other action of this transformation can be postponed until after N_j is applied (without affecting the value of k). It follows that

$$q_1 = u_1(b)w_1v_1(b), \quad q_2 = u_2(b)w_2v_2(b).$$

Let

$$N^*(w_1) = v_1(b)u_1(b)w_1, \qquad N^*(w_2) = w_2v_2(b)u_2(b), \qquad N^*(w_m) = w_m \quad \text{for} \quad m>2.$$

Setting $v_i(b) = u_i(b) = 1$ for $i>2$, and $(v_1q_1\bar{v}_1, v_2q_2\bar{v}_2, \dots) = v(b)q\bar{v}(b)$ gives

$$N^*(w) = N^*N_{j-1}\dots N_1(q) = v(b)q\bar{v}(b).$$

Thus $N^*(w)$ is a Q-transform of q. Therefore $N^*N_{j-1}\dots N_1$ can be rewritten as required.

If now N_j acts on $N^*(w)$ one gets

$$N_jN^*(w_1) = v_1(b)u_1(b)w_1w_2v_2(b)u_2(b),$$

$$N_jN^*(w_2) = w_2v_2(b)u_2(b),$$

$$N_jN^*(w_m) = w_m \quad \text{for} \quad m>2.$$

If N^{**} is the transformation that removes the $u_i(b)$ and $v_i(b)$ displayed here then $N^{**}N_jN^*(w) = N_j(w) = N_jN_{j-1}\dots N_1(q)$. Therefore

$$N(q) = N_c \dots N_{j+1}N^{**}N_jN^*N_{j-1}\dots N_1(q)$$

and, as N_j is also a Q-transformation, only $N_c \dots N_{j+1}N^{**}$ remains to be considered. By its definition, N^{**} contributes nothing to the value of k for $N_c \dots N_{j+1}N^{**}$, so that value is $k_0 - 1$.

This concludes the proof of Theorem 1.

THEOREM 2. *Two t-tuples, r and r^* of $F_n = F(a)$, are Q-transforms of each other, $Q(r) = r^*$ for some $Q \subset Q(t)$ if and only if for every automorphism A of F_n: $Ar^* = Q^*(Ar)$ for some Q^* depending on A.*

Proof. Let $r_1^* = Q(r_1) = r_{i_1}^{x_1} r_{i_2}^{x_2} \ldots, A(x_i) = y_i,$ for A any automorphism of $F(a)$ and $x_i = x_i(a), y_i = y_i(a)$. Then $Ar_1^* = (Ar_{i_1})^{y_1}(Ar_{i_2})^{y_2} \ldots$ and I will show that Ar_1^* is Q-transform of Ar_1 under a mapping Q^* that takes $(Ar_2, \ldots, Ar_t)$ into $A(r_2^*, \ldots, r_t^*)$. Let $p(r^*)$ be a t-tuple in $\{r^*\}$, and let $Q(r) = r^*$. To show that $Ar \to Ar^*$ is a Q-transformation, let $p(r^*)$ reduce to r when r^* is replaced by the r-consequences given for it above; then $r^* \to p(r^*)$ inverts Q: $r \to r^*$ and

$$p_1(r^*) = (r_{j_1}^*)^{z_1}(r_{j_2}^*)^{z_2} \ldots,$$

with similar expressions for $p_2, \ldots, p_t$. Let

$$\tilde{p}_1(r^*) = (r_{j_1}^*)^{Az_1}(r_{j_2}^*)^{Az_2} \ldots,$$

so that $Ap_1(r^*) = \tilde{p}_1(Ar^*)$, etc. for $\tilde{p}_2, \ldots, \tilde{p}_t$. Then $Ar^* \to \tilde{p}(Ar^*)$ is a map that inverts $Ar \to Ar^*$. By virtue of Theorem 1, the latter is then a Q-transformation.

To show the converse, let A be an automorphism of F_n and suppose the two t-tuples Ar and Ar^* connected by a Q-transformation, Q^*: $Ar \to Ar^*$. To prove that, for some Q, $r^* = Q(r)$, one need only apply the argument given above to $Ar^* = Q^*(Ar)$, using the automorphism $\bar{A}$:

$$\bar{A}(Ar^*) = \bar{A}[Q^*(Ar)], \quad \text{with}$$

$$\bar{A}(Ar^*) = r^*, \quad \text{and}$$

$$\bar{A}[Q^*(Ar)] = Q^{**}(\bar{A}Ar);$$

therefore $r^* = Q^{**}(r)$, as claimed. (See in this connection Example 7, Section 11 below.) This proves Theorem 2.

Remark. It does not follow that, for given A, $A(r) = Q(r)$ for some Q. For example, if $H = \{r\}$ and $AH \not\subset H$ then $\{A(r)\} \neq \{r\} = \{Q(r)\}$. (Cf. Example 1, Section 8.) However, when $G = 1 = (a; r)$ and the presentation has deficiency zero, the following holds.

THEOREM 3. *If r is an n-tuple in $F_n = F(a)$ and $Q(r) = a$, then, for every A of F_n, $A(r) = Q^*(r)$ for some Q^*.*

Proof. $r = \bar{Q}(a)$ and $A(a) = s$ give $A(r) = A\bar{Q}(a) = \bar{Q}(A(a)) = \bar{Q}(s)$. I will show that $s = Q'(a)$ and this will give $A(r) = \bar{Q}Q'(a) = \bar{Q}Q'Q(r)$.

It is clear from the definition of Q-transformation at the beginning of this section that when all exponents x, y that occur in the product $Q' = Q_{i_2 j_2} Q_{i_1 j_1}$ are integers, then

9 – 682903. *Acta mathematica.* 121. Imprimé le 18 septembre 1968.

$Q'(a)$ is a Nielsen transform $N(a)$ of a; and vice versa. Since the n-tuple s generates F_n, $s = N(a)$ and so $s = Q'(a)$, for some Q-transformation Q'.

The following lemmas will shorten proofs in the sequel.

Lemma 1. *Let A be any automorphism of $F_n = F(a)$, $A(a) = s$, R a root-extraction, r a t-tuple in F_n, $R^*[w(a)] = R[w(s)]$, and Q^* the map defined in the proof of Theorem 2. Then* $RQ(r) = \bar{A}R^*Q^*A(r)$.

The proof is the same as for Theorem 2.

Lemma 2. *If r is an n-tuple in $F_n = F(a)$ then $\{r\} = F_n$ implies that $r_i = s_iC_i$, for C_i in F', and a set $(s_1, \ldots, s_n)$ of free generators of F_n.*

Proof. r generates F/F' and so the matrix (n_{ij}), with n_{ij} the exponent sum of a_j in r_i, has determinant ± 1. Hence [8] for some C_i' in F', $(r_1C_1', \ldots, r_nC_n')$ freely generate F_n. Setting $r_iC_i' = s_i$ and $C_i = \bar{C}_i'$ gives $r_i = s_iC_i$ as claimed.

