PACIFIC JOURNAL OF MATHEMATICS
Vol. 41, No. 2, 1972

A GENERAL SOLUTION OF BINARY HOMOGENEOUS EQUATIONS OVER FREE GROUPS

M. J. WICKS

Let $\mathscr{F}$ be the free group generated by *variables* X, Y, $\mathscr{C}$ be any given free group and W, g be elements of $\mathscr{F}, \mathscr{C}$, respectively. Then $x=(x, y)$ is a solution of the binary homogeneous equation $W=g$ if and only if $W(x)=g$, where x, y are elements of $\mathscr{C}$. A general method is obtained which will determine, for arbitrarily given W, g, the solution set of $W=g$. Effectiveness is an essential requirement for the method. It may be noted that the problem can also be regarded as the problem of finding embeddings of $\mathscr{F}$ into $\mathscr{C}$.

The problem of solving an equation splits naturally into two parts: the *existence* problem, to determine whether there are solutions; and secondly, the characterization of the general solution. The existence problem here is solved by showing that the equation has a solution if and only if at least one of a finite set of identities has a solution. The set of identities may be obtained in an effective (and quite practical) way from W, g. In order to solve the second part of the problem, it is necessary to analyse the way in which a solution of an identity generates solutions of the equation. This is elucidated by the introduction of a set of mappings $\Phi(W)$, the members of which are (derived from) the automorphisms of $\mathscr{F}$. The members of $\Phi(W)$ serve as parameters for the general solution. It has not been possible to specify $\Phi(W)$ in an effective way (at least, not according to one interpretation of this requirement), but $\Phi(W)$ is a group, and this fact can be used in applications of the theory.

Two special situations must be mentioned. A solution (x, y) is *abelian* if $xy = yx$. The set of abelian solutions may be determined in a completely elementary way. The second matter concerns the case in which W is the power of a generator of $\mathscr{F}$. In such a case there may be solutions of the equation which involve arbitrary members of $\mathscr{C}$, but not, of course, in an arbitrary way.

The general background material pertaining to free groups will be found in [5], but the terminology and notation found there has been modified. Some references to related problems are also listed at the end. Of these, [6] deserves further comment.

Schupp has solved the existence problem in a most concise way. His approach is different from the one that we have followed; the details are not relevant here, except to note the use of Whitehead's results [7, 8]. The direct analysis of § 9 allows us to avoid these

general, and difficult, procedures.

An earlier version of the present work obtained a solution of the existence problem independently of [6], but in a much more lengthy way. Subsequently, in correspondence, Paul Schupp suggested an alternative style of proof, which greatly simplified the work, and which led, in part, to the present extension. It is a pleasure to express thanks for these suggestions and to acknowledge the debt for the improvements that they made possible. A similar acknowledgement is due to the referee. His suggestions, which will be mentioned at the appropriate places below, have also shortened some of the original proofs.

The analysis which follows is divided into a number of separate stages, and it may help to unify these if we conclude this introduction with a description of the method in general terms. One major difficulty in solving an equation over a free group is that a solution (x, y) will generally be such that $W(x, y)$ is not reduced. (If it is reduced, we have the solution of an *identity*.) The deletions that are needed in order to obtain g have the effect of "changing the shape" of W, and of (x, y). It is an essential requirement, for any method which attempts to replace the equation by an equivalent set of identities, that a record of such changes be available. For this reason, it is more convenient to deal with *(substitution) pairs* of the form $(U, \boldsymbol{x})$, where U is a word in two (or more) variables and $\boldsymbol{x}$ is a couple (or n-tuple) of elements of $\mathscr{C}$. We shall show that the deletions in $U(\boldsymbol{x})$, the *value* of $(U, \boldsymbol{x})$, can be implemented by automorphisms. It is these mappings which contain the record of the deletions.

We deal with matters in a cyclic way. For any automorphism φ, U^{φ} and $\varphi\boldsymbol{x}$ are defined so that the following relation holds: the values of $(U^{\varphi}, \boldsymbol{x})$ and $(U, \varphi\boldsymbol{x})$ are conjugate, and we say in such a case that the pairs are *equivalent*. The relation may also be expressed in another way. Let ψ be the inverse of φ, then the pairs $(U, \boldsymbol{x})$ and $(U^{\varphi}, \psi\boldsymbol{x})$ are equivalent.

The next stage is to choose φ, or ψ, so that the value of the second pair is shorter than the value of the first—so that deletions have indeed been implemented by φ. It was a suggestion of Paul Schupp's that the same effect could be obtained by requiring that $\psi\boldsymbol{x}$ be shorter than $\boldsymbol{x}$, where the *length* of $\boldsymbol{x}$ is the sum of the lengths of its components. This is so and leads to an obvious simplification.

There are rather trivial choices for φ in some cases, corresponding to inner automorphisms. Once these are exhausted, we find that

further choices can be confined to one of a couple of mappings. There are two such couples and the relevant couple is determined by the initial x. We arrive in this way at a reduction procedure for pairs: starting with a given (W, x) a finite number of reductions leads to an equivalent pair (W_1, x_1) to which no reduction applies. It may still be the case that the value of this terminal pair is not a cyclically reduced word. However, with the help of a single additional variable, an equivalent inert pair can be obtained by a single step, where a pair is *inert* if its value is cyclically reduced.

The method whereby the words W_1 can be effectively determined is not easy to summarize. One point can, however, be made. We shall ensure that all components of x_1 are nontrivial reduced words, and more generally, that this is true at every stage of the reduction. It then follows that the value of the terminal pair is at least as long as W_1.

Finally, we can indicate the way in which mappings are used as parameters. In the earlier notation, let $\theta = \varphi\psi$. The essential property of θ is not that it is the identity, but simply that W^θ and W are the same (cyclically). The set of all such θ, which we denote by $\Phi(W)$, is the set of parameters. Then, if it is assumed that ψ has been chosen, φ may be taken as any coset representative of ψ^{-1} modulo the subgroup $\Phi(W)$.

2. **Definitions and Notation.** It should be apparent and must be stressed that it is the combinatorial presentation of a free group, in terms of a specified set of generators, that is the working basis throughout. In addition to $\mathscr{F}$, $\mathscr{C}$, we also require a group which incorporates an ancillary variable. This is the free group $\mathscr{A}$ generated by X, Y, P. Thus $\mathscr{F}$ is considered as a subgroup of $\mathscr{A}$.

The following notation will be used systematically. The symbols U, V denote words of $\mathscr{A}$, while W will always be used for a *c.r. word* (*i.e.* cyclically reduced word) of $\mathscr{F}$. Words of $\mathscr{C}$ are denoted by p, u, v, x, y, and g is always a c.r. word. The symbols i, j, k, m, n are used for integers. (The modification of a symbol by the addition of a numerical subscript, without change of denotation, will be allowed in the usual way.) The length of U (with respect to the variables) is denoted by $\Lambda(U)$, while $\lambda(u)$ will denote the length of u.

The following definitions refer to $\mathscr{A}$; there are obvious generalization to any free group. A word of length 1 is a *letter*, and the symbols A, B always denote letters. (We sometimes refer to 1 as the *trivial letter*.) The inverse of A is A^{-1}. A word of length 2 is a *syllable*; AA is *pure*; AA^{-1} is *trivial*; and BA is the *transpose* of AB. There are obvious extensions to words in general. We say that U is a part (or subword) of V in the usual circumstances.

