Math. Proc. Camb. Phil. Soc. (1976), **80**, 19
MPCPS 80–2
Printed in Great Britain

On characteristically simple groups

By J. S. WILSON
Christ's College, Cambridge

(*Received* 14 *March* 1975)

1. *Introduction*

1·1. A group is called *characteristically simple* if it has no proper non-trivial subgroups which are left invariant by all of its automorphisms. One familiar class of characteristically simple groups consists of all direct powers of simple groups: this contains all finite characteristically simple groups, and, more generally, all characteristically simple groups having minimal normal subgroups. However not all characteristically simple groups lie in this class because, for instance, additive groups of fields are characteristically simple. Our object here is to construct finitely generated groups, and also groups satisfying the maximal condition for normal subgroups, which are characteristically simple but which are not direct powers of simple groups.

We state our main result as

THEOREM A. *There are* $2^{\aleph_0}$ *isomorphism classes of 2-generator groups* C *with the following properties:*

(*a*) *a suitable infinite cyclic extension of* C *has* C *as a minimal normal subgroup,*

(*b*) C *has a maximal normal subgroup* M_C *which is residually nilpotent but not finitely generated,*

(*c*) C *is directly indecomposable, and*

(*d*) *central extensions both of* C *and of* C/M_C *have faithful representations as groups of automorphisms of finite dimensional vector spaces over division rings.*

Moreover the simple quotient groups C/M_C *fall into* $2^{\aleph_0}$ *isomorphism classes.*

It follows from (*a*) that each group C is characteristically simple, and from (*b*) and (*c*) that no group C is a direct product of simple groups. Of course there are no more than $2^{\aleph_0}$ isomorphism classes of finitely generated groups.

The construction of finitely generated characteristically simple groups which are not direct powers of simple groups solves problem 4.68 of the Kourov notebook (9).

It is easy to see that if E is a simple homomorphic image of a characteristically simple group G which is not a direct power of a simple group, then each finite direct power E^n of E is a homomorphic image of G. Therefore the simple quotient groups of our groups C are subject to a rather interesting restriction: not only are they 2-generator groups, but so are all of their finite direct powers. Considering the simple groups $E = C/M_C$, we may therefore state

COROLLARY A 1. *There are* $2^{\aleph_0}$ *isomorphism classes of simple groups* E *with the following properties:*

(*a*) *each finite direct power of* E *is a 2-generator group, and*

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

(*b*) *a central extension of E has a faithful representation as a group of automorphisms of a finite dimensional vector space over a division ring.*

Examples of non-trivial groups all of whose finite direct powers may be generated by a fixed number of elements have been constructed before. Proposition 1 of Tyrer Jones (17) shows that there are $2^{\aleph_0}$ non-isomorphic simple groups of the type constructed in Camm (5) all of whose finite direct powers are 3-generator groups; moreover non-trivial 5-generator groups are constructed in (17) which are actually isomorphic to all of their finite direct powers.† It follows from results proved below that *every finite group may be embedded in a simple group E all of whose finite direct powers are 2-generator groups*. Easy extensions of our arguments show that every countable linear group can be embedded in a group E with these properties, and that for each integer $r \geqslant 7$ and prime p there are $2^{\aleph_0}$ non-isomorphic simple groups E each of whose finite direct powers may be generated by an element of order r and an element of order p; however we shall not pursue these points further here.

It may be worth mentioning a further consequence of Theorem A. Let G be one of the infinite cyclic extensions referred to in (*a*) of Theorem A. Then every normal subgroup of G may be generated by three elements, and yet, by (*b*) of the Theorem, not every subnormal subgroup of G is finitely generated. Thus the property of having all normal subgroups finitely generated, though inherited by normal subgroups of finite index (see (18), theorem B), fails to be inherited by arbitrary normal subgroups.

Our results for groups satisfying the maximal condition for normal subgroups are summarized in the following

THEOREM B. *There are groups D of all infinite cardinalities with the following properties:*

(*a*) *D is characteristically simple,*

(*b*) *D has a maximal normal subgroup which is residually nilpotent but not finitely generated,*

(*c*) *D is directly indecomposable, and*

(*d*) *all proper homomorphic images of D have finite chief series.*

Moreover the countable linear groups with these properties fall into $2^{\aleph_0}$ *isomorphism classes.*

It follows immediately from (*d*) that the groups D satisfy the maximal condition for normal subgroups, and from (*b*) and (*c*) that they are not direct powers of simple groups. It is not hard to show that (*c*) is actually a consequence of (*a*), (*b*) and (*d*).

Theorem B is very much easier to establish than Theorem A, apart from the apparent necessity to quote a difficult result from algebraic K-theory. It may be contrasted with the elementary result that characteristically simple groups satisfying the minimal condition for normal subgroups are necessarily finite direct powers of simple groups.

Techniques similar to some of those used here yield results for Lie algebras over fields of characteristic zero corresponding to Theorems A and B. However our results

† *Added October* 1975. If E is any infinite simple group generated by d elements, then each finite direct power E^n of E may be generated by $d+1$ elements. This is proved in J. Wiegold and J. S. Wilson, 'Growth sequences of finitely generated groups', to appear.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

suggest a number of questions which seem beyond the range of the methods of the present paper. We have been unable to decide, for instance, whether or not there are characteristically simple groups which are not direct powers of simple groups and which both are finitely generated and at the same time satisfy the maximal condition for normal subgroups.

1·2. The characteristically simple groups which we consider are all groups of matrices over suitable rings. Their construction is based on the observation (cf. Proposition 1 below) that, if K is an infinite field, then the central factor group $\mathrm{PSL}_n(K[x])$ of the special linear group $\mathrm{SL}_n(K[x])$ of degree $n \geqslant 3$ over the polynomial ring $K[x]$ is characteristically simple. Indeed, some of the examples needed to establish Theorem B will be groups $\mathrm{PSL}_n(K[x])$ for suitable K. However this observation alone is insufficient to establish Theorem A. A group $\mathrm{PSL}_n(K[x])$ can be finitely generated only if K is finitely generated as a ring, and therefore, by a form of the Nullstellensatz, only if K is finite; and it is easy to see that $\mathrm{PSL}_n(K[x])$ is not characteristically simple if K is a finite field. We are obliged to study non-commutative rings, and therefore we replace the functor $\mathrm{PSL}_n(-)$ by a functor whose definition does not depend on the existence of determinants.

For simplicity of exposition, we consider in this paper only rings with an identity element. While our main results for general rings remain valid when suitably interpreted without this restriction, and make possible the construction of locally nilpotent characteristically simple groups unlike those of McLain (12) and Hall (7), their proofs become distinctly more tedious. Let R be any ring and let Ω be an index set with at least two elements. Denoting by 1 the $\Omega \times \Omega$ identity matrix and by $(e_{ij}; i, j \in \Omega)$ the usual $\Omega \times \Omega$ matrix units, we define $\mathrm{E}_\Omega(R)$ to be the group of (invertible) $\Omega \times \Omega$ matrices over R generated by all matrices $1 + re_{ij}$ with $r \in R$ and with i and j distinct elements of Ω; and we define $\mathrm{PE}_\Omega(R)$ to be the central factor group of $\mathrm{E}_\Omega(R)$. Of course, since the elements of $\mathrm{E}_\Omega(R)$ differ from the identity matrix in only finitely many entries, there is no difference between $\mathrm{E}_\Omega(R)$ and $\mathrm{PE}_\Omega(R)$ unless Ω is finite. If $\Omega = \{1, 2, \ldots, n\}$, we write $\mathrm{E}_n(R)$ and $\mathrm{PE}_n(R)$ in place of $\mathrm{E}_\Omega(R)$ and $\mathrm{PE}_\Omega(R)$.

