BOL. SOC. BRAS. MAT., VOL. 11 Nº 1 (1980), 79-102

Equations in groups

*Roger C. Lyndon**

1. Introduction.

This essay was prompted by the desire to supplement a very interesting paper by J. Mycielski (38) on the same subject. We do not attempt a systematic and exhaustive survey, but only to present a variety of interesting results, mainly without proofs, and of unsolved problems. Many of these problems are implicit in the exposition and will not be formulated explicitly. We have tried to provide an extensive bibliography, for anyone who wants to learn more about these matters. However, except for certain papers of central importance, we have not repeated references to be found in the book of Lyndon and Schupp (29), and we refer the reader to the text, the index, and the bibliography of that book for further references.

We bein with some miscellaneous examples, to give the flavor of the subject. First, a property that distinguishes groups among semigroups is the fact that, in a group G, given elements a and b, the equation

$$ax = b \qquad (1.1)$$

always has a unique solution.

By way of contrast, given an element a in a group G, the equation

$$x^2 = a \qquad (1.2)$$

may have no solution in G, or may have arbitrarily many solutions in G. It was observed by B. H. Neumann (39) that (1.2) always has a solution x in some group H containing G (and, indeed, with x not in G itself).

Consider a more complicated equation, say

$$ax^2bxc = 1. \qquad (1.3)$$

Here the sum of the exponents on x is 3, and, from the fact that this sum is not 0, a deep theorem of Gerstenhaber and Rothaus (18) tells us that, for most familiar groups G, and arbitrary a, b, c in G, a solution exists in

---

* This work was supported in part by the National Science Foundation, and partly by CNPq and FINEP while the author was visiting at the Universidade de Brasília.

Recebido em agosto de 1979.

Equations in groups

*Roger C. Lyndon**

1. Introduction.

This essay was prompted by the desire to supplement a very interesting paper by J. Mycielski (38) on the same subject. We do not attempt a systematic and exhaustive survey, but only to present a variety of interesting results, mainly without proofs, and of unsolved problems. Many of these problems are implicit in the exposition and will not be formulated explicitly. We have tried to provide an extensive bibliography, for anyone who wants to learn more about these matters. However, except for certain papers of central importance, we have not repeated references to be found in the book of Lyndon and Schupp (29), and we refer the reader to the text, the index, and the bibliography of that book for further references.

We bein with some miscellaneous examples, to give the flavor of the subject. First, a property that distinguishes groups among semigroups is the fact that, in a group G, given elements a and b, the equation

(1.1) $$ax = b$$

always has a unique solution.

By way of contrast, given an element a in a group G, the equation

(1.2) $$x^2 = a$$

may have no solution in G, or may have arbitrarily many solutions in G. It was observed by B. H. Neumann (39) that (1.2) always has a solution x in some group H containing G (and, indeed, with x not in G itself).

Consider a more complicated equation, say

(1.3) $$ax^2bxc = 1.$$

Here the sum of the exponents on x is 3, and, from the fact that this sum is not 0, a deep theorem of Gerstenhaber and Rothaus (18) tells us that, for most familiar groups G, and arbitrary a, b, c in G, a solution exists in

* This work was supported in part by the National Science Foundation, and partly by CNPq and FINEP while the author was visiting at the Universidade de Brasília.
Recebido em agosto de 1979.

some group H containing G. (The class of groups to which this theorem applies contains all finite groups, all free groups, but not, for example, the group $G = \langle a, b : ab^2 = b^3a \rangle$.)

For an equation such as

$$ax^2bx^{-1}cx^{-1} = 1, \tag{1.4}$$

with exponent sum 0, no known general method is applicable. Indeed, the simple equation

$$ax^{-1}bx = 1 \tag{1.5}$$

clearly has no solution in any group H containing G unless the elements a and b of G have the same order.

For a in G, a solution in G of the equation

$$a = x_1^2x_2^2x_3^2 \tag{1.6}$$

is a representation of a as the product of the squares of three elements of G. Very few elements of a free group have such a representaion, while, as far as in known, every element of a finite simple group has such a representation.

For arbitrary G, one may ask for all solutions of the equation 'without coefficients',

$$x_1x_2 = x_2x_1. \tag{1.7}$$

In a free group, and also in the linear fractional group $SL(2, R)$ all solutions are of the form $x_1 = z^m$, $x_2 = z^n$ for some z in G. Similarly, in a free group, the Vaught equation

$$x_1^2x_2^2 = x_3^2 \tag{1.8}$$

implies that x_1, x_2, x_3 are all powers of some z in G.

One also consider systems of equations in several unknowns, with or without constants, and one may ask for solutions in G, or in some extension H of G. One may ask if there exists any solution, and, if so, for a description of the set of all solutions.

2. Roots.

Consider the equation

$$x^n = a \tag{2.1}$$

for given a in a group G and a given integer $n \geq 1$: since arbitrarily many solutions exist in groups H containing G, we ask about solutions x in G.

If G is abelian, it is usually easy to decide if there exists some solution. If x_0 is any solution, then all other solutions are the form $x = x_0y$ where y is a solution of the 'homogeneous equation'

$$y^n = 1. \tag{2.2}$$

In short, if the set of solutions is not empty, it is a coset of the group of all solutions of (2.2).

If G is any finite group, a theorem of Frobenius yields information about the number of solutions. It is easy to see that the problem reduces to the case that n divides the order of G. Moreover, since any solution x of (2.1) commutes with a, we may replace G by the centralizer of a, that is, we may assume that a is the center of G. Now Frobenius's theorem states that, for a in the center of G and n dividing the order of G, the number of solutions is divisible by n. A famous unsettled conjecture of Frobenius is that if G is a finite group, if n divides the order of G, and if the equation $x^n = 1$ has exactly n solutions in G, then these solutions form a subgroup of G. (For a survey of this problem, with extensive references, see Finkelstein and Mandelberg (16).)

Next, let $G = SL(2, R)$ with elements $a : z \to \dfrac{\alpha z + \beta}{\gamma z + \delta}$, α, β, γ, δ in R, $\alpha\delta - \beta\gamma = 1$. Let $\tau = \alpha + \delta$, the trace of a. From the geometry of the action of G on the upper half of the complex plane one knows the following: (1) If $a = 1$, then G contains infinitely many (conjugate) elliptic elements x such that $x^n = 1$. (2) If $|\tau| < 2$, hence if a is elliptic, the centralizer C of a is the circle group, and, in this group, (2.1) has exactly n solutions. (3) If $|\tau| \geq 2$, but $a \neq 1$, whence a is parabolic or hyperbolic, then C is isomorphic to the additive group of reals, and (2.1) has exactly one solution.

Finally, suppose that G is a free group with a basis $B = \{b_1, b_2, \ldots\}$. Write a as a reduced word in the generators b_i. If $a = h^{-1}a_1h$, then the solutions of (2.1) are exactly the $h^{-1}x_1h$ for the solutions x_1 of the equation $x_1{}^n = a_1$. Thus we may replace a by a conjugate, and suppose that the reduced word for a is cyclically reduced:

$$a = b_{i_1}^{e_1} \ldots b_{i_t}^{e_t}, \quad e_k = \pm 1, \quad \text{with} \quad b_{i_k}^{e_k} b_{i_{k+1}}^{e_{k+1}} \neq 1 \quad \text{for all } k,$$

modulo t. Now a solution (necessarily unique) of (2.1) exists, of the form $x = b_{i_1}^{e_1} \ldots b_{i_k}^{e_k}$, where $nk = t$, if and only if a has period k, that is, $a = xx \ldots x$ (n factors x) *without cancellation.* We emphasize that this gives a simple algorithm for deciding if (2.1) has a solution, and, if so, for finding the solution.

3. Adjunction of solutions.

As we have noted for the case $n = 2$, B. H. Neumann showed that the equation

(3.1) $$x^n = a,$$

for a in G and $n \geq 1$, always has a solution in a group H containing G. In an obvious sence, the general solution is contained in the group

$$\tilde{H} = \langle G, x : x^n = a \rangle.$$

However, by a later result of Neumann (40), if G is finite a solution can always be found in a finite group H containing G.

