ON THE EMBEDDING OF A GROUP IN A JOIN OF
GIVEN GROUPS

Dedicated to the memory of Hanna Neumann

P. HALL

1. Introduction

1.   In their fundamental paper of 1949, Higman, Neumann and Neumann proved for the first time that *a countable group can always be embedded in some 2-generator group*: [1], Theorem IV. Two kinds of improvement of this result have recently appeared. In [4], Theorem 2, Dark has shown that the embedding can always be made *subnormally*. On the other hand, in [2], Theorem 2.1, Levin has shown that the two generators can be given *preassigned orders* $m > 1$ and $n > 2$; and in [3], Miller and Schupp prove that the 2-generator group can also be made to satisfy several additional requirements, such as being complete and Hopfian.

We make here two main contributions, Theorems A and C.

In the first, we adapt the methods of Dark to the direction taken by Levin; and show that, if H and K are non-trivial groups not both of order 2, a group L can always be embedded as a special kind of subnormal subgroup in some group of the form $J = \langle H, K \rangle$, subject only to the obviously necessary condition that $|L| \leq |H * K|$. The corresponding pure embedding theorem, in which no assertion of subnormality is made, has already been obtained, at least for the case of countable L, by Schupp [13], using the methods of 'small cancellation' theory. In §3.5, we show how this result, like the theorem of Levin, may be derived in a quite different way from the original Theorem IV of [1].

In the central part of the paper, we consider the problem of embedding a given group in some simple group with a finite number of preassigned subgroup-generators. Given any four non-trivial groups $K_1, \cdots, K_4$, we show that a group L can always be embedded in some simple group of the form $S = \langle K_1, \cdots, K_4 \rangle$ provided only that the necessary condition $|L| \leq |K_1 * \cdots * K_4|$ holds. We may

434

even allow K_4 to be trivial, provided that at most one of K_1, K_2, K_3 is of order 2. In particular, it follows that *a countable group can always be embedded in some 3-generator simple group.*

The group J of Theorem A is obtained as a subgroup of a complete wreath product, and the group S of Theorem C as a quotient group of an amalgamated free product. It is due in large part to the work of Hanna Neumann that the usefulness of these two constructions is now widely recognised.

The proof of Theorem A occupies §2; that of Theorem C takes §§3 and 4, with some supplementary results in §5. In the final §6, following up a remark of Hanna Neumann, we find necessary and sufficient conditions for a group G to be embeddable as a transitive subgroup in the wreath product of a given set of transitive permutation groups $\Gamma_1, \cdots, \Gamma_r$.

We shall now explain these results in closer detail, so as to place them in the context of their proofs, with the special aim of introducing certain notations of frequent occurrence. The most important of these are : the *subnormality relation* $\lhd_2$, the *vector groups* $\Omega(L, A)$, the *numerical invariant* $l(K)$, the *characteristic subgroup* $\mu(G)$ and the notion of a *hololophic subgroup.*

2.   Let H and K be subgroups of the group G. As usual,

$$H^K, C_G(H) \text{ and } N_G(H)$$

denote respectively the normal closure of H in $J = \langle H, K \rangle$, and the centralizer and normalizer of H in G. We define the relation

(1) $$H \lhd_2 G$$

to mean that the following two conditions hold: (i) H^G is the direct product of all the conjugates of H in G; and (ii) $N_G(H) = HC_G(H)$ i.e. the only automorphisms of H which can arise by transforming it with an element of G are the inner ones.

Obviously, $H \lhd_2 G$ implies $H \lhd H^G$ and hence $H \lhd^2 G$. Thus $\lhd_2$ is a special case of the relation $\lhd^2$ of 2-step subnormality. In this respect $\lhd_2$ resembles the normality relation $\lhd$; but $\lhd_2$, unlike $\lhd$, is transitive, indeed transfinitely so: cf. Lemma 1.3, §2.1.

We can now state

THEOREM A. *Let H, K and L be any groups such that*

(2) $$|H| > 2, \quad |K| > 1 \quad and$$

(3) $$|L| \leqq \aleph_\alpha = \max(\aleph_0, |H|, |K|).$$

Then there always exist groups of the form $J = \langle H, K \rangle$ such that

(4) $$L \lhd_2 J$$

and such that J is soluble if H, K and L are soluble.

Of course, $\aleph_\alpha = |H * K|$.

It is easy to see that we could not replace $\lhd_2$ by $\lhd$ in this theorem without imposing further conditions on H, K and L. For example, a 'small' but non-Abelian group L cannot be normally embedded in any group which is generated by 'large' simple groups $S_1, S_2, \cdots$; for $L \lhd \langle S_1, S_2, \cdots \rangle$ would imply that at least one S_i can be embedded in the group of automorphisms of L. However, suitable direct powers of L can always be normally embedded, as stated in

COROLLARY 1. *Let H, K and L be any groups satisfying* (2) *and* (3), *and let D be the direct product of $\aleph_\alpha$ copies of L. Then D can always be normally embedded in some group of the form $J = \langle H, K \rangle$.*

PROOF. We may suppose $L \neq 1$. Then $|D| = \aleph_\alpha$ and we may take D in place of L in Theorem A. Hence $D \lhd_2 J$ for some $J = \langle H, K \rangle$; and $|J| = \aleph_\alpha$. Thus D has at most $\aleph_\alpha$ conjugates in J; and D^J is their direct product by definition of $\lhd_2$. It follows that $D \cong D^J \lhd J$, which is the result required.

3.   For any group L and any non-empty set A, we write

(5) $\Omega = \Omega(L, A)$

for the multiplicative group of all vectors $v = (v_a)_{a \in A}$ with arbitrary coordinates $v_a \in L$. Given a representation of any group Γ by permuations of A, the semidirect product $W = \Omega\Gamma$ with the transformation law

(6) $(\gamma v \gamma^{-1})_a = v_{a\gamma} \quad (a \in A, \gamma \in \Gamma)$

is the *complete wreath product* of L by Γ with respect to the given representation. We shall assume throughout that this representation is transitive.

Given $b \in A$, the vectors $v \in \Omega$ such that $v_b = 1$ form a group M_b; and those such that $v_a = 1$ for all $a \neq b$ form a copy L_b of L. Let Γ_b be the stabilizer of b in Γ. From the definition of Ω, (6) and the transitivity of Γ, we then have

(7) $\Omega = L_b \times M_b, \gamma^{-1} L_b \gamma = L_{b\gamma}, (L_b)^W = \underset{a \in A}{\mathrm{Dr}} \, L_a$ and $[L_b, \Gamma_b] = 1$.

Here Dr indicates the direct product. It follows that, for all $b \in A$,

(8) $N_W(L_b) = \Omega\Gamma_b = L_b C_W(L_b)$ and $L_b \lhd_2 W$.

When Γ is the symmetric group of all permutations of a countably infinite set A, Dark showed in [4], Theorem 1, that the group W is always perfect; and thereby that any group L can be embedded as a $\lhd_2$-subgroup in some perfect group. When, as in this case, Γ is stated to be a permutation group, the intended representation is clear; and we may write without ambiguity

(9) $W = \mathrm{Wr}(L, \Gamma)$; with $R = L \wr \Gamma$

for the corresponding *restricted wreath product*, referring to W and R as *natural wreath products*. The base group D of R consists of all vectors in Ω which have finite support. Thus $R \leq W$, with equality when the support A of Γ is finite.

When no representation of Γ is implied by the context, W and R in (9) are always to be interpreted as the *standard* wreath products, formed from the regular representation of Γ, so that $A = \Gamma$ in this case. Throughout §§2 to 5 only standard wreath products occur except for the unconventional kind used in §4.4–4.7 and referred to in §1.7 below; but in §6 natural ones predominate.

For standard wreath products, we adopt the usual convention which identifies each $x \in L$ with the corresponding vector of L_1, so that $x = x_1$ and $x_\gamma = 1$ for all $\gamma \neq 1$ in Γ. This convention makes $L = L_1$ a subgroup of W, $D = L^\Gamma$ and $R = \langle L, \Gamma \rangle$. It is easy to see that the standard R is defined to within isomorphism by the conditions

$$R = \langle L, \Gamma \rangle, \; L \triangleleft_2 R \text{ and } \Gamma \cap N_R(L) = 1.$$

Repeated standard wreath products are defined inductively by

$$(10) \qquad \qquad \mathrm{Wr}(L, \Gamma_1, \cdots, \Gamma_r) = \mathrm{Wr}(\mathrm{Wr}(L, \Gamma_1, \cdots, \Gamma_{r-1}), \Gamma_r).$$

The group J of theorem A is constructed as a subgroup of a repeated wreath product of this kind.

4.   A further deduction from Theorem A leads to our major topic of embedding in simple groups. This is

COROLLARY 2. *Let K and L be any groups such that*

$$(11) \qquad \qquad \qquad K \neq 1 \text{ and } |L| \leq |K * K|.$$

Then L can always be embedded in some simple group P which is generated by $\aleph_0$ copies of K.

PROOF. If K is finite, it may be replaced by its free square $K * K$, which is infinite since $K \neq 1$. Hence we may suppose that $|K| = \aleph_\alpha$. We take

$$P = \bigcup_{m=0}^{\infty} P_m, \text{ where } P_0 < P_1 < P_2 < \cdots$$

and the groups P_m, all of order $\aleph_\alpha$, are to be chosen successively as follows.

Let $P_0 = K \times L \times A \times D$, where A is the alternating group of degree and order $\aleph_0$ and $D = \langle t_1, t_2 \rangle$ is the infinite dihedral group generated by two involutions t_1 and t_2. By (11), $|P_0| = \aleph_\alpha$; and P_0 contains elements of all possible orders: for each finite $m > 0$, A contains an element a_m of order m; and the element $a_\infty = t_1 t_2$ of D is of infinite order.

We secure the simplicity of P by the choice of $P_1, P_3, P_5, \cdots$. Suppose P_{2n} to be chosen and of order $\aleph_\alpha$. In its regular representation P_{2n}^*, each $x \in P_{2n}$ is re-

presented by a permutation x^* consisting of $\aleph_\alpha$ cycles of order m, where m is the order of x (whether finite or ∞); and so we may choose for each x a permutation ξ such that $\xi^{-1}x^*\xi = a_m^*$. The group $P_{2n+1} = \langle x^*, \xi; x \in P_{2n} \rangle$ is then of order $\aleph_\alpha$; and if we identify P_{2n} with P_{2n}^*, it will follow that any two elements of the same order in P_{2n} are conjugate in P_{2n+1}. This rule ensures that *in P any two elements of the same order will be conjugate.*

Now let $1 \neq M \lhd P$. We show that $M = P$ by showing that $a_m \in M$ for all m. Since $M \neq 1$, we must have $a_m \in M$ for some $m > 1$. If $a_\infty \in M$, then M contains all elements of infinite order in P; in particular, $a_n a_\infty \in M$ for all finite n, and the required result follows at once. On the other hand, if $a_m \in M$ for some finite $m > 1$, then $A \cap M \neq 1$. Since A is simple, M must contain A. Hence M contains every periodic element in P, in particular t_1 and t_2. Hence $t_1 t_2 = a_\infty \in M$ and again the result follows. Thus P is simple.

We secure that P is generated by $\aleph_0$ copies of K by the choice of $P_2, P_4, \cdots$. Suppose P_{2n-1} to be chosen and of order $\aleph_\alpha$. By Theorem A, P_{2n-1} may be embedded in a group P_{2n} which is generated by two copies K_{2n-1} and K_{2n} of K. Hence $P = \langle K_m; m = 1, 2, \cdots \rangle$. This concludes the proof of Corollary 2.

In this proof only the 'pure embedding' form of Theorem A is needed; subnormality is irrelevant. As remarked above, this weaker form of the theorem is easily deduced, in the countable case, from Theorem IV of [1]. Unfortunately, it is precisely when $\alpha = 0$ that the 'even' steps of the above proof are unnecessary. For any α, omission of these steps gives an elementary proof of a well known fact: *a group of order $\aleph_\alpha$ can always be embedded in some simple group of order $\aleph_\alpha$.*

It is not easy to give a secure attribution of this result. It is implicit in the theorem of Neumann's Essay, [5], 239, that every group can be embedded in a larger group in which any two elements of the same order are conjugates. It is also an easy consequence of the work of Onofri [6], Schreier and Ulam [7], and Baer [8] on the structure of the infinite symmetric groups. These authors showed that, if S is the group of all permutations of a set L of $\aleph_\alpha$ elements and if S_0 is the subgroup of all permutations whose support is of cardinal less than $\aleph_\alpha$, then the group $T = S/S_0$ is simple. When L is a group, the regular representation of L provides an embedding of L in the simple group T; and it follows easily that there are simple subgroups of order $\aleph_\alpha$ in T which contain copies of L.

Corollary 2 suggests the following definition. Given any group $K \neq 1$, let $l(K)$ be the least cardinal number such that a group L satisfying (11) can always be embedded in some simple group which is generated by $l(K)$ copies of K. For completeness, we define $l(1) = 1$. Then Corollary 2 states that

(12) $l(K) \leqq \aleph_0$ for all K.

The decisive step in the proof of Theorem C is to show that $l(K)$ *is always finite.* For this step we use the 'well-known fact' just mentioned, but not Corollary 2.

5.   To prove the finiteness of $l(K)$ two things are needed: a theorem, B_1, on embedding in monolithic groups; and a construction, first used by Graham Higman, involving free products with amalgamations. We consider these in turn.

For any group G, let

(13) $$\mu(G) \;=\; \cap(M; 1 \neq M \lhd G)$$

be the intersection of all the non-trivial normal subgroups of G. We note that G is *monolithic* if and only if $\mu(G) \neq 1$; and simple if and only if $G = \mu(G) \neq 1$. (This definition of 'monolithic' is formally stricter than that given by Hanna Neumann in her book [9] 146–7, where it is merely required that G shall have a unique minimal normal subgroup; but for the finite groups being considered there, the two definitions are equivalent. In dealing with infinite groups, the stricter definition seems essential: cf. [20], 597).

We can now state

THEOREM B1. *Let H, K and L be any groups satisfying (2) and (3). Then there always exist groups of the form $J = \langle H, K \rangle$ such that*

(14) $$L \leqq \mu(J)$$

This is formally similar to Theorem A and easily deduced from it. However, we shall give an indedpendent proof. In view of the 'well known fact' mentioned in the preceding section, it may be assumed that $L = P$ is a perfect simple group.

A second theorem on embedding in monolithic groups, more precise than Theorem B1 but of slightly narrower scope, is

THEOREM B2. *Let H, K and L be any groups satisfying (11) and*

(15) $$l(K) < |H|.$$

Then there exists a perfect simple group P and an embedding of K in the base group P^H of $R = P \wr H$ such that

(16) $$L \lneqq P \text{ and } R = \langle H, K \rangle.$$

It is easy to see that R is monolithic: for all H, we have

(17) $$\mu(P \wr H) = P^H \text{ if } P = P' = \mu(P) \neq 1.$$

Monolithic groups of this special form we shall refer to as groups of *RP-type*.

The proof that $l(K) < \aleph_0$ requires Theorem B1, but only for the case of infinite H. Once this is established, Theorem B2 becomes an easy corollary. To obtain reaslitic bounds for $l(K)$, we require Theorem B2, but only for the case of finite H. (When H is infinite, condition (15) is vacuous). Thus both theorems are essential, but in different ways.

6.   A subgroup H of the group G will be called *hololophic* in G (from λόφος, a crest) if and only if $H \cap M = 1$ for every proper normal subgroup M of G; or equivalently, if

(18) $\langle x^G \rangle = G$ for all $x \neq 1$ in H.

For example, if G is either soluble or periodic, it will have a non-trivial hololophic subgroup if and only if it is generated by a class of conjugate elements of prime order.

The existence of infinite but finitely generated simple groups was first proved by Higman [10] by showing that, in the group $G = \langle a, b, c, d \rangle$ defined by the relations $a^{-1}ba = b^2, b^{-1}cb = c^2, c^{-1}dc = d^2$ and $d^{-1}ad = a^2$, the infinite cyclic groups generated by a, b, c and d are hololophic, for arithmetical reasons. The bearing of this notion on the problem of embedding in simple groups will be clear from this example. If H is a non-trivial hololophic subgroup of G, then by Zorn's Lemma G has a maximal proper normal subgroup N; and the simple group G/N contains copies of every hololophic subgroup of G. Any group which can be embedded in one of these can therefore be embedded in G/N.

For our purpose, the most useful examples are the groups of the form

(19) $G = \langle J_1, \cdots, J_n \rangle$, where $J_i = (J_i \cap \mu(J_{i-1}))^{J_i}$ $(i = 1, \cdots, n)$

and the suffix i is to be taken modulo n. It is easy to see that the subgroups J_i are all hololophic in G. Consequently any group L which can be embedded in one of them can also be embedded in a simple quotient group of G having the form $S = \langle J_i, \cdots, J_n \rangle$.

The method of free products with amalgamations, applied to any four groups $J_1, \cdots, J_4$ gives rise to groups $G = \langle J_1, \cdots, J_4 \rangle$ with four disjoint amalgamated subgroups

(20) $\bar{H}_i = H_{i+1} = J_i \cap J_{i+1}$ where $H_i \cap \bar{H}_i = 1$ ($i \bmod 4$).

The Higman group is an example. We call these *quadrilateral* groups. When the four 'corners' H_i of the quadrilateral are trivial, G reduces to the ordinary free product of its four 'sides' J_i. On the other hand, if

(21) $1 \neq \bar{H}_i \leq \mu(J_i)$ and $J_i = H_i^{J_i}$ $(i = 1, \cdots, 4)$,

then (19) holds with $n = 4$. This construction gives an easy proof of the finiteness of $l(K)$ if we take for the J_i suitable monolithic groups provided by Theorem B1.

If the group H in Theorem B2 is finite, then the base group P^H of $R = P \wr H$ contains a copy $\bar{P}$ of P such that $[H, \bar{P}] = 1$. $\bar{P}$ is the group of all constant vectors. This fact makes it possible to form *bilateral* groups $G = \langle J_1, J_2 \rangle$ with sides J_1 and J_2 of RP-type, such that (19) holds for $n = 2$. Here G is the free product of

J_1 and J_2 with a single amalgamated subgroup having the form of a direct product $H_1 \times \bar{H}_1 = \bar{H}_2 \times H_2$, such that $J_i = H_i^{J_i}$ and $\bar{H}_i \leqq \mu(J_i)$ for $i = 1, 2$.

Using this bilateral construction, we obtain the first part of our second main theorem, viz.

THEOREM C1. *Let $K_1, \cdots, K_4$ and L be any non-trivial groups such that*

$$(22) \qquad\qquad |L| \leqq |K_1 * \cdots * K_4|.$$

Then L can always be embedded in some simple group of the form

$$(23) \qquad\qquad S = \langle K_1, \cdots, K_4 \rangle.$$

It follows at once that

$$(24) \qquad\qquad l(K) \leqq 4 \text{ for all } K.$$

7.   The same construction, based on Theorem B2 for finite H, also yields embeddings in simple groups with only three given subgroup generators. But to obtain a result comparable in generality with Theorem C1 we need a substitute, when H is infinite, for the restricted wreath product $R = P \wr H$, which then no longer lends itself to the bilateral construction. We find this by tapping a higher stratum of $\Omega = \Omega(P, H)$ than that occupied by the base group of R. However, we only need to discuss the case where H is cyclic, and prove

THEOREM B3. *Let H be an infinite cyclic group and let K and L be any groups sarisfying* (11). *Then there exists a perfect simple group P and a semi-direct product $J_2 = H\mu(J_2)$ such that*

$$(25) \qquad L \leqq P, \quad \mu(J_2) = K^H = P_2^H \quad \text{and} \quad [H, \bar{P}_2] = 1,$$

where P_2 and $\bar{P}_2$ are two copies of P contained in $\mu(J_2)$.

Note that $J_2 = \langle H, K \rangle$ and contains the subgroup $H \times \bar{P}_2$.

J_2 may be described as a *Boolean wreath product* of P by H and its base group P_2^H as a *Boolean power* of P. For this notion, cf. [25] where other references will also be found. The connection with the wreath products described above in section 3 may be worth noting here.

Consider any groups P and H. Every transitive representation of H is equivalent to one of the representations $\pi_{H:A}$ of degree $|H : A|$, where A is some subgroup of H. This is the representation defined by

$$(26) \qquad\qquad (Ax)\pi_{H:A}(y) = Axy \ (x, y \in H).$$

The non-standard wreath products — complete and restricted — of P by H with respect to $\pi_{H:A}$ occur naturally as subgroups of the complete standard product W, viz. as the semidirect products

$$(27) \qquad\qquad W_A = \Omega_A H \text{ and } R_A = D_A H,$$

where Ω_A is the group of all vectors $v \in \Omega$ which are constant on each coset of A, and D_A consists of all $v \in \Omega_A$ which are trivial except on a finite number of these cosets. For any subset B of H, let P_B be the group of all vectors in Ω which are constant on B and trivial elsewhere. Then P_B is a copy of P, and the transformation law in W shows that

$$(28) \qquad\qquad \eta^{-1} P_B \eta = P_{B\eta} \quad (\eta \in H);$$

and so, if X is any transversal to A in H, we have

$$(29) \qquad\qquad D_A = \operatorname*{Dr}_{\xi \in X} P_{A\xi} = (P_A)^H \text{ and } R_A = \langle P_A, H \rangle.$$

Now suppose that P is a perfect simple group. For any subsets B and C of H we then have

$$(30) \qquad\qquad [P_B, P_C] = P_{B \cap C} \text{ and } P_{B \cup C} \leqq \langle P_B, P_C \rangle.$$

If $|H : A|$ is finite, then R_A contains the group $\bar{P} = P_H$ of all constant vectors in Ω; but when H is infinite, R_A is not monolithic, since it has the non-trivial normal subgroup

$$(31) \qquad\qquad K_H(A) = \bigcap_{\eta \in H} A^\eta,$$

which is disjoint from D_A.

However, suppose that A is not a subgroup, but is still of finite index in H in the sense that

$$(32) \qquad\qquad H = A\xi_1 \cup A\xi_2 \cup \cdots \cup A\xi_n$$

for some finite set of elements $\xi_1, \cdots, \xi_n$ in H. The group $R_A = \langle P_A, H \rangle$ will nevertheless still contain $\bar{P}$, by (28) and (30); but its base group $D_A = (P_A)^H$ is no longer a direct power of P, but a 'Boolean power', associated with the H-*invariant Boolean algebra* $\mathfrak{B}_A$ generated by the translates $A\eta (\eta \in H)$. As a Boolean algebra with operators, $\mathfrak{B}_A$ is in general no longer simple, as it is when A is a subgroup. Its H-invariant ideals correspond one-to-one to the normal subgroups of R_A which are contained in D_A.

The group J_2 of Theorem B3 has the form R_A/N, where N is the subgroup of D_A which corresponds to a maximal H-invariant ideal of $\mathfrak{B}_A$. To ensure that $\mu(J_2) = D_A/N$, the subset A of the infinite cyclic group H has to be carefully chosen: it may be described as a 'dislocated' subgroup of finite index.

We shall refer to monolithic groups J_2 of this kind as of $\mathfrak{B}P$-*type*.

8. The second part of Theorem C is

THEOREM C2. *Let* K_1, K_2, K_3 *and* L *be non-trivial groups such that*

$$(33) \qquad\qquad |L| \leqq |K_1 * K_2 * K_3|$$

Then L can always be embedded in some simple group of the form

(34) $S = \langle K_1, K_2, K_3 \rangle$,

except possibly when the K_i are all of order 2, or when two of them are of order 2 and the third is uncountable.

This theorem clearly implies the greater part of Theorem C1, but its proof is more difficult. The proof of Theorem C1 depends only on the 'H finite' case of Theorem B2 for which an elementary 'free product' proof is available, and for this reason we have treated it separately. The groups S in (34), like those in (23), are obtained as bilateral quotient groups; but one of the two sides of the bilateral may have to be of $\mathfrak{B}P$-type, or possibly — when two of the K_i are small — a finite simple group.

From Theorem C2 it follows at once that

(35) $l(K) \leqq 3$ if $|K| \neq 2$.

No very obvious reasons appear to forbid the conjecture that in fact

(36) $l(K) = 2$ if $|K| > 2$, and $l(K) = 3$ if $|K| = 2$.

More generally, it should be possible to strengthen Theorem B1 so that the conclusion (14) reads $L \leqq \mu(J) = J$, thus obtaining a theorem on embedding in simple groups of exactly the same scope as Theorem A. But our methods seem incapable of yielding such a result. Given groups H and K which satisfy (2), we cannot even prove the existence of a single simple group of the form $S = \langle H, K \rangle$ except in special cases. Accordingly, we confine attention in §5 to the case where H and K are both finite.