Lemma 3. *If $(s_1, \ldots, s_n)$ freely generate $F_n = F(a)$ then $(s_1C, s_2, \ldots, s_n) = Q(a)$ for any C in F'.*

For F' is in the consequence of $(s_2, \ldots, s_n)$.

Section 6

Let r^* be an n-tuple and $F_n = F(a) = \{r^*\}$ with $r_i^* = a_iC_i$, C_i in F_n'. Let $C_{k+1}, \ldots, C_n \subset \{a_1, \ldots, a_k\}$ with k minimal in the sense that no $n-k+1$ of the C_i vanish modulo that subset of the a_j not associated with them in r^*. If $r^* = a$, set $k = 0$.

Replace $r_1^*, \ldots, r_k^*$ by $a_1, \ldots, a_k$ to get

$$R_a(r^*) = r^{**} = (a_1, \ldots, a_k, r_{k+1}^*, \ldots, r_n^*).$$

Then $\{r^{**}\} = F(a)$. Note that R_a need not be a root-extraction even if $k < n$, as for example when $r_1^*, \ldots, r_k^* \not\subset \{a_1, \ldots, a_k\}$.

Theorem 4. *Let r be an n-tuple and $F_n = F(a) = \{r\}$. Let C_i designate an element of the commutator subgroup F' of F_n. Then there exists three Q-transformations Q_1, Q_2, Q_3 and a root-extraction R such that $Q_1(r) = (a_1C_1, \ldots, a_nC_n) = r^*$, $RQ_2Q_1(r) = R_a(r^*)$ with $k < n$ in the definition of R_a, and $Q_3R_a(r^*) = a$.*

Proof. By Lemma 2, there is a set of free generators $s = (s_1, \ldots, s_n)$ of F_n for which $r_i = s_iC_i'$, and the C_i' are in F'. As in the preceding proof, $s = \bar{N}(a)$ for some Nielsen transformation N, and the formal application of N to r is a Q-transformation, Q_1. Thus $Q_1(r_i) =$

$N(s_iC_i')=N(s_i)N(C_i')=a_iC_i=r_i^*$, for each i. Since F' is contained in the consequence of $a_1, \ldots, a_{n-1}$, at most $n-1$ of the C_i need be dropped from r^* to get a set of the form $R_a(r^*)$ whose normal closure is again $F(a)$. Thus $R_a(r^*)$ exists with $k<n$. This allows the following procedure which effects R_a by a root-extraction R acting on a Q-transform $Q_2Q_1(r)$ of $Q_1(r)$. Having chosen k as small as possible and having so renumbered the $r_i^*=s_iC_i$ that $C_{k+1}, \ldots, C_n \subset \{a_1, \ldots, a_k\}$, multiplication of $r_1^*(a)$ by suitable conjugates of $\bar{a}_{k+1}\bar{C}_{k+1}$, will replace all a_{k+1} symbols in $r_1^*(a)$ by $\bar{C}_{k+1}$. It is not hard to see that such steps are Q-transformations and that $r_1(a)$ can, by steps of this sort, be cleared of all a_{k+1} and $\bar{a}_{k+1}$. Similarly for $k+2, \ldots, n$ and $r_2^*(a), \ldots, r_k^*(a)$. Let Q_2, acting on $Q_1(r)=r^*$ accomplish all this. Then the mapping $Q_2(r^*)\to(a_1, \ldots, a_k, r_{k+1}^*, \ldots, r_n^*)=R_a(r^*)$ is a root-extraction R on $Q_2(r^*)=Q_2Q_1(r)$ and so $R_a(r^*)=RQ_2Q_1(r)$.

Finally, the resulting n-tuple $RQ_2Q_1(r)$ is reduced to the n-tuple a by sending $r_{k+1}^*, \ldots, r_n^*$ into $a_{k+1}, \ldots, a_n$. Since $r_{k+1}^*=a_{k+1}C_{k+1}$ and C_{k+1} vanishes modulo $a_1, \ldots, a_k$, the mapping that sends $R_a(r^*)$ into itself except that $r_{k+1}^*\to a_{k+1}$ is a Q-transformation. Similarly for $r_{k+2}^*\to a_{k+2}, \ldots, r_n^*\to a_n$.

The main point here is that if $\{r_1, \ldots, r_n\}=F(a)$ then modulo Q-transformations a single root-extraction takes r into a: $Q'RQ(r)=a$. It will be seen in the examples that at the same time r may be a Q-transform $Q^*(r)$ of a even though $Q'RQ$ is not a Q-transformation. Next, Theorem 5 takes, similarly, a into r and Theorem 6 gives a substitute for the non-existent inverse of R.

THEOREM 5. *If $F_n=F(a)=\{r\}$ for the n-tuple r, then either $r=Q(a)$ or $r=Q_2RQ_1(a)$: r is Q-transform of a modulo at most one root-extraction.*

Proof. Again, the r_i can be changed to the form a_iC_i, $C_i\subset F'$ by a Q-transformation, so assume $aC=(a_1C_1, \ldots, a_nC_n)=r$. Let $C_{k+1}, \ldots, C_n\subset\{a_1, \ldots, a_k\}$, so that $F(a)=\{a_1, \ldots, a_k, r_{k+1}, \ldots, r_n\}$. Apply any Q-transformation to aC that reduces k as much as possible but retains this form of r; call the result r^*. Since $\{r_1^*, \ldots, r_k^*\}\equiv F(a)$ modulo the remaining r_j^*, there exist words $v_1, \ldots, v_k\subset\{r_1^*, \ldots, r_k^*\}$ and words $w_1, \ldots, w_k\subset\{r_{k+1}^*, \ldots, r_n^*\}$ such that $v_iw_i=a_i$, i: $1, \ldots, k$. Set

$$r''=(v_1w_1, \ldots, v_kw_k, r_{k+1}^*, \ldots, r_n^*)$$

and

$$r'=(v_1, \ldots, v_k, r_{k+1}^*, \ldots, r_n^*).$$

Then $r''=Q'(r')$, and since $r_{k+1}^*=a_{k+1}C_{k+1}^*$, with $C_{k+1}^*\equiv 1 \bmod (a_1, \ldots, a_k)=(v_1w_1, \ldots, v_kw_k)$, one gets $r''=Q'(r')=Q''(a)$. This in turn gives $r'=\overline{Q}'Q''(a)$. Together with $r^*=R(r')$, then $r=\overline{Q}^*R(r')=\overline{Q}^*RQ(a)$.