The groups $\mathrm{E}_n(R)$ and $\mathrm{SL}_n(R)$ actually coincide for some commutative rings R and for large enough n. For example, if R is a (commutative) Euclidean domain, then $\mathrm{E}_n(R) = \mathrm{SL}_n(R)$ for $n \geqslant 3$ (cf. Litoff (11), theorem 9). This fact plays a part in the proof that $\mathrm{PSL}_n(K[x])$ is characteristically simple for each infinite field K and integer $n \geqslant 3$.

We call a ring R *characteristically simple* if it has no *ideals* other than 0 and R which are invariant under all automorphisms of R. It is not hard to show that $K[x]$ is characteristically simple for each infinite field K. More generally, we shall show in Proposition 3 that if S is a characteristically simple ring which is an algebra over an infinite field, then the ring of polynomials over S in any family of commuting indeterminates is characteristically simple. The assertion that $\mathrm{PSL}_n(K[x])$ is characteristically simple for each infinite field K and each integer $n \geqslant 3$ generalizes to

THEOREM C. *Let R be a characteristically simple ring. The group $\mathrm{PE}_\Omega(R)$ is characteristically simple if either*

(*a*) *Ω is infinite, or*

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

(*b*) $|\Omega| \geqslant 3$, *and for all ordered pairs* (a, b) *of elements of* R *with* $a \neq 0$, *there is a pair* (x, y) *with* $y \neq 0$ *and with* $ax + by = 0$.

We observe that the condition on R in (*b*) is obviously satisfied if R is either commutative or a right Ore domain. The finitely generated characteristically simple groups which we construct are groups $\mathrm{PE}_n(R)$, for suitable right Ore domains R.

1·3. One application will serve to illustrate Theorem C. It seems not to have been noticed that characteristically simple groups may have non-isomorphic simple quotient groups. We show that *a countable characteristically simple group may have* $2^{\aleph_0}$ *isomorphism classes of simple quotient groups*. Let R be the ring of polynomials over the rational field $\mathbb{Q}$ in commuting indeterminates $x_1, x_2, \ldots, x_n, \ldots$; then R is a characteristically simple ring, and, by Theorem C, $\mathrm{PE}_3(R)$ is a characteristically simple group. Moreover $\mathrm{PE}_3(R)$ is obviously countable. On the other hand, every countable field K of characteristic zero is a homomorphic image of R, and a homomorphism from R onto K induces in an obvious way a group homomorphism from $\mathrm{PE}_3(R)$ onto $\mathrm{PE}_3(K)$. But $\mathrm{E}_3(K) = \mathrm{SL}_3(K)$ and $\mathrm{PSL}_3(K)$ is simple (see Artin (1), chapter 4), and, by Satz 2 of Schreier and van der Waerden (16), non-isomorphic fields K_1 and K_2 yield non-isomorphic groups $\mathrm{PSL}_3(K_1)$ and $\mathrm{PSL}_3(K_2)$. Because there are $2^{\aleph_0}$ non-isomorphic countable fields of characteristic zero, it follows that $\mathrm{PE}_3(R)$ has $2^{\aleph_0}$ isomorphism classes of simple homomorphic images.

A countable group satisfying the maximal condition for normal subgroups can have only countably many isomorphism classes of simple homomorphic images, because each of its normal subgroups is the normal closure of a finite subset. We shall see below that countable characteristically simple groups with the maximal condition for normal subgroups may have $\aleph_0$ non-isomorphic simple homomorphic images, and that, at the other extreme, they may have all of their simple homomorphic images isomorphic, while still failing to be direct powers of simple groups. We do not know whether or not the simple homomorphic images of a finitely generated characteristically simple group can fall into $2^{\aleph_0}$ isomorphism classes.

1·4. It may be as well to mention that none of the phenomena discussed in sections 1·1 and 1·3 can arise for characteristically simple groups having *finite* simple homomorphic images. Let G be such a group, with finite simple quotient group $H = G/M$. The images of M under the automorphisms of G must have trivial intersection, so that G and H generate the same variety of groups. Because finitely generated free groups have only finitely many subgroups of index $|H|$, it follows that if G is finitely generated, then G is finite. The same conclusion holds if G satisfies the maximal condition for normal subgroups (cf. corollary 2 of Wilson (19)). Whether or not G is finite, theorem 4 of Kovács and Newman (10) shows that all simple homomorphic images of G are isomorphic to H.

The group G actually has a very restricted structure. It is an easy consequence of lemma 3·2 of Kovács and Newman (10) that each finitely generated subgroup of G is contained in a subgroup of G isomorphic to a finite direct power of H. In the terminology of Neumann and Yamamuro (14), G is a Boolean power of H. However G need not itself be a direct power of H.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

1·5. A survey of the literature on characteristically simple groups reveals a striking variety of apparently very dissimilar constructions. However some of the constructions do share one common feature: their use of an algebraic system other than a group, whose automorphisms induce the important group automorphisms. In the cases of McLain's characteristically simple groups (studied in (12) and (13)) and the wreath powers of Hall (7), the algebraic system is a linearly ordered set. Some of the Boolean powers of (characteristically) simple groups, introduced in Neumann and Yamamuro (14) and further discussed by Philip Hall in lectures and in (8), may be proved to be characteristically simple by considering ring automorphisms of an underlying Boolean ring. Finally, of course, our examples based on the functor $\mathrm{PSL}_n(-)$, and similar ones based on other 'Chevalley' functors, depend on ring automorphisms. It seems likely that there will be more constructions for characteristically simple groups, yielding groups with widely disparate properties, and sharing this feature.

2. *Proof of Theorem B and Theorem C*

2·1. It is not difficult to prove that certain groups associated with polynomial rings over infinite fields are characteristically simple, and we shall therefore do this, and deduce Theorem B, before considering more general rings. First we collect some known facts.

LEMMA 1. *Let R be any ring and Ω any index set with at least two elements.*
(*a*) *If $\Omega \times \Omega$ matrices e and f satisfy*

$$e^2 = f^2 = fe = 0,$$

then $1+e$ and $1+f$ are invertible, and

$$[1+e, 1+f] = 1+ef.$$

(*b*) *For all a and b in R and for i, j, k and l in Ω,*

$$[1+ae_{ij}, 1+be_{kl}] = \begin{cases} 1 \text{ if } i,j,k,l \text{ are distinct, and} \\ 1+abe_{il} \text{ if } j = k \text{ and } i,j,l \text{ are distinct.} \end{cases}$$

(*c*) *For all a and b in R and for distinct i and j in Ω,*

$$(1+ae_{ij})(1+be_{ij}) = 1+(a+b)e_{ij}.$$

This is elementary; of course (*b*) is a special case of (*a*).