Elementary calculations then show that the alternating group of degree q is of the form $\langle H, K \rangle$ for infinitely many values of q: cf. Theorem D1; and it follows that a *finite* group L can always be embedded in some *finite* simple group of this form. But the interesting question remains: for which finite pairs H, K can any *countable L* always be embedded in some simple $\langle H, K \rangle$? When H is itself a simple group of composite order, we obtain a positive answer for all finite $K \neq 1$; in particular, $l(H) = 2$ for all such H: cf. Theorem D3, §5.6 We also show that $l(J) = 2$ for a wide class of finite monolithic groups J: cf. the corollary to Theorem D2, §5.5 But the fragmentary nature of these results is clear.

9.   Finally, in §6, we take up an observation of Hanna Neumann: [9], 46, footnote, to the effect that the well known theorem of Kaloujnine and Krasner [23], on the embedding of group-extensions in standard wreath products, is implicit in the much earlier work of Frobenius on monomial groups. What is in question is the connection between the method of induced representations and extension theory. When expressed in qualitative terms, this method lends itself to iteration, and

leads to an abstract characterization of the transitive subgroups of the natural complete wreath product

(37) $$W = \mathrm{Wr}(\Gamma_1, \cdots, \Gamma_r)$$

of any given transitive permutation groups $\Gamma_1, \cdots, \Gamma_r$. If Γ_i acts on the set A_i, then W may be regarded as a transitive group acting on the set $A = A_1 \times \cdots \times A_r$; and by a transitive subgroup of W, we mean one which is transitive on A.

When $r = 2$, $W = \Omega\Gamma_2$, with $\Omega = \Omega(\Gamma_1, A_2)$; and may be regarded as the group of all permutations $\eta\zeta$ of $A_1 \times A_2$, where $\eta\zeta$ is defined for all $\eta \in \Omega$ and $\zeta \in \Gamma_2$ by

(38) $$(b, c)\eta\zeta = (b\eta_c, c\zeta)(b \in A_1, c \in A_2).$$

Equivalently, W may be regarded as the group of all $A_2 \times A_2$-monomial matrices $\eta\zeta$, where the (c, c')-coefficient of $\eta\zeta$ is given, for all c, c' in A_2, by

(39) $$(\eta\zeta)_{c,c'} = \eta_c \delta_{c\zeta,c'}. \ (\eta \in \Omega, \zeta \in \Gamma_2).$$

Here $\delta_{c\zeta,c'} = 1$ if $c\zeta = c'$ and is zero otherwise. In this version, the elements of Γ_2 are identified with the corresponding permutation matrices, while those of Ω become diagonal matrices.

To express the result of Frobenius in the required form without circumlocution, we use the following notation, in which Y and Z are transitive permutation groups acting respectively on the sets B and C. Then

(40)   (i) $Y \approx Z$, and (ii) $Y \operatorname{trans} Z$

are to mean: (i) that Z is a *transcription* of Y, i.e. $Z = \phi^{-1} Y \phi$ for some one-to-one mapping ϕ of B onto C; and (ii) that $Y \approx Y^*$, where Y^* is some subgroup of Z which is transitive on C.

Now let G, H and J be groups such that $J \leq H \leq G$. We write

(41) $$\Pi_{G:H} = \pi_{G:H}(G).$$

where the representation $\pi_{G:H}$ of G is defined as in (26). Thus $\Pi_{G:H}$ is a transitive permutation group acting on the cosets of H in G. As we shall show, the method of induced representations leads to the formula

(42) $$\Pi_{G:H} \operatorname{trans} \mathrm{Wr}(\Pi_{H:J}, \Pi_{G:H});$$

or equivalently:

(43)   If $\Pi_{H:J} \operatorname{trans} \Gamma_1$ and $\Pi_{G:H} \operatorname{trans} \Gamma_2$, then $\Pi_{G:J} \operatorname{trans} \mathrm{Wr}(\Gamma_1, \Gamma_2)$.

The theorem of Kaloujnine and Krasner is the particular case where $J = 1$ and $H \lhd G$; for in this case, $G \cong \Pi_{G,1}$, since $\pi_{G:1}$ is the regular representation of G;

and the wreath product in (42) is isomorphic with the standard wreath product $\mathrm{Wr}(H, G/H)$, since $H \lhd G$.

We recall that the natural wreath multiplication of permutation groups defined by (38) is an associative operation; cf. [15], 96; and so the inductive generalization of (43) is immediate. When a converse is supplied as well, we obtain

THEOREM E1. *Let W be defined by (37). Then a group G can be embedded in W as a transitive subgroup if and only if it has a chain of subgroups $H = H_0 \leqq H_1 \leqq \cdots \leqq H_r = G$ such that*

(44) $K_G(H) = 1$ and $\Pi_{H_i : H_{i-1}}$ trans $\Gamma_i (i = 1, \cdots, r)$.

Here $K_G(H)$ is the kernel of the representation $\pi_{G:H}$ of G, and is defined as in (31). It is sometimes called the *normal core* of H in G.

The most interesting special case of Theorem E1 occurs when the Γ_i are all regular as well as transitive: cf. Theorem E2. Γ_i then has no proper transitive subgroups, and (44) implies that $H_{i-1} \lhd H_i$ and $H_i/H_{i-1} \cong \Gamma_i$ for each i. In this case, W is called the *regular* wreath product of the groups $\Gamma_1, \cdots, \Gamma_r$, although as a permutation group it is not regular except in trivial cases.

To conclude, we apply Frobenius' Theorem in its usual form to analyze the connection between the relation $\lhd_2$ and wreath products: cf. (8) above and Lemma 1.1 with Theorem E3 and Lemmas 23 and 24.

10.   Some conventions of notation will be apparent from the foregoing sketch. A group *of the form* $\langle J_1, J_2, \cdots \rangle$ is any group which can be generated by one copy each of $J_1, J_2, \cdots$; and in passing from one such group to another, we only use distinguishing labels when confusion might otherwise arise. For example, in §1.6 where $S = G/N$, we have written $S = \langle J_1, J_2, \cdots \rangle$ although $S = \langle NJ_1/N, \cdots, NJ_n/N \rangle$ would be more strictly correct. But when a group contains several copies $K_1, K_2, K^*, \cdots$ of a given group K as subgroups, distinguishing marks are essential. For any $y \in K$, we then write $y_1, y_2, y^*, \cdots$ for the corresponding elements of $K_1, K_2, K^*, \cdots$ on the tacit assumption that fixed isomorphisms of K onto each of these groups have been chosen.

Commutators are defined by $[x, y] = x^{-1}x^y = x^{-1}y^{-1}xy$; and inductively, for $n > 2$, by

$$[x_1, x_2, \cdots, x_n] = [[x_1, \cdots, x_{n-1}], x_n].$$

The *support* of a vector $v \in \Omega(L, A)$ is the set of all $a \in A$ such that $v_a \neq 1$; and the support of a permutation θ of A is the set of all $a \in A$ such that $a\theta \neq a$. The support of a vector group or a permutation group K is the union of the supports of its elements. For these supports, we frequently write $\mathrm{Sup}\, v$, $\mathrm{Sup}\, \theta$ or $\mathrm{Sup}\, K$.

2. Proof of Theorem A

1. We begin by noting some elementary properties of the relation $\lhd_2$. In the following three lemmas L is a subgroup of the group G.

LEMMA 1.1. *If* $L \lhd_2 G$, *then* $L \lhd_2 J$ *for every subgroup* J *of* G *which contains* L. *Conversely, if* $L \lhd_2 \langle L, x_1, \cdots, x_n \rangle$ *for every finite set of elements* $x_1, \cdots, x_n$ *in* G, *then* $L \lhd_2 G$.

PROOF. The first part follows easily from the definition of $\lhd_2$. If $L \lhd_2 G$, then L^G is the direct product of all the conjugates of L in G, and so L^J is the direct product of all the conjugates of L in J. Secondly, $N_G(L) = LC_G(L)$; and so, since $L \leqq J$,

$$N_J(L) = J \cap N_G(L) = L(J \cap C_G(L)) = LC_J(L).$$

Thus $L \lhd_2 J$.

For the converse, note first that the join of any n distinct conjugates L^{x_1}, $\cdots, L^{x_n}$ of L in G is their direct product, since $L \lhd_2 \langle L, x_1, \cdots, x_n \rangle$ by hypothesis. From this it follows that L^G is the direct product of all the conjugates of L in G. Secondly, let $x \in N_G(L)$. By hypothesis, $L \lhd_2 \langle L, x \rangle$, and so x transforms L by an inner automorphism. Hence $N_G(L) = LC_G(L)$. Thus $L \lhd_2 G$.

LEMMA 1.2. *Let* $1 \neq L \leqq M \lhd_2 G$ *and suppose that* $L^x \leqq M$ *for some* $x \in G$. *Then* $M = M^x$ *and* $L^x = L^y$ *for some* $y \in M$.

PROOF. Since $M \lhd_2 G$, distinct conjugates of M in G are disjoint. But by hypothesis, $1 \neq L^x \leqq M \cap M^x$. Hence $M = M^x$, and x transforms M by an inner automorphism. Thus $L^x = L^y$ for some $y \in M$.

LEMMA 1.3. *If* $L \lhd_2 M$ *and* $M \lhd_2 G$, *then* $L \lhd_2 G$. *More generally, the relation* $\lhd_2$ *is transfinitely transitive.*

PROOF. The last statement means that, if $L = L_0$, $G = L_\rho$ for some ordinal ρ, $L_\lambda \lhd_2 L_{\lambda+1}$ for all $\lambda < \rho$, and $L_\mu = \bigcup_{\lambda < \mu} L_\lambda$ for all limit ordinals $\mu \leqq \rho$, then $L \lhd_2 G$. This follows by transfinite induction from the first part of the lemma and the converse part of Lemma 1.1.

In proving the first part, we may assume $L \neq 1$. Since $L \lhd_2 M$, L^M is the direct product of the conjugates of L in M; and by Lemma 1.2, these are the only conjugates of L in G which lie in M. Since $M \lhd_2 G$, M^G is the direct product of the conjugates of M in G; and each of these conjugates has, like M itself, as a normal subgroup the direct product of those conjugates of L in G which it contains. It follows that L^G is the direct product of all the conjugates of L in G.

Secondly, $N_G(L) \leqq N_G(M)$ by Lemma 1.2; and $N_G(M) = MC_G(M)$ since $M \lhd_2 G$. Since $C_G(M) \leqq C_G(L)$, this gives $N_G(L) = N_M(L)C_G(L)$. But $N_M(L)$

$= LC_M(L)$ since $L \lhd_2 M$. Hence $N_G(L) = LC_G(L)$. Thus $L \lhd_2 G$, and this concludes the proof of the lemma.

2. We prove next some useful results involving standard wreath products. We recall from 1.10 the definition of Sup v, the support of a vector $v \in \Omega(L, Q)$:

(1) $\alpha \in \text{Sup } v$ if and only if $\alpha \in Q$ and $v_\alpha \neq 1$.

The first result, which plays an important part in the proof of Theorem A, is adapted from Lemma 1 of Dark's paper [4]:

LEMMA 2.1. *Suppose that the group Q contains an element β of infinite order; and let $G = \text{Wr}(L, Q)$ where L is any group. Then there is a subgroup M in G which is generated by $|L|$ copies of Q and is such that*

(2) $L \leqq \langle \beta^M \rangle.$

PROOF. For any $u \in L$, let $v = v(u)$ be the vector in $\Omega = \Omega(L, Q)$ such that

$$v_{\beta^n} = u^{n+1} \text{ if } n \geqq 0, \text{ and } v_\xi = 1 \text{ otherwise.}$$

Thus, if u is not periodic, Sup v consists of the non-negative powers of β. All the coordinates of v^{-1} and v^β being powers of u, these two vectors commute; and the transformation law gives

$$[\beta, \beta^v] = \beta^{-1}v^{-1}\beta^{-1}v\beta v^{-1}\beta v = \beta^{-1}v^{-2}\beta \cdot \beta^{-2}v\beta^2 \cdot v = u,$$

from the definition of v. Define

(3) $M = \langle Q^{v(u)}; u \in L \rangle.$

Then $\gamma = \beta^{v(u)} \in M$ and so $u = \beta^{-1}\beta^\gamma \in \langle \beta^M \rangle$ for all $u \in L$. (Here $v(1) = 1$, so that $Q \leqq M$.)

A very similar calculation shows that, if x, y and ξ are elements of any group such that x commutes with y^ξ, then

$$[x, y] = x^{-1}y^{-1}(\xi^{-1}y\xi)x(\xi^{-1}y^{-1}\xi)y = \xi^{-yx}\xi^x\xi^{-1}\xi^y.$$

With x and y in K, this gives

LEMMA 2.2. *If a group contains a subgroup K and an element ξ such that $[K, K^\xi] = 1$, then $K' \leqq \langle \xi^K \rangle.$*

For example, in the standard wreath product $R = M \wr H$, we have $[M, M^\xi] = 1$ for all $\xi \neq 1$ in H. Hence $K' \leqq \langle \xi^K \rangle$ for every subgroup K of M.

The next result is of frequent application

LEMMA 2.3. *Let X be any subgroup of $\Omega = \Omega(M, H)$ such that the coordinates of all the vectors in X together generate M. Then $M \cap N \lhd M$ for every normal subgroup N of the subgroup $J = \langle X, H \rangle$ of $\text{Wr}(M, H)$.*

PROOF. If $x \in X$ and $\eta \in H$, then $\eta x \eta^{-1} \in \Omega \cap J$. But $M \lhd \Omega$ and $N \lhd J$. Hence $\eta x \eta^{-1}$ normalizes $M \cap N$. Let $u \in M \cap N$, so that $u = u_1$ by convention. Since $(\eta x \eta^{-1})_1 = x_\eta$, this gives $u^{\eta x \eta^{-1}} = u^{x_\eta}$. Hence x_η normalizes $M \cap N$ for all $x \in X$ and $\eta \in H$. By hypothesis, $M = \langle x_\eta; x \in X, \eta \in H \rangle$. Thus $M \cap N \lhd M$, as stated.

Although it is not needed for the proof of Theorem A, it will be convenient to prove here

LEMMA 2.4. *Suppose that in the preceding lemma we have $\mu(M)$ non-Abelian and $M \cap J \neq 1$. Then $\mu(J) = (\mu(M))^H$.*

PROOF. We have only to show that every non-trivial normal subgroup N of J contains the group $D = (\mu(M))^H$; for $1 \neq D \lhd V = \mathrm{Wr}(M, H)$ since $\mu(M) \neq 1$.

By hypothesis, $M \cap J \neq 1$; and $M \cap J \lhd M$ by Lemma 2.3. Hence $\mu(M) \leq J$. Since J contains H, it follows that $D \leq J$. Since $N \neq 1$ and $N_V(\mu(M)) = \Omega$, we must have $\Omega \cap N \neq 1$, since otherwise $[N, D] = 1$. Hence $1 \neq v \in N$ for some $v \in \Omega$. Since J contains H and $N \lhd J$, we may suppose that $v_1 \neq 1$ without loss of generality. By hypothesis, $\mu(M)$ is non-Abelian, and so its centralizer in M is trivial. Hence $[v_1, w_1] \neq 1$ for some $w_1 \in \mu(M)$. But $[v_1, w_1] = [v, w_1] \in N$, since $w_1 \in J$ and $v \in N \lhd J$. Hence $1 \neq M \cap N \lhd M$ by Lemma 2.3; and this gives $\mu(M) \leq N$, $D \leq N = N^H$ as required.

3. In the proof of Theorem A, we shall use an auxiliary group Q which is closely related to the given group $K \neq 1$. Let K_1 and K_2 be two copies of K. In the free product $K_1 * K_2$, the normal subgroup $[K_1, K_2]$ is freely generated by the commutators

$$(4) \qquad [x_1, y_2] \quad (1 \neq x, 1 \neq y; x, y \in K);$$

and K_1 and K_2 are disjoint from $[K_1, K_2]$, the quotient group $K_1 * K_2 / [K_1, K_2]$ being isomorphic in a natural way with the direct product $K_1 \times K_2$. The group $K_1 * K_2 / K_1, K_2]'$ is therefore generated by two copies of K which we may identify with K_1 and K_2. Hence we may define

$$(5) \qquad Q = \langle K_1, K_2 \rangle \cong K_1 * K_2 / [K_1, K_2]'.$$

In Q, the subgroup $[K_1, K_2]$ is a free-Abelian group, the direct product of the infinite cyclic groups generated by the commutators (4).

The proof of the theorem is rather more difficult when both of the given groups H and K are finite. When at least one of H and K is infinite, we may suppose without loss of generality that $|H| \geq |K|$. In this case, Theorem A follows from

THEOREM A1. *Let H, K and L be any groups such that*

$$(6) \qquad |H| = \aleph_\alpha \geq \max(|K|, |L|) \text{ and } K \neq 1;$$

let Q be defined by (5) *and let $G = \mathrm{Wr}(L, Q)$. Then there is a copy K^* of K such that*

$$(7) \qquad\qquad K^* \leq \Omega(G, H) \text{ and } L \leq [H, K^*].$$

Here $\Omega(G, H)$ is the base group of $W = \mathrm{Wr}(L, Q, H)$. As noted in 1.3 (8), we have $L \lhd_2 G \lhd_2 W$, and so $L \lhd_2 W$ by Lemma 1.3. This also follows more directly from the fact that W is also the non-standard wreath product of L by $\mathrm{Wr}(Q, H)$.

Assuming (7), we have $L \leq J = \langle H, K^* \rangle \leq W$. Hence $L \lhd_2 J$ by Lemma 1.1. The solubility clause of Theorem A also follows immediately from Theorem A1. Let $\mathfrak{A}^m$ denote the variety of all soluble groups whose derived length is at most m. Suppose that $H \in \mathfrak{A}^h$, $K \in \mathfrak{A}^k$ and $L \in \mathfrak{A}^l$. Then $Q \in \mathfrak{A}^{k+1}$, and so $W \in \mathfrak{A}^{h+k+l+1}$, and J is soluble.

In [11], Neumann and Neumann proved, among other results, that *a countable $\mathfrak{A}^l$-group can always be embedded in some 2-generator $\mathfrak{A}^{l+2}$-group.* If we take H and K in Theorem A1 to be infinite cyclic groups, we obtain the following: *a countable $\mathfrak{A}^l$-group can always be subnormally embedded in some 2-generator $\mathfrak{A}^{l+3}$-group.*

For the proof of Theorem A1, we shall need

LEMMA 3.1. *Every infinite group H contains a subset A and three distinct elements a_1, a_2, a_3 such that*

$$(8) \qquad\qquad Aa_1^{-1} \cap Aa_2^{-1} \cap Aa_3^{-1} = 1 \text{ and } |A| = |H|.$$

PROOF. If H is of exponent 2, we may take A to be a basis of H and a_1, a_2, a_3 to be any three elements of A. The verification of (8) is immediate.

If H is not of exponent 2, it has an element α such that $\alpha^2 \neq 1$. The two elements 1 and α form a set A_0 such that $A_0 \cap A_0 \alpha^{-1} = 1$; and by Zorn's Lemma, there is a subset A of H containing A_0 and maximal subject to the condition $A \cap A\alpha^{-1} = 1$. Let $\xi \in H - A$ and let A_1 consist of A together with ξ. By the maximal property of A, we have $1 \neq \eta \in A_1 \cap A_1\alpha^{-1}$ for some η; and either $\eta = \xi$ and $\eta\alpha \in A$, or else $\eta = \xi\alpha^{-1} \in A$. In the first case $\xi \in A\alpha^{-1}$, in the second $\xi \in A\alpha$. Hence $H = A \cup A\alpha^{-1} \cup A\alpha$ and so $|A| = |H|$. In this case we may take $a_1 = 1$, $a_2 = \alpha$ and for a_3 any third element of A.

4. PROOF OF THEOREM A1. Since $K \neq 1$, it contains an element $b \neq 1$. Let

$$(9) \qquad\qquad \beta = [b_1, b_2, b_1],$$

so that $\beta \in [K_1, K_2] \leq Q$. In terms of the free-Abelian generators of $[K_1, K_2]$, we have $\beta = [b_1^2, b_2][b_1, b_2]^{-2}$, so that β is of infinite order, even if $b^2 = 1$. By Lemma 2.1, the group G contains a subgroup M, generated by $|L|$ copies of Q, such that (2) holds. Since Q is generated by two copies of K and $|L| \leq \aleph_\alpha$, we may write

$$(10) \qquad\qquad M = \langle K_\alpha; \alpha \in \Gamma \rangle, \text{ where } |\Gamma| \leq \aleph_\alpha,$$

the K_α are copies of K and Γ is a suitable set of labels which we may suppose to include the numbers 1 and 2. Hence there is a mapping θ of the set A of Lemma 3.1 onto Γ such that

(11) $$\theta(a_1) = \theta(a_3) = 1 \text{ and } \theta(a_2) = 2.$$

For each $y \in K$, let y^* be the vector in $\Omega(M, H)$ which is defined by the rule

(12) $$(y^*)_a = y_{\theta(a)} \text{ if } a \in A; \text{ and } (y^*)_x = 1 \text{ if } x \notin A.$$

The vectors y^* form a copy K^* of K; and this is contained in $\Omega(G, H)$, since $M \leq G$. Also, if $y \neq 1$, we have Sup $y^* = A$ by (12), and hence Sup $a_i y^* a_i^{-1} = A a_i^{-1}$ by the transformation law. Let

(13) $$\gamma = [a_1 b^* a_1^{-1}, a_2 b^* a_2^{-1}, a_3 b^* a_3^{-1}],$$

so that $\gamma \in [H, K^*]$. Then Sup $\gamma \leq A a_1^{-1} \cap A a_2^{-1} \cap A a_3^{-1} = 1$, by (8); and so $\gamma \in M$. By (12), $(a_i b^* a_i^{-1})_1 = (b^*)_{a_i} = b_{\theta(a_i)}$; and so $\gamma = \gamma_1 = \beta$ by (13), (11) and (9). Hence

(14) $$1 \neq \beta \in M \cap [H, K^*].$$

Since θ maps A onto Γ, the coordinates of the vectors y^* in K^* together generate M, by (12) and (10); and since $[H, K^*] \lhd J = \langle H, K^* \rangle$, Lemma 2.3 gives $M \cap [H, K^*] \lhd M$. Using (2) and (14), we obtain $L \leq \langle \beta^M \rangle \leq [H, K^*]$.
This concludes the proof of Theorem A1.

ADDENDUM 1. *If* $|H| = \aleph_0$ *and if* H *has an element* α *of infinite order, then we may take* $A = \text{Sup } K^*$ *to be contained in* $\langle \alpha \rangle$. *This makes*

(15) $$L \leq \langle \alpha^J \rangle.$$

PROOF. We may take A to consist of 1 together with the powers α^{2n-1} $(n = 1, 2, \cdots)$ and $a_1 = 1$, $a_2 = \alpha$, $a_3 = \alpha^3$. Then (8) holds since $|A| = \aleph_0 = |H|$. Since $\langle \alpha^J \rangle \lhd J$, we have $M \cap \langle \alpha^J \rangle \lhd M$, by Lemma 2.3. With this choice of the a_i, (13) gives $\gamma \in M \cap \langle \alpha^J \rangle$. Since $\beta = \gamma$, we obtain $L \leq \langle \beta^M \rangle \leq \langle \alpha^J \rangle$, as required.

5. To complete the proof of Theorem A, we must deal with the case where the given groups H and K are both finite. Let Q_1 be a copy of Q. We write

(16) $$G_1 = \text{Wr}(L, Q_1), \ W_1 = \text{Wr}(G_1, Q) \text{ and } W_2 = \text{Wr}(W_1, H).$$

With $1 \neq b \in K$ as before, let

(17) $$|K| = m; \text{ and } \alpha = [b_1, b_2]^m \text{ or } [b_2, b_1, b_1]^{m^2}$$

according to whether H is not or is of exponent 2. Here $[b_2, b_1, b_1]$ $= [b_1, b_2]^2 [b_1^2, b_2]^{-1}$ and so in either case α is of infinite order, even if $b^2 = 1$.

Noting that L is countable and $|Q| = \aleph_0$, we may apply Theorem A1 to the triple Q, Q_1, and L (in place of H, Q and L). Hence there is a copy K_3 of K (corresponding to the K^* of the preceding section) such that

$$(18) \qquad\qquad K_3 \leqq \Omega(G_1, Q), \text{ Sup } K_3 \leqq \langle \alpha \rangle \text{ and } L \leqq \langle \alpha^J \rangle,$$

where

$$(19) \qquad\qquad J = \langle K_1, K_2, K_3 \rangle.$$

Here we have used the Addendum to Theorem A1 and the fact that $Q = \langle K_1, K_2 \rangle$.

