FINITELY GENERATED $\mathscr{D}$-GROUPS

TEKLA LEWIN

(Received 20 January 1966)

This paper is taken from the author's doctoral dissertation at New York University; the work was supported by the National Science Foundation, Grant G19674. The author would like to thank Professor Gilbert Baumslag for suggesting the questions treated in this paper, and for his very helpful guidance.

Introduction

There is an extensive literature concerning groups in which the extraction of roots is always possible. Among the various classes of groups that have been studied is the class of those groups in which the extraction of roots is not only possible but is also unique. More precisely, let $\tilde{\omega}$ be a non-empty set of primes: then we shall call (using the notation of G. Baumslag) a group G a $\mathscr{D}_{\tilde{\omega}}$-group if the equation

$$x^p = g \qquad (p \in \tilde{\omega},\ g \in G)$$

is always uniquely solvable in G. It is with groups of this kind that we shall be concerned in this paper. However, the set $\tilde{\omega}$ of primes turns out to be immaterial as far as this work is concerned, in the sense that our theorems are valid for every set $\tilde{\omega}$ of primes. Therefore we have found it expedient to confine ourselves to the case where $\tilde{\omega}$ is the set of all primes, and henceforth we shall omit the suffix $\tilde{\omega}$. Thus, if G is a $\mathscr{D}$-group, then the equation

$$x^n = g \ (n \text{ a natural number, } g \in G)$$

is always uniquely solvable in G; we shall call the solution x the n^{th} root of g and write $g^{1/n} = x$, and if $r = m/n$ where m is an integer, $g^r = (g^{1/n})^m$.

The starting point for the present considerations is the notion of a free $\mathscr{D}$-group, which was introduced and studied by G. Baumslag [1]. Let us call a subgroup H of a $\mathscr{D}$-group G a $\mathscr{D}$-subgroup if the roots of the elements of H lie in H; a set S of elements of G will be said to $\mathscr{D}$-generate G if every $\mathscr{D}$-subgroup of G containing S coincides with G. Then a $\mathscr{D}$-group F is free if it possesses a set S of elements, called free generators of F, such that

(1) S $\mathscr{D}$-generates F

(2) for every $\mathscr{D}$-group G and every mapping θ of S into G, there is a homomorphism φ of F into G that coincides with θ on S.

It turns out that the cardinality of S, the so-called rank of F, is an invariant [2]. It is not difficult to show that there is a free $\mathscr{D}$-group of rank $\mathfrak{m}$ for every cardinal number $\mathfrak{m}$ [2].

We shall call a normal subgroup N of a $\mathscr{D}$-group G an ideal if G/N is itself a $\mathscr{D}$-group. Now let G be any given $\mathscr{D}$-group; then $G \simeq F/N$ for some suitably chosen free $\mathscr{D}$-group F and some ideal N of F (the choice of F and N are of course not unique). If F can be chosen to be of finite rank, we shall say G is finitely $\mathscr{D}$-generated or that G is a finitely generated $\mathscr{D}$-group. If F and N can be chosen so that there exists a finite set of elements

$$W_1, W_2, \cdots, W_m \in N$$

such that every ideal of F containing these elements contains N itself, then we shall say that G is a finitely related $\mathscr{D}$-group. If G is a finitely generated and finitely related $\mathscr{D}$-group, then we call G a finitely presented $\mathscr{D}$-group.

In order to avoid such awkward locutions as "the set S $\mathscr{D}$-generates the $\mathscr{D}$-group G", we shall strictly adhere to the following convention: *S generates the $\mathscr{D}$-group G means the same as S $\mathscr{D}$-generates G, whereas S generates G means the subgroup of G generated by S is G itself. Likewise, the $\mathscr{D}$-group G is finitely generated means G is $\mathscr{D}$-generated by a finite set.* It is important to keep this convention in mind so that no confusion will arise for a $\mathscr{D}$-group G, between these notations for G qua $\mathscr{D}$-group and for G qua group.

More generally, we would like to define the concept of a presentation for a $\mathscr{D}$-group. To this end, let us notice that if F is a free $\mathscr{D}$-group with a set of free generators $a_1, a_2, \cdots$, then every element $W \in F$ can be written as an expression, or word, involving the generators $a_1, a_2, \cdots$. To see this, we define a word of weight n in F as follows: First we shall call the free generators $a_1, a_2, \cdots$ words of weight 1. Having defined words of weight less than n, we define $(U^r V^s)^t$, where U and V are words of weight less than n and r, s, t are rational exponents, to be a word of weight n. The collection of words of weight n, as n ranges over the natural numbers, constitutes the set of words. Since the elements $a_1, a_2, \cdots$ $\mathscr{D}$-generate F, every element can be written as a word in $a_1, a_2, \cdots$. If $W \in F$ can be expressed as a word in $a_1, a_2, \cdots, a_m$, then we shall indicate this by writing $W = W(a_1, a_2, \cdots, a_m)$.

Now let G be any given $\mathscr{D}$-group. Let F be a free $\mathscr{D}$-group and N an ideal of F such that $F/N \underset{\varphi}{\simeq} G$. Let $a_1, a_2, \cdots$ be a set of free generators of F and let $a_i N\varphi = g_i$. If the elements

$$W_1(a_1, \cdots, a_{m_1}),\ W_2(a_1, \cdots, a_{m_2}), \cdots \in N$$

are such that every ideal containing these elements contains N, then we shall write

$$(*)\quad G = \mathscr{D}\text{-}gp\ \langle g_1, g_2, \cdots; W_1(g_1, \cdots, g_{m_1}) = 1, W_2(g_1, \cdots, g_{m_2}) = 1, \cdots \rangle$$

where $W_j(g_1, \cdots, g_{m_j})$ is the expression obtained from $W_j(a_1, \cdots, a_{m_j})$ by replacing each a_i by g_i. We shall call (*) a presentation for G, and we shall call the expressions

$$W_1(g_1, \cdots, g_{m_1}) = 1, W_2(g_1, \cdots, g_{m_2}) = 1, \cdots$$

defining relations in the generators $g_1, g_2, \cdots$ of the $\mathscr{D}$-group G.

It is well known that every countable group G can be embedded in a 2-generator group G', and that if G is given by n defining relations then G' can be chosen so as to be defined by n relations (see [4]). We shall show, similarly, (Theorem 4) that every countable $\mathscr{D}$-group H can be embedded in a 3-generator $\mathscr{D}$-group H', and that if the $\mathscr{D}$-group H can be given by n defining relations then the $\mathscr{D}$-group H' can be chosen so as also to be defined by n relations — this is our main theorem. Whether 3 can be decreased to 2 here is as yet an unsolved problem.

Theorem 4 enables us to "count" the number of 3-generator $\mathscr{D}$-groups: (Theorem 5) the number of 3-generator $\mathscr{D}$-groups is the power of the continuum. Thus in spite of the apparently severe restrictions of existence and, more important, uniqueness of roots, this class of groups turns out to be very large. Moreover, the structure of even a finitely generated $\mathscr{D}$-group can be quite complicated. Indeed, suppose we term a $\mathscr{D}$-group simple if it has no proper ideals. Then we shall show, by a non-constructive existence proof, that there is a 5-generator non-abelian simple $\mathscr{D}$-group. One might ask whether there exist $\mathscr{D}$-groups which are simple in the group theoretic sense, i.e. which possess no proper normal subgroups; we know of no example.

Preliminaries

The following theorem is well known (von Dyck):
If the group G has a presentation

$$G = gp\ \langle g_1, g_2, \cdots; R_1(g_1, \cdots, g_{m_1}) = 1, R_2(g_1, \cdots, g_{m_2}) = 1, \cdots \rangle$$

and H is a group containing elements h_1, $h_2, \cdots$ such that

$$R_1(h_1, \cdots, h_{m_1}) = 1,\ R_2(h_1, \cdots, h_{m_2}) = 1, \cdots,$$

then the mapping $\varphi : g_i \to h_i$, $i = 1, 2, \cdots$ can be extended to a homomorphism of G into H.

The analogous theorem holds also for $\mathscr{D}$-groups:
If the $\mathscr{D}$-group G has a presentation

$$G = \mathscr{D}\text{-}gp\,\langle g_1, g_2, \cdots; R_1(g_1, \cdots, g_{m_1}) = 1,\ R_2(g_1, \cdots, g_{m_2}) = 1, \cdots\rangle$$

and H is a $\mathscr{D}$-group containing elements $h_1, h_2, \cdots$ such that

$$R_1(h_1, \cdots, h_{m_1}) = 1,\ R_2(h_1, \cdots, h_{m_2}) = 1, \cdots,$$

then the mapping $\varphi : g_i \to h_i$, $i = 1, 2, \cdots$ can be extended to a homomorphism of G into H.

In this paper we shall make repeated use of the free product with an amalgamated subgroup, also called the generalized free product. We shall mention without proof a number of statements, the proofs of which may be found in [5].

Let F be a group, F_1 and F_2 subgroups of F and let $F_1 \cap F_2 = G$. We shall call F the generalized free product of F_1 and F_2 (or the free product of F_1 and F_2 with amalgamated subgroup G) if

(1) F is generated by its subgroups F_1 and F_2, and
(2) For every group H and every pair of homomorphisms

$$\varphi_1 : F_1 \to H,\ \varphi_2 : F_2 \to H$$

which agree on G, there exists a homomorphism $\varphi : F \to H$ that coincides with φ_i on F_i. We shall write

$$F = \{F_1 * F_2; G\}.$$

Suppose groups F_1 and F_2 are given, G_1 a subgroup of F_1 and G_2 a subgroup of F_2, and $G_1 \overset{\varphi}{\cong} G_2$. Then there exists a group F which is the generalized free product of its subgroups $\hat{F}_1$ and $\hat{F}_2$, $\hat{F}_1 \overset{\varphi_1}{\cong} F_1$, $\hat{F}_2 \overset{\varphi_2}{\cong} F_2$, such that $(\hat{F}_1 \cap \hat{F}_2)\varphi_i = G_i$ and if $f \in \hat{F}_1 \cap \hat{F}_2$ then

$$f\varphi_1\varphi = f\varphi_2.$$

In this case we shall identify $\hat{F}_1$ with F_1, $\hat{F}_2$ with F_2, and G_1 with G_2 (via the isomorphisms φ_1, φ_2, and φ) and again call F the generalized free product of F_1 and F_2. We shall use the following notation:

$$F = \{F_1 * F_2; G_1 = G_2\}.$$

If G_1 is generated by elements $g_1, g_2, \cdots$ and if $g_i\varphi = g'_i$, we shall sometimes write

$$F = \{F_1 * F_2; g_1 = g'_1, g_2 = g'_2, \cdots\}.$$

Now let

$$F = \{F_1 * F_2; G\}.$$

The elements in F can be represented by a *normal form*: We choose in

F_i $(i = 1, 2)$ a system S_i of left coset representatives modulo G containing the unit element; thus every element $f \in F_i$ can be uniquely represented in the form

$$f = sg \qquad (s \in S_i,\ g \in G).$$

We call the following string of symbols

$$s_1 s_2 \cdots s_n g$$

a normal form if

(1) Every term s_k is a representative $\neq 1$ belonging to one of the S_i.

(2) Successive components s_k and s_{k+1} belong to different systems of representatives, i.e., if $s_k \in S_i$ and $s_{k+1} \in S_j$, then $i \neq j$.

(3) $g \in G$.

If we interpret this string of symbols as a product, we obtain an element $f = s_1 s_2 \cdots s_n g$, and we say $s_1 s_2 \cdots s_n g$ is the normal form of the element f. Every element is represented by one and only one normal form. We call n the length of f and write $\lambda(f) = n$.

Every element $f \in F$ can be written as $f = f_1 f_2 \cdots f_n$, where each f_i is in F_1 or in F_2, since F_1 and F_2 together generate F. We will describe the procedure by which the normal form of f can be obtained. First, f can be written in the form

(*) $f = h_1 h_2 \cdots h_m$, where each h_i in F_1 or F_2, but h_i and h_{i+1} not in a common factor F_j, and with $m \leqq n$.

For if f_i and f_{i+1} both lie in F_1 or both lie in F_2, then we may write

$$f = f_1 f_2 \cdots f_{i-1} f'_i f_{i+2} \cdots f_n,$$

where $f'_i = f_i f_{i+1}$, which is an element in one of the factors; we may continue in this manner, at each step decreasing the number of terms until we have written f in the desired form (*): $f = h_1 h_2 \cdots h_m$. Notice that if $m > 1$ then $h_i \notin G$ for any i, for then h_i and h_{i+1} (or h_i and h_{i-1}) lie in a common factor. Now if $m = 1$ and $f \in G$, then the normal form of f is f itself. If $f \notin G$, then $h_1 \in F_i - G$ for $i = 1$ or $i = 2$, and

$$h_1 = s_1 g_1 \qquad (1 \neq s_1 \in S_i,\ g_1 \in G).$$

Thus if $m = 1$ and $f \notin G$, then $s_1 g_1$ is the normal form of f. If $m > 1$, then

$$f = s_1 (g_1 h_2) \cdots h_m.$$

Now $h_2 \in F_j - G$ $(j \neq i)$ and so $g_1 h_2 \in F_j - G$; therefore

$$g_1 h_2 = s_2 g_2 \qquad (1 \neq s_2 \in S_j,\ g_2 \in G).$$

If $m = 2$, then $f = s_1 s_2 g_2$ and $s_1 s_2 g_2$ is the normal form of f. If $m > 2$, then

$$f = s_1 s_2 (g_2 h_3) \cdots h_m .$$

Continuing in this way, we will arrive at the normal form of f:

$$f = s_1 s_2 \cdots s_m g_m ,$$

and we note that $\lambda(f) = m$ provided that $m > 1$.

