FINITELY PRESENTED INFINITE SIMPLE GROUPS

Notes on Pure Mathematics

8
1974

FINITELY PRESENTED
INFINITE SIMPLE GROUPS

Graham Higman

Department of Pure Mathematics,
Department of Mathematics, I.A.S.
Australian National University,
Canberra.

Other titles in series:

1. What is the Riemann Integral?
2. Curves and Topological Questions
3. Schwartz Distributions
4. Paths in Complex Analysis
5. Integration and Harmonic Analysis on Compact Groups (out of print)
6. Linear Systems
7. Seminar Schwartz
8. Finitely Presented Infinite Simple Groups
9. Order and Recursion in Topoi
10. Minimal Surfaces and Functions of Bounded Variation.

First published 1974, reprinted 1977.

Printed and manufactured in Australia by
The Australian National University, Canberra. A.C.T.

Library of Congress Catalogue no. 74-77210

National Library of Australia Card and ISBN 0 7081 0300 6

Preface

These notes were written by Dr L.F. Harris and Dr H. Silcock from lectures delivered by Professor Graham Higman during a visit to the Australian National University from July to October 1973. The manuscript was typed by Mrs A. Zalucki.

Ed.

CONTENTS

1. SUMMARY OF RESULTS

The aim of these lectures is to describe an infinite family of finitely presented infinite simple groups. R. Thompson discovered one of these groups in the course of research on the λ-calculus; the construction to be used here is based on work done following a report of Thompson's work by B. Jónsson.

We begin by introducing a formulation in terms of universal algebra for the mathematical system consisting simply of a set S and a one to one mapping from S onto its n-th Cartesian power S^n. (To avoid trivialities we suppose $n \geq 2$.) A mapping $S \to S^n$ may be described using n mappings $\alpha_i : S \to S$ $(i = 1,2,\ldots,n)$, where

$$a \mapsto (a\alpha_1,\ldots,a\alpha_n) \ . \tag{1}$$

We view these mappings $\alpha_1,\ldots,\alpha_n$ as unary operations on S. Because the mapping $S \to S^n$ is one to one and onto, it has an inverse $\lambda : S^n \to S$ which we may view as an n-ary operation on S.

The operations $\alpha_1,\ldots,\alpha_n$ and λ must satisfy

$$a\alpha_1\ldots a\alpha_n\lambda = a \tag{2}$$

$$a_1a_2\ldots a_n\lambda\alpha_i = a_i \qquad (i = 1,2,\ldots,n) \tag{3}$$

for all $a,a_1,\ldots,a_n \in S$; conversely if S is any set on which operations $\alpha_1,\ldots,\alpha_n,\lambda$ are defined and satisfy (2) and (3), the mapping (1) determines a one to one correspondence $S \to S^n$.

We are therefore led to introduce the variety $\mathcal{V}_n$ of universal algebras with n unary operations $\alpha_1,\ldots,\alpha_n$ and one n-ary operation λ satisfying the laws (2) and (3). An algebra of $\mathcal{V}_n$ that contains more than one element is infinite, because it is in one to one correspondence with its n-th Cartesian power.

For each pair of integers $n \geq 2$, $r \geq 1$, let $V_{n,r}$ be the free algebra of $\mathcal{V}_n$ with r free generators. Any free algebra in $\mathcal{V}_n$ that is freely generated by a set X is also freely generated by the set

$$X \setminus \{x\} \cup \{x\alpha_1, \ldots, x\alpha_n\}$$

for each $x \in X$. Hence $V_{n,r} \cong V_{n,s}$ whenever $r \equiv s \ (n-1)$. Less trivially, the condition $r \equiv s \ (n-1)$ is also a necessary condition that $V_{n,r} \cong V_{n,s}$.

For $n \geq 2$, $r \geq 1$, we write $G_{n,r}$ for the automorphism group of $V_{n,r}$. Each of the groups $G_{n,r}$ is a finitely presented infinite group. If n is even, then $G_{n,r}$ is simple; and if n is odd, then $G_{n,r}$ has a simple subgroup $G^+_{n,r}$ of index 2. (Clearly $G^+_{n,r}$ will also be finitely presented.) For uniformity we shall set $G^+_{n,r} = G_{n,r}$ when n is even.

If $G^+_{m,r} \cong G^+_{n,r}$ then $m = n$; from this it follows that there are infinitely many non-isomorphic groups among the groups $G^+_{n,r}$. However for a fixed n the groups $G^+_{n,r}$ corresponding to different values of r can be isomorphic even when the corresponding algebras are not. To decide exactly when this is so a complicated matter, and we give only partial results.

Let P denote the set of residue classes of integers modulo $n-1$. When $r \equiv s \ (n-1)$ we know that $V_{n,r} \cong V_{n,s}$, and hence also $G^+_{n,r} \cong G^+_{n,s}$, so we may think of the second suffix here as ranging over P. Let Φ be the set of residue classes in P that are prime to $n-1$: this is a multiplicative group of order $\phi(n-1)$ (where ϕ is Euler's function) and acts on P by multiplication. Denote the subgroup of Φ generated by the divisors of n by Φ_0. A *necessary* condition for $G^+_{n,r} \cong G^+_{n,s}$ is that r and s belong to the same orbit under the action of Φ on P. A *sufficient* condition is that r and s belong to the same orbit of Φ_0. Notice that it follows from this that $G^+_{n,r}$ and $G^+_{n,s}$ can be isomorphic when $V_{n,r}$ and $V_{n,s}$ are not.

To illustrate the gap left by the above results, take $n = 40$. Here $|\Phi| = 24$ whereas $|\Phi_0| = 12$, and the Φ-orbit containing 1, (namely Φ itself) splits into two orbits under the action of Φ_0 (namely the cosets of Φ_0 in Φ). Thus we cannot decide from the above conditions whether, for example, $G_{40,1} \cong G_{40,7}$ because 1 and 7 are in the same Φ-orbit but in different Φ_0-orbits.

The proofs of the above results rely on arguments that establish non-isomorphisms between different groups $G^+_{n,r}$ by counting conjugacy classes of embeddings of finite groups (and, in particular, of cyclic groups). Similar arguments show that each $G^+_{n,r}$ contains an isomorphic copy of every countable locally finite group. The words "locally finite" are certainly not redundant here, as there are quite strong restrictions on the torsion-free subgroups of the groups $G^+_{n,r}$. For instance, if H is a torsion-free abelian group of finite rank contained in $G = G_{n,r}$ (or $G^+_{n,r}$), then :

(i) H is free abelian,

(ii) $C_G(H)$ has finite index in $N_G(H)$,

(iii) there exists a direct factor B of $N_G(H)$ and a free abelian subgroup C of B of finite rank such that C has finite index in HB.

From (ii) it follows, for example, that every torsion-free nilpotent subgroup of $G_{n,r}$ is abelian. (Recall that in a torsion-free nilpotent group R the centralizer of a subgroup is always isolated - that is, $x^n \in C_R(H)$ implies $x \in C_R(H)$ for any $n > 0$ - so that $N_R(H)/C_R(H)$ is torsion-free [Kurosh, Vol. II, §66]).

The "smallest" of these groups, $G_{2,1}$, can be generated by 4 generators, subject to 16 defining relations, all of which can be comfortably written on a single sheet of paper. Though we do not prove it here, there is a common upper bound to the number of elements needed to generate a $G_{n,r}$: probably 6 would be enough. It is not known if there is a bound on the minimal number of defining relations of the $G_{n,r}$.

In $G_{n,r}$ the conjugacy and order problems are soluble, as we shall show in the last section. The word problem is soluble because *a finitely generated simple group whose defining relations are recursively enumerable has a soluble word problem.*

Let G be such a group. If $G = 1$ the result is trivial, so we may suppose that some word u defines a non-trivial element of G .

Let w be any word. To test whether $w = 1$ in G, we simultaneously compile two lists. The first list consists of the defining relations of G and their consequences : it is easy to see that these form a recursively enumerable set, since the defining relations of G do. The second list consists of all the consequences of the defining relations of G and the additional relation $w = 1$: again this is a recursively enumerable set, for similar reasons.

Eventually either w will appear on the first list, and so $w = 1$ in G, or u will appear on the second list, and $w \neq 1$ in G . For if $w \neq 1$ in G the relations on the second list are those of a proper homomorphic image of G . But this can only be the trivial group, so those relations will certainly include $u = 1$.

B.M. Hurley is considering a variation from the approach here. In it the one to one correspondence between the sets S and S^n is replaced by an isomorphism between elementary abelian p-groups S and S^n. One could also look at isomorphisms between S^m and S^n for $m \neq n$. Both of these variations were suggested by P.M. Neumann.

2. THE ALGEBRAS $V_{n,r}$

For any set X, we let $F_n(X)$ denote the free algebra of $\mathcal{V}_n$ freely generated by X. It will be useful to have a method of constructing $F_n(X)$ explicitly : the construction we describe now also suggests how to solve the word problem in $F_n(X)$.

We continue to write $\alpha_1,\ldots,\alpha_n,\lambda$ for the operations associated with the algebras in $\mathcal{V}_n$. Let $A = \{\alpha_1,\ldots,\alpha_n\}$. For the construction of $F_n(X)$ we shall assume that

$$X \cap (A \cup \{\lambda\}) = \emptyset .$$

By a *standard form over* X we shall mean one of the finite sequences of elements of $X \cup A \cup \{\lambda\}$ specified by the following rules :

(i) $x\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$ is a standard form whenever $x \in X$, $k \geq 0$ and $1 \leq i_j \leq n$ for $j = 1,2,\ldots,k$.
(The case $k = 0$ is to be interpreted as stating that x is a standard form.)

(ii) If $w_1,w_2,\ldots,w_n$ are standard forms, then so is $w_1w_2\ldots w_n\lambda$ *unless* there is a standard form u such that $w_i = u\alpha_i$ for $i = 1,2,\ldots,n$.

(iii) No sequence is a standard form unless this follows from (i) and (ii).

We make the set of standard forms into an algebra by defining operations $\alpha_1,\ldots,\alpha_n,\lambda$ as follows :

$$(x\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k})\alpha_i = x\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}\alpha_i \qquad (1)$$

$$(w_1w_2\ldots w_n\lambda)\alpha_i = w_i \qquad (2)$$

for $i = 1,2,\ldots,n$ and

$$(w_1,w_2,\ldots,w_n)\lambda = w_1w_2\ldots w_n\lambda \tag{3}$$

unless there is a standard form u such that $w_i = u\alpha_i$ for $i = 1,2,\ldots,n$ in which case we define

$$(w_1,w_2,\ldots,w_n)\lambda = (u\alpha_1,\ldots,u\alpha_n)\lambda = u\ . \tag{4}$$

LEMMA 2.1. *The algebra of standard forms defined above is a free algebra of* V_n *, freely generated by* X .

From the way the operations $\alpha_1,\ldots,\alpha_n$, were defined it is clear that every standard form can be obtained by applying these operations successively to elements of X . Thus X generates the algebra.

To prove that the algebra belongs to V_n we need to check that the laws

$$((w)\alpha_1,(w)\alpha_2,\ldots,(w)\alpha_n)\lambda = w \tag{5}$$

$$(w_1,w_2,\ldots,w_n)\lambda\alpha_i = w_i \quad (i = 1,2,\ldots,n) \tag{6}$$

hold. If w is a standard form involving no λ then (5) is a direct consequence of (4). On the other hand if w has the form $w = u_1\ldots u_n\lambda$ then, by (2),

$$(w\alpha_1,\ldots,w\alpha_n)\lambda = u_1\ldots u_n\lambda = w\ ,$$

so (5) holds in this case too. Thus (5) is a law. Similarly (6) is a direct consequence of (2) except in the case where there exists a standard form u with $w_j = u\alpha_j$ for $j = 1,2,\ldots,n$. In this case (4) shows that

$$(w_1,\ldots,w_n)\lambda = u ,$$

whence $((w_1,\ldots,w_n)\lambda)\alpha_i = (u)\alpha_i = w_i$ for each i, as required. So (6) is a law, and hence the algebra is in V_n.

To show that X is a free generating set, suppose $\theta : X \to S$ is a mapping of X into an algebra S in V_n. We extend this to a map $\hat{\theta}$ from the algebra of standard forms by defining

$$(x\alpha_{i_1}\ldots\alpha_{i_k})\hat{\theta} = x\theta\alpha_{i_1}\ldots\alpha_{i_k} \tag{7}$$

$$(w_1\ldots w_n\lambda)\hat{\theta} = w_1\hat{\theta}\ldots w_n\hat{\theta}\lambda \tag{8}$$

(This defines $\hat{\theta}$ by induction on the number of λ involved in a standard form.) To prove that $\hat{\theta}$ is a homomorphism we need to check that

$$w\alpha_i\hat{\theta} = w\hat{\theta}\alpha_i \quad (i = 1,2,\ldots,n) \tag{9}$$

$$w_1\ldots w_n\lambda\hat{\theta} = w_1\hat{\theta}\ldots w_n\hat{\theta}\lambda \tag{10}$$

for all standard forms $w, w_1, w_2, \ldots, w_n$.

If w involves no λ then (9) follows from the definition (7). On the other hand if w has the form $w = v_1\ldots v_n\lambda$ then by (2) the left-hand side of (9) is

$$w\alpha_i\hat{\theta} = v_i\hat{\theta} \quad (i = 1,2,\ldots,n)$$

whereas, by (8), the right-hand side is

$$w\hat{\theta}\alpha_i = v_i\hat{\theta}\ldots v_n\hat{\theta}\lambda\alpha_i = v_i\hat{\theta} \quad (i = 1,2,\ldots,n)$$

so that (9) holds in all cases.

Similarly (10) follows directly from (8) unless there is a standard form u such that $w_i = u\alpha_i$ for $i = 1,2,\ldots,n$ in which case the left-hand side of (10) is

$$w_1 \ldots w_n \lambda \hat{\theta} = u\hat{\theta} .$$

By (9) we have $w_i\hat{\theta} = u\hat{\theta}\alpha_i$ for each i, so the right-hand side of (10) is

$$w_1\hat{\theta} \ldots w_n\hat{\theta}\lambda = u\hat{\theta}\alpha_1 \ldots u\hat{\theta}\alpha_n\lambda = u\hat{\theta} .$$

Thus (10) holds in all cases.

Therefore $\hat{\theta}$ is a homomorphism extending θ. It is the unique homomorphism with this property, because a homomorphism extending θ must satisfy equations analogous to (7) and (8) and so will coincide with $\hat{\theta}$. Consequently X is a free generating set and the proof is complete.

If we need to think concretely about the free algebra of V_n freely generated by a set S, it will be this algebra of standard forms that we have in mind. This makes it clear what we mean when we speak, for instance, of the "number of λ" in an element of such an algebra.

For a subset X of an algebra S in V_n we shall write $X\langle A\rangle$ for the A-subalgebra of S generated by X, and $X\langle\lambda\rangle$ for the λ-subalgebra generated by X.

<u>LEMMA 2.2.</u> *If a set* X *generates an algebra* S *in* V_n *then* $S = X\langle A\rangle\langle\lambda\rangle$. *Also, for each* y *in* S, *the set* $y\langle A\rangle \setminus X\langle A\rangle$ *is finite.*

It is sufficient to consider the case where S is free on X. Then S is isomorphic to the algebra of standard forms on X, so the first part holds, by the definition of standard forms.

For the second part, note that if $y \in S$ and the number of λ involved in y (in a standard form) is m, then we have $y\alpha_{i_1}\ldots\alpha_{i_r} \in X\langle A\rangle$ whenever $r \geq m$. Hence the only elements in $y\langle A\rangle \setminus X\langle A\rangle$ are those of the form $y\alpha_{i_1}\ldots\alpha_{i_r}$ with $r < m$ and these are clearly finite in number.

LEMMA 2.3. *(i) If* $x \in X$, *then* $F_n(X)$ *is also freely generated by*

$$X \setminus \{x\} \cup \{x\alpha_i \mid 1 \leq i \leq n\} .$$

(ii) If $x_1,\ldots,x_n$ *are distinct elements of* X, *then* $F_n(X)$ *is freely generated by*

$$X \setminus \{x_1,\ldots,x_n\} \cup \{x_1\ldots x_n\lambda\} .$$

(i) Write $Y = X \setminus \{x\} \cup \{x\alpha_1,\ldots,x\alpha_n\}$, and suppose that $\theta : Y \to S$ is a mapping from Y into an algebra S in V_n. Define a mapping $\theta^* : X \to S$ by

$$y\theta^* = y\theta \quad \text{for } y \in X \setminus \{x\}$$

$$x\theta^* = x\alpha_1\theta\ldots x\alpha_n\theta\lambda .$$

Because X is a free basis, there is a unique homomorphism $\hat{\theta}$ from $F_n(X)$ into S that extends θ^*. But $\hat{\theta}$ is also a homomorphism extending θ, as we have

$$y\hat{\theta} = y\theta^* = y\theta \quad \text{for } y \in X \setminus \{x\} ,$$

$$\begin{aligned} x\alpha_i\hat{\theta} &= x\hat{\theta}\alpha_i = x\theta^*\alpha_i \\ &= x\alpha_1\theta\ldots x\alpha_n\theta\lambda\alpha_i \\ &= x\alpha_i\theta \quad \text{for } i = 1,2,\ldots,n . \end{aligned}$$

This shows that every mapping from Y into an algebra in V_n can be extended to a homomorphism from $F_n(X)$. Since Y generates $F_n(X)$ it follows that Y is a free basis of $F_n(X)$.

(ii) is proved similarly.

The operation described in *(i)* will be called a *simple expansion.* The operation obtained by composing d simple expansions will be called a d-*fold expansion*, and an *expansion* will mean a d-fold expansion for some $d \geq 0$. The operation described in *(ii)* is the inverse of a simple expansion and will be called a *simple contraction.*

We shall also say that a basis Y is a d-*fold expansion of* X, meaning that it is the result of applying a d-fold expansion to X. Observe that $X\langle A\rangle$ is the set of all elements of $F_n(X)$ that occur in expansions of X. Also if Y is a d-fold expansion of a finite basis X, then

$$|Y| = |X| + (n-1)d .$$

LEMMA 2.4. *If X is a finite set, then the following conditions on a subset U of $F_n(X)$ contained in $X\langle A\rangle$ are equivalent :*

(i) $U = X\langle A\rangle \cap Y\langle A\rangle$, *for some set Y generating $F_n(X)$*,

(ii) U is A-closed and $X\langle A\rangle \setminus U$ is finite,

(iii) $U = Z\langle A\rangle$ *for some expansion Z of X.*

[*(i)* ⇒ *(ii)*] Assume that $U = X\langle A\rangle \cap Y\langle A\rangle$, where Y generates $F_n(X)$. As it is an intersection of A-closed sets, U is itself A-closed. For each $x \in X$, the set $x\langle A\rangle \setminus Y\langle A\rangle$ is finite, by Lemma 2.2 (with X replaced by Y). Since X is finite, this implies $X\langle A\rangle \setminus Y\langle A\rangle = X\langle A\rangle \setminus U$ is finite.

[*(ii)* ⇒ *(iii)*] Assume that U is A-closed and that $X\langle A\rangle \setminus U$ is finite. We prove *(iii)* by induction on $|X\langle A\rangle \setminus U|$. If $|X\langle A\rangle \setminus U| = 0$ then *(iii)* holds with $Z = X$. Otherwise, choose an element w in $X\langle A\rangle \setminus U$ of greatest length (that is, w is to involve the largest possible number of α_i). Then the set $U^* = U \cup \{w\}$ is A-closed, and $|X\langle A\rangle \setminus U^*| = |X\langle A\rangle \setminus U| - 1$. So by induction there is an expansion Z^* of X such that $U^* = Z^*\langle A\rangle$. The element w belongs to Z^*; for if not w would have the form $w = z\alpha_{i_1}\ldots\alpha_{i_r}$, where $z \in Z^*$ and $r > 0$, and hence $z \in U^* \setminus \{w\} = U$. But U is A-closed, so this would imply that $w \in U$, a contradiction. Take

$$Z = Z^* \setminus \{w\} \cup \{w\alpha_i \mid 1 \leq i \leq n\} ;$$

this is an expansion of X and, by the choice of w, we have $w\alpha_i \in U$ for each i, and therefore $U = Z\langle A\rangle$ as required.

[*(iii)* ⇒ *(i)*] is trivial.