We make a clear distinction (notationally) between four equivalence relations on the set of words. These are the relations of *identity*, *cyclic identity* (being a cycle of), *equality* and *conjugacy*; they are denoted by $U \equiv V$, $U \cong V$, $U = V$ and $U \sim V$, respectively. The last two are (assumed to be) defined in terms of the elementary transformations of deletion and insertion; and the fundamental relation between deletions, reduced (or c.r.) words, equality and identity is implicitly involved in many of the proofs. The equivalence relations have natural extensions to n-tuples. These are clear in the case of identity and of equality. The extensions in the cyclic cases will be explained below.

A harmless ambiguity will be allowed by the use of phrases such as "*the* c.r. word conjugate to". It is assumed that in any $\boldsymbol{x}$ the components of $\boldsymbol{x}$ are reduced words. In the binary case, we say that $\boldsymbol{x}$ is a *substitution* if and only if $\boldsymbol{x}$ is non-abelian; then, certainly, each component of $\boldsymbol{x}$ is non-trivial. It is in this latter sense that we use substitution to refer to n-tuples in general. Finally, in the pairs $(U, \boldsymbol{x})$ which occur below, it is always the case that U is a c.r. word and $\boldsymbol{x}$ is a substitution.

3. **Some preliminary simplification.** We dispose of the problem of finding abelian solutions of an equation $W = g$. We can find m, n and a word U of the derived group of $\mathscr{F}$ such that $W = X^m Y^n U$. Then $\boldsymbol{x} \equiv (u^i, u^j)$ is an abelian solution if and only if $u^d = g$, where $d = mi + nj$. The extraction of roots does not present any difficulty and, once g is expressed as a power, the determination of the possible u is straightforward. Finally, the parametric specification of i, j is a piece of elementary number theory.

There is no loss of generality in assuming that W, g are reduced words, and indeed, that g is a c.r. word. The same is true of W. To see this, consider an equation $U = g$, where $U \in \mathscr{F}$. There are words V, W, where W is a c.r. word, such that $U \equiv VWV^{-1}$. Let (x, y) be a solution of $W = g$. Put $v = V(x, y)$, $x_1 = v^{-1}xv$, $y_1 = v^{-1}yv$, then $V(x_1, y_1) = v$, and it may be verified that (x_1, y_1) is a solution of $U = g$. The way in which solutions of the latter yield solutions of $W = g$ is clear.

Finally, we consider a consequence of dealing with matters in a cyclic way. This has the effect of replacing the equation by the *conjugation* $W \sim g$. Every solution of the equation is obviously a solution of the conjugation. Conversely, if $\boldsymbol{x}$ is a solution of the conjugation, then $W(\boldsymbol{x}) = ugu^{-1}$, where u can be found effectively, so solutions of the equation can be obtained from solutions of the conjugation.

Something must be said, in conclusion, about these simplifications. The algebraic consequences of the modifications are difficult to express in a general way. Of course, particular cases (of W for example) which may have a special interest, are amenable to more detailed analysis. We do not consider this question further and the remainder of the work will be concerned with solving binary conjugations in c.r. words.

4. **Automorphisms.** A pair of words U, V (which generate $\mathscr{F}$) define an automorphism φ such that $X\varphi = U$, $Y\varphi = V$. We let W^φ (the *image* of W under φ) be the c.r. word conjugate to $W(U, V)$; and for $\boldsymbol{x} \equiv (x, y)$, $\varphi\boldsymbol{x} \equiv (u, v)$, where $u = U(\boldsymbol{x})$ and $v = V(\boldsymbol{x})$. (The definition of φ can then be expressed in the form $\varphi X \equiv (U, V)$, where $X \equiv (X, Y)$.) It is immediate that $(W^\varphi, \boldsymbol{x})$ and $(W, \varphi\boldsymbol{x})$ are equivalent for any W, $\boldsymbol{x}$.

A simplifying feature, which results from using classes of conjugate words, is that if φ is an inner automorphism, then W^φ is a cycle of W. That the procedure can be iterated is well known: for if θ, φ, ψ are such that $\theta = \varphi\psi$, then W^θ is a cycle of $(W^\varphi)^\psi$. The automorphisms also act naturally on the substitutions in the sense that $\theta\boldsymbol{x} = \varphi(\psi\boldsymbol{x})$. However, something further is required if the full advantage is to be gained.

The group of inner automorphisms is a normal subgroup of the group of automorphisms (of $\mathscr{F}$) and we wish to work with *mappings* of the factor group Φ. There is a difficulty. Let φ, ψ be mappings such that $\varphi = \psi$ in Φ. Then it may no longer be true that $\varphi\boldsymbol{x} = \psi\boldsymbol{x}$. What is true is that if $\varphi\boldsymbol{x} \equiv (u, v)$ and $\psi\boldsymbol{x} \equiv (u', v')$, then there is p (a member of the subgroup generated by $\boldsymbol{x}$) such that $u' = pup^{-1}$ and $v' = pvp^{-1}$.

This motivates the extension of the conjugacy relation to $\mathscr{C}^2$. Let $\boldsymbol{x}' \equiv (x', y')$ be such that there is u for which $x' = uxu^{-1}$, $y' = uyu^{-1}$. We denote this by writing $\boldsymbol{x} \sim \boldsymbol{x}'$, or sometimes as $\boldsymbol{x}' = u\boldsymbol{x}u^{-1}$, where $\boldsymbol{x} = (x, y)$. It is clear that $(W, \boldsymbol{x})$ and $(W, \boldsymbol{x}')$ are equivalent for any W.

This extension makes it convenient to introduce some further notation. If $\boldsymbol{x}$, $\boldsymbol{u}$ and $\varphi \in \Phi$ are such that $\boldsymbol{u} \sim \varphi\boldsymbol{x}$, we denote this by writing

$$\varphi\colon \boldsymbol{x} \to \boldsymbol{u} .$$

In such a case, the components of $\boldsymbol{u}$ are in a conjugate of the subgroup generated by $\boldsymbol{x}$. Thus $\boldsymbol{u}$ is abelian if and only if $\boldsymbol{x}$ is abelian.

After these general matters, we come now to consider the particular mappings that are needed below. Three of these, which are of primary importance, are defined by

$$\alpha X \equiv (XY^{-1}, Y); \tau X \equiv (Y, X); \varepsilon X \equiv (X^{-1}, Y) .$$

It is also convenient to denote α^{-1} by β and $\tau\varepsilon\tau$ by η, so that $\beta X \sim (XY, Y)$ and $\eta X \sim (X, Y^{-1})$.

It is well known that $\alpha, \tau, \varepsilon$ generate Φ and it is also known that Φ can be generated by two elements, [2, p. 88]. The same result is contained in

PROPOSITION. $\alpha\tau\beta = \tau\alpha\tau\varepsilon$.