Therefore if

$$f = f_1 f_2 \cdots f_n$$

where each f_i is in F_1 or F_2, but f_i and f_{i+1} are not in a common factor, then the length of f is n if $n > 1$, the length of f is 1 if $n = 1$ and $f \notin G$, and the length of f is 0 if $n = 1$ and $f \in G$.

Now suppose that

$$f = (t_1 t_2 \cdots t_n g)(k_1 k_2 \cdots k_m)$$

where $t_1 t_2 \cdots t_n g$ is a normal form, each k_i is in F_1 or F_2, and k_i and k_{i+1} do not lie in a common factor F_j. If also t_n and k_1 are not in a common factor, then it is clear from the above procedure that the normal form of f is

$$f = t_1 t_2 \cdots t_n t'_{n+1} \cdots t'_{n+m} g'$$

for some representatives $t'_{n+1}, \cdots, t'_{n+m}$ and some $g' \in G$. This fact is frequently used in this paper.

Suppose $f = f_1 f_2 \cdots f_n$ where each f_i is in F_1 or F_2, but f_i and f_{i+1} are not in the same factor F_j. Suppose $h = h_1 h_2 \cdots h_m$ where each h_i is in F_1 or F_2, but h_i and h_{i+1} do not lie in a common factor. If also f_n and h_1 do not lie in a common factor, then $\lambda(fh) = \lambda(f) + \lambda(h)$; we shall sometimes write

$$fh = f_1 f_2 \cdots f_n \wedge h_1 h_2 \cdots h_m \text{ or } f \wedge h$$

to indicate that f_n and h_1 do not lie in a common factor.

The element f is *cyclically reduced* if none of its conjugates in F has smaller length than itself. If f is cyclically reduced and

$$f = f_1 f_2 \cdots f_n$$

with $n > 1$, each f_i in F_1 or F_2, but f_i and f_{i+1} not in the same factor F_j, then f_1 and f_n belong to different factors F_j. Conversely, if f is of the above form and f_1 and f_n belong to different factors, then f is cyclically reduced.

NOTATION. We list here some of the notations used.

A group G is called an *R-group* if the equation

$$x^n = g \qquad (n \text{ a natural number, } g \in G)$$

has at most one solution x in G.

If G is a group and $g \in G$, the *centralizer* of g in G, written $C(g, G)$ is $\{x \in G \mid x^{-1}gx = g\}$.

Γ is a multiplicative copy of the additive rationals. For definiteness, we may take the elements of Γ to be the formal symbols z^r, where r runs through the additive rationals, and multiplication is defined by $z^r z^s = z^{r+s}$.

If S is a subset of a $\mathscr{D}$-group G, then the intersection of all the $\mathscr{D}$-subgroups of G containing S is itself a $\mathscr{D}$-subgroup and contains S. This $\mathscr{D}$-subgroup is called *the $\mathscr{D}$-subgroup generated by* S and we shall denote it by $\mathscr{D}$-$gp(S)$. If $S = \{a_1, a_2, a_3, \cdots\}$ we shall sometimes write $\mathscr{D}$-$gp(a_1, a_2, a_3 \cdots)$ for $\mathscr{D}$-$gp(S)$.

If G is a group, then

$$H < G$$

means H is a (not necessarily proper) subgroup of G.

1

Our primary aim in this paper is to embed every countable $\mathscr{D}$-group in a 3-generator $\mathscr{D}$-group. The procedure we have adopted is modelled on earlier work of G. Higman, B. H. Neumann, and H. Neumann [4] and G. Baumslag [1] making use of free products with amalgamations. In particular, we make frequent use of a theorem of Baumslag [1] (Theorem 1 below) that states that every group in a certain class $\mathscr{P}$, whose definition can be couched in terms of the centralizers of group elements, can be embedded in a $\mathscr{D}$-group. For this reason we have found it essential to carry out a careful analysis of certain kinds of generalized free products. By keeping track of centralizers, we are able to show that certain generalized free products of groups in $\mathscr{P}$ also are in $\mathscr{P}$ (Theorem 2 and Theorem 3). This procedure turns out to be useful in determining the number of finitely generated $\mathscr{D}$-groups.

Before we can state Theorem 1 more exactly, it is necessary to first define and discuss the notion of the free $\mathscr{D}$-closure of a group.

Let G be a subgroup of a $\mathscr{D}$-group G^*. G^* is called the free $\mathscr{D}$-closure of the group G provided that

1. the $\mathscr{D}$-subgroup of G^* generated by G is G^* itself,
2. for every homomorphism φ of G into a $\mathscr{D}$-group H there exists a homomorphism φ^* of G^* into H that coincides with φ on G.

Now, if G is a given group we say that the free $\mathscr{D}$-closure of G exists if there is a monomorphism μ of G into a $\mathscr{D}$-group G^* such that G^* is the free $\mathscr{D}$-closure of $G\mu$; in this case we identify G with $G\mu$ and we say that G^* is the free $\mathscr{D}$-closure of G. It is not difficult to see that if it exists the free $\mathscr{D}$-closure of a group is unique up to isomorphism. Also, it is not difficult to see that if G is a group that can be embedded in some $\mathscr{D}$-group then the free $\mathscr{D}$-closure G^* of G exists and that G^* has the presentation

$$G^* = \mathscr{D}\text{-}gp\,\langle a_1, a_2, \cdots; R_1(a_1, a_2, \cdots, a_{m_1}) = 1, R_2(a_1, a_2, \cdots, a_{m_2}) = 1, \cdots \rangle,$$

if

$$G = gp\,\langle a_1, a_2, \cdots; R_1(a_1, a_2, \cdots, a_{m_1}) = 1, R_2(a_1, a_2, \cdots, a_{m_2}) = 1, \cdots \rangle$$

is a presentation for G.

To verify this remark let us suppose that G is a subgroup of a $\mathscr{D}$-group H, and let

$$G = gp\,\langle a_1, a_2, \cdots; R_1(a_1, a_2, \cdots, a_{m_1}) = 1, R_2(a_1, a_2, \cdots, a_{m_2}) = 1, \cdots \rangle$$

be a presentation for G. We define

$$G^* = \mathscr{D}\text{-}gp\,\langle \alpha_1, \alpha_2, \cdots; R_1(\alpha_1, \alpha_2, \cdots, \alpha_{m_1}) = 1, R_2(\alpha_1, \alpha_2, \cdots, \alpha_{m_2}) = 1, \cdots \rangle.$$

Now by the theorem of von Dyck there is a homomorphism φ mapping G into G^* determined by

$$a_i\varphi = \alpha_i, \qquad i = 1, 2, \cdots,$$

because $R_j(a_1\varphi, a_2\varphi, \cdots, a_{m_j}\varphi) = 1$ for the defining relations R_j of the group G. By the corresponding theorem for $\mathscr{D}$-groups there is a homomorphism ψ mapping G^* into the $\mathscr{D}$-group H determined by

$$\alpha_i\psi = a_i, \qquad i = 1, 2, \cdots,$$

because $R_j(\alpha_1\psi, \alpha_2\psi, \cdots, \alpha_{m_j}\psi) = 1$ for the defining relations R_j of the $\mathscr{D}$-group G^*. $\varphi\psi$ is a homomorphism of G into H, and $a_i\varphi\psi = a_i$ for $i = 1, 2, \cdots$. $\varphi\psi$ acts as the identity on a set of generators of the group G implies that $\varphi\psi$ is the identity mapping of G; therefore φ is a monomorphism, and so G can be embedded in G^*, identifying a_i with α_i $(i = 1, 2, \cdots)$.

Since G^* is $\mathscr{D}$-generated by $\alpha_1 = a_1$, $\alpha_2 = a_2, \cdots$, the $\mathscr{D}$-subgroup of G^* generated by G is G^* itself. Now suppose that η is a homomorphism of G into a $\mathscr{D}$-group K. Because η is a homomorphism, $R_j(a_1, a_2, \cdots, a_{m_j}) = 1$ implies that $R_j(a_1\eta, a_2\eta, \cdots, a_{m_j}\eta) = 1$; however, the R_j are the defining relations of the $\mathscr{D}$-group G^*, and so by the analogue for $\mathscr{D}$-groups of the theorem of von Dyck η can be extended to a homomorphism η^* of G^* into K. This establishes that G^* is in fact the free $\mathscr{D}$-closure of G.

We now define the class of groups that Baumslag has shown can be embedded in $\mathscr{D}$-groups; he has given a procedure for constructing the free $\mathscr{D}$-closure of a group in this class.

Let $\mathscr{P}$ be the class of groups G such that

1. G is an R-group.

2. If $h \in G$ and h does not have an n^{th} root for some natural number n, then

a) $C(h, G)$ is isomorphic to a subgroup of Γ, and

b) if $f^{-1}h^k f = h^l$ for some $f \in G$ and integers k and l, then $k = l$.

THEOREM 1 (Baumslag [1]). *Every group G in $\mathcal{P}$ can be embedded in a $\mathcal{D}$-group. For G a group in $\mathcal{P}$ and G^* the free $\mathcal{D}$-closure of G:*

If $1 \neq h \in G$ and h has an n^{th} root in G for every n, then $C(h, G^*) = C(h, G)$.

If $1 \neq h \in G^*$ and h is not conjugate in G^* to an element of G having an n^{th} root in G for every n, then $C(h, G^*) \simeq \Gamma$.

We now state Theorems 2 and 3; the proofs of these theorems appear after a number of lemmas. The proofs of the two theorems are patterned after the proof of the theorem just quoted.

THEOREM 2. *Let $A = \{G_1 * G_2; U\}$. Suppose that for each non-trivial element $u \in U$ one of the following holds:*

$$\text{(a) } \{x \in G_1 \,|\, x^{-1}ux \in U\} = U \quad \text{or} \quad \text{(b) } \{x \in G_2 \,|\, x^{-1}ux \in U\} = U.$$

Then the centralizer of an element in A is either infinite cyclic or is isomorphic to $C(g, G_i)$ for some element g in one of the factors G_i.

More specifically:

If $1 \neq u \in U$ and (a) *holds for u, then $C(u, A) = C(u, G_2)$.*

If $1 \neq u \in U$ and (b) *holds for u, then $C(u, A) = C(u, G_1)$.*

If $g \in G_i$ and g is not conjugate in G_i to an element in U, then $C(g, A) = C(g, G_i)$.

If $h \in A$ and h is not conjugate in A either to an element in G_1 or an element in G_2, then $C(h, A)$ is infinite cyclic.

The following special case of this theorem turns out to be particularly useful:

Let $A = \{G_1 * G_2; U\}$. Suppose that if $1 \neq u \in U$ and $g \in G_1 - U$ then $g^{-1}ug \notin U$. Then for $h \in A$ the centralizer $C(h, A)$ is either infinite cyclic or is isomorphic to $C(g, G_i)$ for some element g in one of the factors G_i.

THEOREM 3. *Let $A = \{G_1 * G_2; U\}$ where G_1 and G_2 are in $\mathcal{P}$. Suppose that if $u \in U$, $u \neq 1$, then either $\{x \in G_1 \mid x^{-1}ux \in U\} = U$ or $\{x \in G_2 \mid x^{-1}ux \in U\} = U$. Then A is in $\mathcal{P}$.*

Before proving Theorem 2, we state and prove three lemmas.

LEMMA 1. *Suppose $A = \{G_1 * G_2; U\}$. Suppose also that for each non-trivial element $u \in U$ one of the following holds:*

$$\text{(a) } \{x \in G_1 \,|\, x^{-1}ux \in U\} = U \quad \textit{or} \quad \text{(b) } \{x \in G_2 \,|\, x^{-1}ux \in U\} = U.$$

Let $1 \neq u \in U$; if (a) *holds for u then*

$$\{x \in A \mid x^{-1}ux \in U\} \subseteqq G_2,$$

and if (b) *holds for* u *then*

$$\{x \in A \mid x^{-1}ux \in U\} \subseteqq G_1.$$

PROOF. Let $1 \neq u \in U$ and, for convenience, assume (a) holds for u. Let $x \in A$ such that $x^{-1}ux \in U$. If $x \in G_2$, then there is nothing to prove. $x \notin G_1 - U$, because (a) holds for u. So let $x = x_1 x_2 \cdots x_n$, $n \geqq 2$, where each x_i in one of the factors but x_i and x_{i+1} not in a common factor.

$$x^{-1}ux = x_n^{-1} \cdots x_2^{-1} x_1^{-1} u x_1 x_2 \cdots x_n.$$

If $x_1 \in G_1 - U$, then $x_1^{-1}ux_1 \in G_1 - U$ and $\lambda(x^{-1}ux) = 2(n-1)+1 \geqq 3$, which is impossible because $x^{-1}ux \in U$ and so $\lambda(x^{-1}ux) = 0$. If $x_1 \in G_2 - U$ and $x_1^{-1}ux_1 \in G_2 - U$, then $\lambda(x^{-1}ux) = 2(n-1)+1 \geqq 3$, which is again impossible.

If $x_1 \in G_2 - U$ and $x_1^{-1}ux_1 \in U$, then (a) holds for $x_1^{-1}ux_1$ since (b) cannot hold for $x_1^{-1}ux_1$ because $x_1(x_1^{-1}ux_1)x_1^{-1} \in U$ and $x_1 \in G_2 - U$. Now $x_2 \in G_1 - U$, so $x_2^{-1}(x_1^{-1}ux_1)x_2 \notin U$; therefore $\lambda(x^{-1}ux) = 2(n-2)+1 \geqq 1$, which is impossible.