We have noted also that the equation

(3.2) $$x^{-1}ax = b$$

can have a solution in a group H containing G only in case the elements a and b of G have the same order. G. Higman, B. H. Neumann, and H. Neumann (19) showed that, in this case, a solution always exists. Indeed, they showed more generally that a system (finite or infinite) of equations

(3.3) $$x^{-1}a_i x = b_i$$

has a solution in a group H containing G if and only if the map $\phi : a_i \to b_i$ defines an isomorphism from the subgroup A of G generated by the a_i to the subgroup B generated by the b_i. The 'general solution' lies in the group

$$H = \langle G, x : x^{-1}a_i x = b_i \rangle,$$

an HNN-*extension* of G. (HNN-extension has arisen independently in topogy and in logic, and is one of the basic constructions of combinatorial group theory.)

A result of Gerstenhaber and Rothaus (18) was alluded to earlier. Let

(3.4) $$w(x, a_1, \ldots, x_n) = 1$$

be an equation involving the unknown x and elements $a_1, \ldots, a_n$ of a group G, and suppose the sum of the exponents of x in w is $e \neq 0$. Then a solution exists in some H containing G provided that

(3.5) *G is embeddable in a compact Lie group:*

(The proof, by continuity, is topological.) Rothaus (48) replaced (3.5) by a purely combinatorial condition:

(3.6) *G is locally residually finite.*

(This means that if $g \neq 1$ lies in a finitely generated subgroup G_0 of G, then there exists a homomorphism ϕ from G_0 onto a finite group $G_0\phi$ such that $g\phi \neq 1$.)

Most familiar groups have this property. However, it fails for the group of G. Higman:

$$G = \langle a, b, c, d : a^b = c,\ b^c = d,\ c^d = a,\ d^a = b \rangle,$$

which has no non-trivial finite quotient groups. A simpler example (pointed out to me by *R*. Hunter) is the group

$$G = \langle a, b : a^{-1}b^2a = b^3 \rangle.$$

In a finite quotient group G_1 of G, the image b_1 of b will have some finite order n. Since b_1^2 and b_1^3 must have the same order, $(n, 6) = 1$, and hance $b_1 = b_1^{2k}$ for some k. Now $a_1^{-1}b_1a = b_1^{3k}$ has order n, hence generates $\langle b_1 \rangle$. It follows that $b_1^{a_1} = a_1^{-1}b_1a_1$ commutes with b_1, that is, the commutador $[b_1^{a_1}, b_1] = 1$. But, by Britton's Lemma, the element $[b^a, b]$ of the HNN-extension G is not trivial.

For G a free group we to not need the theorem of Gerstenhaber and Rothaus; the existence of a solution of (3.4) follows without any special hypothesis (except that, always, we assume that w contains x essentially — that is, w is not conjugate to any word that does not contain x). This follows from the Freiheitssatz of Magnus (see 33; 29). Let G have a basis $B = \{b_1, b_2, \ldots\}$ and let $H = \langle x, b_1, b_2, : w = 1 \rangle$. Then the Freiheitssatz states that the obvious map from G into H is injective.

In particular, if $G = \langle a \rangle$ is an infinite cyclic group, and $w(x; a)$ is a cyclically reduced word in x and a that contains x, then the equation

(3.7) $$w(x; a) = 1$$

has a solution in some group H containing G.

Next, let $G = \langle a \rangle$ be a finite cyclic group; for simplicity we assume it has prime order p. When does (3.7) have a solution? This is equivalent to the question:

(3.8) *In a free group with basis $\{a, x\}$, do the equations*

$$a^p = 1 \text{ and } w(x; a) = 1 \text{ imply } a = 1?$$

If $w(1;a) = 1$, we may take $H = G$ with $x = 1$. Assume that $w(1;a) = a^k \neq 1$: after change of generator for G we may suppose that $w(1;a) = a$. Let $w(x;1) = x^e$. If $e \neq 0$, we can take H cyclic of order ep, on generator x, with $x^e = a$.

We now examine the case that $w(1;a) = a$ and $w(x;1) = 1$. Then (3.7) is equivalent to an infinite set of relations among the elements $v_i = x^{-i}ax^i$. We look for solutions in a group H such that the subgroup V generated by the v_i is abelian, and hence a vector space over Z_p. If we define $T: V \to V$ by $T: v_i \to v_{i+1}$, then T is a linear transformation on V, and (3.7) takes the form of a condition

$$(3.9) \qquad f(T) = 0$$

for a certain polynomial $f(\xi)$ over Z_p. Since $w(1;a) = a$, $f(1) = 1$, and $f(\xi)$ is not the polynomial 0. If $f(\xi)$ has degree n, then we may take V to have dimension n, and we are seeking an invertible transformation $T: V \to V$ such that $f(T) = 0$. We may write $f(\xi) = \xi^m\ g(\xi)$ where $g(\xi)$ is not divisible by ξ. If $g(\xi) = 1$, hence $f(\xi) = \xi^m$, there exists no invertible T satisfying $f(T) = 0$. Otherwise we can choose invertible T satisfying $g(T) = 0$, and hence $f(T) = 0$. We now let H be the split extension of V by its automorphism T: if we identify $a = v_1$, $G = Z_p v_1$, and $x = T$, then the equation $w(x;a) = 1$ is satisfied.

Example. We use the standard notation $\bar{u} = u^{-1}$, $u^v = v^{-1}uv$, $[u, v] = u^{-1}v^{-1}uv$. Let $G = \langle a \rangle$ be a cyclic group, and consider the equation

$$(3.10) \qquad a^{x^2} = [a, a^x].$$

Here we have $f(\xi) = \xi^2$, and the argument above (for G of prime order) does not apply. (In fact, in any group H generated by elements a and x satisfying (3.10), the normal closure V of a is its own derived group, hence cannot be solvable unless it is trivial.)

We have noted that it follows from the Freiheitssatz that (3.10) has a solution for G an infinite cyclic group; this follows also by an argument below. Let G have finite order m. We shall see that (3.10) has no solution if $m = 2$, but that it has a solution whenever $m \geq 6$.

We prove first that, in a free group with generators a and x,

$$(3.11) \qquad a^{x^2} = [a, a^x] \textit{ and } a^2 = 1 \textit{ implies } a = 1.$$

Since $a^2 = 1$ implies $a^{-1} = a$ and $(a^x)^{-1} = a^x$, we have $[a, a^x] = (aa^x)^2$, and hence $a^{x^2} = [a, a^x] = (aa^x)^2$. Now $a^2 = 1$ implies $(a^{x^2})^2 = 1$ and so $(aa^x)^4 = 1$, whence $a^x(aa^x)^2 = aa^xa$. We thus have $(aa^x)^x = a^xa^{x^2} = a^x(aa^x)^2 = aa^xa = a^{-1}a^xa$, whence $((aa^x)^x)^2 = (a^{-1}a^xa)^2 = 1$, $(aa^x)^2 = 1$, $a^{x^2} = (aa^x)^2 = 1$, and, finally, $a = 1$.

We next prove, using small cancellation theory, that, for G of order $m \geq 6$, equation (3.10) has a solution. In fact, we obtain a solution satisfying the additional condition $x^n = 1$, provided that $n \geq 11$: Precisely, we prove the following:

(3.12) *Let* $m \geq 6$, $n \geq 11$, *and* $0 < k < m^k$. *Then, in a free group with generators* a *and* x, *the element* a^k *is not in the normal closure of the three elements* $a^{-x^2}[a, a^x]$, a^m *and* x^n.