Proof. It is sufficient to make the calculations:

$$\begin{aligned} \alpha\tau\beta X = \alpha\tau(XY, Y) = \alpha(Y, XY) &\equiv (YY^{-1}X^{-1}, XY) \\ &= (X^{-1}, XY) . \\ \tau\alpha\tau\varepsilon X = \tau\alpha\tau(X^{-1}, Y) = \tau\alpha(Y, X^{-1}) &= \tau(YX, X^{-1}) \\ = (X^{-1}, YX) \sim X(X^{-1}, YX)X^{-1} &= (X^{-1}, XY) . \end{aligned}$$

It follows that $\varepsilon = \tau\beta\tau\alpha\tau\beta$, and hence, that α, τ generate Φ. However, our main interest in the Proposition is that it furnishes a solution of the word problem of Φ, and this solution was the inspiration of the reduction procedure. The treatment below was suggested by the referee.

Let Σ_α be the *subsemigroup* of Φ generated by $\alpha, \tau\alpha$; Σ_β the subsemigroup generated by $\beta, \tau\beta$; and Δ the subsemigroup generated by τ, ε. Then we have

For any $\varphi \in \Phi$ there exists $\sigma \in \Sigma_\xi$, $\xi = \alpha$ or β, and $\delta \in \Delta$ such that $\varphi = \sigma\delta$.

Proof. Let φ be a word in $\alpha, \beta, \tau, \varepsilon, \eta$. The relations $\alpha\varepsilon = \varepsilon\beta$, $\alpha\eta = \eta\beta$, $\tau\varepsilon = \eta\tau$ and $\varepsilon^2 = \eta^2 = \tau^2 = 1$ show that there is a word σ in α, β, τ and $\delta \in \Delta$ such that $\varphi = \sigma\delta$. We may assume that σ is freely reduced, so if σ is not of the required form, either $\alpha\tau\beta$ or $\beta\tau\alpha$ is a part of σ. These may be replaced by $\tau\alpha\tau\varepsilon$ or $\varepsilon\tau\beta\tau$, respectively, and the ε (or η) moved rightward, leading to an expression for φ in which the number of occurrences of α and β has been decreased. The proof is completed by induction.

It is also true that $\sigma \in \Sigma_\xi$ can be uniquely factorized as a product of ξ and $\tau\xi$, $\xi = \alpha, \beta$. (Unique factorization in Σ_ξ will always refer to this presentation.) This may be seen as follows:

For any $\sigma \in \Sigma_\beta$ there are positive words U, V such that $\sigma X \sim (U, V)$. Let $\sigma' \in \Sigma_\beta$ and ξ be one of β or $\tau\beta$ such that $\sigma = \xi\sigma'$. There are positive words U', V' such that $\sigma' X \sim (U', V')$. Then, one of U or V is conjugate to $U'V'$ and the other is conjugate to V'. Since the

words are positive, U or V is a cycle of $U'V'$, etc., and whether ξ is β or $\tau\beta$ is uniquely determined by whether U is longer or shorter than V. The proof is completed by induction.

A similar proof can be made for Σ_α by using different classes of homogeneous words (see §9). It is clear that Σ_α and Σ_β have trivial intersection.

5. **The classification of pairs.** The set of all pairs $(U, \boldsymbol{x})$ with $U \in \mathscr{T}$ is subdivided into various categories. This is mainly to facilitate the application of the reduction procedure, but there are some other aspects. The categories parallel, to some extent, the division of Φ by the subsemigroups Σ_ξ. There are three main divisions: the *terminal pairs*, to which no reduction applies; *pairs of type O*, which can be reduced in a trivial way; and *pairs of type A or B* to which reduction applies non-trivially. It is assumed that once a category has been specified, the subsequent definitions refer to the pairs which remain; so the categories are disjoint.

Two kinds of terminal pairs may be specified at once. The first is the class of *abelian pairs*, where $(U, \boldsymbol{x})$ is abelian if $\boldsymbol{x}$ is abelian or U is pure. The second is the class of inert pairs. Any pair which remains is said to be *active*.

Let $(U, \boldsymbol{x})$ be an active pair. Since U is a c.r. word and the components of $\boldsymbol{x}$ are non-trivial reduced words, there must be a syllable S, which is part of a cycle of U, and such that $S(\boldsymbol{x})$ is not reduced. (Note that it is indifferent for the conclusion whether S or S^{-1} is referred to.) Now consider the terminal letters of the components of $\boldsymbol{x}$; let a_i, b_i^{-1} be the initial and final letters, respectively, of the ith component, $i = 1, 2$. (A gloss is needed if one component is a letter, but this is easily supplied.) Since S is non-trivial, at least two of a_1, b_1, a_2, b_2 are identical.

Suppose at least three of the letters are identical—to the letter a say—then the substitution $\boldsymbol{x}'$, such that $\boldsymbol{x}' = a^{-1}\boldsymbol{x}a$, is shorter than $\boldsymbol{x}$ and is such that $(U, \boldsymbol{x})$ and $(U, \boldsymbol{x}')$ are equivalent. A pair of this kind is of type O. A sequence of conjugations, which may be regarded as trivial reductions, will yield an equivalent pair, with a shorter substitution, which is not of type O.

Let $(U, \boldsymbol{x})$ be active and not of type O. If one of the components of $\boldsymbol{x}$ is not a c.r. word, then (in the notation above) either $a_1 \equiv b_1$, or $a_2 \equiv b_2$, and if both be true, a_1 and a_2 are different. The pair is terminal of type OT. There must be words u, v and non-trivial c.r. words x, y such that $\boldsymbol{x}$ is (uxu^{-1}, vyv^{-1}), and $p \equiv v^{-1}u$ is a non-trivial reduced word. An equivalent inert pair is obtained as follows.

Let $\boldsymbol{A} \equiv (X, Y, P)$ and γ be the automorphism of $\mathscr{A}$ such that $\gamma\boldsymbol{A} \equiv (PXP^{-1}, Y, P)$. The equivalent pair is $(U^\gamma, \boldsymbol{x}_0)$, where $\boldsymbol{x}_0 \equiv (x, y, p)$.

The conditions on u, v, x, y ensure that the pair is inert and that $\boldsymbol{x}_0$ is a substitution.

The active pairs which remain are such that the substitution is a *c.r. substitution, i.e.* each component is a c.r. word. Let $(U, \boldsymbol{x})$ be such a pair. Then there is S, one of XY or XY^{-1}, such that $(S, \boldsymbol{x})$ is active. There is a connection between S and U.

We say that S *occurs* in U if S or S^{-1} is part of a cycle of U. It will be shown in §9 that XY occurs in a c.r. word if and only if YX occurs; and similarly for XY^{-1}, $Y^{-1}X$. Thus the relation between S and U in the case above is that S occurs in U.

Let S be XY^{-1}. Then either the initial letters of the components of $\boldsymbol{x}$ are identical, or the final letters are. Let u be the longest word which is an initial part of each component of $\boldsymbol{x}$. It may happen that one component is u, but both cannot be else $\boldsymbol{x}$ is abelian. Also, u may be trivial. If neither component is u, consider the words obtained by removing the initial part u from the components of $\boldsymbol{x}$. Let v^{-1} be the longest word which is the final part of each truncated component. It may again happen that one of these components is v^{-1}, but both cannot be. Further, v^{-1} may be trivial, but $v^{-1}u$ is a non-trivial reduced word. There are two cases.