LEMMA 2. *Let* $A = \{G_1 * G_2; U\}$.

If $g \in G_i$ $(i = 1$ *or* $2)$ *and* g *is not conjugate in* G_i *to an element in* U, *then* $\{x \in A \mid x^{-1}gx \in G_i\} \subseteqq G_i$.

PROOF. For convenience suppose $g \in G_1$ and g is not conjugate in G_1 to an element in U, in particular $g \notin U$, and that $x^{-1}gx \in G_1$. So $\lambda(g) = 1$ and $\lambda(x^{-1}gx) \leqq 1$. Let $x = x_1 x_2 \cdots x_n$ where x_i in G_1 or G_2 but x_i and x_{i+1} not in the same factor.

Then $x^{-1}gx = x_n^{-1} \cdots x_2^{-1} x_1^{-1} g x_1 x_2 \cdots x_n$.

If $x_1 \in G_2 - U$, then $\lambda(x^{-1}gx) = 2n+1 \geqq 3$, which is a contradiction.

If $x = x_1 \in G_1$, there is nothing to prove.

If $x_1 \in G_1$, $n \geqq 2$, then $x_1^{-1}gx_1 \notin U$ because g is not conjugate in G_1 to an element of U; so $x_1^{-1}gx_1 \in G_1 - U$ and $\lambda(x^{-1}gx) = 2(n-1)+1 \geqq 3$, which is a contradiction.

LEMMA 3. *Let* $A = \{G_1 * G_2; U\}$. *Suppose that if* $g \in A$ *and* g *lies in one of the factors, then* $C(g, A)$ *is conjugate to a subgroup of one of the factors. If* $g \in A$ *and* g *is not conjugate to an element in one of the factors, then* $C(g, A)$ *is infinite cyclic.*

The proof of Lemma 3 is broken up into four steps.

(i) It is sufficient to prove the statement for elements g that are cyclically reduced of length $\geqq 2$.

PROOF. For let $g \in A$, g not conjugate to an element in one of the factors. Then $g = x^{-1}hx$ for some element h that is cyclically reduced of length $\geqq 2$. Therefore $C(g, A) = x^{-1}C(h, A)x$.

(ii) Let $g \in A$, g cyclically reduced of length $\geqq 2$. If $h \in C(g, A)$, then h is cyclically reduced of length $\geqq 2$.

PROOF. Let $h \in C(g, A)$. The length of h must be $\geqq 2$. For otherwise h is in one of the factors G_i and so $C(h, A)$ is conjugate to a subgroup of one of the factors; $g \in C(h, A)$, therefore g is conjugate to an element in one of the factors — this, however, is impossible because g is cyclically reduced of length $\geqq 2$.

Now g can be written $g = g_1 g_2 \cdots g_n$ where $n \geqq 2$, each g_i lies in one of the factors, and g_i and g_{i+1} do not lie in the same factor. Because g is cyclically reduced, g_1 and g_n lie in different factors. h can be written $h = h_1 h_2 \cdots h_m$ where $m \geqq 2$, each h_i lies in one of the factors, and h_i and h_{i+1} do not both lie in the same factor. If h is not cyclically reduced, h_1 and h_m lie in the same factor. Now suppose that h_1 and h_m do lie in the same factor G_i. Either g_1 or g_n lies in G_i also, say $g_1 \in G_i$, and so $g_n \notin G_i$.

Then $gh = g_1 g_2 \cdots g_n h_1 h_2 \cdots h_m$, and since g_n and h_1 lie in different factors, $\lambda(gh) = n+m$.

$$hg = h_1 h_2 \cdots h_{m-1}(h_m g_1) g_2 \cdots g_n;\ (h_m g_1) \in G_i,$$

so $\lambda(hg) \leqq n+m-1$. This, however, is impossible because $gh = hg$. So h_1 and h_m lie in different factors, and h is cyclically reduced.

(iii) If $g \in A$ and g is cyclically reduced of length at least 2, and if $h \neq 1$ is such that $[h, g] = 1$, then g and h are powers of a common element: $\exists f$ such that $f^i = h$ and $f^j = g$ for some integers i and j.

PROOF. Suppose the statement is false. Let g^* be an element of minimal length in

$$\left\{ g \in A \mid \begin{array}{l} g \text{ is cyclically reduced of length at least 2;} \\ \exists\, h \neq 1 \text{ such that } [h, g] = 1 \text{ but } g \text{ and } h \\ \text{are not powers of a common element} \end{array} \right\}.$$

Let h^* be an element of minimal length in

$$\left\{ \begin{array}{l} h \in A \mid h \neq 1;\ [h, g^*] = 1 \text{ but } g^* \text{ and } h \\ \qquad\qquad\qquad \text{are not powers of a common element} \end{array} \right\}.$$

h^* is cyclically reduced of length $\geqq 2$ by (ii); therefore $\lambda(h^*) \geqq \lambda(g^*)$ because of the choice of g^*. Let the normal form for g^* be $g^* = s_1 s_2 \cdots s_n u_1$; without loss of generality we may assume that $s_1 \in G_1$ and $s_n \in G_2$. Let the normal form for h^* be $h^* = t_1 t_2 \cdots t_k u_2$; we may also assume $t_1 \in G_1$ and $t_k \in G_2$ (if not, consider h^{*-1} which also commutes with g^*).

Now $g^* h^* = s_1 s_2 \cdots s_n (u_1 t_1) t_2 \cdots t_k u_2$, so the normal form for $g^* h^*$

is $g^*h^* = s_1s_2 \cdots s_n t'_1 t'_2 \cdots t'_k u'$ for some representatives $t'_1, t'_2, \cdots, t'_k$ and some $u' \in U$. Similarly the normal form of h^*g^* is $h^*g^* = t_1t_2 \cdots t_k s'_1 \cdots s'_n u''$ for some $s'_1, \cdots, s'_n, u''$. Because $g^*h^* = h^*g^*$, these normal forms are the same. $k = \lambda(h^*) \geqq \lambda(g^*) = n$. So $s_1 = t_1$, $s_2 = t_2 \cdots$, and $s_n = t_n$.

$$\begin{aligned} g^{*-1}h^* &= u_1^{-1}s_n^{-1} \cdots s_2^{-1}s_1^{-1}t_1t_2 \cdots t_k u_2 \\ &= u_1^{-1}t_{n+1} \cdots t_k u_2 \end{aligned}$$

and

$$\lambda(g^{*-1}h^*) = k-n < k.$$

Now $g^{*-1}h^* \neq 1$ because then g^* and h^* are certainly powers of a common element; $g^{*-1}h^*$ commutes with g^* because h^* does, and its length is less than that of h^*. So it must be that $g^{*-1}h^*$ and g^* are powers of a common element (otherwise the choise of h^* is contradicted); however, this implies that g^* and h^* are powers of a common element, contrary to the choice of h^*.

(iv) If $g \in A$ and g is cyclically reduced of length at least 2, then $C(g, A)$ is infinite cyclic.

Proof. Let f^* be a non-trivial element of minimal length in $C(g, A)$. If $h \neq 1$, $h \in C(g, A)$, then h is a power of f^*.

Suppose not. Let h^* be an element of minimal length in

$$\{h \in C(g, A) \mid h \neq 1,\ h \text{ not a power of } f^*\}.$$
$$\lambda(h^*) \geqq \lambda(f^*) \text{ by the choice of } f^*.$$

By (iii) $\exists\, f$ such that $f^i = f^*$ and $f^j = g$ for some integers i and j. $f \neq 1$ and f commutes with g, so f is cyclically reduced of length at least 2 by (ii). Therefore $\lambda(f^*) = |i|\lambda(f)$; if $|i| > 1$, then $\lambda(f^*) > \lambda(f)$, which is contrary to the choice of f^*. This means $i = 1$ or $i = -1$, and so $g = f^{*m}$ for some integer m; we may assume $m > 0$.

Again by (iii) $\exists\, h$ such that $h^i = h^*$ and $h^j = g$ for some integers i and j. $h \neq 1$ and h commutes with g, so h is cyclically reduced of length at least 2 by (ii). Suppose $|i| > 1$. Then $\lambda(h^*) = |i|\lambda(h) > \lambda(h)$. Since $h \in C(g, A)$ and of shorter length than h^*, it must be that h is a power of f^*, for otherwise the choice of h^* is contradicted. But this implies $h^* = h^i$ is a power of f^*, which is also contrary to the choice of h^*. So $|i| = 1$ and $g = h^{*n}$ for some integer n; we may assume $n > 0$.

If $f^* = s_1s_2 \cdots s_k u_1$ is the normal form of f^* and

$$h^* = t_1t_2 \cdots t_l u_2 \text{ is the normal form of } h^*,$$

then

$$\overbrace{(s_1 s_2 \cdots s_k u_1)(s_1 s_2 \cdots s_k u_1) \cdots (s_1 s_2 \cdots s_k u_1)}^{m}$$
$$= g = \underbrace{(t_1 t_2 \cdots t_l u_2)(t_1 t_2 \cdots t_l u_2) \cdots)t_1 t_2 \cdots t_l u_2)}_{n}.$$

Because f^* and h^* are cyclically reduced, the normal form for g is $s_1 s_2 \cdots s_k s'_1 s'_2 \cdots s'_{mk} u'$ for some coset representatives $s'_1, s'_2, \cdots, s'_{mk}$ and some $u' \in U$ and also $t_1 t_2 \cdots t_l t'_1 t'_2 \cdots t'_{ln} u''$ for some $t'_1, t'_2, \cdots, t'_{ln}$ and some u''. Since

$$k = \lambda(f^*) \leqq \lambda(h^*) = l,$$

it must be that

$$s_1 = t_1, \quad s_2 = t_2, \cdots, \quad s_k = t_k.$$

So

$$f^{*-1} h^* = u_1^{-1} s_k^{-1} \cdots s_1^{-1} t_1 \cdots t_l u_2 = u_1^{-1} t_{k+1} \cdots t_l u_2$$

and

$$\lambda(f^{*-1} h^*) = l - k < l \text{ since } k \geqq 2.$$

$f^{*-1}h^*$ commutes with g because both f^* and h^* do. $f^{*-1}h^* = 1$ contradicts the choice of h^*, for in this case h^* is a power of f^*. Therefore, unless $f^{*-1}h^*$ is a power of f^*, the choice of h^* is contradicted; but if $f^{*-1}h^*$ is a power of f^* so is h^*, again contrary to the choice of h^*. So $C(g, A) = gp(f^*)$. f^* is not of finite order, because $\lambda(f^{*n}) = |n|\, \lambda(f^*)$, which is zero only if $n = 0$; therefore this subgroup is infinite cyclic.

We are now in a position to prove Theorem 2.

THEOREM 2. *Let $A = \{G_1 * G_2; U\}$. Suppose that for each non-trivial element $u \in U$ one of the following holds:*

(a) $\{x \in G_1 \mid x^{-1}ux \in U\} = U$ or (b) $\{x \in G_2 \mid x^{-1}ux \in U\} = U$.

Then the centralizer of an element in A is either infinite cyclic or is isomorphic to $C(g, G_i)$ for some element g in one of the factors G_i.

More specifically:

If $1 \neq u \in U$ and (a) holds for u, then $C(u, A) = C(u, G_2)$.

If $1 \neq u \in U$ and (b) holds for u, then $C(u, A) = C(u, G_1)$.

If $g \in G_i$ and g is not conjugate in G_i to an element in U, then $C(g, A) = C(g, G_i)$.

If $h \in A$ and h is not conjugate in A either to an element in G_1 or an element in G_2, then $C(h, A)$ is infinite cyclic.

PROOF. Let $u \in U$, $u \neq 1$, and suppose (a) holds for u. By Lemma 1 $\{x \in A \mid x^{-1}ux \in U\} \subseteqq G_2$; since $C(u, A) \subseteqq \{x \in A \mid x^{-1}ux \in U\}$, $C(u, A) \subseteqq G_2$ and therefore $C(u, A) = C(u, G_2)$.

By symmetry if $u \in U$, $u \neq 1$, and (b) holds for u, then $C(u, A) = C(u, G_2)$.

If $g \in G_i$ and g is not conjugate in G_i to an element in U, then by Lemma 2 $\{x \in A \mid x^{-1}gx \in G_i\} \subseteqq G_i$. Since $C(g, A) \subseteqq \{x \in A \mid x^{-1}gx \in G_i\}$, $C(g, A) \subseteqq G_i$. Therefore $C(g, A) = C(g, G_i)$.

Now, every element f in one of the factors G_i is conjugate to an element g of one of the three preceding kinds; therefore $C(f, A)$ is conjugate to $C(g, A)$, and we have just shown that $C(g, A) = C(g, G_i)$ for one of the factors G_i. Thus if $f \in A$ and f lies in one of the factors, then $C(f, A)$ is conjugate to a subgroup of one of the factors. Therefore, by Lemma 3 if $h \in A$ and h is not conjugate to an element in one of the factors, then $C(h, A)$ is infinite cyclic.

This completes the proof of the theorem because every element of A is conjugate to an element x of one of the preceding four kinds and so has centralizer isomorphic to $C(x, A)$.

We now give two more lemmas needed to prove Theorem 3.

LEMMA 4. *Suppose*

$$A = \{G_1 * G_2; U\}$$

where G_1 *and* G_2 *are in* $\mathscr{P}$. *Suppose also that each non-trivial element in one of the factors is conjugate in* A *to an element* f *in one of the factors* G_i *such that* $C(f, A) = C(f, G_i)$.