<u>COROLLARY 1.</u> *Any two finite free bases* X, Y *of the same algebra have a common expansion* Z.

(Note that $Z\langle A\rangle$ determines Z: for Z is the set of elements of $Z\langle A\rangle$ that do *not* have the form $z\alpha_i$ for some $z \in Z\langle A\rangle$.)

<u>COROLLARY 2.</u> $V_{n,r} \cong V_{n,s}$ *if and only if* $r \equiv s\ (n-1)$.

For if $r \equiv s\ (n-1)$ then $V_{n,r} \cong V_{n,s}$ by Lemma 2.3. Conversely, if $V_{n,r} \cong V_{n,s}$ then there are sets X, Y with $|X| = r$ and $|Y| = s$ which freely generate the same algebra in V_n; these have a common expansion, Z say, and for some non-negative integers d and e we have

$$|Z| = |X| + (n-1)d = |Y| + (n-1)e ,$$

whence $r \equiv s\ (n-1)$.

<u>LEMMA 2.5.</u> *Let* X *be a set and* V *a subset of* $F_n(X)$ *contained in* $X\langle A\rangle$.

(i) *If* X *and* V *are finite, then* V *is contained in an expansion of* X *if and only if the following condition is satisfied :*

no element of V *is an initial segment of another.* (*)

(ii) *If* X *and* V *are finite, then* V *is an expansion of* X *if and only if (*) is satisfied and for each* $u \in X\langle A\rangle$ *there exists* $v \in V$ *such that one of* u, v *is an initial segment of the other.*

(iii) V *is a set of free generators for the subalgebra it generates if and only if (*) is satisfied. (Here neither* X *nor* V *is assumed finite.)*

(iv) *Let* Y *and* Z *be* d-*fold expansions of* X, *for some* $d \geq 1$. *If* $Y \neq Z$ *then some element of* Y *is a proper initial segment of an element of* Z.

(i) "Only if" is obvious.

Suppose V satisfies (*) and write

$$U = X\langle A\rangle \setminus \{\text{proper initial segments of } V\}.$$

Then (*) implies that $V \subseteq U$. Also U is A-closed, and $X\langle A\rangle \setminus U$ consists of the initial segments of the elements of the finite set V, so it is finite. Thus by Lemma 2.4 there is an expansion Z of X such that $U = Z\langle A\rangle$. Therefore $V \subseteq Z\langle A\rangle$, and this implies that $V \subseteq Z$ (for an element of $Z\langle A\rangle \setminus Z$ has a proper initial segment in $Z \subseteq U$ so it cannot be in V, by the definition of U). Hence V is contained in an expansion of X.

(ii) "Only if" is again obvious.

Suppose V satisfies (*) and the additional condition in *(ii)*. By *(i)*, V is contained in an expansion Z of X. If $V \neq Z$, then there is an element $z \in Z \setminus V$, and hence by hypothesis there exists $v \in V$ such that one of v, z is an initial segment of the other. But no element of Z can be an initial segment of another, so this is a contradiction. Hence $V = Z$.

(iii) "Only if" is again obvious.

Suppose (*) is satisfied. If V is not a free generating set then the same is true of some finite subset V_0, and clearly (*) is also satisfied with V replaced by V_0. However $V_0 \subseteq X_0 \langle A \rangle$ for some finite subset X_0 of X. This contradicts *(ii)*.

(iv) If no element of Y is a proper initial segment of an element of Z, then we must have $Y \subseteq Z \langle A \rangle$ and hence $Y \langle A \rangle \subseteq Z \langle A \rangle$. This implies that Y is an expansion of Z. But Y, Z are both d-fold expansions of X, so it follows that $Y = Z$.

<u>LEMMA 2.6</u>. *If $|X| > 1$, then all elements of $X \langle A \rangle$ are equivalent under the automorphism group of $F_n(X)$. If $|X| > 2$, then all pairs of elements in which neither member is an initial segment of the other are also equivalent under the automorphism group of $F_n(X)$.*

Let $u \in X \langle A \rangle$: then u belongs to some expansion of X. If we assume that $|X| > 1$, then any expansion of X containing u will contain other elements also, so we can apply a further simple expansion to it to obtain a larger basis which still contains u. As each simple expansion increases the size of a basis by $n-1$, this shows that each element of $X \langle A \rangle$ belongs to a basis of size $|X| + (n-1)d$ for all sufficiently large d. Therefore, given any two elements of $X \langle A \rangle$, we can find two bases of the same size, each of which contains one of the given elements. Every one to one mapping from one basis onto the other extends to an automorphism of $F_n(X)$; hence there is an automorphism mapping one of the given elements onto to the other.

Similarly given any pair of elements of $X\langle A\rangle$, neither of them an initial segment of the other, we know by Lemma 2.5 that there is a basis of $F_n(X)$ containing both the elements. Moreover, by the Corollary 1 to Lemma 2.4, we may assume that this basis is an expansion of X. If we assume that $|X| > 2$, then any such basis must contain elements other than the given two, so it can be expanded to a larger basis also containing the given elements. The result now follows exactly as above.

<u>LEMMA 2.7.</u> *(i) A subalgebra of* $F_n(X)$ *is generated by its intersection with* $X\langle A\rangle$.

(ii) V_n *is a Schreier variety - subalgebras of free algebras in* V_n *are free.*

(iii) Finitely generated subalgebras of free algebras in V_n *are free factors.*

(iv) $F_n(X)$ *has no non-trivial characteristic subalgebras.*

(i) Let S be a subalgebra of $F_n(X)$ and write S_0 for the subalgebra generated by $S \cap X\langle A\rangle$. We prove that an arbitrary v in S belongs to S_0 by induction on the number of λ in v. If this number is zero, then $v \in X\langle A\rangle$ and so $v \in S_0$. If this number is positive, then v has the form $v = w_1 \ldots w_n\lambda$, where each w_i involves fewer λ than v. But then $w_i = v\alpha_i \in S$ for each i, so by induction $w_i \in S_0$, and hence $v \in S_0$, as required.

(ii) Suppose that S is a subalgebra of $F_n(X)$. By *(i)*, S is generated by $S \cap X\langle A\rangle$; moreover, if we omit from $S \cap X\langle A\rangle$ those elements that have a proper initial segment also in S, then the resulting set also clearly generates S. In this set no element is a proper initial segment of another, so by Lemma 2.5 the set is a free basis for S. Hence S is free.

(iii) Suppose that S is a finitely generated subalgebra of $F_n(X)$. Then the argument used for *(ii)* shows that S has a *finite* free basis, G say, and this is contained in $X_0\langle A\rangle$ for some finite set $X_0 \subseteq X$. By Lemma 2.5, G is contained in an expansion of X_0, and hence also in a free basis of $F_n(X)$. Therefore S is a free factor of $F_n(X)$.

(iv) Let S be a non-empty characteristic subalgebra of $F_n(X)$. Then, by *(i)*, we have $S \cap X\langle A\rangle \neq \emptyset$. We may assume that $|X| > 1$, so Lemma 2.6 shows that any two elements of $X\langle A\rangle$ are equivalent under the automorphism group of $F_n(X)$. Therefore $X\langle A\rangle \subseteq S$ and so $S = F_n(X)$.

A *congruence* $\equiv$ on $F_n(X)$ is an equivalence relation such that if $a \equiv b$ then $a\alpha_i \equiv b\alpha_i$ for all i and if $a_i \equiv b_i$ for $i = 1,2,\ldots,n$ then $a_1\ldots a_n\lambda \equiv b_1\ldots b_n\lambda$. Its intersection with $X\langle A\rangle$ is the set of congruent pairs (a,b) with both a and b in $X\langle A\rangle$.

<u>LEMMA 2.8.</u> *(i) Each congruence on* $F_n(X)$ *is generated by its intersection with* $X\langle A\rangle$.

(ii) $F_n(X)$ *has no non-trivial characteristic congruences.*

(iii) V_n *is a minimal variety, for each* n.

(i) Let $\equiv$ be any congruence on $F_n(X)$ and let $\equiv_0$ be the congruence generated by $\{(a,b) \mid a \equiv b \text{ and } a,b \in X\langle A\rangle\}$. We show that

$$u \equiv v \Rightarrow u \equiv_0 v\,,$$

using induction on the total number of λ involved in u and v. If this number is zero then $u, v \in X\langle A\rangle$, so $u \equiv_0 v$ by definition of $\equiv_0$. So suppose one of these elements, say u, involves at least one λ : then it can be expressed in the form $u = u_1 \ldots u_n\lambda$, where $u_1, \ldots, u_n$ are elements involving fewer λ than u . Since $\equiv$ is compatible with the operations in A , we have

$$u_i = u\alpha_i \equiv v\alpha_i$$

for each i , and u_i involves fewer λ than u and $v\alpha_i$ involves no more λ than v . So by induction

$$u_i \equiv_0 v\alpha_i \quad (i = 1,2,\ldots,n) ,$$

whence $u = u_1 \ldots u_n\lambda \equiv_0 v\alpha_1 \ldots v\alpha_n\lambda = v$.

(ii) Assume that $\equiv$ is a characteristic congruence on $F_n(X)$, other than $=$. Replacing X by an expansion if necessary, we may assume that $|X| > 2$. Let a , b be elements with $a \equiv b$ but $a \neq b$; by *(i)* we may assume that $a,b \in X\langle A\rangle$.

We claim that we may further assume that neither of these elements is an initial segment of the other. For suppose, for example, that a is an initial segment of b . Then b has the form

$$b = a\alpha_{i_1} \ldots \alpha_{i_r} ,$$

where $r > 0$, and so by applying to a and b an operation α_j with suffix j not equal to i_1 , we obtain elements $a\alpha_j$, $b\alpha_j$, neither of which is an initial segment of the other. These elements also satisfy $a\alpha_j \equiv b\alpha_j$, because $\equiv$ is compatible with A , and therefore may be used in place of the elements a,b originally chosen.

As $\equiv$ was taken to be a characteristic congruence, it now follows from Lemma 2.6 that $u \equiv v$ *for every* pair of elements $u,v \in X\langle A\rangle$ in which neither member is an initial segment of the other. In particular,

$x \equiv y$ for all $x,y \in X$, so that the quotient algebra modulo $\equiv$ is generated by the equivalence class $[x]$ for every $x \in X$. Further, if $x,y \in X$ and $x \neq y$ then in the same way we have $x \equiv y\alpha_i$ for $i = 1,2,\ldots,n$. Therefore

$$[x]\alpha_i = [y]\alpha_i = [y\alpha_i] = [x] \qquad (i = 1,2,\ldots,n)$$

and
$$\begin{aligned} [x]\ldots[x]\lambda &= [y\alpha_1]\ldots[y\alpha_n]\lambda \\ &= [y\alpha_1\ldots y\alpha_n\lambda] \\ &= [y] = [x] . \end{aligned}$$

This shows that the quotient algebra is a one-element algebra, so that $\equiv$ is the trivial congruence under which all elements are congruent. Thus $F_n(X)$ has no non-trivial characteristic congruences.

(iii) Suppose $\mathcal{V}_n$ is not a minimal variety. Then there exists a variety $\mathcal{W}$ properly contained in $\mathcal{V}_n$ and not consisting only of algebras with at most one element. For a sufficiently large set X, the free algebra of $\mathcal{W}$ freely generated by X is a quotient of the algebra $F_n(X)$ modulo a non-trivial congruence. This congruence must be fully invariant and *a fortiori* characteristic. But this contradicts *(ii)*.

3. ALGEBRAS OF V_n AS ALGEBRAS OF V_N FOR $N > n$

If a set S is in one to one correspondence with its Cartesian square S^2, then this correspondence can be used to define a one to one correspondence between S and S^3. There are the following two essentially different natural ways to do this. Suppose that the correspondence $S \to S^2$ associates a in S with (b,c) in S^2; and suppose that the elements b,c are in turn associated with (d,e), (f,g) respectively. Then either of the mappings $a \mapsto (b,f,g)$, $a \mapsto (d,e,c)$ determines a one to one correspondence between S and S^3.

This means that an algebra in V_2 can be viewed, in two essentially different natural ways, as an algebra in V_3. Expressing this formally, we can define new operations $\beta_1, \beta_2, \beta_3, \mu$ on any algebra in V_2 in terms of the operations $\alpha_1, \alpha_2, \lambda$ either by

$$a\beta_1 = a\alpha_1 , \quad a\beta_2 = a\alpha_2\alpha_1 , \quad a\beta_3 = a\alpha_2\alpha_2 , \quad a_1a_2a_3\mu = a_1a_2a_3\lambda\lambda$$

or by

$$a\beta_1 = a\alpha_1\alpha_1 , \quad a\beta_2 = a\alpha_1\alpha_2 , \quad a\beta_3 = a\alpha_2 , \quad a_1a_2a_3\mu = a_1a_2\lambda a_3\lambda .$$

In either case this makes the original algebra in V_2 into an algebra in V_3, because the laws

$$a\beta_1a\beta_2a\beta_3\mu = a , \quad a_1a_2a_3\mu\beta_i = a_i \qquad (i = 1,2,3)$$

are consequences of the laws of V_2.

This situation, and the obvious generalizations of it that we now consider, will later provide the setting for our discussion of the isomorphisms $G_{n,r} \cong G_{n,s}$ between the automorphism groups of certain pairs of non-isomorphic free algebras $V_{n,r}$, $V_{n,s}$.

In general, algebraic operations that are defined in terms of some given set of operations by formulas of the sort used above to define $\beta_1,\beta_2,\beta_3,\mu$ are called *derived operations*. We shall not attempt to give a formal definition of this term as we only need it to describe obvious generalizations of the operations already defined. We write Der C for the set of all derived operations associated with a given set C of operations. Thus in the above examples β_1,β_2,β_3 belong to Der A (where $A = \{\alpha_1,\alpha_2\}$) and μ belongs to Der $\{\lambda\}$. Note that, since $A = \{\alpha_1,\ldots,\alpha_n\}$ consists of unary operations for any n , the set Der A will also always consist of unary operations.

A set $B = \{\beta_1,\ldots,\beta_N\}$ of unary operations in Der A will be called a *fundamental set* if for any element x of an algebra in V_n the set $\{x\beta_1,\ldots,x\beta_N\}$ is a proper expansion of $\{x\}$. It follows from what has been said about expansions that there is a fundamental set of size N for each integer N of the form $N = 1 + (n-1)d$, where $d \geq 1$. In particular if $n = 2$ then there is a fundamental set of size N for every $N \geq 2$.

<u>LEMMA 3.1.</u> *If* $B = \{\beta_1,\ldots,\beta_N\}$ *is a fundamental set in* Der A *then there exists an* N*-ary operation* μ *in* Der $\{\lambda\}$ *such that*

$$a\beta_1\ldots a\beta_N\mu = a$$

$$a_1\ldots a_N\mu\beta_i = a_i \qquad (i = 1,2,\ldots,N)$$

are laws of every algebra in V_n .

By the remarks preceding the lemma, there is a positive integer d such that $N = 1 + (n-1)d$. We prove the lemma by induction on d .

If $d = 1$, then $N = n$ and $\beta_1,\ldots,\beta_N$ are a permutation of $\alpha_1,\ldots,\alpha_n$. Suppose $\beta_i = \alpha_{\pi(i)}$, for $i = 1,2,\ldots,n$, where $\pi \in S_n$.

In this case we define μ by

$$a_1a_2\ldots a_n\mu = a_{\pi^{-1}(1)}\ldots a_{\pi^{-1}(n)}\lambda \ .$$

It is easy to check that the above laws hold.

Suppose next that $d > 1$. Then there is a fundamental set C such that the set xB is a simple expansion of xC for every element x . Suppose that $C = \{\gamma_1,\ldots,\gamma_{N-n+1}\}$. By rearranging elements if necessary we may assume that B has the form

$$B = \{\gamma_1,\ldots,\gamma_{N-n},\gamma_{N-n+1}\alpha_1,\ldots,\gamma_{N-n+1}\alpha_n\} \ .$$

Now $|C| = N-n+1 = 1 + (n-1)(d-1)$, so by induction there is an $(N-n+1)$-ary operation ν in $\mathrm{Der}\,\{\lambda\}$ such that

$$a\gamma_1\ldots a\gamma_{N-n+1}\nu = a$$
$$a_1\ldots a_{N-n+1}\nu\gamma_i = a_i \qquad (i = 1,2,\ldots,N-n+1) \ ,$$

for all elements $a,a_1,\ldots,a_{N-n+1}$. If we define μ by

$$a_1\ldots a_N\mu = a_1\ldots a_{N-n}(a_{N-n+1}\ldots a_N\lambda)\nu$$

then it is again easy to check that μ has the required properties.

This lemma shows that if S is an algebra of V_n under the operations $\alpha_1,\ldots,\alpha_n,\lambda$ then, for any fundamental set $B = \{\beta_1,\ldots,\beta_N\}$, we can make S into an algebra of V_N under new operations $\beta_1,\ldots,\beta_N,\mu$. We shall denote the algebra obtained from S in this way by S_B . (It is not necessary to specify μ , as B determines μ uniquely.)

LEMMA 3.2. *The subalgebra of* $(F_n(X))_B$ *generated by* X *is a free algebra of* V_N *freely generated by* X .

We may suppose that X is non-empty, for if $X = \emptyset$ then $F_n(X) = \emptyset$ and the result is trivial.

Let S denote the subalgebra of $(F_n(X))_B$ generated by X . We show first that S is relatively free. Let θ be any mapping from X into S . If we think of θ as a mapping from X into $F_n(X)$ then because $F_n(X)$ is free we can extend θ to an endomorphism, $\hat{\theta}$ say, of $F_n(X)$. The mapping $\hat{\theta}$ is also an endomorphism of $(F_n(X))_B$ because $\beta_1,\ldots,\beta_N,\mu$ are derived operations; moreover since $X\theta \subseteq S$ the restriction of $\hat{\theta}$ to S is an endomorphism of S . Thus an arbitrary map $X \to S$ can be extended to an endomorphism of S : hence S is a relatively free algebra, freely generated by X .

However S belongs to V_N , which is a minimal variety by Lemma 2.8 *(iii)*. Therefore, since it is non-empty, S must be a free algebra of V_N , freely generated by X .

LEMMA 3.3. *If* X *is finite and* B *is a fundamental set, then a set of elements of* $X\langle B\rangle$ *is an expansion of* X *quâ* B*-basis if and only if it is an expansion of* X *quâ* A*-basis.*

A simple B-expansion (that is, a simple expansion using the operations in B) is an A-expansion by definition, so the "only if" part of the lemma is obvious.

Suppose now that U is an A-expansion of X such that $U \subseteq X\langle B\rangle$. We apply the criterion of Lemma 2.5 *(ii)* to show that U is a B-expansion of X . Firstly, U cannot contain a pair of elements such that, as B-words, one is an initial segment of the other, otherwise one of these would be an initial segment of the other as A-words also, which would contradict the assumption that U is an A-expansion of X . Secondly, if

v is any element of $X\langle B\rangle$ then by Lemma 2.5 *(ii)* there is an element u in U such that, as A-words, one of u,v is an initial segment of the other. If

$$u = x\beta_{i_1}\ldots\beta_{i_k} ,$$

$$v = x'\beta_{j_1}\ldots\beta_{j_\ell} ,$$

where $x,x' \in X$, then it follows that $x = x'$, and that one of β_{i_1},β_{j_1} is an initial segment of the other when these are expressed as products of elements of A. Since B is a fundamental set, the latter can be true only if $\beta_{i_1} = \beta_{j_1}$. Similarly we find that $\beta_{i_2} = \beta_{j_2}, \ldots ,\beta_{i_s} = \beta_{j_s}$ where $s = \min(k,\ell)$; hence one of u,v is an initial segment of the other as B-words also. Lemma 2.5 *(ii)* now shows that U is a B-expansion of X, as claimed.

<u>LEMMA 3.4.</u> *If* B *and* C *are fundamental sets, then so is* $BC = \{\beta\gamma \mid \beta \in B, \gamma \in C\}$.

Let x be an element of any algebra in V_n. Since C is a fundamental set, $x\beta C = \{x\beta\gamma \mid \gamma \in C\}$ is a proper expansion of $\{x\beta\}$ for every $\beta \in B$. It follows that xBC is a proper expansion of xB. But xB is a proper expansion of $\{x\}$ because B is a fundamental set. Hence xBC is a proper expansion of $\{x\}$, and the result follows.