The first is that one component of $\boldsymbol{x}$ is uv^{-1} and the other is uxv^{-1}. Then $(U, \boldsymbol{x})$ is a pair of type B. It is not assumed that u, v are necessarily obtained in the way just described, so the factorization may not be uniquely determined by $\boldsymbol{x}$.

In the second case, $\boldsymbol{x}$ has the form (uxv^{-1}, uyv^{-1}), where x, y and $p \equiv v^{-1}u$ are non-trivial words such that px, xy^{-1} and py are c.r. words. Then $(U, \boldsymbol{x})$ is a terminal pair of type BT. The equivalent inert pair is again obtained with the help of an automorphism ν of $\mathscr{A}$ defined by $\nu A \equiv (PX, PY, P)$. The pair is $(U^{\nu}, \boldsymbol{x}_0)$, where $\boldsymbol{x}_0 \equiv (x, y, p)$. That the pair is inert follows from Lemma 4 in §9.

The last case is that of a pair $(U, \boldsymbol{x})$ which is active, $\boldsymbol{x}$ is a c.r. substitution, XY occurs in U and $(XY, \boldsymbol{x})$ is active. Then the equivalent pair $(U^{\eta}, \eta\boldsymbol{x})$ is either of type B or BT. The pair $(U, \boldsymbol{x})$ is of type A if one component of $\boldsymbol{x}$ has the form uxv^{-1} and the other is vu^{-1}.

The pair is terminal of type AT if $\boldsymbol{x} \equiv (uxv^{-1}, vyu^{-1})$, where x, y and $p \equiv u^{-1}v$ are non-trivial words such that xp^{-1}, xy and py are c.r. words. Let μ be the automorphism of $\mathscr{A}$ defined by $\mu A \equiv (XP^{-1}, PY, P)$. Then $(U^{\mu}, \boldsymbol{x}_0)$ is the inert equivalent pair, where $\boldsymbol{x}_0 = (x, y, p)$.

The further analysis could be confined to pairs of a single type. However, there are formal advantages in being able to deal with either case and this we shall do. Results for one type can be transferred to the other by using η and we shall usually assume this without explicit mention.

6. **The reduction procedure.** We begin with a procedure for reduction of substitutions. The terminology for pairs carries over to substitutions in an obvious way.

Let $\boldsymbol{x}$ be a substitution of type A for which, in the earlier notation, one component is uxv^{-1} and the other is vu^{-1}. Reduction produces a substitution $\boldsymbol{x}'$ and a mapping ξ. If the first component is longer, $\xi = \alpha$, while in the contrary case, $\xi = \tau\alpha$. In either case, $\boldsymbol{x}' \equiv (x, u^{-1}v)$. It is immediately evident that $\boldsymbol{x}'$ is shorter than $\boldsymbol{x}$ and that

$$\xi\colon \boldsymbol{x}' \to \boldsymbol{x} .$$

Certainly, $\boldsymbol{x}'$ is not abelian. Moreover, if the initial letters of x and $u^{-1}v$ were identical, or the final letters were, then the component uxv^{-1} of $\boldsymbol{x}$ would not be a c.r. word. Hence, $\boldsymbol{x}'$ cannot be of type O, B or BT and we have proved:

THEOREM 1. *If $\boldsymbol{x}$ is obtained by reduction of a substitution of type A, then $\boldsymbol{x}$ is either of type A, or it is terminal and inert, or of type OT or AT.*

It may be noted that the second component is a c.r. word so that $Y^2(\boldsymbol{x})$ is a reduced word.

Reduction of a substitution of type B yields one of the mappings β or $\tau\beta$, and the substitution $(x, v^{-1}u)$, where it is assumed that the components of the original substitution are uxv^{-1} and uv^{-1}.

Suppose a substitution of type B can be factorized as $(u_i x_i v_i^{-1}, u_i v_i^{-1})$, $i = 1, 2$. The substitution obtained by reduction will be $(x_i, v_i^{-1}u_i)$, $i = 1, 2$. It is clear that if $\lambda(u_1) = \lambda(u_2)$, then the factorizations are identical. If this is not so, we may assume by symmetry that $\lambda(u_1) < \lambda(u_2)$.

The identities

$$u_1 x_1 v_1^{-1} \equiv u_2 x_2 v_2^{-1} \text{ and } u_1 v_1^{-1} \equiv u_2 v_2^{-1}$$

imply, in the first place, that there is w such that $u_1 w \equiv u_2$. It follows that $v_1^{-1} \equiv w v_2^{-1}$, and then that $x_1 w \equiv w x_2$. We then have, for the substitutions obtained by reduction, that

$$\begin{aligned} w^{-1}(x_1, v_1^{-1}u_1)w &\equiv (w^{-1}x_1 w, w^{-1}v_1^{-1}u_1 w) \\ &\equiv (w^{-1}w x_2, w^{-1}w v_2^{-1}u_2) \\ &= (x_2, v_2^{-1}u_2) . \end{aligned}$$

Thus the substitutions obtained by reduction satisfy the condition: *they are conjugate and corresponding components are of the same length.* For any pair of c.r. substitutions $\boldsymbol{x}_1$, $\boldsymbol{x}_2$ which satisfy this condition we write $\boldsymbol{x}_1 \cong \boldsymbol{x}_2$. This is clearly an equivalence relation.

The relation can be characterized in another way. Suppose first that there is a letter a such that $\boldsymbol{x}_2 = a^{-1}\boldsymbol{x}_1 a$. Then it can be shown by induction that, in the general case, $\boldsymbol{x}_1$ can be taken into $\boldsymbol{x}_2$ by a finite number of such conjugations by a single letter. It follows in particular that the substitutions are of the same type.

Let $\boldsymbol{x}_1, \boldsymbol{x}_2$ be substitutions of type B such that $\boldsymbol{x}_1 \cong \boldsymbol{x}_2$, and let $\boldsymbol{x}_i'$ be obtained by reduction, $i = 1, 2$. We wish to show that $\boldsymbol{x}_1' \cong \boldsymbol{x}_2'$. It follows from the remarks above that it is enough to consider the case $\boldsymbol{x}_1 \equiv (auxv^{-1}, auv^{-1})$ and $\boldsymbol{x}_2 \equiv (uxv^{-1}a, uv^{-1}a)$. The substitution obtained in each case is $(x, v^{-1}au)$ and the result follows. Thus the reduction procedure is unique in this cyclic sense.