Then

1. *If* $g \in A$ *and* g *does not have an* n^{th} *root in* A *for some natural number* n, *then* $C(g, A)$ *is isomorphic to a subgroup of* Γ.

and

2. *A is an R-group.*

PROOF OF 1. Suppose g does not have an n^{th} root in A for some natural number n and g is conjugate to an element h in one of the factors. h, and so also g, is conjugate to an element f in one of the factors G_i such that $C(f, A) = C(f, G_i)$. Since g fails to have an n^{th} root in A for some natural number n, f fails to have an n^{th} root in A for that same n; a fortiori, f fails to have an n^{th} root in G_i. Since G_i is in $\mathscr{P}$, $C(f, G_i)$ is isomorphic to a subgroup of Γ; therefore so is $C(g, A)$, which is conjugate to $C(f, A) = C(f, G_i)$.

If g is not conjugate to an element in one of the factors, then by Lemma 3 $C(g, A)$ is infinite cyclic, and so isomorphic to a subgroup of Γ.

PROOF OF 2. Suppose $x^n = y^n = g$ in A. A is torsion-free because G_1 and G_2 are, and a generalized free product of torsion-free groups is torsion-free; so if $g = 1$ then $x = y = 1$. Assume $g \neq 1$. Both x and y are in $C(g, A)$. If g is conjugate to an element in one of the factors, then, as in the proof of 1., $C(g, A)$ is conjugate to $C(f, G_i)$ (for some f in one of the factors G_i), a subgroup of G_i; since G_i is in $\mathscr{P}$, every subgroup is an R-group — hence $C(g, A)$ is also an R-group. If g is not conjugate to an element in one of the factors, then $C(g, A)$ is infinite cyclic by Lemma 3, so $x = y$.

LEMMA 5. *Suppose* $A = \{G_1 * G_2; U\}$ *where* G_1 *and* G_2 *are in* $\mathscr{P}$. *Suppose also that if* $1 \neq u \in U$ *then either*

$$\{x \in G_1 \mid x^{-1}ux \in U\} = U \quad \text{or} \quad \{x \in G_2 \mid x^{-1}ux \in U\} = U.$$

If $g \in A$, g *does not have an* n^{th} *root for some natural number* n, *and for some* $y \in A$ $y^{-1}g^k y = g^l$, *then* $k = l$.

PROOF. The proof of Lemma 5 is broken down into four cases:

a. $g^k \in U$. If $g^k = 1$ and so $g^l = y^{-1}g^k y = 1$ then $k = l = 0$, because A is torsion-free and $g \neq 1$. If $g^k \neq 1$ and $g^l \in U$ also, then y and g are both in $\{x \in A \mid x^{-1}g^k x \in U\}$, which is contained in G_1 or G_2 by Lemma 1; so this is an equation in a group in $\mathscr{P}$, hence $k = l$. But if $g^l \notin U$, we may consider instead the equation $y^{-1}g^{k^2}y = g^{kl}$, which is a consequence of the above equation. g^{k^2} and g^{kl} are in U, so by the foregoing $k^2 = kl$; $g^k \neq 1$ implies $k \neq 0$, hence $k = l$.

b. g^k in one of the factors but g^k not conjugate to an element in U. g^k is in one of the factors implies g is also in one of the factors G_i; therefore g^k and g^l both in G_i. By Lemma 2 $y \in G_i$. So this is an equation in a group in $\mathscr{P}$, hence $k = l$.

c. g^k is cyclically reduced of length at least 2. Then also g and g^l are cyclically reduced of length at least 2.

We can assume $k > 0$. Suppose also $l > 0$. Then we may assume $k \geqq l$; for if not we could consider the equation $yg^l y^{-1} = g^k$. Let $g^k = s_1 s_2 \cdots s_m$, s_i in one of the factors, but s_i and s_{i+1} not in the same factor, $g^l = t_1 t_2 \cdots t_n$, t_i in one of the factors, but t_i and t_{i+1} not in the same factor, $y = y_1 y_2 \cdots y_j$, y_i in one of the factors, but y_i and y_{i+1} not in the same factor. Now s_1 and s_m lie in different factors, so either y_1 is not in the same factor as s_1 or y_1 is not in the same factor as s_m. If y_1 is not in the same factor as s_1, consider the equation

$$y_j^{-1} \cdots y_2^{-1} y_1^{-1} \wedge s_1 s_2 \cdots s_m = y^{-1} g^k = g^l y^{-1} = t_1 t_2 \cdots t_n y_j^{-1} \cdots y_1^{-1}.$$

This implies $j + m = \lambda(t_1 t_2 \cdots t_n y_j^{-1} \cdots y_1^{-1}) \leqq n + j$, or $k\lambda(g) = m \leqq n = l\lambda(g)$, which implies $k \leqq l$. So $k = l$. If y_1 is not in the same factor as s_m, consider the equation

$$s_1 s_2 \cdots s_m \wedge y_1 \cdots y_j = g^k y = y g^l = y_1 y_2 \cdots y_j t_1 t_2 \cdots t_n.$$

This implies $m + j = \lambda(y_1 y_2 \cdots y_j t_1 t_2 \cdots t_n) \leqq j + n$; as before this implies $k = l$.

https://doi.org/10.1017/S1446788700004201 Published online by Cambridge University Press

Now assume $k > 0$ but $l < 0$. Then

$$y^{-2}g^{k^2}y^2 = y^{-1}(y^{-1}g^k y)^k y = y^{-1}g^{lk}y = (y^{-1}g^k y)^l = g^{l^2}.$$

Since $k^2 > 0$ and $l^2 > 0$, by what we have just shown $k^2 = l^2$; therefore $l = -k$. Now $y^{-1}g^k y = g^{-k}$ implies

$$y^{-2}g^k y^2 = y^{-1}g^{-k}y = (y^{-1}g^k y)^{-1} = g^k;$$

i.e. y^2 commutes with g^k though y does not. It follows from Theorem 2 that each non-trivial element in one of the factors is conjugate to an element f in one of the factors G_i such that $C(f, A) = C(f, G_i)$. Therefore by Lemma 4 A is an R-group, and in an R-group, if x and y^n (n a non-zero integer) commute then x and y commute (see [1]). Thus we have a contradiction.

d. In all other cases either g^k is conjugate to an element in one of the factors or to an element cyclically reduced of length at least 2; say $z^{-1}g^k z \in G_i$ or $z^{-1}g^k z$ is cyclically reduced of length at least 2. $y^{-1}g^k y = g^l$ implies $(z^{-1}yz)^{-1}(z^{-1}gz)^k(z^{-1}yz) = (z^{-1}gz)^l$, and by a or b or c, $k = l$.

We will now restate and prove Theorem 3.

THEOREM 3. *Let $A = \{G_1 * G_2; U\}$ where G_1 and G_2 are in $\mathscr{P}$. Suppose that if $u \in U$, $u \neq 1$, then either*

$$\{x \in G_1 \mid x^{-1}ux \in U\} = U \quad \text{or} \quad \{x \in G_2 \mid x^{-1}ux \in U\} = U.$$

Then A is in $\mathscr{P}$.

PROOF. It follows from Theorem 2 that each non-trivial element h in one of the factors is conjugate to an element f in one of the factors G_i such that $C(f, A) = C(f, G_i)$: for if, for example, $h \in G_1$, then either h is not conjugate in G_1 to an element in U so that $C(h, A) = C(h, G_1)$ or else h is conjugate to an element $u \in U$ and $C(u, A) = C(u, G_i)$ for $i = 1$ or $i = 2$. Therefore by Lemma 4

1. A is an R-group, and

2. (a) If $h \in A$ and h does not have an n^{th} root in A for some natural number n, then $C(h, A)$ is isomorphic to a subgroup of Γ.

And by Lemma 5

(b) If $h \in A$ and h does not have an n^{th} root in A for some natural number n and $f^{-1}h^k f = h^l$ for some $f \in A$, then $k = l$.

2

In this section it is shown that every countable $\mathscr{D}$-group A can be embedded in a 3-generator $\mathscr{D}$-group A'; if A is a finitely related $\mathscr{D}$-group, say given by n defining relations, then the $\mathscr{D}$-group A' can be chosen so as to be defined by n relations (Theorem 4). It follows (Theorem 5) that there are at least continuously many non-isomorphic 3-generator $\mathscr{D}$-groups. Now every countable $\mathscr{D}$-group is a homomorphic image of a fixed free $\mathscr{D}$-group F of countably infinite rank. Since F is itself countable, the number of subsets of F is $\mathfrak{c}$, the cardinality of the continuum, and so the number of ideals of F can be no more than $\mathfrak{c}$. Consequently, there are at most $\mathfrak{c}$ countable $\mathscr{D}$-groups and, in particular, there are at most $\mathfrak{c}$ 3-generator $\mathscr{D}$-groups. Putting this together with Theorem 5 yields:

THEOREM 5'. *The number of* 3*-generator* (*and indeed the number of countably generated*) $\mathscr{D}$*-groups is the power of the continuum.*

The number of 2-generator $\mathscr{D}$-groups is still unknown.

G. Higman, B. H. Neumann, and H. Neumann have shown that any countable group G can be embedded in a 2-generator group G', and that if G is defined by n relations, then G' can be chosen so as to be defined by n relations [4], and the proof of Theorem 4 utilizes in part their embedding procedure. The proof of Theorem 4 was greatly simplified by a suggestion of Professor Baumslag. It is not known whether every countable $\mathscr{D}$-group can be embedded in a 2-generator $\mathscr{D}$-group.

THEOREM 4. *Every countable* $\mathscr{D}$*-group* A *can be embedded in a* 3*-generator* $\mathscr{D}$*-group* A'. *Moreover, if the* $\mathscr{D}$*-group* A *is finitely related, say by* n *defining relations, then the* $\mathscr{D}$*-group* A' *can be chosen so as to be finitely related, also given by* n *relations.*

PROOF. Suppose $S = \{a_1, a_2, a_3, \cdots\}$ is a set of generators of the $\mathscr{D}$-group A, that is, $A = \mathscr{D}\text{-}gp(a_1, a_2, a_3, \cdots)$. We may assume that $a_i \neq 1$ for any i and that $a_i \neq a_j$, $a_i \neq a_j^{-1}$ for $i \neq j$. For if S fails to satisfy these conditions, there is some subset S' of S that $\mathscr{D}$-generates A and that does satisfy these conditions; we may replace S by S'. We may also assume that S is infinite. For if S is finite, we will consider $(A * F)^*$ instead of A, where F is a free $\mathscr{D}$-group of countably infinite rank and $(A * F)^*$ is the free $\mathscr{D}$-closure of $A * F$. This makes sense because the free product of two $\mathscr{D}$-groups is in $\mathscr{P}$, by Theorem 3. The mapping that sends each element of A into 1 and each element of F onto itself can be extended to a homomorphism of $A * F$; any homomorphism of $A * F$ into a $\mathscr{D}$-group can be extended to a homomorphism of $(A * F)^*$; therefore F is a homomorphic image of $(A * F)^*$. It follows that $(A * F)^*$ cannot be finitely $\mathscr{D}$-generated because F, a homomorphic image, is not. Notice that the number of relations needed to define A with the set S' is no more than the number of relations needed to define A with the set S; and in replacing A by $(A * F)^*$, the number of relations has not been increased.

Let F_1 be a free group, freely generated by x and y, let F_2 be a free group freely generated by u and v. We wish to consider a certain generalized free product of F_1 and $F_2 * A$.

The subgroup of F_1 generated by $x, y^{-1}xy, y^{-2}xy^2, y^{-3}xy^3, \cdots$ is freely generated by these elements. The subgroup of $F_2 * A$ generated by u, $v^{-1}ua_1v,\ v^{-2}ua_2v^2,\ v^{-3}ua_3v^3, \cdots$ is freely generated by these elements. For if it is not, there is some non-trivial word $R(u, v^{-1}ua_1v, \cdots, v^{-m}ua_mv^m)$ in these generators that is equal to 1. But if φ is the endomorphism of $F_2 * A$ that is the identity on F_2 and maps every element of A onto 1, we have

$$1 = 1\varphi = R(u, v^{-1}ua_1v, \cdots, v^{-m}ua_mv^m)\varphi = R(u, v^{-1}uv, \cdots, v^{-m}uv^m),$$

which is impossible since the subgroup generated by $u, v^{-1}uv, v^{-2}uv^2, \cdots$ is freely generated by these elements.

Therefore, we may form

$$H = \{F_1 * (F_2 * A); W\}$$

where

$$W = gp(x, y^{-1}xy, y^{-2}xy^2, \cdots) = gp(u, v^{-1}ua_1v, v^{-2}ua_2v^2, \cdots)$$

and the identifications

$$x = u \text{ and } y^{-i}xy^i = v^{-i}ua_iv^i \text{ for } i = 1, 2, \cdots$$

are made.

We will establish later that H is in $\mathscr{P}$. It follows that H^*, the free $\mathscr{D}$-closure of H, is a $\mathscr{D}$-group containing A. We now show that H^* is a 3-generator $\mathscr{D}$-group: we show that

$$H^* = \mathscr{D}\text{-}gp(x, y, v).$$

Now $x = u$, so $\mathscr{D}\text{-}gp(x, y, v) \ni u$; therefore $\mathscr{D}\text{-}gp(x, y, v)$ contains both F_1 and F_2. $y^{-i}xy^i = v^{-i}ua_iv^i$ implies that

$$a_i = u^{-1}v^iy^{-i}xy^iv^{-i} = x^{-1}v^iy^{-i}xy^iv^{-i};$$

hence $\mathscr{D}\text{-}gp(x, y, v)$ contains $\{a_1, a_2, \cdots\}$ — therefore $\mathscr{D}\text{-}gp(x, y, v)$ contains $\mathscr{D}\text{-}gp(a_1, a_2, \cdots) = A$. Since $\mathscr{D}\text{-}gp(x, y, v)$ contains F_1, F_2, and A, it contains all of H and therefore contains $\mathscr{D}\text{-}gp(H) = H^*$.