4. THE GROUPS $G_{n,r}$: FINITE PRESENTATION

In this and the following sections $G_{n,r}$ is the automorphism group of $V_{n,r} = F_n(X)$, for a fixed set X of r elements. The symbols Y and Z will be reserved for expansions of X .

LEMMA 4.1. *If* $\{\theta_1,\ldots,\theta_s\}$ *is a finite subset of* $G_{n,r}$ *then there is a unique minimal expansion* Y *of* X *such that* $Y\theta_i \subseteq X\langle A\rangle$, $i = 1,2,\ldots,s$. *In other words any other expansion of* X *with this property is an expansion of* Y .

By Lemma 2.4, there is an expansion Y of X such that $X\langle A\rangle \cap \bigcap_{i=1}^{s} (X\theta_i^{-1})\langle A\rangle = Y\langle A\rangle$. Then

$Y\theta_i \subseteq Y\langle A\rangle\,\theta_i \subseteq (X\theta_i^{-1})\langle A\rangle\,\theta_i = X\langle A\rangle$. Conversely, if $Z \subseteq X\langle A\rangle$, and $Z\theta_i \subseteq X\langle A\rangle$ for all i then $Z \subseteq Y\langle A\rangle$, whence Z is an expansion of Y .

In the notation of the lemma, if Y is a d-fold expansion of X , so that $|Y| = r + (n-1)d$, we say that the set $\{\theta_1,\ldots,\theta_s\}$ has *depth* d . The two most important cases are (i) when the set consists of a single element and (ii) when the set consists of elements $\theta_1, \theta_1\theta_2, \ldots, \theta_1\theta_2\ldots\theta_s$; in this second case we shall say that d is the *depth of the relation* $\theta_1\ldots\theta_s = \theta$ (and s is its length).

If θ is an element of $G_{n,r}$, by a *symbol* for θ we mean an expression

$$\begin{pmatrix} y_1 & \cdots & y_N \\ z_1 & \cdots & z_N \end{pmatrix}$$

where $Y = \{y_1,\ldots,y_N\}$ and $Z = \{z_1,\ldots,z_N\}$ are expansions of X , and $y_i\theta = z_i$, $i = 1,\ldots,N$. If $Y\langle A\rangle = X\langle A\rangle \cap X\theta^{-1}\langle A\rangle$ then

$Y\theta\langle A\rangle = X\theta\langle A\rangle \cap X\langle A\rangle$ and by Lemma 2.4, $Y\theta$ is an expansion of X. Hence by Lemma 4.1, every element has a symbol. If $N = r + (n-1)d$, then θ has depth at most d. If θ has depth less than d then since any expansion whose image under θ is in $X\langle A\rangle$ is an expansion of the minimal one, the columns of the symbol can be so reordered that it has the form

$$\begin{Bmatrix} u\alpha_1 \ldots u\alpha_n & y_{n+1} \ldots y_N \\ v\alpha_1 \ldots v\alpha_n & z_{n+1} \ldots z_N \end{Bmatrix},$$

and conversely.

Similarly, by a *symbol for the relation* $\theta_1\theta_2\ldots\theta_s = \theta$ we mean an array

$$\begin{Bmatrix} y_{11} & \ldots & y_{1N} \\ \vdots & & \vdots \\ y_{s+1,1} & \ldots & y_{s+1,N} \end{Bmatrix}$$

where for $i = 1,\ldots,s$

$$\begin{Bmatrix} y_{i1} & \ldots & y_{iN} \\ y_{i+1,1} & \ldots & y_{i+1,N} \end{Bmatrix}$$

is a symbol for θ_i, and hence

$$\begin{Bmatrix} y_{11} & \ldots & y_{1N} \\ y_{s+1,1} & \ldots & y_{s+1,N} \end{Bmatrix}$$

is a symbol for θ. Again, if $N = r + (n-1)d$, the relation has depth at most d, and it has depth less than d if and only if, after rearrangement of the columns if necessary, the symbol has the form

$$\begin{pmatrix} u_1\alpha_1 \cdots u_1\alpha_n & y_{1,n+1} \cdots y_{1N} \\ u_2\alpha_1 \quad\;\; u_2\alpha_n & y_{2,n+1} \cdots y_{2N} \\ \vdots \qquad\quad \vdots & \vdots \qquad\quad \vdots \\ u_{s+1}\alpha_1 \cdots u_{s+1}\alpha_n & y_{s+1,n+1} \cdots y_{s+1,N} \end{pmatrix} .$$

LEMMA 4.2. *If* $d \geq 4$, *an element* θ *of* $G_{n,r}$ *of depth* d *can be expressed as a product of elements of depth less than* d .

Because $d \geq 4$, we have (i) $N = r + (n-1)d \geq 3n-1$ and (ii) there exists a d-fold expansion of X of the form $(u\alpha_1,\ldots,u\alpha_n,v\alpha_1,\ldots,v\alpha_n,w_{2n+1},\ldots,w_N)$. Let

$$\begin{pmatrix} y_1 & \cdots & y_N \\ z_1 & \cdots & z_N \end{pmatrix}$$

be a symbol for θ . Because $d \geq 1$, $\{y_1,\ldots,y_N\}$ contains a subset $\{a\alpha_1,\ldots,a\alpha_n\}$ and $\{z_1,\ldots,z_N\}$ a subset $\{b\alpha_1,\ldots,b\alpha_n\}$. There are two cases. Suppose first that no column of the symbol contains more than one of the $2n$ elements. Then, rearranging the columns if necessary, and using (ii); we can insert an extra row in the symbol to obtain

$$\begin{pmatrix} a\alpha_1 & \cdots & a\alpha_n & y_{n+1} & \cdots & y_{2n} & y_{2n+1} & \cdots & y_N \\ u\alpha_1 & \cdots & u\alpha_n & v\alpha_1 & \cdots & v\alpha_n & w_{2n+1} & \cdots & w_N \\ z_1 & \cdots & z_n & b\alpha_1 & \cdots & b\alpha_n & z_{2n+1} & \cdots & z_N \end{pmatrix}$$

which is the symbol of a relation $\theta = \theta_1\theta_2$, where θ_1, θ_2 have depth at most $d-1$ in view of the observation made in the paragraph in which symbol is defined. If, on the other hand $\{a\alpha_1,\ldots,a\alpha_n\}$, $\{b\alpha_1,\ldots,b\alpha_n\}$ between them occupy at most $2n-1$ columns, then by (i) there are n free columns at least left over. Again we rearrange the columns if necessary to obtain

$$\left\{\begin{matrix} a\alpha_1\ldots a\alpha_n & y_{n+1}\ldots y_{N-n} & y_{N-n+1}\ldots y_N \\ u\alpha_1\ldots u\alpha_n & \ldots & v\alpha_1 \;\ldots\; v\alpha_n \\ \ldots u\alpha_{i_1} \;\ldots & u\alpha_{i_n} \;\ldots & v\alpha_1 \;\ldots\; v\alpha_n \\ \ldots b\alpha_{i_1} \;\ldots & b\alpha_{i_n} \;\ldots & z_{N-n+1}\ldots z_N \end{matrix}\right\}$$

which is a symbol of a relation $\theta = \theta_1\theta_2\theta_3$, where $\theta_1, \theta_2, \theta_3$ have depth at most $d-1$.

Note that we have defined θ_1, θ_2 in the first case and $\theta_1, \theta_2, \theta_3$ in the second case such that the relation $\theta = \theta_1\theta_2$ (respectively $\theta = \theta_1\theta_2\theta_3$) has depth (exactly) d .

REMARK : If $r \geq 2$, then we can replace $d \geq 4$ in the lemma by $d \geq 3$ since (i) and (ii) are still true.

COROLLARY $G_{n,r}$ *is generated by the elements of depth at most* 3.

We prove next a result which, though it is essentially only a restatement of what we have already, puts in some technical detail which will be useful when we come to consider defining relations.

LEMMA 4.3. *With each element* θ *of* $G_{n,r}$ *we can associate a word* w_θ *in the elements of depth at most* 3 *such that*

(i) *if* θ *has depth* $d \leq 3$, *then* $w_\theta \equiv \theta$;

(ii) *if* θ *has depth* $d \geq 4$, *then* $w_\theta = \theta$ *is a relation of depth* d ;

(iii) *if* $\theta_1\theta_2\ldots\theta_s = 1$ *is a relation of depth* d , *then* $w_{\theta_1}w_{\theta_2}\ldots w_{\theta_s} = 1$ *is a relation of depth at most* d .

We first discuss the meaning of condition *(ii)*. If $\theta_1\ldots\theta_s = \theta$ is a relation of depth d , where d is the depth of θ , we have a symbol

$$(*) \qquad \left\{\begin{matrix} y_{11} & \ldots & y_{1N} \\ \vdots & & \vdots \\ y_{s+1,1} & \ldots & y_{s+1,N} \end{matrix}\right\}$$

for the relation, where $N = r + (n-1)d$. Then $Y_1 = \{y_{11},\ldots,y_{1N}\}$ is an expansion of X such that $Y_1 \subseteq X\langle A\rangle$, and so it is an expansion of the minimal such expansion Y , whose existence is guaranteed by Lemma 4.1. But since θ has depth d , we have $|Y| = r + (n-1)d = N$ also, so that $Y = Y_1$. If now

$$\begin{pmatrix} u_1 & \cdots & u_M \\ v_1 & \cdots & v_M \end{pmatrix}$$

is any symbol for θ , then $U = \{u_1,\ldots,u_M\}$ is an expansion of Y_1 . Applying this expansion to each row of (*), we see that the symbol

$$\begin{pmatrix} u_1 & \cdots & u_M \\ v_1 & \cdots & v_M \end{pmatrix}$$

can be filled out, by adding more rows, to a symbol for the relation $\theta_1\ldots\theta_s = \theta$. That is, *if (ii) holds for some element* θ , *then every symbol for* θ *can be filled out, by adding more rows, to a symbol for the relation* $w_\theta = \theta$.

We now choose, by induction on d , words w_θ satisfying *(i)* and *(ii)*. Suppose θ has depth d , and words have been chosen for all θ_i of depth less than d . If $d \leq 3$ there is no problem. So assume $d \geq 4$. Then by the argument in the proof of Lemma 4.2, $\theta = \theta_1\theta_2$ or $\theta = \theta_1\theta_2\theta_3$, where each θ_i has depth less than d , and this relation is of depth d . By the argument of the previous paragraph, a symbol for the relation $\theta = \theta_1\theta_2$, or $\theta = \theta_1\theta_2\theta_3$ can be filled out to a symbol for the relation $\theta = w_{\theta_1}w_{\theta_2}$ or $\theta = w_{\theta_1}w_{\theta_2}w_{\theta_3}$, so that this relation also is of depth d . So we may define $w_\theta = w_{\theta_1}w_{\theta_2}$, or $w_\theta = w_{\theta_1}w_{\theta_2}w_{\theta_3}$ and have *(ii)*.

Now *(iii)* follows automatically; for any symbol for the relation $\theta_1\ldots\theta_s = 1$ can be filled out to a symbol for the relation $w_{\theta_1}\ldots w_{\theta_s} = 1$.

<u>LEMMA 4.4.</u> *If* $d \geq 7$, *then any relation* $\theta_1 \ldots \theta_s = 1$ *of depth* d *between elements* $\theta_1, \ldots, \theta_s$ *of depth less than* d *is a consequence of relations of depth less than* d .

Because $d \geq 7$ we have (i) $N = r + (n-1)d \geq 5n-2$, and (ii) there exists a d-fold expansion of X of the form $(u\alpha_1, \ldots, u\alpha_n, v\alpha_1, \ldots, v\alpha_n, w\alpha_1, \ldots, w\alpha_n, y_{3n+1}, \ldots, y_N)$. Let

$$\begin{pmatrix} y_{11} & \cdots & y_{1N} \\ \vdots & & \vdots \\ y_{s+1,1} & \cdots & y_{s+1,N} \end{pmatrix}$$

be a symbol for the relation $\theta_1 \ldots \theta_s = 1$. If we modify this symbol by inserting the row $(c_1, \ldots, c_N)$ between the i-th and (i+1)-st rows, we get a symbol for the relation $\theta_1 \ldots \theta_{i-1} \phi_1 \phi_2 \theta_{i+1} \ldots \theta_s = 1$, where

$$\begin{pmatrix} y_{i1} & \cdots & y_{iN} \\ c_1 & \cdots & c_N \\ y_{i+1,1} & \cdots & y_{i+1,N} \end{pmatrix}$$

is a symbol of the relation of $\phi_1 \phi_2 = \theta_i$, and these two relations are obviously equivalent to the original relation. We shall say one set of symbols is *equivalent* to another if the relations defined by the first set are equivalent to those defined by the second set. The symbol above corresponds to a relation of depth less than d , if possibly after permuting the columns, it has the form

$$\begin{pmatrix} a\alpha_1 \ldots a\alpha_n \ldots \\ b\alpha_1 \ldots b\alpha_n \ldots \\ c\alpha_1 \ldots c\alpha_n \ldots \end{pmatrix}$$

We shall describe these rows as being *linked* by the first n columns and say the *linkage* between them occupies the first n columns. If three rows of the new symbol are linked, then the original symbol is equivalent to the new symbol and a symbol of depth less than d. *Thus if we insert into the symbol new rows which are linked to the rows on either side, or remove such rows, we transform the symbol of the relation we started with into a symbol for a relation equivalent to it under the relations of depth less than* d. Thus to prove the lemma we have to show that by a sequence of such transformations we can transform the given symbol to a symbol for the identical relation : that is, to a symbol consisting just of two identical rows. We do this by induction on s, so that it is sufficient to produce a symbol with fewer rows than the one we started with. Notice that since each θ_i has depth less than d, each pair of consecutive rows is linked, and because we are dealing with a relation $\theta_1 \ldots \theta_s = 1$, the first and last rows are the same.

If $s = 1$, we are finished, so we may suppose $s \geq 2$. If three consecutive rows are linked by the same n columns, we can remove the middle one. This is a *type* I *reduction*. Because the first and last rows are identical, a type I reduction is always possible if $s = 2$, so we may suppose $s \geq 3$. Suppose next that there exist four consecutive rows, such that the $3n$ columns by which they are linked are all different. Then, using (ii) we can insert a new row between the second and third, and then delete the original second and third rows :

$$\left(\begin{array}{lll} a\alpha_1\ldots a\alpha_n & & \\ b\alpha_1\ldots b\alpha_n & c\alpha_1\ldots c\alpha_n & \\ & d\alpha_1\ldots d\alpha_n & e\alpha_1\ldots e\alpha_n\ldots \\ & & f\alpha_1\ldots f\alpha_n\ldots \end{array}\right) \longrightarrow \left(\begin{array}{lll} a\alpha_1\ldots a\alpha_n & & \\ b\alpha_1\ldots b\alpha_n & c\alpha_1\ldots c\alpha_n & \\ x\alpha_1\ldots x\alpha_n & y\alpha_1\ldots y\alpha_n & z\alpha_1\ldots z\alpha_n\ldots \\ & d\alpha_1\ldots d\alpha_n & e\alpha_1\ldots e\alpha_n\ldots \\ & & f\alpha_1\ldots f\alpha_n\ldots \end{array}\right)$$

$$\longrightarrow \left(\begin{array}{lll} a\alpha_1\ldots a\alpha_n & & \\ x\alpha_1\ldots x\alpha_n & y\alpha_1\ldots y\alpha_n & z\alpha_1\ldots z\alpha_n \\ & & f\alpha_1\ldots f\alpha_n \end{array}\right) .$$

This is a *type* II *reduction*. Again we notice that if $s = 3$ then because the first and last rows are identical and any two consecutive rows are linked, either a type I reduction or a type II reduction is always possible. So we may suppose that $s \geq 4$, and that no type I or type II reduction is possible.

Then there are 5 consecutive rows, and because a type II reduction is impossible, the linkages between them occupy at most $4n-2$ columns; for there is overlap between the linkages between row 1 and row 2 and between row 3 and row 4, and also between the linkages between row 2 and row 3 and between row 4 and row 5 :

$$\left(\begin{array}{llll} a\alpha_1\ldots a\alpha_n & & & \\ b\alpha_1\ldots b\alpha_n & & c\alpha_1\ldots c\alpha_n & \\ \ldots\ e\alpha_1\ldots e\alpha_2\ldots & e\alpha_n & d\alpha_1\ldots d\alpha_n & \\ \quad f\alpha_1\ldots f\alpha_2\ldots & f\alpha_n\ldots & & g\alpha_1\ldots g\alpha_2\ldots g\alpha_n\ldots \\ & & & h\alpha_1\ldots h\alpha_2\ldots h\alpha_n\ldots \end{array}\right)$$

Thus by (i) there are n columns not involved in any of these linkages. Now given any three consecutive rows, we can apply a transformation of the form

$$\left\{\begin{array}{ll} a\alpha_1\ldots a\alpha_n & \\ b\alpha_1\ldots b\alpha_n & c\alpha_1\ldots c\alpha_n\ldots \\ & d\alpha_1\ldots d\alpha_n\ldots \end{array}\right\} \longrightarrow \left\{\begin{array}{lll} a\alpha_1\ldots a\alpha_n & & \\ b\alpha_1\ldots b\alpha_n & c\alpha_1\ldots c\alpha_n & \\ x\alpha_1\ldots x\alpha_n & y\alpha_1\ldots y\alpha_n & z\alpha_1\ldots z\alpha_n\ldots \\ & d\alpha_1\ldots d\alpha_n & \end{array}\right\}$$

$$\longrightarrow \left\{\begin{array}{lll} a\alpha_1\ldots a\alpha_n & & \\ x\alpha_1\ldots x\alpha_n & y\alpha_1\ldots y\alpha_n & z\alpha_1\ldots z\alpha_n \\ & d\alpha_1\ldots d\alpha_n & \end{array}\right\}$$

to replace the middle row by another one, which is linked to the first and third by the same columns, and has entries of the form $z\alpha_1\ldots z\alpha_n$ in any given n columns distinct from these. If we replace the second, third and fourth rows of our original set of five consecutive rows using the same n "free" columns in each case, we can then delete the new middle row. So we achieve a reduction in any case, completing the proof of the lemma.

REMARK : If $r \geq 2$ we can replace $d \geq 7$ by $d \geq 6$, and if $r \geq 3$, by $d \geq 5$, since (i) and (ii) still hold.

LEMMA 4.5. *If we take* $G_{n,r}$ *to be generated by the elements of depth at most* 3, *then as defining relations we may take the relations between them of depth at most* 6 .

This is not quite a corollary of Lemma 4,4 , because the process there described introduces new generators whose depths we have no obvious means of controlling. This is the difficulty that Lemma 4.3 was designed to overcome. Let R be the set of relations of depth at most 6 , between generators of depth at most 3 , and let us prove by induction on its depth d that any relation $\theta_1\ldots\theta_s = 1$ say between generators of depth at most 3 is a consequence of R . If $d \leq 6$ there is nothing to prove. If $d \geq 7$, then the relation is a consequence of a number of others, of which $\phi_1\ldots\phi_t = 1$ say is typical, of depth less than d. Introduce words w_{ϕ_i} as in Lemma 4.4. The relation $\phi_1 \ldots \phi_t = 1$, and hence our original relation $\theta_1 \ldots \theta_s = 1$ is a consequence of the relations $w_\phi = \phi$, for generators of depth greater than 3, and the relations $w_{\phi_1} \ldots w_{\phi_t} = 1$. These relations are relations between generators of depth at most 3 and have depth less than d, so by the induction hypothesis they are consequences of R. Hence our original relation is a consequence of R and the relations $w_\phi = \phi$. But these relations merely define generators which do not occur in the relation $\theta_1 \ldots \theta_s = 1$. Hence this relation is a consequence of R, as required.

THEOREM 4.6. *Each group* $G_{n,r}$ *is finitely presented.*

For fixed d, the number of ordered bases of depth d is finite, and equal to K_d, say. Thus there are only a finite number of generators of depth d. There are an infinity of relations of depth d. However, if a relation of depth d has length greater than K_d, some two rows in a symbol for it (apart from the first and last) must coincide, and it is easy to see that this implies that it is a consequence of shorter relations (between the same generators). Thus as a set of defining relations we may take those of depth at most 6 and length at most K_6, and these are certainly finite in number.