Let $\boldsymbol{x}_0$ be a given substitution of type B. Since reduction is length decreasing, there is a finite sequence of reductions which, starting with $\boldsymbol{x}_0$, terminates with a substitution $\boldsymbol{x}_k$ which is either inert or of type BT or OT. If $\boldsymbol{x}_i$ is the substitution obtained by the ith reduction, then $\boldsymbol{x}_i$ is of type B, $1 \leqq i < k$. Further, let ξ_i be the mapping obtained from the ith reduction, then with $\sigma_0 = 1$, $\sigma_i = \sigma_{i-1}\xi_i$, $1 \leqq i \leqq k$, it follows that $\sigma_i \in \Sigma_\beta$ and

$$\sigma_i \colon \boldsymbol{x}_i \rightarrow \boldsymbol{x}_0 .$$

We conclude by carrying over the results to pairs. Let $(W, \boldsymbol{x})$ be a given active pair. Then there is $\boldsymbol{x}_0$, which is not longer than $\boldsymbol{x}$ and either terminal or of type A or B, such that $(W, \boldsymbol{x})$ and $(W, \boldsymbol{x}_0)$ are equivalent. Let $\boldsymbol{x}_i$ and σ_i be obtained as above, and let W_i be the image of W under σ_i, $i = 1, \cdots, k$. The pairs $(W_i, \boldsymbol{x}_i)$ are all equivalent, and since $(W_k, \boldsymbol{x}_k)$ is terminal, there is a least m, $0 \leqq m \leqq k$, such that $(W_m, \boldsymbol{x}_m)$ is terminal. Then the pairs $(W_i, \boldsymbol{x}_i)$, $i = 0, \cdots, m-1$, are all of type A or all of type B.

7. **The fundamental theorem.** The results of the preceding sections may be formulated in terms of conjugations. Let W, g be given fixed words, W not a pure word. Then we have

THEOREM 2. *For any non-abelian solution $\boldsymbol{x}$ of $W \sim g$ there is $\sigma \in \Sigma_\xi$, $\xi = \alpha$ or β, and a substitution $\boldsymbol{x}_1$ such that*

(i) *$\boldsymbol{x}_1$ is a solution of $W^\sigma \sim g$;*

(ii) *the pair $(W^\sigma, \boldsymbol{x}_1)$ is terminal;*

(iii) $\sigma \colon \boldsymbol{x}_1 \rightarrow \boldsymbol{x}$.

A more detailed, and definitive, result can be obtained by considering the nature of the terminal pair. This is straightforward except, perhaps, in the abelian case. It cannot be that $\boldsymbol{x}_1$ is abelian, so W^σ must be pure. Further, since $Y^\alpha = Y^\beta = Y$, we may take it that W^σ is a power of X. Then if $\boldsymbol{x}_1 \equiv (x, y)$, y may be arbitrary, so we may assume that x is a solution of $W^\sigma \cong g$.

THEOREM 3. *For any non-abelian solution* $\boldsymbol{x}$ *of* $W \sim g$ *there are mappings* σ, ψ *and a substitution* $\boldsymbol{x}_0$ *such that*

$$\sigma\colon \psi\boldsymbol{x}_0 \to \boldsymbol{x} ,$$

and σ, ψ, $\boldsymbol{x}_0$ *satisfy either*

(I) $\psi = 1$, $\sigma \in \Sigma_\xi$, $\xi = \alpha$ *or* β, $W^\sigma \cong X^m$, $\boldsymbol{x}_0 \equiv (x, u)$, *where* $x^m \cong g$ *and* u *is an arbitrary (non-trivial) member of* $\mathscr{C}$.

(II) *Let* U_0 *be the image of* W *under* $\sigma\psi$. *Then* $\boldsymbol{x}_0$ *is a solution of the identity*

$$U_0 \cong g$$

and one of the following holds:

(a) $\psi = 1$;

(b) $\psi = \gamma$; *if* $\sigma = 1$, *either* X^2 *or* Y^2 *occurs in* W, *while if* $\sigma \neq 1$, X^2 *occurs in* W^σ;

(c) $\psi = \mu$; $\sigma \in \Sigma_\alpha$ *and* XY *occurs in* W^σ;

(d) $\psi = \nu$; $\sigma \in \Sigma_\beta$ *and* XY^{-1} *occurs* in W^σ.

The converse is obvious. The Theorem needs further modification before an effective method can be obtained.

8. **The parameters.** We recall that $\Phi(W)$ is the subgroup of Φ consisting of all the mappings φ for which W^φ is a cycle of W. Thus, if σ, σ' are in the same (left) coset of $\Phi(W)$ (so that $\sigma' = \varphi\sigma$ for some $\varphi \in \Phi(W)$) then the images of W under σ, σ' are the same. Moreover, for any substitution $\boldsymbol{x}$, $\sigma'\boldsymbol{x} \sim \varphi(\sigma\boldsymbol{x})$. We now define an (irreducible) set of representatives for Σ_ξ modulo $\Phi(W)$, which we denote by $\Sigma_\xi(W)$, $\xi = \alpha, \beta$.

Some preparation is necessary. Uniqueness of factorization allows Σ_ξ to be ordered lexicographically as a sequence (assuming, for example, that α is *before* $\tau\alpha$). The fact that σ is *before* σ' is denoted by writing $\sigma < \sigma'$.

There is also a partial order of Σ_ξ which is useful. We say that σ *precedes* σ' if σ is a proper factor of σ'. The set $\Sigma_\xi(W)$ is defined so that if σ is a member, then it is immediately evident that all the predecessors of σ are also members. The representative property will be established as a theorem.

The definition of $\Sigma_\xi(W)$ is inductive, and at the kth stage two subsequences of Σ_ξ will be obtained, denoted by $\Sigma_{\xi k}$ and Σ_ξ^k, respectively (where reference to W has been omitted). For $k = 1$, the first subsequence is 1, while the second is the rest of Σ_ξ.

Suppose, for $k \geqq 1$, that $\Sigma_{\xi k}$ is $\sigma_0 = 1, \sigma_1, \cdots, \sigma_m$. If Σ_ξ^k is empty, then $\Sigma_{\xi n} = \Sigma_{\xi k}$ and Σ_ξ^n is empty for all $n \geqq k$.

Otherwise, let σ be the first member of Σ_ξ^k, U be the image of W under σ, and W_i the image of W under σ_i, $i = 0, 1, \cdots, m$. If there is an i, $0 \leqq i \leqq m$, such that $U \cong W_i$, then $\sigma\sigma'$ is removed from Σ_ξ^k for every σ' in Σ_ξ(*i.e.* σ and all its successors are removed). The resulting sequence is Σ_ξ^{k+1}, while $\Sigma_{\xi k+1}$ is $\Sigma_{\xi k}$. In the contrary case, when there is no such i, only σ is removed from Σ_ξ^k; then σ is added to $\Sigma_{\xi k}$ (as last member) to obtain $\Sigma_{\xi k+1}$.

The limit of $\Sigma_{\xi k}$ is $\Sigma_\xi(W)$.

We now show that if $\sigma \in \Sigma_\xi$ and $\sigma \notin \Sigma_\xi(W)$, then there is $\sigma' \in \Sigma_\xi$, $\varphi \in \Phi(W)$ such that $\sigma' < \sigma$ and $\sigma = \varphi\sigma'$.

Let σ be as stated. Then there is a greatest k such that $\sigma \in \Sigma_\xi^k$ (and from which it is removed). If σ_2 is the first member of Σ_ξ^k, let σ_1, σ_3 be such that $\sigma_1 \in \Sigma_{\xi k}$, $\sigma_3 \in \Sigma_\xi$, $\sigma = \sigma_2\sigma_3$ and $\varphi\sigma_1 = \sigma_2$ for some $\varphi \in \Phi(W)$. Since $\sigma_1 < \sigma_2$, it is clear that $\sigma' = \sigma_1\sigma_3$ has the required property.

