Math. Proc. Camb. Phil. Soc. (1997), **122**, 91
Printed in Great Britain

A note on powers in simple groups

By JAN SAXL
Gonville and Caius College, Cambridge
and JOHN S. WILSON
School of Mathematics and Statistics, University of Birmingham

(*Received* 19 *December* 1995; *revised* 25 *April* 1996)

1. *Introduction*

In [**7**], the second author proved that there is an integer k such that every element of a finite non-abelian simple group S is a product of k commutators in S. The motivation for proving this result came from a model-theoretic question about simple groups. The proof depended on the classification of the finite simple groups, a theorem of Malle, Saxl and Weigel[**5**] which shows that in many finite simple classical groups S there is a real conjugacy class R such that $S = R^3 \cup \{1\}$, and an ultraproduct argument. Here we shall use a similar combination of ideas to prove the following result.

Theorem 1. *Let n be a positive integer. There is an integer k, depending only on n, such that each element of each finite simple group S not of exponent dividing n is a product of k nth powers.*

The motivation for this result comes from a question on open subgroups in profinite groups. We shall prove Theorem 1 in Section 2 and describe the application in Section 3.

2. *Proof of Theorem* 1

In this section, n is a fixed integer satisfying $n \geqslant 2$. We begin by proving that all elements are products of two nth powers in alternating groups of high enough degree and in simple classical groups of high enough dimension, except for certain orthogonal groups; and that the elements of these latter groups are products of six nth powers.

Lemma 1. *Each element of the alternating group A_m is a product of two nth powers, provided that $m \geqslant 4n$.*

Proof. Write $m = qn + r$ with $r < n$. Let k be the largest odd number smaller than qn and let g be a k-cycle. Then any conjugate of g is an nth power in A_m, since k is prime to n. Moreover $k > \frac{3}{4}m$, and so the assertion follows from corollary 2·1 of Bertram[**1**].

Lemma 2. *Every element of the linear group $L_d(q)$ is a product of two nth powers, provided that $d > n$ (with $d > 3$, and in fact $d > 7$ if $q = 2$).*

Proof. Let p_1 and p_2 be primitive prime divisors corresponding to $q^d - 1$ and $q^{d-1} - 1$. These are primes bigger than $d - 1$ and hence prime to n. Hence the elements

https://doi.org/10.1017/S030500419600165X Published online by Cambridge University Press

of orders p_1, p_2 are nth powers. Let C_i be the conjugacy class of elements of order p_i. The argument in section 2·1 of [**5**] shows that the set $C_1 C_2 = \{c_1 c_2 \mid c_1 \in C_1, c_2 \in C_2\}$ meets all non-trivial conjugacy classes in $L_d(q)$: to prove this, one uses the usual character formula as in lemma 2·1 of [**5**], observing that, as in proposition 2·1 of [**5**], the only irreducible characters contributing are the unipotent characters; and, finally, theorem 2·1 (a) of [**5**] holds for our classes, since the unipotent characters take equal values on any two regular semisimple elements lying in the same maximal torus. The assertion now follows.

LEMMA 3. *Let S be a simple classical group of dimension d, other than an orthogonal group $\mathrm{P}\Omega_d^+$ with d divisible by 4. If $d \geqslant 2n$ (with $d > 5$, and in fact $d > 13$ if $q = 2$) then every element of S is a product of two nth powers.*

Proof. This is proved exactly as the previous lemma, using the results in sections 2·1–2·4 of [**5**].

LEMMA 4. *Let S be a simple orthogonal group $P\Omega_{4m}^+(q)$, and suppose that $2m > n$ (with $m > 2$, and in fact $m > 3$ if $q = 2$). Then every element of S is a product of six nth powers.*

Proof. It is known that Ω_{4m}^+ has a factorization as $\mathrm{SL}_{2m}\,\Omega_{4m-1}$, where the first factor is the derived subgroup of the Levi subgroup stabilizing a maximal totally isotropic subspace and the second factor stabilizes a non-singular vector (see lemma 2·4 in [**7**]). Write $S = AB$ for the corresponding factorization of the simple group S. The elements of each of the groups $A/Z(A) \cong L_{2m}(q)$ and B are products of two nth powers by Lemma 2 and Lemma 3, and so it suffices to show that every element in $Z(A)$ is the product of two nth powers in S. We use the argument on p. 107 of [**5**]. Take the classes C_1, C_2 as indicated there, so that they certainly consist of nth powers, and replace C_3 by the class of a non-identity element $z \in Z(A)$. We note that $\mathrm{St}(z)$ is positive and that because A is normal in $C_S(z)$ we have $|C_S(z)| < q^{(2m)^2}$, so that the argument applies (note also that $4m > 8$ here).

We must now consider the remaining simple groups. The sporadic groups can clearly be ignored, and the remaining Chevalley groups belong to finitely many Lie types. Therefore Theorem 1 will be established if we prove the following result.

LEMMA 5. *Let X be a (twisted or untwisted) Lie type. There is an integer k_X such that, in each finite group $X(K)$ not of exponent dividing n, every element is a product of k_X nth powers.*

We shall use the following result of F. Point [**6**].