We shall now show that if

$$A = \mathscr{D}\text{-}gp\ \langle a_1, a_2, \cdots; R_1(a_1, \cdots, a_{m_1}) = 1,\ R_2(a_1, \cdots, a_{m_2}) = 1, \cdots\rangle,$$

then

$$\begin{aligned} H^* = \mathscr{D}\text{-}gp\langle x, y, v;\ & R_1(x^{-1}vy^{-1}xyv^{-1}, \cdots, x^{-1}v^{m_1}y^{-m_1}xy^{m_1}v^{-m_1}) = 1, \\ & R_2(x^{-1}vy^{-1}xyv^{-1}, \cdots, x^{-1}v^{m_2}y^{-m_2}xy^{m_2}v^{-m_2}) = 1, \cdots\rangle. \end{aligned}$$

To see this let

$$B = \mathscr{D}\text{-}gp\langle X, Y, V;\ R_1(X^{-1}VY^{-1}XYV^{-1}, \cdots, X^{-1}V^{m_1}Y^{-m_1}XY^{m_1}V^{-m_1}) = 1,$$
$$R_2(X^{-1}VY^{-1}XYV^{-1}, \cdots, X^{-1}V^{m_2}XY^{m_2}V^{-m_2}) = 1, \cdots\rangle.$$

There is a homomorphism φ of B into H^* determined by $X\varphi = x$, $Y\varphi = y$, $V\varphi = v$ by the analogue of von Dyck's theorem for $\mathscr{D}$-groups since

$$R_j((X\varphi)^{-1}V\varphi(Y\varphi)^{-1}X\varphi Y\varphi(V\varphi)^{-1}, \cdots,$$
$$(X\varphi)^{-1}(V\varphi)^{m_j}(Y\varphi)^{-m_j}X\varphi(Y\varphi)^{m_j}(V\varphi)^{-m_j})$$
$$= R_j(x^{-1}vy^{-1}xyv^{-1}, \cdots, x^{-1}v^{m_j}y^{-m_j}xy^{m_j}v^{-m_j}) = R_j(a_1, \cdots, a_{m_j}) = 1$$

for $j = 1, 2, \cdots$.

Let ψ_1 and ψ_2 be the homomorphisms of the free groups F_1 and F_2, respectively, into B determined by

$$x\psi_1 = X, \quad y\psi_1 = Y,$$
$$u\psi_2 = X, \quad v\psi_2 = V.$$

There is a homomorphism ψ_3 of the $\mathscr{D}$-group A into the $\mathscr{D}$-group B such that

$$a_i\psi_3 = X^{-1}V^iY^{-i}XY^iV^{-i} \quad \text{for} \quad i = 1, 2, \cdots$$

by von Dyck's theorem for $\mathscr{D}$-groups because

$$R_j(a_1\psi_3, \cdots, a_{m_j}\psi_3) = 1, \qquad j = 1, 2, \cdots.$$

There exists a homomorphism ψ of the free product $F_2 * A$ into B that coincides with ψ_2 on F_2 and with ψ_3 on A. A straightforward verification will show that ψ_1 and ψ coincide on

$$x = u, y^{-1}xy = v^{-1}ua_1v, y^{-2}xy^2 = v^{-2}ua_2v^2, \cdots,$$

the generators of W; hence ψ_1 and ψ coincide on W. Therefore there is a homomorphism η of $H = \{F_1 * (F_2 * A); W\}$ into B that agrees with ψ_1 on F_1 and with ψ on $F_2 * A$. Any homomorphism of H into a $\mathscr{D}$-group can be extended to a homomorphism of H^*. So η can be extended to a homomorphism η^* of H^* into B.

$$X\varphi\eta^* = x\eta^* = x\eta = x\psi_1 = X,$$
$$Y\varphi\eta^* = y\eta^* = y\eta = y\psi_1 = Y, \text{ and}$$
$$V\varphi\eta^* = v\eta^* = v\eta = v\psi \ = v\psi_2 = V.$$

Since $\varphi\eta^*$ is the identity map on the $\mathscr{D}$-generators of B, $\varphi\eta^*$ is the identity mapping of B. Since φ is onto, it follows that φ is an isomorphism, and so H^* has the presentation we claimed.

Therefore, if the $\mathscr{D}$-group A is given by n defining relations

$R_1(a_1, \cdots, a_{m_1}), \cdots, R_n(a_1, \cdots, a_{m_n})$, the $\mathscr{D}$-group H^* is presented on 3 generators and n relations.

It remains to verify that H is in $\mathscr{P}$. Now any free group is in $\mathscr{P}$, so F_1 and F_2 are in $\mathscr{P}$; also any $\mathscr{D}$-group is in $\mathscr{P}$. $F_2 * A$ is therefore in $\mathscr{P}$, being the free product of two groups in $\mathscr{P}$. These statements follow from Theorem 3, but a more direct proof can be found in [1]. The following lemma shows that $\{x \in F_2 * A \mid x^{-1}wx \in W\} = W$ for each non-trivial element $w \in W$. Therefore, by Theorem 3, $H = \{F_1 * (F_2 * A); W\}$ is in $\mathscr{P}$. The lemma completes the proof of the theorem.

LEMMA. *Let F be a free group freely generated by u and v. Let A be a group and $\{a_1, a_2, \cdots\}$ be a subset of A such that $a_i \neq 1$ for any i and $a_i \neq a_j$, $a_i \neq a_j^{-1}$ for any $i \neq j$. Let*

$$G = F * A$$

and let

$$W = gp(u, v^{-1}ua_1v, v^{-2}ua_2v^2, \cdots).$$

If $1 \neq w \in W$ and $gwg^{-1} \in W$ for $g \in G$, then $g \in W$.

PROOF. As we have already pointed out, W is freely generated by u, $v^{-1}ua_1v, v^{-2}ua_2v^2, \cdots$. Therefore any element $w \in W$ can be written uniquely as

$$\begin{aligned} w &= u^{k_1}(v^{-i_1}ua_{i_1}v^{i_1})^{m_1}u^{k_2}(v^{-i_2}ua_{i_2}v^{i_2})^{m_2}\cdots u^{k_n}(v^{-i_n}ua_{i_n}v^{i_n})^{m_n}u^{k_{n+1}} \\ &= u^{k_1}v^{-i_1}(ua_{i_1})^{m_1}v^{i_1}u^{k_2}v^{-i_2}(ua_{i_2})^{m_2}v^{i_2}\cdots u^{k_n}v^{-i_n}(ua_{i_n})^{m_n}v^{i_n}u^{k_{n+1}} \end{aligned}$$

where the i_j are positive integers, the m_j are non-zero integers, the k_j are integers, and if $k_j = 0$ then $i_{j-1} \neq i_j$. Since $a_i \neq 1$ for any i, it can be seen by inspection that if $w_1w_2\cdots w_l$ is the free product normal form for w, then

$$\begin{array}{llll} w_1 = u^{k_1} & \text{and} & l = 1 & \text{if} \quad n = 0, \\ w_1 = u^{k_1}v^{-i_1}u & \text{and} & w_2 = a_{i_1} & \text{if} \quad m_1 > 0, \\ w_1 = u^{k_1}v^{-i_1} & \text{and} & w_2 = a_{i_1}^{-1} & \text{if} \quad m_1 < 0. \end{array}$$

We wish to show that if $1 \neq w \in W$, $g \in G$ and $gwg^{-1} \in W$, then $g \in W$; so let us suppose that this is false. Let

$$T = \{g \in G - W \mid \exists\, w \in W, w \neq 1, \text{ such that } gwg^{-1} \in W\},$$

and let

$$p = \min\{\lambda(g) \mid g \in T\}.$$

Let g be an element of length p in T, let $1 \neq w \in W$ be such that $gwg^{-1} \in W$, and let

$$\begin{aligned} g &= g_1g_2\cdots g_p \\ w &= w_1w_2\cdots w \end{aligned}$$

be the normal forms for g and w.

https://doi.org/10.1017/S1446788700004201 Published online by Cambridge University Press

First let us notice that if $p \geqq 2$, then the first two terms, g_1 and g_2, of g are not the same as the first two terms w_1' and w_2' of any word $w' \in W$. For if this were false then either $g_1 = u^k v^{-i} u$ and $g_2 = a_i$ (for some i, k) or $g_1 = u^k v^{-i}$ and $g_2 = a_i^{-1}$ (for some i, k). Thus suppose

$$g_1 = u^k v^{-i} u \quad \text{and} \quad g_2 = a_i.$$

Set

$$g' = (u^k v^{-i} u a_i v^i)^{-1} g;$$

$g' \notin W$ since $u^k v^{-i} u a_i v^i \in W$ and $g \notin W$. Now

$$g' w g'^{-1} = (u^k v^{-i} u a_i v^i)^{-1} (g w g^{-1}) (u^k v^{-i} u a_i v^i),$$

and this element is in W because $gwg^{-1} \in W$ and $(u^k v^{-i} u a_i v^i) \in W$. $gwg^{-1} \neq 1$ because $w \neq 1$. Thus $g' \in T$ — but $g' = v^{-i}$ if $p = 2$ and $g' = v^{-i} g_3 \cdots g_p$ if $p > 2$; in either case $\lambda(g') < p$, which is a contradiction. The supposition that $g_1 = u^k v^{-i}$ and $g_2 = a_i^{-1}$ leads in the same way by consideration of the element $g' = (v^{-i} u a_i v^i u^{-k}) g$ to a contradiction of the minimality of p.

Now g^{-1} is also an element of length p in T: for $g^{-1}(gwg^{-1})g = w \in W$, $gwg^{-1} \in W$ by assumption, $gwg^{-1} \neq 1$ because $w \neq 1$, $g^{-1} \notin W$ because $g \notin W$, and $\lambda(g^{-1}) = \lambda(g) = p$. So if $p \geqq 2$ then g_p^{-1} and g_{p-1}^{-1} are not the same as the first two terms of any word in W.

It follows that if $p \geqq 2$ it cannot be that g_2 or g_2^{-1} is left uncancelled and unamalgamated in the product

$$gwg^{-1} = g_1 g_2 \cdots g_p w_1 w_2 \cdots w_l g_p^{-1} \cdots g_2^{-1} g_1^{-1}.$$

For if g_2 is left uncancelled and unamalgamated, then g_1 and g_2 are the first two terms of gwg^{-1}, an element in W; if g_2^{-1} is left uncancelled and unamalgamated, then g_1 and g_2 are the first two terms of $(gwg^{-1})^{-1}$, which is in W. Also, if $p \geqq 2$, $l \geqq 2$, and $g_p = w_1^{-1}$, then $g_{p-1} \neq w_2^{-1}$; and if $p \geqq 2$, $l \geqq 2$, and $g_p = w_l$, then $g_{p-1} \neq w_{l-1}$ (because w_l^{-1} and w_{l-1}^{-1} are the first two terms of w^{-1}).

The first and last terms of any element in W lie in F. It follows that $g_p \in F$. For suppose $g_p \in A$. Then in the product

$$gwg^{-1} = g_1 g_2 \cdots g_p w_1 w_2 \cdots w_l g_p^{-1} \cdots g_2^{-1} g_1^{-1}$$

there is no cancellation and no amalgamation. Since g_2 cannot be left unaffected, this implies $p = 1$ and $g = g_p \in A$. Therefore the first term of gwg^{-1} is in A, which is impossible because $gwg^{-1} \in W$.

We have already observed that g^{-1} is also an element of length p in T, and it follows that g_1^{-1} and so also g_1 is in F.

Because both g and w begin and end with terms in F, $\lambda(w)$ and $\lambda(g)$

https://doi.org/10.1017/S1446788700004201 Published online by Cambridge University Press

are odd. We will consider separately various cases depending on $\lambda(w) = l$ and $\lambda(g) = p$.

(a) $l = 1$. In this case $w = u^k$, $k \neq 0$. Thus

$$gwg^{-1} = g_1 \cdots g_{p-1}(g_p u^k g_p^{-1})g_{p-1}^{-1} \cdots g_1^{-1}.$$

$u^k \neq 1$ implies $g_p^{-1} u_k g_p \neq 1$. So $g_1, \cdots, g_{p-1}$ are left uncancelled and unamalgamated; hence $p \leqq 2$ (because g_2 cannot be left unaffected). $p \neq 2$ because p is odd. Therefore, $p = 1$, and $g = g_1 \in F$; so $gwg^{-1} \in F$. Now $gwg^{-1} \in F \cap W$ means $gwg^{-1} = u^m$ for some integer m. So we have

$$gu^k g^{-1} = u^m.$$

Such an equation in a free group implies $k = m$ and so $g \in C(u^k, F)$. Since u belongs to a set of free generators of F,

$$C(u^k, F) = gp(u).$$

Thus $g \in gp(u) < W$, which is a contradiction.

(b) $l = 3$. $w = w_1 w_2 w_3$.

First we will establish that $w_3 \neq w_1^{-1}$. Now either $w_1 = u^k v^{-i} u$ and $w_2 = a_i$ or $w_1 = u^k v^{-i}$ and $w_2 = a_i^{-1}$. In the first case

$$w_1 w_2 w_1^{-1} = u^k v^{-i} u a_i u^{-1} v^i u^{-k},$$

and if this were in W then the element $(u^k v^{-i} u a_i v^i)^{-1} w_1 w_2 w_1^{-1} = v^{-i} u^{-1} v^i u^{-k}$ would also be in W. But the only elements of length 1 in W are powers of u. In the second case

$$w_1 w_2 w_1^{-1} = u^k v^{-i} a_i^{-1} v^i u^{-k},$$

and if this were in W then also $(v^{-i} u a_i v^i u^{-k}) w_1 w_2 w_1^{-1} = v^{-i} u v^i u^{-k}$ would be in W, but it is not. Hence $w_3 \neq w_1^{-1}$, as we claimed.