The element $a^{-x^2}[a, a^x]$ has a cyclically reduced conjugate

$$u = \bar{x}\bar{a}xx\bar{a}\bar{x}\bar{a}\,xa\bar{x}a,$$

with

$$\bar{u} = \bar{a}x\bar{a}\bar{x}ax\,a\bar{x}\bar{x}ax.$$

Let R^* consist of a^m, a^{-m}, x^n, x^{-n}, and all cyclic permutations of u and $\bar{u}$. A *piece* is a common initial segment of two distinct elements of R^*. Inspection shows that the only pieces are the following words and their subwords:

$$xx, \quad \bar{x}\bar{x}, \quad xa\bar{x}, \quad x\bar{a}\bar{x}, \quad \bar{x}ax, \quad \bar{x}\bar{a}x.$$

Suppose given a factorization $u' = p_1, \ldots, p_k$ of a conjugate u' of u into k pieces $p_1, \ldots, p_k$. Let $\tilde{p}_1$ be a maximal piece containing p_1. Then a conjugate u'' of u has a factorization $u'' = \tilde{p}_1, \ldots, \tilde{p}_{\tilde{k}}$ where, for $1 < i \leq \tilde{k}$, $u'' = \tilde{p}_1, \ldots, \tilde{p}_{i-1}w_i$ and $\tilde{p}_i$ is the longest piece beginning w_i. Evidently $\tilde{k} \leq k$.

Since a is the longest piece of a^m, a^m cannot be the product of fewer that $m \geq 6$ pieces. Since xx is the longest piece of x^n, x^n cannot be the product of fewer than $\left[\frac{n+1}{2}\right] \geq 6$ pieces. We now consider a factorization of a conjugate of u into pieces. If xx is a piece in this factorization, we may suppose that $xx = \tilde{p}_1$. Then the method above gives a factorization

$$u'' = (xx)(\bar{a}\,\bar{x})(\bar{a}\,x)(a\,\bar{x})(a\,\bar{x})(\bar{a})$$

into $\tilde{k} = 6$ pieces. The remaining possibility is that the two letters of the part xx of u belong to different pieces in the factorization, and hence the second x begins a piece. This gives four maximal factorizations $u'' = \tilde{p}_1, \ldots, \tilde{p}_{\tilde{k}}$ as above, all with $\tilde{k} = 5$; these are

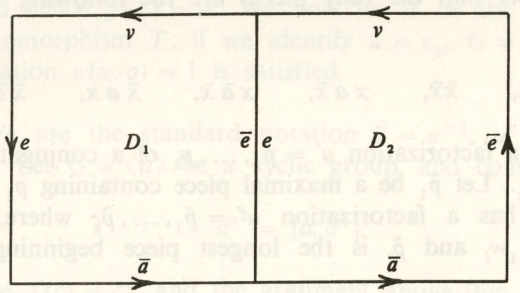
$$u'' = (x\bar{a}\bar{x}) \begin{Bmatrix} (\bar{a})(xa\bar{x}) \\ (\bar{a}x)(a\bar{x}) \end{Bmatrix} \begin{Bmatrix} (a)(\bar{x}\bar{a}x) \\ (a\bar{x})(\bar{a}x) \end{Bmatrix}.$$

In all cases, the segment $x\bar{a}\bar{x}$ of u'' is a piece in the factorization.

For fixed $w \neq 1$ in the normal closure of u, a^m, and x^n, we consider a reduced diagram Δ over these relators with boundary label w. Here Δ is a finite, connected, and simply connected planar 2-complex whose edges are labelled with elements of the free group F with basis $\{a, x\}$, and the boundary labels on the faces (2-cells) of Δ are u, a^m, or x^n. If two faces D_1 and D_2 of Δ have a side in common, the label on that side must be a piece. Now a face D_1 of Δ, interior to Δ (that is, not abutting on the boundary of Δ), can have fewer than 6 sides only if the boundary label on D_1 is u, and D_1 abuts on a second face D_2, necessarily also with boundary label u, along a side with label $x\bar{a}\bar{x}$. We write $u'' = e\bar{a}\bar{e}v$ where $e = x\bar{a}\bar{x}$ and $v = a\bar{x}\bar{a}x = [\bar{a}, x]$. Then the label on the boundary of the union $D = D_1 \cup D_2$ is

$$(v\,e\,\bar{a}\,\bar{e})(e\,\bar{a}\,\bar{e}\,v) = v\,e\,\bar{a}^2\,\bar{e}\,v$$

conjugate to $u_2 = e\bar{a}^2\bar{e}\,v^2$. See Figure 1 below.



We now modify Δ by uniting all such pairs of faces D_1 and D_2 related in this way. The resulting diagram Δ^* will have faces with boundary labels a^m and x^n as before, and also with labels

$$u_k = e\,\bar{a}^k\bar{e}\,v^k, \quad \text{for} \quad k = 1, 2, 3, \ldots$$

By construction, no interior face of Δ^* with label u_1 has fewer than 6 sides.

It is easy to see that no conjugate of any u_k has a factorization into fewer than $2k + 3$ pieces of the sorts considered earlier; now, for $k \geq 2$, we have $2k + 3 > 6$. The possibility remains that u_k could have a factorization into fewer pieces, where now some piece, longer than those considered above, is a segment common to u_k and some $u_{k'}$. It is easy to see that such a longer piece must contain a factor v from u_k. We consider then faces D_1 and D_2 of Δ^* with boundary labels u_k, $u_{k'}$, abutting along a side

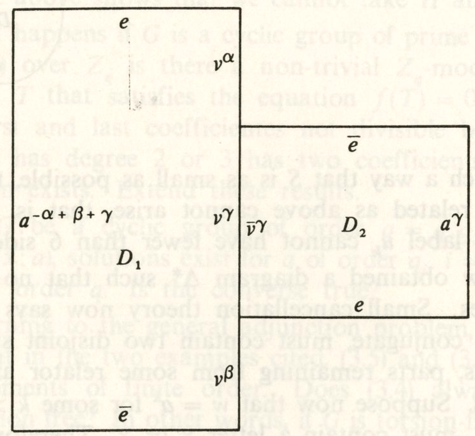
whose label contains a factor v. The label on the union $D = D_1 \cup D_2$ is then

$$(v^p\,e\,\bar{a}^{p+q+1}\,\bar{e}\,v^q\,v)(\bar{v}\,\bar{v}^{q'}\,e\,a^{p'+q'+1}\,\bar{e}\,\bar{v}^{p'})$$

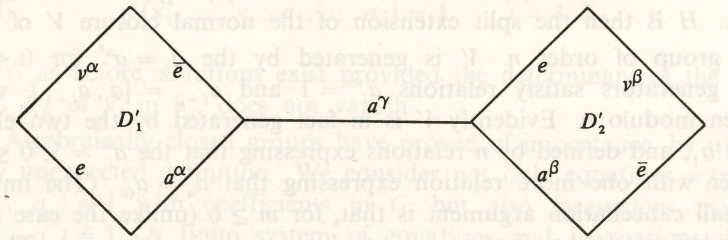
where $p, q, p', q' \geq 0$ and $p + q + 1 = k$, $p' + q' + 1 = k'$. This is conjugate to

$$z = v^{p-p'}\,e\,\bar{a}^{p+q+1}\,\bar{e}\,v^{q-q'}\,e\,a^{p'+q'+1}\,\bar{e} =$$
$$= v^{\alpha}\,e\,\bar{a}^{\alpha+\beta+\gamma}\,\bar{e}\,v^{\beta}\,e\,a^{\gamma}\,\bar{e},$$

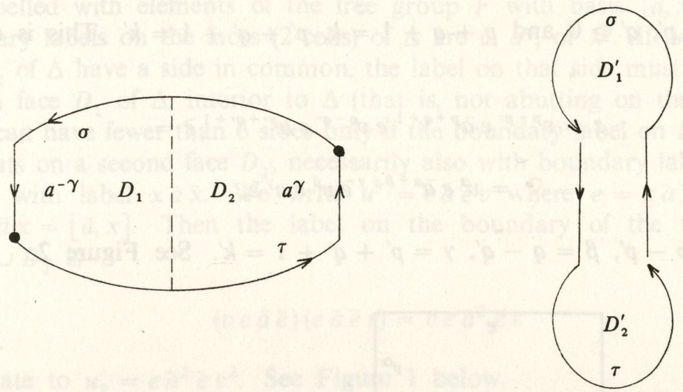
where $\alpha = p - p'$, $\beta = q - q'$, $\gamma = p' + q' + 1 = k'$. See Figure 2:



We now observe that the same label z can be obtained as the boundary label of a second 2-complex K, with two faces D_1' and D_2', as shown in Figure 3. We now modify the complex Δ^* by deleting the part $D = D_1 \cup D_2$,



leaving a 'hole' H with boundary label z; after deforming the 'hole' H (or, rather, Δ^* H) to bring the two arcs labelled $\bar{a}^{\gamma}$ and a^{γ} together, we fill in the hole with the complex K. See Figure 4. Since the sum of the lengths of the boundary labels of D_1' and D_2' is less than for D_1 and D_2, we have decreased the sum S of the lengths of the boundary labels on the faces of Δ^*. If we now suppose that, for given $w \neq 1$, Δ^* with boundary label w has



been chosen in such a way that S is as small as possible, then the situation with D_1 and D_2 related as above cannot arise, that is, for all $k \geq 1$, an interior face with label u_k cannot have fewer than 6 sides.