By (17), $\alpha \in [K_1, K_2]$; and by (18), Sup $y_3 = A \leqq \langle \alpha \rangle$ for all $y \neq 1$ in K. Hence Sup $y_1^{-1} y_3 y_1 = A y_1$ and Sup $y_2^{-1} y_3 y_2 = A y_2$ are both disjoint from A; and so the coordinates of the vectors $[y_2, y_3] = y_3^{-y_2} y_3$ and $[y_3, y_1] = y_3^{-1} y_3^{y_1}$ all lie in various copies of K. Therefore, by (17),

$$(20) \qquad\qquad [y_2, y_3]^m = [y_3, y_1]^m = 1.$$

Similarly, if H is of exponent 2, we have $[y_1, y_2]^m \notin \langle \alpha \rangle$, if $y \neq 1$, since in this case $\alpha = [b_2, b_1, b_1]^{m^2}$; and so

$$(21) \qquad\qquad [[y_1, y_2]^m, y_3]^m = 1.$$

Further, since $[K_1, K_2]$ is Abelian, we have

$$(22) \qquad\qquad [[y_2, y_1]^m, y_1]^m = [y_2, y_1, y_1]^{m^2}.$$

This follows from the identity $[uv, w] = [u, w]^v [v, w]$ by induction on r, taking $v = [y_2, y_1]$, $u = v^r$ and $w = y_1$.

We can now state

THEOREM A2. *Let H and K be any finite groups such that*

$$(23) \qquad\qquad |H| > 2 \text{ and } |K| > 1;$$

and let L be any countable group. Then there is a copy $K^\dagger$ of K in $\Omega(W_1, H)$ such that

$$(24) \qquad\qquad L \leqq [H, K^\dagger].$$

As in the case of Theorem A1, it follows from this that $L \triangleleft_2 J^\dagger$, where $J^\dagger = \langle H, K^\dagger \rangle$; and that $J^\dagger$ is soluble whenever H, K and L are soluble. The proof of Theorem A2 will therefore complete the proof of Theorem A.

PROOF. Since $J \leqq W_1$ by (19) we may choose $K^\dagger$ to be a subgroup of $\Omega(J, H)$. If H is not of exponent 2, we choose d in H such that $d^2 \neq 1$; and define the vector $y^\dagger$, for $y \in K$, by writing only the 1, d^{-1} and d-coordinates in order as

$$(25) \qquad\qquad y^\dagger = (y_1, y_2, y_3);$$

the remaining coordinates, if any, are to be trivial. The corresponding coordinates of $d^{-1}b\dagger d$ are then b_2, b_3, b_1 or $b_2, 1, b_1$ according as $d^3 = 1$ or not. In either case, $[b\dagger, d^{-1}b\dagger d]^m = [b_1, b_2]^m = \alpha$, by (20) and (17). Hence

$$(26) \qquad\qquad \alpha \in [H, K\dagger].$$

If H is of exponent 2, it has a subgroup of order 4, by (23). Let $1, d_1, d_2$ and $d_3 = d_1 d_2$ be the elements of such a subgroup. In this case, we take the $1, d_1, d_2$ and d_3-coordinates of $y\dagger$ in order to be given by

$$(27) \qquad\qquad y\dagger = (y_2, y_1, y_1, y_3)$$

the remaining coordinates again being trivial. Then

$$d_1 b\dagger d_1 = (b_1, b_2, b_3, b_1) \text{ and } d_2 b\dagger d_2 = (b_1, b_3, b_2, b_1).$$

Writing $c = [b_1, b_2]^m$ and using (20), we have $[b\dagger, d_1 b\dagger d_1]^m = (c^{-1}, c, 1, 1)$. Then (21) gives $[c, b_3]^m = 1$; and since in this case $\alpha = [c^{-1}, b_1]^m$ by (17) and (22), we obtain $\alpha = [[b\dagger, d_1 b\dagger d_1]^m, d_2 b\dagger d_2]^m$. Thus (26) holds in this case also.

By (19) and (25) or (27), the coordinates of the vectors $y\dagger$ in $K\dagger$ together generate J. Since $[H, K\dagger] \lhd J\dagger = \langle H, K\dagger \rangle$, it follows that $J \cap [H, K\dagger] \lhd J$, by Lemma 2.3. Hence $L \leq \langle \alpha' \rangle \leq [H, K\dagger]$ by (18) and (26).

This completes the proof of the theorem, and therewith of Theorem A.

6. In the proof of Theorem A1, the role of Lemma 3.1 is to provide supports, for conjugate vectors in a wreath product, which have small intersections. More powerful lemmas give more precise results, and we now consider a few of these.

A subset A of any group will be called *azygetic* if there is no relation of the form $a_1^{-1} a_2 = a_3^{-1} a_4$ connecting any four distinct elements a_i of A. Thus every set of at most 3 elements is azygetic; and by Zorn's Lemma, every subset X of a group contains azygetic subsets which are maximal in X.

LEMMA 3.2. *Let X be any infinite set of elements in a group H and let A be a maximally azygetic subset of X. Then $|A| = |X|$.*

PROOF. We may suppose that $A \neq X$. Let x be any element of X not in A. By the maximal property of A, there are three distinct elements a_1, a_2, a_3 in A such that $x = a_1 a_2^{-1} a_3$. Hence $X \leq AA^{-1}A$; and so $|A| = |X|$ since X is infinite.

LEMMA 3.3. *Let A be any azygetic subset of a group H, and let a_1, a_2, a_3 be any three distinct elements of A. Then*

$$(28) \qquad\qquad Aa_1^{-1} \cap Aa_2^{-1} \cap Aa_3^{-1} = 1$$

except when $a_1 a_2^{-1}$ is of order 3 and $a_3 = a_1 a_2^{-1} a_1 = a_2 a_1^{-1} a_2$.

PROOF. Suppose that $1 \neq x \in Aa_1^{-1} \cap Aa_2^{-1} \cap Aa_3^{-1}$. Then $x = b_i a_i^{-1} (i = 1, 2, 3)$ where b_1, b_2, b_3 are also three distinct elements of A. Thus $b_i^{-1} b_j = a_i^{-1} a_j$;

and if $i \neq j$, we have $b_i \neq a_i$ and $b_i \neq b_j$. Since A is azygetic, this leaves only two possibilities. Either (i) $b_1 = a_2, b_2 = a_3$ and $b_3 = a_1$; or else (ii) $a_1 = b_2, a_2 = b_3$ and $a_3 = b_1$. Hence $a_1 a_2^{-1} = a_2 a_3^{-1}$ is of order 3 and equal to x^{-1} in case (i), or x in case (ii). The result now follows.

We mention without proof

LEMMA 3.4. *Let x and y be any two distinct elements of the group H. Then $|Ax \cap Ay| \leqq 3$ for every azygetic subset of A of H.*

Another result which will be useful is

LEMMA 3.5. *Let $x_1, \cdots, x_n$ be distinct elements of the infinite group H. Then H contains a subset A such that*

$$(29) \qquad |A| = |H| \text{ and } |Ax_i \cap Ax_j| = 0 \text{ for } i \neq j \quad (i,j = 1, \cdots, n).$$

PROOF. Since the elements x_i are distinct, H contains a non-empty subset A which is maximal subject to the condition that the n sets $Ax_1, \cdots, Ax_n$ are (set-theoretically) disjoint in pairs. Let y be any element of H not in A. By the maximal property of A, there is a pair $i \neq j$ and an element $a \in A$ such that $yx_i = ax_j$. Hence $y \in Ax_j x_i^{-1}$. Since y was arbitrary, this shows that

$$H = \bigcup_{i,j=1}^{n} Ax_j x_i^{-1};$$

and since H is infinite, it follows that $|A| = |H|$.

7. We now reconsider the proof of Theorem A1. Use of the group Q and the form (9) for β appears to be the path of least resistance. When H is not of exponent 2, the form $\beta = [b_1, b_2]$ would do just as well, as the proof of Lemma 3.1 makes clear. Perhaps of more interest is

ADDENDUM 2. *In Theorem A1, if the group $[K', K]$ contains an element β of infinite order, then we may replace Q by K.*

PROOF. In Lemma 2.1, we may take $G = \mathrm{Wr}(L, K)$ and obtain $L \leqq \langle \beta^M \rangle$, where M is contained in G and has the same form (10) as before, in which we suppose that $K_1 = K$. But in place of the simple expression (9), we now have

$$(30) \qquad \beta = \bigcup_{i=1}^{n} [x_i, y_i, z_i]^{\pm 1}$$

for suitably chosen elements x_i, y_i and z_i in K. This means that the subset A of H, which is to be the support of the vector group K^*, must be chosen more carefully.

We may take A to be any maximally azygetic subset of H. Then $|A| = |H|$ by

Lemma 3.2, since the group H in Theorem A1 is infinite. Let the a_{i1} and a_{i2} $(i = 1, \cdots, n)$ be any $2n$ distinct elements of A. We may then select n further elements distinct from these and from each other and such that $a_{i3} \neq a_{i1}a_{i2}^{-1}a_{i1}$, $(i = 1, \cdots, n)$. Then Lemma 3.3 gives

(31) $$Aa_{i1}^{-1} \cap Aa_{i2}^{-1} \cap Aa_{i3}^{-1} = 1 \ (i = 1, \cdots, n).$$

Since $|\Gamma| \leqq |A|$, we may choose the mapping θ of A onto Γ such that

(32) $$\theta(a_{ij}) = 1 \ (i = 1, \cdots, n; \quad j = 1, 2, 3).$$

With K^* defined by (12), we must now take

(33) $$\gamma = \prod_{i=1}^{n} [a_{i1}x_i^*a_{i1}^{-1}, a_{i2}y_i^*a_{i2}^{-1}, a_{i3}z_i^*a_{i3}^{-1}]^{\pm 1}.$$

(31) ensures that each of the n factors of γ lies in M; and by (12) and (32), the i-th factor of γ coincides with the i-th factor of β. Thus $\gamma = \beta$, and the rest of the proof proceeds as before.

8. PROOF OF THEOREM B1. We have to show that, if the groups H, K and L satisfy the same conditions as in Theorem A, then $L \leqq \mu(G)$ for some group of the form $G = \langle H, K \rangle$. Assuming $L \neq 1$, the well known fact mentioned in §1.4, viz. that L can always be embedded in a perfect simple group P such that $|P| = |L^* L|$, allows us to suppose without loss of generality that L is itself a perfect simple group:

(34) $$L = L' = \mu(L) \neq 1.$$

We deduce Theorem B1 from Theorem A, using the groups of the form $J = \langle H, K \rangle$ provided (with $K = K^*$ or $K^\dagger$, respectively) by Theorems A1 and A2. Hence $L \lhd_2 J$ in each case; and (34) therefore implies that L' is a minimal normal subgroup of J. We define

(35) $$G = J/N,$$

where N is any normal subgroup of J which is maximal subject to

(36) $$L \cap N = 1.$$

This ensures that G is monolithic, with $\mu(G) = NL^J/N$, so that L can be embedded in $\mu(G)$.

It only remains to show that G is of the form $\langle H, K \rangle$; or more precisely, that $H \cap N = 1$ and $K \cap N = 1$. These two relations will follow from (36), if we can show that

(37) $$L \leqq \langle x^L \rangle \ \text{for all} \ x \neq 1 \ \text{in} \ H$$

and

(38) $$L \leqq \langle y^J \rangle \text{ for all } y \neq 1 \text{ in } K.$$

In Theorem A1, we have $L \leqq \text{Wr}(L, Q) \leqq \text{Wr}(\text{Wr}(L, Q), H)$, so that (37) follows directly from (34) and Lemma 2.2. Note further that the element

$$\gamma(y) = [a_1 y^* a_1^{-1}, a_2 y^* a_2^{-1}, a_3 y^* a_3^{-1}] \in \langle (y^*)^H \rangle,$$

since the a_i lie in H. Just as for the element $\gamma = \gamma(b)$ used in the proof of Theorem A1, we find here the relation $\gamma(y) = [y_1, y_2, y_1]$, which is a non-trivial element of Q since $y \neq 1$. Since $L \leqq \text{Wr}(L, Q)$, we have $[L, L^{\gamma(y)}] = 1$; and so $L \leqq \langle \gamma(y)^L \rangle$ by (34) and Lemma 2.2. Hence $L \leqq \langle (y^*)^J \rangle$, which gives (38) for this case, where $K = K^*$.

In Theorem A2, we have $L \leqq W_1 \leqq \text{Wr}(W_1, H)$; so that once again $[L, L^x] = 1$ and (37) follows from (34) and Lemma 2.2. Further, using (25) and (27), we have $L^{y\dagger} = L^{y_2}$ or L^{y_1} according as H is of exponent 2 or not. Since $y \neq 1$, y_1 and y_2 are non-trivial elements of Q. By (16), $L \leqq G_1 \leqq W_1 = \text{Wr}(G_1, Q)$; and it follows that $[L, L^{y\dagger}] = 1$. Hence $L \leqq \langle (y\dagger)^L \rangle$ by (34) and Lemma 2.2. Here $L \leqq J\dagger = \langle H, K\dagger \rangle$ and this gives (38) in this case also, where $K = K\dagger$.

This completes the deduction of Theorem B1 from Theorem A.

For the proof of the finiteness of the invariant l, we need to know a little more, though only in the case of infinite H, viz. that the definition (12) of K^* can be so chosen that

(39) $$[K^*, K^*] \leqq H^J.$$

To ensure this we need only choose the support A of K^*, which is provided by Lemma 3.1, such that $A \cap Au = \varnothing$ for some $u \in H$; for then $[K^*, u^{-1}K^*u] = 1$, and so the derived group of K^* is contained in $\langle u^{K^*} \rangle \leqq H^J$, by Lemma 2.2. If K is perfect, (39) implies that $K^* \leqq H^J$ and so $J = H^J$.

That the support A can always be chosen to satisfy this additional condition follows easily from Lemma 3.5, 3.2 and 3.3. However, we shall give a direct proof of the important part of Theorem B1, making no appeal to Theorem A, although using a similar method.

3. The finiteness of $l(K)$.

1. LEMMA 4. *Let the perfect simple group P be generated by $|A|$ not necessarily distinct copies of the group K and let $a_1, a_2, \cdots, a_n$ be n distinct elements of A. Then there exist elements $b^{(1)}, \cdots, b^{(n)}$ in K and an expression*

(1) $$P = \langle K_a; a \in A \rangle$$

for P as the join of copies K_a of K such that $c \neq 1$, where

(2) $$c = [b_{a_1}^{(1)}, \cdots, b_{a_n}^{(n)}].$$

We recall the convention that b_a is the element of K_a which corresponds, in some fixed isomorphism, to the element $b \in K$.

PROOF. By hypothesis, some expression of the form (1) exists for P. Since P is simple, $P \neq 1$ and so $K \neq 1$. When $n = 1$, this leaves nothing to prove. Suppose that, for some $n \geq 1$ and for some choice of the $b^{(i)}$ in K and the expression (1), we have $c \neq 1$. Let $a_{n+1} = \alpha$ be any element of A distinct from $a_1, \cdots, a_n$. Then $P = \langle P_\alpha, K_\alpha \rangle$, where $P_\alpha = \langle K_a; a \in A, a \neq \alpha \rangle$. Hence $1 \neq K_\alpha^{P_\alpha} \lhd P$; and so $K_\alpha^{P_\alpha} = P$, since P is simple. Since P is also perfect, its centre is trivial; and since $c \neq 1$, it follows that $c^* = [c, (\beta_\alpha)^{x_\alpha}] \neq 1$ for some $\beta = b^{(n+1)} \in K$ and some $x_\alpha \in P_\alpha$. Then $P = \langle P_\alpha, K_\alpha^{x_\alpha} \rangle$; and if we replace K_α in (1) by $K_\alpha^{x_\alpha}$, we obtain a new expression of the same form with respect to which the $n + 1$-fold commutator $c^* \neq 1$ and has the form corresponding to (2). The lemma now follows by induction on n.

LEMMA 5. *Suppose that, in Lemma 4, A is a subset of the group H and that*

(3) $$Aa_1^{-1} \cap Aa_2^{-1} \cap \cdots \cap Aa_n^{-1} = 1.$$

Then there is a copy K^* of K in the base group $\Omega = \Omega(P, H)$ of $W = \mathrm{Wr}(P, H)$, such that

(4) $$\mu(J) = P^H, \text{ where } J = \langle H, K^* \rangle \text{ and } \mathrm{Sup}\, K^* = A;$$

so that $J = P \wr H$ if A is finite.

PROOF. By Lemma 4, there is an expression (1) for P and elements $b^{(i)} \in K$ such that $c \neq 1$. For $y \in K$, let y^* be the vector in Ω defined by

(5) $$y_a^* = y_a \text{ if } a \in A; \quad y_h^* = 1 \text{ if } h \notin A.$$

The vectors y^* form a copy K^* of K, and their coordinates together generate P, by (1) and (5). Since $(K^*)^H \lhd J$, we have $P \cap (K^*)^H \lhd P$ by Lemma 2.3.

If $a \in A$ and $1 \neq y \in K$, we have $\mathrm{Sup}\, ay^*a^{-1} = Aa^{-1}$ by (5). Hence the commutator $\gamma = [a_1 b^{(1)*} a_1^{-1}, a_2 b^{(2)*} a_2^{-1}, \cdots, a_n b^{(n)*} a_n^{-1}] \in P$ by (3). The 1-coordinate of $a_i b^{(i)*} a_i^{-1}$ is $b_{a_i}^{(i)}$ by (5). Hence $\gamma = c$, by (2). But $c \neq 1$ and $\gamma \in (K^*)^H$. We conclude that, since P is simple, $(K^*)^H$ must contain P. Hence $R = P \wr H \leqq J$. Since $P = \mu(P)$, we have $\mu(J) = P^H$ by Lemma 2.4.

If A is finite, we have $K^* \leqq P^H$, which is the group of all vectors in Ω of finite support. Hence $J = \langle H, K^* \rangle = R$ in this case.

2. We now prove a key lemma, which not only contains the major part of Theorem B1 in the form required to prove the finiteness of $l(K)$, but then has Theorem B2 as an immediate corollary. This is

LEMMA 6. *Let H, K and L be any non-trivial groups such that either*

(6)   (i) $|H| = \aleph_\alpha \geqq \max(|K|, |L|)$; *or* (ii) $|L| \leqq |K * K|$ *and* $l(K) < |H|$.

Then there exists a perfect simple group P and a copy K^* of K in $\Omega(P.H)$ such that

(7) $L \leqq P$ *and* $\mu(J) = P^H$, *where* $J = \langle H, K^* \rangle$;

and further

(8) $J = H^{K^*}$ *if K is perfect.*

PROOF. We begin by choosing the perfect simple group P and the subset A oï H so that the conditions (1) of *Lemma 4* and (3) of *Lemma 5* hold. Then (7) will follow from *Lemma 5* if we define K^* by (5).

In case (i), $|K \times L| \leqq \aleph_\alpha$ and we may therefore choose P to be of order $\aleph_\alpha$ with $K \times L$ as a subgroup. Since $K \neq 1$, this gives $P = \langle K^u; u \in P \rangle$. By Lemma 3.1, H has a subset A and three distinct elements such that (3) holds with $n = 3$ and $|A| = |H|$. This makes $|A| = |P|$, so that P is generated by $|A|$ copies of K.

In case (ii), by the definition of $l(K)$, we may suppose that P contains L and is generated by $l(K)$ copies of K. If H is infinite, we choose A and the a_i as in case (i). If $|H| = n + 1$ is finite, we take A to consist of all the non-trivial elements a_1, $\cdots, a_n$ of H. Then (3) holds; and since $l(K) < |H|$, P is generated by at most $|A|$ copies of K.

It remains to prove (8). Suppose that $K = K'$. Then K coincides with the n-th term of its lower central series; it is therefore generated by all the commutators of the form $u = [y^{(1)}, y^{(2)}, \cdots, y^{(n)}]$, where $y^{(1)}, \cdots, y^{(n)}$ run independently through K. We have

(9) $u^* \equiv [a_1 y^{(1)*} a_1^{-1}, a_2 y^{(2)*} a_2^{-1}, \cdots, a_n y^{(n)*} a_n^{-1}] \bmod D = H^{K^*}$.

By (3) and (5), the right-hand commutator in (9) lies in P. But $1 \neq D \lhd J$ and so D contains $\mu(J) = P^H$. Hence $u^* \in D$. Since the commutators u^* generate K^* this gives $K^* \leqq D$ and hence $J = \langle H, K^* \rangle$ coincides with D, as required.

This concludes the proof of the Lemma 6.

Once the finiteness of $l(K)$ has been established for all groups K, we may take the set A in case (ii) of the lemma to be finite, even when H is infinite. This makes $J = P \wr H$ by Lemma 5 and Theorem B2 follows and therewith a major part of Theorem B1.

We shall then show, without further appeal to Theorem B1, that $l(K) \leqq 3$ for $|K| \neq 2$ and $l(K) \leqq 4$ for $|K| = 2$. Since the conclusion of Theorem B1 is symmetrical as between H and K, this will leave only a small squad of awkward cases requiring special treatment viz. those in which $|H|$ and $|K|$ are respectively (i) 3 and 3; (ii) 4 and 2; and (iii) 3 and 2. These cases are only required in the proof

of our two '$l = 2$'-theorems $D1$ and $D3$. The first two are dealt with in Lemma 18: cf. § 5.3–4; and the third in Lemma 20: cf. § 5.8. We shall then have a complete proof of Theorem B1 which makes no appeal to Theorem A.

3. As noted in §1.6, the problem of embedding a given group L in some simple group of the form $S = \langle K_1, K_2, \cdots \rangle$, where the groups $K_1, K_2, \cdots$ are also given, is equivalent to that of embedding L in a hololophic subgroup of any group G having the same form as S and in which the generating subgroups $K_1, K_2, \cdots$ are also hololophic. Useful for this purpose are the groups G described in

LEMMA 7. *Let* $G = \langle J_1, J_2, \cdots, J_n \rangle$ *and suppose that the* J_i *are subgroups of* G *which satisfy the n conditions*

(10) $J_i = (J_i \cap \mu(J_{i-1}))^{J_i}$ *(i* mod *n).*

Then $J_1, \cdots, J_n$ *are hololophic in* G.

PROOF. If any $J_{i-1} = 1$, then J_i is also trivial; and it follows in cyclic order that $J_{i+1}, \cdots, J_{i-2}$ are all trivial and $G = 1$. Dismissing this case, let $M \triangleleft G$ and suppose $J_{i-1} \cap M \neq 1$. Since $J_{i-1} \cap M \triangleleft J_{i-1}$, we have $\mu(J_{i-1}) \leqq M$. Hence $J_i \leqq M$ by (10); and so $J_i \cap M \neq 1$; and M contains all the J_i by cyclic induction, giving $M = G$. The lemma now follows.

Let $J_1, \cdots, J_4$ be any four groups with subgroups H_i and $\bar{H}_i$ such that

(11) $\langle H_i, \bar{H}_i \rangle \leqq J_i, H_i \cap \bar{H}_i = 1$ and $\bar{H}_i \cong H_{i+1}$ *(i* mod 4).

Supposing the four isomorphisms in (11) to be given, we may form the groups

(12) $G_1 = J_1 * J_2 / \bar{H}_1 = H_2$ and $G_2 = J_3 * J_4 / \bar{H}_3 = H_4$

each of which is a free product with a single amalgamated subgroup, as indicated. The subgroups H_1 of J_1 and $\bar{H}_2$ of J_2 are both disjoint from the amalgamated subgroup $\bar{H}_1 = H_2$ of G_1, by (11). Hence the subgroup $\langle H_1, \bar{H}_2 \rangle$ of G_1 is the ordinary free product $H_1 * \bar{H}_2$: cf. Neumann's paper [12]. Similarly, the subgroup $\langle H_3, \bar{H}_4 \rangle$ of G_2 is $H_3 * \bar{H}_4$. Since $H_1 \cong \bar{H}_4$ and $\bar{H}_2 \cong H_3$ by (11), we may now form the free product G of G_1 and G_2 with the subgroups $\langle H_1, \bar{H}_2 \rangle$ and $\langle H_3, \bar{H}_4 \rangle$ amalgamated in the obvious way. Thus the *quadrilateral group.*

(13) $G = J_1 * J_2 * J_3 * J_4 / \bar{H}_1 = H_2, \bar{H}_2 = H_3, \bar{H}_3 = H_4, \bar{H}_4 = H_1$

has the form

(14) $G = \langle J_1, \cdots, J_4 \rangle$ with $\bar{H}_i = H_{i+1} = J_i \cap J_{i+1}$ *(i* mod 4).

Although the four corners H_i of the quadrilateral are the intersections of adjacent sides J_i, in general J_i will be larger than the group-theoretical join of the two corners H_i and H_{i+1} which it contains. The two 'diagonals' are the free products $H_1 * H_3$ and $H_2 * H_4$.

4. LEMMA 8. *Let H be any infinite group, $K_1, \cdots, K_4$ four icosahedral groups, and L any group such that $|L| \leq |H|$. Then L can always be embedded in some simple group of the form*

(15) $$S = \langle H_1^{K_1}, \cdots, H_4^{K_4} \rangle,$$

where $H_1, \cdots, H_4$ are four copies of H.