Remark. Here $v_1, \dots, v_k$ may be replaced by $a_1, \dots, a_k$ in r' and that would be a mapping R_a with $\{R_a(r')\} = F(a)$, but R_a can be done as a Q-transformation in the present case.

In preparation for the examples, these results will now be spelled out for F_2 (cf. [14]) in two corollaries. They are followed by two easy consequences of Theorem 3 for F_n in general.

COROLLARY 5.1. *In $F_2 = F(a, b)$, for any C in F', $\{aC, b\} = F(a, b)$ and any pair r such that $\{r\} = F(a, b)$ is Q-transform of a pair $RQ(aC)$, $Q(b)$.*

COROLLARY 5.2. *If $K_1 \subset \{s_1 C_1\}$, $K_2 \subset \{s_2 C_2\}$ in $F(a) = F_2 = F(s_1, s_2)$, and $K_1 K_2 = s_1$, then $(K_1, s_2 C_2) = Q(a)$.*

Proof. As (s_1, s_2) is a free generating set for $F(a)$, the normal closure of either s_i contains the commutator subgroup F' of $F(a)$ and so the following are Q-transformations:

$$(K_1, s_2 C_2) \rightarrow (K_1 K_2, s_2 C_2) = (s_1, s_2 C_2),$$

$$(s_1, s_2 C_2) \rightarrow (s_1, s_2).$$

By definition, $(s_1, s_2) = A(a_1, a_2)$ and so by Theorem 3, $(s_1, s_2) \rightarrow (a_1, a_2)$ is a Q-transformation.

COROLLARY 5.3. *If the set $s = (s_1, \dots, s_n)$ freely generates $F_n = F(a)$ and if C is in the commutator subgroup F' of $F(a)$ then any root of $s_1 C$ has a completion to an n-tuple $RQ(a)$. In particular, any root of $s_1 C$ has the form $s_1^* C^*$.*

COROLLARY 5.4. *If $\{r\} = F_n = F(a)$, the subset $(r_1, \dots, r_k)$ of the n-tuple r may be replaced by the subset $(s_1, \dots, s_k)$ of a free generating set s of $F(a)$ without diminishing the normal closure if and only if $\{r_{k+1}, \dots, r_n\}$ contains $s_{k+1}, \dots, s_n$ modulo $(s_1, \dots, s_k)$. If $k = n-1$ the condition is always satisfied.*

Proof. Let $s_1 C \subset \{r_1^*\}$ so that r_1^* is root of $s_1 C$. Then $(r_1^*, s_2, \dots, s_n) = R(s_1 C, s_2, \dots, s_n)$ and since C is in the consequence of $(s_2, \dots, s_n)$, the set $(s_1 C, s_2, \dots s_n)$ is Q-transform $\tilde{Q}(s)$ of $(s_1, \dots, s_n)$. As $s = A(a)$, by Theorem 3, $\tilde{Q}(s) = \tilde{Q}(A(a)) = Q(a)$. Now it follows that $\{r_1^*, s_2, \dots, s_n\} = F(a)$, whence, with Lemma 2, one gets $r_1^* = s_1^* C_1^*$.

Section 7

The question whether the n-tuple r is always Q-transform of the n-tuple a when $F(a) = \{r\}$ depends then on the nature of root-extractions: can every R be effected by a

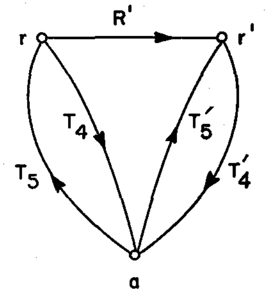
Q-transformation? (This in turn depends on the nature of the identities the $r_i(a)$ satisfy.) It was remarked already that some can; thus in Example 3 below $r_i \subset \{a_i\}$ for each i and $r = Q(a)$. To my knowledge Examples 1 and 4, in F_3 and F_2 respectively, leave the question open. One may well recall here that there is a growing list of undecidable group-theoretic problems [11].

Suppose that it is undecidable whether all root extractions can be written as Q-transformations. Then it is useless to study examples: if faced with root-extractions R not negotiable by a Q-transformation, the fact cannot be proven, while if all are so negotiable examples are pointless.

This came to the fore when I had to scrap what looked like a proof that the set (R, Q) is larger than the set (Q) (The abstract announcing it was withdrawn before presentation to the American Mathematical Society but unfortunately not before printing [15].)

THEOREM 6. *If R' is a root-extraction on the n-tuple r in $F_n = F(a) = \{r\}$ and $R'(r) = r'$, then modulo Q-transformations at most two further root-extractions take r' back to r.*

Proof. Let $T_4(r) = a$ in Theorem 4, so that T_4 is an $R \bmod Q$. Let $T_5\,(a) = r$ in Theorem 5, so that T_5' is an $R \bmod Q$. The choice of T depends on r. Then the diagram below contains Theorems 4 and 5. An arrow is reversible there only if the mapping involved can be effected by some Q.



If $r' = Q(r)$, $\bar{Q}$ takes r' back to r; otherwise $T_5 T_4'$ does, with each T containing at most one root-extraction: if $r' = Q(a)$ then T_4', if $r = Q(a)$ then T_5 is the identity transformation modulo Q. Accordingly, the effect of R' is undone by at most two successive root-extractions separated by Q-transformations.

So it is possible to reverse the effect of a root-extraction by further such steps, but the latter do not constitute an inversion in the combinatorial sense (as given above in the definition of invertibility).

This is just what Theorem 1 says. On the other hand, it can happen that $r' = Q(r)$, while also $r' = R(r)$. In this case $\bar{Q}$ inverts Q and not R, since inversion is a formal procedure by definition.

If not every R can be effected by some Q, then the set of all n-tuples r with consequence $F_n = F(a)$ in $F(a)$ falls into several subsets, $S_1, \ldots$ such that each subset is closed under the group $Q(n)$, each is connected to the one containing $a = (a_1, \ldots. a_n)$ by a single R, and each pair of subsets is connected by at most two R's.

Section 8

In the proof of Theorem 1, the expression under (1) gives the a-word p_1 as a consequence of the n-tuple r of a-words. It is chosen so as to make statement (3) there correct for each p_i in $p = (p_1, \ldots, p_n)$. By going over to the expression (1′) the machinery to deal with Nielsen transformations (in F_{2n} though) is made available [12, 8]. This will be utilized to study n-tuples r whose consequence is all of F_n.

In the expression (2) replace p_i by a_i for each i and drop the requirement (3) for it. That is, for a given n-tuple of a-words r, consider any expression of r as a-consequence. It will represent a Q-transformation if a matching n-tuple of expressions of the type (1) exists making statement (3) true. A necessary condition is that the corresponding expressions (2′) reduce to the n-tuple a under an automorphism of F_{2n}. The condition is not generally sufficient since only certain automorphisms of F_{2n} correspond to Q-transformations of F_n.