We have now obtained a diagram Δ^* such that no interior face has fewer than 6 sides. Small cancellation theory now says that w, or some cyclically reduced conjugate, must contain two disjoint subwords that are *3-remnants*, that is, parts remaining from some relator after deletion of 3 consecutive pieces. Suppose now that $w = a^k$ for some $k > 0$. A 3-remnant of x^n or of any u_k must contain a letter x or $\bar{x}$. Therefore the 3-remnants in w must be obtained from a^m by deleting 3 pieces a or 1, that is, they must have the form a^s for $s \geq m - 3$. It follows that $k \geq 2(m-3) = 2m - 6 \geq m$. This completes the proof.

Remark 1. Let $H = \langle a, x : a^m = x^n = 1, a^{x^2} = [a, a^x]\rangle$, where $m \geq 6$ and $n \geq 11$. H is then the split extension of the normal closure V of a by a cyclic group of order n. V is generated by the $a_i = a^{x^i}$ for $0 \leq i < n$. These generators satisfy relations $a_i^m = 1$ and $a_{i+2} = [a_i, a_{i+1}]$, where i is taken modulo n. Evidently V is in fact generated by the two elements a_0 and a_1, and defined by n relations expressing that the $a_i^m = 1$, $0 \leq i < n$, together with one more relation expressing that $a_n = a_0$. (The impact of the small cancellation argument is that, for $m \geq 6$ (unlike the case $m = 2$), these relations do not force $a_0 = a$ to have order less than m). The small cancellation argument given above also shows that no relation $(ax)^k = 0$, for $k > 0$, holds in H, whence ax has infinite order, H is infinite, and hence V is infinite. It is not known whether a solution of (3.10) holds in

any finite group H_0 (a finite quotient of H in which the image of a retains order m), or, indeed, whether V is residually finite, or even if V has any non-trivial finite homomorphic image.

Remark 2. The same small cancellation arguments apply (without the special complications above) to show that the equation

$$(a^s)^{x^t} = [a, a^x], \qquad (3.13)$$

for larger values of s and t, has a solution with $a^m = 1$ and $x^n = 1$, provided that $m \geq 6s$, $n \geq 6t$.

Problems. (1) Find conditions, in the case that $f(\xi) = \xi^m$, for the existence of a solution to (3.7): When can H be taken as nilpotent? When solvable? (The argument above shows that we cannot take H abelian or metabelian.)

(2) What happens if G is a cyclic group of prime power order $q = p^k$? For what $f(\xi)$ over Z_q is there a non-trivial Z_q-module V admitting an automorphism T that satisfies the equation $f(T) = 0$? If $g(\xi)$ has degree $n \geq 1$ with first and last coefficientes not divisible by p, then a solution exists. If $f(\xi)$ has degree 2 or 3 has two coefficients not divisible by p, then a solution exists. Extend these results.

(3) Let G be a cyclic group of order $q = q_1 q_2$ where $(q_1, q_2) = 1$. If, for given $w(x; a)$, solutions exist for a of order q_i, $i = 1, 2$, then a solution exists for a of order q. Is the converse true?

(4) Returning to the general adjunction problem, of solving (3.4) over G, we note that in the two examples cited, (3.5) and (3.12), the group G has non-trivial elements of finite order. Does (3.4) always have a solution when G is torsion free? In other words, if G is torsion-free, and $P = G * \langle x \rangle$ where $\langle x \rangle$ is infinite cyclic, and if cyclically reduced w in P does not lie in G, does the normal closure of w in P have trivial intersection with G?

We remark in passing that the results of Gerstenhaber and Rothaus extend to a system of n equations in n unknowns:

$$w_i(x_1, \ldots, x_n; a_1, \ldots, a_m) = 1, \qquad i = 1, 2, \ldots, n. \qquad (3.14)$$

For G as before, solutions exist provided the determinant of the exponent sums e_{ij}, of x_j in w_i, does not vanish.

Algebraically closed groups have proved of importance, by using a slightly unexpected definition. We consider not only equations $w_i(x_1, \ldots, x_n; a_1, \ldots, a_m) = 1$ with coefficients in G, but also *inequations* $z_i(x_1, \ldots, x_n; a_1, \ldots, a_m) \neq 1$. A finite system of equations and inequations over G is *consistent* if it has a solution in some H containing G. Now we call G *algebraically closed* if every consistent finite system over G has a solution in G itself. W. R. Scott (50), who introduced this notion, showed that every group is contained in some algebraically closed group. B. H. Neumann (41) showed that every algebraically closed group is simple. Neumann (41) showed that if a finitely generated group G has solvable word problem, then G can be embedded in every algebraically closed group, and Macintyre (32) proved the converse. This despite Miller's (37) result that no algebraically closed group has a recursive presentation, that is, can be described effectively.

4. Commutators.

We write $\bar{u} = u^{-1}$ and $[u, v] = \bar{u}\bar{v}uv$.

Consider the equation

$$[x, y] = a, \tag{4.1}$$

for a in a group G. There always exists a solution in some group H containing G (and even with $x^2 = y^2 = 1$, hence $(xy)^2 = a$). Therefore we confine attention to solutions with x, y in G itself.

Clearly a solution exists only if a is in the commutator subgroup (derived group) G' of G. Now every element of G' is a product of commutators, but not every product of commutators is equal to a single commutator. Rodney (45) gave a simple example of a group G. of order 2^{10}, in which some product of two commutators is not itself a commutator, and Guralnick (18*a*, *b*) gave an example of such a group G of minimal order, $|G| = 96$. Dark and Newell (9) examine the same question for 'higher commutators' $[[\ldots[[x_1, x_2], x_3], \ldots], x_n]$.

If $G = S_n$, the symmetric groups of degree n, then $G' = A_n$, the alternating group. It is easy to see that every a in A_n is the commutator of two elements x, y from G_n. If $n \geq 5$, then A_n is simple, and $A_n' = A_n$. In this case, every element a of A_n is the commutator of two elements from A_n itself. For the known non-abelian finite simple groups G, for all a in G the equation (4.1) has a solution with x, y in G.

(1) What other groups have this property?

(2) Can this property be proved for all, finite simple groups without appeal to a catalog of such groups? Can it be deduced from simplicity, or from some other property of all known finite simple groups? Do all infinite simple groups have this property?

We next ask what elements of a free group G are commutators, that is, for which a in G does the equation (4.1) have a solution in G. This question is answered by a theorem of Wicks (58):

(4.2) *Let a be an element of a free group G with given basis B. Then a is a commutator of two elements of G if an only some conjugate a_1 of a is represented, relative to B, by a cyclically reduced wor $a_1 = \bar{u}\bar{v}\bar{w}uvw$, where there is no cancellation among the displayed factors* (*some of which may be trivial*).

Note that this theorem provides an easy test for an element to be a commutator. For example, let $a = [b_1, b_2][b_3, b_4] = \bar{b}_1\bar{b}_2 b_1 b_2 \bar{b}_3 \bar{b}_4 b_3 b_4$. It is immediate that no cyclic permutation of this word has a factorization of the required form. Thus the product of two commutators is not always a commutator (indeed, that a is a commutator follows also from the examples, in finite groups, mentioned above).