THEOREM 4. *For any $\sigma \in \Sigma_\xi$, $\xi = \alpha, \beta$, there is $\sigma' \in \Sigma_\xi(W)$ and $\varphi \in \Phi(W)$ such that $\sigma = \varphi\sigma'$; σ' is unique.*

Proof. The result proved above assures the existence of the *first* $\sigma' \in \Sigma_\xi$ such that $\sigma = \varphi\sigma'$ for some $\varphi \in \Phi(W)$. It then follows that $\sigma' \in \Sigma_\xi(W)$ and that it is unique.

The parametric role of $\Phi(W)$ is shown by

THEOREM 5. *The conclusion of Theorem* 3 *may be modified by replacing σ by $\varphi\sigma$, where $\sigma \in \Sigma_\xi(W)$ and $\varphi \in \Phi(W)$. Further, if $\boldsymbol{x}_1 = \sigma(\psi\boldsymbol{x}_0)$, then*

$$\varphi\colon \boldsymbol{x}_1 \to \boldsymbol{x}\ .$$

9. Combinatorial properties of mappings. There is a connection between the partial order of Σ_ξ introduced in the previous section and the ordering by length of the set of words W^σ, $\sigma \in \Sigma_\xi$. Let $\sigma \in \Sigma_\xi$ and be of length k; the $k+1$ mappings $\sigma_0, \sigma_1, \cdots, \sigma_k$ such that $\sigma_0 = 1$, $\sigma_k = \sigma$ and σ_i precedes σ_{i+1}, $0 \leqq i < k$, constitute the *branch* of Σ_ξ to σ. The branch is uniquely determined by σ, and if $\sigma \in \Sigma_\xi(W)$, then so does every other member of the branch. The aim of the present section is to prove

THEOREM 6. *Let $\sigma_1, \sigma_2, \sigma_3$ be three successive members of a branch of Σ_ξ, and let W_i be the image of W under σ_i, $1 \leqq i \leqq 3$.*

Then $\Lambda(W_1) < \Lambda(W_2)$ implies $\Lambda(W_2) < \Lambda(W_3)$.

The present proof was suggested by the referee. It is reminiscent

of [3], but was obtained originally in ignorance of that work. Some further definitions and notation are required.

Since W is fixed, the lengths of W, W^σ will be denoted by Λ, Λ^σ, respectively. In addition, we make use of some refinements of the length function; for example, the number of occurrences of X in W, which is denoted by Λ_x. Note then that Λ_x^σ has an unambiguous interpretation in an obvious sense. Another modification is made for ease of printing. For example, the number of occurrences of X^{-1} (which is, of course, equal to Λ_x) will be denoted by $\Lambda_{\bar{x}}$. The extension of this notation to other letters—and to words—is clear.

The definition of Λ_s for a syllable S will illustrate the general case. Suppose $\Lambda = m$, $m \geqq 2$, and $W \equiv A_1 \cdots A_m$. The syllable parts of W are A_1A_2, A_2A_3, $\cdots$, A_mA_1. Then Λ_s is the number of these which are occurrences of S.

There are some obvious properties, *e.g.* $\Lambda = \Lambda_x + \Lambda_y$, and $\Lambda_u = \Lambda_{\bar{u}}$ for any U. For others, we introduce the notion of a *homogeneous* word: a positive word is one example, and in general, U is *homogeneous* if there is $\delta \in \Delta$ for which U^δ is positive. Positive and negative words will be denoted by the symbols Q and R, respectively. Any c.r. word W can be factorised as a product of (non-trivial) positive and negative factors. Before dealing with this in a general way, it is instructive to consider first a c.r. word of the form QR, where Q and R are both non-trivial. We let $Q \equiv Q_0A$, $R \equiv BR_0$; then, since QR is reduced, AB is an occurrence of XY^{-1}. Thus, if W is a c.r. word for which $\Lambda_{x\bar{y}} > 0$, then there is $k \geqq 1$ and words Q_i, R_i (possibly trivial) such that

$$W \cong Q_1S_1R_1 \cdots Q_kS_kR_k ,$$

where each S_i is an occurrence of XY^{-1}. It is clear that $\Lambda_{x\bar{y}} = k$. Further, by considering parts of the form RQ, it follows that $\Lambda_{\bar{y}x} = k$. We have

LEMMA 1. (a) $\Lambda_{x\bar{y}} = \Lambda_{\bar{y}x}$; (b) $\Lambda_{xy} = \Lambda_{yx}$.

The proof of the following, which is elementary, will be omitted.

LEMMA 2. (a) $\Lambda_x = \Lambda_{xx} + \Lambda_{xy} + \Lambda_{x\bar{y}}$;
(b) $\Lambda_s \geqq \Lambda_{as}$, *for any* A, S.

We now consider Λ^β. It is clear that if $\Lambda_{x\bar{y}} = 0$, then $W^\beta \cong W(XY, Y)$, since the latter is a c.r. word.

Suppose now that $\Lambda_{x\bar{y}} > 0$. We use the notation above and let $U_i \equiv Q_iS_iR_i$. Let $Q_i' \equiv Q_i(XY, Y)$, so that Q_i' is certainly reduced. Further, if Q_i is not empty, the initial letters of Q_i and Q_i' are identical,

while the final letter of Q_i' is Y. In a similar way, it follows that if R_i is nonempty, then the initial letter of R_i' is Y^{-1}, while the final letters of R_i and R_i' are identical, where $R_i' \equiv R_i(XY, Y)$. If $S_i \equiv AB$, then $S_i(XY, Y) = X^e$, where $e = 1$ if A is X and $e = -1$ if A is Y. Hence $U_i(XY, Y) = Q_i'X^eR_i'$ and it is clear that the latter word is non-trivial and reduced. Let W' be the product of these words (in the obvious order) so that $W(XY, Y)$ is conjugate to W'. To show that W' is a c.r. word it suffices to show that products of pairs of successive words are all reduced. Moreover, since any (appropriate) cycle of W may be taken, it is enough to show that $Q_1'X^{e_1}R_1'Q_2'X^{e_2}R_2'$ is reduced.

This follows immediately from the remarks above if R_1 and Q_2 are both non-trivial. If $R_1 \equiv 1$, consider $X^{e_1}Q_2'$. If $S_1 \equiv XY^{-1}$, then $e_1 = 1$ and the initial letter of Q_2, and of Q_2' also, is X. In the other alternative, the initial letter of Q_2' is easily seen to be Y. The case where $Q_2 \equiv 1$ is similar. Finally, if R_1 and Q_2 are both 1, then $S_1 \equiv S_2$ and $e_1 = e_2$.

It follows that W' is a c.r. word and thus is a cycle of W^β. We note that k deletions of the syllable YY^{-1} have been made in order to obtain W' from $W(XY, Y)$, and so we have proved the crucial

LEMMA 3. (a) $\Lambda_x^\beta = \Lambda_x$; (b) $\Lambda_y^\beta = \Lambda - 2\Lambda_{x\bar{y}}$;
(c) $\Lambda_{x\bar{y}}^\beta = \Lambda_{x\bar{y}\bar{y}} \leqq \Lambda_{x\bar{y}}$.

We digress for a moment to state

LEMMA 4. *The only syllables which can occur in W^ν are PX, XY^{-1}, PY and the transposes of these.*

Proof. The result is evident by considering the part in $W(PX, PY)$ corresponding to the part QR in W.