PROOF. For each $i = 1, \cdots, 4$, let H_i and $\bar{H}_i$ be two copies of H and L_i a copy of L. Note that H_i is infinite, $K_i = K_i'$ is finite and non-trivial, and $|L_i \times \bar{H}_i| = |H_i|$. By case (i) of Lemma 6, there exists a perfect simple group P_i and a subgroup of the form $J_i = \langle H_i, K_i \rangle$ in $\mathrm{Wr}(P_i, H_i)$ such that

(16) $$L_i \times \bar{H}_i \leq \mu(J_i) = P_i^{H_i} \text{ and } J_i = H_i^{K_i} \quad (i = 1, \cdots, 4).$$

This implies that $H_i \cap \bar{H}_i = 1$. By hypothesis, $\bar{H}_i \cong H \cong H_{i+1}$ for i mod 4. Hence the conditions (11) hold and we may form the quadrilateral group G defined by (13). In G we have $H_i = \bar{H}_{i-1} \leq J_i \cap \mu(J_{i-1})$ for all i mod 4, by (16); and since $J_i = H_i^{K_i}$, (10) holds with $n = 4$. Hence $J_1, \cdots, J_4$ are hololophic in G by Lemma 7; and so there is a simple quotient group $S = G/N$ of the form $S = \langle J_1, \cdots, J_4 \rangle$. The relations $J_i = H_i^{K_i}$ in (16) show that S has the required form (15); and L is embedded in S as any one of the subgroups $L_i \leq J_i$.

This concludes the proof of Lemma 8.

Since $|K_i| = 60$ for each i, S is generated by 240 copies of H. Hence $l(H) \leq 240$ for all infinite H. For any finite $K \neq 1$, the group $H = K * K$ is infinite. Hence $l(K) \leq 480$. Thus $l(K)$ *is finite for all groups K.* As noted above, *Theorem B2 now follows* as a corollary of Lemma 6.

Another easy deduction from Lemma 8, although it will be superseded by better results in § 4, is that *a countable group can always be embedded in some 9-generator simple group.* For we have $H_{i+1} = \bar{H}_i \leq J_i = \langle H_i, K_i \rangle$ in the group S of (15), and hence $S = \langle H_1, K_1, K_2, K_3, K_4 \rangle$. Taking H to be an infinite cyclic group in Lemma 8, and noting that the icosahedral groups K_i can each be generated by two elements, it follows that S is a 9-generator group.

5. We show finally how to deduce from the original Theorem IV of [1] a *pure embedding theorem for countable groups* which is not a direct corollary of Theorems A and B1.

For any group G and ordinal α, let

(17) $\mathfrak{U}_\alpha$ and $\mathrm{SQ}(G)$

denote respectively the class of all groups of order at most $\aleph_\alpha$, and the class of all groups which can be embedded in some quotient group G/N of G. Thus Theorem IV of [1] implies that

(18) $$\mathfrak{U}_0 = \mathrm{SQ}(F_2),$$

where F_2 is the free group of rank 2.

LEMMA 9. *Suppose that the group G has a normal subgroup F such that $|G : F|$ is finite and $\mathfrak{U}_\alpha \leq \mathrm{SQ}(F)$. Then $\mathfrak{U}_\alpha \leq \mathrm{SQ}(G)$. More precisely, every group L in $\mathfrak{U}_\alpha$ is isomorphic with some M/N, where $N \lhd G$ and $M \leq F$.*

PROOF. We may suppose without loss of generality that L is a perfect simple group. By hypothesis, $L \in \mathrm{SQ}(F)$ and so $L \cong C_0/N_0$ for some $N_0 \lhd F$ and some subgroup C_0 of F which contains N_0. By Zorn's Lemma, we may choose the normal subgroup N_1 of F to be maximal subject to the condition that $C_0 \cap N_1 = N_0$. Then $C_1/N_1 \cong L$, where $C_1 = C_0 N_1$. By the maximal property of N_1, every nontrivial normal subgroup of F/N_1 must contain C_1/N_1, since by hypothesis L is simple. Hence $C_1/N_1 \leq \mu(F/N_1)$.

Now let $N = \bigcap_{x \in G} N_1^x$. Since $|G : F|$ is finite, we can choose a minimal expression $N = N_1 \cap N_2 \cap \cdots \cap N_r$ for N has the intersection of conjugates N_i of N_1 in G. It follows that $N^* = N_2 \cap \cdots \cap N_r > N = N_1 \cap N^*$; where we must take $N^* = F$ if $N_1 \lhd G$. Hence $N^*/N \cong N_1 N^*/N_1$, which is a non-trivial normal subgroup of the monolithic group F/N_1. Hence N^*/N contains a copy of $\mu(F/N_1)$; and so it also contains a copy of $L \cong C_1/N_1$. Since $N \lhd G$ and $N^* \leq F$, the lemma now follows.

COROLLARY 9.1. *If a group G has a non-cyclic free subgroup of finite index, then $\mathfrak{U}_0 \leq \mathrm{SQ}(G)$.*

For G then has a normal free subgroup F of finite index, with F of rank at least 2. Hence $\mathfrak{U}_0 \leq \mathrm{SQ}(F)$ by (18).

COROLLARY 9.2. *Given any groups H and K with $|H| > 2$ and $|K| > 1$, a countable group L can always be embedded in some group of the form $J = \langle H, K \rangle$.*

Unlike Corollary 9.1, this is a direct consequence of both Theorems A and B1. A quite different proof has been obtained by Schupp [13], using the methods of 'small cancellation' theory[1]. Here we deduce it from Lemma 9.

PROOF. We may suppose that H and K are either both finite, or both cyclic. For in the general case, there will always exist subgroups H_1 of H and K_1 of K such that $|H_1| > 2$; $|K_1| > 1$, and such that either H_1 and K_1 are both cyclic, or else H_1 is the 4-group and $|K_1| = 2$. Assuming that $L \leq J_1 = \langle H_1, K_1 \rangle$, we can form the free product J_2 of H and J_1 with amalgamated H_1, and then the free product J of J_2 and K with amalgamated K_1, giving $L \leq J = \langle H, K \rangle$.

If H and K are both finite, we take $G = H * K$ and $F = [H, K]$ in Lemma 9; since the rank of F is $(|H| - 1)(|K| - 1) \geq 2$, the result follows from Corollary 9.1. In particular, when $H = \langle u \rangle$ and $K = \langle v \rangle$, we obtain an embedding of L in

---

$\langle w^J \rangle$ for some $J = \langle u, v \rangle$, where $w = [u, v]$. If $\langle t \rangle$ is an infinite cyclic group, the subgroup $J^* = \langle tu, v \rangle$ of $\langle t \rangle \times J$ will then also contain L. Here tu is of infinite order. In this way we deal with the case in which one of H and K is an infinite cyclic group and the other is a finite cyclic group. When both H and K are infinite cyclic groups, the result is contained in Theorem IV of [1].

Let $\mathfrak{B}$ be any variety of groups; and for any group G let $\phi(G)$ be the corresponding verbal subgroup of G, so that $\phi(G) \leq H \triangleleft G$ if and only if $G/H \in \mathfrak{B}$.

COROLLARY 9.3. *Provided that $\mathfrak{B}$ is not the variety of all groups, the group J and the embedding of L from Corollary 9.2 can always be chosen so that $L \leq \phi(J)$.*

PROOF. The countable group $L \times F_2$ can be embedded in a countable simple group P; and by Corollary 9.2, we may suppose that $P \leq J = \langle H, K \rangle$. If $P \cap \phi(J) = 1$, then $\phi(P) = 1$. But F_2, and therefore P, contains a free subgroup of infinite rank; and so $\phi(P) = 1$ would imply that $\mathfrak{B}$ is the variety of all groups, contrary to hypothesis. Since P is simple, the only alternative to $P \cap \phi(J) = 1$ is $P \leq \phi(J)$.

4. Proof of Theorem C

1. The basic method is the bilateral construction and the key lemma is

LEMMA 10. *Let K_1, K_2, K_3 and L be non-trivial groups such that*

(1) $$\left| L \times K_3 \right| \leq \left| K_1 * K_1 \right|.$$

Suppose further that there exists a non-trivial group H_2 which can be embedded in K_3, a group of the form $J_2 = \langle H_2, K_2 \rangle$ and a finite group $\bar{H}_2$ such that

(2) $$i(K_1) < \left| \bar{H}_2 \right|, \quad H_2 \times \bar{H}_2 \leq J_2 \quad and \quad \langle \bar{H}_2, K_2 \rangle \leq \mu(J_2).$$

Then L can be embedded in some simple group of the forms

(3) $$S = \langle K_1, K_2, K_3 \rangle = \langle K_1, J_2 \rangle.$$

PROOF. Let H_1 be a copy of $\bar{H}_2$. Then $i(K_1) < \left| H_1 \right|$, by (2). It follows from (1) and Theorem B2, that there exists a perfect simple group P_1 which contains a copy of $L \times K_3$ and is such that $P_1 \wr H_1$ has the form $J_1 = \langle H_1, K_1 \rangle$.

Since H_1 is finite, the base group $P_1^{H_1}$ of J_1 contains a copy $\bar{P}_1$ of P_1 consisting of all the constant vectors in $\Omega(P_1, H_1)$. Since P_1 contains a copy of K_3, so does $\bar{P}_1$ and we may identify the latter with K_3 itself. Since H_2 can be embedded in K_3, we have $H_2 \cong \bar{H}_1 \leq K_3 \leq \bar{P}_1$. Here we have denoted the copy of H_2 in K_3 by $\bar{H}_1$. But $[H_1, \bar{P}_1] = 1$. Hence the subgroup $\langle H_1, \bar{H}_1 \rangle$ of J_1 is the direct product $H_1 \times \bar{H}_1$, and is therefore isomorphic with the subgroup $\bar{H}_2 \times H_2$ of J_2. Thus we may form the bilateral group

(4) $$G = J_1 * J_2 / H_1 = \bar{H}_2, \quad H_2 = \bar{H}_1,$$

which is the free product of J_1 and J_2 with their direct product subgroups amalgamated in the obvious way.

In G, we have $H_1 = \bar{H}_2 \leqq J_1 \cap \mu(J_2)$ by (2); and $J_1 = P_1 \wr H_1 = H_1^{J_1}$ since P_1 is a perfect simple group and $H_1 \neq 1$. Further, $K_2 \leqq \mu(J_2)$ by (2), and so $J_2 = \langle H_2, K_2 \rangle = H_2^{J_2}$ since $H_2 \neq 1$; and $H_2 = \bar{H}_1 \leqq J_2 \cap \mu(J_1)$. Hence $J_i = (J_i \cap \mu(J_{i-1}))^{J_i}$ for each i mod 2; and so J_1 and J_2 are hololophic in G by Lemma 7. Hence G has a simple quotient group of the form $S = \langle J_1, J_2 \rangle$.

Since $J_1 = \langle H_1, K_1 \rangle$ and $H_1 = \bar{H}_2 \leqq J_2$, we have $S = \langle K_1, J_2 \rangle$. But $J_2 = \langle H_2, K_2 \rangle = \langle \bar{H}_1, K_2 \rangle$ and the subgroup $\bar{H}_1$ of J_1 is contained in the subgroup K_3 of $\bar{P}_1$. Hence $S = \langle K_1, K_2, K_3 \rangle$; and this completes the proof of the lemma.

The group J_1 is of RP-type. If we take J_2 also to be of RP-type and make a slight change of notation, we obtain

LEMMA 11. *Let H, K_1, K_2 and L be non-trivial groups such that*

(5) $$|H \times L| \leqq |K_1 * K_1|;$$

and suppose further that H has a finite subgroup H_2 such that

(6) $$l(K_2) < |H_2|.$$

Then L can be embedded in some simple group of the form

(7) $$S = \langle H, K_1, K_2 \rangle.$$

Here H corresponds to the K_3 of Lemma 10.

PROOF. Since $l(K_1)$ is finite (cf. §3.4), we can select a finite group H_1 such that $l(K_1) < |H_1|$. By (6) and Theorem B2, there is a perfect simple group P_2 which contains a copy of H_1 and is such that

(8) $$J_2 = P_2 \wr H_2 = \langle H_2, K_2 \rangle \text{ where } K_2 \leqq P_2^{H_2}.$$

Since H_2 is finite, the base group $P_2^{H_2}$ of J_2 contains a copy $\bar{P}_2$ of P_2 such that $[H_2, \bar{P}_2] = 1$; and $\bar{P}_2$ contains a copy $\bar{H}_2$ of H_1. Hence J_2 contains the subgroup $H_2 \times \bar{H}_2$.

We now have $l(K_1) < |\bar{H}_2|$ and $\langle \bar{H}_2, K_2 \rangle \leqq \mu(J_2) = P_2^{H_2}$. The conditions (1) and (2) of Lemma 10 are all fulfilled with $K_3 = H$; and (7) now follows.

COROLLARY 11.1. *Let K_1, K_2 and K_3 be non-trivial finite groups such that $l(K_2) < |K_3|$. Then a countable group L can always be embedded in some simple group of the form $S = \langle K_1, K_2, K_3 \rangle$. In particular, L can always be embedded in some 3-generator simple group.*

This follows from Lemma 11 by taking $H = H_2 = K_3$.

2. PROOF OF THEOREM C1. Now let $K_1, \cdots, K_4$ and L be any non-trivial groups such that $|L| \leqq |K_1 * \cdots * K_4|$. We may suppose without loss of generality that $|K_1| \geqq |K_i|$ for $i = 2, 3, 4$. Then

(9) $$\left|(K_3 * K_4) \times L\right| \leq \left|K_1 * K_1\right|.$$

We have to show that L can be embedded in some simple group of the form $S = \langle K_1, \cdots, K_4 \rangle$. By (9) and Lemma 11, it will be enough to prove the existence of some group of the form $H = \langle K_3, K_4 \rangle$ which contains a finite subgroup H_2 satisfying (6).

If K_3 and K_4 are both of order 2, we may take $H = H_2$ to be a sufficiently large but finite dihedral group. If K_3 and K_4 are not both of order 2, any preassigned finite group H_2 can be embedded in some group of the form $\langle K_3, K_4 \rangle$ by Theorem A. Alternatively, since subnormal embedding is not required, we may appeal to Corollary 9.2.

This concludes the proof of Theorem C1 and therewith of the relations

(10) $$l(K) \leq 4 \quad \text{for all } K,$$

which are an immediate consequence. If we take the three groups H, K_1 and K_2 in Lemma 11 to be isomorphic, (10) gives

COROLLARY 11.2. $l(H) \leq 3$ *for every group* H *which has a finite subgroup of order greater than* 4.

The appeal to a general embedding theorem for the final step in the above proof of Theorem C1 can easily be avoided. If K_3 and K_4 are both finite, let M be the subgroup of $K_3 * K_4$ which is generated by $[K_3, K_4]'$ together with the p-th powers of all elements of $[K_3, K_4]$. Then the group $K_3 * K_4/M$ is finite and of the form $\langle K_3, K_4 \rangle$; and since K_3 and K_4 are non-trivial, its order can be made arbitrarily large by a suitable choice of p.

If at least one of K_3 and K_4 is infinite, we may use the following well known result

LEMMA. *Let* K_3^* *and* K_4^* *be the regular representations of the non-trivial groups* K_3 *and* K_4 *and suppose that* $K_3 \cap K_4 = 1$. *Then* $[K_3^*, K_4^*] = \text{Alt}(K_3 \cup K_4)$, *the group of all even permutations (of finite support) of the set* $K_3 \cup K_4$.

PROOF. Let $1 \neq x_3 \in K_3$ and $1 \neq y_4 \in K_4$. The hypothesis $K_3 \cap K_4 = 1$ and an elementary calculation then show that $[x_3^*, y_4^*]$ is the 3-cycle $(x_3, 1, y_4)$. All 3-cycles on $K_3 \cup K_4$ can be obtained from those of this special form by a succession of at most three transformations by suitable elements of K_3^* and K_4^*. Since the alternating group is generated by its 3-cycles, and $[K_3^*, K_4^*]$ by the commutators $[x_3^*, y_4^*]$, the result follows.

If at least one of K_3 and K_4 is infinite, the group $H = \langle K_3^*, K_4^* \rangle$ therefore contains alternating subgroups of every finite degree n. Hence this group H meets the requirements of the proof of Theorem C1.

3. An important part of Theorem C2, which concerns embedding in simple groups with three given subgroup generators, is already contained in Lemma 11.

The condition (6) there imposed on the group H amounts, in view of (10), to this: *H must have a finite subgroup of order greater than* 4. This allows the group J_2 of Lemma 10 to be of RP-type, as provided by Theorem B2. If, as we shall see, we take for J_2 the kind of monolithic group provided by Theorem B3, we obtain a result similar in form to Lemma 11 except that the condition becomes: *H must have an infinite cyclic subgroup*. Only a few groups fail to satisfy one or other of these two conditions:

LEMMA 12. *Let H be a periodic group with no finite subgroup of order greater than* 4. *Then $|H| \leq 4$.*

PROOF. Any two involutions t_1 and t_2 in H must commute, since otherwise $\langle t_1, t_2 \rangle$ would be a finite dihedral group of order at least 6. Hence the involutions in H, if any, generate a normal subgroup M of exponent 2. Clearly $|M| \leq 4$. Since H is periodic, $|M| = 4$ implies that $H = M$; and $|M| = 2$ implies that H/M must be of exponent 2, and so $|H| \leq 4$. If H contains no involutions, it must be of exponent 3 and therefore locally finite, by a theorem of Burnside: cf. [14], 321. Hence $|H| \leq 3$ in this case.

Once Theorem B3 has been proved and the analogue of Lemma 11 deduced from it, only a small gap will remain in the proof of Theorem C2. This gap can be bridged by using for J_2 the linear fractional group $LF(2, 41)$.

4. Let P be any group and $\mathfrak{B}$ any Boolean ring. By a classical theorem of M. H. Stone, we may assume without loss of generality that $\mathfrak{B}$ is a subring of the Boolean ring of all subsets $A, B, \cdots$ of some suitable set C; we express this by writing

$$(11) \qquad\qquad \mathfrak{B} \leq 2^C.$$

Two elements A and B of 2^C will be called *orthogonal* (in preference to disjoint) whenever $A \cap B = \varnothing$. Apart from this, we shall use set-theoretical terms and notations throughout: the sum of A and B is $(A \cap B') \cup (A' \cap B)$, where A' is the *complement* of A in C; and their product is $A \cap B$.

Given $x \in P$ and $A \leq C$, we define the vector $x_A \in \Omega = \Omega(P, C)$ by

$$(12) \qquad\qquad (x_A)_\alpha = x \text{ if } \alpha \in A; \text{ and } (x_A)_\alpha = 1 \text{ if } \alpha \in A';$$

and the *Boolean power* of P by $\mathfrak{B}$ to be the group

$$(13) \qquad\qquad \mho = \mho(P, \mathfrak{B}) = \langle x_A; x \in P, A \in \mathfrak{B} \rangle.$$

If $A \neq \varnothing$, the elements $x_A (x \in P)$ form a copy P_A of P. Since $x_\varnothing = 1$ for all x, we write $P_\varnothing = 1$. For any x, y in P and any A, B in 2^C, the relations

$$(14) \qquad\qquad x_A y_B = x_{A \cap B'}(xy)_{A \cap B} y_{A' \cap B}$$

and

(15) $$[x_A, y_B] = [x, y]_{A \cap B}$$

follow immediately from (12). Note that, if A and B are in $\mathfrak{B}$, so also are the sets $A \cap B'$, $A \cap B$ and $A' \cap B$ which appear in (14). There is an evident generalisation of (14) for a product of any finite number of factors $x_A y_B \cdots t_D$; and this shows that

(16) $$\mho(P, 2^C) = \Omega_0(P, C),$$

where $\Omega_0 = \Omega_0(P, C)$ consists of all those vectors in Ω which have only finitely many unequal coordinates. Every $w \neq 1$ in Ω_0 has a *normal form*

(17) $$w = (w_1)_{A_1}(w_2)_{A_2} \cdots (w_n)_{A_n},$$

where $w_1, \cdots, w_n$ are distinct non-trivial elements of P and $A_1, \cdots, A_n$ are mutually orthogonal non-empty subsets of C, which we shall the *constancy sets* of w. The form (17) is unique apart from the ordering of the factors.

The generalised form of (14) also gives

LEMMA 13.1. $w \in \mho = \mho(P, \mathfrak{B})$ *if and only if all the constancy sets of w belong to $\mathfrak{B}$.*

If $\mathfrak{B}$ is finitely generated, it is finite; and $|\mathfrak{B}| = 2^n$ for some n. $\mathfrak{B}$ then has a *basis* of n mutually orthogonal non-empty elements $A_1, \cdots, A_n$; and (15) shows that, in this case,

(18) $$\mho = P_{A_1} \times P_{A_2} \times \cdots \times P_{A_n}.$$

For general $\mathfrak{B}$, it follows that every finite subset of $\mho$ is contained in some direct product of the form (18). Thus Boolean powers form a natural generalisation of direct powers.

In general, Ω_0 is not normal in Ω, nor is Ω a Boolean power of P. For example, the Cartesian power $\Omega = \Omega(A, C)$ of an infinite alternating group A by an infinite set C is not even periodic; whereas all Boolean powers of a locally finite group, such as A, are locally finite.

The group $\mho = \mho(P, \mathfrak{B})$ has a simple abstract definition in terms of generators and relations. If x and y run independently through P, and A and B through all pairs of orthogonal elements of $\mathfrak{B}$, then the defining relations are

(19) $$x_A y_A = (xy)_A, \ x_A x_B = x_{A \cup B} \text{ and } [x_A, y_B] = 1.$$

We omit the proof.

More important is

LEMMA 13.2. *Let $V = \mho(P, \mathfrak{A})$, where $\mathfrak{A}$ is an ideal of $\mathfrak{B}$. Then $V \lhd \mho$; and if $\mathfrak{A}$ is a principal ideal, V is a direct factor of $\mho$.*

When P is a perfect simple group, every normal subgroup of $\mho$ has the form $V = \mho(P, \mathfrak{A})$ for some ideal $\mathfrak{A}$ of $\mathfrak{B}$; and in $\mho$ all subnormal subgroups are normal, cf. [25], Theorem 5.

PROOF. V is generated by the elements x_A $(x \in P, A \in \mathfrak{A})$, and $\mho$ is generated by the elements y_B $(y \in P, B \in \mathfrak{B})$. By (15) $y_B^{-1} x_A y_B = x_A[x, y]_{A \cap B}$; and here $A \cap B \in \mathfrak{A}$ for all $A \in \mathfrak{A}$ and $B \in \mathfrak{B}$, since $\mathfrak{A}$ is an ideal, Noting that $(y_B)^{-1} = (y^{-1})_B$ it follows that $V \lhd \mho$.

For given $A \in \mathfrak{B}$, we have $X = (A \cap X) \cup (A' \cap X)$ for all $X \in \mathfrak{B}$. The elements $A \cap X (X \in \mathfrak{B})$ form the principal ideal $\mathfrak{A} = (A)$ determined by A. The elements $A' \cap X$ $(X \in \mathfrak{B})$ form another ideal $\mathfrak{A}^*$, in general not a principal ideal since A' need not belong to $\mathfrak{B}$; and $\mathfrak{B} = \mathfrak{A} \oplus \mathfrak{A}^*$ is the direct sum of $\mathfrak{A}$ and $\mathfrak{A}^*$. The generators y_X $(y \in P, X \in \mathfrak{B})$ of $\mho$ have the form $y_X = y_{A \cap X} y_{A' \cap X}$; and the $y_{A \cap X}$ generate $V = \mho(P, \mathfrak{A})$, while the $y_{A' \cap X}$ generate $V^* = \mho(P, \mathfrak{A}^*)$. Since $\mathfrak{A} \cap \mathfrak{A}^* = (\varnothing)$, we have $V \cap V^* = 1$; and since $[y_{A \cap X}, z_{A' \cap Y}] = 1$ for all y and z in P and all X and Y in $\mathfrak{B}$, we have $[V, V^*] = 1$. Hence $\mho = V \times V^*$.

Now let P be a perfect simple group, and let $N \lhd \mho$ and $w \in N$, where w is given by (17). Here $w_i \neq 1$ and so the elements $[w_i, u]$ with $u \in P$ generate P. By Lemma 13.1, $A_i \in \mathfrak{B}$; and so $u_{A_i} \in \mho$, and $[w, u_{A_i}] \in N$ since $N \lhd \mho$. But $[w, u_{A_i}] = [w_i, u]_{A_i}$, since $A_1, \cdots, A_n$ are mutually orthogonal. It follows that $P_{A_i} \leqq N$ for each i. Since $w \in P_{A_1} \times \cdots \times P_{A_n}$, we conclude that $N = \langle P_A; A \in \mathfrak{A} \rangle$, where $\mathfrak{A}$ consists of $\varnothing$ together with all the constancy sets of the non-trivial elements of N. In (14), we may choose x and y in P such that the four elements $1, x, y$ and x^{-1} are distinct; and it follows that, if A and B are in $\mathfrak{A}$, so is their sum $(A \cap B') \cup (A' \cap B)$. Since P is perfect, (15) gives

(20) $[P_A, P_B] = P_{A \cap B}$.