LEMMA 2. (*a*) *For each Euclidean domain A and integer $n \geqslant 3$, $\mathrm{E}_n(A) = \mathrm{SL}_n(A)$.*
(*b*) *For each ring R and integer $n \geqslant 3$, the group $\mathrm{E}_n(R)$ contains all $n \times n$ monomial matrices with non-zero entries ± 1 and with determinant 1, and the normal closure in $\mathrm{E}_n(R)$ of a matrix $1+r_0e_{lm}$ with $l \neq m$ contains all matrices $1+r_0e_{ij}$ with $i \neq j$.*

We have already mentioned the well known result (*a*) of Litoff (11); a much more general result is proved in theorem V.4.1 of Bass (2). The first assertion of (*b*) follows easily, on taking for A the ring of integers, and the second assertion is a straightforward consequence of the first.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

For the next lemma we need some notation for certain normal subgroups of $\mathrm{E}_\Omega(R)$, where R is a Euclidean domain. We suppress reference to the index set Ω, and, for each ideal I of R, we write C_I and Z_I respectively for the inverse images of the identity and the centre of $\mathrm{E}_\Omega(R/I)$ under the homomorphism from $\mathrm{E}_\Omega(R)$ induced by the ring homomorphism $R \to R/I$, and we write P_I for the normal subgroup of $\mathrm{E}_\Omega(R)$ generated by all matrices $1 + re_{ij}$ with $r \in I$ and $i \neq j$.

LEMMA 3. *If R is a Euclidean domain and if $|\Omega| \geqslant 3$, then*

(*a*) *for each normal subgroup N of $\mathrm{E}_\Omega(R)$ there is an ideal I of R such that*

$$P_I \leqslant N \leqslant Z_I,$$

and

(*b*) *for each ideal I and each integer $m > 0$, the mth term of the lower central series of C_I is contained in C_{I^m}.*

The first assertion follows from Lemma 2(*b*) and the case in which Ω is finite, and this is essentially proved in Brenner (4) (though stated there only for the ring of integers); again there are more general results (cf. Bass (2), theorem V.4.1 and Wilson (20), corollary 1). Assertion (*b*) is the result of a simple computation.

We may now prove

PROPOSITION 1. *Let K be an infinite field and Ω an index set with $|\Omega| \geqslant 3$. Then*

(*a*) $\mathrm{PE}_\Omega(K[x])$ *is characteristically simple, and*

(*b*) $\mathrm{PE}_\Omega(K[x])$ *is directly indecomposable and has a maximal normal subgroup which is residually nilpotent and which is not finitely generated.*

In particular, these assertions hold for $\mathrm{PSL}_n(K[x])$ for $n \geqslant 3$.

Proof. The final statement here follows from the earlier ones by virtue of Lemma 2.

(*a*) Let N be the preimage in $\mathrm{E}_\Omega(K[x])$ of a non-trivial characteristic subgroup of $\mathrm{PE}_\Omega(K[x])$; then N is normal in $\mathrm{E}_\Omega(K[x])$. Since N does not lie in the centre of $\mathrm{E}_\Omega(K[x])$, we may conclude from Lemma 3 that N contains a matrix $1 + f(x)e_{ij}$ with $i \neq j$ and with $0 \neq f(x) \in K[x]$. Choose such a matrix with $f(x)$ having degree (as a polynomial in x) as small as possible. For each $k \in K$, the automorphism of $K[x]$ fixing each element of K and mapping x to $x + k$ induces an automorphism of

$$\mathrm{PE}_\Omega(K[x]).$$

Thus N contains both $1 + f(x+k)e_{ij}$ and

$$(1 + f(x+k)e_{ij})(1 + f(x)e_{ij})^{-1} = 1 + (f(x+k) - f(x))e_{ij}.$$

By choice of $f(x)$, it follows that $f(x+k) - f(x) = 0$ for each $k \in K$. But the coefficient of degree zero in $f(x+k) - f(x)$ is $f(k) - f(0)$. Because K is infinite, the polynomial equation $f(x) - f(0) = 0$ therefore has infinitely many roots, so that $f(x) = f(0) \in K$. It follows that the ideal I of $K[x]$ for which $P_I \leqslant N \leqslant Z_I$ contains elements of K, and so must be $K[x]$. Therefore $N = \mathrm{E}_\Omega(K[x])$, and $\mathrm{PE}_\Omega(K[x])$ is characteristically simple.

(*b*) Let N_1 and N_2 be preimages in $\mathrm{E}_\Omega(K[x])$ of non-trivial normal subgroups of $\mathrm{PE}_\Omega(K[x])$; then

$$P_{I_1} \leqslant N_1 \quad \text{and} \quad P_{I_2} \leqslant N_2,$$

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

for non-zero ideals I_1 and I_2 of $K[x]$. Writing $I_3 = I_1 \cap I_2$, we have $I_3 \neq 0$ and

$$P_{I_3} \leqslant P_{I_1} \cap P_{I_2} \leqslant N_1 \cap N_2;$$

and $N_1 \cap N_2$ is not central in $\mathrm{E}_\Omega(K[x])$. Therefore $\mathrm{PE}_\Omega(K[x])$ is directly indecomposable.

Any element of the centre Z of $\mathrm{E}_\Omega(K[x])$ is an invertible scalar matrix; thus $Z \leqslant \mathrm{E}_\Omega(K)$ and Z is the centre of $\mathrm{E}_\Omega(K)$. Let I be the ideal of $K[x]$ generated by x. Since (by Lemma 3, for instance) $\mathrm{E}_\Omega(K[x])/Z_I$ is simple, Z_I/Z is a maximal normal subgroup of $\mathrm{PE}_\Omega(K[x])$. The image of any element $g(x)$ of Z_I under the homomorphism induced by the ring homomorphism from $K[x]$ to K mapping x to 0 is an element $g(0)$ of the centre of $\mathrm{E}_\Omega(K)$; and $g(0)^{-1}g(x) \in C_I$. Therefore $Z_I = C_I Z$, and obviously also $C_I \cap Z = 1$, so that Z_I/Z is isomorphic to C_I. It follows from Lemma 3(*b*) that Z_I/Z is residually nilpotent. Further, for arbitrary distinct l and m in Ω, the subgroup of matrices $1 + re_{lm}$ with $r \in I$ has image in the Abelian group C_I/C_{I^2} isomorphic to the additive group of I/I^2, so that neither C_I/C_{I^2} nor Z_I/Z can be finitely generated.

This concludes the proof of Proposition 1.

2·2. Next we derive a sufficient condition on a field K for all proper homomorphic images of groups $\mathrm{PE}_\Omega(K[x])$ for suitable Ω to have finite chief series. We need more precise information about normal subgroups than is given by Lemma 3; we shall use

LEMMA 4. *Let K be an absolutely algebraic field of prime characteristic p, and let Ω be an index set with $|\Omega| \geqslant 3$. Suppose that $|\Omega|$ is either infinite or coprime to p. Then for each ideal I of $K[x]$ we have*

(*a*) $P_I = C_I$, *and*

(*b*) Z_I/P_I *is finite.*

Proof. If K is finite, then (*a*) is a special case of the deep results theorem 3·6 and theorem 4·1 of Bass, Milnor and Serre (3). If K is infinite, and if there were an element $g \in C_I \backslash P_I$, then, writing F for the (finite) field generated by the coefficients of the entries of the matrix g, we would have strict inequality of the normal subgroups

$$C_{I \cap F[x]} \quad \text{and} \quad P_{I \cap F[x]}$$

of $\mathrm{E}_\Omega(F[x])$, contradicting the results from (3) mentioned above.