A formally similar result concerns $n - by - n$ matrices over a field. H. Flanders (17) characterizes pairs of matrices, a and b, such that the pair of equations

$$a = xy, \qquad b = yx \tag{4.3}$$

has a solution in matrices x, y. Taussky-Todd (53) showed that, for a and b non singular, the system

$$a = xyz, \qquad b = zyx \tag{4.4}$$

has a solution if and only if $\det a = \det b$. This means that $\det(ab^{-1}) = 1$ and that $ab^{-1} = xyzx^{-1}y^{-1}z^{-1}$ in $SL(n, K) = G'$, for $G = GL(n, K)$. Brenner and Lim (5) showed that, for arbitrary a, b in any group G, (4.4) has a solution if and only if ab^{-1} is a commutator.

In case (4.1) has a solution, $g = [x_0, y_0]$, in a free group G, the problem remains of describing all solutions in G, that is, all x, y in G such that

$$[x, y] = [x_0, y_0]. \tag{4.3}$$

(Henceforth we exclude the trivial case that $a = [x_0, y_0] = 1$.) A theorem of Nielsen says that, in the case that $G = \langle x_0, y_0 \rangle$, $[x, y]$ is conjugate to $[x_0, y_0]^{\pm 1}$ if and only if the map $x_0 \to x$, $y_0 \to y$ defines an automorphism of G, that is, if and only if $\{x, y\}$ is another basis for G. It follows that, in this case, the stabilizer of $[x_0, y_0]$ in Aut G has index 8, and is generated by the transformations

$$A: (x, y) \to (x, xy), \qquad B: (x, y) \to (yx, y).$$

However, for arbitrary x_0, y_0 in a free group G, $[x_0, y_0]$ is left unchanged by more general transformations

$$A^*: (x, y) \to (x, x_1 y) \text{ where } [x, x_1] = 1,$$

$$B^*: (x, y) \to (y_1 x, y) \text{ where } [y, y_1] = 1.$$

Burns, Edmunds, and Farouqi (8), following Malcev and Hmelevskii, showed that every solution of (4.1) is (A^*, B^*)-equivalent to a solution (x, y) with lengths $|x|$, $|y| < \frac{1}{2}|a|$, whence it follows that all solutions fall into a finite number of (A^*, B^*)-families: They asked if all solutions fall within one such family, but an example of Lyndon and Wicks (31) shows that this is not always the case. A different counterexample is as follows:

(4.4) *Let* $G = \langle x, y\rangle$, *free of rank* 2, *and let*

$$a_1 = y^{-1}x^2y^2x^2, \qquad b_1 = x^3y^2x^2y^2x^3y,$$

$$a_2 = yx^2y^2x^5y^2x^2, \qquad b_2 = y^2x^3y.$$

Then $[a_1, b_1] = [a_2, b_2]$, *but* (a_1, b_1) *and* (a_2, b_2) *are not* (A^*, B^*)*-equivalent. Explicitly, the group* $U_1 = \langle a_1, b_1\rangle$ *is root-closed:* $\dot{z} \in G$ & $z^n \in U_1$ & $n \neq 0 \Rightarrow z \in U_1$; *and* $U_1 \neq U_2 = \langle a_2, b_2\rangle$.

We note that the above example was obtained by solving the condition: $\bar{u}_1\bar{v}_1u_1v_1$ conjugate $\bar{u}_2\bar{v}_2u_2v_2$ under the assumption that both expressions are cyclically reduced without cancellation. This is essentially a problem concerning a free monoid equipped with an involutory automorphism $u \to \bar{u}$, and, as such, was solved in principle by A. Lentin (letter, 1978).

5. Equations in free groups.

We return to the equation

(5.1) $$w(x; b_1, \ldots, b_r) = 1,$$

where $b_1, \ldots, b_r$ form a basis for a free group G, and we ask now for all solutions x in G.

We have seen that the equation

(5.2) $$x^n = a,$$

for $n \geq 1$, has at most one solution. Similarly, it is easily decided if the equation

(5.3) $$x^{-1}ax = b,$$

has a solution x_0; if a is not a proper power, then the general solution is $x = a^\mu x_0$ for arbitrary $\mu \in Z$. To consider another equation in one unknown, it is not difficult to see that the solutions of

(5.4) $$[[a, x], [b, x]] = 1,$$

in G free with basis $\{a, b\}$, are precisely the elements of the three forms

(5.5) $$a^\mu,\ b^\mu,\ (ab^{-1})^\mu, \text{ arbitrary } \mu \in Z.$$

Lorents (21, 22) improved *a* result of Lyndon (24, 25) by showing that the totality of solutions of (5.1) always of precisely the elements of one of a finite number of forms:

(5.6) $$u_1^{\mu_1}v_1, \ldots, u_n^{\mu_n}v_n.$$

The equation, in two unknowns, over G free with basis $\{a, b\}$,

(5.7) $$[[a, x], [b, y]] = 1$$

has its solutions given by six pairs of parametric word. Three of these are

(5.8) $$\begin{cases} (x, y) = (a^\mu, v), \text{ for } v \text{ arbitrary}, \\ (x, y) = (a^\mu b, b^\nu a), \\ (x, y) = (a^\mu ba^{-1}, b^\nu a^{-1}); \end{cases}$$

the other three are their symmetric counterparts under exchange of (x, a) with (y, b).

On the other hand, Appel (1) showed that an equation

(5.6) $$w(x, y;\ b_1, \ldots, b_r) = 1,$$

in two (or more) unknowns, need not have its solutions given by any finite set of parametric words, even admitting nested parameters, and arbitrary variables (as v in (5.8) above). Specifically, over G free with basis $\{a, b\}$, the equation

(5.10) $$[x, y] = [a, b]$$

admits among its solutions all instances of the following parametric words:

(5.11) $$(a, b), (b^{\mu_1}a, b), (b^{\mu_1}a, (b^{\mu_1}a)^{\nu_2}b),$$

$$(((b^{\mu_1}a)^{\nu_1}b)^{\mu_2}b^{\mu_1}a, (b^{\mu_1}a)^{\nu_1}b), \ldots .$$

It is not difficult to see that not all instances of these are instances of any finite set of parametric words.

Lorents (23) showed, however, that it is decideble whether an equation (5.9), in two unknowns, has *a* solution given by a finite set parametric words.

We now turn to equations 'without constants' over a free group G. That is, we seek all solutions of an equation

$$w(x_1, \ldots, x_n) = 1 \tag{5.12}$$

in a free group G.

The first such equation studied was the Vaught equation,

$$x^2 y^2 = z^2. \tag{5.13}$$

Vaught (unpublished) had conjectured that (5.13), for x, y, z elements of any free group, implies $xy = yx$. This was proposed as a test problem for the question of the decidability of implications of the form

$$w_1(x_1, \ldots, x_n) = 1 \quad \textit{implies} \quad w_2(x_1, \ldots, x_n) = 1 \tag{5.14}$$

in the theory of free groups.

Many proofs of Vaught's conjecture, and variants, have been given. For example, Lyndon and Schützenberger (30) proved that

$$x^p y^q = z^r, \text{ where } p, q, r \geq 2, \tag{5.15}$$

implies $xy = yx$, or, equivalently, that x, y, and z all lie in a cylic subgroup of G: $x = z^\ell$, $y = z^m$, $y = z^n$ for some z. Schützenberger proved also that the equation

$$[x, y] = z^r, \qquad r \geq 2, \tag{5.16}$$

implies $z = 1$; that is, no non-trivial commutator is a proper power.