For example, in F_2, on the pair of (single) symbols a and b, let $r = (a^2b\bar{a}\bar{b}, b)$ be written as $(ab^{\bar{a}}b^{-1}, b)$. Then $Q_{12}(r) = (ab^{\bar{a}}, b)$, $Q'_{12}Q_{12}(r) = (a, b)$ for the obvious choice of Q_{ij}. In this sense the expression $(ab^{\bar{a}}b^{-1}, b)$ of r in terms of (a, b)-conjugates represents r as Q-transform of (a, b):

$$r = Q(a, b) \quad \text{for} \quad Q = [Q'_{12}Q_{12}]^{-1}.$$

Now if $r = (a^2b\bar{a}\bar{b}, b^2a\bar{b}\bar{a})$ is written as $(ab^{\bar{a}}b^{-1}, ba^{\bar{b}}a^{-1})$, then no such Q exists even though this r is Q-transform of the pair (a, b). The latter fact is shown in Example 3 below, the former is seen as follows. Replace the a-symbols in the exponents by c, and the b-symbols by d, to get $(ab^{\bar{c}}b^{-1}, ba^{\bar{d}}a^{-1})$. Write this as the pair of elements $(acb\bar{c}\bar{b}, bda\bar{d}\bar{a})$ in $F_4 = F(a, b, c, d)$. It can be shown [12, 8] that this pair is not reducible in terms of (a, b, c, d)-length by automorphisms of F_4.

The foregoing is geared to certain generators Q_{ij} of the group $Q(n)$. For example, each Q_{ij} in the Q given above reduces the number of conjugates of a and b in the pair of words it acts on. (Of course this statement is meaningful only when the words are given as products of specific conjugates of a and b.) Thus Q effects here a "direct" reduction of the length in question. In special cases an element of $Q(n)$ can be so written on the generators Q_{ij} defined in Section 5 that it reduces a-length directly (that is, $Q=Q_k \dots Q_1$, each Q_h some Q_{ij} and each shortens $Q_{h-1} \dots Q_1(r)$). In other cases another set of generators Q'_{ij} may do this and the Q'_{ij} needed can actually be found. For each of these cases an example will be given along with another for which the method fails. (See also [14].)

Example 1: $G=(a, b, c; \bar{b}^2\bar{c}bc, \bar{c}^2\bar{a}ca, \bar{a}^2\bar{b}ab)=(a, b, c; r_1, r_2, r_3)$. Conjugation and sending the generators into their inverses take r into the triple known [10] (see also [13]) to give a presentation of the trivial group and so $G=1$.

It remains undecided whether $r=Q(a, b, c)$; the problem will now be reduced to a presentation of the trivial group on two generators.

Let

$$A_1(a, b, c) = (a, cb, c), \quad \mathrm{A}_2(a, b, c) = (a, b, cb\bar{a}^2\bar{b}a),$$

$$Q_1(T, W, Z) = (T, W^{\bar{c}}, Z^{\bar{b}}), \quad Q_2(T, W, Z) = (T, W, ZW),$$

and let Q_3 remove every c-symbol from the (a, b, c)-words T, W: $Q_3(T(a, b, c), W(a, b, c), c) = (T(a, b, 1), W(a, b, 1), c)$.

Then $Q_2Q_1A_1(r)=((\bar{b}\bar{c})^2bc, \bar{c}\bar{a}ca\bar{c}, b\bar{a}^2\bar{b}a\bar{c})$, and if one sets $T(a, b, 1)=U(a, b)$, $W(a, b, 1)=V(a, b)$, then $Q_3A_2Q_1A_1(r)=(U(a, b), V(a, b), c)$. The words U and V will be explicitly needed only in Example 4 below, so these two long words are not given here.

The A_i are automorphisms of $F_3=F(a, b, c)$ and the Q_i are clearly Q-transformations. It can be shown that the product $\bar{A}_1\bar{A}_2Q_3A_2Q_2Q_1A_1$ is a Q-transformation, but the product that is of interest here is $Q_3A_2Q_2Q_1A_1$. It differs from the former by an automorphism of F_3. The situation is as follows. Since Theorem 3 is applicable only when $r=Q(a, b, c)$, and I have been unable to decide whether or not it is in the present example, it is clear only that $Q_3A_2Q_2Q_1A_1$ takes r into a triple that gives a presentation of the trivial group and that $(a, b; U(a, b), V(a, b))=1$.

It may be noted that while $r=Q(a, b, c)$ would follow from $(U, V)=\tilde{Q}(a, b)$, whether the converse is true remains an open question.

Computation shows further that the, subgroup H generated by $r_1, r_2^{\bar{c}}$, and $r_3^{\bar{b}c}$ contains the element $\bar{c}b\bar{a}^2\bar{b}ca\bar{c}=r_3^{\bar{b}c}r_2^{\bar{c}}$ which is a free generator of $F(a, b, c)$. While this word generates $F(a, b, c)$ with a and $\bar{c}b$, it generates H with r_1 and $r_2^{\bar{c}}$.

What follows is a general statement for which this is an example and a few related facts.

THEOREM 7. *If the t-tuple w in F_n generates a subgroup, H, containing a free generator s_1 of F_n, then there is a Q-transform of w that contains s_1 and generates H.*

Proof. Let $A(s_1) = a_1$ and $A(w) = v$. Then v generates $H^* = AH$, a_1 is in H^*, and [2] there is a Nielsen transformation N such that $N(v)$ contains a_1. Of course $N(v)$ generates H^*, and $N(w) = N[\bar{A}(v)] = \bar{A}N(v)$. Hence $N(w)$ contains $\bar{A}(a_1) = s_1$ and generates H. N is a Q-transformation, so that the proof is complete.

COROLLARY 7. *If $t = n$ and $\{w\} = F(a)$, then s_1 of Theorem 7 is contained in w modulo Q.*

THEOREM 8. *If, for arbitrary n, $w = (w_1, ..., w_n)$ and $F_n = F(a) = \{w\}$ imply that the subgroup H generated by w contains a free generator of $F(a)$, then $a = Q(w)$.*

Proof. Let $s = s(a) = \bar{A}(a)$ and $s_1 = \bar{A}(a_1)$ the free generator contained in H. Then Theorem 7 applies. Form the $Q(w)$ of Corollary 7 that contains s_1 and set $Q(w_1) = s_1$. Rewrite the remaining $Q(w_i)$ in terms of the generators $s(a)$ of $F(a)$ and drop all the $s_1(a)$ occurring in them. This results in a Q-transform $Q_1(w)$ consisting of s_1 and $Q_1(w_2, ..., w_n)$. The $(n-1)$-tuple $Q_1(w_2, ..., w_n)$ is written on the $(n-1)$-tuple $s_2(a), ..., s_n(a)$ and its normal closure in the free group $F_{n-1} = F(s_2(a), ..., s_n(a))$ is $F(s_2(a), ..., s_n(a))$. Since $F(a)$ is the free product of this F_{n-1} with the free cyclic group generated by $s_1(a)$, the element $s_1(a)$ completes any full set of free generators of this F_{n-1} to a full set of free generators of $F(a)$. Thus, if the theorem holds for $n-1$, it holds for n. Since the case $n = 1$ is trivial (for then $w = a^{\varepsilon}$), the proof if complete.