5. THE GROUPS $G_{n,r}$: SIMPLICITY

We order the finite basis X arbitrarily and the set A of operations by setting $\alpha_i < \alpha_j$ whenever $i < j$, and then any expansion of X lexicographically. If θ is an element of $G_{n,r}$, then by Lemma 4.1 there is an expansion Y of X such that $Y\theta \subseteq X\langle A\rangle$. If Y is taken to be an ordered set in lexicographic order, then there will be another expansion Z of X, ordered lexicographically, such that $Y\theta$ with the order inherited from Y (that is $y_1 < y_2$ implies $y_1\theta < y_2\theta$) is a permutation of Z. Consider the case n odd. We show that the parity of the permutation $Y\theta$ of Z depends only on θ and (*a priori* at least) on X, and not on Y. For the permutation is odd or even respectively when the number of pairs (y_1, y_2) with $y_1 < y_2$ but $y_1\theta > y_2\theta$ (in the Z-ordering) is odd or even. Suppose we replace Y by $Y^* = Y \setminus \{y\} \cup \{y\alpha_1, \ldots, y\alpha_n\}$ and correspondingly Z by $Z^* = Z \setminus \{z\} \cup \{z\alpha_1, \ldots, z\alpha_n\}$ where $z = y\theta$. Then $y < y_2$ and $y\theta > y_2\theta$ imply $y\alpha_i < y_2$ and $y\alpha_i\theta = y\alpha\theta_i > y_2\theta$ so the pair (y, y_2) is replaced by the pairs $(y\alpha_i, y_2)$, and similarly a pair (y_1, y) with $y_1 < y$ is replaced by n pairs $(y_1, y\alpha_i)$. Since n is odd the parity of the number of pairs is unchanged. Since any two expansions Y_1, Y_2 with $Y_i\theta \subseteq X\langle A\rangle$ are expansions of the shortest such Y, the invariance of parity extends to all such Y_i. Thus elements of $G_{n,r}$ can be classified as either odd or even and, since the odd and even elements multiply with the usual rules for parity the even elements form a normal subgroup $G^+_{n,r}$ of index two in $G_{n,r}$. *A priori*, as we have said, this subgroup depends on X, but we shall prove that it is simple whence it is independent of X. (A nonabelian group cannot have two distinct simple subgroups of index 2, or they would each have a subgroup of index 2, contradicting their simplicity.)

For the sake of a uniform notation, we write $G^+_{n,r} = G_{n,r}$ when n is even.

LEMMA 5.1. *A nontrivial normal subgroup of* $G_{n,r}$ *contains a nontrivial element of finite order.*

Suppose the normal subgroup N contains the element $\theta \neq 1$, and that Y and Z are expansions of X such that $Y\theta = Z$. If $Y = Z$ then θ, being a permutation of Y, is of finite order, and we are home; so we suppose $Y \neq Z$. By Lemma 2.5 we can choose z_0 in Z so that z_0 is a proper initial segment of some element y of Y. Thus Y contains an expansion of $z_0\alpha_1,\dots,z_0\alpha_n$ and y may be chosen in this expansion such that $y\theta \neq z_0$; let $z = y\theta$. We now define ϕ by

$$z'\phi = z' \quad \text{for} \quad z' \in Z \setminus \{z\}, \quad z\alpha_i\phi = z\alpha_{i+1} \quad \text{for} \quad i = 1,\dots,n-1$$

and

$$z\alpha_n\phi = z\alpha_1 .$$

(If n is odd, ϕ induces an even permutation of $Z^* = Z \setminus \{z\} \cup \{z\alpha_1,\dots,z\alpha_n\}$ so that $\phi \in G^+_{n,r}$). Observe that $z_0\phi = z_0$ and, since z_0 is an initial segment of y, $y\alpha_i\phi = y\alpha_i$ for any i. We then easily calculate that if $\psi = \theta\phi\theta^{-1}\phi^{-1}$,

$$y'\psi = y'\phi^{-1} \quad \text{for} \quad y' \in Y \setminus \{y\},$$

$$y\alpha_i\psi = y\alpha_{i+1}\phi^{-1} = y\alpha_{i+1} \quad \text{for} \quad i = 1,\dots,n-1,$$

and

$$y\alpha_n\psi = y\alpha_1\phi^{-1} = y\alpha_1 .$$

Plainly ψ is a nontrivial element of N. Clearly ϕ and ψ have order n.

LEMMA 5.2. *A nontrivial normal subgroup of* $G^+_{n,r}$ *contains all elements of* $G^+_{n,r}$ *of finite order.*

Let ϕ be an element of $G^+_{n,r}$ of finite order. By Lemma 2.4 for every expansion Y of Z there is an expansion Z of X such that

$\cap\, (Y\phi^i) \langle A \rangle = Z \langle A \rangle$. Because ϕ commutes with the elements of A , $Z\phi = Z$. If n is odd, the fact that ϕ belongs to $G^+_{n,r}$ implies that ϕ induces an even permutation on Z . If n is even, then ϕ induces an even permutation on $Z^* = \{z\alpha_i \mid z \in Z , \alpha_i \in A\} = ZA$ since the pair (z_1,z_2) is replaced by the n^2 pairs $(z_1\alpha_i, z_2\alpha_j)$. In any case ϕ induces an even permutation on ZA^s for all $s \geq 1$ so *there is an arbitrarily large expansion* Z *of* X *such that* $Z\phi = Z$ *and* ϕ *induces an even permutation on* Z .

Now by Lemma 5.1, a nontrivial normal subgroup N of $G^+_{n,r}$ contains a nontrivial element θ_1 of finite order. Applying the above argument to θ_1 , there is an expansion Y of X with $Y\theta_1 = Y$, and $|Y| \geq 5$. By the normality of N , N contains the whole alternating group on Y , and hence contains a nontrivial element θ_2 with $Y\theta_2 = Y$ such that θ_2 has a fixed point on Y (for example θ_2 could be a 3-cycle). But then $Y^*\theta_2 = Y^*$ also, where $Y^* = Y \setminus \{y\} \cup \{y\alpha_i \mid i = 1,\ldots,n\}$; and iterating θ_2 stabilizes bases of size $|Y| + (n-1)d$ for all non-negative d . By the normality of N , N contains the alternating group on each such basis. But if two bases U and V have $|U| = |V| \geq 2$ then there is an element ψ of $G^+_{n,r}$ with $U\psi = V$, whence if N contains the whole alternating group on one of these, it contains the alternating group on the other. Thus N contains the alternating group on all sufficiently large bases. Now by the result of the first paragraph of this proof, N contains all elements of $G^+_{n,r}$ of finite order.

<u>LEMMA 5.3.</u> $G^+_{n,r}$ *is generated by its elements of finite order.*

Using an expansion if necessary we can and will suppose $r \geq 3$. We prove, by induction on d , that an element θ of $G^+_{n,r}$ of depth d belongs to the subgroup generated by the elements of finite order. If $d = 0$ then θ permutes X and so is of finite order. If $d \geq 1$ then

θ has a symbol

$$\begin{pmatrix} u\alpha_1 \ldots u\alpha_n \; w_1 \ldots w_k \\ \ldots v\alpha_1 \ldots v\alpha_2 \ldots v\alpha_n \ldots \end{pmatrix}$$

where $k \geq 2$ because $r \geq 3$. Because $k \geq 2$, we can insert a row

$$\begin{pmatrix} u\alpha_1 \ldots u\alpha_n \; w_1 \ldots w_k \\ \ldots u\alpha_1 \ldots u\alpha_2 \ldots u\alpha_n \ldots \\ \ldots v\alpha_1 \ldots v\alpha_2 \ldots v\alpha_n \ldots \end{pmatrix}$$

which is an even permutation of the first row, and obtain a symbol for a relation $\theta = \phi\psi$, where ϕ permutes the basis $u\alpha_1,\ldots,u\alpha_n,w_1,\ldots,w_k$ and hence is an element of $G^+_{n,r}$ of finite order, and ψ has depth at most $d-1$. The lemma follows.

The next theorem is an obvious consequence of the last three lemmas.

THEOREM 5.4. *For all* n,r, $G^+_{n,r}$ *is simple.*

6. FINITE SUBGROUPS OF THE $G_{n,r}$: NON-ISOMORPHISMS

If H is a fixed finite group, we are interested in this section in the conjugacy classes of homomorphisms of H into $G_{n,r}$. Of course, $\rho : H \to G_{n,r}$, $\sigma : H \to G_{n,r}$ are conjugate if, for some θ in $G_{n,r}$ and all h in H, $h\sigma = \theta^{-1}h\rho\theta$.

Let $X_1,\dots,X_t$ be a set of representatives of the isomorphism classes of transitive H-spaces. Let $n_1,\dots,n_t$ be non-negative integers, not all zero, such that $n_1|X_1| + \dots + n_t|X_t| \equiv r\ (n-1)$. Then we can find a free basis X of $V_{n,r}$ of size $\Sigma n_i|X_i|$; we can make X into an H-space which is split into n_i sets isomorphic to X_i for $i = 1,\dots,t$, and we can extend this action to produce a homomorphism of H into $G_{n,r}$. Obviously the choices involved here do not affect the conjugacy class of the homomorphism because there are elements of $G_{n,r}$ which send one free basis to another of the same size or permute a free basis. Thus each such (ordered) set $(n_1,\dots,n_t)$ of integers determines a conjugacy class of homomorphisms. Each conjugacy class of homomorphisms arises in this way : for by an obvious modification of the proof of Lemma 4.1, if $\alpha : H \to G_{n,r}$ is a homomorphism then $H\alpha$ fixes some free basis of $V_{n,r}$. So the question is, which sets of integers correspond to the same conjugacy class of homomorphisms?

If $H\alpha$ fixes both X and Y, then it fixes some expansion Z of both of them, (defined by $Z\langle A\rangle = X\langle A\rangle \cap Y\langle A\rangle$). So the question becomes, how do the n_i change if we pass from X to an expansion also fixed by $H\alpha$? If X_0 is an orbit of H in X, then it is clear that

$$X^* = X \setminus X_0 \cup \{x\alpha_i \mid x \in X_0,\quad i = 1,\dots,n\}$$

is an expansion of X fixed by $H\alpha$, and that every such expansion is the result of a sequence of moves of this sort. But if X corresponds to

$(n_1,\dots,n_t)$ and X^* to $(n_1^*,\dots,n_t^*)$ it is clear that, if X_0 is isomorphic to X_i as H-space then $n_i \neq 0$ and $n_i^* = n_i + n-1$ and $n_j^* = n_j$ for $j \neq i$ since for each k, $\{x\alpha_k \mid x \in X_0\}$ is also isomorphic to X_0. If we define $a \overset{*}{\equiv} b \ (n-1)$ for integers $a \geq 0$ and $b \geq 0$ to mean that $a \equiv b \ (n-1)$ and $a = 0$ if and only if $b = 0$, and extend the notation componentwise to sequences, we see that $(m_1,\dots,m_t)$ and $(n_1,\dots,n_t)$ determine the same conjugacy class of embedding if and only if $(m_i) \overset{*}{\equiv} (n_i) \ (n-1)$. We sum up the discussion in a lemma.

<u>LEMMA 6.1.</u> *If* $X_1,\dots,X_t$ *is a set of representatives of the isomorphism classes of transitive* H*-spaces, then the conjugacy classes of homomorphisms of* H *into* $G_{n,r}$ *are in one to one correspondence with the equivalence classes of solutions of* $n_1|X_1| + \dots + n_t|X_t| \overset{*}{\equiv} r \ (n-1)$ *under the equivalence relation* $\overset{*}{\equiv} \ (n-1)$.

If we are interested in embeddings rather than in homomorphisms, or in $G^+_{n,r}$ rather than $G_{n,r}$, this result has to be modified; but we deal with such questions when they arise rather than try to state general answers.

<u>LEMMA 6.2.</u> *If* p *is a prime which does not divide* $n-1$ *then the number of conjugacy classes of elements of order* p *in* $G^+_{n,r}$ *is* n.

A cyclic group of order p has transitive spaces of 1 and p elements. Thus by Lemma 6.1 the number of conjugacy classes of homomorphisms of a cyclic group of order p in $G_{n,r}$ is the number of inequivalent solutions of

$$n_1 + pn_2 \overset{*}{\equiv} r \ (n-1) .$$

Now n_1 can take any of the n possible values $0,1,\dots,n-1$. The congruence class of n_2 mod $(n-1)$ is then uniquely determined, since p does not divide $n-1$; and so the $(\overset{*}{\equiv})$-class is uniquely determined unless

$n_1 \overset{*}{\equiv} r$, when we may have $n_2 \overset{*}{\equiv} 0$ or $n_2 \overset{*}{\equiv} n-1$. So there are $n+1$ classes of homomorphisms. One of these is the trivial homomorphism, sothere are n embeddings, that is, n conjugacy classes of elements of order p in $G_{n,r}$. If n is even we are done. If n is odd then p is also odd, so elements of order p in $G_{n,r}$ lie in $G^+_{n,r}$. Since p does not divide $n-1$ there is an m such that $m \equiv r\ (n-1)$ and $m \equiv 2\ (p)$ by the Chinese Remainder Theorem. An element of order p of $G^+_{n,r}$ fixes two elements in an expansion Y of size m , and the element of $G_{n,r} \setminus G^+_{n,r}$ which simply interchanges these two will commute with the chosen element of order p in $G^+_{n,r}$. Thus elements of order p conjugate in $G_{n,r}$ are conjugate in $G^+_{n,r}$.

LEMMA 6.3. *If* p^a *is the exact power of* p *dividing* $n-1$ *, then there are positive integers* $c_0, c_1, \ldots, c_a$ *such that if* p^b *is the exact power of* p *dividing* $(n-1,r)$ *then the number of conjugacy classes of elements of order* p^a *in* $G^+_{n,r}$ *is* $c_0 + c_1 + \ldots + c_b$.

A cyclic group of order p^a has, to within isomorphism, precisely one transitive space of size p^b for each integer b with $0 \leq b \leq a$. Thus by Lemma 6.1 the conjugacy classes of homomorphisms from such a group into $G_{n,r}$ are in one-to-one correspondence with the solutions of

$$n_1 + n_2 p + \ldots + n_{a+1} p^a \overset{*}{\equiv} r\ (n-1) .$$

The embeddings evidently correspond to solutions with $n_{a+1} \neq 0$.

Let C be the set of all equivalence classes (under $\overset{*}{\equiv}$) of sequences $(n_1, \ldots, n_{a+1})$ with $n_{a+1} \neq 0$. Every element of C is a solution of the above congruence for some value of r . Writing C_b for the subset of C consisting of equivalence classes of sequences $(n_1, \ldots, n_{a+1})$ with $n_1 = \ldots = n_b = 0$ and $n_{b+1} \neq 0$, we now count the number of elements of C_b satisfying the congruence, for each choice of b and r . If p^b

does not divide r then clearly no element of C_b can be a solution. On the other hand, for each r divisible by p^b there are exactly p^b solutions of the form $(0,\ldots,0,n_{b+1},n_{b+2},\ldots,n_{a+1})$ corresponding to each choice of $n_{b+2},\ldots,n_{a+1}$; this is so because the congruence

$$p^b n_{b+1} \equiv r - (n_{b+2}p^{b+1} + \ldots + n_{a+1}p^a)\ (n-1)$$

has exactly p^b solutions for n_{b+1} when $p^b = (p^b,n-1)$ divides the number on the right-hand side. (Recall that a congruence of the form $cx \equiv d\ (m)$ has (c,m) solutions whenever (c,m) divides d .) Hence, in particular, the number of solutions of the original congruence belonging to C_b is the same for every r divisible by p^b , and is therefore equal to $p^b|C_b| \,/\, (n-1)$. Thus, taking $c_b = p^b|C_b| \,/\, (n-1)$ for each b, we have the result, apart from the fact that we have used $G_{n,r}$ instead of $G^+_{n,r}$.

To obtain the result in the form required, we first show that elements of order p^a in $G^+_{n,r}$ are conjugate in $G^+_{n,r}$ whenever they are conjugate in $G_{n,r}$. It will be enough to show that each element of order p^a in $G^+_{n,r}$ commutes with an element of $G_{n,r} \setminus G^+_{n,r}$. If p is odd, this follows from an argument like that used in the proof of Lemma 6.2. If $p = 2$, then an element of order p^a in $G^+_{n,r}$ induces a permutation on a basis of $V_{n,r}$ whose orbits all have length a power of 2 . Disregarding the trivial case where $a = 0$, we choose an element of $G_{n,r}$ that induces the same cyclic permutation on one of the non-trivial orbits and leaves the other basis elements fixed. This element induces an odd permutation on the basis, so it belongs to $G_{n,r} \setminus G^+_{n,r}$. It also clearly commutes with the chosen element of $G^+_{n,r}$, so our claim is now verified for all p .

If p is odd, then all the conjugacy classes of elements of order p^a lie in $G^+_{n,r}$, so the required result follows from the first part of the proof. Suppose again therefore that $p = 2$. Then the conjugacy classes of elements of order p^a are in one to one correspondence with the solutions of

$$n_1 + 2n_2 + \dots + 2^a n_{a+1} \overset{*}{\equiv} r\,(n-1) \ .$$

Under this correspondence a solution $(n_1,\dots,n_{a+1})$ is associated with a conjugacy class whose elements each induce a permutation having n_i orbits of length 2^{i-1} for $i = 1,2,\dots,a+1$. Since a cycle of even length is an odd permutation, such an element will induce an even permutation if and only if $n_2 + \dots + n_{a+1}$ is even. However, the mapping

$$(n_1,\dots,n_a,n_{a+1}) \mapsto (n_1,\dots,n_a,n_{a+1} + (n-1)/2^a)$$

determines a one-to-one correspondence on the set of solutions of the congruence, and since $(n-1)/2^a$ is odd by hypothesis, the numbers $n_2 + \dots + n_{a+1}$ and $n_2 + \dots + n_a + n_{a+1} + (n-1)/2^a$ have opposite parities. Hence exactly half the conjugacy classes of $G_{n,r}$ lie in $G^+_{n,r}$. We therefore obtain the required result by taking c_b to have half the value assigned to it in the case of odd p , for every b .

THEOREM 6.4. *Necessary conditions for the isomorphism* $G^+_{m,r} \cong G^+_{n,s}$ *are that* $m = n$ *and* $(n-1,r) = (n-1,s)$.

If $m \neq n$ we can choose p to divide neither $m-1$ nor $n-1$; and then by Lemma 6.2 $G^+_{m,r}$ and $G^+_{n,s}$ have different numbers of conjugacy classes of elements of order p . If $(n-1,r) \neq (n-1,s)$ then for some prime p the powers of p dividing $(n-1,r)$ and $(n-1,s)$ are different. By Lemma 6.3, $G^+_{n,r}$ and $G^+_{n,s}$ have different numbers of conjugacy classes of elements of order p^a , for some a .

It may be observed that the present methods can do no more.

LEMMA 6.5. *If* $(r,n-1) = (s,n-1)$ *the number of conjugacy classes of homomorphisms of* H *into* $G_{n,r}$ *and into* $G_{n,s}$ *are the same for any finite* H .

We have $s \equiv ar\ (n-1)$ for some a prime to $n-1$. We use Lemma 6.1. Solutions of $\Sigma n_i|X_i| \overset{*}{\equiv} r$ can be mapped into solutions of $\Sigma n_i|X_i| \overset{*}{\equiv} s$ in a fashion which is one to one on equivalence classes, by mapping $(n_1,\ldots,n_t)$ onto $(an_1,\ldots,an_t)$, the reverse mapping using the inverse of a modulo $n-1$.

The following embedding theorem belongs to this section because of its method of proof, which is similar to that used by P. Hall, "Some constructions for locally finite groups", J. London Math. Soc. **34** (1959), 305-319.