The first three lemmas combine to give

Proof of Theorem 6. In the first place, let $\xi = \beta$, replace W_1 by W and suppose $W_2 \equiv W^\beta$. By Lemmas 1, 3

$$\Lambda^\beta - \Lambda = \Lambda_x^\beta + \Lambda - 2\Lambda_{x\bar{y}} - \Lambda = \Lambda_x - 2\Lambda_{x\bar{y}} ,$$

so the hypothesis is equivalent to

$$\Lambda_x - 2\Lambda_{x\bar{y}} > 0 .$$

For the case that $W_3 \equiv W_2^\beta$ we have

$$\Lambda^{\beta\beta} - \Lambda^\beta = \Lambda_x^\beta - 2\Lambda_{x\bar{y}}^\beta \geqq \Lambda_x - 2\Lambda_{x\bar{y}} > 0 .$$

For the case $W_3 \equiv W_2^{\tau\beta}$ we have

$$\begin{aligned}
\Lambda^{\beta\tau\beta} - \Lambda^{\beta} &= \Lambda^{\beta\tau\beta} - \Lambda^{\beta\tau} \\
&= \Lambda_x^{\beta\tau} - 2\Lambda_{x\bar{y}}^{\beta\bar{\tau}} \\
&= \Lambda_y^{\beta} - 2\Lambda_{yx}^{\beta\bar{\tau}} \\
&= \Lambda - 2\Lambda_{x\bar{y}} - 2\Lambda_{x\bar{y}}^{\beta\bar{\tau}} \\
&> \Lambda_y - 2\Lambda_{x\bar{y}}^{\beta\bar{\tau}} \\
&= \Lambda_{yy} + \Lambda_{yx} + \Lambda_{y\bar{x}} - 2\Lambda_{x\bar{y}}^{\beta\bar{\tau}} \\
&\geqq \Lambda_{yy} + \Lambda_{x\bar{y}} - 2\Lambda_{x\bar{y}\bar{y}} \geqq 0 .
\end{aligned}$$

The cases in which $W_2 \equiv W^{\tau\beta}$ follow on replacing W by W^{τ}. Finally, for $\xi = \alpha$, W is replaced by W^{η}.

10. The cyclic identities. We construct now the method which allows Theorems 3, 5 to be implemented in an effective way.

We dispose first of case (I) and assume that there is $\sigma \in \Sigma_\xi$ such that W^σ is a power of X, X^m say. Then there is a word W_0 such that $W \cong W_0^m$ and $W_0^\sigma \equiv X$. Conversely, W_0 must be the image of a letter under a mapping of Σ_ξ. It is clearly sufficient to consider mappings whose length does not exceed $\Lambda(W_0)$. (It may be noted that this case will only arise if W is in a cyclic free factor of $\mathscr{F}$.)

Consider now the identities under case (II). Since $\boldsymbol{x}_0$ is a substitution, $\Lambda(U_0) \leqq \lambda(g)$; moreover, U_0 is not shorter than the W^σ from which it is obtained. It is sufficient to consider the set of words W^σ with $\sigma \in \Sigma_\xi(W)$, which set we denote by $\mathscr{S}_\xi$.

The members of $\mathscr{S}_\xi$ are all distinct (even cyclically) so that the partial order on $\Sigma_\xi(W)$ induces a corresponding ordering of $\mathscr{S}_\xi$. We let the *kth level* of $\mathscr{S}_\xi$ consist of the final words from all the branches of length k. Let U be a word in the $(k+1)$st level and $W_0 \equiv W$, $W_1, \cdots, W_k \equiv U$ be the branch to U.

If M is the number of all words whose length does not exceed that of W, then $\log M \leqq 5 \log \Lambda(W)$. Thus, if $k > M$, there is i such that $\Lambda(W_i) < \Lambda(W_{i+1})$, $0 \leqq i < k$. It follows by Theorem 6 that

$$\Lambda(W_j) < \Lambda(W_{j+1}),\ i \leqq j \leqq k .$$

Finally, if $k > M + \lambda(g)$, then $\Lambda(W_k) > \lambda(g)$. Therefore, the subset of $\mathscr{S}_\xi$, of those words U such that U is not longer than g, is a subset of the first $M + \lambda(g)$ levels of $\mathscr{S}_\xi$.

Some further economy is possible in the set of words that need be considered. For example, if W^σ, $\sigma \in \Sigma_\alpha(W)$, is the word of a terminal pair, then XY must occur in the predecessor of W^σ. A rather minor point concerns the exceptional case, Theorem 3, (I).

Suppose $\sigma\xi$ is such that $W^{\sigma\xi} \cong X^m$ and $\sigma \in \Sigma_\alpha(W)$. Then Theorem

2 shows that it is necessary to provide for solutions of the form (uxv^{-1}, vyu^{-1}) of $W^{\sigma} \sim g$. All such solutions can be obtained, by conjugation, from (xv^{-1}, vy), where $(xy)^m \cong g$ and v is arbitrary. This solution in turn is obtained as $\alpha(xy, vy)$, where (xy, vy) is a solution of $X^m \cong g$. Finally, this last solution is already obtained under case (I). It should also be noted that no successor of a power of X occurs as the word of a terminal pair obtained by non-trivial reduction.

We are in a position now to define the enumeration of a set of words $\mathscr{S}(W, g)$ which clearly satisfies

THEOREM 7. *Every word U_0 of Theorem* 3, (II), *is a member of $\mathscr{S}(W, g)$. Moreover, the enumeration is such as to determine the mappings $\sigma \in \Sigma_{\xi}(W)$, $\psi \in \{1, \gamma, \mu, \nu\}$ for which $U_0 \cong W^{\sigma\psi}$.*

The enumeration is by levels.

The first level consists of W, and W^{ψ} if it is not longer than g subject to: a square occurs in W, then $\psi = \gamma$; XY occurs in W, then $\psi = \mu$; XY^{-1} occurs in W, then $\psi = \nu$.

Now suppose that U is a member of $\mathscr{S}_{\alpha}$ which has already been taken into $\mathscr{S}(W, g)$. Then, if XY occurs in U, U contributes the following: U^{ξ}, $\xi = \alpha, \tau\alpha$, provided U^{ξ} is not a power of XY and is a member of $\mathscr{S}_{\alpha}$, and further, either $\Lambda(U^{\xi}) \leqq \Lambda(U)$ or $\Lambda(U) < \Lambda(U^{\xi}) \leqq \lambda(g)$. Further, if U^{ξ} is taken in, so is $U^{\xi\psi}$ if it is not longer than g and $\psi = \gamma$ if X^2 occurs in U^{ξ}; $\psi = \mu$ if XY occurs in U^{ξ}.

The words which $\mathscr{S}_{\beta}$ contributes to $\mathscr{S}(W, g)$ are obtained in a similar way.

11. **The subgroup $\Phi(W)$.** The problem of specifying the subgroup $\Phi(W)$ may be taken in the form: *to determine, for arbitrarily given W, a presentation of $\Phi(W)$ in a finite number of steps.* We have not solved this problem. However, there are some facts about the parametric subgroups which are worth recording.