Edmunds (13) gave the following elegant solution of the Vaught problem. It is to be shown that (5.13) implies that the subgroup $U = \langle x, y, z \rangle$ of G is cyclic. The topological fact that a torus with one crosscap is homeomorphic to a sphere with three crosscaps takes the algebraic from that, in a free group F of rank 3 with basis $\{x, y, z\}$, there is an automorphism of F carrying $[x, y] z^2$ to $x^2 y^2 z^2$. In fact, we have the identity

$$[x, y] z^2 = (x^{-1} z^{-1} y^{-1})^2 (yzxyzy^{-1} z^{-1} y^{-1})^2 (yz)^2, \tag{5.17}$$

where inspection shows that the three words in parenthesis are a basis for F. In view of this, Vaught's problem is equivalent to that of showing that

$$[x, y] = z^2 \tag{5.18}$$

implies that $U = \langle x, y, z \rangle$ is cyclic (a special case of Schützenberger's result). By Wicks's theorem ((4.2) above), after conjugation we may suppose

that we have $\bar{u}\,\bar{v}\,\bar{w}\,u\,v\,w = zz$, cyclically reduced and with no cancellation on the left; since zz is cyclically reduced, z is also, and there is no cancellation on the right. But this implies that $z = \bar{u}\,\bar{v}\,\bar{w} = u\,v\,w$ without cancella tion, hence (comparing lengths) that $\bar{u} = u$, $\bar{v} = v$, $\bar{w} = w$ and that $u = v = w = 1$. Finally, this gives $z = 1$, hence $\langle x, y, z \rangle$ cyclic.

This example suggests considering, in connection with a word w in a free group G, the maximum renk $r = r(U)$ of the subgroup $U = \langle x_1, \ldots, x_n \rangle$ generated by a solution of the equation $w(x_1, \ldots, x_n)$. Alternatively, r is the maximum rank of a free homomorphic image of the group $H = \langle x_1, \ldots, x_n : w = 1 \rangle$. This concept of *inner rank* has arisen independently in topology. For example, it is well known that the inner rank of $w = x_1^2, \ldots, x_n^2$ is $[\frac{n}{2}]$, the greatest integer in $\frac{n}{2}$. For $w = [x_1, x_2], \ldots, [x_{2g-1}, x_{2g}]$ it is g: (From (5.17) it follows that $w = [x_1, x_2], \ldots, [x_{2k-1}, x_{2k}] x_{2k+1}^2, \ldots, x_n^2$ has inner rank $[\frac{n}{2}]$.)

By analogy with Galois theory, one may ask for the group of automorphisms of G that fixes $S = w(x_1, \ldots, x_n)$ (or its conjugacy class). For w the defining relator of the fundamental group of a surface, $w = \Pi\,[x_{2i-1}, x_{2i}]$ or $w = \Pi x_i^2$, these stabilizers are the 'mapping class groups' for which McCool (36) obtained finite presentations. The stabilizer of a word of the form $w = x_1^{m_1}, \ldots, x_n^{m_n}$ has been studied by Zieschang (60).

It is implicit in Nielsen's work that if n elements of a free group satisfy a non-trivial relation, then the subgroup they generate has rank less than n. Thus if $w(x_1, \ldots, x_n)$ is not trivial, it has inner rank $r \leq n - 1$. Steinberg (52) showed that $r = n - 1$ if and only if w lies in the normal closure in G of an element of a basis for G. Baumslag and Steiberg (4) showed that if $w(x_1, \ldots, x_{n-1})$ is not a proper power or an element of a basis, and $k > 1$, then the equation

$$w(x_1, \ldots, x_{n-1}) = x_n^k \tag{5.19}$$

has rank $r \leq n - 2$:

At the other extreme, for $k > 1$ the word $w = x_1^k$ has rank $r = 0$, while all other words have rank $r \geq 1$, that is, admit a solution in an infinite cyclic group. Stallings (51) cites a family of words w, in $n \geq 2$ variables, of rank $r = 1$. Let $n \geq 2$ and, for $1 \leq i < j \leq n$, let a_{ij} and b_{ij} be integers such that all a_{ij} are different and all $a_{ij} b_{ij} = 2^N$ for some fixed N. Then the word

$$w = \prod_{1 \leq i < j \leq n'} [x_i^{a_{ij}}, x_j^{a_{ij}}]^{b_{ij}},$$

where the product may be taken in any order, has rank $r = 1$.

The equation

$$x^p y^p = z^p \tag{5.20}$$

in a free metabelian group was studied by G. Baumslag and Mahler (3) and by Lyndon (26).

Wicks (59) considered the Vaught problem in free products. He showed that it groups G_1 and G_2 both satisfy the two conditions

(1) $x^2 = 1$ *implies* $x = 1$,

(2) $x^2y^2 = z^2$ *implies* $xy = yx$,

then their free product $G = G_1 * G_2$ also satisfies these conditions.

This result can be generalized: Let Q_n be the condition, on a group G, that, for all $m \le n$, if $x_1^2, \ldots, x_m^2 = 1$, for elements $x_1, \ldots, x_m$ of G, then $U = \langle x_1, \ldots, x_m \rangle$ has rank $r \le \frac{1}{2}n$ (that is, U can be generated by $r \le n/2$ elements). By the methods of (27) it can be shown that if G_1 and G_2 satisfy Q_n, then $G = G_1 * G_2$ will also satisfy Q_n. For $n = 4$, this implies that if G_1 and G_2 both satisfy (1), (2) and the condition.

(3) $x_1^2x_2^2x_3^2x_4^2 = 1$ *implies that* $U = \langle x_1, \ldots, x_4 \rangle$ *is the free product of two abelian groups*, then $G = G_1 * G_2$ will also satisfy (1), (2), and (3).

An analogous result holds with Q_n replaced by the condition P_n, that, for all g such that $2g \le n$, $[x_1, x_2], \ldots, [x_{2g-1}, x_{2g}] = 1$ implies that $U = \langle x_1, \ldots, x_{2g} \rangle$ has rank $r \le g$.

6. The substitution problem.

We have discussed the question of when a given element a of a group G is the square of an element of G, or the commutator of two elements of G. More generally, one may ask if a can be represented in a given form, that is, whether an equation

$$w(x_1, \ldots, x_n) = a \tag{6.1}$$

has solutions in G. (Note that if $a = 1$, this reduces to the class of problems considered above.)

If F is a free group with basis $x_1, \ldots, x_r$, $r \le n$ this amounts to asking if there exists a homomorphism ϕ from F into G such that $w\phi = a$. In the special case that G is a free group, we may identify F with G, whence we are looking for an endomorphism ϕ of G carrying w to a. For this reason, in the case that G is free, this problem is commonly called the *endomorphism problem*.

Let G be a finite group. If G has odd order, the map $g \to g^2$ is one-to-one, whence the equation

$$x^2 = a \tag{6.2}$$

has a solution for all in G. If G has elements of even order, and a has maximal even order (or generates a maximal cyclic subgroup of even order), then, for this a, (6.2) has no solution.

We skip to the equation

$$x^2y^2z^2 = a. \tag{6.3}$$

By virtue of the well known identity

$$[x, y] = (x^{-1}y^{-1})^2(yxy^{-1})^2y^2, \tag{6.4}$$

every commutator is a product of three squares. It follows that, as far as is known, every element of a non-abelian finite simple group is a product of three squares.

Not every commutator is a product of two squares; from (6.4) and (5.17) it follows that every product of n commutators is a product of $2n + 1$ squares, and Lyndon, McDonough, and Newman (28) showed that the number $2n + 1$ is best possible. Nonetheless, it is easy to show directly that every element of the alternating group A_n, for $n \ge 5$, is the product of the squares of two elements of A_n. That is, the equation

$$x^2y^2 = a \tag{6.5}$$

has a solution of every a in A_n, $n \ge 5$. We have not examined the question whether the same is true in other finite simple groups, or perhaps yet other groups.