If $|\Omega|$ is infinite, then $Z_I = C_I$, since elements of Z_I are congruent to scalar matrices modulo C_I and differ from the identity matrix in only finitely many entries. Thus if $|\Omega|$ is infinite, Z_I/P_I is actually trivial. Suppose that $|\Omega| = n$ is finite; then, by (*a*), Z_I/P_I is isomorphic to a group of elements t of $K[x]/I$ satisfying $t^n = 1$. However it is easy to verify that the group of nth roots of 1 in $K[x]/I$ is finite, since, by hypothesis, p does not divide n.

PROPOSITION 2. *Let K be an absolutely algebraic field of prime characteristic p, and let Ω be any index set with $|\Omega| \geqslant 3$ and with $|\Omega|$ either infinite or coprime to p. Then, for each non-central normal subgroup N of $\mathrm{E}_\Omega(K[x])$, the group $\mathrm{E}_\Omega(K[x])/N$ has a finite chief series. In particular, every proper homomorphic image of $\mathrm{PE}_\Omega(K[x])$ has a finite chief series.*

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

Proof. By Lemma 3, it is sufficient to show that $\mathrm{E}_\Omega(K[x])/P_I$ has a finite chief series for each non-zero ideal I. Now all chains of ideals containing I are finite. Let

$$I = I_0 < I_1 < \ldots < I_m = K[x]$$

be a maximal such chain. We assert that each factor of the chain

$$P_{I_0} \leqslant Z_{I_0} \cap P_{I_1} \leqslant P_{I_1} \leqslant Z_{I_1} \cap P_{I_2} \leqslant \ldots \leqslant Z_{I_{m-1}} \leqslant \mathrm{E}_\Omega(K[x])$$

of normal subgroups is either finite or a chief factor of $\mathrm{E}_\Omega(K[x])$; the conclusion of Proposition 2 follows immediately from this assertion. The finiteness of the factors

$$Z_{I_r} \cap P_{I_{r+1}}/P_{I_r}$$

follows from Lemma 4. Suppose that the normal subgroup N_1 of $\mathrm{E}_\Omega(K[x])$ satisfies

$$Z_{I_r} \cap P_{I_{r+1}} \leqslant N_1 \leqslant P_{I_{r+1}}$$

for some r. By Lemma 3, we have

$$P_J \leqslant N_1 \leqslant Z_J$$

for some ideal J. Thus $P_J \leqslant N_1 \leqslant P_{I_{r+1}}$, and $J \leqslant I_{r+1}$;

on the other hand, $P_{I_r} \leqslant N_1 \leqslant Z_J$, so that $I_r \leqslant J$.

Therefore either $J = I_r$ and $N_1 = Z_{I_r} \cap P_{I_{r+1}}$,

or $J = I_{r+1}$ and $N_1 = P_{I_{r+1}}$.

Our assertion follows, and Proposition 2 is proved.

It is an easy matter to deduce Theorem B from Propositions 1 and 2. Indeed these show that, for any infinite absolutely algebraic field K of characteristic p and any index set Ω with $|\Omega|$ not less than 3 and, if finite, coprime to p, the group $\mathrm{PE}_\Omega(K[x])$ has all of the properties (a), (b), (c) and (d) of Theorem B; and, if $|\Omega|$ is infinite, then the cardinality of $\mathrm{PE}_\Omega(K[x])$ is equal to $|\Omega|$.

To complete the proof of Theorem B, it will suffice to show that there are $2^{\aleph_0}$ isomorphism classes of groups $\mathrm{SL}_3(K[x])$ where K is an infinite absolutely algebraic field of characteristic not equal to 3 having no cube roots of 1 except 1. Now there are $2^{\aleph_0}$ isomorphism classes of fields K having these properties. Suppose that for two such fields K_1 and K_2 we have $\mathrm{SL}_3(K_1[x]) \cong \mathrm{SL}_3(K_2[x])$. The simple quotient groups of $\mathrm{SL}_3(K_1[x])$ are, by Lemma 3, the groups $\mathrm{SL}_3(K_1[x])/Z_I$ with I a maximal ideal of $K_1[x]$, and therefore are isomorphic to the groups $\mathrm{PSL}_3(L)$ with L a finite (simple) extension of K_1. But, by Satz 2 of Schreier and van der Waerden (16), non-isomorphic fields L give rise to non-isomorphic groups $\mathrm{PSL}_3(L)$. It follows that each of K_1 and K_2 is isomorphic to a finite extension of the other, and that $K_1 \cong K_2$.

We note that the characteristically simple group $\mathrm{PSL}_3(K[x])$, with K an infinite absolutely algebraic field, has just one isomorphism class or $\aleph_0$ isomorphism classes of simple homomorphic images according as K is or is not algebraically closed.

2·3. We now turn to more general characteristically simple rings and associated matrix groups. We remind the reader that all rings considered are assumed to have an identity element. First we prove

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

PROPOSITION 3. *Let $R = S[x_\lambda; \lambda \in \Lambda]$ be the polynomial ring over the ring S in indeterminates x_λ which commute with each other and with S. If S is a characteristically simple ring and is an algebra over an infinite field K, then R is a characteristically simple ring.*

Proof. Let I be a non-zero ideal of R invariant under all automorphisms of R, and let $0 \neq f \in I$. Then

$$f \in S[x_{\lambda_1}, \ldots, x_{\lambda_n}]$$

for some finite set $\{x_{\lambda_1}, \ldots, x_{\lambda_n}\}$. But any automorphism of

$$R_1 = S[x_{\lambda_1}, \ldots, x_{\lambda_n}]$$

may be extended to an automorphism of R fixing each $x_\lambda \notin \{x_{\lambda_1}, \ldots, x_{\lambda_n}\}$, so that $I \cap R_1$ is a non-trivial ideal of R_1 invariant under all automorphisms of R_1. Thus if Proposition 3 holds for the case in which Λ is finite, it will follow that $1 \in I \cap R_1$ and that $I = R$. It is therefore sufficient to consider the case in which Λ is finite, and indeed, by a trivial induction argument, the case in which Λ has just one element.

Suppose then that I is a non-zero ideal of $R = S[x]$ invariant under all automorphisms of R, and let

$$f(x) = \sum_{r=0}^{n} x^r a_r$$

be a non-zero element of I with minimal degree n. For each $k \in K \setminus 0$ there is an automorphism of R fixing each element of S and mapping x to kx; thus $k^n f(x) - f(kx)$ lies in I. It follows from our choice of $f(x)$ that

$$k^n f(x) - f(kx) = 0, \quad \text{and that} \quad (k^n - k^r) a_r = 0$$

for $r < n$. Since K is infinite, for each $r < n$ there is a $k \in K$ for which $k^n - k^r$ does not vanish. Therefore $a_r = 0$ for $r < n$, and $f(x) = x^n a_n$. But now, considering the automorphism of R fixing each element of S and mapping x to $x + 1$, we see that I contains $f(x+1) - f(x)$; and if $n > 0$, this has degree less than n and has coefficient of degree zero a_n, so is non-zero. Therefore $n = 0$ and $f(x) \in S$. Because each automorphism of S extends to an automorphism of R, it follows that $I \cap S$ is a non-zero ideal of S invariant under all automorphisms of S. Hence $1 \in I$ and $I = R$. Proposition 3 is therefore proved.