Hence $A \cap B \in \mathfrak{A}$ for all $A \in \mathfrak{A}$ and $B \in \mathfrak{B}$. Thus $\mathfrak{A}$ is an ideal of $\mathfrak{B}$ and $N = \mho(P, \mathfrak{A})$.

In a Boolean ring $\mathfrak{B}$, any ideal of an ideal of $\mathfrak{B}$ is itself an ideal of $\mathfrak{B}$. It follows that, when P is a perfect simple group, every subnormal subgroup of $\mho$ is normal in $\mho$.

This concludes the proof of the lemma. It is easy to verify that, in the general case, the quotient group $\mho/V$ is isomorphic in a natural way with $\mho(P, \mathfrak{B}/\mathfrak{A})$.

5. Now let any group H be represented by ring-automorphisms η^* of the Boolean ring $\mathfrak{B}$:

(21) $\eta^* : A \to A\eta \, (A \in \mathfrak{B}, \eta \in H)$.

For any group P, we may then form the semidirect product $W = \mho H$, where $\mho = \mho(P, \mathfrak{B})$, with the transformation law

(22) $\eta^{-1} x_A \eta = x_{A\eta} \, (x \in P, A \in \mathfrak{B}, \eta \in H)$.

Since the η^* are ring-automorphisms of $\mathfrak{B}$ and $(\xi\eta)^* = \xi^*\eta^*$ for all ξ, η in H, it is clear that the relations (22) determine a representation of H by automorphisms of the group $\mathfrak{V}$. We call W the *Boolean wreath product* of P by H with respect to the representation (21).

We shall only be concerned with the *standard* case in which

$$(23) \qquad\qquad\qquad \mathfrak{B} \leqq 2^H,$$

so that the elements A of $\mathfrak{B}$ are subsets of H, and the representation (21) is the natural one for which $\xi \in A\eta$ if and only if $\xi\eta^{-1} \in A$ $(\xi, \eta \in H)$. $\mathfrak{B}$ is then an H-*invariant* subring of 2^H: a Boolean ring with the elements of H as right-hand operators.

We recall from §1.7 the definition: a subset A is of *finite index* in H whenever

$$(24) \qquad\qquad H = A\xi_1 \cup A\xi_2 \cup \cdots \cup A\xi_n$$

for some finite set of elements $\xi_1, \cdots, \xi_n$ in H. If $\mathfrak{B}$ is H-invariant and contains an element A of finite index in H, then $H \in \mathfrak{B}$, and so $\mathfrak{B}$ is a *Boolean algebra* with H as its unit element. The group of constant vectors

$$(25) \qquad\qquad\qquad \bar{P} = P_H$$

is then contained in $\mathfrak{V}$.

LEMMA 14.1. *Let P be a perfect simple group, A any subset of finite index in H and*

$$(26) \qquad\qquad \mathfrak{V}_A = \mathfrak{V}(P, \mathfrak{B}_A), \; R_A = \mathfrak{V}_A H,$$

where $\mathfrak{B}_A$ is the Boolean ring generated by all the translates $A\eta(\eta \in H)$ of A. Then

$$(27) \qquad\qquad \mathfrak{V}_A = \langle P_{A\eta}; \eta \in H \rangle \text{ and } R_A = \langle P_A, H \rangle.$$

PROOF. Let X and Y be any subsets of H. Since P is perfect, we have

$$(28) \qquad P_{X \cup Y} \leqq P_{X \cap Y'} \times P_{X \cap Y} \times P_{X' \cap Y} = \langle P_X, P_Y \rangle,$$

by (14) and (15). Assuming (24), it follows that the group $V = \langle P_{A\eta}; \eta \in H \rangle$ contains $\bar{P}$. If P_X and P_Y are both contained in V, then $P_{X \cap Y} = [P_X, P_Y] \leqq V$ and $P_{X'} \leqq V$ since $\langle P_X, \bar{P} \rangle = P_X \times P_{X'}$. But $\mathfrak{B}_A$ is a Boolean algebra and is the smallest system of subsets of H which contains all the $A\eta$ and is closed with respect to intersection and complementation in H. Hence $V = \mathfrak{V}_A = \langle P_X; X \in \mathfrak{B}_A \rangle$.

Clearly $\mathfrak{B}_A$ is H-invariant and so H normalizes $\mathfrak{V}_A$. Thus R_A is the semidirect product of $\mathfrak{V}_A$ by H. By (22),

$$(29) \qquad\qquad \eta^{-1}P_X\eta = P_{X\eta} (\eta \in H, X \leqq H).$$

Hence $\mathfrak{V}_A = (P_A)^H$ and $R_A = \langle P_A, H \rangle$.

We have chosen the notation R_A for this Boolean wreath product, in

preference to W_A, because the analogy with the standard restricted product $R = P \wr H = \langle P, H \rangle$ is particularly close. Indeed the base group of R is precisely $\mho(P, \mathfrak{B}_0)$. where $\mathfrak{B}_0$ is the ring of all finite subsets of H.

With the notation and assumptions of Lemma 14.1, we have

LEMMA 14.2. (i) *For any $\eta \in H$ and $w \in \mho_A$, the normal closure N of ηw in R_A contains η.*

(ii) *If $\xi \in H$ and is such that $A \cap A'\xi$ is of finite index in H, then $\mho_A \leqq \langle \xi^{R_A} \rangle$.*

PROOF. (i) We may suppose that $\eta \neq 1$ and $w \neq 1$. Let the normal form of w be (17). Then $A_i \in \mathfrak{B}_A$ and $P_{A_i} \leqq \mho_A$ for each $i = 1, \cdots, n$, by Lemma 13.1. Since $w_i \neq 1$ and P is a perfect simple group, we may choose u and v in P such that $[w_i, u, v] \neq 1$. Here u and v may depend on i. Writing $u_H = \bar{u}$ for any $u \in P$, we have $[\eta w, \bar{u}] = [w, \bar{u}]$, since $[H, \bar{P}] = 1$ by (22). But $\bar{P} \leqq \mho_A$ since A is of finite index in H. Hence N contains $[\eta w, \bar{u}, v_{A_i}] = [w_i, u, v]_{A_i}$, which is a non-trivial element of P_{A_i}. By Lemma 13.2, $N \cap \mho_A = \mho(P, \mathfrak{A})$ for some ideal $\mathfrak{A}$ of $\mathfrak{B}_A$. Hence $A_i \in \mathfrak{A}$ for each i, and $w \in N$. This gives $\eta \in N$ as stated.

(ii) For any $u \in P$ and $\xi \in H$, the transformation law gives

(30) $$[u_A, \xi] = u_{A \cap A'\xi}^{-1} u_{A' \cap A\xi}.$$

Here $A \cap A'\xi \in \mathfrak{B}_A$; and $[u_A, \xi] \in \langle \xi^{R_A} \rangle \cap \mho_A = \mho(P, \mathfrak{A})$ for some H-invariant ideal $\mathfrak{A}$ of $\mathfrak{B}_A$, by Lemma 13.2. Taking $u \neq 1$ in (30), it follows that $A \cap A'\xi \in \mathfrak{A}$. If ξ is such that $A \cap A'\xi$ is of finite index in H, then $\mathfrak{A}$ contains the unit element H of $\mathfrak{B}_A$; and so $\mathfrak{A} = \mathfrak{B}_A$ and $\mho_A \leqq \langle \xi^{R_A} \rangle$.

It is easy to see that, when P is a perfect simple group, $\bar{P}$ is hololophic in $\mho_A$.

6 Now let $H = \langle \tau \rangle$ be an infinite cyclic group. We wish to construct a semidirect product $J_2 = H\mu(J_2)$, where $\mu(J_2) = P_2^H$ and P_2 is a copy of a given perfect simple group P. It is also required that $[H, \bar{P}_2] = 1$ for some copy $\bar{P}_2$ of P contained in $\mu(J_2)$. If $\mu(J_2)$ is to have the form $\mho(P, \mathfrak{B})$ for some H-invariant Boolean ring $\mathfrak{B}$, then $\mathfrak{B}$ must be countably infinite and characteristically-simple since it must have no H-invariant ideals distinct from itself and the zero ideal. To within isomorphism, only three such rings $\mathfrak{B}$ exist; we may take them to be

$\mathfrak{B}_0$, the system of all finite subsets of H, which makes $\mho(P, \mathfrak{B}_0)$ the direct product of $\aleph_0$ copies of H, and leads to the restricted wreath product $P \wr H$;

$\mathfrak{B}_1$, the free Boolean ring with $\aleph_0$ generators, which like $\mathfrak{B}_0$ fails to have a unit element; and which is the direct sum of $\aleph_0$ ideals each isomorphic with

$\mathfrak{B}_2$, the Boolean algebra obtained by the standard process of adjoining a unit element to $\mathfrak{B}_1$.

It is necessary to have $\mu(J_2) \cong \mho(P, \mathfrak{B}_2)$. A natural definition of $\mathfrak{B}_2$ is as the $\cup$-closure of the system of all residue classes

(31) $2^r Z + n$ $(r \geqq 0, n \in Z)$,

where Z is the ring of rational integers. With $\mathfrak{B}_2$ in this form, there is a natural representation of H in which the generator τ is represented by the automorphism

(32) $\tau^* : 2^r Z + n \rightarrow 2^r Z + n + 1$.

But every element $A \neq \varnothing$ in $\mathfrak{B}_2$ is here the union, for some $r = r(A)$, of a certain number of residue classes mod 2^r; and this implies that, with the representation (32) $(P_A)^H$ is the direct product of finitely many copies of P, and so is a proper subgroup of $\mho(P, \mathfrak{B}_2)$. Hence we must choose a different representation of H or else another form for $\mathfrak{B}_2$. We shall therefore proceed indirectly.

Let Γ be the set of all integers of the form

(33) $\gamma(k, r) = (4k)!\,(r + \tfrac{1}{2})$,

where r is any integer and k any positive integer; and let A consist of the elements $a_n \in H$ $(n \in Z)$ defined by

(34) $a_n = \tau^{24n+1}$ if $n \in \Gamma$, and $a_n = \tau^{24n}$ if $n \notin \Gamma$.

Thus A nearly coincides with the subgroup $\langle \tau^{24n} \rangle$. Since $a_n^{-1} a_{n+1}$ is always one of τ^{23}, τ^{24} or τ^{25}, we have

(35) $$H = \bigcup_{i=0}^{24} A\tau^i,$$

so that A is of finite index in H. Also

(36) $A\tau^i \cap A\tau^j = \varnothing$ if $0 < |i - j| < 23$.

Let A_k consist of those a_n for which $n = \gamma(k, r)$ for some $r \in Z$. By (33) and (34), A_k is a coset of the subgroup of index $24(4k)!$ in H. Hence A_k is of finite index in H. We shall show that

(37) $A_k \leqq A \cap A'\xi$, where $\xi = \tau^{(4k)!}$.

For suppose not. Then $a_n \xi^{-1} = \tau^m \in A$ for some $a_n \in A_k$. Here $m \equiv 1 \bmod 24$, and hence $\tau^m \in A_l$ for some l, by (34). Hence we obtain a relation of the form

$$24\gamma(k, r) - (4k)! = 24\gamma(l, s)$$

for some integers r and s. Such a relation is impossible. If $l \geqq k$, it would make an odd multiple of $(4k)!$ equal to an even multiple; and if $l < k$, it would make an even multiple of $12(4l)!$ equal to an odd multiple. These contradictions prove (37).

Now let $\mathfrak{B}_A$, $\mho_A$ and R_A be defined as in Lemma 14.1, but with $H = \langle \tau \rangle$ and A given by (34). As before, P is any perfect simple group. Since A is of finite index in H, we may use Lemmas 14.1 and 14.2 and obtain

LEMMA 14.3. *Let* $N \lhd R_A$. *Then either* $\mho_A \leqq N$ *or else* $N \leqq \mho_A$

PROOF. Suppose that $N \nleqq \mathfrak{V}_A$. Then $\eta w \in N$ for some $\eta \neq 1$ in H and some $w \in \mathfrak{V}_A$. Then $\eta \in N$ by the first part of Lemma 14.2. For a sufficiently large value of k, the element ξ in (37) is a power of η. Since A_k is of finite index in H, so also is $A \cap A'\xi$ by (37). Hence $\mathfrak{V}_A \leqq \langle \xi^{R_A} \rangle \leqq N$, by the second part of Lemma 14.2. Lemma 14.3 now follows.

Now let N be any normal subgroup of R_A which is maximal subject to the condition $N \cap \bar{P} = 1$. The lemma shows that $N < \mathfrak{V}_A$, and $\mathfrak{V}_A/N$ is a chief factor of R_A. If we define

$$(38) \qquad J_2 = R_A/N, \quad P_2 = NP/_A N \text{ and } \bar{P}_2 = N\bar{P}/N,$$

it now follows that J_2 is monolithic, with $\mu(J_2) = \mathfrak{V}_A/N$. $N \cap P_A \neq 1$ would imply that $P_A \leqq N$ and hence $\mathfrak{V}_A \leqq N$ by (27). Since this is not the case, it follows that P_2, and similarly $\bar{P}_2$, are copies of P. We may identify H with NH/N to obtain $[H, \bar{P}_2] = 1$. The relation $\mu(J_2) = P_2^H$ then also follows from (27).

7. PROOF OF THEOREM B3. We are given groups $K \neq 1$ and L such that $|L| \leqq |K * K|$. We have to fit K and L into the group R_A considered in the preceding section by making a special choice of the perfect simple group P. By (10), we may suppose that

$$(39) \qquad L \leqq P = \langle K_1, \cdots, K_4 \rangle$$

where $K_1, \cdots, K_4$ are four copies of K. We may further suppose, by Lemma 4 that P contains a commutator

$$(40) \qquad c = [b_1^{(1)}, b_2^{(2)}, b_3^{(3)}, b_4^{(4)}] \neq 1,$$

where $b^{(1)}, \cdots, b^{(4)}$ are suitable elements of K.

For each $y \in K$, let y^* be the vector in $\mathfrak{V}_A$ defined by

$$(41) \qquad y^* = (y_1)_A (y_2)_{A\tau} (y_3)_{A\tau 3} (y_4)_{A\tau 7}.$$

By (36), the sets $A, A\tau, A\tau^3$ and $A\tau^7$ are orthogonal in pairs, and so the vectors y^* form a copy K^* of K which is contained in $\mathfrak{V}_A$. If $y \neq 1$, we have

$$[y^*, P_A] = [y_1, P]_A = P_A,$$

since y_1 is then a nontrivial element of P. Since $P_A \cap N = 1$, it follows that

$$(42) \qquad K^* \cap N = 1.$$

The common support of the vectors $y^* \neq 1$ of K^* is the set

$$(43) \qquad B = A \cup A\tau \cup A\tau^3 \cup A\tau^7.$$

Let $A^* = B \cap B\tau^{-1} \cap B\tau^{-3} \cap B\tau^{-7}$. Clearly $A \leqq A^*$. But A^* is the union of the 256 sets of the form $X = A\tau^\alpha \cap A\tau^{\beta-1} \cap A\tau^{\gamma-3} \cap A\tau^{\delta-7}$, where $\alpha, \beta, \gamma, \delta$ take

independently the values $0, 1, 3$ and 7. If either $\alpha = 0$ or $\beta = 1$, then $X \leq A$. But if both $\alpha \neq 0$ and $\beta \neq 1$, then $A\tau^\alpha$ is one of $A\tau$, $A\tau^3$ or $A\tau^7$, while $A\tau^{\beta-1}$ is one of $A\tau^{-1}$, $A\tau^2$ or $A\tau^6$. By (36), $X = \varnothing$ in all these cases. Hence $A^* \leq A$, and so we have

$$(44) \qquad A = B \cap B\tau^{-1} \cap B\tau^{-3} \cap B\tau^{-7}.$$

This shows that the support of the vector

$c^* = [b^{(1)^*}, \tau b^{(2)^*} \tau^{-1}, \tau^3 b^{(3)^*} \tau^{-3}, \tau^7 b^{(4)^*} \tau^{-7}]$ is contained in A. By (41), each of the four components of c^* is constant on A; and we have in fact $c^* = c_A$, using (40). Since $c \neq 1$, this shows that

$$(45) \qquad P_A \cap (K^*)^H \neq 1.$$

An argument similar to the proof of Lemma 2.3 shows that $P_A \cap (K^*)^H \lhd P_A$. For, by (39) and (41), given $u \in P$, the group $\langle K^*, \tau K^* \tau^{-1}, \tau^3 K^* \tau^{-3}, \tau^7 K^* \tau^{-7}\rangle$ contains a vector $v = v(u)$ such that $v_\alpha = u$ for all $\alpha \in A$. Since P_A is simple, we therefore have $P_A \leq (K^*)^H$; and so

$$(46) \qquad \mho_A = (K^*)^H, R_A = \langle H, K^* \rangle.$$

By (42), we may identify K with the isomorphic subgroup NK^*/N of $\mu(J_2)$ and obtain $\mu(J_2) = K^H$. Since L is embedded in P by (39), this completes the proof of Theorem B3.

Theorem B3 may be extended to cover other infinite groups H besides Z_∞. For example, if H is *oligolithic* i.e. has a finite set of elements $\xi_i \neq 1$ such that $1 \neq M \lhd H$ always implies that $\xi_i \in M$ for some i, then we may give these ξ_i the role of the elements $\xi = \tau^{(4k)!}$ in the above proof, and use Lemma 3.5 to provide a suitable subset A.

8. PROOF OF THEOREM C2. We begin by deducing the theorem from Lemma 11 (in which we take $H = K_3$) and the two parts of the following lemma, which will then remain to be proved:

LEMMA 15. *Let K_1, K_2, K_3 and L be any non-trivial groups; and suppose that either (i) K_3 is non-periodic and $|L \times K_3| \leq |K_1 * K_1|$, or else (ii) max $(|K_2|, |K_3|)$ is 3 or 4 and $|L| \leq |K_1 * K_1|$. Then L can be embedded in some simple group of the form $S = \langle K_1, K_2, K_3 \rangle$.*

We recall the hypothesis of Theorem C2. K_1, K_2, K_3 and L are non-trivial, as in Lemma 15 and (with $H = K_3$) in Lemma 11, and the desired conclusion is the same as in both lemmas; but in the theorem we are given only that

$$(47) \qquad |L| \leq \aleph_\alpha = |K_1 * K_2 * K_3|,$$

that not all three K_i are of order 2, and that when $\alpha > 0$ at most one K_i is of order 2.

If $\alpha > 0$, we may suppose $|K_1| = \aleph_\alpha$; and if $\alpha = 0$, we may suppose that $|K_1| \leqq \max (|K_2|, |K_3|)$, without loss of generality. This ensures that $|L \times K_3| \leqq |K_1 * K_1|$ and the hypothesis of the theorem ensures that $\max (|K_2|, |K_3|) > 2$.

Suppose first that $\max (|K_2|, |K_3|) \leqq 4$. The result then follows from Lemma 15 (ii). In the contrary case we may suppose that $|K_3| > 4$. By Lemma 12, K_3 is either non-periodic and the result follows from Lemma 15 (i); or else K_3 has a finite subgroup of order greater than 4, and the result follows from Lemma 11 (with $H = K_3$), since $l(K_2) \leqq 4$ by (10).

This completes the deduction of Theorem C2.

We now prove the first part of Lemma 15. By Theorem B3, there is a group of the form $J_2 = \langle H_2, K_2 \rangle$, where H_2 is an infinite cyclic group, with the following properties: (i) J_2 is the semidirect product $H_2 \mu(J_2)$); (ii) $\mu(J_2) = P_2^{H_2}$ where P_2 is a perfect simple group which may be supposed to contain a finite subgroup of order greater than 4; and (iii) $\mu(J_2)$ contains K_2 and also a copy $\bar{P}_2$ of P_2 such that $[H_2, \bar{P}_2] = 1$. Hence $\bar{P}_2$ has a finite subgroup $\bar{H}_2$ such that $l(K_1) < |\bar{H}_2|$, using (10); and J_2 contains the subgroup $H_2 \times \bar{H}_2$. Since $\langle \bar{H}_2, K_2 \rangle \leqq \mu(J_2)$, all the conditions (2) of Lemma 10 hold. Also H_2 can be embedded in K_3, since K_3 is non-periodic, by hypothesis. Lemma 15 (i) now follows from Lemma 10.

9. It only remains to prove Lemma 15 (ii); and again we use Lemma 10, but now with

(48) $$J_2 = LF(2, 41) = PSL(2, 41).$$

We note first the needful properties of J_2, for which cf. [15], particularly Theorems 6.13, 8.5 and 8.27; or the account in [19], Chapter 20.

(a) J_2 is simple and of order $2pqr$, where $p = 41$, $q = 20$, $r = 21$.

(b) J_2 has cyclic subgroups P, Q, R of orders p, q, r respectively.

(c) Each non-trivial element of J_2 lies in exactly one conjugate of one of P, Q or R.

(d) The normalizers of Q and R in J_2 are dihedral groups of orders $p - 1$ and $p + 1$, and they are maximal subgroups of J_2.

(e) J_2 is generated by any two distinct conjugates of P.

(f) Any two non-trivial cyclic subgroups of the same order are conjugate in J_2 (a corollary of (c)).

Let the elements σ and τ of J_2 be defined by $z\sigma = z + 1$ and $z\tau = -1/z$, for any point z on the projective line of $p + 1$ points. Then σ is of order p and we may take $P = \langle \sigma \rangle$. The involution τ maps the unique fixed point ∞ of P onto 0. Hence τ does not normalize P, and so

(49) $$J_2 = \langle \sigma, \tau \rangle,$$

by (e): cf. [16], 93.

To deduce Lemma 15 (ii) from Lemma 10, we may suppose without loss of generality that $|K_2| \geqq |K_3|$. Hence $|K_2|$ is 3 or 4. To satisfy (2), we have two alternative choices for the subgroup $H_2 \times \bar{H}_2$ of J_2: either as a subgroup of Q with $|H_2| = 2$ and $|\bar{H}_2| = 5$, or else as a subgroup of R with $|H_2| = 3$ and $|\bar{H}_2| = 7$. We require H_2 to be embeddable in K_3; and so if $|K_3|$ is 2 or 4, we must choose the first alternative; while if $|K_3| = 3$, we must choose the second. In either case, we have $l(K_1) \leqq 4 < |\bar{H}_2|$, by (10).

It only remains to show that J_2 has the form $\langle H_2, K_2 \rangle$ with a suitable choice of K_2 for each of the six possible combinations of $|H_2| = 2$ or 3 and $|K_2| = 3$ or 4. Since $J_2 = \mu(J_2)$ by (a), all the conditions of Lemma 10 will then hold, and Lemma 15 (ii) will follow. Writing Z_n for the cyclic group of order n and D_n for the dihedral group of order n, we need only verify

LEMMA 16. *The group* $J_2 = LF(2, 41)$ *is of the six forms* $\langle Z_2, Z_3 \rangle$, $\langle Z_3, Z_3 \rangle$, $\langle Z_2, Z_4 \rangle$, $\langle Z_2, D_4 \rangle$, $\langle Z_3, Z_4 \rangle$ *and* $\langle Z_3, D_4 \rangle$.

PROOF. By (49), we have

$$J_2 = \langle \tau, \tau\sigma \rangle = \langle \sigma\tau, \tau\sigma \rangle = \langle \tau\sigma^{17}, \tau \rangle.$$

Here τ is of order 2, $\tau\sigma$ and $\sigma\tau$ are of order 3 and, as follows easily from $17^2 \equiv 2$ mod 41, $\tau\sigma^{17}$ is of order 4. This gives the first three forms of the lemma.

By (d), the normalizer of Q in J_2 is a D_{40}, which contains subgroup D_4; and by (f), all involutions in J_2 are conjugate. Hence the last two forms of the lemma may be obtained from the first by choosing a Z_4 or a D_4 which contains τ. Finally, let the involutions τ_1 and τ_2 generate the normalizer D_{42} of R. By (f), J_2 contains a D_4 of the form $\langle \tau_2, \tau_3 \rangle$. By (d), D_{42} is a maximal subgroup of J_2, and cannot contain $\langle \tau_2, \tau_3 \rangle$. Hence $J_2 = \langle \tau_1, \tau_2, \tau_3 \rangle$ has the form $\langle Z_2, D_4 \rangle$.

This completes the proof of Lemma 16, and therewith of Lemma 15 (ii) and of Theorem C2. We note the corollary of Theorem C2:

(50) $l(K) \leqq 3$ if $|K| \neq 2$.

5. Simple groups generated by two given finite groups

1. In the remarkable paper [17] of 1953, Camm proved the existence of $2^{\aleph_0}$ non-isomorphic 2-generator simple groups. Each of her groups is the free product with an amalgamated subgroup of two copies of the free group of rank 2, and is torsion-free. We confine our attention here to simple groups of the form $S = \langle H, K \rangle$, where H and K are given finite groups with $|H| > 2$ and $|K| > 1$; and to the question whether every countable group L can be embedded in some such S. We shall obtain a positive answer to this question for many such pairs H and K, and this implies the existence of $2^{\aleph_0}$ non-isomorphic simple groups

$S = \langle H, K \rangle$, since a given S has only countably many finitely generated subgroups. But in every case, at least one of the groups H and K has to be non-cyclic monolithic, so that our simple groups — unlike those of Camm — all appear to require at least 3 generators.