PROPOSITION. *Let $\{X(K_j) \mid j \in J\}$ be a family of finite Chevalley groups of type X, and let $\mathscr{U}$ be a non-principal ultrafilter on the set J. Then $\Pi_{j\in J} X(K_j)/\mathscr{U} \cong X(\Pi_{j\in J} K_j/\mathscr{U})$.*

We shall also use the fact that if K is a pseudofinite field (in particular, if K is an ultraproduct of finite fields) then $X(K)$ is simple. In fact, $X(K)$ is simple for every infinite field K; for $X \neq {}^2G_2$, this follows from theorems 11·1·2 and 14·4·1 in [**2**], but some extra arguments are needed when $X = {}^2G_2$. The simplicity of ${}^2G_2$ when $|K| > 3$ and each element of K is either a square or minus a square follows from the argument of theorems 13·7·4 and 14·4·1 in [**2**] together with the argument on p. 313 in [**2**]; evidently every pseudofinite field K of characteristic 3 has the above property.

https://doi.org/10.1017/S030500419600165X Published online by Cambridge University Press

Now suppose that the conclusion of Lemma 5 is false. Then for each integer $d > 0$ there is a finite field E_d such that the exponent of $X(E_d)$ does not divide n and such that $X(E_d)$ has an element g_d which is not a product of d nth powers. Let $\mathscr{U}$ be a non-principal ultrafilter on $\mathbb{N}$, write $G = \Pi_{d\in\mathbb{N}} X(E_d)/\mathscr{U}$ and let g be the image of the sequence (g_d) in G. Clearly g is not a product of nth powers in G. However, by the proposition above we have $G \cong X(K)$ where $K = \Pi_{d\in\mathbb{N}} E_d/\mathscr{U}$, so that G is a non-abelian simple group. It follows that the subgroup generated by the nth powers in G is trivial. We conclude from Los' theorem (see, for example Eklov [**3**]) that $X(E_d)$ has exponent dividing n for all d in a set belonging to $\mathscr{U}$, and this is a contradiction.

3. *Open subgroups in profinite groups*

If G is a profinite group, then every open subgroup of G has finite index, since G is compact. Easy examples, for instance infinite profinite groups of exponent 2, show that the converse statement does not hold in general. However, Serre (unpublished) proved that if G is a finitely generated pro-p group, then every subgroup of finite index is open, and the question arises whether subgroups of arbitrary finitely generated profinite groups are open. It was shown by Brian Hartley [**4**] that if G is a finitely generated profinite group which is an inverse limit of finite soluble groups of bounded Fitting length, then every subgroup of finite index is open, and it seems hard to make further progress with prosoluble groups. Theorem 1 gives the same conclusion for finitely generated profinite groups all of whose finite continuous images are products of non-abelian simple groups: such groups are isomorphic to Cartesian products of finite simple groups with the product topology.

THEOREM 2. *Let C be the Cartesian product of a family $\{S_\lambda \mid \lambda\in\Lambda\}$ of non-abelian finite simple groups and suppose that C is finitely generated, regarded as a profinite group. Then every subgroup of finite index in C is open.*

Proof. It suffices to show that every normal subgroup N of finite index is open. Let N have index n and let k be the integer given by Theorem 1. The finite simple groups of exponent dividing n fall into finitely many isomorphism classes, and each such isomorphism class contains only finitely many groups S_λ since the profinite group C is finitely generated. Let $\Lambda_0 = \{\lambda_1, \ldots, \lambda_m\}$ be the set of λ such that S_λ has exponent dividing n, and let K be the kernel of the continuous map from C to $S_{\lambda_1} \times \ldots S_{\lambda_m}$. Thus K is an open normal subgroup isomorphic to the Cartesian product of the family $\{S_\lambda \mid \lambda\in\Lambda\backslash\Lambda_0\}$, and from Theorem 1 it follows that every element of K is a product of k nth powers. Thus every element of K lies in N, so that N is a union of finitely many cosets of K and is therefore open.

The hypothesis of finite generation in Theorem 2 can be weakened a little – all that is required is that each isomorphism class of finite groups contains only finitely many groups S_λ. However, this restriction cannot be lifted. Suppose that infinitely many of the groups S_λ are isomorphic to S. Thus C has as a continuous image the Cartesian product D of groups isomorphic to S and indexed by $\mathbb{N}$. We regard the elements of D as functions from $\mathbb{N}$ to S. Let $\mathscr{U}$ be an ultrafilter on $\mathbb{N}$. Then the set of all functions $f\in D$ such that $f^{-1}(1)\in\mathscr{U}$ is a normal subgroup of D. The quotient group D/L is an ultraproduct of copies of the finite group S and so is isomorphic to S. On the other hand, D is not open unless $\mathscr{U}$ is a principal ultrafilter. The maximal normal subgroups

https://doi.org/10.1017/S030500419600165X Published online by Cambridge University Press

of finite index in D are precisely the subgroups arising from different choices of the ultrafilter $\mathscr{U}$ and these include an abundance of subgroups of finite index which are not open.

REFERENCES

[1] E. BERTRAM. Even permutations as a product of two conjugate cycles. *J. Combinatorial Theory* (*A*) **12** (1972), 368–380.
[2] R. W. CARTER. *Simple groups of Lie type* (John Wiley and Sons, 1972).
[3] P. C. EKLOV. Ultraproducts for algebraists. In *Handbook of mathematical logic* (North-Holland, 1977), pp. 105–138.
[4] B. HARTLEY. Subgroups of finite index in profinite groups. *Math. Z.* **168** (1979), 71–76.
[5] G. MALLE, J. SAXL and T. WEIGEL. Generation of classical groups. *Geom. Dedicata* **49** (1994), 85–116.
[6] F. POINT. Ultraproducts of Chevalley groups, submitted for publication.
[7] J. S. WILSON. On simple pseudofinite groups. *J. London Math. So.* (2) **51** (1995), 471–490.

https://doi.org/10.1017/S030500419600165X Published online by Cambridge University Press