THEOREM 6.6. *Each group* $G^+_{n,r}$ *contains an isomorphic copy of every countable locally finite group.*

For any finite group H , by a *standard* embedding of H in $G_{n,r}$ we mean an embedding α such that for some free basis X of $V_{n,r}$, $|X| = (n-1)|H| + r$, $H\alpha$ fixes X and acts so that it has $n-1$ regular orbits and r fixed points, or an embedding conjugate to one of this form. Observe that α in fact embeds H in $G^+_{n,r}$ (this is obvious if n is even, and if n is odd then $n-1$ is even). Of course, standard embeddings always exist since there are expansions of size $N = (n-1)d + r$ for any $d \geq 0$, and any two standard embeddings of the same H are conjugate because we are dealing with two free bases of the same size. If K is a subgroup of H of index k , then K fixes X , and so acts that it has $(n-1)k$ regular orbits and r fixed points. But $(n-1)k \overset{*}{\equiv} n-1\ (n-1)$, so that $\alpha|_K$ is in fact a standard embedding of K. Put in the other direction, this says that if $K \leq H$, a standard embedding of K can be extended to a standard embedding of H (since all standard embeddings of K are conjugate, and therefore "alike"). But a countable locally finite group L is the union of an ascending chain $H_1 < H_2 < H_3 < \ldots$ of finite subgroups. We choose a standard embedding of H_1 , extend it to a standard embedding of H_2 , then to a standard embedding of H_3 , *etc.*, finishing up with a standard embedding of L .

7. EMBEDDINGS AND ISOMORPHISMS OF THE GROUPS $G_{n,r}$

In this section we use the ideas of section 3 to study the relationships between different groups $G_{n,r}$.

As usual, $A = \{\alpha_1,\ldots,\alpha_n\}$ will denote the set of unary operations of V_n , and $B = \{\beta_1,\ldots,\beta_N\}$ will be a fundamental set in Der A . The operation "inverse" to $\alpha_1,\ldots,\alpha_n$ is denoted by λ , and μ will denote the operation in Der $\{\lambda\}$ "inverse" to $\beta_1,\ldots,\beta_N$: the existence of μ is guaranteed by Lemma 3.1.

For a fixed set X of r elements we now write $F_A(X) = F_n(X) = V_{n,r}$ for the free algebra of V_n freely generated by X . By Lemma 3.2 the subalgebra of $(F_A(X))_B$ generated by X is a free algebra of V_N : we denote this free algebra by $F_B(X)$. Thus the automorphism groups of $F_A(X)$ and $F_B(X)$ are the groups $G_{n,r}$ and $G_{N,r}$ respectively.

LEMMA 7.1. *The group* $G_{n,r}$ *has a subgroup isomorphic to* $G_{N,r}$ *, consisting of those automorphisms* θ *of* $F_A(X)$ *such that* $X\theta \subseteq F_B(X)$ *. A necessary and sufficient condition for an element* ϕ *in* $G_{n,r}$ *to belong to this subgroup is that, for all sufficiently large integers* s *,*

$$(XB^s)\phi \subseteq F_B(X) .$$

Let θ be an element of $G_{n,r}$ such that $X\theta \subseteq F_B(X)$. As in the proof of Lemma 3.2, we see that the restriction $\theta|_{F_B(X)}$ of θ to $F_B(X)$ is an endomorphism of $F_B(X)$.

As $X\theta$ is a finite set there is a bound on the number of μ's involved in any element. Provided we choose s to exceed this bound, we have $(X\theta)B^s \subseteq X\langle B\rangle$. Since θ is an endomorphism, $(XB^s)\theta = (X\theta)B^s$, and hence

$$(XB^s)\theta \subseteq X\langle B\rangle .$$

Now XB^s is a B-expansion of X and hence is also an A-expansion. Since θ is an automorphism of $F_A(X)$, it follows that $(XB^s)\theta$ is an A-expansion of X. But by Lemma 3.3 an A-expansion of X contained in $X\langle B\rangle$ is also a B-expansion of X. Hence $(XB^s)\theta$ is a B-expansion of X, and therefore a free basis of $F_B(X)$. Thus $\theta|_{F_B(X)}$ maps one (finite) free basis of $F_B(X)$ onto another, so it is an automorphism of $F_B(X)$.

It follows that the elements θ such that $X\theta \subseteq F_B(X)$ form a subgroup of $G_{n,r}$, for the above shows that $X\theta^{-1} \subseteq F_B(X)$ for all such elements θ. Also from the above we see that the mapping $\theta \to \theta|_{F_B(X)}$ is an isomorphism from this subgroup onto $G_{N,r}$. Thus the first part of the lemma is proved.

We have already seen that if θ belongs to this subgroup then the condition

$$(XB^s)\theta \subseteq X\langle B\rangle$$

is satisfied for all sufficiently large integers s. Conversely if an element θ satisfies this condition for some s, then since X and XB^s are both free generating sets for $F_B(X)$ we have $X\theta \subseteq F_B(X)$, and the proof is therefore complete.

<u>THEOREM 7.2.</u> $G_{N,r}$ *is a subgroup of* $G_{n,r}$ *whenever* N *has the form* $N = 1 + (n-1)d$ *for some* $d \geq 1$.

By the observation before Lemma 3.1, fundamental sets of size N exist in $\text{Der}\,\{\alpha_1,\ldots,\alpha_n\}$ if and only if N has the form $N = 1 + (n-1)d$, with $d \geq 1$. When N has this form we can choose one such fundamental set B, and we obtain the result by applying Lemma 7.1.

THEOREM 7.3. *If* c *is a divisor of* n , *then* $G_{n,r} \cong G_{n,cr}$.

We prove this by embedding both $G_{n,r}$ and $G_{n,cr}$ in $G_{2,1}$ and showing that the images of the two embeddings coincide.

Suppose that $n = cd$, and let C, D be fundamental sets in $\mathrm{Der}\{\alpha_1, \alpha_2\}$ with $|C| = c$, $|D| = d$. (Here α_1, α_2 are the unary operations of V_2 .) Then by Lemma 3.4 both CD and DC are fundamental sets of size n . Using the fundamental set CD we first embed $V_{n,r}$ in $V_{2r} = F_2(X)$ as in Lemma 3.2. By Lemma 7.1, $G_{2,r} = G_{2,1}$ contains a subgroup $\hat{G}_{n,r}$ isomorphic to $G_{n,r}$, consisting of those elements θ such that, for sufficiently large integers s ,

$$X(CD)^s\theta \subseteq X\langle CD\rangle \quad . \qquad (1)$$

Now C is a fundamental set, so XC is an expansion of X , and consequently $V_{2,r} = F_2(X) = F_2(XC)$. We now embed $V_{n,rc}$ in $F_2(XC)$ using the fundamental set DC . As above, $G_{2,1}$ contains a subgroup $\hat{G}_{n,rc}$ isomorphic to $G_{n,rc}$, consisting of those elements θ such that, for sufficiently large s ,

$$(XC)(DC)^2\theta \subseteq XC\langle DC\rangle \quad . \qquad (2)$$

However if θ is an element for which (1) holds, then

$$\begin{aligned}(XC)(DC)^s\theta &= X(CD)^s \subset \theta \\ &= X(CD)^s\theta C \\ &\subseteq X\langle CD\rangle\ C = XC\langle DC\rangle \ ,\end{aligned}$$

so (2) holds also for this element. Conversely if θ is an element such that (2) holds for some s , then

$$\begin{aligned} X(CD)^{s+1}\theta &= XC(DC)^{s}D\theta \\ &= XC(DC)^{s}\theta D \\ &\subseteq XC\langle DC\rangle D \\ &= X\langle CD\rangle . \end{aligned}$$

Therefore θ belongs to $\hat{G}_{n,r}$ if and only if it belongs to $\hat{G}_{n,rc}$, so that $\hat{G}_{n,r} = \hat{G}_{n,rc}$, and consequently

$$G_{n,r} \cong G_{n,rc}$$

as claimed.

8. EXPLICIT GENERATORS AND RELATIONS FOR $G_{2,1}$

The algebra $V_{2,1}$ has two unary operations α_1, α_2, which we write as α, β in this section for simpiicity. Elements of $V_{2,1}$ are standard forms over a set X with one element, x say, and we simplify our notation by omitting the x and writing simply α, for example, in place of $x\alpha$.

The generators that we take for $G_{2,1}$ are the elements $\kappa, \lambda, \mu, \nu$ defined by the following symbols :

$$\kappa : \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}$$

$$\lambda : \begin{pmatrix} \alpha\alpha & \alpha\beta & \beta \\ \alpha\alpha & \beta & \alpha\beta \end{pmatrix}$$

$$\mu : \begin{pmatrix} \alpha & \beta\alpha & \beta\beta \\ \beta\alpha & \alpha & \beta\beta \end{pmatrix}$$

$$\nu : \begin{pmatrix} \alpha\alpha & \alpha\beta & \beta\alpha & \beta\beta \\ \alpha\alpha & \beta\alpha & \alpha\beta & \beta\beta \end{pmatrix} .$$

(Here λ is a generator, not an operation.) As defining relations between these generators we have the following, the last two of which, in brackets, are consequences of the others :

(1) $\kappa^2 = \lambda^2 = \mu^2 = \nu^2 = 1$

(2) $\lambda\kappa\mu\kappa\lambda\nu\kappa\nu\mu\kappa\lambda\kappa\mu = 1$

(3) $\kappa\nu\lambda\kappa\mu\nu\kappa\lambda\nu\mu\nu\lambda\nu\mu = 1$

(4) $(\lambda\kappa\mu\kappa\lambda\nu)^3 = (\mu\kappa\lambda\kappa\mu\nu)^3 = 1$

(5) $(\lambda\nu\mu)^2\kappa(\mu\nu\lambda)^2\kappa = 1$

(6) $(\lambda\nu\mu\nu)^5 = 1$

(7) $(\lambda\kappa\nu\kappa\lambda\nu)^3\kappa\nu\kappa(\mu\kappa\nu\kappa\mu\nu)^3\kappa\nu\kappa\nu = 1$

(8) $((\lambda\kappa\mu\nu)^2(\mu\kappa\lambda\nu)^2)^3 = 1$

(9) $(\lambda\nu\lambda\kappa\mu\kappa\mu\nu\lambda\nu\mu\kappa\mu\kappa)^4 = 1$

(10) $(\mu\nu\mu\kappa\lambda\kappa\lambda\nu\mu\nu\lambda\kappa\lambda\kappa)^4 = 1$

(11) $(\lambda\mu\kappa\lambda\kappa\mu\lambda\kappa\nu\kappa)^2 = 1$

(12) $(\mu\lambda\kappa\mu\kappa\lambda\mu\kappa\nu\kappa)^2 = 1$

$$\left[\begin{array}{ll} (13) & (\lambda\kappa\mu\kappa)^3 = 1 \\ (14) & (\kappa\nu)^4 = 1 \end{array}\right].$$

In this section we shall sketch the method by which these generators and relations were derived.

In section 4 it was shown that each of the groups $G_{n,r}$ is generated by its elements of depth at most 3 and that every relation between these generators is a consequence of relations of depth at most 6. We shall show that, in the case of $G_{2,1}$, relations of depth at most 6 also suffice to define the group when we use the generators $\kappa, \lambda, \mu, \nu$. A set of generators for $G_{n,r}$ is said to be *smooth* if, for every element θ in $G_{n,r}$, there is a word w_θ in these generators such that $\theta = w_\theta$ is a relation of the same depth as θ. The proof of Lemma 4.5 shows that as defining relations between *any* smooth set of generators we may take the relations of depth at most 6. A *diagram of depth* d for $G_{n,r}$ is a graph whose nodes are identified with d-fold expansions of a free generating set X of $V_{n,r}$ and whose edges are identified with the elements of a specified subset of $G_{n,r}$ (in practice this will be a generating set), such that an edge between two nodes is an element mapping one basis onto the other. We shall construct diagrams for $G_{2,1}$ using the elements $\kappa, \lambda, \mu, \nu$ as edges : because these elements are involutions there will be no need to specify directions on our diagrams.

Observe that the paths on a diagram for $G_{n,r}$ represent elements of $G_{n,r}$ that are expressible as words in the elements used to label the edges. An element θ is represented by a path associated with a word w_θ on a diagram of depth d if and only if $G_{n,r}$ has a relation $\theta = w_\theta$ of depth at most d. Paths that begin and end at the same basis (in other words, circuits) correspond to elements that induce permutations on this basis. In particular paths representing the identity element are circuits, and on a diagram of depth d these correspond to relations $w_\theta = 1$ of depth at most d between the elements used to label the edges.

LEMMA 8.1. *A necessary and sufficient condition for a set of elements of* $G_{n,r}$ *to be a smooth generating set is that, for all* $d \leq 3$, *the diagram of depth* d *be connected and the permutations corresponding to paths beginning and ending at a fixed basis* Y *constitute the full symmetric group* S_Y .

Let S be a set of elements for which the condition on diagrams is satisfied. Note first that, on a connected diagram, if the permutations corresponding to paths beginning and ending at one basis constitute the symmetric group, then the same is true of the permutations corresponding to paths beginning and ending at any other basis.

Now let θ be an element of depth $d \leq 3$ in $G_{n,r}$. Then there exist d-fold expansions Y, Z of X such that $Y\theta = Z$. These bases occur as nodes on the diagram of depth d , and since this diagram is connected there is a path joining the nodes. Hence there is an element

ϕ in $G_{n,r}$ mapping Y onto Z which can be expressed as a word w_ϕ in elements of S so that $\phi = w_\phi$ is a relation of depth at most d. The element $\psi = \theta\phi^{-1}$ induces a permutation on Y so by hypothesis it is represented on the diagram by a path beginning and ending at Y. This path determines a word w_ψ in elements of S such that $\psi = w_\psi$ is a relation of depth at most d. If we now define $w_\theta = w_\psi w_\phi$ then w_θ is a word in elements of S and $\theta = w_\theta$ is a relation of depth d, as required.

To complete the proof of the sufficiency we show how to construct a word w_θ with these properties when θ has depth greater than 3. By Lemma 4.3 the elements of depth at most 3 form a smooth generating set. Hence an element θ of depth $d > 3$ can be expressed as a word, $\theta_1\theta_2\ldots\theta_s$ say, in elements θ_i of depth at most 3 such that the relation $\theta = \theta_1\theta_2\ldots\theta_s$ has depth d. By the first part of the proof we can find words w_{θ_i} of the required type for each θ_i, and we can therefore take for w_θ the word $w_{\theta_1}w_{\theta_2}\ldots w_{\theta_s}$. This proves that the condition on diagrams is sufficient.

For the necessity, suppose S is a smooth generating set for $G_{n,r}$ and consider the diagram of depth d, for arbitrary d. If Y and Z are any two nodes on this diagram, then Y and Z are also d-fold expansions of X. Hence there is an automorphism θ in $G_{n,r}$ mapping Y onto Z. By hypothesis there is a relation $\theta = w_\theta$ of depth at most d which expresses θ as a word in elements of S. As in the proof of Lemma 4.3 we see that the symbol for θ having Y and Z as its rows can be filled out to a symbol for the relation $\theta = w_\theta$. It follows that there is a path from Y to Z on the diagram. Therefore the diagram is connected.

Finally, if π is a permutation belonging to the symmetric group on a basis Y on this diagram, then π extends to an automorphism of

$V_{n,r}$ which maps Y onto itself. This automorphism can be expressed as a word in elements of S by means of a relation of depth at most d, so as above there is a path beginning and ending at Y that corresponds to the permutation π.

Using this lemma we shall verify that $\kappa, \lambda, \mu, \nu$ form a smooth generating set for $G_{2,1}$. To do this we construct the diagrams of depths at most 3 for $G_{2,1}$ and check that the hypothesis of the lemma are fulfilled.

On the diagrams we denote expansions of X by symbols of the form $\textcircled{\alpha}$, $\textcircled{\beta\alpha}$, $\textcircled{\beta\beta\beta}$ and so on. To find the basis represented by such a symbol on the diagram of depth d, start from the unique minimal expansion containing the circled element and expand it to a d-fold expansion of X, first expanding symmetrically from the circled element as far as possible and then carrying out any additional expansions needed at either α or β, whichever one has so far been left unexpanded. Thus, for example,

$\textcircled{\beta\alpha} = (\alpha,\beta\alpha\alpha,\beta\alpha\beta,\beta\beta)$ on the depth 3 diagram,

$\textcircled{\beta\alpha} = (\alpha\alpha,\alpha\beta,\beta\alpha\alpha,\beta\alpha\beta,\beta\beta)$ on the depth 4 diagram,

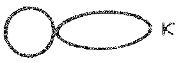
$\textcircled{\beta\alpha} = (\alpha\alpha,\alpha\beta,\beta\alpha\alpha\alpha,\beta\alpha\alpha\beta,\beta\alpha\beta\alpha,\beta\alpha\beta\beta,\beta\beta)$ on the depth 6 diagram,

$\textcircled{\alpha} = (\alpha\alpha,\alpha\beta,\beta)$ on the depth 2 diagram,

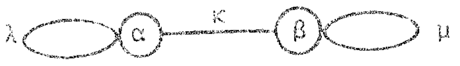
$\textcircled{\alpha} = (\alpha\alpha\alpha,\alpha\alpha\beta,\alpha\beta\alpha,\alpha\beta\beta,\beta)$ on the depth 4 diagram.

In conformity with this notation a basis obtained by expanding X symmetrically is denoted simply by $\bigcirc$. Later we shall introduce further symbols for bases not expressible in this way.

The diagram of depth 0 consists of one node (the basis X) and no edges. The diagram of depth 1 is



(Here ◯ stands for $(\alpha \quad \beta)$.) The permutation induced by κ is non-trivial, so it generates the full symmetric group (of degree 2). The diagram of depth 2 is

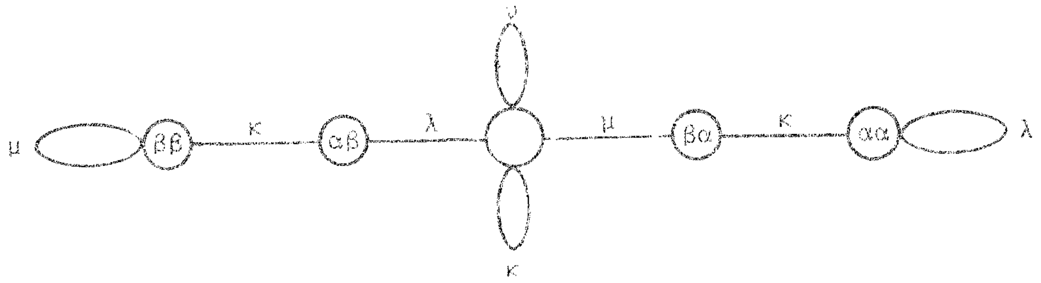


Writing 1, 2, 3 for the elements $\alpha\alpha$, $\alpha\beta$, β of the basis $\textcircled{\alpha}$, we find that the permutations corresponding to the circuits λ, $\kappa\mu\kappa$ at this node are $1(23)$ and $(13)2$ respectively. These generate the symmetric group $S_{\textcircled{\alpha}}$ and, using defining relations for the symmetric group, we obtain the following relations in $G_{2,1}$:

$$\lambda^2 = (\kappa\mu\kappa)^2 = (\lambda\kappa\mu\kappa)^3 = 1 \ .$$

The last of these is relation (13) on page 50; the other relations merely tell us that λ and μ are involutions, which we know already.