The reason for this is the character of the quadrilateral construction of §3.3 and the bilateral construction of §4.1. In the notations of those sections, we obtain simple groups of the forms

(1) $S = \langle J_1, J_3 \rangle$ and $S = \langle K_1, J_2 \rangle$.

In the first of these, J_1 and J_3 are opposite sides of a quadrilateral which has to be completed by sides J_2 and $J_4 = J_4(L)$, the given countable group L being embedded in J_4, while J_2 can be chosen independently of L. In the second form, the side $J_1 = J_1(L)$ of the bilateral has to contain both K_1 and L, but here K_1 can be any non-trivial finite group. But the J_2 of the second form is subject to more stringent requirements than the J_1 and J_3 of the first form.

The monolithic groups required to complete these constructions, viz. J_2 and $J_4(L)$ in the first form and $J_1(L)$ in the second, are in the main those of RP-type provided by Theorem B2. Obviously, an appeal to Theorem B3 would allow more general results to be obtained. It seems more interesting to show that the sides of RP-type can often be replaced by finite simple groups: cf. the role of $LF(2,41)$ in the proof of Theorem C2.

2. For this purpose, alternating groups are adequate, as is shown by

THEOREM D1. *Let H and K be finite groups which have subgroups $H_1 \leqq H$ and $K_1 \leqq K$ such that*

(2) $|H_1| = m > 2$ and $|K_1| = n > 1$;

and let A_q be the alternating group of degree q. Then for infinitely many values of q there are embeddings of H and K in A_q such that

(3) $H \cap K = 1$ *and* $\langle H_1, K_1 \rangle = A_q$.

Given a finite group L, there is a least integer $q_0 = q_0(L)$ such that A_q contains copies of L for all $q \geq q_0$. It follows from the theorem that L can always be embedded in some finite simple group A_q of the form $\langle H, K \rangle$.

PROOF. Without loss of generality, we may suppose that H_1 and K_1 are chosen as small as possible, consistently with (2). Interchanging H and K if necessary, we may therefore assume that either

(4) $H_1 = \langle s_1, s_2 \rangle \cong D_4$, $K_1 = \langle t \rangle \cong Z_2$, $m = 4$ and $n = 2$;

or else

(4)* $H_1 = \langle s \rangle$ and $K_1 = \langle t \rangle$ and $m \geqq n$.

Let

(5) $$q = 1 + (m + n - 2)r, \text{ where } r = 2|H \times K|l,$$

and l is a positive integer. By a theorem of Dirichlet, we may suppose that

(6) $$q \text{ is a prime,}$$

since this is the case for infinitely many values of l.

It will be enough to show that H_1 and K_1 can be embedded in A_q, each in its r-fold regular representation in such a way that $A_q = \langle H_1, K_1 \rangle$. For by (5), r is an even multiple of $|H|$ and so the embedding of H_1 can be extended to an embedding of H in A_q in its $2lm|K|$-fold regular representation, with the same support as that of H_1. This support consists of rm symbols and no $x \neq 1$ in H will fix any of them. Similarly, the embedding of K_1 can be extended to an embedding of K in A_q in its $2ln|H|$-fold regular representation, with the same support as that of K_1. This support consists of rn symbols and no $y \neq 1$ in K will fix any of these. The supports of H_1 and K_1 cannot be the same since r does not divide q, and so the relation $H \cap K = 1$ is assured.

Four cases need to be distinguished.

(i) Suppose that (4) holds. We take the $q = 4r + 1$ symbols permuted by A_q to be a_i, b_i, c_i, d_i $(i = 1, \cdots, r)$ together with d_0, and represent H_1 and K_1 as follows:

(7) $$s_1 = \prod_{i=1}^{r} (a_i, b_i)(c_i, d_i); \quad s_2 = \prod_{i=1}^{r} (a_i, c_i)(b_i, d_i); \quad t = \prod_{i=1}^{r} (a_i, d_{i-1}).$$

This makes $\langle H_1, K_1 \rangle$ transitive on the q symbols. By (6), it is therefore a primitive permutation group. It is easy to verify that $s_1 t$ consists of $r - 1$ cycles of order 4 and one cycle each of orders 2 and 3; and more precisely that $(s_1 t)^4$ is the 3-cycle (d_0, a_1, b_1). By a well known theorem it follows that $A_q = \langle H_1, K_1 \rangle$: cf. [18], Theorem 13.3; or [19], §160.

In the remaining three cases (4)* holds, so that H_1 and K_1 are cyclic.

(ii) Let $m > 3$ and $n > 2$. Then we take

(8) $$s = \prod_{i=1}^{r} (a_i, b_i, c_i, d_i, X_i) \text{ and } t = \prod_{i=1}^{r} (a_{i-1}, b_i, e_i, Y_i).$$

Here X_i stands for a sequence (empty when $m = 4$) of $m - 4$ symbols, and Y_i for a sequence of $n - 3$ symbols which do not enter into the calculations. It is to be understood that the symbols involved are all distinct unless the contrary is explicitly indicated. It follows that $\langle s, t \rangle = \langle H_1, K_1 \rangle$ is again a primitive permutation group permuting the $q = 1 + (m + n - 2)r$ symbols transitively, and contained in the alternating group A_q on these symbols. Writing $c_0 = a_0$ for convenience, we have

$$s^{-2}ts^2 = \prod_{i=1}^{r} (c_{i-1}, d_i, e_i, Y_i).$$

An easy calculation shows that $[t, s^2]$ consists of $r - 1$ cycles of order 5 and a single cycle of order 3; more precisely, $[t, s^2]^5$ is the 3-cycle (b_1, e_1, d_1). Hence $\langle H_1, K_1 \rangle = A_q$ for the same reason as in case (i).

(iii) Next let $m > n = 2$. Then we take

(9) $$s = \prod_{i=1}^{r} (a_{i+1}, b_i, c_i, X_i) \quad \text{and } t = \prod_{i=1}^{r} (a_i, b_i),$$

using the same convention as in the previous case. X_i is now a sequence of $m - 3$ symbols. Here $\langle s, t \rangle$ is a primitive group of degree $q = 1 + mr$. It is easy to check that $[t, s]$ consists of $r - 2$ cycles of order 3 and one cycle each of orders 2 and 4. Writing $u = [t, s]^6$, we have in fact $u = (a_1, b_1)(c_1, c_2)$, so that $sus^{-1} = (a_1, a_2)$ (b_1, b_2). This gives $v = [u, s^{-1}]^2 = (a_1, b_1)(a_2, b_2)$. Hence $\langle H_1, K_1 \rangle$ contains the transitive subgroup $\langle sus^{-1}, v \rangle$ of order and degree 4. By a theorem of Marggraff, it follows that $\langle H_1, K_1 \rangle$ coincides with the alternating group A_q on the q symbols of its support: cf. [18], Theorems 13.4 and 13.5.

(iv) It only remains to consider the case $m = n = 3$. Here $q = 4r + 1$ and we take the support of A_q to be the same as in case (i), and

(10) $$s = \prod_{i=1}^{r} (a_i, b_i, d_i), \quad t = \prod_{i=1}^{r} (a_i, c_i, d_{i-1}).$$

Then $s^t t^{-s}$ has $r - 2$ cycles of order 3 and 4 cycles of order 2. More precisely, writing $u = (s^t t^{-s})^3$, we have $u = (c_1, d_0)(a_1, c_2)(a_r, b_{r-1})(b_r, d_r)$. This gives $[u, s] = (a_1, b_1, c_2)(d_{r-1}, b_r, a_r, b_{r-1}, d_r)$. Hence the primitive group $\langle H_1, K_1 \rangle$ of degree q contains the 3-cycle $[s, u]^5 = (a_1, b_1, c_2)$. As in cases (i) and (ii), this implies that $\langle H_1, K_1 \rangle = A_q$.

The proof of Theorem D1 is now complete.

3. We give next an elementary proof of Theorem B2 for the important case of finite H, which will prepare the way for a useful though marginal improvement. It is probable that the hypothesis $l(K) < |H|$ of that theorem could be weakened to $l(K) \leqq |H|$. By (10) and (50) of §4, we know that $l(K) \leqq 3$ if $|K| > 2$ and $l(K) \leqq 4$ if $|K| = 2$; but the interesting cases $|H| = 4$, $|K| = 2$ and $|H| = 3$, $|K| > 2$ remain to be covered.

LEMMA 17. *Let H and K be non-trivial groups such that $|H| = n$ is finite; and let*

(11) $$P = \langle K_1, \cdots, K_m \rangle \text{ and } R = P \wr H,$$

where P is a perfect simple group which is generated by m copies K_i of K. Then

K can be embedded in P^H in such a way that $R = \langle H, K \rangle$ provided that one of the following conditions holds: (i) $m < n$; or (ii) $m = n$, but no automorphism of P induces a non-trivial regular permutation of degree m on the m groups $K_1, \cdots, K_m$.

PROOF. Let $G = H * K$. Then $F = K^H$ is the free product of the n conjugates $K^\zeta (\zeta \in H)$. Since $m \leq n$ in both cases, there is a homomorphism θ of F onto P. Let M be the kernel of θ and $N = \cap_{\zeta \in H} M^\zeta$. Then $M \lhd F$ and so $N \lhd G = FH$.

For each ζ, F/M^ζ is isomorphic with the perfect simple group P. Hence F/N is the direct product of r copies of P, where r is the smallest number of conjugates M^ζ of M which have N as their intersection. Since the direct product of r copies of P has exactly r maximal proper normal subgroups, it follows that $r = |G : N_G(M)|$ is the total number of conjugates of M in G. If $r = n$, then G/N is isomorphic with R in an obvious way; and it will have the form $\langle H, K \rangle$ provided that $M \cap K^\zeta = 1$ for at least one $\zeta \in H$, since $G = \langle H, K^\zeta \rangle$. Thus we have only to show that, in each of the two cases, θ can be so chosen as to map at least one of the conjugates K^ζ isomorphically into P and to make $r = n$.

In case (i), we have a spare conjugate of K and can afford to make $K^\theta = 1$. Let θ map each of the other $n - 1$ conjugates $K^\zeta (1 \neq \zeta \in H)$ isomorphically onto one of the groups $K_1, \cdots, K_m$, taking care that each K_i is the image under θ of at least one K^ζ. Then K^ζ will be the only one of the n conjugates of K under H to be contained in M^ζ. Hence the $M^\zeta (\zeta \in M)$ are all distinct and $r = n$.

In case (ii), where $m = n$, we may number the elements of H as $\xi_i (i = 1, \cdots, n)$. Let θ map K^{ξ_i} isomorphically onto K_i for each i. Suppose if possible that $r < n$. Then $M^\eta = M$ for some $\eta \neq 1$ in H. The inverse image of K_i under θ is MK^{ξ_i}, and $\theta^{-1}\eta\theta$ is an automorphism of P which maps K_i isomorphically onto $K_{j(i)}$, where the non-trivial regular permutation $i \to j(i)$ of $1, 2, \cdots, n$ is determined by the relations $\xi_i\eta = \xi_{j(i)}$. The existence of such an automorphism is contrary to hypothesis, and we conclude that $r = n$ in this case also.

This concludes the proof of the lemma.

Let L be any group such that $|L| \leq |K * K|$. Then we may choose P so that $L \leq P$ and $m = l(K)$. If $l(K) < |H| = n$, case (i) of Lemma 17 gives Theorem B2 for finite H.

If $|H| = 4$ and $P = \langle K_1, \cdots, K_4 \rangle$, a regular permutation of order 2 of the K_i must either interchange $\langle K_1, K_2 \rangle$ with $\langle K_3, K_4 \rangle$, or else $\langle K_2, K_3 \rangle$ with $\langle K_1, K_4 \rangle$, or possibly both. Case (ii) of Lemma 17 will therefore certainly apply whenever

(12) $\langle K_1, K_2 \rangle \not\cong \langle K_3, K_4 \rangle$ and $\langle K_2, K_3 \rangle \not\cong \langle K_1, K_4 \rangle$.

If $|H| = 3$ and $P = \langle K_1, K_2, K_3 \rangle$, the lemma will apply for a similar reason whenever

(13) $\langle K_1, K_2 \rangle \not\cong \langle K_2, K_3 \rangle$.

These remarks will be used in the proof of the following result, which supplements Theorem B2:

LEMMA 18. *Let L be any countable group; and let H and K be finite groups such that either (i) $|H| = 3$ and $|K| > 2$, or else (ii) $|H| = 4$ and $|K| = 2$. Then there is a perfect simple group P which contains L, and an embedding of K in the base group P^H of $R = P \wr H$ such that $R = \langle H, K \rangle$.*

PROOF OF CASE (i). Here we use the bilateral construction. Let G be any finite group with $|G| > 3$. Then $l(K) < |G|$ by §4, (50), since $|K| > 2$. By Theorem B2, we can embed L in a perfect simple group P_1 which is generated by 3 copies of K in such a way that $J_1 = P_1 \wr G$ has the form $\langle G, K_1 \rangle$, where $K \cong K_1 \leq P_1^G$. There will then be another copy $\bar{K}_1$ of K, contained in the group $\bar{P}_1$ of constant vectors in P_1^G. Hence J_1 contains the subgroup $G \times \bar{K}_1$.

By Theorem D1, there is a finite alternating group $J_2 = \langle K_2, K_3 \rangle$, where K_2 and K_3 are two further copies of K, such that J_2 contains a subgroup $K_2 \times \bar{G}$, with $\bar{G} \cong G$. For the degree q of J_2 infinitely many values are available. Hence we may suppose that J_2 is not isomorphic with the subgroup $\langle K_1, \bar{K}_1 \rangle$ of J_1.

We now form the bilateral group $J_1 * J_2/G = \bar{G}$, $\bar{K}_1 = K_2$, Since $\bar{K}_1 \leq \mu(J_1)$ $= P_1^G, J_1 = G^{J_1}$ and $J_2 = \mu(J_2)$, we have in this bilateral group the relations

$$(J_1 \cap \mu(J_2))^{J_1} = G^{J_1} = J_1 \text{ and } (J_2 \cap \mu(J_1))^{J_2} = K_2^{J_2} = J_2;$$

and so its subgroups J_1 and J_2 are hololophic by Lemma 7. Hence there is a simple quotient group of the form $P = \langle J_1, J_2 \rangle = \langle K_1, K_2, K_3 \rangle$. By our choice of q,

$$\langle K_1, K_2 \rangle = \langle K_1, \bar{K}_1 \rangle \ncong J_2 = \langle K_2, K_3 \rangle,$$

so that (13) holds. Hence case (i) of Lemma 18 follows from case (ii) of Lemma 17.

4. For economy, we combine the proof of Lemma 18 (ii) with that of the following theorem, which employs the quadrilateral construction:

THEOREM D2. *Let L be any countable group, and let J_1 and J_3 be finite groups with subgroups $H_i, \bar{H}_i (i = 1, 3)$ such that*

(14) $1 \neq \bar{H}_i \leq \mu(J_i), H_i \cap \bar{H}_i = 1 \text{ and } J_i = H_i^{J_i} (i = 1, 3).$

Suppose further that $\bar{H}_1$ and H_3 are not both of order 2, and that either

(15) $l(H_1) < |\bar{H}_3|; \text{ or } |\bar{H}_3| = 3, |H_1| > 2; \text{ or } |\bar{H}_3| = 4, |H_1| = 2.$

Then L can always be embedded in some simple group of the form

(16) $S = \langle J_1, J_3 \rangle.$

Obviously (14) implies that $H_1 \neq 1$ and $H_3 \neq 1$. The second and third alternatives in (15) correspond to the two parts of Lemma 18. We shall first prove the

theorem under the assumption of the first or the second alternative in (15). We can then prove Lemma 18 (ii) and this will allow the proof of Theorem D2 to be completed.

PROOF. Let H_2, $\bar{H}_2$, H_4 and $\bar{H}_4$ be copies of $\bar{H}_1$, H_3, $\bar{H}_3$ and H_1, respectively. If $l(H_1) < |\bar{H}_3|$, then $l(\bar{H}_4) < |H_4|$; and so, by Theorem B2, there is a perfect simple group P_4 such that $J_4 = P_4 \wr H_4$ has the following properties:

$$(17) \qquad\qquad L \leqq P_4, \ \bar{H}_4 \leqq \mu(J_4) \text{ and } J_4 = \langle H_4, \bar{H}_4 \rangle.$$

Alternatively, if $|\bar{H}_3| = 3$ and $|H_1| > 2$, then $|H_4| = 3$ and $|\bar{H}_4| > 2$; and so (17) holds for a suitable P_4 by Lemma 18 (i) which has already been proved. In both cases, $H_4 \cap \bar{H}_4 = 1$ and $J_4 = H_4^{J_4}$.

By hypothesis, $\bar{H}_1$ and H_3 are not both of order 2. By Theorem D1, there is therefore an alternating group of the form $J_2 = \langle H_2, \bar{H}_2 \rangle$ with $H_2 \cap \bar{H}_2 = 1$; and $J_2 = \mu(J_2)$. We may now complete the quadrilateral to form the group

$$G = J_1 * J_2 * J_3 * J_4 \,/\, \bar{H}_1 = H_2, \ \bar{H}_2 = H_3, \ \bar{H}_3 = H_4, \ \bar{H}_4 = H_1.$$

By (14) and (17), we then have $(J_i \cap \mu(J_{i-1}))^{J_i} = J_i$ for each i mod 4; and so the J_i are hololophic in G by Lemma 7. Hence L is embedded, as a subgroup of J_4, in a simple quotient group of G of the form $S = \langle J_1, \cdots, J_4 \rangle$. But $J_2 = \langle H_2, \bar{H}_2 \rangle = \langle \bar{H}_1, H_3 \rangle$ and $J_4 = \langle H_4, \bar{H}_4 \rangle = \langle \bar{H}_3, H_1 \rangle$ are both contained in $\langle J_1, J_3 \rangle$, and (16) now follows.

This proves Theorem D2 under the first two alternatives in (15). Under the third alternative, $|\bar{H}_3| = 4$ and $|H_1| = 2$, i.e. $|H_4| = 4$ and $|\bar{H}_4| = 2$; and the existence of a suitable P_4 satisfying (17) will follow, once case (ii) of Lemma 18 has been proved. The remaining part of the proof of the theorem can then proceed exactly as under the first two alternatives. Thus it only remains to prove Lemma Lemma 18 (ii); and by Lemma 17, it will be enough to show that *a countable group L can always be embedded in some perfect simple group P which is generated by four involutions* $\tau_1, \cdots, \tau_4$ *such that*

$$(18) \qquad\qquad \langle \tau_1, \tau_2 \rangle \ncong \langle \tau_3, \tau_4 \rangle \text{ and } \langle \tau_2, \tau_3 \rangle \ncong \langle \tau_1, \tau_4 \rangle;$$

cf. (12) above.

To prove this, let $J_1 = \langle \sigma_1, \sigma_2 \rangle$ and $J_3 = \langle \sigma_3, \sigma_4 \rangle$ be dihedral groups of orders 10 and 14, the σ_i being involutions. Thus $\xi = \sigma_1 \sigma_2$ is of order 5 and $\eta = \sigma_3 \sigma_4$ of order 7. Taking $H_1 = \langle \sigma_1 \rangle$, $H_3 = \langle \sigma_3 \rangle$, $\bar{H}_1 = \langle \xi \rangle = \mu(J_1)$ and $\bar{H}_3 = \langle \eta \rangle = \mu(J_2)$, the conditions of Theorem D2 hold. We are under the first alternative in (15), since $l(H_1) \leqq 4 < |\bar{H}_3| = 7$. Hence L can be embedded in a simple group of the form $S_1 = \langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle$ with $J_1 = \langle \sigma_1, \sigma_2 \rangle \ncong \langle \sigma_3, \sigma_4 \rangle = J_3$. But we have no information about the subgroups $\langle \sigma_2, \sigma_3 \rangle$ and $\langle \sigma_1, \sigma_4 \rangle$ of S_1, except that they are necessarily dihedral. We use S_1 as the starting point of a bilateral construction.

Let $T_1 = \langle \tau_2, \tau_4 \rangle$ be a copy of J_3, where τ_2 and τ_4 are involutions and $\zeta = \tau_2 \tau_4$ is of order 7; and let $G_1 = S_1 \wr T_1$. By Theorem B2, there is an involution $\tau_1 \in S_1^{T_1}$ such that $G_1 = \langle T_1, \tau_1 \rangle$. To be precise, we may take the support A of the vector τ_1 to consist of the elements $1, \zeta, \zeta^2$ and ζ^3 of T_1, the corresponding coordinates of τ_1 being $\sigma_1, \sigma_3, \sigma_4, \sigma_2$ respectively. Since $1 \neq [\sigma_1, \sigma_2] = [\tau_1, \zeta^3 \tau_1 \zeta^{-3}]$ is a non-trivial element of $S_1 \cap \langle \tau_1^{T_1} \rangle$, we obtain the relation $G = \langle T_1, \tau_1 \rangle$ in the usual way. Since $A \leqq \langle \zeta \rangle$, $A\tau_2 \cap A = A\tau_4 \cap A = \varnothing$; here $A\tau_2 = \mathrm{Sup}\ \tau_1^{\tau_2}$ and $A\tau_4 = \mathrm{Sup}\ \tau_1^{\tau_4}$. Hence $[\tau_1, \tau_1^{\tau_2}] = [\tau_1, \tau_1^{\tau_4}] = 1$ and so

$$(19) \qquad\qquad\qquad \langle \tau_1, \tau_2 \rangle \cong \langle \tau_1, \tau_4 \rangle \cong D_8,$$

the octic group.

On the other hand, the group $\bar{S}_1$ of all constant vectors in the base group $S_1^{T_1}$ of G_1 contains a copy $\bar{T}_1 = \langle \bar{\sigma}_3, \bar{\sigma}_4 \rangle$ of T_1; and $\eta = \sigma_3 \sigma_4$ is the ζ-coordinate of $\tau_1 \bar{\sigma}_4$ and also the ζ^2-coordinate of $\bar{\sigma}_3 \tau_1$. Hence the dihedral groups $\langle \tau_1, \bar{\sigma}_3 \rangle$ and $\langle \tau_1, \bar{\sigma}_4 \rangle$ are of order at least 14. Note also that G_1 contains the subgroup $T_1 \times \bar{T}_1$.

Now let $G_3 = S_3 \wr T_3 = \langle T_3, \tau_3 \rangle$ be a copy of G_1, with $S_3 \cong S_1$, $T_3 \cong T_1$ and τ_3 an involution in the base group $S_3^{T_3}$. Then G_3 contains a subgroup $T_3 \times \bar{T}_3$, where $\bar{T}_3 \cong T_1$ and is contained in $S_3^{T_3} = \mu(G_3)$. Hence we may form the bilateral group

$$G = G_1 * G_3 / \bar{T}_1 = T_3, \quad \bar{T}_3 = T_1.$$

In G, $T_1 = \bar{T}_3 \leqq G_1 \cap \mu(G_3)$ and so $(G_1 \cap \mu(G_3))^{G_1} = T_1^{G_1} = G_1$; and similarly $(G_3 \cap \mu(G_1))^{G_3} = G_3$. Hence G_1 and G_3 are hololophic in G, by Lemma 7; and so G has a simple quotient group of the form $P = \langle G_1, G_3 \rangle$. Since $T_3 = \bar{T}_1 \leqq G_1$ and $G_3 = \langle T_3, \tau_3 \rangle$, it follows that $P = \langle G_1, \tau_3 \rangle = \langle \tau_1, \tau_2, \tau_3, \tau_4 \rangle$.

The subgroups $\langle \tau_2, \tau_3 \rangle$ and $\langle \tau_3, \tau_4 \rangle$ of P are contained in the base group of G_3. They are the subgroups of G_3 which correspond to the subgroups $\langle \tau_1, \bar{\sigma}_3 \rangle$ and $\langle \tau_1, \bar{\sigma}_4 \rangle$ of G_1. Hence they are of order at least 14, and so (18) follows from (19). L is embedded in P as a subgroup of $S_1 \leqq G_1$.

The proof of Lemma 18 and Theorem D2 is now complete.

5. Taking $J_1 \cong J_3$ in Theorem D2, we obtain the

COROLLARY. *Let J be a finite group with subgroups H and $\bar{H}$ such that*

$$(20) \qquad\qquad \bar{H} \leqq \mu(J), \ H \cap \bar{H} = 1 \ and \ J = H^J; \ and \ either$$

$$(21) \qquad\qquad |H| > 1, |\bar{H}| > 3, \ or \ |H| > 2, |\bar{H}| = 3.$$

Then $l(J) = 2$.

For by (50) of §4, we have $l(H) < |\bar{H}|$ whenever $|H| > 2$ and $|\bar{H}| > 3$. The remaining cases are covered by the second and third alternatives in (15).