2·4. The proof of Theorem C under the hypothesis that the index set Ω is infinite is an easy application of theorem V.2.1 of Bass (2). This theorem asserts, among other things, that if N is a normal subgroup of $\mathrm{E}_\Omega(R)$, where R is any ring and Ω is the set of positive integers, and if I is the ideal of R generated by all h_{ij} with $i \neq j$ and all $h_{ii} - h_{jj}$ with $h = (h_{ij}) \in N$, then N contains all matrices $1 + re_{ij}$ with $r \in I$ and with $i \neq j$. The extension of this result to the case in which Ω is an arbitrary infinite index set is elementary.

Now suppose that R is characteristically simple, and that N above is a characteristic subgroup of $\mathrm{E}_\Omega(R)$. Because every automorphism of R induces an automorphism of $\mathrm{E}_\Omega(R)$, the ideal I is invariant under all automorphisms of R, so that $I = 0$ or $I = R$; in the former case $N = 1$ and in the latter case $N = \mathrm{E}_\Omega(R)$. The conclusion of Theorem C follows.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

For the proof of Theorem C under the alternative hypothesis we need

LEMMA 5. *Suppose that for each ordered pair (a, b) of elements of the ring R with $a \neq 0$ there is a pair (x, y) with $y \neq 0$ and with $ax + by = 0$. If $n \geqslant 3$ and if N is a normal subgroup of $\mathrm{E}_n(R)$ not lying in the centre Z of $\mathrm{E}_n(R)$, then N contains a matrix $1 + r_0 e_{lm}$ with $0 \neq r_0 \in R$ and with $l \neq m$.*

Proof. We proceed in a number of steps. If a is an $n \times n$ matrix over R, a_{ij} will as usual denote the entry in its ith row and jth column.

First we note that N contains non-diagonal matrices: if $h \in N \setminus Z$ and if h is a diagonal matrix, then $h_{rr} \neq h_{ss}$ for some r and s, and $(1 - e_{rs})\, h (1 + e_{rs})$ is a non-diagonal element of N. For definiteness, we suppose that there is an element $h \in N$ with $h_{21} \neq 0$.

We assert that there is a matrix $p \in N \setminus Z$ with $p_{21} = 0$ and $p_{22} = 1$. For let h be as above with $h_{21} \neq 0$, and let $k = h^{-1}$. Because of the hypothesis on R we may solve the equation

$$h_{21} x_1 + h_{22} x_2 = 0,$$

with $x_2 \neq 0$. Let $\quad a = (1 + x_1 e_{13})(1 + x_2 e_{23}) = 1 + x_1 e_{13} + x_2 e_{23}.$

Then N contains $\quad p = h a^{-1} k a = a - (h x_1 e_{13} + h x_2 e_{23})\, k a.$

The matrix in brackets here has its second row zero; thus $p_{2j} = a_{2j}$ for each j, so that $p_{21} = 0$ and $p_{22} = 1$. But $p \notin Z$ since

$$p_{23} = x_2 \neq 0.$$

We next show that there is a matrix $b \in N \setminus Z$ with $(b - 1)_{i1} = 0$ for all i. Let p be as in the previous paragraph and let $q = p^{-1}$. If $(q - 1)_{i1} = 0$ for all i, we set $b = q$. Otherwise we define

$$b = [p, 1 + e_{12}] = 1 + e_{12} - q e_{12} p.$$

Clearly $b \in N$ and $(b - 1)_{i1} = 0$ for each i; and since

$$(b - 1)_{i2} = \delta_{i1} - q_{i1}$$

is non-zero for some i, we have $b \notin Z$.

Now we prove that there is a matrix $c \in N \setminus Z$ differing from the identity matrix only in its first row, and having $c_{11} = 1$. We may assume that b does not already have this property, so that $b_{rs} \neq \delta_{rs}$ for some $r > 1$ and some s. We define

$$c = [b, 1 + e_{1r}] = 1 + e_{1r} - (b^{-1})\, e_{1r} b.$$

Then $c \in N$. Because $\quad (b^{-1})_{i1} = b_{i1} = \delta_{i1}$

for each i, c differs from the identity matrix only in its first row, and $c_{11} = 1$. Moreover $c \notin Z$, because

$$c_{1s} = \delta_{rs} - b_{rs} \neq 0.$$

Finally, let c be as chosen above with $c_{1s} \neq 0$, and let t be an integer different from 1 and s with $t \leqslant n$. Then N contains

$$[1 + e_{st}, c^{-1}] = 1 - e_{st} + (1 - e_{st})\, c e_{st} c^{-1} = 1 - e_{st} + c e_{st} = 1 + c_{1s} e_{1t}.$$

This concludes the proof of Lemma 5.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

We now resume the proof of Theorem C. The hypothesis is that R is a characteristically simple ring such that for every ordered pair (a, b) of elements of R with $a \neq 0$ there is a pair (x, y) with $y \neq 0$ and with $ax + by = 0$, and that Ω is a finite index set with at least three elements; we have to show that the group $\mathrm{PE}_\Omega(R)$ is characteristically simple.

Let N be the preimage in $\mathrm{E}_\Omega(R)$ of a non-trivial characteristic subgroup of $\mathrm{PE}_\Omega(R)$. By Lemma 5, N contains a matrix $1 + r_0 e_{lm}$ with $0 \neq r_0 \in R$ and with l and m distinct; and from Lemma 2, $1 + r_0 e_{ij} \in N$ for all distinct i and j. It follows easily from Lemma 1 that the set I of elements $r \in R$ such that $1 + re_{ij} \in N$ for all distinct i and j is a non-zero ideal of R. Since each automorphism of R induces an automorphism of $\mathrm{PE}_\Omega(R)$, I is invariant under all automorphisms of R, so that $I = R$. Therefore $N = \mathrm{E}_\Omega(R)$, and the proof of Theorem C is finished.

An argument similar to the one above, again invoking Lemma 5, establishes

PROPOSITION 4. *If R is a simple right Ore ring, then $\mathrm{PE}_n(R)$ is simple for all $n \geqslant 3$.*

The corresponding assertion for infinite index sets (with no restriction on R apart from simplicity) was proved in Robertson (15).

3. *Finitely generated groups: Theorem A*

3·1. For any finitely generated ring R, generated (as a ring with identity) by elements $x_1, \ldots, x_r$, and for any integer $n \geqslant 3$, the group $\mathrm{E}_n(R)$ is finitely generated, with generating set

$$\{1 + x_k e_{ij}; 1 \leqslant k \leqslant r, i \neq j\} \cup \{1 + e_{ij}; i \neq j\}.$$

This is an immediate consequence of Lemma 1. However there are generating sets with a smaller number of elements, and indeed we have

PROPOSITION 5. *If the ring R can be generated by r elements, then $\mathrm{E}_n(R)$ is a 2-generator group for $n \geqslant r + 4$. Moreover, if R is generated by elements $x_1, \ldots, x_r$ with $r \geqslant 2$ and with $x_1 x_r = 1$, then $\mathrm{E}_n(R)$ is a 2-generator group for $n \geqslant r + 2$.*

Proof. The first statement above follows from the second.