THEOREM 9. *Let $r = (r_1, ..., r_t)$, $r^* = (r_1^*, r_2, ..., r_{.})$ in F_n. Then r and r^* are consequences of each other if and only if either 1) $r^* = RQ(r)$ and $r = R^*Q^*(r^*)$ with Q and Q^* products of Q_{ij} which leave $r_2, ..., r_t$ fixed or 2) $r^* = Q(r)$.*

Proof. Let $K(X)$ mean a consequence of X in F_n. The sufficiency of either condition is clear. To prove their necessity, let $\{r\} = \{r^*\}$. Then $r_1^* = K_1(r_1)K(r_2, ..., r_t)$ and $r_1 = K_1^*(r_1^*)K^*(r_2, ..., r_t)$. If now $r^* \neq Q(r)$, then r^* may be constructed from r (or vice versa) as follows: the mapping that takes r_1 into $K_1^*(r_1^*)$ and leaves $r_2, ..., r_t$ fixed is the product Q of certain Q_{1j} with $j \geqslant 2$, each of which leaves $r_2, ..., r_t$ fixed. In the resulting t-tuple $Q(r) = (K_1^*(r_1^*), r_2, ..., r_t)$, $Q(r_1) \subset \{r_1^*\}$ so $r_1^* = RQ(r_1)$ and $RQ(r) = r^*$ with $R(r_j) = r_j$ for $j > 1$.

It may be noted that when $r^* = Q(r)$, then Q may not possess the property stated under 1).

Remark. Both 1) and 2) may be true, as in Example 2 below. Whether some Q can be effected by root-extractions when $\{r\} \neq F(a) = F_n$ seems to be an open question.

Also this: under what conditions is $\{R(r)\} = \{r\} \neq F(a)$ possible. $F_n/R(r) \simeq F_n/r = G$ may be another matter, as indeed it is when $\{r\}$ is proper subgroup of $\{R(r)\}$ (and G is non-Hopfian).

The following is easily verified.

THEOREM 10. *Let $r = (r_1, \ldots, r_n)$, $r^* = (s_1, r_2, \ldots, r_n)$, and $s_1^{\varepsilon} \neq r_1^{x}$ for any x in $F_n = F(a) = \{r\}$. If $s = (s_1, \ldots, s_n)$ freely generates $F(a)$ then each of the following four conditions is necessary and sufficient for $\{r^*\} = F(a)$.*

1. *r_1 and s_1 are roots of one another modulo $r_2, \ldots, r_n$.*
2. *The consequence modulo s_1 of $r_2, \ldots, r_n$ contains $s_2, \ldots, s_n$.*
3. *If $r_1 \neq s_1^{x}$ modulo $r_2, \ldots, r_n$ for any εx in $F(a)$ then it can be replaced by some consequence $K(s_1) \neq s_1^{x}$ of s_1 without altering $\{r\}$.*
4. *r_1 is consequence of $r_2, \ldots, r_n$ modulo s_1.*

Example 2. If $r_1 = a_1 C_1$, $r_2 = a_2 C_2$ and $\{r_1, r_2\} = F(a_1, a_2) = F_2$, then a_1 is a root of $a_1 C_1$, and $(a_1, a_2 C_2) = Q(a_1, a_2)$ (Lemma 3). For $n = 2$ Theorem 10 says just this. A narrower generalization of this observation is the following direct consequence of Lemma 3.

THEOREM 11. *If $\{r_1, \ldots, r_n\} = F_n = F(a)$ then any $n-1$ of the r_i may be replaced by a suitable subset of some free generators $s_1, \ldots, s_n$ of $F(a)$.*

Example 3. If $X = a^2 b \bar{a} \bar{b}$, $Y = b^2 a \bar{b} \bar{a}$, then $b = R(Y)$, and $Q^*(X, b) = (a, b)$. Thus, $R(X) = X$, $Q^* R(X, Y) = (a, b)$. While this does not prove that $\{X, Y\} = F(a, b)$, finding a Q' to replace R would. Such a Q' can be constructed from the Q_i given below. For $Q = Q_3 Q_2 Q_1$, $Q(X, Y) = (a, b)$, and since $Q_4(a, b) = R(X, Y)$, one gets $Q_4 Q(X, Y) = R(X, Y)$. Thus $Q' = Q_4 Q_3 Q_2 Q_1$. The Q_i are as follows:

$$Q_1(V, W) = (V W^{b}, W),$$

$$Q_2(V, W) = (V, W V^{1-\bar{b}}),$$

$$Q_3(V, W) = (V \overline{W}, W),$$

$$Q_4(V, W) = (V W^{\bar{a}-1}, W).$$

In this example $Q_4 Q(X)$ reduces to X in terms of the symbols (a, b) but not in terms of the (X, Y)-conjugates that define it. In contrast, an automorphism A that leaves the symbol a fixed, changing only b, can be carried out (as a product of generating automorphisms) so the symbol a never changes. For in this case the set $A(a, b) = (s_1, s_2)$ has the form $(a, a^k b^{\varepsilon} a^h)$ [2, 12].

Example 4. Let $X=\bar{a}^2\bar{b}ab$ serve as an abbreviation to write U and V of Example 1. Then $U=\bar{b}\bar{X}^{bX}$, $V=X^{1-2\bar{a}^2}$, and $R(U, V)=(U, X)=Q(a, b)$. This Q has the effect of stripping U of $\bar{X}^{bX}$ and then reducing $X=\bar{a}\cdot b^{-a+1}$ to $\bar{a}$. Can the work of the root-extraction R be done in an invertible manner? My many attempts to decide this, only some fortuitous, revealed nothing. For example Marshall Hall's commutator calculus [5] stumbles over identities, while an algorithm involving length-arguments stumbles over the necessity to distinguish between relative and absolute minima [12]: if $|r|$ is the sum of the lengths $|r_i|$ (the number of a-sumbols in r_i cyclically reduced), then the shortest $Q(r)$ for all Q may be shorter than minima relative to direct reductions, whether under the generators Q_{ij} or some others. This is true even if one allows $|Q_{ij}(r)|\leqslant|r|$ instead of strict inequality. That $|U|+|V|$ is minimal with respect to the Q_{ij} follows by inspection from the next theorem. It is readily (if a little messily) established that this pair is minimal under automorphisms of $F(a, b)$. That all this is not decisive will be seen from further examples.