From the elementary fact that every group of exponent 2 is abelian, it follows that some such formula as (6.4) must hold, expressing an arbitrary commutator as the product of some number of squares. In the same way, it is known that in a group of exponent 3 conjugate elements commute, that is, all $[x^y, x] = 1$. It follows that $[x^y, x]$ is identically equal (that is, equal in F free with basis $\{x, y\}$) to a product of some number of cubes. In fact, one finds that

$$[y^{-1}xy, x] = (y^{-1}x^{-1}y^2)^3y^{-3}(yx)^3(x^{-1}y^{-1}x^{-1}y^{-1}xyx)^3. \tag{6.6}$$

It is also known that the second derived group of a group of exponent 3 is trivial, whence there exists a formula

$$[[x_1, x_2], [x_3, x_4]] = u_1^3, \ldots, u_k^3 \tag{6.7}$$

for some integer k and some words $u_i = u_i x_1, \ldots, x_4)$. Thus, although a commutator is not always a product of any number of cubes, every commutator of commutators is a product of a bounded number of cubes. In A_n,

$n \geq 5$, or any group G in which every element is a commutator, it follows that every element is a product of k cubes.

Problems. (1) Find an explicit formula (6.7) with k as small as possible.

(2) What is the smallest k_0 such every element of A_n, $n \geq 5$, is a product of k_0 cubes?

(3) Is every element of A_n, $n \geq 5$, *a* product of fifth powers? A product of a bounded number of fifth powers?

(4) In analogy with the equation $[x, y] = a$, is it possible to describe the set of all solutions of the equation $x^2y^2 = a$? (This is perhaps implicit in the work of Edmunds: what about $x^3y^3 = a$?)

(5) (Edmunds) If an element a of a free group is a product of two commutators, and is also a square, must it then be the square of a commutator?

We conclude our discussion with a sketch of Edmunds' (11, 14, 15) treatment of the endomorphism problem. We take F a free group with basis $x_1, x_2, \ldots$, and $w(x_1, \ldots, x_n)$ an element of F. For a in F, we define a solution of the equation (6.1) to be an endomorphism ϕ of F such that $w\phi = a$. If we write $x_i\phi = u_i$, then we have $w\phi = w(u_1, \ldots, u_n) = a$.

If α is any automorphism of F and ϕ is a solution of $w = a$, then $\phi' = \alpha^{-1}\phi$ is a solution of $w' = a$, where $w' = w\alpha$. If some $x_i\phi = 1$, say $x_n\phi = 1$, then let ε be the endomorphism of F sending x_n to 1 and fixing the remaining x_i. Then ϕ is also a solution of $w' = a$, where $w' = w\varepsilon = w(x_1, \ldots, x_{n-1}, 1)$.

If there is cancellation in the equation $w(u_1, \ldots, u_n) = a$, and if no $u_i = 1$, then there is cancellation in the image of some part xy^{-1} of w, where $x = x_i^{\pm 1}$, $y = x_j^{\pm 1}$ for some i, j and some choice of exponents. Writing $x\phi = u$, $y\phi = v$, there is cancellation in a part uv^{-1} of $w\phi$. For some $z \neq 1$, and some u', v', we have $u = u'z$, $v = v'z$, $uv^{-1} = u'v'^{-1}$, all right members reduced. We make the substitution $\alpha : x \to xx_{n+1}$, $y \to yx_{n+1}$, leaving all x_k fixed for $k \neq i, j$. (In the case $i = j$, this requires special interpretation.) We define ϕ' by $x\phi' = u'$, $y\phi' = v'$, $x_{n+1}\phi' = z$, with $x_k\phi' = x_k\phi$ for all $k \neq i, j, n+1$. Then, if $w\alpha = w'(x_1, \ldots, x_{n+1})$, we have $w'\phi' = w\phi = a$. It is important to note that $\sum_{i=1}^{n+1} |x_i\phi'| < \sum_{i=1}^{n} |x_i\phi|$.

If any solution ϕ of (6.3) is given, by iteration of the transformations described above we obtain an endomorphism ε^*, a word $w^* = w\varepsilon^*$, and a homomorphism ϕ^*, such that ϕ^* is a solution of $w^* = a$ with the following properties:

(1) *no* $x_i\phi^* = 1$,

(2) *the equation* $w^*\phi^* = a$ *holds without any cancellation* among the factors $x_i\phi^*$.

Let $D(w)$ be the set of all w^* obtainavle from w in this way; it follows that (6.3) has a solution, for given a, if and only if a is the *cancellation free image* of some w^* in $D(w)$, in the sense of (1) and (2). Moreover, if a has length $|a| = n$, it is necessary to consider only w^* of length $|w^*| \leq n$. Now the description of $D(w)$ above departs from that of Edmunds, in that he makes certain technical modifications to eliminate redundancy, thereby decreasing $D(w)$. After this, he shows that the decidability of the existence of solutions for (6.3), for arbitrary a, is equivalent to the condition that the set $D(w)$ be recursive.

This generalizes the theorem of Wicks ((4.2) above). (Here the set $D(w)$ could be taken to consist of

(1) $x_1x_2x_3x_4x_2^{-1}x_5x_3^{-1}x_4^{-1}x_5^{-1}x_1^{-1}$;

(2) all words obtained from the above by setting some of x_1, x_4, x_5 equal to 1;

(3) the trivial word 1.)

Edmunds' method shows that (6.3) is decidable whenever w is quadratic, in that each x_i occurs at most twice (as x_i or x_i^{-1}) in w. For then each w^* in $D(w)$ is also quadratic, and the set of quadratic words is clearly recursive.

Edmunds also recovers a result of Schupp (49), that (6.3) is decidable whenever w contains at most two unknowns. This follows from the fact that, in this case, an element of $D(w)$, not of the form x_i^k, is always equivalent to w under an automorphism of F, together with Whitehead's algorithm for deciding whether two given elements of a free group F are equivalent under an automorphism of F. We note that some of Edmunds' arguments make substantial use of the coinitial graph (or star graph) introduced by Hoare, Karrass, and Solitar.

Added October 1979.

1. Marc Culler [62] has shown that $[x, y]^n$ can be written as a product of $[\frac{n}{2}] + 1$ commutators, giving the following example:

$$[x, y]^3 = [xyx^{-1}, y^{-1}xyx^{-2}]\,[y^{-1}xy, y^2].$$

He also shows that if $w = x^2y^2$ for some x, y in a free group, the w is conjugate to a cancellation-free instance of one the words a^2b^2, $abca^{-1}cb$, $a^2bc^2b^{-1}$.

2. R. M. Guralnick [64] discusses the least number $\lambda = \lambda(G) \leq \infty$ such that every element of G' is a product of λ commutators of elements from G. M. Rosenlicht [65] showed that if $[G : Z(G)] = n$, then $\lambda \leq n^3$. P. X. Gallagher [63] gave a character-theoretic condition for an alement of a finite group to be a product of k commutators, whence Guralnick deduces, for finite G, that λ is less than the number of different degrees of irreducible complex representations. Form this he concludes, for arbitrary

G, that $[G : Z(G)] = n$ implies $\lambda < \frac{1}{2}\, d(n)$, the number of divisors of n. Among further results, he shows that if G is nilpotent and $G/Z(G)$ is generated by n elements, then $\lambda \leq n$.

References

[1] Appel, K. I., *On two-variable equations in free groups*, Proc. Amer. Math. Soc. 21 (1969) 179-181.

[2] Baudisch, A., *Kommutatorsgleichungen in semifreiern Gruppen*, Acta Math. Acad. Sci. Hungar. 29 (1977) 235-249.

[3] Baumslag, G., Mahler, K., *Equations in free metabelian groups*, Mich. Math. J. 12 (1963) 375-379.

[4] Baumslag, G., Steinberg, A., *Residual nilpotence and relations in free groups*, Bull. Amer. Math. Soc. 70 (1964) 283-284.

[5] Brenner, J. L., Lim, M. J. S., *The matrix equations* $A = XYZ$ *and* $B = ZYX$ *and related ones*, Canad. Math. Bull. 17 (1974) 179-183.

[6] Bulitko, V. K., *Equations and inequalities in a free group and a free semigroup*, Tul. Gos. Ped. Inst. Ucen. Zap Mat. Kaf. *Vyp* 2 Geom. Alg. 1972, 242-252.

[7] Burns, R. G., Edmunds, C. C., Formanek, E., *The equation* $s^{-1}t^{-1}st = u^{-1}v^{-1}uv$ *in a free product of groups*, Math. Z. 153 (1977) 83-88.