We have

$$gwg^{-1} = g_1 \cdots g_{p-1}(g_p w_1) w_2 (w_3 g_p^{-1}) g_{p-1}^{-1} \cdots g_1^{-1}.$$

Either $g_p \neq w_1^{-1}$ or $g_p \neq w_3$; for convenience we may assume $g_p \neq w_1^{-1}$ (otherwise instead of g, w, and gwg^{-1} we could consider g, w^{-1}, and $gw^{-1}g^{-1}$). Even if $g_p = w_3$, the term w_2 is at most amalgamated, so the first p terms of gwg^{-1} are $g_1, \cdots, g_{p-1}$, $(g_p w_1)$; therefore $p \leqq 2$. But $p \neq 2$ because p is odd, so $p = 1$. Therefore $g = g_p \in F$, and

$$gwg^{-1} = (gw_1) w_2 (w_3 g^{-1}),$$

where gw_1 and $w_3 g^{-1}$ are in F and $gw_1 \neq 1$.

Thus the first two terms of gwg^{-1} are gw_1 and w_2. Now, either $w_1 = u^k v^{-i} u$ and $w_2 = a_i$ or $w_1 = u^k v^{-i}$ and $w_2 = a_i^{-1}$. Suppose $w_1 = u^k v^{-i} u$ and $w_2 = a_i$.

Because $a_i \neq a_j^{-1}$ for any j and $a_i \neq a_j$ for $i \neq j$, the fact that the second term of gwg^{-1} is a_i implies that the first term of gwg^{-1} is $u^m v^{-i} u$ for some m. Therefore

$$u^m v^{-i} u = gw_1 = gu^k v^{-i} u;$$

hence

$$g = u^{m-k},$$

which is in W, a contradiction. So it must be that $w_1 = u^k v^{-i}$ and $w_2 = a_i^{-1}$. That the second term of gwg^{-1} is a_i^{-1} implies that the first term of gwg^{-1} is $u^m v^{-i}$ for some m. Hence

$$u^m v^{-i} = gw_1 = gu^k v^{-i},$$

and so

$$g = u^{m-k},$$

which is an element of W, and this again is a contradiction.

(c) $l \geqq 5$, $p = 1$. In this case $g = g_1 \in F$.

$$gwg^{-1} = (gw_1)w_2 \cdots w_{l-1}(w_l g^{-1}).$$

If $g = w_1^{-1}$, than the first term of gwg^{-1} is w_2, which is in A; this is impossible; so $g \neq w_1^{-1}$. Therefore, as in the case just examined, the first term of gwg^{-1} is gw_1 and the second is w_2; as before this leads to the conclusion $g = u^{m-k}$ for some integers m and k, which is a contradiction.

(d) $l \geqq 5$, $p \geqq 3$. Let us assume in addition that we have chosen w to be of minimal length among all non-trivial elements w' in W such that $g'w'g'^{-1} \in W$ for any element g' of length p not in W.

$$gwg^{-1} = g_1 \cdots g_{p-1}(g_p w_1)w_2 \cdots w_{l-1}(w_l g_p^{-1})g_{p-1}^{-1} \cdots g_1^{-1}.$$

If $g_p \neq w_1^{-1}$, then g_{p-1} is uncancelled and unamalgamated; since $p-1 \geqq 2$, this means g_2 is uncancelled and unamalgamated — but we have shown that this cannot happen. Likewise, if $g_p \neq w_l$, then g_{p-1}^{-1} is left unaffected and so also g_2^{-1} is left unaffected — but we have shown that this cannot happen.

Therefore $g_p = w_1^{-1} = w_l$. This means that g_{p-1} is amalgamated with w_2, w_{l-1} is amalgamated with g_{p-1}^{-1}, and the other terms are unaffected because $l \geqq 5$. That g_{p-2} is unaffected implies $p-2 < 2$ and so $p = 3$. Therefore

$$gwg^{-1} = g_1 g_2 g_3 w_1 w_2 \cdots w_{l-1} w_l g_3^{-1} g_2^{-1} g_1^{-1} = g_1(g_2 w_2)w_3 \cdots (w_{l-1} g_2^{-1})g_1^{-1}.$$

Either $w_1 w_2 = u^k v^{-i} u a_i$ or $w_1 w_2 = u^k v^{-i} a_i^{-1}$. If $w_1 w_2 = u^k v^{-i} u a_i$, set $z = w_1 w_2 v^i = u^k v^{-i} u a_i v^i$, which is in W. Let $w' = z^{-1} w z$; w' is also in W. We will show that the length of w' is shorter than the length of w and that there exists g' of length p not in W such that $g'w'g'^{-1} \in W$. Now

$$w' = v^{-i}w_2^{-1}w_1^{-1}w_1w_2 \cdots w_{l-1}w_lw_1w_2v^i = (v^{-i}w_3) \cdots (w_{l-1}w_2)v^i,$$

since $w_l = w_1^{-1}$. So $\lambda(w') \leqq \lambda(w)-2$, since v^{-i} and w_3 lie in the same factor and w_{l-1} and w_2 lie in the same factor. That $w \neq 1$ implies that $w' \neq 1$. Let $g' = gz$; $g' \notin W$. However,

$$g'w'g'^{-1} = (gz)z^{-1}wz(gz)^{-1} = gwg^{-1} \in W.$$

Now

$$g' = g_1g_2g_3w_1w_2v^i = g_1(g_2w_2)v^i,$$

because $g_3 = w_1^{-1}$; therefore $\lambda(g') = 3 = p$. This, however, is in contradiction to the minimality of w.

If $w_1w_2 = u^kv^{-i}a_i^{-i}$, set $z = w_1w_2u^{-1}v^i$; by the same argument one is again led to a contradiction.

In every possible case we have arrived at a contradiction; so there can be no element $g \in G-W$ such that $gwg^{-1} \in W$ for $1 \neq w \in W$.

THEOREM 5. *There are at least continuously many non-isomorphic 3-generator $\mathscr{D}$-groups.*

PROOF: Let α be a subset of the natural numbers containing 1. For each such set α we will construct a $\mathscr{D}$-group G_α^* and then by the procedure of Theorem 4 embed G_α^* in a 3-generator $\mathscr{D}$-group H_α^*. We will show that H_α^* is not isomorphic to H_β^* if $\alpha \neq \beta$; this will prove the theorem since there are continuously many such sets α.

Now let

$$G_\alpha = \prod_{k\in\alpha} * \Gamma^k$$

where Γ^k is the direct product of k copies of Γ. Γ^k is a $\mathscr{D}$-group and so is in $\mathscr{P}$. The free product of two groups in $\mathscr{P}$ is itself a group in $\mathscr{P}$, as a special case of Theorem 3, and by an induction so is the free product of countably many groups in $\mathscr{P}$ itself a group in $\mathscr{P}$. So G_α is in $\mathscr{P}$ and can be embedded in the $\mathscr{D}$-group G_α^*, its free $\mathscr{D}$-closure.

By Theorem 2 (and again an induction), if $1 \neq g \in G_\alpha$ then either $C(g, G_\alpha)$ is infinite cyclic or $C(g, G_\alpha)$ is isomorphic to $C(h, \Gamma^k)$ for some $k \in \alpha$. $C(h, \Gamma^k) = \Gamma^k$; so if $1 \neq g \in G_\alpha$ then either $C(g, G_\alpha)$ is infinite cyclic or $C(g, G_\alpha)$ is isomorphic to Γ^k for some $k \in \alpha$. It follows that the elements of G_α having n^{th} roots for every n are just those elements having centralizers isomorphic to Γ^k, $k \in \alpha$.

By Theorem 1 if $1 \neq g \in G_\alpha$ and g has an n^{th} root in G_α for every n, then $C(g, G_\alpha^*) = C(g, G_\alpha)$; in this case $C(g, G_\alpha)$ is isomorphic to Γ^k for some $k \in \alpha$, so $C(g, G_\alpha^*)$ is isomorphic to Γ^k for some $k \in \alpha$. If $1 \neq g \in G_\alpha^*$ and g is conjugate in G_α^* to an element $h \in G_\alpha$ having all its roots in G_α, then $C(g, G_\alpha^*)$ is isomorphic to $C(h, G_\alpha^*)$ and this is isomorphic to Γ^k for

$k \in \alpha$. Again by Theorem 1 if $g \in G_\alpha^*$ and g is not conjugate in G_α^* to an element of G_α having all its roots in G_α, then $C(g, G_\alpha^*)$ is isomorphic to Γ. $\Gamma = \Gamma^1$, and $1 \in \alpha$. Thus we have shown that if $1 \neq g \in G_\alpha^*$, then $C(g, G_\alpha^*)$ is isomorphic to Γ^k with $k \in \alpha$.

G_α^* is countable because it is countably generated. Let us recall that G_α^* can be embedded in a 3-generator $\mathscr{D}$-group H_α^*, the free $\mathscr{D}$-closure of a group H_α:

$$H_\alpha = \{F_1 * (F_2 * G_\alpha^*); W\},$$

(see Theorem 4) where F_1, F_2, and W are free groups, and if $1 \neq w \in W$ then $\{x \in F_2 * G_\alpha^* \mid x^{-1}wx \in W\} = W$. The centralizer in F_2 of each non-trivial element in F_2 is infinite cyclic, and the centralizer in G_α^* of a non-trivial element in G_α^* is isomorphic to Γ^k, $k \in \alpha$. Therefore, by Theorem 2, the centralizer of any non-trivial element in $F_2 * G_\alpha^*$ is either infinite cyclic or isomorphic to Γ^k, $k \in \alpha$. The centralizer of a non-trivial element of F_1 is infinite cyclic. Since $\{x \in F_2 * G_\alpha^* \mid x^{-1}wx \in W\} = W$ for $1 \neq w \in W$, it follows from Theorem 2 that the centralizer of a non-trivial element in H_α is either infinite cyclic or isomorphic to Γ^k, $k \in \alpha$. It follows that the elements of H_α having n^{th} roots for every n are just those elements having centralizers isomorphic to Γ^k with $k \in \alpha$.

H_α^* is the free $\mathscr{D}$-closure of a group H_α in $\mathscr{P}$, and by Theorem 1, we see that: if $1 \neq g \in H_\alpha^*$ and g is conjugate to an element $h \in H_\alpha$ having n^{th} roots in H_α for every n, then

$$C(g, H_\alpha^*) \simeq C(h, H_\alpha^*) = C(h, H_\alpha) \simeq \Gamma^k, \text{ where } k \in \alpha,$$

while if $1 \neq g \in H_\alpha^*$ and g is not conjugate to an element $h \in H_\alpha$ having n^{th} roots in H_α for every n, then

$$C(g, H_\alpha^*) \simeq \Gamma.$$

Since $1 \in \alpha$, in any case $C(g, H_\alpha^*)$ is isomorphic to Γ^k for some $k \in \alpha$, provided $g \neq 1$.

Now suppose α and β are two different subsets of the natural numbers containing 1. We wish to show that H_α^* is not isomorphic to H_β^*. Either α contains a number not in β or β contains a number not in α; for convenience let us suppose $m \in \alpha$, $m \notin \beta$. Now H_β^* contains no element g such that $C(g, H_\beta^*)$ is isomorphic to Γ^m; so if we can show that there is an element $g \in H_\alpha^*$ such that $C(g, H_\alpha^*)$ is isomorphic to Γ^m, then H_α^* cannot be isomorphic to H_β^*.

Now $\Gamma^m < G_\alpha < H_\alpha^*$. Let g be any non-trivial element in Γ^m. $C(g, G_\alpha) = C(g, \Gamma^m) = \Gamma^m$, by Theorem 2. g has an n^{th} root in G_α for every n, so by Theorem 1 $C(g, G_\alpha^*) = C(g, G_\alpha) = \Gamma^m$. Again using Theorem 2, $C(g, F_2 * G_\alpha^*) = C(g, G_\alpha^*) = \Gamma^m$.

$H_\alpha = \{F_1 * (F_2 * G_\alpha^*); W\}$, and by Theorem 2 either $C(g, H_\alpha) = C(g, F_2 * G_\alpha^*)$ or g is conjugate in $F_2 * G_\alpha^*$ to an element in W. But it cannot be that g is conjugate in $F_2 * G_\alpha^*$ to an element $w \in W$. For if g is conjugate to w, then $w \neq 1$ and so by Theorem 2 $C(w, H_\alpha) = C(w, F_1)$, which is infinite cyclic because F_1 is a free group. However g is conjugate to w implies that $C(g, H_\alpha)$ is also infinite cyclic, and this is impossible because $C(g, H_\alpha)$ contains $C(g, F_2 * G_\alpha^*) = \Gamma^m$. Therefore $C(g, H_\alpha) = C(g, F_2 * G_\alpha^*) = \Gamma^m$. Since g has an n^{th} root in H_α for every natural number n, $C(g, H_\alpha^*) = C(g, H_\alpha) = \Gamma^m$ by Theorem 1. This shows that H_α^* is not isomorphic to H_β^* if $\alpha \neq \beta$.

3

In 1951 Graham Higman gave the first example of a finitely generated infinite simple group [3]. This section will be concerned with a similar example for $\mathscr{D}$-groups. We will show, by a non-constructive proof, that there is a 5-generator non-abelian simple $\mathscr{D}$-group, that is to say a $\mathscr{D}$-group with no proper ideals.