It would be tedious to discuss the conditions (20) and (21) in detail, but a few

points may be made. They imply that J is monolithic; that J is not nilpotent i.e. is not a prime-power group with cyclic centre: that $|\mu(J)| > 2$; and that J is not one of the dihedral groups of order $2 \cdot 3^n$.

Of the 80 monolithic groups of order not exceeding 60, just 49 are nilpotent. Of the remaining 31, three have centre of order 2 $viz.$ the binary tetrahedral group of order 24, its central product with a Z_4 and the binary octahedral group — both of these being of order 48. If we exclude these three groups and also the dihedral groups of orders 6, 18 and 54, there remain 25 groups J with $|J| \leq 60$ all of which satisfy the conditions (20) and (21) for a suitable choice of H and $\bar{H}$, and for which therefore $l(J) = 2$.

Some general classes of finite groups with $l = 2$ may be noted:

(1) The simple groups of composite order. For these we may take $\bar{H}$ to be a Sylow subgroup of order greater than 4 and H to be a Sylow subgroup belonging to a different prime from $\bar{H}$.

(2) The symmetric groups of degree $q \geq 4$. If $q > 4$, we can choose $H = \langle t \rangle$ where t is a transposition and $\bar{H} = A_q$. If $q = 4$, we must take $|\bar{H}| = 4$, $|H| = 6$.

(3) The soluble monolithic groups J such that $[M, J] = M$, where $M = \mu(J)$ excluding only the dihedral groups $D_{2 \cdot 3^n}$. If H is a system normalizer of J, then $H \cap M = 1$ and $J = H^J$: cf. [15], Theorem 11.10; and the conditions (20) and (21) will be satisfied with $\bar{H} = M$ unless $|H| = 2$ and $|M| = 3$. In the latter case, the Fitting subgroup F of J must be a 3-group. Since J is soluble, we have $C_J(F) \leq F$: cf. [15], Theorem 4.2 b); and if F is cyclic, this would imply $J \cong D_{2 \cdot 3^n}$ for some n. This case being excluded it is easy to show that F contains a cyclic subgroup $M_1 \neq M$ such that $|M_1| = 3$ and $M_1^H = M_1$. With $\bar{H} = M$ as before, we may satisfy the conditions of the corollary by replacing the system normalizer H by $\langle H, M_1 \rangle \cong D_6$ or Z_6.

(4) The soluble monolithic groups J such that $[M, J] = 1$, $|M| = p > 2$ and $|J : J'|$ prime to p. Except when $|J| = 2 \cdot 3^n$ we may take H to be any $S_{p'}$-subgroup of J. Again $H \cap M = 1$ and $J = H^J$, so that $\bar{H} = M = \mu(J)$ is again a suitable choice. In the exceptional case we may take H to be one of the dihedral subgroups which J then contains.

It may be of interest to remark that $l(S) = 2$ also for all countably infinite simple groups S, except possibly when S is torsion-free and has the peculiar property that any two of its non-trivial subgroups have a non-trivial intersecion. (Whether there exist simple groups with this peculiar property is problematic.) The proof follows similar lines to that of Theorem D2, but the quadrilateral sides of RP-type may need to be supplemented by sides of $\mathcal{B}P$-type as provided by Theorem B3.

6. The other main result of §5 is similar to Theorem D2, but requires the bilateral construction. This is

THEOREM D3. *Let $K \neq 1$ and J be finite groups and let L be any countable group. Suppose that J is either (i) a simple group of composite order, or else (ii) has a direct-product subgroup $H \times \bar{H}$ such that*

(22) $$\bar{H} \trianglelefteq \mu(J), \ |\bar{H}| > 2 \text{ and } J = H^J.$$

Then L can always be embedded in some simple group of the form

(23) $$S = \langle J, K \rangle.$$

Conditions (22) imply that $H \neq 1$; and a simple group of composite order clearly satisfies them provided it has a subgroup $H \times \bar{H}$ with $|H| > 1$ and $|\bar{H}| > 2$. For example, consider the simple group $J = LF(2, p)$, where p is a prime greater than 3. J has cyclic subgroups of orders $\frac{1}{2}(p - 1)$ and $\frac{1}{2}(p + 1)$, and therefore J fails to satisfy (ii) only when one of these two numbers is a power of 2 and the other is a power of 3. The only values of p for which this occurs are the Fermat primes 5 and 17 and Mersenne prime 7. The corresponding simple groups, of orders 60, 2448 and 168, contain D_4's but no other genuine direct products.

But we do not need to examine the finite simple groups in detail. Instead we prove

LEMMA 19. *Suppose that the finite group G has no direct-product subgroup $H \times \bar{H}$ with $|H| > 1$ and $|\bar{H}| > 2$, and no tetrahedral subgroup. Then G is soluble.*

PROOF. For odd primes p, the S_p-subgroups of G must be cyclic, since otherwise G would contain a subgroup $Z_p \times Z_p$: cf. [15], 310, 8.2 Satz. Let S be any S_2-subgroup of G. If S is either cyclic or normal in G, then G is soluble, by the Hölder-Burnside Theorem: cf. [15], 420, 2.11 Satz.

Let T be a non-trivial subgroup of S; and suppose, if possible, that $T^x = T$ for some element $x \in G$ whose order is an odd prime p. Let T_1 be a minimal characteristic subgroup of T. Then T_1 is of exponent 2; and $|T_1|$ is 2 or 4, since otherwise G would contain a subgroup $Z_2 \times D_4$. Also $T_1^x = T_1$. If $[T_1, x] = 1$, G would contain a $Z_2 \times Z_p$; and if not, then $|T_1| = 4$, $p = 3$ and $\langle T_1, x \rangle$ is tetrahedral. In either case we obtain a contradiction of the hypothesis of the lemma. Hence $N_G(T)$ is a 2-group. But if T is a maximal intersection of S with one of its conjugates in G, then $N_G(T)$ cannot be a 2-group. We conclude that $S = N_G(S)$ is disjoint from all its conjugates in G. By a theorem of Frobenius, it follows that $G = SN$, where $N \lhd G$ and $S \cap N = 1$: cf. [15], 495. Since all the Sylow subgroups of N are cyclic, G is therefore soluble.

In particular, if J is a simple group of composite order, then J has subgroups H and $\bar{H}$ which either satisfy the conditions (ii) of Theorem D2, or else are such that

(22)* $|\bar{H}| = 3, |H| = 2, \bar{H} \leqq \mu(J)$ and $H^J = J$,

where $\langle H, \bar{H} \rangle = A_4$ is a tetrahedral subgroup of J, with $H^{\bar{H}} = A'_4 \cong D_4$.

7. PROOF OF THEOREM D3. We now write $J_2, H_2, \bar{H}_2$ for the groups $J, H, \bar{H}$ of the theorem, including those in (22)*; and K_1 for K. To apply the bilateral construction we have to find a suitable mate J_1 for J_2. We require that J_1 shall contain L and also have subgroups $H_1, \bar{H}_1$ such that

(23) $J_1 = \langle H_1, K_1 \rangle = H_1^{J_1}, \bar{H}_1 \leqq \mu(J_1)$ and $\langle H_1, \bar{H}_1 \rangle \cong \langle \bar{H}_2, H_2 \rangle$,

where it is to be understood that in the isomorphism H_1 maps onto $\bar{H}_2$ and $\bar{H}_1$ onto H_2.

If these requirements are satisfied, the construction can proceed exactly as in §4.1 We form the bilateral group $G = J_1 * J_2 / H_1 = \bar{H}_2, \bar{H}_1 = H_2$. In G we have $H_1 = \bar{H}_2 \leqq \mu(J_2)$ by (22) or (22)*, and so $(J_1 \cap \mu(J_2))^{J_1} = J_1$ by (23); while $H_2 = \bar{H}_1 \leqq \mu(J_1)$ by (23), and so $(J_2 \cap \mu(J_1))^{J_2} = J_2$ by (22) or (22)*. Hence J_1 and J_2 are hololophic in G by Lemma 7; and so there is a simple quotient group of G of the form $S = \langle J_1, J_2 \rangle$. Since $J_1 = \langle H_1, K_1 \rangle$ by (23), and $H_1 = \bar{H}_2 \leqq J_2$, this gives $S = \langle K_1, J_2 \rangle = \langle J, K \rangle$, as required; and L is embedded in S as a subgroup of J_1.

Except when $|H_1| = 3$ and $|K_1| = 2$, we may satisfy (23) by taking $J_1 = P_1 \wr H_1$ for a suitable perfect simple group P_1. This follows from Theorem B2 and Lemma 18. Here (22) holds but we must take care that P_1 contains not only L but also a copy of the finite group H_2. The group of constant vectors $\bar{P}_1$ in $P_1^{H_1}$ will then contain a subgroup $\bar{H}_1 \cong H_2$ such that $\langle H_1, \bar{H}_1 \rangle$ is the direct product $H_1 \times \bar{H}_1$.

Theorem B2 covers the case $|H_1| > 3, |K_1| > 2$, since then $l(K_1) < |H_1|$ by §4, (50). The two parts of Lemma 18 cover the cases $|H_1| = 3, |K_1| > 2$ and $|H_1| = 4, |K_1| = 2$. This leaves only the exceptional case $|H_1| = 3, |K_1| = 2$ mentioned above.

8. To cover this case we prove

LEMMA 20. Let L be any countable group. Then there exists a group of the form $J = \langle u, b \rangle$, where u is of order 3 and b is of order 2, such that

(24) $L \leqq J = \langle u, u^b \rangle, \langle u, \alpha \rangle \cong Z_6$ and $\langle u, \beta \rangle \cong A_4$

for suitable chosen involutions α and β in $\mu(J)$.

As before, Z_6 is the cyclic group of order 6 and A_4 is the tetrahedral group. We may satisfy (23) by taking $J_1 = J, H_1 = \langle u \rangle, K_1 = \langle b \rangle$ and $\bar{H}_1 = \langle \alpha \rangle$ or $\langle \beta \rangle$, according to whether (22) or (22)* holds.

PROOF. By §4, (10), there is a perfect simple group P such that

(25) $$L \leq P = \langle \sigma_1, \cdots, \sigma_4 \rangle \text{ and } [\sigma_1, \sigma_4] \neq 1,$$

where the σ_i are involutions. The relation $[\sigma_1, \sigma_4] \neq 1$ may be obtained by a suitable numbering of the σ_i. Let

(26) $$C = \langle \xi \rangle, \quad R = P \wr C \text{ and } M = \langle R, \tau_1 \rangle,$$

where ξ is of order a prime $p \geq 11$ and τ_1 is an involution which transforms R as follows:

(27) $$\xi^{\tau_1} = \xi^{-1} \text{ and } (v^{\tau_1})_{\xi^i} = v_{\xi^{p-i}} \quad (i = 1, \cdots, p)$$

Here v is any vector in the base group P^C of R. Thus $\tau_2 = \tau_1 \xi$ is also an involution, $D_{2p} = \langle \tau_1, \tau_2 \rangle$ is dihedral, and M is the non-standard wreath product of P by D_{2p} with respect to the representation of degree p.

We now define a third involution $\tau_3 \in P^C$: $A = \operatorname{Sup} \tau_3$ is to consist of the four elements ξ, ξ^2, ξ^3 and ξ^4, the corresponding coordinates of τ_3 being $\sigma_1, \sigma_2, \sigma_3, \sigma_4$. Since $p \geq 11$, $A \cap A\xi^{-3}$ contains only ξ; and so $[\xi \tau_3 \xi^{-1}, \xi^4 \tau_3 \xi^{-4}] = [\sigma_1, \sigma_4] \neq 1$ by (25). Since the coordinates of τ_3 generate P, the usual argument based on Lemma 2.3 and the simplicity of P gives

(28) $$R = \langle \xi, \tau_3 \rangle \text{ and } M = \langle \tau_1, \tau_2, \tau_3 \rangle.$$

Writing $H = \langle u \rangle$, we take b to be the vector in the base group M^H of $M \wr H$ given by

(29) $$b = (\tau_1, \tau_2, \tau_3),$$

the coordinates being in the order $1, u, u^2$. We have to show that the group $J = \langle u, b \rangle$ satisfies (24).

In P^C, we have $\operatorname{Sup} \tau_3^{\tau_1} = A^{-1}$ and $\operatorname{Sup} \tau_3^{\tau_2} = A^{-1}\xi$ by (27). Since $p \geq 11$, we have $A \cap A^{-1} = A \cap A^{-1}\xi = \varnothing$. Hence all the coordinates of $[\tau_1, \tau_3]$ and $[\tau_3, \tau_2]$ are involutions, and so $[\tau_1, \tau_3]^2 = [\tau_3, \tau_2]^2 = 1$. But in M^H, the vector ubu^{-1} has coordinates (τ_2, τ_3, τ_1). This gives, with the usual convention,

(30) $$[b, ubu^{-1}]^2 = [\tau_1, \tau_2]^2 = \xi^2 \neq 1.$$

By (28) and (29), the coordinates of b generate M. Writing $K = \langle b \rangle$, it follows that $M \cap [H, K] \lhd M$ by Lemma 2.3. But $C = \langle \xi^2 \rangle \leq [H, K]$ by (30); and $C^R = R$ since P is perfect. Combining these three relations and noting that $R \leq M$ and $[H, K] \lhd J = \langle H, K \rangle$, we obtain

(31) $$R^H \leq [H, K].$$

But $\tau_1 \equiv \tau_2$ and $\tau_3 \equiv 1 \bmod R^H$ and so J/R^H is a tetrahedral group by (29). Hence $J = H^J = \langle u, u^b \rangle$ by (31).

Since $\mu(R) = P^C$ and τ_1 transforms R by an outer automorphism, we have $\mu(M) = P^C$. Hence $\mu(J) = (P^C)^H$ by Lemma 2.4; and so it contains the elements

(32) $$\alpha = \sigma_1\sigma_1^u\sigma_1^{u^2} \text{ and } \beta = \sigma_1\sigma_1^u.$$

Since σ_1, σ_1^u and $\sigma_1^{u^2}$ all commute, α and β satisfy (24).

The proof of Lemma 20 is now complete, and with it also the proof of Theorem D3.

In conclusion we note, for comparison with those mentioned in §5.5 above, some of the groups J which satisfy the conditions (ii) of Theorem D3. They include the symmetric groups of degree $q \geqq 5$, in which we can take $H = \langle t \rangle$ and $\bar{H} = \langle u \rangle$, where t is a transposition and u is a 3-cycle commuting with t. The finite groups $J = P \wr H$ of RP-type (with $H \neq 1$) also satisfy (ii), with $\bar{H} = \bar{P}$ the group of constant vectors in P^H. Another interesting example is the ternary Hessian group $J = AQH$, a subgroup of the holomorph of the non-Abelian group A of exponent 3 and order 27, Q being the quaternion group and QH the binary tetrahedral group of order 24. $\mu(J) = A'$ is the centre of J and is the only possible choice for $\bar{H}$.

But the conditions (ii) of Theorem D3 are in general more exacting than those of the Corollary to Theorem D2. Of the 25 groups of order at most 60 which satisfy the latter, only one satsisfies the former. This is the group $J = \langle A, \tau \rangle$ of order 54 with $\tau^2 = 1$ and $\xi^\tau = \xi^{-1}$, $\eta^\tau = \eta^{-1}$, where $A = \langle \xi, \eta \rangle$ is the Fitting subgroup of the ternary Hessian group mentioned above.

6. Transitive subgroups of wreath products

1. By a *transitive subgroup* of a transitive permutation group W we shall mean throughout any subgroup of W which is transitive on the full set Sup W of symbols permuted by W. (This is a different convention from that sometimes used, e.g. in the discussion of case (iii) in §5.2, where a transitive subgroup merely means any subgroup which is transitive on its own support.)

Let Y and Z be transitive groups, with Sup $Y = B$ and Sup $Z = C$; and let

(1) $$W = \text{Wr}(Y,Z) = \Omega Z, \text{ where } \Omega = \Omega(Y,C),$$

be the natural complete wreath product of Y by Z. For convenience of reference, we recall here some remarks made in §1.9 and 1.3. W is a transitive permutation group with support $B \times C$. Its elements $\eta\zeta$ ($\eta \in \Omega, \zeta \in Z$) act as follows:

(2) $$(b,c)\eta\zeta = (b\eta_c, c\zeta) \quad (b \in B, c \in C).$$

Each 'point' (b,c) lies on a unique 'line' $L_c = (B,c)$ consisting of all the points (b',c) with $b' \in B$; and the family of 'parallel' lines L_c forms a system of imprimitivity for W.

For each $c \in C$, we have a direct decomposition

(3) $$\Omega = Y_c \times M_c,$$

where Y_c is a copy of Y and $\eta \in Y_c$ if and only if $\eta_{c'} = 1$ for all $c' \neq c$; while

$\eta \in M_c$ if and only if $\eta_c = 1$. Further,

(4) $\zeta^{-1} Y_c \zeta = Y_{c\zeta}$ and $\zeta^{-1} M_c \zeta = M_{c\zeta}$ $(c \in C, \zeta \in Z)$.

The restricted wreath product $R = Y \wr Z$ is the semidirect product DZ, where

(5) $D = \underset{c \in C}{\mathrm{Dr}}\, Y_c = (Y_c)^Z$ and $R = \langle Y_c, Z \rangle (c \in C)$.

Here it is relevant that Z permutes C transitively. If $u = \eta \zeta \in R$, where $\eta \in D$ and $\zeta \in Z$, then $\mathrm{Sup}\, \eta$ is finite; and so

(6) $$|u| = Y \prod_{c \in C} \eta_c = |\eta|$$

is a well defined element of the Abelian group Y/Y'. If $v = \eta^* \zeta^*$ is also in R, we have $uv = \eta(\zeta \eta^* \zeta^{-1}) \zeta \zeta^*$. Since $|\eta^*| = |\zeta \eta^* \zeta^{-1}|$ by the transformation law, this gives

(7) $$|uv| = |u| \cdot |v| \qquad (u, v \in R).$$

The homomorphism $u \to |u|$ of R maps Z trivially and maps each Y_c onto Y/Y'. Its kernel is $Z^R = Z[D, Z]$ cf. Lemma 2.2. Hence

(8) $$Y/Y' \cong R/Z^R.$$

LEMMA 21. *For given $b \in B$ and $c \in C$, let $J = \mathrm{St}_W(b, c)$ and $H = \mathrm{St}_W(L_c)$ be the stabilizers in W of the point (b, c) and the line L_c, respectively. Then*

(9) $$\Pi_{H:J} \approx Y \text{ and } \Pi_{W:H} \approx Z.$$

The notation here is that explained in §1.9.

PROOF. Let $Y^{(b)} = \mathrm{St}_Y(b)$ and $Z^{(c)} = \mathrm{St}_Z(c)$ be the stabilizers of b in Y and of c in Z, respectively; and let $Y_c^{(b)}$ be the subgroup of Y_c which corresponds to the subgroup $Y^{(b)}$ of Y. By (2) and (3), we have

$$H = \Omega Z^{(c)} = M_c Z^{(c)} \times Y_c \quad \text{and } J = M_c Z^{(c)} \times Y_c^{(b)},$$

since the elements of $M_c Z^{(c)}$ fix every point of the line L_c. Given $b' \in B$, there is an element $\beta' \in Y_c$ such that $(b, c)\beta' = (b', c)$, since Y is transitive on B. The elements β', one for each $b' \in B$, form a transversal to J in H; and the one-to-one mapping ϕ of B onto the cosets of J in H defined by $\phi(b') = J\beta'(b' \in B)$ gives the required relation $\phi^{-1} Y \phi = \Pi_{H:J}$.

Similarly, for each $c' \in C$ we choose an element $\gamma' \in Z$ such that $c\gamma' = c'$; and the elements γ' form a transversal to $H = \Omega Z^{(c)}$ in $W = \Omega Z$. The one-to-one mapping ψ of C onto the cosets of H in W defined by $\psi(c') = H\gamma'(c' \in C)$ then gives $\psi^{-1} Z \psi = \Pi_{W:H}$.

2. Now let H be a subgroup of any group G and let $t_c (c \in C)$ be a transversal to H in G. For any $x \in G$, the permutation $\pi_{G:H}(x) : Hy \to Hyx$ of the cosets

Hy of H in G may then be transcribed into the permutation $t(x)$ of C defined by the rule

(10) $ct(x) = c'$ if and only if $t_c x t_{e'}^{-1} \in H$.

t is a transitive representation of G by permutations of C and clearly

(11) $\Pi_{G:H} \approx t(G)$.

The kernel of t is

(12) $$K_G(H) = \bigcap_{x \in G} H^x.$$

t does not depend on the choice of the transversal elements t_c in their respective cosets Ht_c, but only on the implied labelling of these cosets by the elements of C.

The theorem of Frobenius referred to in §1.9 may be stated in several equivalent ways, FI — FIII.

FI. *Let Z be any permutation group on C which contains $t(G)$, and let θ be any homomorphism of H into Y. Then there is a homomorphism θ^* of G into $W = \mathrm{Wr}(Y, Z)$ defined, for each $x \in G$, by*

(13) $\theta^*(x) = \eta\zeta$, where $\zeta = t(x)$ and $\eta_c = \theta(t_c x t_{c\zeta}^{-1})$ $(c \in C)$;

and the kernel of θ^* is $K_G(M)$ where M is the kernel of θ.

This version expresses the method of induced representations: cf. [15], 413; [21], §6.

If $|G : H|$ is finite, then C is finite since $|C| = |G : H|$; and W coincides with $R = Y \wr Z$. From (7) we obtain in this case the *transfer* homomorphism — of G into Y/Y' viz.

(14) $$x \to |\theta^*(x)| = Y \prod_{c \in C} \theta(t_c x t_{c\zeta}^{-1})   (x \in G, \zeta = t(x)).$$

Next, let J be a subgroup of H and let s_b $(b \in B)$ be a transversal to J in H. Then the elements

(15) $u_{b,c} = s_b t_c$ $(b \in, c \in C)$

form a transversal to J in G. By the labelling of these transversals, the representations $\pi_{H:J}$ of H and $\pi_{G:J}$ of G can be transcribed into representations s of H and u of G, $s(H)$ being transitive on B and $u(G)$ transitive on $B \times C$.

Assuming that $s(H) \leqq Y$ and $t(G) \leqq Z$, where Y and Z are permutation groups on B and C respectively, we then have

FII. *The induced homomorphism s^* of G into $W = \mathrm{Wr}(Y, Z)$ coincides with u, i.e. for $x \in G$,*

(16) $u(x) = \sigma\zeta$,   where $\zeta = t(x)$ and $\sigma_c = s(t_c x t_{c\zeta}^{-1})$ $(c \in C)$.

PROOF. Let $b \in B$, $c \in C$. Rule (10) applied to the transversal (15) shows that $(b, c) u(x) = (b', c')$ if and only if $s_b t_c x t_{c'}^{-1} s_{b'}^{-1} \in J$. This condition is equivalent to (i) $t_c x t_{c'}^{-1} \in H$ i.e. $c' = c\zeta$, and (ii) $bs(t_c x t_c^{-1}) = b'$. Comparison with (2) shows that $u(x)$ is the element $\sigma\zeta \in W$ defined by (16).

Besides (11) we have $\Pi_{H:J} \approx s(H)$ and $\Pi_{G:J} \approx u(G)$. Since the representations s, t and u are transitive, the relations $s(H) \leq Y$ and $t(G) \leq Z$, which imply $u(G) \leq W$ by FII, and the definition of 'trans' given in §1.9, allow us to restate FII in more qualitative terms as

FIII. *If $\Pi_{H:J}$ trans Y and $\Pi_{G:H}$ trans Z, then $\Pi_{G:J}$ trans $W = \mathrm{Wr}(Y, Z)$*

For convenience of reference, we note here some obvious properties of the relations $\approx$ and 'trans'. Proofs are superfluous.

LEMMA 22. 1. $\approx$ is an equivalence relation, and 'trans' is a transitive relation.

2. Let Γ be a transitive permutation group and let Λ be any one of the stabilizers in Γ. Then $\Pi_{\Gamma:\Lambda} \approx \Gamma$.

3. Let $\Sigma = \mathrm{Sym} \, A$ be the group of all permutations of the set A and let H be a subgroup of the group G. Then $\Pi_{G:H}$ trans Σ if and only if $|G : H| = |A|$.