To simplify some statements, I will call conjugates w^x of w in $F(a)$ *short conjugates* if $|w^x|=|w|$. Thus $w=abc$ has the short conjugates abc, bca, cab and their inverses. *The cyclic word w* will mean some one of these, chosen in advance.

In the definition $Q_{12}(r_1)=(r_1r_2^{\bar{x}})^y$ the word εy was chosen to make the image-word cyclically reduced once it is reduced. Thus $(r_1r_2^{\bar{x}})^z$ would be at least as long for any element z (or $-z$) of F_n.

In $(r_1r_2^{\bar{x}})^y=r_1^yr_2^{\bar{x}y}$ the factors, r_1^y and $r_2^{\bar{x}y}$, need not reduce to short conjugates. If r_1^u, r_2^v do, $r_1^ur_2^v$ need not reduce to a short conjugate. To avoid the verbal complications this would cause the theorem below does not mention Q-transformations. A rough but simple way of putting it is: reductions by Q-transformations can be effected by using only short conjugates.

THEOREM 12. *In $F(a)$, let A,B be cyclically reduced words and neither the empty word; let A^y, B^z and all words appearing in exponents be reduced, and A^u, B^v, A^yB^z cyclically reduced when reduced. If $|A^yB^z|\leqslant|A|$ then there is an A^u and a B^v such that $|A^uB^v|\leqslant|A^yB^z|$ and $(A^uB^v)^w=A^yB^z$.*

Proof. Suppose first that B^z is a short conjugate. Assume $B^z=B$ (this will be corrected for). So $|A^yB|\leqslant|A|$. A^y can be taken reduced as written, for if it is not then A can be replaced by a short conjugate A^w and y replaced by $\bar{w}y$ (this too will be corrected for).

If $y=\pm1$ there is nothing to prove. Otherwise some segment of B, and some of y, certainly cancels in A^yB: $y=Uw$, $B=\bar{w}C$. Then $A^yB=\bar{w}\bar{U}AUw\cdot\bar{w}C$, $A^U=A^{y\bar{w}}$, $|A^{y\bar{w}}|<|A^y|$, $|B^{\bar{w}}|=|B|$, and $A^{y\bar{w}}B^{\bar{w}}=(A^yB)^{\bar{w}}$. This process reduces the length of y, until a short conjugate, A^u, of A and a short conjugate, B^v, of B give a conjugate $A^u B^v$ of $A^y B^z$. Clearly $|A^u B^v| \leqslant |A^y B^z|$. To effect the promised corrections one need only replace A respectively B by a suitable short conjugate.

It remains to reduce B^z to a short conjugate. Again take B^z reduced as written. Since $|A^y B^z| \leqslant |A|$, at least half of B^z, and so of B, must cancel; hence all of $\bar{z}$ does: $A^y B^z = Uz \cdot \bar{z} B z$. Then $A^{y\bar{z}} B = (A^y B^z)^{\bar{z}}$, $|A^{y\bar{z}}| \leqslant |A^y|$, and B is cyclically reduced. The necessary correction now consists of replacing B in $A^{y\bar{z}} B$ with a short conjugate B^v. This concludes the proof.

Let $Q = \prod_k^1 Q_i$, with the Q_i chosen from a fixed set of generators of the group of Q-transformations of n-tuples in $F_n = F(a)$, and $X = \prod_{i-1}^1 Q_j(r) = X(a)$. If $|Q_i(X)| \leqslant |X|$ for each i: 1, ..., k, then Q is said to be semidirect on these generators (cf. [2] and [12]). That semidirect reductions take the presentation $(a_1, ..., a_n; r_1, ..., r_n)$ of the trivial group into the trivial presentation $(a_1, ..., a_n; s_1, ..., s_n)$ only in some cases will be seen in Section 10.

Section 9

The machinery gotten so far generates all presentations of zero deficiency of $G = 1$ for fixed n. In the process of applying it, new, often interesting, presentations arise. This can be most helpful with the work on the decision problem: when is a presentation that of $G = 1$.

Two further methods of generating presentations of deficiency zero of $G = 1$ follow. They are essentially Tietze-transformations (see for example [8]) and do not keep n fixed. One is a construction from $(a; r)$ when $r = Q(a)$. It is a by-product of a result on Q-transformations (Theorem 13). The other uses the method of Magnus [6] and is tied to my next example.

Let r and $Q(r)$ be two n-tuples in $F_n = F(a)$. Let $F_{2n} = F(b_1, ..., b_n, c_1, ..., c_n)$. Fix the manner in which the $Q(r_i)$ are written as products of r-conjugates (in case this is not unique) by setting $Q(r_1) = K_1(r) = r_j^{x_{1j}} r_k^{x_{1k}} ...$, and so on for each r_i, using fixed short conjugates of each r_i throughout (Section 8), and reduced a-words in the exponents.

Next replace the exponents $x(a)$ by the exponents $x(b)$, and the words $r_i(a)$ by the symbols c_i. This turns the $K_j(r)$ into (b, c)-words $K'_j(b, c) = K'_j$. On setting $Q(b_i) = b_i$ for each i, Q turns into an element Q' of $Q(2n)$: $Q'(b, c) = (b, K')$. Clearly, $Q'(b, c)$ generates $F(b, c)$ freely so Q' is an automorphism of F_{2n}. The inverse, written as a combination of the $2n$ symbols $b_1, ..., K'_1, ...$ freely reduces to (b, c) when $K'_j(b, c)$ is substituted for each symbol K'_j. Combinatorially then one may put $\bar{Q}'(b, c) = \bar{A}(b, c) = (b_1, ..., b_n, w_1(b, c), \ldots, w_n(b, c)) = (b, w(b, c))$. They are associated free generators of $F(b, c)$.