We begin by constructing five isomorphic copies of the following group

$$G = gp\,\langle \Gamma, x; x^{-1}zx = z^2 \text{ for all } z \in \Gamma \rangle.$$

G is a splitting extension of Γ by an infinite cyclic group generated by x. Now let G_i be an isomorphic copy of G for $i = 1, 2, 3, 4, 5$; if $g \in G$, the corresponding element of G_i will be denoted by g_i. We choose now arbitrarily an element y in Γ, $y \neq 1$. The order of y is infinite, and so we may form the generalized free products

$$\begin{aligned} H &= \{G_1 * G_2; y_1 = x_2\}, \\ K &= \{G_3 * G_4; y_3 = x_4\}, \text{ and} \\ L &= \{K * G_5; y_4 = x_5\}. \end{aligned}$$

Now, in H,

$$gp(x_1, y_2) = gp(x_1) * gp(y_2),$$

(see [5] for a proof); therefore $gp(x_1, y_2)$ is a free group freely generated by x_1 and y_2. Similarly, the subgroup of L generated by x_3 and y_5 is a free group freely generated by these elements. Therefore, we may form

$$M = \{H * L; x_1 = y_5, y_2 = x_3\}.$$

We show later that M is in $\mathscr{P}$ and therefore can be embedded in M^*, its free $\mathscr{D}$-closure. The group M is generated by the elements $x_1 = y_5$, $x_2 = y_1$, $x_3 = y_2$, $x_4 = y_3$, and $x_5 = y_4$, together with their roots; therefore the $\mathscr{D}$-group M^* is generated by x_1, x_2, x_3, x_4 and x_5. For convenience we put

$$a = x_1 = y_5, \quad b = x_2 = y_1, \quad c = x_3 = y_2,$$
$$d = x_4 = y_3, \text{ and } e = x_5 = y_4.$$

Now since $y \in \Gamma$, $x^{-1}yx = y^2$; hence $x_i^{-1}y_ix_i = y_i^2$ for $i = 1, 2, 3, 4, 5$. Therefore the following relations hold among these generators of M^*:

$$a^{-1}ba = b^2, \quad b^{-1}cb = c^2, \quad c^{-1}dc = d^2, \quad d^{-1}ed = e^2, \quad e^{-1}ae = a^2.$$

By Zorn's lemma we may choose in M^* a maximal ideal not containing a; let I be such an ideal. Set $A = M^*/I$. It is this $\mathscr{D}$-group A that turns out to be non-abelian and simple. A is non-abelian because

$$(eI)^{-1}(aI)(eI) = (aI)^2, \text{ and } aI \neq I.$$

Now if A were not simple, A would contain a proper ideal, and so M^* would have a proper ideal J properly containing I. J properly contains I implies that $a \in J$, because of the choice of I. Now, for $g \in M^*$, let $\tilde{g} = gJ$; in M^*/J we have

$$\tilde{a} = 1 \Rightarrow \tilde{b} = \tilde{a}^{-1}\tilde{b}\tilde{a} = \tilde{b}^2 \Rightarrow \tilde{b} = 1.$$

Similarly

$$\tilde{b} = 1 \Rightarrow \tilde{c} = 1 \Rightarrow \tilde{d} = 1 \Rightarrow \tilde{e} = 1.$$

Thus, the $\mathscr{D}$-group M^*/J is trivial because its generators, $\tilde{a}$, $\tilde{b}$, $\tilde{c}$, $\tilde{d}$ and $\tilde{e}$, are all trivial. Therefore, J coincides with M^*. Thus A contains no proper ideal and so is simple.

It remains to verify that M is in $\mathscr{P}$; this is the difficult part of the proof, and we will continue by a number of lemmas.

Lemma 1. *$G = gp\langle \Gamma, x; x^{-1}zx = z^2$ for all z in $\Gamma\rangle$ is in $\mathscr{P}$.*

Proof. G is a splitting extension of Γ by an infinite cycle generated by x, since $z \to z^2$ for z in Γ is an automorphism of Γ. $x^{-1}zx = z^2$ implies $x^{-k}zx^k = z^{2^k}$ for k any positive integer, and hence $x^kzx^{-k} = z^{2^{-k}}$. So for any integer k, $x^{-k}zx^k = z^{2^k}$.

Choose $y \in \Gamma$, $y \neq 1$. Every element $g \in G$ can be written uniquely as

$$g = x^ky^r, \ k \text{ an integer, } r \text{ rational.}$$

First, we will show that G is an R-group, and to this end we now investigate the n^{th} roots of x^ky^r. Suppose that $(x^ly^s)^n = x^ky^r$, n a natural number.

$$\begin{aligned}(x^ly^s)^n &= \overbrace{(x^ly^s)(x^ly^s)\cdots(x^ly^s)}^{n} \\ &= x^{nl}\left(x^{-(n-1)l}y^sx^{(n-1)l}\right)\left(x^{-(n-2)l}y^sx^{(n-2)l}\right)\cdots\left(x^{-l}y^sx^l\right)y^s \\ &= x^{nl}y^{2^{(n-1)l}s}y^{2^{(n-2)l}s}\cdots y^{2^ls}y^s \\ &= x^{nl}y^{s(2^{(n-1)l}+2^{(n-2)l}+\cdots+2^l+1)}.\end{aligned}$$

https://doi.org/10.1017/S1446788700004201 Published online by Cambridge University Press

Thus $nl = k$ and $s(2^{(n-1)l}+2^{(n-2)l}+\cdots+2^l+1) = r$. So if x^ky^r has an n^{th} root, $n|k$. Whether k/n is positive, negative, or zero,

$$2^{(n-1)k/n}+2^{(n-2)k/n}+\cdots+2^{k/n}+1 \neq 0$$

because the complex solutions of the equation $z^{n-1}+z^{n-2}+\cdots+z+1 = 0$ are the n^{th} roots of unity different from 1. So $(x^ly^s)^n = x^ky^r$ if and only if $n|k$, $l = k/n$, and

$$s = \frac{r}{2^{(n-1)k/n}+2^{(n-2)k/n}+\cdots+2^{k/n}+1}.$$

Thus whenever $n|k$, x^ky^r has a unique n^{th} root; if $n \nmid k$, x^ky^r has no n^{th} root. This establishes that G is an R-group.

We will now show that if $g \in G$ and g fails to have an n^{th} root in G for some n then (a) $C(g, G)$ is cyclic and (b) if $h^{-1}g^ph = g^q$ for $h \in G$ and integers p and q, then $p = q$. First let us notice that the elements y^r have n^{th} roots in G for all n, so that we are only trying to prove these statements for elements g of the form $g = x^ky^r$ where $k \neq 0$. Now, in an R-group G, if $g = h^n$, $n \neq 0$, then $C(g, G) = C(h, G)$; so that it is sufficient to establish (a) and (b) for the elements xy^r, since $x^ky^r = (xy^s)^k$ for some s. xy^r is conjugate to x, since

$$y^rxy^{-r} = xy^{2r-r} = xy^r;$$

and so it is sufficient to establish (a) and (b) for $g = x$.

Suppose $x^ly^s \in C(x, G)$. Then

$$x^ly^s = x^{-1}(x^ly^s)x = x^l(x^{-1}y^sx) = x^ly^{2s}.$$

Therefore $s = 0$, which means that $C(x, G) = gp(x)$. Now suppose $h^{-1}x^ph = x^q$ for some $h = x^ly^s$. Then

$$x^q = (x^ly^s)^{-1}x^p(x^ly^s) = y^{-s}x^{-l}x^px^ly^s = y^{-s}x^py^s = x^py^{-2^ps+s},$$

and we see that $p = q$.

Lemma 2. *The groups* $H = \{G_1 * G_2; y_1 = x_2\}$, $K = \{G_3 * G_4; y_3 = x_4\}$ *and* $L = \{K * G_5; y_4 = x_5\}$ *are in* $\mathscr{P}$.

Proof. The groups G_i are isomorphic to G, so by Lemma 1 they are in $\mathscr{P}$. We have just shown that $h^{-1}x^ph = x^q$ for $h \in G$ and integers p and q implies $p = q$, and so $h \in C(x^p, G) = gp(x)$. This means that if $1 \neq g \in gp(x)$ that

$$\{h \in G | h^{-1}gh \in gp(x)\} = gp(x).$$

In the isomorphism of G and G_i x corresponds to x_i; therefore if $1 \neq g \in gp(x_i)$ then

$$\{h \in G_i | h^{-1}gh \in gp(x_i)\} = gp(x_i).$$

In H the amalgamated subgroup is $gp(x_2)$, in K it is $gp(x_4)$, and in L it is $gp(x_5)$. Therefore, by Theorem 3, H, K, and L are in $\mathscr{P}$.

Finally we come to the most troublesome lemma of all,

LEMMA 3. *The group* $M = \{H * L;\ x_1 = y_5,\ y_2 = x_3\}$ *is in* $\mathscr{P}$.

Let $U = gp(x_1, y_2) = gp(y_5, x_3)$. The proof of Lemma 3 will be broken up into two parts. First we will show that if $u \in U$ and u is not conjugate in U to a power of y_5, then

$$\{h \in L | h^{-1}uh \in U\} = U.$$

Then we will show that if $1 \neq u \in U$ and u is conjugate in U to some power of $x_1 = y_5$, then

$$\{h \in H | h^{-1}uh \in U\} = U.$$

By Theorem 3, this will establish that $M \in \mathscr{P}$.

1. If $u \in U = gp(y_5, x_3)$ and u is not conjugate in U to a power of y_5, then

$$\{h \in L\,|\,h^{-1}uh \in U\} = U.$$

PROOF. Let us recall that

$$c = x_3, \quad d = x_4 = y_3, \quad e = x_5 = y_4, \quad \text{and} \quad a = y_5.$$

Thus G_3 is a splitting extension of Γ_3 (isomorphic to Γ), which contains an element d, by an infinite cycle generated by c. G_4 is a splitting extension of Γ_4, which contains an element e, by the infinite cycle generated by d. So

$$K = \{G_3 * G_4;\ gp(d)\}.$$

G_5 is a splitting extension of Γ_5, which contains an element a, by the infinite cycle generated by e. Hence

$$L = \{K * G_5;\ gp(e)\}.$$

$U = gp(a, c)$, and we have already remarked that this group is free and freely generated by a and c. We wish to show that if $u \in U$, u is not conjugate in U to a power of a, and $h^{-1}uh \in U$, then $h \in U$; so let us suppose this statement is false.

For $h \in L$ let $\lambda(h)$ be the length associated with the factorization $L = \{K * G_5;\ gp(e)\}$.

Let

$$p = \min \left\{ \lambda(h) \,\middle|\, \begin{array}{l} h \in L - U,\ \exists\, u \in U,\ u \text{ not conjugate in } U \\ \text{to a power of } a, \text{ such that } h^{-1}uh \in U \end{array} \right\}.$$

Let h be an element of length p in $L - U$ and $u \in U$, u not conjugate in U to a power of a, such that $h^{-1}uh \in U$. Let $w = h^{-1}uh$. Because u and w are in U, they can be written uniquely as

$$u = u_1 u_2 \cdots u_m,$$
$$w = w_1 w_2 \cdots w_l,$$

where each u_i and each w_j is either a power of a or a power of c, but u_i and u_{i+1} not both powers of a nor both powers of c, w_i and w_{i+1} not both powers of a nor both powers of c. This means that each u_i is either in K (in case u_i is a power of c) or in G_5 (in case u_i is a power of a) but u_i and u_{i+1} not both in the same factor; therefore $\lambda(u) = m$. Similarly, $\lambda(w) = l$.

Now suppose that $p \geqq 1$. Then

$$h = h_1 h_2 \cdots h_p,$$

where h_i is in one of the factors K or G_5, but h_i and h_{i+1} not both in the same factor. It cannot be that $h_p = e^k x$ where k is an integer and x is a power of a or a power of c. For if this were so, then $h' = hx^{-1} \notin U$ because $h \notin U$ and $x \in U$, while

$$h'^{-1}uh' = x(h^{-1}uh)x^{-1},$$

which is in U because $h^{-1}uh \in U$ and $x \in U$; however

$$h' = h_1 \cdots h_{p-1}h_p x^{-1} = h_1 \cdots (h_{p-1}e^k),$$

so $\lambda(h') = p-1$, a contradiction. Furthermore, $h_1 \neq xe^k$ where k is an integer and x is a power of a or a power of c. For if $h_1 = xe^k$, then $h' = x^{-1}h \notin U$, $u' = x^{-1}ux \in U$, and u' is not conjugate in U to a power of a because u is not. Now

$$h'^{-1}u'h' = h^{-1}x(x^{-1}ux)x^{-1}h = h^{-1}uh,$$

which is in U. But

$$x^{-1}h = x^{-1}h_1 h_2 \cdots h_p = (e^k h_2) \cdots h_p,$$

so $\lambda(h') = p-1$, a contradiction.

We will consider separately various cases depending on the lengths of u and h.

(a) $p > 1$, $m > 1$.

$$w_1 w_2 \cdots w_l = w = h^{-1}uh = h_p^{-1} \cdots h_2^{-1}h_1^{-1}u_1 u_2 \cdots u_m h_1 h_2 \cdots h_p.$$

Because $h_1 \neq xe^k$ where x is a power of a or a power of c, $h_1^{-1}u_1 \notin gp(e)$ and $u_m h_1 \notin gp(e)$; therefore after all cancellations and amalgamations have taken place in this product the initial term h_p^{-1} is unaffected. But $\lambda(w_1^{-1}w) = \lambda(w) - 1$ and

$$w_1^{-1}w = w_1^{-1}h_p^{-1} \cdots h_2^{-1}h_1^{-1}u_1 u_2 \cdots u_m h_1 h_2 \cdots h_p$$

imply that $w_1^{-1}h_p^{-1} \in gp(e)$, and so $h_p = e^k w_1^{-1}$ for some integer k; but w_1^{-1} is either a power of a or a power of c, and we have seen that this is impossible.