In proving the second statement, we may assume that $n \geqslant 3$, so that, by Lemma 2, $\mathrm{E}_n(R)$ contains a monomial matrix π with $\pi_{ij} = 1$ whenever $j = i + 1$ and with $\pi_{n1} = \pm 1$. $\mathrm{E}_n(R)$ also contains each of the matrices

$$1 + x_k e_{1,2+k} \quad (k \leqslant r - 1)$$

and

$$1 + x_r e_{2,n-1},$$

and so contains their product

$$g = 1 + \sum_{k=1}^{r-1} x_k e_{1,2+k} + x_r e_{2,n-1}.$$

Now $\pi^{-1} g \pi$ is of form

$$1 + \sum_{k=1}^{r-1} \epsilon_k x_k e_{2,3+k} + \epsilon_r x_r e_{3n}$$

where $\epsilon_k = \pm 1$ for $1 \leqslant k \leqslant r$, and

$$(g - 1)^2 = (\pi^{-1} g \pi - 1)(g - 1) = 0.$$

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

Therefore, by Lemma 1(*a*), the subgroup H of $\mathrm{E}_n(R)$ generated by π and g contains

$$k = [g, \pi^{-1}g\pi] = 1 \pm e_{1n}.$$

Repeated conjugation of k by π and use of Lemma 1(*b*) shows that H contains all matrices $1 + e_{ij}$ with $i \neq j$. Further, H contains

$$[g, 1 + e_{2+k,n}] = 1 + x_k e_{1n}$$

for $1 \leqslant k \leqslant r-1$, and therefore contains all $1 + x_k e_{ij}$ with $i \neq j$ and with $k \leqslant r-1$. Finally, H contains

$$\left(\prod_{k=1}^{r-1} (1 - x_k e_{1,2+k})\right) g = 1 + x_r e_{2,n-1},$$

and so contains all $1 + x_r e_{ij}$ with $i \neq j$. It now follows easily that $H = \mathrm{E}_n(R)$, and the Proposition is proved.

We remark that the nth power of the matrix π above is either the identity matrix or its additive inverse, while no smaller power of π is a diagonal matrix, so that $\mathrm{PE}_n(R)$ is in fact generated by an element of order n and an element whose order is equal to the characteristic of R if this is finite, and is otherwise infinite.

3·2. We shall construct some rings R which yield 2-generator characteristically simple groups $\mathrm{PE}_n(R)$. Each of these will be a polynomial ring $R = S[x]$ in a (commuting) indeterminate x over a ring S having the following properties:

(*a*) S is a simple ring with centre a field of characteristic zero,

(*b*) S is a right Ore domain, and

(*c*) S is generated by four elements z_0, u, t and $(z_0 ut)^{-1}$.

It follows from (*a*) and Proposition 3 that R is characteristically simple. Since S is a right Ore domain, so is R (cf. Lemma 6 below); thus Theorem C is applicable, and $\mathrm{PE}_n(R)$ is a characteristically simple group for $n \geqslant 3$. Finally, Proposition 5 and condition (*c*) imply that $\mathrm{PE}_n(R)$ is a 2-generator group for $n \geqslant 8$.

The notation which we now introduce will be maintained throughout sections 3·2 and 3·3.

Let L be the ring $\qquad \mathbb{C}[z_i, z_i^{-1}; i \in \mathbb{Z}]$

of polynomials over the complex field $\mathbb{C}$ in indeterminates z_i and their inverses, where $\mathbb{Z}$ denotes the ring of integers. We define automorphisms t and u of L, fixing each element of $\mathbb{C}$, as follows:

$$z_i^t = z_{i+1}, \quad (z_i^{-1})^t = z_{i+1}^{-1}$$

and

$$z_i^u = z_i c_i, \quad (z_i^{-1})^u = (z_i c_i)^{-1}$$

for each i, where

$$c_i = 1 \quad \text{for} \quad i < 0,$$

$$c_0 = 2,$$

c_{2i-1} is the ith rational prime for $i > 0$,

and where the remaining complex numbers c_i are chosen arbitrarily subject to the condition that

$$\mathbb{Z}[c_i, c_i^{-1}; i \in \mathbb{Z}] = \mathbb{Q}[c_{2i}, c_{2i}^{-1}; i > 0]$$

be a field.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

For each integer r, we define $u_r = t^{-r}ut^r$; then $z_i^{u_r} = z_i c_{i-r}$ for every i. It follows that $u_r u_s = u_s u_r$ for all r and s. It is also easy to see that $\langle u_r; r \in \mathbb{Z}\rangle$ is a free Abelian group with basis $\{u_r; r \in \mathbb{Z}\}$, so that the group W generated by u and t is in fact the wreath product of $\langle u\rangle$ by $\langle t\rangle$.

Let T be the ring of finite sums

$$\sum_\alpha w_\alpha l_\alpha \quad (w_\alpha \in W, l_\alpha \in L),$$

with the obvious definition of addition, and with multiplication defined by

$$lw = wl^w \quad (w \in W, l \in L).$$

Thus T is a twisted group ring of W over L. It is easy to check that $\mathbb{C}$ is the centre of T.

We may now define S to be the subring of T generated by the elements z_0, u, t and their inverses, or, equivalently, by z_0, u, t and $(z_0 ut)^{-1}$. Then S satisfies condition (c) above and has centre

$$\mathbb{C} \cap S = \mathbb{Q}[c_{2i}, c_{2i}^{-1}; i > 0],$$

a field of characteristic zero. It remains to show that S is a right Ore domain and is simple. We require

LEMMA 6. (a) *Nested unions of right Ore domains are right Ore domains.*

(b) *If A is a right Ore domain with division ring of right fractions Q, and if A_1 is a ring satisfying $A \leqslant A_1 \leqslant Q$, then A_1 is a right Ore domain.*

(c) *Any skew polynomial ring over a right Ore domain is a right Ore domain.*

The proofs of assertions (a) and (b) of Lemma 6 are trivial, and (c) is proposition **0**.8.4 of Cohn (6).

We use Lemma 6 repeatedly in the proof of

LEMMA 7. *S is a right Ore domain.*

Proof. We write

$$S_1 = L \cap S = (\mathbb{C} \cap S)[z_i, z_i^{-1}; i \in \mathbb{Z}],$$

and for $r \geqslant 1$ we let S_{2r} and S_{2r+1} respectively denote the ring generated by S_1 and the u_k with $-r < k < r$ and the ring generated by S_{2r} and u_r. Then S_1 is a right Ore domain, and since the u_r commute with each other, S_{r+1} is a skew polynomial ring over S_r for each $r \geqslant 1$. Therefore each S_r is a right Ore domain, and so is the union S_ω of the rings S_r. The ring S' generated by S_1 and all elements u_r and their inverses is contained in a division ring of right fractions of S_ω, and so is again a right Ore domain. But now the ring generated by S' and t is a skew polynomial ring over S', and S is contained in its division ring of right fractions. Lemma 7 follows.

LEMMA 8. *S is simple.*

Proof. Let I be a non-zero ideal of S. Then I has non-zero elements expressible as polynomials in t over the ring S' generated by $L \cap S$ and the elements u_r and their inverses. Choose such an element

$$g = \sum_{i=0}^{n} t^i s_i,$$

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

with $s_i \in S'$ for $0 \leqslant i \leqslant n$, and with degree n as small as possible. Thus $s_0 \neq 0$, and we may write

$$s_0 = \sum_\alpha (\prod_j u_j^{\phi_{\alpha j}}) l_\alpha,$$

where each $\phi_{\alpha j}$ is an integer and each l_α is a non-zero element of $L \cap S$. For each α, let l_α be a linear combination of d_α monomials in the z_i and z_i^{-1} over $\mathbb{C} \cap S$. We suppose g chosen further with the following properties:

(i) the number of terms in the sum $\sum_\alpha$ is as small as possible, and

(ii) subject to (i), $\sum_\alpha d_\alpha$ is as small as possible.