4. If G_1 is a subgroup of G such that $HG_1 = G$, then $\Pi_{G_1:H_1}$ trans $\Pi_{G:H}$, where $H_1 = G_1 \cap H$.

5. If Γ is regular as well as transitive, then $\Pi_{G:H}$ trans Γ if and only if $H \lhd G$ and $G/H \cong \Gamma$.

3. PROOF OF THEOREM E1. Let $\Gamma_1, \cdots, \Gamma_r$ be transitive permutation groups and Sup $\Gamma_i = A_i$ $(i = 1, \cdots, r)$. Then the natural complete wreath product $W = \mathrm{Wr}$ $(\Gamma_1, \cdots, \Gamma_r)$ is a transitive permutation group with Sup $W = A = A_1 \times \cdots \times A_r$. As noted in §1.9, this kind of wreath multiplication is associative. Hence, when $r > 2$, we have

$$(17) \qquad W = \mathrm{Wr}(\Gamma_1, W_1), \text{ where } W_1 = \mathrm{Wr}(\Gamma_2, \cdots, \Gamma_r),$$

on the understanding that the support A of W is to be identified in the obvious way with the set

$$(18) \qquad B \times C, \text{ where } B = A_1 \text{ and } C = A_2 \times \cdots \times A_r.$$

Let G be any group with a chain of subgroups $H = H_0 \leq H_1 \leq \cdots \leq H_r = G$ such that

$$(19) \qquad K_G(H) = 1 \text{ and } \Pi_{H_i:H_{i-1}} \text{ trans } \Gamma_i \quad (i = 1, \cdots, r).$$

Then $G \cong \Pi_{G:H}$. If $r = 2$, we have $\Pi_{G:H}$ trans W by FIII. If $r > 2$, we may assume inductively that $\Pi_{G:H_1}$ trans W_1: and again FIII gives $\Pi_{G:H}$ trans W by (17). It follows by induction on r that G is isomorphic with a transitive subgroup of W.

To prove the converse part of the theorem, we may clearly suppose that G

itself is a transitive subgroup of W, and have to infer the existence of a chain of subgroups satisfying (19). Given $b \in B$ and $c \in C$, consider the stabilizers $J = J_0 = \text{St}_W(b, c)$ and $J_1 = \text{St}_W(L_c)$, where L_c consists of all the points (b', c) with $b' \in B$. Let $H = H_0 = J \cap G$. Then $H = \text{St}_G(b, c)$ and so $K_G(H) = 1$ since G is transitive on $B \times C$. For the same reason, $JG = W$; and so $J_1 G = W$ and $JH_1 = J_1$, where $H_1 = G \cap J_1$. By Lemmas 22.4 and 21, we have

(20) $\Pi_{H_1:H}$ trans $\Pi_{J_1:J} \approx \Gamma_1$, and $\Pi_{G:H_1}$ trans $\Pi_{W:J_1} \approx W_1$.

When $r = 2$, it follows that G satisfies (19), with $H_2 = G$.

If $r > 2$, let $M = K_G(H_1)$. The relation $\Pi_{G:H_1}$ trans W_1 from (20) shows that G/M is isomorphic with a transitive subgroup of W_1, the subgroup H_1/M corresponding to the stabilizer in the image group of the point $c \in C = \text{Sup } W_1$. From this, we may assume inductively that there is a chain of subgroups $H_1 \leqq H_2 \leqq \cdots \leqq H_r = G$ such that $\Pi_{H_1/M:H_{i-1}/M}$ trans $\Gamma_i (i = 2, \cdots, r)$. Since $\Pi_{H_i/M:H_{i-1}/M} \approx \Pi_{H_i:H_{i-1}}$, these relations together with the first relation in (20) show that G satisfies (19).

This completes the proof of Theorem E1.

In general, the theorem cannot be said to give conditions for the embedding of a group in *a join of given groups*, and it is therefore peripheral to the main concern of the paper. Only when the given groups Γ_i are all finite will W coincide with the natural restricted wreath product $R = \Gamma_1 \wr \Gamma_2 \wr \cdots \wr \Gamma_r$, which has the form

(21) $R = \langle \Gamma_1, \cdots, \Gamma_r \rangle$,

by (15) and its inductive generalization.

Two special cases of the theorem may be noted. The first, in which the Γ_i are chosen maximally i.e. as symmetric groups $\Sigma_i = \text{Sym } A_i$, is familiar from the theory of imprimitive permutation groups: a group G can be embedded as a transitive subgroup in $\text{Wr}(\Sigma_1, \Sigma_2, \cdots, \Sigma_r)$ if and only if it has a chain of subgroups $H = H_0 \leqq H_1 \leqq \cdots \leqq H_r = G$ such that $K_G(H) = 1$ and $|H_i : H_{i-1}| = |A_i|$ for each $i = 1, \cdots, r$. This case corresponds to Lemma 22.3.

The opposite extreme is when the Γ_i are all regular as well as transitive. This case corresponds to Lemma 22.5, and appears to have been overlooked, although special instances are well known. We state it as

THEOREM E2. *A group G can be embedded as a transitive subgroup in the regular wreath product $W = \text{Wr}(\Gamma_1, \cdots, \Gamma_r)$ if and only if it has a series of subgroups $H = H_0 \lhd H_1 \lhd \cdots \lhd H_r = G$ such that*

(22) $K_G(H) = 1$ and $H_i/H_{i-1} \cong \Gamma_i$ $(i = 1, \cdots, r)$

As remarked in §1.9, the theorem of Kaloujnine and Krasner is the special case $r = 2$ but with the unnecessary assumption $H = 1$ in place of $K_G(H) = 1$:

cf. [15], 99, 15.9 Satz; or [22], 100, III. 5. k. Also well known from the work of Kaloujnine [24] on the Sylow subgroups of the finite symmetric groups is the case where $|\Gamma_i| = p$ is a given prime for all i.

It should be noted that the regular wreath product W in Theorem E2 is isomorphic with the repeated standard wreath product of the given groups $\Gamma_1, \cdots, \Gamma_r$, provided that this is defined inductively, as in §2, by

$$\mathrm{Wr}(\Gamma_1, \cdots, \Gamma_r) = \mathrm{Wr}(\mathrm{Wr}(\Gamma_1, \cdots, \Gamma_{r-1}), \Gamma_r).$$

If the standard product $\mathrm{Wr}(\Gamma_1, \Gamma_2, \Gamma_3)$ is to be equated with $\mathrm{Wr}(\Gamma_1, \mathrm{Wr}(\Gamma_2, \Gamma_3))$, the latter must be defined with respect to the natural representation of $\mathrm{Wr}(\Gamma_2, \Gamma_3)$ on the set $\Gamma_2 \times \Gamma_3$ as support.

4. We shall now use Frobenius' result FI (for the case where $H \lhd G$) to throw light on the relation $\lhd_2$.

First, let G be any group with subgroups M and H such that

(23) $$M \lhd H \lhd G \text{ and } K_G(M) = 1.$$

Then FI gives an embedding of G in the standard wreath product.

(24) $$W = \mathrm{Wr}(L, \Gamma), \text{ where } L \cong H/M \text{ and } \Gamma = G/H.$$

We take θ to be a homohorphism of H onto L with M as kernel. Then the embedding of G in W is θ^*, defined as in (13)

Let $t_\alpha(\alpha \in \Gamma)$ be a transversal to H in G. We may suppose that $t_1 = 1$. Every element of G is then uniquely expressible in the form ut_α $(u \in H, \alpha \in \Gamma)$. Let

(25) $$c_{\alpha,\beta} = t_\alpha t_\beta t_{\alpha\beta}^{-1} \qquad (\alpha, \beta \in \Gamma).$$

Then the $c_{\alpha,\beta}$ are elements of H by (23); and $c_{\alpha,1} = c_{1,\beta} = 1$ for all α, β in Γ, since $t_1 = 1$. Let τ_α be the automorphism of H defined, for each $\alpha \in \Gamma$, by

(26) $$u^{\tau_\alpha} = t_\alpha u t_\alpha^{-1} \qquad (u \in H).$$

By (13), the vector part of the element $\theta^*(ut_\alpha) \in W$ has the γ-coordinate $\theta(t_\gamma u t_\alpha t_{\gamma\alpha}^{-1})$. Hence the embedding θ^* is given explicitly by

(27) $$\theta^*(ut_\alpha) = u^* c^{(\alpha)} \alpha, \text{ where } u^* = \theta^*(u) \qquad (u \in H, \alpha \in \Gamma);$$

and the vectors u^* and $c^{(\alpha)}$ in $\Omega = \Omega(L, \Gamma)$ have as γ-coordinates the elements

(28) $$u_\gamma^* = \theta(u^{\tau_\gamma}) \text{ and } c_\gamma^{(\alpha)} = \theta(c_{\gamma,\alpha}) \qquad (\gamma \in \Gamma).$$

It follows from FI without further calculation that, for all u, v in H and α, β in Γ,

(29) $$u^* c^{(\alpha)} \alpha \cdot v^* c^{(\beta)} \beta = w^* c^{(\alpha\beta)} \alpha\beta, \text{ where } w = uv^{\tau_\alpha} c_{\alpha,\beta},$$

since $ut_\alpha v t_\beta = wt_{\alpha\beta}$ by (25).

In the Kaloujnine-Krasner Theorem, $M = 1$ and θ is the identity mapping of $H = L$; and the usual proofs of it are equivalent to deriving (29) directly from (28). This method has the merit of giving at the same time a proof of Otto Schreier's Existence Theorem for extensions of H by Γ; and it applies equally well under the present weaker assumption that

(30) $$\bigcap_{\alpha \in \Gamma} M^{\tau_{\sim}^{-1}} = 1.$$

The theorem in question may be stated as follows, H and Γ being any given groups.

Let θ be a homomorphism of H into L with kernel M, and let $\tau_\alpha(\alpha \in \Gamma)$ be automorphisms of H and the $c_{\alpha,\beta}$ $(\alpha, \beta \in \Gamma)$ elements of H satisfying (30) and also the congruences

(31) $$c_{\alpha,\beta}^{\tau_\gamma} \equiv c_{\gamma,\alpha} c_{\gamma\alpha,\beta} c_{\gamma,\alpha\beta}^{-1} \quad and \quad v^{\tau_\alpha \tau_\gamma} \equiv c_{\gamma,\alpha} v^{\tau_{\gamma\alpha}} c_{\gamma,\alpha}^{-1} \bmod M$$

for all $v \in H$ and α, β, γ in Γ. Then the elements $u*c^{(\alpha)}\alpha$ $(u \in H, \alpha \in \Gamma)$ of $W = \mathrm{Wr}$ (L, Γ) defined by (28) form an extension G^* of H by Γ such that $\Omega G^* = W$ and $\Omega \cap G^* = H^* \cong H$; and the elements $s_\alpha = c^{(\alpha)}\alpha \, (\alpha \in \Gamma)$ form a transversal to H^* in G^* such that

(32) $$s_\alpha s_\beta s_{\alpha\beta}^{-1} = (c_{\alpha,\beta})^* \quad and \quad s_\alpha u*s_\alpha^{-1} = (u^{\tau_\alpha})^* \quad (\alpha, \beta \; in \; \Gamma, u \in H).$$

The verification is immediate. The γ-coordinate of the vector

$$u*c^{(\alpha)} \cdot \alpha(v*c^{(\beta)})\alpha^{-1} \cdot (c^{(\alpha\beta)})^{-1} \; is$$

$$\theta(u^{\tau_\gamma} c_{\gamma,\alpha} v^{\tau_{\gamma\alpha}} c_{\gamma\alpha,\beta} c_{\gamma,\alpha\beta}^{-1}) = \theta(u^{\tau_\gamma} v^{\tau_{-\tau_\gamma}} c_{\alpha,\beta}^{\tau_\gamma}) = w_\gamma^*$$

by (28), the transformation law and (31). This gives (29) and shows that G^* is a group, the inverse of $u*c^{(\alpha)}\alpha$ being $v*c^{(\alpha^{-1})} \alpha^{-1}$ where v is determined from $uv^{\tau_\alpha} c_{\alpha,\alpha^{-1}} = 1$. Clearly $\Omega G^* = W$ and so $G^*/H^* \cong \Gamma$; and H^*, which consists of all $u*$ with $u \in H$, is isomorphic with H by (28) and (30), since $u* = 1$ implies that $u^{\tau_\gamma} \in M$ for all $\gamma \in \Gamma$. The statements concerning the transversal elements s_α follow from (31).

5. We now consider the special case where

(33) $$L \triangleleft_2 G, \; H = L^G, \; \Gamma = G/H \; and \; \Delta = N_G(L)/H.$$

Let X be a transversal to Δ in Γ. We may suppose that $1 \in X$. By definition of $\triangleleft_2$,

(34) $$H = \mathop{\mathrm{Dr}}_{\zeta \in X} t_\zeta^{-1} L t_\zeta = L \times M \; and \; K_G(M) = 1,$$

where M is the direct product of all the conjugates of L in G other than L itself, and $t_\zeta(\zeta \in X)$ is a transversal to $N_G(L)$ in G, with $t_1 = 1$. Further $N_G(L) = L C_G(L)$; and since every $\gamma \in \Gamma$ is uniquely of the form $\delta\zeta$ with $\delta \in \Delta$ and $\zeta \in X$, we may complete the definition of a transversal $t_\gamma(\gamma \in \Gamma)$ to H in G by taking

(35) $t_{\delta\xi} = t_\delta t_\xi$ and $t_\delta \in C_G(L)$ $(\delta \in \Delta, \xi \in X)$.

By (34), each $u \in H$ is uniquely of the form $u_1 u_2$ with $u_1 \in L$, $u_2 \in M$; and $\theta(u) = u_1$ defines θ as a homomorphism of H onto L. The induced embedding θ^* of G in $W = \mathrm{Wr}(L, \Gamma)$ is defined by (27) and (28), and we shall write $G^* = \theta^*(G)$, $H^* = \theta^*(H)$ etc. It will be convenient to use the notations of §4.4 (12) for certain vectors in $\Omega = \Omega(L, \Gamma)$. We recall that if $x \in L$ and A is any subset of Γ, then the vector x_A has the constant value x on A and is trivial elsewhere.

Now let $y \in L$ and $\eta \in X$. By (28) and (35), the $\delta\xi$-coordinate of $(t_\eta^{-1} y t_\eta)^*$ is $\theta(y t_\eta t_\xi^{-1} t_\delta^{-1})$. If $\xi \neq \eta$, then $y t_\eta t_\xi^{-1} \in M \lhd N_G(L)$, and so this $\delta\xi$-coordinate is trivial; but if $\xi = \eta$, it reduces to y since $t_\delta \in C_G(L)$. Hence $(t_\eta^{-1} y t_\eta)^* = y_{\Delta\eta}$, and so

(36) $L^* = L_\Delta, H^* = \Omega \cap G^* = \underset{\xi \in X}{\mathrm{Dr}}\ L_{\Delta\xi} = D_\Delta$ and $W = \Omega G^*$.

Thus H^* coincides with the base group D_Δ of the restricted wreath product $R_\Delta = \langle L_\Delta, \Gamma \rangle$ of L by Γ with respect to the representation $\pi_{\Gamma:\Delta}$ of Γ. Since R_Δ occurs in this way as a subgroup of the standard wreath product W, we may conveniently call it a *substandard* wreath product.

(36) contains the first part of

THEOREM E3. *If the groups G, L, H, Γ and Δ satisfy* (33), *then G can be embedded in the standard wreath product $W = \mathrm{Wr}(L, \Gamma)$ as a subgroup G^* satisfying* (36).

Conversely, let G^* be any subgroup of W such that

(37) $W = \Omega G^*$ and $\Omega \cap G^* = D_\Delta$,

and let Z be the centre of $\Omega = \Omega(L, \Gamma)$. Then

(38) $L_\Delta \lhd_2 G^* \leq Z W_\Delta$,

where $W_\Delta = \Omega_\Delta \Gamma$.

We recall that Ω_Δ consists of all vectors in Ω which are constant on each coset of Δ so that W_Δ is the complete wreath product of L by Γ with respect to the resentation $\pi_{\Gamma:\Delta}$. Note also that $Z = \Omega(Z_1, \Gamma)$, where Z_1 is the centre of L.

PROOF OF THE CONVERSE: Let $\gamma v \in G^*$ where $\gamma \in \Gamma$ and $v \in \Omega$. Given $\xi \in X$, we have $\xi\gamma^{-1} = \delta\eta$ for some $\delta \in \Delta$ and $\eta \in X$. Since $L_{\Delta\eta} \leq D_\Delta \lhd G^*$, it follows that $(L_{\Delta\eta})^{\gamma v} \leq D_\Delta$. If $1 \neq y \in L$, the vector $(y_{\Delta\eta})^{\gamma v} = (y_{\Delta\eta\gamma})^v = (y_{\Delta\xi})^v$ has the support $\Delta\xi$. But the only elements of D_Δ whose support is contained in $\Delta\xi$ are those of $L_{\Delta\xi}$. Hence $(y_{\Delta\xi})^v$ is constant on $\Delta\xi$, and so $y^{v_\alpha} = y^{v_\beta}$ for all α, β in $\Delta\xi$. Since y is any non-trivial element of L and ξ any element of X, it follows that

(39) $v_\alpha v_\beta^{-1} \in Z_1$ whenever $\alpha\beta^{-1} \in \Delta$ $(\alpha, \beta \in \Gamma)$.

Hence $v \in Z\Omega_\Delta$ and so $G^* \leqq \Gamma Z\Omega_\Delta$. Since $Z \lhd W$, this gives $G^* \leqq Z\Gamma\Omega_\Delta = ZW_\Delta$ as required.

We have shown incidentally that, for any $\gamma v \in G^*$ and $\eta \in X$, we have $(L_{\Delta\eta})^{\gamma v}$ $= L_{\Delta\xi}$ where $\xi \in \Delta\eta\gamma$. Taking $\eta = 1$, it follows that the subgroups $L_{\Delta\xi}(\xi \in X)$ form the complete set of conjugates of L_Δ in G^*, since $W = \Omega G^* = G^*\Omega$ by (37); and $D_\Delta = (L_\Delta)^{G^*}$ is their direct product. Further, $N_W(L_\Delta) \leqq \Delta\Omega$ and, as we have shown, $G^* \leqq \Gamma Z\Omega_\Delta$. Hence $N_{G^*}(L_\Delta) \leqq \Delta\Omega \cap \Gamma Z \Omega_\Delta = \Delta Z\Omega_\Delta$. But $[\Delta, L_\Delta] = [Z, L_\Delta] = 1$ and L_Δ is a direct factor of Ω_Δ. Hence $N_{G^*}(L_\Delta) = L_\Delta C_{G^*}(L_\Delta)$. Thus $L_\Delta \lhd_2 G^*$.

This completes the proof of Theorem E3.

A corollary, which is not difficult to prove independently, is

LEMMA 23. *Let $L \lhd_2 G$ and suppose that L has trivial centre and only finitely many conjugates in G. Then G is isomorphic with the substandard restricted wreath product R_Δ of L by Γ with respect to the representation $\pi_{\Gamma:\Delta}$. Here Γ and Δ are defined by (33).*

PROOF. We have $G \cong G^*$, where G^* satisfies (38), by Theorem E3. By hypothesis, the centre Z_1 of L is trivial, and so $Z = 1$. Also $|\Gamma : \Delta| = |G : N_G(L)|$ is finite, and so $\Omega_\Delta = D_\Delta$ and $W_\Delta = R_\Delta$. Thus (38) gives $G^* \leqq R_\Delta = D_\Delta\Gamma$. But $G^* \cap \Omega = D_\Delta$ by (36), and $\Omega G^* = \Omega\Gamma$. Hence $G^* = R_\Delta$.

The lemma may be regarded as a splitting theorem: it implies that, under the given conditions, G splits over $H = L^G$.

6. Finally, as an application of the transfer (14) we prove

LEMMA 24. *Let $L \lhd_2 G = G'$ and suppose that L has only finitely many conjugates in G. Then L is the product of its centre and its derived group.*

PROOF. In FI, we take $H = Y = N_G(L)$ and θ to be the identity mapping of H. By hypothesis, $|G : H|$ is finite, so that (14) applies. Since $G = G'$, the image of G in the transfer homomorphism must be trivial, so that (in the notation of FI)

$$\prod_{c \in C} t_c x t_{c\zeta}^{-1} \in H', \quad \text{where } \zeta = t(x), \tag{40}$$

for all $x \in G$. But $L \lhd_2 G$ and so L^G is the direct product of the conjugates of L in G and is contained in H. Hence $\zeta = 1$ for all $x \in L$. Since $H = N_G(L)$, we have (for $x \in L$) $t_c x t_c^{-1} \in C_G(L)$ whenever $t_c \notin H$. We may take $t_1 = 1$ as the representative of the coset H, and conclude from (40) that $x \in H'C_G(L)$ for all $x \in L$. But $H = LC_G(L)$ since $L \lhd_2 G$, and so $H' \leqq L'C_G(L)$. Hence $L = L'(L \cap C_G(L))$, which is the result stated.

COROLLARY. *Let L be a finite group which is not the product of its centre and its derived group, and let P and Q be non-trivial perfect finite groups. Then there is no finite group of the form $J = \langle P, Q \rangle$ such that $L \lhd_2 J$.*

By Theorem A, we know that $L \lhd_2 J$ for some $J = \langle P, Q \rangle$; and the corollary states that any such J must be infinite. This is in contrast with Theorem D1 which shows that L can always be embedded in some finite simple group of the form $\langle P, Q \rangle$.

In [4], Theorem 3, Dark showed that D_6, the smallest non-Abelian group, cannot even be subnormally embedded in any finite perfect group. However, the subnormal — and indeed the normal — subgroups of finite perfect groups are less severely limited in character than their $\lhd_2$-subgroups. Given any integer $d \geqq 0$, let G_d be a non-trivial finite perfect monolithic group which has a normal soluble subgroup N_d of derived length d. (We could take G_0 to be the icosahedral group.) If p is any prime not dividing $|G_d|$, then G_d has a faithful irreducible representation, of some degree m, over the field of p elements. The corresponding semidirect product $G_{d+1} = G_d M$, where $M = \mu(G_{d+1})$, is then also perfect and monolithic and of order $p^m |G_d|$. The normal subgroup $N_{d+1} = N_d M$ of G_{d+1} is then soluble and of derived length precisely $d + 1$. Thus d can be arbitrarily large.

References

[1] Graham Higman, B. H. Neumann and Hanna Neumann, 'Embedding theorems for groups', *J. London. Math. Soc.* 24 (1949), 247–254.

[2] F. Levin, 'Factor groups of the modular groups', *ibid.* 43 (1968), 195–203.

[3] Charles F. Miller III and Paul E. Schupp, 'Embeddings into Hopfian groups', *J. of Algebra* 17 (1971), 171–176.

[4] R. S. Dark, 'On subnormal embedding theorems for groups', *J. London. Math. Soc.* 43 (1968), 387–390.

[5] B. H. Neumann, 'An Essay on free products of groups with amalgamations', *Phil. Trans. Royal Soc. London Ser.* A, 246 (1954), 503–554.

[6] L. Onofri, 'Teoria delle sostituzioni che operano su una infinità numerabile di elemente, III', *Annali di Mat.* (4) 7 (1929), 103 -130.

[7] J. Schreier and S. Ulam, 'Über die Permutationsgruppe der natürlichen Zahlenfolge', *Studia Math.* 4 (1933), 134–141.

[8] R. Baer, 'Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich', *Studia Math.* 5 (1935), 15–17.

[9] Hanna Neumann, *Varieties of Groups*, (Springer-Verlag, 1967).

[10] Graham Higman, 'A finitely generated infinite simple group', *J. London Math. Soc.* 26 (1951), 61–64.

[11] B. H. Neumann and Hanna Neumann, 'Embedding theorems for groups', *ibid.* 34 (1959) 465–479.

[12] Hanna Neumann, 'Generalized free products with amalgamated subgroups', *Amer. J. of Math.* 70 (1948), 590–625.

[13] P. E. Schupp, 'A Survey of Small Cancellation Theory', *unpublished*.

[14] Marshall Hall Jr. *The Theory of Groups* (Macmillan Co. of New York, 1959).

[15] B. Huppert, *Endliche Gruppen* I, (Springer-Verlag, 1967).

[16] H. S. M. Coxeter and W. O. J. Moser, Generators and Relations for Discrete Groups, (Springer-Verlag, 1957).

[17] Ruth Camm, 'Simple free products', *J. London Math. Soc.* 28 (1953), 66–76.

[18] Helmut Wielandt, *Finite Permutation Groups*, (Academic Press, 1964).

[19] W. Burnside, *Theory of Groups of Finite Order*, (Cambridge 2nd ed. 1911).

[20] P. Hall, 'On the finiteness of certain soluble groups', *Proc. London Math. Soc.* (3) 9 (1959), 595–622.

[21] H. Wielandt and B. Huppert, 'Arithmetical and normal structure of finite groups', *Proc. Symposia Pure Math.* VI (1962), *Amer. Math. Soc.*

[22] E. Schenkman, *Group Theory*, (Van Nostrand, 1965).

[23] Marc Kranser et Léo Kaloujnine, 'Produit complet des groupes de permutations et problème d'extension de groupes III', *Acta .Sci. Math. Szeged* 14 (1951), 69–82.

[24] Léo Kaloujnine, 'La structure des *p*-groupes de Sylow des groupes symétriques finis', *Ann. Sci. Ecole Norm. Sup.* (3) 65 (1948), 239–276.

[25] B. H. Neumann and Sadayuki Yamanuro, 'Boolean Powers of simple groups', *J. Austral. Math. Soc.* 5. (1965), 315–324.

50, Impington Lane
Histon, Cambs
England