Suppose now that $Q(r)=a$. Then the n words $K_j'(b, c)$ reduce to the n symbols a_i when the c-symbols are replaced by the words $r(a)$ and b-symbols by a-symbols, subscripts matching. It follows that the n-tuple $w(b, a)$ (gotten from $w(b, c)$ by writing a_i in place of c_i for each i) generates $F(a, b)$ with the n-tuple b: $F(a, b)$ is a free product

$$F(a, b) = F_n(w(b, a)) * F_n(b),$$

while the $w_i(a, a)$ freely reduce to the $r_i(a)$. To get $w(a, a)$ from $w(b, a)$ the substitution $b=a$ was made. This amounts to setting $b\bar{a}$ equal to 1. Let A^* be the automorphism that takes b_i into $b_i a_i$ for each i, and let $A^*(a_1, ..., a_n, b_1, ..., b_n)=(a_1, ..., a_n, b_1 a_1, ..., b_n a_n)=(a, ba)$, $A^*(w(b, a))=v(b, a)$. To get the n-tuple $w(a, a)$ from the n-tuple $v(b, a)$, one must set $A^*(b\bar{a})=b$ equal to 1, since $v(b, a)=w(ba, a)$. Thus, $v(1, a)=r(a)$ identically in $F(a)$. This gives (cf. [13])

THEOREM 13. *If* $Q(r)=a$ *then by using dummy symbols* $b_1, ..., b_n$, *the n-tuple* $r(a)$ *can be written as an n-tuple* $v(b, a)$ *such that the 2n-tuple* $(v(b, a), ba)$ *freely generates the 2n-tuple* (a, b), *and* $v(1, a)=r(a)$ *identically.*

The converse is of course not true: if $b_1, ..., b_n$ are dummy symbols and the $r_i(a)$ can be written as words $s_i(a, b)$ that freely generate $F(a, b)$ with $b_1 a_1, ..., b_n a_n$, it does not follow that $Q(r)=a$; not even if $s(a, 1)=a$. For this to happen the n-tuple $s(a, b)$ must be a special kind. But when $Q(r)=a$, the n-tuple $r=r(a)$ may now be said to arise from a free generating set in F_{2n} by dropping half the symbols in half of the set.

This may be compared with the following situation. Let G be any group having a presentation on $n+1$ generators and n defining relations

$$P'\colon (g, a_1, ..., a_n; r_1', ..., r_n')$$

for which $G/g=1$. Knot groups are the most studied among these. (See [4] for example.) Thus, droppping all g-symbols in P' gives

$$P\colon (a_1, ..., a_n; r_1, ..., r_n)=1.$$

Conversely, the insertion of powers of a new symbol in any way into the r_i in P gives some presentation P'.

But knot groups are small comfort here: the topologist manufactures his presentations from knots [3] or braids [1] and then the resulting P has the form $(a; s)$ for a set of free generators $s=s(a)$ of F_n. Every known presentation of knot groups seems to be derived from these. So the shoe may be on the other foot: one must first decide how to make P into a presentation of a knot group [3].

Replacing the r_i of Example 1 (Section 8) by $\bar{a}^{2\bar{g}}\bar{b}a^g b$, $\bar{b}^2\bar{c}bc$, $\bar{c}^{2g}\bar{a}ca$ gives a presentation of type P'. (This is no knot group as its Alexander polynomial is $2g^3 - g^2 - 4g + 2$. [4]).

Section 10

Example 5. This starts out with a variant [9] of Example 1:

$$r_1 = ba\bar{b}\bar{a}^2, \quad r_2 = cb\bar{c}\bar{b}^2, \quad r_3 = ac\bar{a}\bar{c}^2.$$

Let
$$Q = Q_3 Q_2 Q_1, \quad A(a, b, c) = (ac, b, c),$$

$$Q_1(U, V, W) = (UV^{aca}, V, W),$$

$$Q_2(U, V, W) = (U, U^{\bar{a}} V U^{-b^2\bar{a}}, W),$$

$$Q_3(U, V, W) = (U, V, UWU^{-c\bar{a}-\bar{a}}).$$

Use $w = \bar{b}^2\bar{a}ba$ as an abbreviatton to write $Q(Ar) = (c, w^{2-\bar{b}^2}, aw^P)$, $P = \bar{a}\bar{b} - \bar{b}^2 - \bar{b}^2\bar{a}$. Set

$$u(a, b) = w^{2-\bar{b}^2} = Q(Ar_2),$$

$$v(a, b) = aw^P = Q(Ar_3).$$

Then $u(a, b) = \bar{b}C_1$, $v(a, b) = abC_2$, with C_i in F', and $|u| = 15$, $|v| = 16$. Of course,

$$P^*: \ (a, b; u, v) = 1.$$

The pair (u, v) is minimal with respect to automorphisms of $F(a, b)$ and the Q_{ij}.

Let $\bar{b}^k a b^k = a_k$, k: 0, $\pm 1, \dots$. When rewritten in terms of these symbols and powers of b, the Q-transform $(u^{\bar{b}}, u^{\bar{b}}v^{\bar{a}})$ of (u, v) becomes

$$U_0 = u^{\bar{b}} = \bar{b}\bar{a}_0 a_{-1} \bar{a}_1 a_0 \bar{a}_{-2} a_{-1},$$

$$V_0 = u^{\bar{b}} v^{\bar{a}} = a_0 a_{-1} \bar{a}_1 \bar{a}_{-1} a_0^2 \bar{a}_{-2} \bar{a}_0 a_{-1} \bar{a}_1 a_0 \bar{a}_{-2} a_{-1}.$$

Set $U_0 = f(a_{-2}, a_{-1}, a_0, a_1, b)$ and define U_k to be $f(a_{k-2}, a_{k-1}, a_k, a_{k+1}, b)$ for every integer k. Similarly for V_0, and any other word $W_0 = g(a_i, a_{i+1}, \dots, a_j, b)$. This gives a presentation

$$P': \ (b, a_k; U_k, V_k, \bar{a}_k b a_{k+1} \bar{b}, \ k: 0, \pm 1, \dots) = 1.$$

Let $W_0 = \bar{a}_0 a_{-1} \bar{a}_1 a_0 \bar{a}_{-2} a_{-1}$ so that $W_0 = bU_0$. Then the relation $U_0 = 1$ can be written as $b = W_0$ and the relation $U_k = 1$ as $b = W_k$. It follows that the U_k may be replaced by the $W_k \overline{W}_{k+1}$, for every k, in P' and the symbol b by any W_k. Choosing W_0 to replace b changes P' to

$$P'' : (a_k;\ V_k, \bar{a}_k W_0 a_{k+1} \overline{W}_0, W_k \overline{W}_{k+1}, \quad k: 0, \pm 1, \ldots) = 1.$$

Since V_0 and W_0 contain only a_{-2}, a_{-1}, a_0, a_1,

$$H_0 = (a_{-2}, a_{-1}, a_0, a_1;\ V_0, \bar{a}_i W_0 a_{i+1} \overline{W}_0, \quad i: -2, -1, 0)$$

is a group. If there are no further relations between these symbols in the presentation P'' then $H_0 = 1$ (and conversely). By introducing the symbol b and the relation $b = W_0$ and replacing W_0 with b in the $\bar{a}_i W_0 a_{i+1} \overline{W}_0, H_0$ gets the new presentation

$$P^{**} : (b, a_{-2}, a_{-1}, a_0, a_1;\ V_0, U_0, \bar{a}_i b a_{i+1} \bar{b}, \quad i: -2, -1, 0).$$

Eliminating a_{-2}, a_{-1}, and a_1 in the obvious way reduces P^{**} to $(a_0, b; u(a_0, b), v(a_0, b))$, which is just P^*. Thus P^{**} and H_0 are presentations of the trivial group.