Multiplying g on the right by a suitable monomial in the z_i and z_i^{-1}, we may assume that some l_{α_0} is of form $l_{\alpha_0} = c + l'$, with c a non-zero element of $\mathbb{C} \cap S$ and with l' a (possibly zero) linear combination of non-trivial monomials in the z_i and z_i^{-1}. Suppose that not all l_α are in $\mathbb{C} \cap S$, and let k be the largest index for which z_k or z_k^{-1} is involved in some l_α. Then I contains

$$g' = g - u_k^{-1} g u_k.$$

As a polynomial in t, this has degree at most n, and its coefficient of degree zero is

$$s_0 - u_k^{-1} s_0 u_k = \sum_\alpha (\prod_j u_j^{\phi_{\alpha j}}) (l_\alpha - u_k^{-1} l_\alpha u_k).$$

Thus, on passage from g to g', the number in (i) does not increase; and the number in (ii) does decrease, but not to zero, because $u_k^{-1} m u_k = qm$ with $1 \neq q \in \mathbb{Q}$ for each monomial m involving z_k or z_k^{-1} but no z_i or z_i^{-1} with $i > k$, while $u_k^{-1} m u_k = m$ for each m involving no z_i or z_i^{-1} with $i \geqslant k$. Since $g' \neq 0$, a contradiction ensues.

We therefore conclude that

$$s_0 = \sum_\alpha (\prod_j u_j^{\phi_{\alpha j}}) l_\alpha,$$

with each $l_\alpha \in \mathbb{C} \cap S$. Thus s_0 commutes with each u_j, and, for each j, the element $t^{-1}(g - u_j^{-1} g u_j)$ of I is a polynomial of degree less than n. It follows that $g = u_j^{-1} g u_j$ for each j; that is,

$$\sum_{i=0}^{n} t^i s_i = \sum_{i=0}^{n} u_j^{-1} t^i s_i u_j = \sum_{i=0}^{n} t^i u_{i+j}^{-1} s_i u_j.$$

Therefore $s_i = u_{i+j}^{-1} s_i u_j$ for all i and j. Choosing j larger than the indices of all u_k and u_k^{-1} involved in the s_i, and remembering that the monomials in the u_k and u_k^{-1} are linearly independent over L, we conclude that $s_i = 0$ for $i \geqslant 1$.

Therefore $n = 0$, and

$$g = s_0 = \sum_\alpha (\prod_j u_j^{\phi_{\alpha j}}) l_\alpha \in I,$$

where $l_\alpha \in \mathbb{C} \cap S$ for each α and where the sum $\sum_\alpha$ has as few terms as possible. We now suppose that the number of suffices k for which u_k or u_k^{-1} is involved in g is as small as possible, and we suppose that this number is not zero. Let k be the least suffix for which u_k or u_k^{-1} is involved. We may assume that not all terms in the sum $\sum_\alpha$ involve u_k or u_k^{-1}. Now I contains

$$g - z_k^{-1} g z_k = \sum_\alpha (\prod_j u_j^{\phi_{\alpha j}}) l'_\alpha,$$

where $l'_\alpha = 0$ if and only if $\phi_{\alpha k} = 0$; and because this is the case for some but not all of the α, we have another contradiction.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

It follows that none of the u_k or u_k^{-1} is involved in g, so that the sum $\sum_\alpha$ has only one term and g is a unit in S. Therefore $I = S$, and the proof that S is simple is complete.

3·3. We now show that the groups $\mathrm{PE}_n(R)$, with $n \geqslant 8$ and with $R = S[x]$ constructed as above, have all properties required of the groups C in Theorem A. It has already been remarked that these groups are 2-generator groups. We define M to be the kernel of the homomorphism from $\mathrm{PE}_n(R)$ onto $\mathrm{PE}_n(S)$ determined by the ring homomorphism from R to S which maps x to 0; then $\mathrm{PE}_n(S)$ is simple by Proposition 5, and M is a maximal normal subgroup of $\mathrm{PE}_n(R)$. M will play the role of the subgroup M_C in the statement of Theorem A. Both $\mathrm{E}_n(R)$ and $\mathrm{E}_n(S)$ have n-dimensional representations as groups of automorphisms of vector spaces over a division ring of right fractions of R, and condition (d) of Theorem A is satisfied. We treat conditions (a), (b) and (c) of Theorem A in

LEMMA 9. (a) *There is an infinite cyclic extension of* $\mathrm{PE}_n(R)$ *having* $\mathrm{PE}_n(R)$ *as a minimal normal subgroup.*

(b) *M is residually nilpotent but not finitely generated.*

(c) $\mathrm{PE}_n(R)$ *is directly indecomposable.*

Proof. Let θ be the automorphism of $\mathrm{PE}_n(R)$ induced by the ring automorphism of R which fixes each element of S and maps x to $x+1$, and let N be the preimage in $\mathrm{E}_n(R)$ of a non-trivial normal subgroup, contained in $\mathrm{PE}_n(R)$, of the split extension of $\mathrm{PE}_n(R)$ by $\langle\theta\rangle$. By Lemma 5, N contains a matrix $1+f(x)\,e_{ij}$ with $i \neq j$ and $f(x) \neq 0$. We choose such a matrix with $f(x)$ having minimal possible degree as a polynomial in x; then, since N contains

$$(1+f(x+1)\,e_{ij})\,(1+f(x)\,e_{ij})^{-1} = 1+(f(x+1)-f(x))\,e_{ij},$$

we conclude that $f(x)$ has degree zero and lies in S. Repeated use of Lemma 1 and Lemma 2 now shows that $N = \mathrm{E}_n(R)$, and assertion (a) follows.

The proof of (b) proceeds in exactly the same way as the proof of a similar assertion in Proposition 1. M is isomorphic to the subgroup M_1 of $\mathrm{E}_n(R)$ of matrices congruent to 1 modulo the ideal generated by x, and, for each integer r, the rth term of the lower central series of M_1 consists of matrices congruent to 1 modulo the ideal generated by x^r; hence M_1 is residually nilpotent but not finitely generated.

Now let N_1 and N_2 be the preimages in $\mathrm{E}_n(R)$ of two non-trivial normal subgroups of $\mathrm{PE}_n(R)$. By Lemma 5 and Lemma 2(b), there are elements

$$1+f(x)\,e_{ij} \in N_1 \quad \text{and} \quad 1+g(x)\,e_{jk} \in N_2$$

with $f(x) \neq 0$ and $g(x) \neq 0$ and with i, j and k distinct. Therefore $[N_1, N_2]$ contains

$$[1+f(x)\,e_{ij},\, 1+g(x)\,e_{jk}] = 1+f(x)\,g(x)\,e_{ik},$$

which does not lie in the centre of $\mathrm{E}_n(R)$. It follows that $\mathrm{PE}_n(R)$ is directly indecomposable, and the proof of Lemma 9 is finished.