The first thing to note is that if W is a proper power, of W_0 say, then $\Phi(W)$ and $\Phi(W_0)$ are the same. Another observation of the same kind is that if W is the image of W_1 under some $\varphi \in \Phi$, then $\Phi(W)$ is the conjugate subgroup $\varphi^{-1}\Phi(W_1)\varphi$. It may be advantageous to work with a W_1 of minimal length.

One approach to the problem of finding a presentation of $\Phi(W)$ might be to find an irreducible transversal in Φ. It is easily verified that the $\Sigma_{\xi}(W)$ provide such a transversal for a double coset decomposition of Φ with respect to the pair $\Phi(W)$, Δ. Coset representatives for Φ can be obtained in a straightforward way.

It had been conjectured earlier that $\Phi(W)$ is finitely generated. This is confirmed by Professor Lyndon (private communication) who

supplied the reference [10]. He was also able to indicate a proof of the following: *$\Phi(W)$ is of finite index only if W is a power of a commutator of a pair of generators of $\mathfrak{F}$.*

The following question was raised (privately) in connection with [9]: *if it is known that g is a commutator, in how many ways can g be so expressed?* The subgroup $\Phi(W)$ can provide some information in this case. It is easily shown that if $W \equiv XYX^{-1}Y^{-1}$, then $\Phi(W)$ is of index 2 in Φ; 1 and τ are a pair of coset representatives and $\Phi(W)$ is the subgroup of all elements whose τ-length is even. Thus, modulo the solution of the fundamental identities, $\Phi(W)$ provides a straightforward way of generating solutions—of the conjugation $W \sim g$. It may be possible in this way to give an explicit description of the solution set for a given g; however, to deal with the problem in a general way would seem to present considerable difficulty.

We mention one conclusive application. If $W \equiv X^2Y^2$, then $\mathscr{S}(W, g)$ has at most 6 elements for any g. It can then be shown that if g is a square, $g \equiv h^2$ say, the solutions of $U_0 \cong h^2$, $U_0 \in \mathscr{S}(W, h^2)$, lead solely to abelian solutions of $W \sim h^2$. In the notation of Theorem 5, every possible $\boldsymbol{x}_1$ is abelian, and hence, all solutions of the form $\varphi\boldsymbol{x}_1$ are likewise abelian. This provides yet another confirmation of Vaught's conjecture [4]. It would be of interest to know other examples, of W, for which $\mathscr{S}(W, g)$ is "bounded", and whether this fact has any further (algebraic) significance.

There are further problems connected with the subgroups. The subgroup structure of Φ is known to be complicated. Hence, the question: *which subgroups of Φ may appear as $\Phi(W)$ for a suitable W?* may be of interest. However, it seems to be a difficult problem even to determine, for a given $\varphi \in \Phi$, whether there exists W such that W^φ is a cycle of W. One last question is suggested by the commutator example. What conditions on W ensure that $\Phi(W)$ is a normal subgroup, and what further significance, if any, is there to this fact?

12. Further problems. There are two more general problems which immediately arise out of the present work. The problem of solving an inhomogeneous binary equation, and that of solving a system of binary equations.

Consider the inhomogeneous equation

$$W_1g_1W_2g_2 \cdots W_mg_m = 1 ,$$

where $m \geqq 2$, $W_i \in \mathfrak{F}$, $g_i \in \mathfrak{C}$, $i = 1, \cdots, m$. This is equivalent to a system of homogeneous equations. One such system can be obtained by introducing additional variables $Z_1, \cdots, Z_{m-1}$ and letting

$$W_i g_i Z_i = Z_{i-1},\ i = 1, \cdots, m\ ,$$

where, for notational convenience, $Z_0 \equiv Z_m \equiv 1$.

We can say something more substantial about systems of binary homogeneous conjugations. Suppose $\boldsymbol{x}$ is a solution of

$$W_i \sim g_i,\ i = 1, 2\ .$$

Then there will be solutions $\boldsymbol{x}_i$ of a pair of associated identities, $i = 1, 2$. If the $\boldsymbol{x}_i$ are derived from terminal substitutions, then by the uniqueness of the reduction procedure, $\psi\boldsymbol{x}_1 \cong \psi\boldsymbol{x}_2$. If the $\boldsymbol{x}_i$ are not terminal substitutions, then a further sequence of reductions will determine terminal substitutions $\boldsymbol{x}_i'$ and mappings σ_i' such that

$$\sigma_i' \colon \boldsymbol{x}_i' \to \boldsymbol{x}_i,\ i = 1, 2\ .$$

It follows that $\boldsymbol{x}_1' \cong \boldsymbol{x}_2'$ is a necessary condition in this case. If $\sigma_i \in \Sigma_\xi(W_i)$, $\varphi_i \in \Phi(W_i)$ are such that

$$\varphi_i\sigma_i \colon \boldsymbol{x}_i \to \boldsymbol{x},\ i = 1, 2\ ,$$

then the σ_i and $\boldsymbol{x}_i$ can be determined and it remains to find the φ_i. The reduction of $\boldsymbol{x}$ to $\psi\boldsymbol{x}_i$ or $\boldsymbol{x}_i'$ determines a unique σ, so the condition on φ_i is

$$\varphi_1\sigma_1\sigma_1' = \sigma = \varphi_2\sigma_2\sigma_2'\ .$$

This condition requires the solution of a generalized word problem of the $\Phi(W_i)$.

Another generalization of the present problem is to the problem of solving equations in many variables. The formulation of a reduction procedure would not appear to offer much difficulty. However, the degenerate cases, corresponding to the abelian pairs above, would be of far greater complexity. The methods of [3] may offer a way of approach to the combinatorial aspects of this problem.

In conclusion, we mention the problem of extending the present theory to a theory of equations over free products. Such an extension was made in [9] and it was an attempt on another special case which led to the present work. It is hoped to deal with the case of free products in a subsequent publication.

References

1. K. I. Appel, *On two variable equations in free groups*, Proc. Amer. Math. Soc., **21** (1969), 179-184.

2. H. S. M. Coxeter and W. O. J. Moser, *Generators and Relations for Discrete Groups*, Springer-Verlag, Berlin, 1957.

3. P. J. Higgins and R. C. Lyndon, *Equivalence of Elements Under Automorphisms of a Free Group*, Mimeographed notes, Queen Mary College, London, 1962.

4. R. C. Lyndon, *The equation $a^2b^2=c^2$ in free groups*, Michigan Math. J. **6** (1959), 89-95.
5. W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Wiley, N. Y., 1966.
6. P. E. Schupp, *On the substitution problem for free groups*, Proc. Amer. Math. Soc., Soc., **23** (1969), 421-423.
7. J. H. C. Whitehead, *On certain sets of elements in a free group*, Proc. London Math. Soc., **41** (1936), 48-56.
8. ———, *On equivalent sets of elements in a free group*, Annals of Math., **37** (1936), 782-800.
9. M. J. Wicks, *Commutators in free products*, J. London Math. Soc., **37** (1962), 433-444.
10. H. Zieschang, E. Vogt and H.-D. Coldewey, *Flachen und ebene diskontinuierliche Gruppen*, Springer-Verlag, Berlin, 1970.

Received June 28, 1971 and in revised form November 17, 1971.

UNIVERSITY OF SINGAPORE