The diagram of depth 3 is



If we identify the elements $\alpha\alpha$, $\alpha\beta$, $\beta\alpha$, $\beta\beta$ of ◯ with 1, 2, 3, 4 respectively, we can associate the circuits at this node with permutations as follows :

ν	$1(23)4$
κ	$(13)(24)$
$\lambda\kappa\mu\kappa\lambda$	$(12)34$
$\mu\kappa\lambda\kappa\mu$	$12(34)$

Since the symmetric group is generated by transpositions of neighbouring elements, the first, second and fourth of these generate $S_{\bigcirc}$. Now S_4 has the following defining relations on the generators $a = (12)34$, $b = 1(23)4$, $c = 12(34)$, $d = (13)(24)$:

$$a^2 = b^2 = c^2 = (ab)^3 = (bc)^3 = (ac)^2 = 1 \ , \quad bdb = ac \ .$$

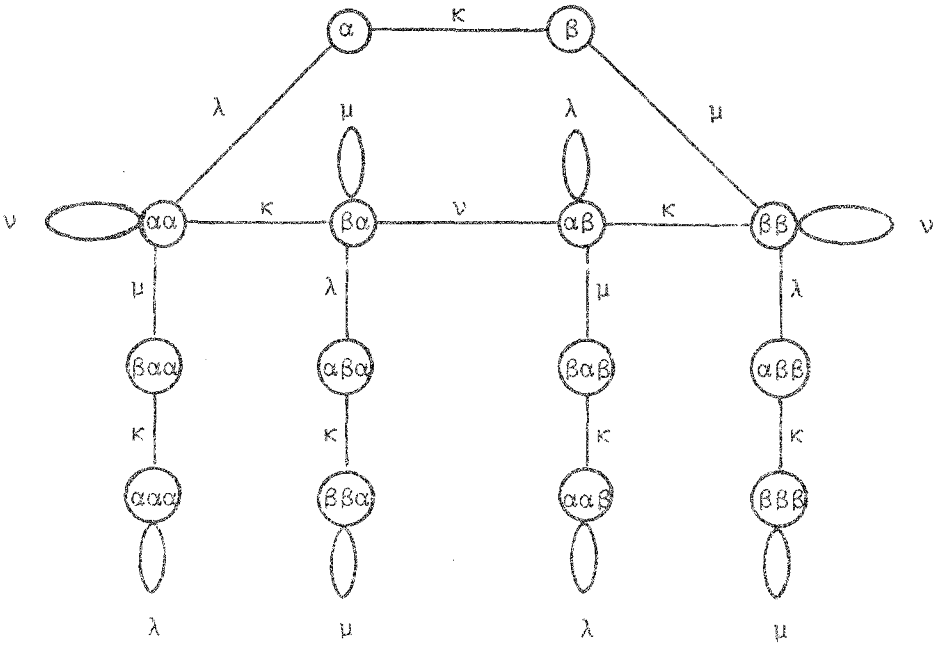
Since every circuit at the node ○ is expressible as a product of circuits corresponding to these permutations, it follows that every relation of depth at most 3 in $G_{2,1}$ is a consequence of the following relations :

$$\kappa^2 = \lambda^2 = \mu^2 = \nu^2 = 1 \ ,$$
$$(\lambda\kappa\mu\kappa\lambda\nu)^3 = (\mu\kappa\lambda\kappa\mu\nu)^3 = 1 \ ,$$
$$\nu\kappa\nu = \lambda\kappa\mu\kappa\lambda\mu\kappa\lambda\kappa\mu \ .$$

These give us relations (2) and (4) on page 50. Also, if we note that $\kappa\nu$ corresponds to the permutation $(13)(24).(23) = (1234)$, we obtain the relation $(\kappa\nu)^4 = 1$, which is relation (14) on page 50.

The information derived so far tells us that the conditions of Lemma 8.1 are satisfied, and we conclude that $\{\kappa,\lambda,\mu,\nu\}$ is a smooth generating set. Thus to obtain defining relations for $G_{2,1}$ it would now be sufficient to construct the diagram of depth 6 and examine all the circuits. In practice, however, this would mean working with a diagram having 132 nodes, and it is simpler to use relations at lower depths first to reduce the size of the diagram.

We therefore next consider the diagram of depth 4, which is :



The relation $\kappa\nu\lambda\kappa\mu\nu\kappa\lambda\nu\mu\nu\lambda\nu\mu = 1$, which is relation (3) on page 50, corresponds to a circuit at $\beta\alpha$ and may be verified as follows. Identify the elements $\beta\alpha\alpha$, $\beta\alpha\beta$, $\beta\beta$, $\alpha\alpha$, $\alpha\beta$ of $\beta\alpha$ with 1,2,3,4,5 in the order given and note that the circuits $\kappa\nu\lambda\kappa\mu\nu\kappa\lambda\nu$, μ, $\nu\lambda\nu$ correspond to the permutations 1(24)(35), (14)(25)3, (15)(23)4 respectively : the required relation is obtained by multiplying permutations.

We use this relation and relation (2), which was derived above, to "reduce" the diagram as follows. Write relation (2) in the form

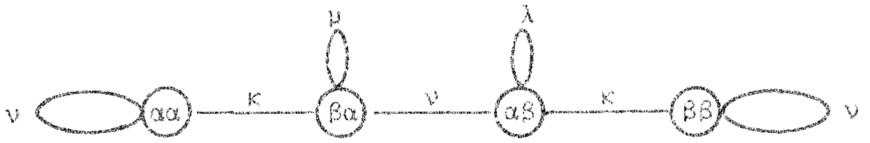
$$\lambda = \kappa\mu\lambda\kappa\mu\kappa\lambda\nu\kappa\nu\mu\kappa$$

and observe that the word on the right-hand side represents a circuit at $\alpha\alpha\alpha$, whereas the λ on the left-hand side represents a loop at $\alpha\alpha\alpha$. As this loop does not occur as part of the circuit represented by the right-hand side, we can replace any circuit on the diagram that involves the loop by one that does not, in such a way that the corresponding permutations induced on any fixed basis are the same. It follows that any relation of depth at most 4 is a consequence of relation (2) together with relations on the diagram that remains when the loop is deleted. On the latter diagram the only circuits passing through $\textcircled{\alpha\alpha\alpha}$ and $\textcircled{\beta\alpha\alpha}$ are those involving a trivial circuit consisting of a path followed by its inverse. Hence we may also delete these nodes and the edges that end at them. In this way we remove the whole "tassel" at the left-hand side of the diagram. The other three tassels may be removed exactly similarly, using the same relation.

Next we rewrite relation (3) in the form

$$\kappa = \lambda\nu\kappa\mu\nu\lambda\nu\mu\nu\lambda\kappa\nu\mu$$

and use it in the same way to remove the edge joining $\textcircled{\alpha}$ and $\textcircled{\beta}$. As before, when we have removed this edge, the nodes $\textcircled{\alpha}$ and $\textcircled{\beta}$ no longer occur in an essential way on any remaining circuits, so they may be removed, together with the edges joining them to the rest of the diagram. We are thus left with the reduced diagram :

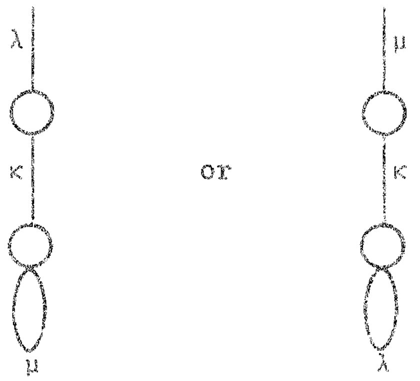


On this diagram the element $\lambda\nu\mu\nu$ represents a circuit at $\textcircled{\alpha\beta}$, and if we label the elements $\alpha\alpha$, $\alpha\beta\alpha$, $\alpha\beta\beta$, $\beta\alpha$, $\beta\beta$ of this basis by 1,2,3,4,5 respectively, then the permutation corresponding to turns out to be the cycle (1 2 3 5 4). Hence we obtain the relation

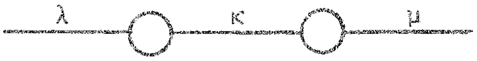
$$(\lambda\nu\mu\nu)^5 = 1 ,$$

which is relation (6) on page 50. We could now use defining relations of the symmetric group $S_{\textcircled{\alpha\beta}}$ to find a basis for the relations of depth at most 4, but since we shall later find a basis for all the relations of $G_{2,1}$ there is not much point in doing this. (In fact, relation (6) was derived only because we shall need it to reduce the depth 6 diagram.)

The reductions that were carried out above consisted in removing nodes that occurred as endpoints of only two edges on the diagram of depth 4 . It is easy to see that on every diagram of depth greater than 3 the nodes with this property are precisely those that represent bases in which either α or β is unexpanded. By examining the effect of the generators κ, λ, μ, ν on such bases it is not hard to see that these nodes will occur in pairs on diagrams of depth greater than 3 , either as tassels :



or in the form



.

These correspond precisely to the sections that we removed from the diagram of depth 4 , and we can use the same relations to remove them from the diagram of depth 6 .

After applying these reductions we obtain the reduced diagram of depth 6 shown on page 60. On this diagram we use the following notation. The bases

$$\left(\begin{matrix}\alpha\beta\\ \beta\beta\beta\end{matrix}\right) = (\alpha\alpha,\ \alpha\beta\alpha,\ \alpha\beta\beta,\ \beta\alpha,\ \beta\beta\alpha,\ \beta\beta\beta\alpha,\ \beta\beta\beta\beta)$$

$$\left(\begin{matrix}\beta\beta\\ \beta\alpha\alpha\end{matrix}\right) = (\alpha\alpha,\ \alpha\beta,\ \beta\alpha\alpha\alpha,\ \beta\alpha\alpha\beta,\ \beta\alpha\beta,\ \beta\beta\alpha,\ \beta\beta\beta)$$

etc. are obtained by expanding symmetrically about both the circled elements, starting from the unique minimal expansion containing both and proceeding as before. The symbols $\boxed{\alpha\alpha}$, $\boxed{\alpha\beta}$, $\boxed{\beta\alpha}$, $\boxed{\beta\beta}$ denote the following bases :

$$\boxed{\alpha\alpha} = (\alpha\alpha,\ \alpha\beta\alpha,\ \alpha\beta\beta,\ \beta\alpha\alpha,\ \beta\alpha\beta,\ \beta\beta\alpha,\ \beta\beta\beta)$$

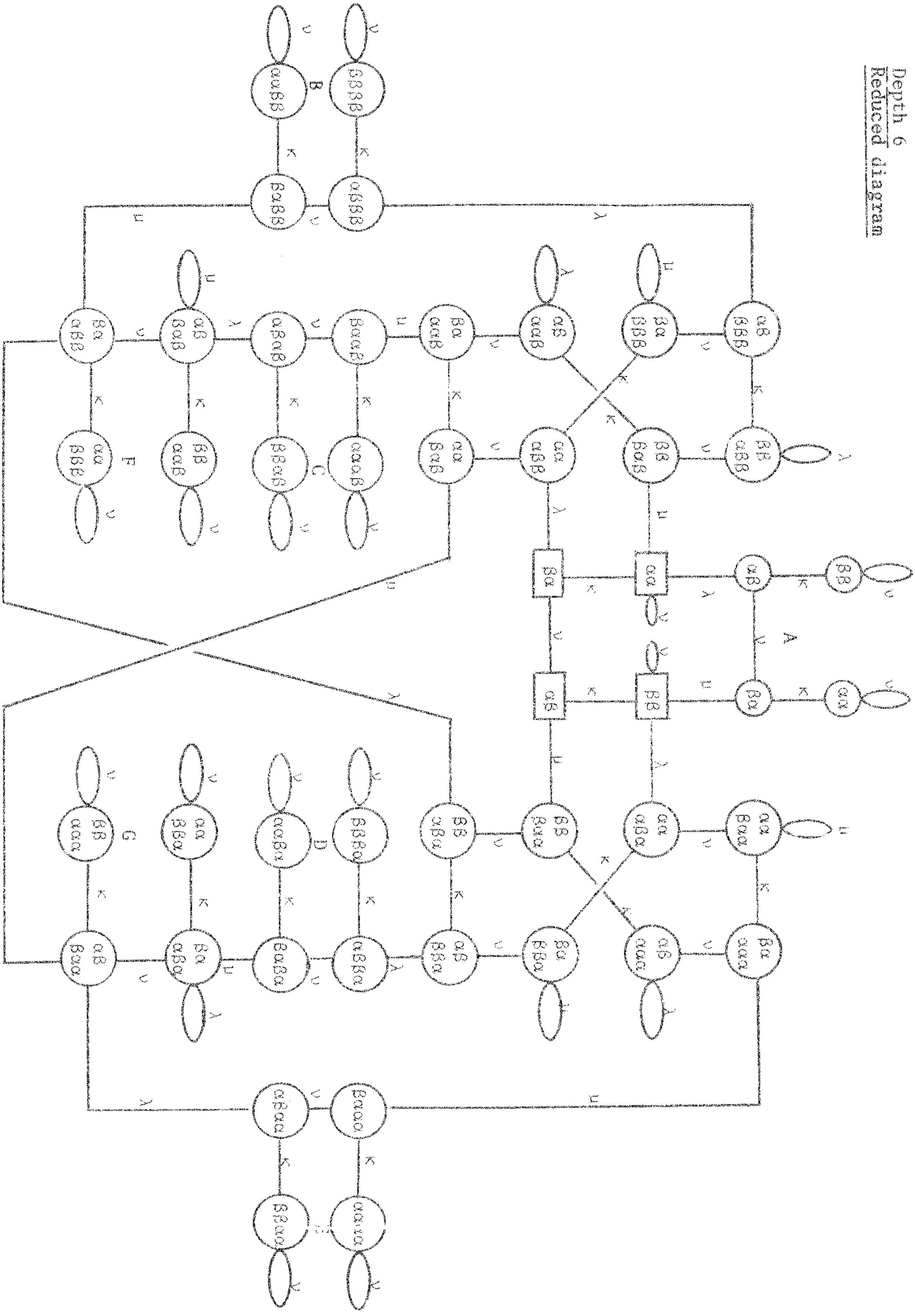
$$\boxed{\alpha\beta} = (\alpha\alpha\alpha,\ \alpha\alpha\beta,\ \alpha\beta,\ \beta\alpha\alpha,\ \beta\alpha\beta,\ \beta\beta\alpha,\ \beta\beta\beta)$$

$$\boxed{\beta\alpha} = (\alpha\alpha\alpha,\ \alpha\alpha\beta,\ \alpha\beta\alpha,\ \alpha\beta\beta,\ \beta\alpha,\ \beta\beta\alpha,\ \beta\beta\beta)$$

$$\boxed{\beta\beta} = (\alpha\alpha\alpha,\ \alpha\alpha\beta,\ \alpha\beta\alpha,\ \alpha\beta\beta,\ \beta\alpha\alpha,\ \beta\alpha\beta,\ \beta\beta)\ .$$

The remaining bases are labelled according to the scheme already explained.

Depth 6
Reduced diagram



We now carry out further reductions on this diagram, beginning by removing the branches surrounding the areas labelled A - G . Note first that relations (14) can be written as

$$\kappa\nu\kappa = \nu\kappa\nu\kappa\nu ,$$

which shows that the two branches surrounding each area are "equivalent" to one another : that is, any relation corresponding to a circuit that involves one branch is equivalent to a relation corresponding to a circuit involving the other. Next we use the relation

$$(\kappa\nu\kappa\lambda\nu\mu\nu\lambda\nu\mu\nu\lambda)^2 = 1 ,$$

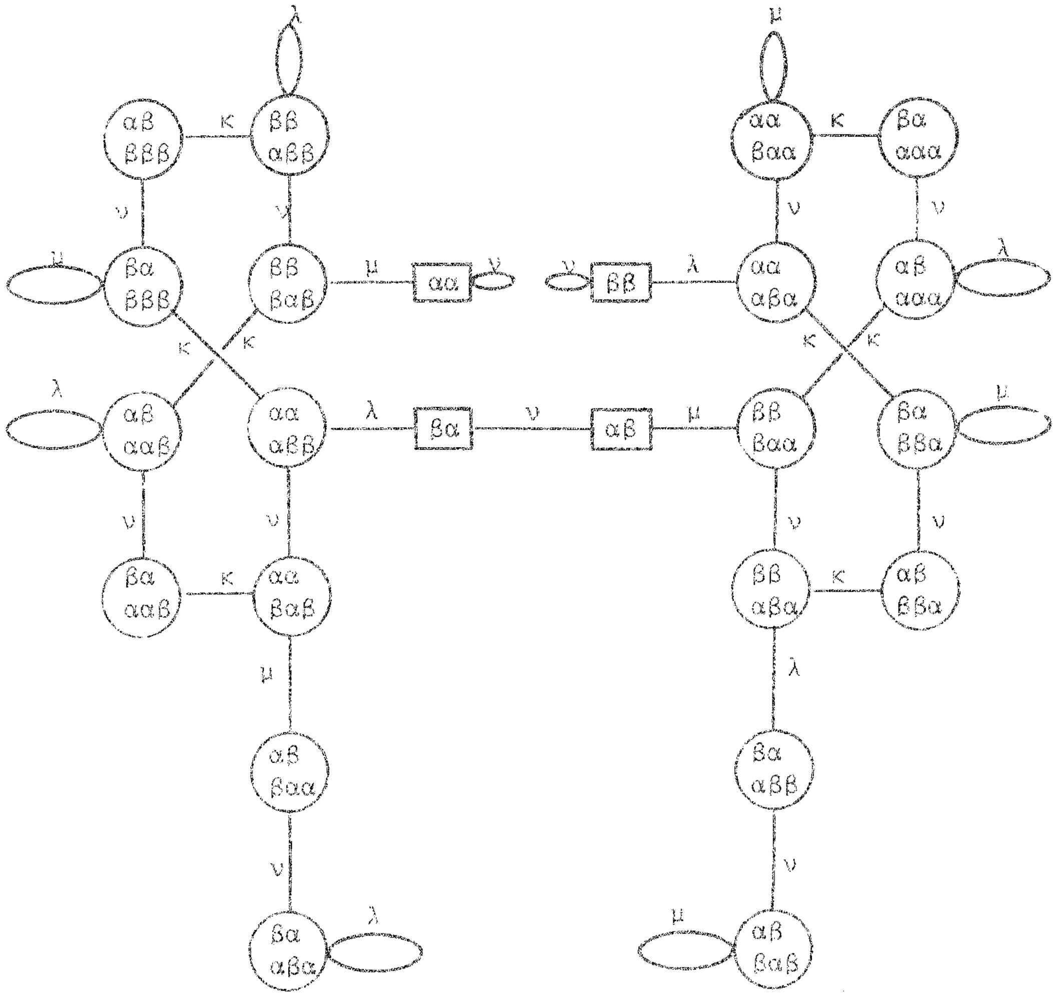
which follows from (2) and (3), to see that the lower branch at C is equivalent to the upper one at B , and that the upper bran ch at D is equivalent to the lower one at E . By what we have just said, this means that the pair of branches at C is equivalent to the pair at B , and the pair at D is equivalent to the pair at E . We express this by writing B ≡ C and D ≡ E . We now delete the branches at A using the relation

$$\lambda\kappa\nu\kappa\lambda = \nu\mu\nu\lambda\nu\mu\kappa\lambda\nu\mu\nu\lambda\nu\mu\kappa\nu\kappa\mu ;$$

observe that both sides are represented by circuits at $\boxed{\alpha\alpha}$. (It can be verified by calculating the permutations that this is a relation.) The same relation can be used to delete the branches at E (consider circuits at $\left(\begin{smallmatrix}\alpha\beta\\ \beta\alpha\alpha\end{smallmatrix}\right)$) and those at B (consider circuits at $\left(\begin{smallmatrix}\beta\alpha\\ \alpha\beta\beta\end{smallmatrix}\right)$, or use symmetry). Also, by writing this relation as

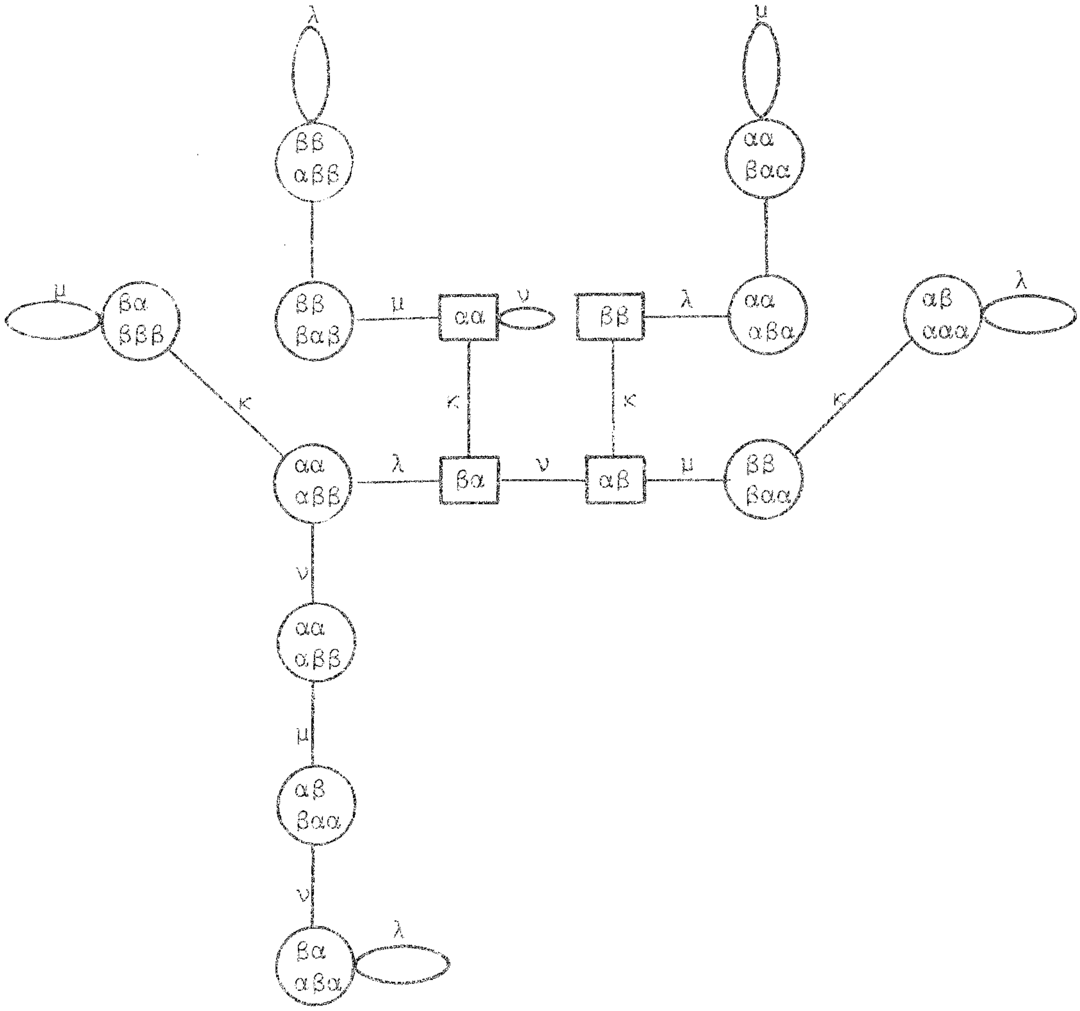
$$\lambda\kappa\nu\kappa\lambda\mu\kappa\nu\kappa\mu = \nu\mu\nu\lambda\nu\mu\kappa\lambda$$

and considering circuits at $\left(\begin{smallmatrix}\alpha\beta\\ \beta\alpha\beta\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\beta\alpha\\ \alpha\beta\alpha\end{smallmatrix}\right)$, we find that $C \equiv F$ and $D \equiv G$. It now follows that every pair of branches may be deleted, so we are left with the diagram :



Using relation (14) : $(\kappa\nu)^4 = 1$, which was derived from the depth 3 diagram, we can delete the nodes $\left(\begin{smallmatrix}\alpha\beta\\ \beta\beta\beta\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\beta\alpha\\ \alpha\alpha\alpha\end{smallmatrix}\right)$ (and the edges joining them to the rest of the diagram). We then use relation (3) (depth 4) to delete $\left(\begin{smallmatrix}\beta\alpha\\ \alpha\alpha\beta\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\alpha\beta\\ \beta\beta\alpha\end{smallmatrix}\right)$, relation (13) (depth 2) to delete $\left(\begin{smallmatrix}\alpha\beta\\ \alpha\alpha\beta\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}\beta\alpha\\ \beta\beta\alpha\end{smallmatrix}\right)$, relation (6) (depth 4) to delete the remaining tassel on the right, and finally relation (14) to delete the loop at $\boxed{\beta\beta}$.