To complete the proof of Theorem A, it only remains to show that the groups $\mathrm{PE}_n(R)$ and the simple homomorphic images $\mathrm{PE}_n(S)$ with $n \geqslant 8$ fall into $2^{\aleph_0}$ isomorphism classes: of course this possibility exists, because the complex numbers c_{2i}

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

with $i > 0$ in the definition of S were left arbitrary subject to the requirement that the centre

$$\mathbb{C} \cap S = \mathbb{Q}[c_{2i}, c_{2i}^{-1}; i > 0]$$

of S be a field, so that there are $2^{\aleph_0}$ non-isomorphic choices for the centre of S. Now it may seem reasonable to suppose that R and S are determined up to isomorphism by $\mathrm{PE}_n(R)$ and $\mathrm{PE}_n(S)$; however we do not need to prove this as there is a more direct approach. We require

LEMMA 10. *Let G be the multiplicative group generated by z_0, u and t, and let B be the multiplicative group generated by all c_i with $i \geqslant 0$.*

(a) B is a subgroup of G, and B contains all elements of G of finite order.

(b) G may be embedded in $\mathrm{PE}_n(S)$ (and therefore in $\mathrm{PE}_n(R)$) for $n \geqslant 4$.

Proof. The normal closure A of z_0 in G contains both

$$z_r = t^{-r} z_0 t^r \quad \text{and} \quad c_r = z_r^{-1} u^{-1} z_r u$$

for each r; thus $B \leqslant G$. It follows from the definition of S that G is a split extension of A by $W = \langle u, t \rangle$, and since W is a wreath product of two infinite cyclic groups, and so is torsion free, all elements of G of finite order lie in A. But the join of B and the free Abelian group $\langle z_r; r \in \mathbb{Z} \rangle$ contains z_0 and is a normal subgroup of G, and so is equal to A. Therefore all elements of G of finite order lie in B, and assertion (a) is proved.

The automorphism of A inverting each element of A commutes with all automorphisms of A, and so extends to an automorphism α of G satisfying

$$z_0^\alpha = z_0^{-1}, \quad u^\alpha = u \quad \text{and} \quad t^\alpha = t.$$

There are endomorphisms β_1 and γ_1 of the wreath product W satisfying

$$u^{\beta_1} = u^{-2}, \quad t^{\beta_1} = 1$$

and

$$u^{\gamma_1} = 1, \quad t^{\gamma_1} = t^{-2};$$

and because G is a split extension of A by W, these extend to endomorphisms β and γ of G satisfying

$$z_0^\beta = z_0^\gamma = 1.$$

We consider the monomorphism ϕ from G into the group of diagonal matrices of $\mathrm{GL}_n(S)$ defined by

$$(g^\phi)_{11} = g, \quad (g^\phi)_{22} = g^\alpha,$$

$$(g^\phi)_{33} = g^\beta, \quad (g^\phi)_{44} = g^\gamma,$$

and

$$(g^\phi)_{ii} = 1 \quad (4 < i < n).$$

Clearly

$$z_0^\phi \in \mathrm{SL}_n(\mathbb{Q}[z_0]) = \mathrm{E}_n(\mathbb{Q}[z_0]) \leqslant \mathrm{E}_n(S),$$

the equality here holding by Lemma 2(a). Similarly $u^\phi \in \mathrm{E}_n(S)$ and $t^\phi \in \mathrm{E}_n(S)$, so that the image of G lies in $\mathrm{E}_n(S)$. Because the image of G is disjoint from the centre of $\mathrm{E}_n(S)$, it follows that G may be embedded in $\mathrm{PE}_n(S)$. This finishes the proof of Lemma 10.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press

It is now easy to prove that the groups $\mathrm{PE}_8(R)$ and the groups $\mathrm{PE}_8(S)$ fall into $2^{\aleph_0}$ isomorphism classes. For any set ϖ of primes, we may choose the c_{2i} with $i > 0$ in such a way that the group $B = \langle c_i; i \geqslant 0 \rangle$ has elements of prime order p if and only if $p \in \varpi$. We may, for instance, take the c_{2i} themselves all to be pth roots of 1 for primes $p \in \varpi$ if ϖ is non-empty. By Lemma 10, the group G then has elements of prime order p if and only if $p \in \varpi$, so that one obtains in this way $2^{\aleph_0}$ non-isomorphic 3-generator groups G as ϖ runs through all sets of primes. Each of these groups G may be embedded in the corresponding groups $\mathrm{PE}_8(R)$ and $\mathrm{PE}_8(S)$. However, since countable groups can have only countably many finitely generated subgroups, only countably many of the groups G may be embedded in any given group $\mathrm{PE}_8(R)$. It follows that the groups $\mathrm{PE}_8(R)$, and the groups $\mathrm{PE}_8(S)$, fall into $2^{\aleph_0}$ isomorphism classes, and our proof of Theorem A is complete.

REFERENCES

(1) Artin, E. *Geometric algebra* (New York and London, Interscience, 1957).

(2) Bass, H. *Algebraic K-theory* (New York and Amsterdam, Benjamin, 1968).

(3) Bass, H., Milnor, J. and Serre, J.-P. Solution of the congruence subgroup problem for SL_n ($n \geqslant 3$) and Sp_{2n} ($n \geqslant 2$). *Inst. Hautes Études Sci. Publ. Math.* **33** (1967), 59–137.

(4) Brenner, J. L. The linear homogeneous group. III. *Ann. of Math.* (2) **71** (1960), 210–223.

(5) Camm, R. Simple free products. *J. London Math. Soc.* **28** (1953), 66–76.

(6) Cohn, P. M. *Free rings and their relations* (London and New York, Academic Press, 1971).

(7) Hall, P. Wreath powers and characteristically simple groups. *Proc. Cambridge Philos. Soc.* **58** (1962), 170–184.

(8) Hall, P. On the embedding of a group in a join of given groups. *J. Austral. Math. Soc.* **17** (1974), 434–495.

(9) Kourov notebook. *Unsolved problems in the theory of groups.* Fourth augmented edition. Academy of Sciences of the U.S.S.R., Siberian Branch, Institute of Mathematics, 1973.

(10) Kovács, L. G. and Newman, M. F. Minimal verbal subgroups. *Proc. Cambridge Philos. Soc.* **62** (1966), 347–350.

(11) Litoff, O. On the commutator subgroup of the general linear group. *Proc. Amer. Math. Soc.* **6** (1955), 465–470.

(12) McLain, D. H. A characteristically-simple group. *Proc. Cambridge Philos. Soc.* **50** (1954), 641–642.

(13) McLain, D. H. *A class of locally nilpotent groups.* Cambridge dissertation, 1956.

(14) Neumann, B. H. and Yamamuro, S. Boolean powers of simple groups. *J. Austral. Math. Soc.* **5** (1965), 315–324.

(15) Robertson, E. F. A remark on the derived group of GL(R). *Bull. London Math. Soc.* **1** (1969), 160–162.

(16) Schreier, O. and van der Waerden, B. L. Die Automorphismen der projektiven Gruppen. *Abh. Math. Sem. Univ. Hamburg* **6** (1928), 303–322.

(17) Tyrer Jones, J. M. Direct products and the Hopf property. *J. Austral. Math. Soc.* **17** (1974), 174–196.

(18) Wilson, J. S. Some properties of groups inherited by normal subgroups of finite index. *Math. Z.* **114** (1970), 19–21.

(19) Wilson, J. S. Groups satisfying the maximal condition for normal subgroups. *Math. Z.* **118** (1970), 107–114.

(20) Wilson, J. S. The normal and subnormal structure of general linear groups. *Proc. Cambridge Philos. Soc.* **71** (1972), 163–177.

https://doi.org/10.1017/S0305004100052622 Published online by Cambridge University Press