Note that in P^{**} the last four words are free generators in $F_5 = F(a_{-2}, a_{-1}, a_0, a_1, b)$, though not associated. In particular U_0 is a way of writing the word $u(a, b)$ of P^* as a free generator on five symbols.

Section 11

Concerning a-length of words, absolute minima and minima obtained by random semi-direct reductions relative to given generators of the group $Q(n)$, may not coincide. If they do then $r = Q(a)$ only if any semi-direct reduction of r yields a, and so one has an algorithm to decide whether $r = Q(a)$ or not. Naturally, the generating set of Q-transformations must be a reasonable set, in the sense that if $|Q'(r)| \leqslant |r|$ for some member Q' of the set (for the r in question), one can actually find Q'. The following examples show that the two minima in question do not coincide for any reasonable choice of generators (cf. [11]).

Example 6. Let $u = \bar{b}^2 \bar{c} b c$, $v = \bar{c}^4 b c^3 \bar{b}$. To simplify the notation allow $Q_{12}(u)$ to take the form $u^y v^{xy}$ as well as $v^{xy} u^y$. The transformation Q given below reduces $|u| + |v| = (5+9)$ to $(1+8)$. Let $Q_1(u) = u$, $Q_1(v) = u^{P_2} v u^{P_1} = V$, $P_1 = -\bar{b} - \bar{b}cb - \bar{b}cbcb$, $P_2 = -2\bar{b}^2 c - \bar{b}^2 c^2$. Let $Q_2(u) = V u^{\bar{b}^2} V^{\bar{b}^2} = U$, $Q_2(V) = V$. Then Q_1 is the product of Q_{21}-transformations, Q_2 that of Q_{12}-transformations, and $Q = Q_2 Q_1$ takes (u, v) into $(\bar{b}, \bar{c} b^7)$. As $|Q_1(u, v)| = (5+8)$, Q_1 is a reduction on (u, v) and Q_2 a reduction on $Q_1(u, v)$; but the Q_{ij} that make them up produce fluctuations of length which cannot be avoided; that is, the transformation is not semi-direct.

Q_1 and Q_2 above are instances of a transformation of the type

$$Q(X, Y) = ([X^z Y^P]^w, Y).$$

If z is an arbitrary monomial, P an arbitrary polynomial in the group ring of F_2, X and Y elements of F_2, then these transformations include all Q_{ij}. Thus they generate but are not a reasonable choice of generators in terms of which length-reductions might be made semi-direct. For there is no way of saying what z and P will reduce the length of a given X. For example we do not know whether X has a conjugate X^z equivalent modulo Y to some given word W; if we did, we could check through all the W that are shorter than X. As Theorem 12 does not apply here, the arbitrariness of z is already a stumbling block.

Example 7. This will show that for an n-tuple which is minimal with respect to the Q_{ij} but not minimal Q, Theorem 2 may provide an algorithm for finding the Q-minimum.

Let $u = b^2 c\bar{b}\bar{c}$, $v = c\bar{b}^7$. Then if $Q = Q_3 Q_2 Q_1$, then $Q(u, v) = (b, c)$ for

$$Q_1(X, Y) = (X^{b^2} Y^{b^2 - b}, Y),$$

$$Q_2(X, Y) = (X^c Y^{-c}, Y),$$

$$Q_3(X, Y) = (X, YX^7).$$

Let $A(b, c) = (b, cb)$, so that $\bar{A}(b, c) = (b, c\bar{b})$. As $Q_1(u, v) = (c\bar{b}^6, c\bar{b}^7)$, Q_1 is not direct; in fact there is no direct reduction here on the generators Q_{ij}. How was Q found then? First one notes that $A^7(u, v)$ is direct for each application of A, and that $Q_1 A^7(u, v) = (b, c)$ is direct. Then Q is found by converting this into a Q-transformation as follows. $Q_1 A^7(u, v) = (b, c)$ implies $Q_1(u, v) = \bar{A}^7(b, c)$; this is used to find $Q_1(u, v)$. Then A^7 is converted into a Nielsen transformation and is applied to $Q_1(u, v)$. Nielsen transformations are Q-transformations and this one turns out to be $Q_3 Q_2$. The reason for the appearance of Q_2 is that an automorphism, such as A, changes both words of a pair while a Nielsen transformation N_{ij} changes only one.

References

[1]. Artin, E., Theorie der Zöpfe. *Abh. Sem. Hamburg Univ.*, 4 (1926), 47–72.

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

[3]. Fox, R. H., Some problems in knot theory. *Topology of 3-manifolds. Proc. of the 1961 Topological Institute*, p. 168, Problem 2. Prentice Hall, 1962.

[4]. —— A quick trip through knot theory. *Ibid.*, pp. 120–167.

[5]. Hall, M., Jr., *The theory of groups*, 434 pp. Macmillan, 1959.

[6]. Magnus, W., Über diskontinuierliche Gruppen mit einer definierenden Relation (Der Freiheitssatz). *J. reine angew. Math.*, 163 (1930), 141–165.

[7]. —— Über n-dimensionale Gittertransformationen. *Acta Math.*, 64 (1934), 353–367.

[8]. Magnus, W., Karrass, A. & Solitar, D., *Combinatorial group theory*, 444 pp. Interscience Publ., 1966.

[9]. Mennicke, J., Einige endliche Gruppen mit drei Erzeugenden und drei Relationen. *Arch. Math.*, 10 (1959), 409–418.

[10]. Neumann, B. H., On some finite groups with trivial multiplicator. *Publ. Math. Debrecen*, 4 (1956), 190–194.

[11]. Rabin, M. O., Recursive unsolvability of group theoretic problems. *Ann. of Math.*, 67 (1958), 172–194. [MR 22, No. 1611.]

[12]. Rapaport, E. S., On free groups and their automorphisms. *Acta Math.*, 99 (1958), 139–163.

[13]. —— Groups of order 1. *Proc. Amer. Math. Soc.*, 15 (1964), 828–833.

[14]. —— Remarks on groups of order 1. *Amer. Math. Monthly*, 75 (1968).

[15]. —— Groups of order 1. Part II. *Notices Amer. Math. Soc.*, 12 (1965), 329.

Received October 23, 1967