These reductions leave us with the diagram :



It is now easy to see that all circuits on this diagram passing through the node $\boxed{\beta\alpha}$ are expressible as products of the six circuits through this node representing the elements κνκ, λκμκλ, νμκλκμν, κμνλνμκ, νκλνμνλκν, λνμνλνμνλ, respectively.

These elements determine the following permutations :

$\kappa\nu\kappa$	(16)(27)345
$\lambda\kappa\mu\kappa\lambda$	(13)(25)467
$\kappa\mu\nu\lambda\nu\mu\kappa$	12(36)4(57)
$\nu\kappa\lambda\nu\mu\nu\lambda\kappa\nu$	1(24)(36)(57)
$\lambda\nu\mu\nu\lambda\nu\mu\nu\lambda$	(13)(25)(46)7

The complete list of defining relations is obtained by taking those used so far together with a set of defining relations for the symmetric group S_7 on these generators.

9. A SEMINORMAL FORM FOR ELEMENTS OF $G_{n,r}$

In this section we pick an automorphism θ of $V_{n,r}$ and construct a basis for $V_{n,r}$ which makes the study of θ easy. We shall then apply the construction to study algorithmic questions, showing that one can solve the conjugacy problem in $G_{n,r}$ and also recognize when θ is of infinite order. We shall use the same method to study torsion free abelian subgroups of $G_{n,r}$ of finite rank.

The method is based on a consideration of the orbit structure of θ on $X\langle A\rangle$ for any basis X. Since θ is one to one on $V_{n,r}$, θ may have orbits in $X\langle A\rangle$ of any or all of the following five kinds.

(i) *Complete infinite orbits.* For y in such an orbit, $y\theta^i$ belongs to $X\langle A\rangle$ for all integers i, and the elements $y\theta^i$ are all different.

(ii) *Complete finite orbits.* For y in such an orbit, $y\theta^n = y$ for some positive integer n, and $y, y\theta, \ldots, y\theta^{n-1}$ all belong to $X\langle A\rangle$.

(iii) *Right semi-infinite orbits.* For some y in the orbit, $y\theta^i$ belongs to $X\langle A\rangle$ for all $i \geq 0$, but $y\theta^{-1}$ does not. The elements $y\theta^i$, $i \geq 0$, are then, of course, necessarily all different.

(iv) *Left semi-infinite orbits.* Interchange θ and θ^{-1} in (iii).

(v) *Finite incomplete orbits.* Here for some y and some non-negative integer n, $y, y\theta, \ldots, y\theta^n$ belong to $X\langle A\rangle$ but $y\theta^{-1}$ and $y\theta^{n+1}$ do not.

(In the case of incomplete orbits, several of them may really belong to the same orbit of θ on $V_{n,r}$, but we are not concerned about this.) By Lemma 4.1, for suitable expansion s Y and Z of X we have $Y\theta = Z$, so that $(Y\langle A\rangle)\theta \subseteq X\langle A\rangle$ and $(Z\langle A\rangle)\theta^{-1} \subseteq X\langle A\rangle$. Since $X\langle A\rangle \setminus Z\langle A\rangle$ is finite and an orbit of type (iii) must contain an element $y \in X\langle A\rangle \setminus Z\langle A\rangle$, there are only a finite number of orbits of type (iii). Similarly there are only finitely many orbits of type (iv) and (v). Furthermore we may assume that Y is chosen so that θ maps no proper contraction of Y into $X\langle A\rangle$, in which case we see from the proof of Lemma 4.1 that

$$Y\langle A\rangle = X\langle A\rangle \cap X\langle A\rangle\theta^{-1}$$

and hence

$$Z\langle A\rangle = Y\langle A\rangle\theta = X\langle A\rangle\theta \cap X\langle A\rangle .$$

Thus if $u \in X\langle A\rangle \setminus Z\langle A\rangle$ then $u \notin X\langle A\rangle\theta$, so $u\theta^{-1} \notin X\langle A\rangle$ and hence u is the initial element either of an incomplete finite orbit or of a right semi-infinite orbit. Similarly if $v \in X\langle A\rangle \setminus Y\langle A\rangle$ then v is the terminal element either of an incomplete finite orbit or of a left semi-infinite orbit. But $|X\langle A\rangle \setminus Z\langle A\rangle| = |X\langle A\rangle \setminus Y\langle A\rangle|$, and the initial and terminal elements of the finite incomplete orbits are evidently in one-to-one correspondence. Therefore there are as many right semi-infinite orbits as left semi-infinite orbits. We summarize the discussion.

LEMMA 9.1. *There are only finitely many orbits of types* (iii), (iv) *and* (v) *and there are as many of type* (iii) *as of type* (iv).

We shall say that θ is in *seminormal form* with respect to the basis X if there are no finite incomplete orbits. The letters Γ, Δ, Λ, *etc.* will be used for sequences, possibly empty, of the form $\Gamma = \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$, and we write $|\Gamma| = k$.

LEMMA 9.2. *For an automorphism θ there exists a basis with respect to which θ is in seminormal form.*

The proof is by induction on k, the number of elements in the orbits of type (v) for some X. If $k = 0$ we are done. Otherwise there is an element $x\Gamma$, with $x \in X$ and $\Gamma \in \langle A \rangle$, in an orbit of type (v). If θ is the orbit containing x then $x \in X\langle A \rangle$ while for some m and n, $x\theta^{-m}$ and $x\theta^{n}$ are not in $X\langle A \rangle$ because $x\Gamma\theta^{-m}$ and $x\Gamma\theta^{n}$ are not, so θ is also of type (v). If $X^* = X \setminus \{x\} \cup \{x\alpha_1, \ldots, x\alpha_n\}$ then $X^*\langle A \rangle = X\langle A \rangle \setminus \{x\}$. Thus the only change in orbits when we pass from X to X^* is that we have reduced by one the number of elements in orbits of type (v). By induction we are done.

If θ is in seminormal form with respect to X then θ is also in seminormal form with respect to every expansion of X. It follows that given a finite set of elements of $G_{n,r}$ there is an X with respect to which they are all in seminormal form.

LEMMA 9.3. *Let θ be in seminormal form with respect to the basis X. Then*

(A) For x in X, if some $x\Gamma$ belongs to a finite (complete) orbit, then x itself belongs to a finite (complete) orbit, which consists of elements of X.

(B) If for some x in X and some Γ, Δ with $\Gamma \neq \Delta$, $x\Gamma$ and $x\Delta$ belong to the same orbit, then for some $n \neq 0$, $\Lambda \neq 1$, $x\theta^{n} = x\Lambda$. Furthermore (i) the orbit containing x is right semi-infinite if $n > 0$ and (ii) the orbit containing x is left semi-infinite if $n < 0$.

(C) If x in X does not fall under (A) or (B) above, the orbit containing x contains $y\Gamma$, for some y falling in case (B), and some Γ.

We use repeatedly the principle that if $\mathcal{O}$ is an orbit (complete or not) then $\mathcal{O}\Gamma$ $(= \{y\Gamma \mid y \in \mathcal{O}\})$ is at least part of an orbit. In case *(A)* this implies immediately that the orbit containing x is finite, and it is therefore complete, since θ is in seminormal form. If the orbit containing x contains also $y\Delta$, where y is in X, then it is $\Delta\mathcal{O}$, where $\mathcal{O}$ is the orbit containing y. Since x belongs to the orbit, this implies $\Delta = 1$, completing case *(A)*.

It follows that if x belongs to a finite orbit, then the orbit containing $x\Gamma$ is $\{x_1\Gamma,\ldots,x_k\Gamma\}$ for some set of distinct generators x_i in X. Thus in case *(B)* the orbit containing x must be at least semi-infinite since $\Gamma \neq \Delta$. We may suppose that $x\Delta$ stands to the right of $x\Gamma$ in the orbit that contains them both. If the orbit $\mathcal{O}$ containing x is right semi-infinite, then $\mathcal{O}\Gamma$ contains $x\Gamma$ and everything in its orbit to the right of it. In particular, it contains $x\Delta$. So for some $\Lambda \neq 1$, $\Delta = \Lambda\Gamma$, and $x\theta^n = x\Lambda$ for some $n > 0$. Similarly if $\mathcal{O}$ is left semi-infinite then for some $\Lambda \neq 1$ we have $\Gamma = \Lambda\Delta$, and $x\theta^n = x\Delta$ for some $n < 0$. If $\mathcal{O}$ were a complete infinite orbit, each of Γ, Δ would be a proper final segment of the other, which is impossible. This completes the proof of *(B)*.

Finally *(C)* is obvious, for if x does not come under case *(A)* the orbit containing it is infinite; but X is finite, so the orbit contains some $y\Gamma$ and $y\Delta$, y in X, $\Gamma \neq \Delta$, and y falls under case *(B)*.

COROLLARY. *If* θ *is an element of infinite order in* $G_{n,r}$ *then there is a bound on the set of integers* i *such that there is a* ϕ *in* $G_{n,r}$ *with* $\phi^i = \theta$.

Since θ has infinite order so does every such ϕ and by Lemma 9.3 each such ϕ has a semi-infinite orbit. For some i this orbit is a disjoint union of i semi-infinite orbits for θ, and since θ has only finitely many semi-infinite orbits by Lemma 9.1, there is a bound on the i.

When we apply Lemma 9.3 we shall speak of generators or elements of X of types *(A)*, *(B)* and *(C)*. Following a vector space analogy, we call an element u of $V_{n,r}$ such that for some Γ, $u\theta = u\Gamma$ *a characteristic element*, with *characteristic multiplier* Γ. The element and the multiplier are *proper* if $\Gamma \neq 1$.

THEOREM 9.4. *An element θ of $G_{n,r}$ is of infinite order if and only if for some $m \neq 0$, θ^m has a proper characteristic element.*

If u is a characteristic element of θ^m with multiplier Γ then $u\theta^{mj} = u\Gamma^j$, $j = 1,2,\ldots$. But if $\Gamma \neq 1$, the elements $u\Gamma^j$ are all different as soon as j is large enough for $u\Gamma^j$ to belong to $X\langle A\rangle$, so that θ has infinite order. For the converse let θ be in seminormal form with respect to the basis X. If no θ^m has a proper characteristic element, then X has no elements of type *(B)* and hence none of type *(C)*. Thus all elements of X are of type *(A)*, whence θ is a permutation of X and has finite order.

Next, if θ, ϕ are automorphisms of two isomorphic free algebras $V_{n,r}$ and $V'_{n,r}$, we write $\theta \sim \phi$ if there is an isomorphism $\rho : V_{n,r} \to V'_{n,r}$ such that $\phi = \rho^{-1}\theta\rho$. Observe that $\sim$ reduces to conjugacy in $G_{n,r}$ if θ and ϕ are automorphisms of the same algebra. For a finitely generated free algebra V in $\mathcal{V}_n$ with an automorphism θ, let V_P and V_{RI} be the subalgebras generated by elements of V in finite orbits of θ and proper characteristic elements of powers of θ respectively. By Theorem 9.4, θ is periodic if and only if V_{RI} is empty; if V_P is empty we shall say that θ is *regular infinite*.

THEOREM 9.5. *The finitely generated free algebra* V *is a free product of the* θ*-admissible subalgebras* V_P *and* V_{RI} . *If* $\theta_P = \theta|_{V_P}$ *and* $\theta_{RI} = \theta|_{V_{RI}}$ *then, for two automorphisms* θ *and* ϕ , $\theta \sim \phi$ *if and only if* $\theta_P \sim \phi_P$ *and* $\theta_{RI} \sim \phi_{RI}$.

Let X be a basis with respect to which θ is in seminormal form, let V'_P be generated by the elements of X of type *(A)* of Lemma 9.3 and V'_{RI} by the elements of types *(B)* and *(C)*. Then V is certainly the free product of V'_P and V'_{RI} so we have to show they are θ-admissible and $V'_P = V_P$, $V'_{RI} = V_{RI}$. We use frequently the fact that an element u belongs to a subalgebra if and only if there is an integer s such that all $u\Gamma$ do for all Γ such that $|\Gamma| = s$.

If u lies in a finite orbit of θ then there is an s such that for all Δ of length s , $u\Delta \in X\langle A\rangle$, and $u\Delta$ is in a finite orbit of θ . Thus $u\Delta = x\Gamma$ for some $x \in X$ and $\Gamma \in \langle A\rangle$, and by Lemma 9.3*(A)*, x is in a finite orbit so $x \in V'_P$ and $u\Delta = x\Gamma \in V'_P$. Since this is true for all Δ of length s , $u \in V'_P$. Thus V'_P contains all finite orbits of θ . It is generated by these orbits because it is already generated by the ones which lie in X . Thus $V_P = V'_P$ and it is clearly θ-admissible.

We show next that V'_{RI} is θ-admissible; that is, if u belongs to V'_{RI} , so do $u\theta$ and $u\theta^{-1}$. Because we can replace u by the set of all $u\Gamma$, $|\Gamma|$ large enough, and $(u\Gamma)\theta = u\theta\Gamma$, *etc.*, it is sufficient to prove this statement in case $u, u\theta, u\theta^{-1}$ all belong to $X\langle A\rangle$. But then, by assumption, u is $x\Delta$ with x of type *(B)* or *(C)* of Lemma 9.3; and $u\theta$ and $u\theta^{-1}$, belonging to the same orbit as u , are also of the form $x\Gamma$ with x of type *(B)* or *(C)*, and so belong to V'_{RI} , as required. We show V'_{RI} contains no proper characteristic elements of powers of θ . If u is a proper characteristic element for θ^m , $u\theta^m = u\Gamma$, where $\Gamma \neq 1$, and so $u\theta^{mi} = u\Gamma^i$. Choose i

so large that $u\Gamma^i$ belongs to $X\langle A\rangle$. Then $u\Gamma^i$ belongs to a semi-infinite orbit (right semi-infinite if $m > 0$, left semi-infinite if $m < 0$) and so it is $x\Delta$ for some x in X of type *(B)* and some Δ. Thus $u\Gamma^i$ belongs to V'_{RI}, and since V'_{RI} is θ-admissible, u belongs to V'_{RI}. That is, V'_{RI} contains all proper characteristic elements of powers of θ. Now V'_{RI} is generated by elements x in X of type *(B)* or *(C)*. An element of type *(B)* is a proper characteristic element of a power of θ. If x is of type *(C)*, $x\theta^m = y\Delta$, for some integer m, generator y of type *(B)*, and word Δ. Then $x = (y\theta^{-m})\Delta$, and $y\theta^{-m}$, like y, is a proper characteristic element of a power of θ. Thus V'_{RI} is generated by these characteristic elements and so $V'_{RI} = V_{RI}$.

We have now provided an invariant description for the subalgebras V_P and V_{RI}; the last sentence of the theorem is therefore clear.

It is convenient next to introduce a slight strengthening of the notion of seminormal form. We shall say that θ is in *quasinormal form* with respect to the basis X if it is in seminormal form with respect to X, but not with respect to any proper contraction of X. We show there is a basis X with respect to which θ is in quasinormal form. Let Y be a basis with respect to which θ is in seminormal form. If there is a contraction of Y with respect to which θ is in seminormal form call it Z; otherwise take $Y = X$. Apply the same process to Z, if necessary, to get a chain $Y, Z, \ldots$ with $|Y| > |Z| > \ldots$. Since Y is finite the process terminates after a finite number of steps at a basis with respect to which θ is in quasinormal form. The following result shows the usefulness of the quasinormal form.

LEMMA 9.6. *If* θ *is in quasinormal form with respect to* X, *and if* $v = u\theta^m$, $m > 0$ *and* u, v *belong to* $X\langle A\rangle$ *then* $u\theta^i$ *belongs to* $X\langle A\rangle$ *for* $i = 1,\ldots,m-1$.

If not then there is no loss of generality in assuming that $u\theta$ does not belong to $X\langle A\rangle$. Furthermore, since, for any Γ, $u\Gamma$ and $(u\Gamma)\theta^m = v\Gamma$ belong to $X\langle A\rangle$ we may replace u by a suitable $u\Gamma$ and assume that $(u\alpha_1)\theta,\ldots,(u\alpha_n)\theta$ all belong to $X\langle A\rangle$. Since u is in an incomplete orbit and θ is in seminormal form with respect to X, u is in an infinite orbit. Similarly all orbits that we shall mention are infinite. We show next that $w_i = (u\alpha_i)\theta$ is an element of X. If not it is $y\alpha_j$ say where y also belongs to $X\langle A\rangle$. Because y is in $X\langle A\rangle$ and belongs to an infinite orbit either $y\theta^{-1}$ or $y\theta^{m-1}$ belongs to $X\langle A\rangle$. But $(y\theta^{-1})\alpha_j = (y\alpha_j)\theta^{-1} = u\alpha_i$ and $(y\theta^{m-1})\alpha_j = (y\alpha_j)\theta^{m-1} = (u\alpha_i)\theta^m = v\alpha_i$ so that in either case $\alpha_i = \alpha_j$. Since $v\theta^{-m} = u$ we have $y\theta^{-1} = u$ in any case so that $u\theta = y$ contrary to the assumption that $u\theta$ is not in $X\langle A\rangle$. Thus $w_1,\ldots,w_n$ are distinct elements of X. Let $w = w_1\ldots w_n\lambda$ and define the contraction X^* of X by

$$X^* = X \setminus \{w_1,\ldots,w_n\} \cup \{w\}.$$

Then $X^*\langle A\rangle = X\langle A\rangle \cup \{w\}$. As $w_i = u\theta\alpha_i$ for each i, $u\theta = w$ and $w\theta^{-1} = u \in X^*\langle A\rangle$. Since $X\langle A\rangle$ does not include any finite incomplete orbits it now follows that the same is true of $X^*\langle A\rangle$. That is, θ is in seminormal form with respect to X^*. This contradicts the assumption that θ is in quasinormal form with respect to X, and the contradiction proves the lemma.