(b) $p = 1$, $m > 1$.

$$w_1 w_2 \cdots w_l = w = h^{-1}uh = h^{-1}u_1 u_2 \cdots u_m h.$$

If h is in a different factor than u_1, then h^{-1} is unaffected in the product $h^{-1}uh$, and so by the argument used in case (a) $w_1^{-1}h^{-1} \in gp(e)$. But this means $h = h_p = e^k w_1^{-1}$ for some k, which is impossible.

If h is in the same factor as u_1, $h^{-1}u_1 \notin gp(e)$ (otherwise $h = h_1 = u_1 e^k$ for some k), and this initial term $h^{-1}u$, is unaffected after all cancellations and amalgamations in the product have taken place. Therefore $w_1^{-1}h^{-1}u_1 = e^k$ for some k. Let $h' = u_1^{-1}hw_1 = e^{-k}$; h' is not in U and $\lambda(h') = 0$. Let $u' = u_1^{-1}uu_1$; $u' \in U$ because u, $u_1 \in U$, and u' is not conjugate in U to a power of a because u is not.

$$h'^{-1}u'h' = w_1^{-1}h^{-1}u_1(u_1^{-1}uu_1)u_1^{-1}hw_1 = w_1^{-1}(h^{-1}uh)w_1,$$

and this is in U because $w_1 \in U$ and $h^{-1}uh \in U$. But this contradicts the assumption $p = 1$.

(c) $p > 1$, $m = 1$.

We have assumed that u is not conjugate in U to a power of a; in particular u is not a power of a. Therefore, since $\lambda(u) = 1$, $u = c^n$ for some $n \neq 0$.

$$w_1 w_2 \cdots w_l = w = h^{-1}uh = h_p^{-1} \cdots h_2^{-1} h_1^{-1} c^n h_1 h_2 \cdots h_p.$$

If h_1 and c^n lie in different factors, then no terms in this product are affected, and as before we can conclude that $w_1^{-1}h_p^{-1} \in gp(e)$, which implies $h_p = e^k w_1^{-1}$ for some k, a contradiction.

Therefore h_1 lies in the same factor as c^n, namely in K. If $h_1^{-1}c^n h_1 \notin gp(e)$, then

$$h^{-1}uh = h_p^{-1} \cdots h_2^{-1} \wedge (h_1^{-1}c^n h_1) \wedge h_2 \cdots h_p;$$

thus h_p^{-1} is unaffected after all cancellations and amalgamations have taken place, and as before $w_1^{-1}h_p^{-1} \in gp(e)$, which leads to a contradiction. Hence

$$h_1^{-1}c^n h_1 = e^k$$

for some k, and we wish to show that such an equation in the group $K = \{G_3 * G_4; gp(d)\}$ is impossible. G_4 is a splitting extension of Γ_4, which contains e, by the cycle generated by d. Therefore G_4 possesses an endomorphism φ that maps d onto itself and each element of Γ_4 onto 1. The identity map of G_3 coincides with φ on the amalgamated subgroup. It follows that K has an endomorphism η that is the identity on G_3 and agrees with φ on G_4. Now

$$e^k\eta = e^k\varphi = 1,$$

and

$$(h_1^{-1}c^n h_1)\eta = (h_1\eta)^{-1}(c^n\eta)(h_1\eta) = (h_1\eta)^{-1}c^n(h_1\eta).$$

So

$$1 = e^k\eta = (h_1^{-1}c^n h_1)\eta = (h_1\eta)^{-1}c^n(h_1\eta),$$

but this implies $c^n = 1$, or $n = 0$, which is a contradiction.

(d) $p = 1$, $m = 1$.

Since $\lambda(u) = 1$ and u is not a power of a, $u = c^n$, $n \neq 0$.

$$w_1 w_2 \cdots w_l = w = h^{-1}c^n h.$$

If h and c^n lie in different factors, then as before $w_1^{-1}h^{-1} \in gp(e)$, which leads to a contradiction.

Thus h lies in the same factor as c^n; that is, $h \in K$. Hence $h^{-1}c^n h$ is in $K \cap gp(a, c) = gp(c)$, so

$$h^{-1}c^n h = c^k$$

for some integer k. We now examine this equation in the group $K = \{G_3 * G_4; gp(d)\}$. G_3 is isomorphic to G with $x \to c$, $y \to d$. From the proof of Lemma 1 we know that $C(c, G_3) = gp(c)$, and c is not conjugate in G_3 to an element of $gp(d)$ (because d has n^{th} roots in G_3 for every n, while c does not). Therefore, by Theorem 2 $C(c, K) = C(c, G_3) = gp(c)$. This implies c does not have, for example, a square root in K; therefore, since K is in $\mathscr{P}$ (Lemma 2) and $h^{-1}c^n h = c^k$, it follows that $n = k$ and so $h \in C(c, K) = gp(c) < U$. This is a contradiction.

(e) $p = 0$, $m > 1$. In this case $h = e^k$, k a non-zero integer.

$$w_1 w_2 \cdots w_l = w = h^{-1}uh = (e^{-k}u_1)u_2 \cdots (u_m e^k).$$

This means that $l = m$, w_1 and u_1 in the same factor and

$$w_1^{-1}e^{-k}u_1 = e^n, \qquad n \text{ an integer.}$$

If w_1 and u_1 lie in K, then $w_1^{-1} = c^i$ and $u_1 = c^j$ for some non-zero integers i and j; we have

$$c^i e^{-k} c^j e^{-n} = 1, \quad i \neq 0,\ k \neq 0, \quad j \neq 0,$$

an equation in $K = \{G_3 * G_4; gp(d)\}$. However, this is impossible, because $c^i \in G_3 - gp(d)$, $e^{-k} \in G_4 - gp(d)$, $c^j \in G_3 - gp(d)$, and $e^{-n} \in G_4$; such an element cannot be 1 in a generalized free product.

Thus w_1 and u_1 lie in G_5. Therefore $w_1^{-1} = a^i$ and $u_1 = a^j$ for some non-zero integers i and j, and so

$$e^n = w_1^{-1}e^{-k}u_1 = a^i e^{-k} a^j = e^{-k}a^{2^{-k}i+j}$$

(because $e^{-1}ae = a^2$, $e^k a^i e^{-k} = a^{2^{-k}i}$ — see Lemma 1). So $n = -k$. Now, $l = m > 1$. If $l > 2$, then we have

$$w_2 \cdots w_l = (w_1^{-1} e^{-k} u_1) u_2 \cdots (u_m e^k) = e^{-k} u_2 \cdots (u_m e^k).$$

This implies

$$w_2^{-1} e^{-k} u_2 = e^q, \qquad q \text{ an integer.}$$

Now w_2 and u_2 lie in K and so $w_2^{-1} = c^i$, $u_2 = c^j$ for non-zero integers i and j. Thus in K we have the equation

$$c^i e^{-k} c^j e^{-q} = 1, \quad i \neq 0, \quad k \neq 0, \quad j \neq 0,$$

and we have already remarked that such an equation is impossible in K. Therefore $l = m = 2$, and we have

$$w_2 = (w_1^{-1} e^{-k} u_1)(u_2 e^k) = e^{-k} u_2 e^k.$$

Since w_2 and u_2 are in K, $w_2^{-1} = c^i$ and $u_2 = c^j$ for non-zero integers. This gives us the equation

$$c^i e^{-k} c^j e^k = 1, \quad i \neq 0, \quad k \neq 0, \quad j \neq 0,$$

which is impossible.

(f) $p = 0$, $m = 1$.

In this case $h = e^k$, $k \neq 0$, and $u = c^n$, $n \neq 0$ (because u is not a power of a). Thus $h^{-1}uh = e^{-k}c^n e^k$. e and c are in K, so $h^{-1}uh \in K \cap gp(a, c) = gp(c)$. Therefore for some integer q we have

$$e^{-k} c^n e^k = c^q, \quad k \neq 0, \quad n \neq 0,$$

and as we have shown, such an equation is impossible in the generalized free product $K = \{G_3 * G_4; gp(d)\}$.

This completes the proof of part 1 of Lemma 3.

2. If $u \in U = gp(x_1, y_2)$ and u is conjugate in U to a power of x_1, then

$$\{h \in H | h^{-1}uh \in U\} = U.$$

Proof. Let us recall that $a = x_1$, $b = x_2 = y_1$, and $c = y_2$. G_1 is a splitting extension of Γ_1, which contains b, by the infinite cycle generated by a. G_2 is a splitting extension of Γ_2, which contains c, by the cycle generated by b. Thus

$$H = \{G_1 * G_2; gp(b)\}.$$

For $h \in H$ let $\lambda(h)$ be the length associated with this factorization. We wish to show that if $u \in U = gp(a, c)$, u is conjugate in U to a power of a, and $h^{-1}uh \in U$, then $h \in U$. Suppose we can show that if $h^{-1}a^n h \in U$ $(n \neq 0)$ then $h \in U$; it follows from this that if $v \in U$ and $h^{-1}(v^{-1}a^n v)h \in U$ then $vh \in U$ and so $h \in U$. Thus it is sufficient to show that if $h^{-1}a^n h \in U$, $n \neq 0$, then $h \in U$. Let us suppose then that this is false.

https://doi.org/10.1017/S1446788700004201 Published online by Cambridge University Press

Let

$$p = \min\{\lambda(h) | h \in H - U,\ h^{-1}a^n h \in U \text{ for some } n \neq 0\}.$$

Let h be an element of length p in $H-U$ and $n \neq 0$ such that $h^{-1}a^n h \in U$. If $p \geqq 1$, then h can be written in the form

$$h = h_1 h_2 \cdots h_p$$

where h_i is in one of the factors G_1 or G_2 but h_i and h_{i+1} are not in a common factor. Let $w = h^{-1}a^n h$. Since $w \in U$, which is freely generated by a and c, w can be written uniquely in the form

$$w = w_1 w_2 \cdots w_l,$$

where each w_i is either a power of a or a power of c, but not both w_i and w_{i+1} powers of a, not both w_i and w_{i+1} powers of c. This means that each w_i is either in G_1 (in case w_i is a power of a) or in G_2 (in case w_i is a power of c) but u_i and u_{i+1} not both in the same factor; therefore $\lambda(w) = l$.

If $p \geqq 1$, it cannot be that $h_p x \in gp(b)$ where x is a power of a or a power of c. For if $h_p x = b^k$, k an integer, let $h' = hx$; $h' \notin U$ because $x \in U$ and $h \notin U$.

$$h'^{-1}a^n h' = x^{-1}h^{-1}a^n hx = x^{-1}(h^{-1}a^n h)x,$$

and this is in U because $h^{-1}a^n h \in U$ and $x \in U$. But

$$hx = h_1 \cdots h_{p-1} h_p x = h_1 \cdots (h_{p-1} b^k),$$

and so $\lambda(hx) = p-1$ because b^k is in the amalgamated subgroup. And this is in contradiction to the minimality of p.

Let us consider separately various cases.

(a) $h_1 \in G_2\text{-}gp(b)$. In this case we have

$$w_1 w_2 \cdots w_l = w = h^{-1}uh = h_p^{-1} \cdots h_1^{-1} \wedge a^n \wedge h_1 \cdots h_p.$$

It follows that $w_1^{-1}h_p^{-1} \in gp(b)$, or $h_p w_1 \in gp(b)$; however, as we have just shown this is impossible because w_1 is either a power of a or a power of c.

(b) $h_1 \in G_1$, $p > 1$.

$$w_1 w_2 \cdots w_l = w = h^{-1}uh = h_p^{-1} \cdots h_2^{-1}(h_1^{-1}a^n h_1)h_2 \cdots h_p$$

$h_1^{-1}a^n h_1 \notin gp(b)$ because b has n^{th} roots for every n in G_1, while a does not, so no power of a can be conjugate in G_1 to a power of b. Therefore $h_1^{-1}a^n h_1 \in G_1\text{-}gp(b)$, and the terms $h_p^{-1}, \cdots, h_2^{-1}$ are unaffected by amalgamations. Hence $w_1^{-1}h_p^{-1} \in gp(b)$, which we have shown is impossible.

(c) $h \in G_1$. Both a^n and $h \in G_1$ implies $h^{-1}a^n h \in G_1$. Therefore $h^{-1}a^n h \in G_1 \cap U = gp(a)$. But in the proof of Lemma 1 it was shown that $h^{-1}a^n h = a^k$ implies $h \in gp(a)$, which is contrary to assumption.

References

[1] Baumslag, G., 'Some aspects of groups with unique roots'. *Acta Mathematica*, 104 (1960), 217–303.

[2] Birkhoff, G., 'On the structure of abstract algebras'. *Proc. Cambridge Philos. Soc.*, 31 (1935), 433–454.

[3] Higman, G., 'A finitely generated infinite simple group'. *Journal London Math. Soc.*, 26 (1951), 61–64.

[4] Higman, G., Neumann, B. H. and Neumann, H., 'Embedding theorems for groups'. *Journal London Math. Soc.*, 24 (1949), 247–254.

[5] Neumann, B. H., 'An essay on free products of groups with amalgamations'. *Philos. Trans. Royal Soc. London, Series A*, No. 919, Vol. 246 (1954), 503–554.

Mathematics Department
Syracuse University
Syracuse, N.Y.