[8] Burns, R. G., Edmunds, C. C., Farouqi, I. H., *On commutator equalities and stabilizers in free groups*, Canad. Math. Bull. 19 (1976) 263-267.

[9] Dark, R. S., Newell, M. L., *On conditions for commutators to form a subgroup*, J. London Math. Soc. 17 (1978) 251-262.

[10] Dey, I. M. S., Wiegold, J., *Generators for alternating and symmetric groups*, Austral. J. Math. 12 (1971) 63-68.

[11] Edmunds, C. C., *On the endomorphism problem for free groups*, Comm. Algebra 3 (1975) 7-20.

[12] Edmunds, C. C., *Products of commutators as products of squares*, Canad. J. Math. 27 (1975) 1329-1338.

[13] Edmunds, C. C., *A short combinatorial proof of the Vaught conjecture*, Canad. Bull. Math. 18 (1975) 607-608.

[14] Edmunds, C. C., *On the endomorphism problem for free groups*, II. Proc. London Math. Soc. 38 (1979) 153-168.

[15] Edmunds, C. C., *On conditions equivalent to the solvability of the endomorphism problem for free groups*, To appear.

[16] Finkelstein, H., Mandelberg, K. I., *On solutions of equations in symmetric groups*, J. Combinatorial Theory A25 (1978) 142-152.

[17] Flanders, H., *Elementary divisors of* AB *and* BA, Proc. Amer. Math. Soc. 2 (1951) 871-874.

[18] Gerstenhaber, M., Rothaus, O. S., *The solution of sets of equations in groups*, Proc. Nat. Acad. Sci. U.S.A. 48 (1962) 1531-1533.

[18*a*] Guralnick, R. M., *On groups with decomposable commutator subgroups*, Glasgow Math. J. 19 (1978) 159-162.

[18*b*] Guralnick, R. M., *On cyclic commutator groups*, To appear.

[19] Higman, G., Neumann, B. H., Neumann, H., *Embedding theorems for groups*, J. London Math. Soc. 24 (1949) 247-254.

[20] Itô, N., *A theorem on the alternating group* $A_n (n \geq 5)$, Math. Japon. 2 (1951) 59-60.

[21] Lorents, A. A., *Solution of systems of equations in one unknown in free groups*, Dokl. Akad. Nauk SSSR 148 (1963) 1253-1256.

[22] Lorents, A. A., *Coefficient-free equations in free groups*, Dokl. Akad. Nauk SSSR 160 (1965) 538-540.

[23] Lorents, A. A., *Representation of sets of solutions of systems of equations with one unknown in a free group*, Dokl. Akad. Nauk SSSR 178 (1968) 290-292.

[24] Lyndon, R. C., *Equations in free groups*, Trans. Amer. Math. Soc. 96 (1960) 445-457.

[25] Lyndon, R. C., *Groups with parametric exponents*, Trans. Amer. Math. Soc. 96 (1960) 518-533.

[26] Lyndon, R. C., *Equations in free metabelian groups*, Proc. Amer. Math. Soc. 17 (1966) 728-730.

[27] Lyndon, R. C., *Quadratic equation in free groups with amalgamation*, Houston J. Math.

[28] Lyndon, R. C., McDonough, T., Newman, M., *On products of powers in groups*, Proc. Amer. Math. Soc. 40 (1973) 419-420.

[29] Lyndon, R. C., Schupp, P. E., *Combinatorial group theory*, Ergebnisse der Math. 89 (1977).

[30] Lyndon, R. C., Schützenberger, M. P., *The equation* $a^M = b^N c^P$ *in a free group*, Mich. Math. J. 9 (1962) 289-298.

[31] Lyndon, R. C., Wicks, M. J., *Commutators in free groups*, To appear.

[32] Macintyre, A., *On algebraically closed groups*, Ann. of Math. 96 (1972) 53-97.

[33] Magnus, W., Karrass, A., Solitar, D., *Combinatorial group theory*, Wiley, New York, 1966.

[34] Makanin, G. S., *The rank of coefficient-free equations with four unknowns in a free semigroup*, Mat. Sb. 100 (1976) 285-311.

[35] Makanin, G. S., *The problem of the solvability of equations in a free semigroup*, Mat. Sb. 103 (1976) 147-236, 319.

[36] McCool, J., *Some finitely presented subgroups of the automorphism group of a free group*, J. Algebra 35 (1975) 265-270.

Miller, C. F. III.

[38] Mycielski, J., *Can one solve equations in groups?*, Amer. Math. Monthly 84 (1977) 723-726.

[39] Neumann, B. H., *Adjunction of elements to groups*, J. London Math. Soc. 18 (1943) 4-11.

[40] Neumann, B. H., *An essay on free products of groups with amalgamations*, Philos. Trans. Roy. Soc. London Ser. A 246 (1954) 503-554.

[41] Neumann, B. H., *The isomorphism problem for algebraically closed groups*, Word Problems, North-Holland, Amsterdam, 1973, 553-562.

[42] Ore, O., *Some remarks on commutators*, Proc. Amer, Math. Soc. 2 (1951) 307-314.

[43] Qin, Jian-Min., *On commutators in orthogonal groups*, Acta Math. Sinica 15 (1969) 708-719.

[44] Ree, R., *Commutators in semisimple algebraic groups. Proc. Amer. Math. Soc.* 15 (1964) 457-460.

[45] Rodney, D. M., *Commutators and abelian groups*, J. Austral. Math. Soc. 24 (1977) 79-91.

[46] Rosenberger, G., *Produkte von Potenzen und Kommutatoren in freien Gruppen*, J. Alg.

[47] Rosenberger, G., *Alternierende Produkte in freien Gruppen.* I11. *J. Math.*

[48] Rothaus, O. S., *On the non-triviality of some group extensions given by generators and relations*, Ann. of Math. 106 (1977) 599-612.

[49] Schupp, P. E., *On the substitution problen for free groups*, Proc. Amer. Math. Soc. 23 (1969) 421-423.

[50] Scott, W. R., *Algebraically closed groups*, Proc. Amer. Math. Soc. 2 (1951) 118-121.

[51] Stallings, J. R.

[52] Steinberg, A., *On equations in free groups*, Mich. Math. J. 18 (1971) 87-95.

[53] Taussky-Todd, O., *Problems on matrices and operators*, Bull. Amer. Math. Soc. 76 (1970) 977.

[54] Thompson, R. C., *Commutators in the special and general linear groups*, Trans. Amer. Math. Soc. 101 (1961) 16-33.

[55] Thompson, R. C., *Commutators of matrices with coefficients from the field of two elements*, Duke Math. J. 29 (1962) 367-374.

[56] Thompson, R. C., *On matrix commutators*, *Port. Math.* 21 (1962) 143-153.

[57] Warlimont, R., *Über die Anzahl der Lösungen von* $x^n = 1$ *in der symmetrischer Gruppe* S_n, Archiv der Math. 30 (1978) 591-594.

[58] Wicks, M. J., *Commutators in free products*, J. London Math. Soc. 37 (1962) 433-444.

[59] Wicks, M. J., *A relation in free products*, Proc. Cong. Canberra 1973, Springer Lecture Notes 372 (1974) 709-716.

[60] Zieschang, H., *Über Worte* $S_1^{a_1} S_2^{a_2} \dots S_p^{a_p}$ *in einer freien Gruppen mit p freien Erzeugenden*, Math. Ann. 147 (1962) 143-153.

[61] Brenner, J. L., Some simultaneous equations in matrices, Duke Math J. 39 (1972) 801-805.

[62] Culler, M., Using surfaces to solve equations in free groups, Topology. To appear.

[63] Gallagher, P. X., Group characters and commutators, Math. Z. 79 (1962) 122-126.

[64] Guralnick, R. M., On a result of Schur, J. Algebra 59 (1979) 302-310.

[65] Rosenlicht, M., On a result of Baer, Proc. Amer. Math. Soc. 13 (1962) 99-101.

University of Michigan
Ann Arbor, Michigan 48109
U.S.A.