We turn now to algorithmic questions. Usually, when we ask such questions about a group G, G is given by generators and relations, and to speak of a "given" element of G is to speak of a word in the generators. In the case of $G_{n,r}$ it is more convenient to regard an element as "given" if we know a symbol for it (in terms of a fixed basis X of the algebra $V_{n,r}$ of which $G_{n,r}$ is the automorphism group). This is legitimate because the set of all symbols of elements can be effectively enumerated. The analogue of the *word problem* is then the question when two symbols represent the same elements. This is clearly soluble for, given any symbol for θ , we can find a "shortest possible" such symbol, and by Lemma 4.1 two such shortest possible symbols differ only by a permutation of columns. Equally trivially, if we change the basis X of our algebra, we can find from a given symbol for θ a symbol relative to the new basis.

LEMMA 9.7. *Given an element* θ *of* $G_{n,r}$ *(i) we can construct a basis with respect to which* θ *is in quasinormal form and (ii) for* u,v *in* $V_{n,r}$ *we can tell whether* u,v *are in the same orbit of* θ , *and if so, what are the integers* m *for which* $u\theta^m = v$.

(i) Starting with an arbitrary basis X and an element x of X we construct the orbit

$$\ldots, x\theta^{-3}, x\theta^{-2}, x\theta^{-1}, x, x\theta, x\theta^2, x\theta^3, \ldots$$

going forward until either we reach $x\theta^m$, $m \geq 0$, for which $x\theta^{m+1}$ is not in $X\langle A\rangle$, or we reach $x\theta^m$, $m > 0$, such that for some $x\theta^\ell$, $0 \leq \ell \leq m$, we have $x\theta^\ell = y\Gamma$ and $x\theta^m = y\Delta$, for some $y \in X$, Γ, Δ, and going backward similarly until we are stopped, or reach the repetition of a generator. If for some x we are stopped in both directions, then θ is not in seminormal form with respect to X ; we expand at the element x as in Lemma 9.2 and start again. If for no x are we stopped in both directions, θ is in seminormal form with respect to X ; and after a finite amount of time this must happen. When we have found a basis X with respect to which θ is in seminormal form, we test similarly all the contractions of X (there are only a finite number) to find a basis with respect to which θ is in quasinormal form.

(ii) We may assume we have a basis X with respect to which θ is in quasinormal form. Moreover, because $u\theta^m = v$ if and only if $(u\Gamma)\theta^m = v\Gamma$ for all Γ of any fixed length s, we may assume that u and v belong to $X\langle A\rangle$. By Lemma 9.6, if u,v belong to the same orbit of θ in $V_{n,r}$, they belong to the same orbit in $X\langle A\rangle$. Suppose that $u = x\Gamma$ and that $v = y\Delta$, where x,y belong to X. If, in the classification of Lemma 9.3, x is of type *(B)*, then for some $m \neq 0$, $\Lambda \neq 1$, we have $x\theta^m = x\Lambda$. If $\Gamma = \Lambda^i\Gamma_0$, where Γ_0 has no initial segment Λ, and $u_0 = x\Gamma_0$, then $u_0\theta^{mi} = x\Gamma_0\theta^{mi} = x\theta^{mi}\Gamma_0 = x\Lambda^i\Gamma_0 = x\Gamma = u$. Thus we may replace u by u_0; that is, we may suppose Γ has no initial segment Λ, and similarly Δ has no initial segment equal to the characteristic multiplier of y, if y is of type *(B)*. Now construct, as in part *(i)*, the orbit

$$\ldots, u\theta^{-3}, u\theta^{-2}, u\theta^{-1}, u, u\theta, u\theta^2, \ldots \quad ;$$

again we stop going forward or back if we reach a point at which the next element is not in $X\langle A\rangle$, or if we reach a term $z\Phi$, z in X, for which some $z\Phi$ has already been included in the same half of the orbit. Then, given that we have made the reductions mentioned above, v will belong to the orbit only if it is already written down. In this case we can also see whether we have a finite complete orbit, and hence see what integers m satisfy $u\theta^m = v$.

If x is or type *(C)* then for some t, $x\theta^t = z\Lambda$ for some z of type *(B)* and now we apply the above process to $z\Lambda\Gamma$ and v to determine the m for which $u\theta^m = v$.

<u>THEOREM 9.3.</u> *The order problem and the conjugacy problem are soluble in* $G_{n,r}$.

If θ is an element of $G_{n,r}$, we can find (constructively) a basis X with respect to which θ is in quasinormal form, and classify the elements of X as in Lemma 9.3. If there are elements of X of type *(B)*, θ has infinite order; if there are no elements of X of type *(B)* and hence of type *(C)*, the order of θ is the least common multiple of the lengths of the cycles containing elements of type *(A)*.

To deal with the conjugacy problem let automorphisms θ, ϕ of algebras $V_{n,r}$ and $V'_{n,r}$ be given and we will show whether $\theta \sim \phi$. By Theorem 9.5, $\theta \sim \phi$ if and only if $\theta_P \sim \phi_P$ and $\theta_{RI} \sim \phi_{RI}$. The methods of section 6 enable us to deal with periodic elements, so we can and will suppose θ and ϕ regular infinite (θ_P and θ_{RI} can be obtained constructively from θ).

Suppose we have found, as we can, bases X and Y respectively with respect to which θ and ϕ are in quasinormal form. We shall show how to find a finite set R of maps ρ_0 of X into $F_n(Y)$ such that if $\theta \sim \phi$, then for some ρ_0 in R, there is an isomorphism $\rho : F_n(X) \to F_n(Y)$ such that $\rho|_X = \rho_0$, and $\phi = \rho^{-1}\theta\rho$. Since we can clearly test, for a given ρ_0, whether its unique extension to a homomorphism $\rho : F_n(X) \to F_n(Y)$ is an isomorphism, and if so, whether $\phi = \rho^{-1}\theta\rho$, this is enough. Note that there are, in fact, an infinity of automorphisms ρ such that $\phi = \rho^{-1}\theta\rho$ if there are any at all, since if ψ is an automorphism of $F_n(X)$ commuting with θ (e. g. if $\psi = \theta^i$ for some i) we can replace ρ by $\psi\rho$. From now on when we speak of an isomorphism ρ we shall mean one such that $\phi = \rho^{-1}\theta\rho$.

We shall introduce an equivalence relation on the elements of X; taking $\equiv$ to be the least equivalence relation such that $x \equiv y$ whenever some $x\Gamma$ and $y\Delta$ are in the same orbit of θ. The method of proof is as follows. First we pick an x of type *(B)* in an equivalence class X_0. We show that there is a finite set V of elements of $V'_{n,r}$ such that, if it is true that $\phi = \rho^{-1}\theta\rho$ for some isomorphism ρ, then it is possible to choose ρ so that $x\rho$ is in V. Next we show that if y is another element of type *(B)* in X_0 then there are only finitely many possibilities for $y\rho$, provided we restrict ourselves to isomorphisms ρ chosen as above. Then we deal separately with elements of type *(C)*, and repeat the whole procedure for the other equivalence classes. Let ψ be defined by $x\psi = x\theta$ for x in X_0, $x\psi = x$ for x in X not in X_0 and extend ψ to a map of $F_n(X)$. Then ψ is an automorphism of $F_n(X)$ which commutes with θ. By Lemma 9.3 and since θ is regular infinite we can choose an x in X_0 of type *(B)*. Then x is a characteristic element of a power θ^m of θ with some multiplier $\Gamma \neq 1$. We assume an isomorphism ρ exists with $\phi = \rho^{-1}\theta\rho$. Then $x\rho$ must be a characteristic element of ϕ^m with multiplier Γ. It must therefore belong to a semi-infinite orbit of ϕ (right semi-infinite if $m > 0$, left if $m < 0$). We can look at each such orbit and see whether or not its elements are characteristic elements with the right multiplier (if one is, they all are). If no orbit of appropriate characteristic exists, ρ does not exist, and we are done. Returning to the assumption that ρ exists we have for some initial or terminal element y of a semi-infinite orbit and some i, $x\rho = y\phi^i$. We can replace ρ by $\rho' = \psi^{-i}\rho$ so that $x\rho' = x\psi^{-i}\rho = x\theta^{-i}\rho = y$ is the initial or terminal element of the orbit in which it lies. (Observe that this adjustment does not affect $z\rho$ for z in any other equivalence class.) That is, $x\rho$ may be taken to be one of a fixed finite set V of elements.

Suppose next that $x\Gamma$ and $y\Delta$ are in the same orbit, say $y\Delta = (x\Gamma)\theta^m$, where y is also of type *(B)*. By the argument of the last paragraph there is a finite set, W say, of elements such that if ρ exists then there is a $w \in W$ and an integer i such that $y\rho = w\phi^i$. (We cannot multiply by ψ again to normalize.) Given the fact that ρ is an isomorphism and knowing $x\rho$ is a specified element of V and

w in W is such that $y\rho = w\phi^i$ then we show that we can determine i uniquely. If $y\rho = w\phi^i$ we have

$$(w\Delta)\phi^i = (y\Delta)\rho = (x\Gamma)\theta^m\rho = (x\rho)\Gamma\phi^m .$$

Thus $w\Delta$ and $(x\rho)\Gamma$ are in the same orbit of ϕ. Because ϕ is regular infinite, $Y\langle A\rangle$ decomposes into a disjoint union of infinite orbits under ϕ. Thus if $w\Delta$ and $x\rho\Gamma$ are in the same orbit there will be a unique i such that $w\Delta\phi^i = x\rho\Gamma\phi^m$, and we can find the i by Lemma 9.7*(ii)*. Hence we can find the unique i for which $y\rho = w\phi^i$ is a possibility. Thus given that ρ is an isomorphism and $x\rho$ is a specified element of V, since W is finite there are only a finite number of possibilities for $y\rho$. We can test whether in fact there are any possibilities for $y\rho$ by using Lemma 9.7*(ii)* to see for each w in W if $w\Delta$ and $(x\rho)\Gamma$ are in the same orbit of ϕ.

Given that ρ is an isomorphism and $x\rho$ is in V, since V is finite and there are only finitely many y of type*(B)* in X_0, the number of possibilities for the y is finite. Note that in using the transitivity of $\equiv$ to show that $x \equiv y$ where both x and y are of type *(B)* we need never go through an element of type *(C)*; for if z is of type *(C)* then by Lemma 9.3 there is a $z_1\Gamma$ in the orbit of z for some z_1 of type *(B)*, and any orbit containing some $z\Delta$ contains also $z_1\Gamma\Delta$. Finally if $z \equiv x$ and z is of type *(C)* then $z = z_1\Gamma\theta^k$ for some z_1 of type *(B)*, Γ, and k, and $z\rho$ is determined once $(z_1\rho)\Gamma\theta^k$ is chosen.

Since X is finite there are a finite number of equivalence classes. Repeating the above argument for each equivalence class, and noting again that adjustments made for one equivalence class do not affect those made for others, we see that we have constructed R.

We conclude with the proof of the following theorem.

THEOREM 9.9. *Let* A *be a torsion free abelian group of finite rank contained in* $G = G_{n,r}$. *Then (i)* A *is a free abelian group of finite rank, (ii) the centralizer* $C_G(A)$ *is of finite index in the normalized* $N_G(A)$ *and (iii)* $N_G(A)$ *has a direct factor* B *which has a free abelian subgroup* C *such that* C *is of finite index in* AB .

A *characteristic* of A is an infinite sequence

$$\{\underset{\sim}{u}\} = \ldots, u_{-2}, u_{-1}, u_0, u_1, u_2, \ldots$$

of elements of $V_{n,r}$ such that for some θ in A and $\Gamma \neq 1$, $u_i\theta = u_i\Gamma = u_{i+1}$ for all i. If ϕ is an element of $N_G(A)$ then $\{\underset{\sim}{u}\}\phi$ is a characteristic for $\phi^{-1}\theta\phi$: the theorem is proved by studying the action of $N_G(A)$ on the characteristics.

We begin by showing that if an element of $V_{n,r}$ belongs to a characteristic at all then there is a unique maximal characteristic containing it. Suppose u belongs to a characteristic $\{u\theta^i\}$ where $u\theta = u\Gamma$. If $\{u\phi_1^i\}$ and $\{u\phi_2^i\}$ are characteristics containing $\{u\theta^i\}$ with $\phi_1, \phi_2 \in A$ and $u\phi_i = u\Delta_i$ for $i = 1,2$ then Δ_1 and Δ_2 are initial segments of Γ. Also

$$u\Delta_2\Delta_1 = u\phi_1\phi_2 = u\phi_2\phi_1 = u\Delta_1\Delta_2 ,$$

so that for some word Λ we have $\Delta_1 = \Lambda^a$, $\Delta_2 = \Lambda^b$, where a and b are positive integers. Replacing Λ by a power Λ^e if necessary, we may assume that a and b are relatively prime, so for some c,d, $ac + bd = 1$. Therefore $u\phi_1^c\phi_2^d = u\Lambda$, and thus $\{u(\phi_1^c\phi_2^d)^i\}$ is a characteristic containing both $\{u\phi_1^i\}$ and $\{u\phi_2^i\}$. Since Γ has only a finite number of initial segments it follows that $\{u\theta^i\}$ is contained in a unique maximal characteristic as required. By Lemma 9.3 a maximal characteristic contains a semi-infinite orbit and there are only a finite number by Lemma 9.1 *so for any element* θ *of* A *there are only a finite number of maximal characteristics each fixed setwise but not pointwise by some power of* θ .

Since A is of finite rank there exist elements $\theta_1,\ldots,\theta_k$ such that for any θ in A there are integers $a, a_1,\ldots, a_k$ with $a \neq 0$ such that $\theta^a = \theta_1^{a_1}\ldots\theta_k^{a_k}$. We shall show that *for any maximal characteristic there are integers* i *and* m *such that* θ_i^m *fixes the maximal characteristic setwise but not pointwise.* For if $\{\underset{\sim}{u}\}$ is the characteristic and $u_i\theta = u_i\Gamma = u_{i+1}$, $\Gamma \neq 1$, and if $\phi \in C_G(A)$, in particular if $\phi \in A$, then $\{\underset{\sim}{u}\}\phi$ is one of the finite number of characteristics fixed setwise but not pointwise by θ . Thus A has a subgroup B of finite index, m say, fixing $\{\underset{\sim}{u}\}$ setwise. In particular θ_i^m fixes $\{\underset{\sim}{u}\}$ setwise for each i . Suppose $\theta^a = \theta_1^{a_1}\ldots\theta_k^{a_k}$ as above. Since $\theta^{am} = \theta_1^{a_1m}\cdots\theta_k^{a_km}$ does not fix $\{\underset{\sim}{u}\}$ pointwise, one θ_i^m must not fix $\{\underset{\sim}{u}\}$ pointwise, giving the result.

Putting together the results of the last two paragraphs : *there are in all only a finite number of maximal characteristics.* We next show that if ϕ in $N_G(A)$ fixes setwise the maximal characteristic $\{u_i\}$ we must have $u_i\phi = u_{\varepsilon i+t}$ where $\varepsilon = \pm 1$ and t is an integer. For $u_i\phi = u_0\theta^i\phi = u_0\phi(\phi^{-1}\theta\phi)^i = u_t(\phi^{-1}\theta\phi)^i$ for some t . Let $\psi = \phi^{-1}\theta\phi$ and observe that ψ commutes with θ . If $u_t\psi = u_r$ then $u_{r+s} = u_t\psi\theta^s = u_t\theta^s\psi = u_{t+s}\psi$. Hence there is an η such that $u_t\psi = u_{\eta+t}$. If $u_t\psi^{-1}$ then $u_t = u_t\psi^{-1}\psi = u_s\psi = u_{s+\eta}$ so that $u_t\psi^{-1} = u_{-\eta+t}$. Inductively we get for all integers i , $u_t\psi^i = u_{\eta i+t} = u_i\phi$. If $|\eta| \neq 1$ then ϕ maps $\{u_i\}$ into a proper subset so $\{u_i\phi^{-1}\} \supset \{u_i\}$. Since $\{u_i\phi^{-1}\}$ is a characteristic for $\phi\theta\phi^{-1}$ we have a characteristic properly containing a maximal one, which is impossible. Thus $|\eta| = 1$.

We regard each characteristic as giving rise to two *oriented characteristics* : ϕ preserves the oriented characteristics corresponding to $\{u_i\}$ if $\varepsilon = 1$. Since there are only a finite number of oriented maximal characteristics, the elements of $N = N_G(A)$ preserving each oriented characteristics form a normal subgroup M of finite index. An element ϕ of M acts on the characteristics $\{\underset{\sim}{u}\}$ as $u_i \to u_{i+t}$. If we let the maximal characteristics be $\{\underset{\sim}{u}\}_1, \ldots, \{\underset{\sim}{u}\}_d$ and the t's corresponding to an element ϕ of M be $t_1, \ldots, t_d$, it is easy to check that the map $\phi \to (t_1, \ldots, t_d)$ is a homomorphism of M into a free abelian group of finite rank, whose kernel L is the set of elements ϕ of N which fix each characteristic pointwise. Let θ be a nontrivial element of A . Since θ has infinite order, by Lemma 9.3 some power of it has a proper characteristic multiplier, Γ say. Let

$$u_0\theta^m = u_0\Gamma = u_1 \quad \text{and} \quad u_0\theta^{mi} = u_i .$$

Then

$$u_i\theta^m = u_0\theta^{mi}\theta^m = u_0\Gamma\theta^{mi} = u_i\Gamma .$$

Since θ acts nontrivially on the characteristic $\{u_i\}$, $A \cap L = 1$.

We thus have the normal series

$$N_G(A) = N \triangleright M \triangleright L \triangleright 1$$

with N/M finite, M/L free abelian of finite rank and $L \cap A = 1$. We can now easily obtain the first two parts of the theorem. Since $A \cap M \cong (A \cap M)L/L$ is free abelian and $A \cap M$ is of finite index in A , there is an n such that $A \cap M \geq A^n$ so A^n is free abelian and $A \cong A^n$ because A is torsion free. Notice $A^n \leq A \cap M \leq M$. Now since A is abelian and contains $[A,M]$,

$$[A,M]^n = [A^n,M] \leq [M,M] \cap [N,A] \leq L \cap A = 1$$

and since $[A,M]$ is torsion free, $[A,M] = 1$. Thus $M \leq C_G(A)$, whence $C_G(A)$ has finite index in $N_G(A)$.

The third part of the theorem will be proved by showing that if $\theta_1,\ldots,\theta_k$ generate A then $V_{n,r}$ is the free product of algebras V_P and V_{RI} as in Theorem 9.5, where each θ_i is periodic on V_P, and V_{RI} is generated by the characteristic of A. For by the remark following the proof of Lemma 9.2 there is an X such that all the θ_i are in seminormal form with respect to X. Now let V_P be generated by the x in X of type *(A)* for all θ_i, and V_{RI} by the x of type *(B)* or *(C)* for some θ_i. Clearly $V_{n,r}$ is the free product of V_P and V_{RI} and each θ_i is periodic on V_P. An element ϕ of $N_G(A)$ can be regarded as a pair (ϕ_1,ϕ_2) where $\phi_1 = \phi|_{V_P}$ and $\phi_2 = \phi|_{V_{RI}}$ which gives the required direct product decomposition, and L above is the first factor of this decomposition (that is, the set of ϕ with $\phi_2 = 1$). If B is the second factor then $M \cap B = C$ is free abelian, and of finite index in B. But B is of finite index in AB, since the first factor of elements in A form a group generated by a finite set of commuting periodic elements. This proves the theorem.

COROLLARY. *No group* $G_{n,r}$ *has a subgroup isomorphic to* $GL(3,Z)$.

(Note that $GL(3,Z)$ has a soluble word problem.)

The subgroup A of $GL(3,Z) = G$ of elements of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is abelian and normalized by elements of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

but not centralized by them when $c \neq 0$ so $C_G(A)$ has infinite index in $N_G(A)$.