TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 348, Number 1, January 1996

POWERS IN FINITELY GENERATED GROUPS

E. HRUSHOVSKI, P. H. KROPHOLLER, A. LUBOTZKY, AND A. SHALEV

ABSTRACT. In this paper we study the set Γ^n of n^{th}-powers in certain finitely generated groups Γ. We show that, if Γ is soluble or linear, and Γ^n contains a finite index subgroup, then Γ is nilpotent-by-finite. We also show that, if Γ is linear and Γ^n has finite index (i.e. Γ may be covered by finitely many translations of Γ^n), then Γ is soluble-by-finite. The proof applies invariant measures on amenable groups, number-theoretic results concerning the S-unit equation, the theory of algebraic groups and strong approximation results for linear groups in arbitrary characteristic.

1. INTRODUCTION

Let Γ be a finitely generated group and let $n \geq 2$ be an integer. In this paper we write Γ^n for the set of n^{th}-powers in Γ,

$$\Gamma^n := \{x^n | x \in \Gamma\}.$$

While the subgroup $\langle \Gamma^n \rangle$ generated by all n^{th}-powers has been studied thoroughly in various contexts (e.g. the Burnside problem), not much seems to be known about the subset Γ^n. This paper is devoted to the study of groups for which Γ^n is large in some sense.

According to a result of Mal′cev [11], if Γ is finitely generated nilpotent, then Γ^n always contains a subgroup of finite index. Obviously this remains valid for finitely generated nilpotent-by-finite groups.

Note that this property does not characterize nilpotent-by-finite groups; constructions by Guba [5], Rips and others of (highly complicated) finitely generated divisible groups show that even the condition $\Gamma^n = \Gamma$ for all n does not imply virtual nilpotence. However, the situation becomes rather different if one imposes suitable restrictions on Γ.

Our main result establishes a converse to Mal′cev's theorem for two classes of finitely generated groups: the soluble ones, and the linear ones. We shall actually prove a little more. In order to formulate the results, fix a finite set J of integers greater than 1, and let Γ^J denote the union over $n \in J$ of the subsets Γ^n.

Received by the editors January 20, 1995.
1991 *Mathematics Subject Classification.* Primary 20G15, 20F16; Secondary 11D99, 20G40, 43A05.

Theorem A. *Let Γ be a finitely generated soluble-by-finite group. Suppose that, for some finite set J of integers greater than 1, Γ^J contains a finite index subgroup. Then Γ is nilpotent-by-finite.*

Other authors have considered converses to Mal′cev's Theorem. For example Lennox and Wiegold [10] have proved that if Γ is finitely generated and soluble, and there exists an integer c such that, for all n,

$$\langle \Gamma^{n^c} \rangle \subseteq \Gamma^n \tag{1}$$

then Γ is nilpotent. Since $\langle \Gamma^{n^c} \rangle$ is automatically of finite index, it follows from Theorem A that condition (1) for just a single value of n is sufficient to conclude that Γ is nilpotent-by-finite.

Our next result deals with linear groups. Here we weaken our assumption on the set Γ^J of J^{th}-powers. We say that a subset $S \subseteq \Gamma$ *has finite index* in Γ if $\Gamma = TS$ for a suitable finite subset $T \subseteq \Gamma$. For example, this is the case if S contains a coset of a finite index subgroup.

Theorem B. *Let Γ be a finitely generated linear group. Suppose that, for some finite set J of integers greater than 1, Γ^J has finite index in Γ. Then Γ is soluble-by-finite.*

In section 4 we construct an example of a finitely generated soluble linear group Γ in which Γ^n has finite index for almost all n, and yet Γ is not nilpotent-by-finite. However, combining Theorem A and Theorem B we clearly obtain:

Corollary C. *Let Γ be a finitely generated linear group. Suppose that, for some finite set J of integer greater than 1, Γ^J contains a finite index subgroup. Then Γ is nilpotent-by-finite.*

The following is a somewhat surprising consequence:

Corollary D. *Let Γ be a finitely generated group which is either soluble-by-finite or linear. Suppose that there exists $n \geq 2$ such that Γ^n contains a finite index subgroup. Then Γ^m contains a finite index subgroup for all m.*

The proofs of Theorem A and Theorem B are completely different on the one hand, but have a common feature: in both the size of the set Γ^J is 'measured' and shown to be zero in a minimal counterexample Γ; this then contradicts the basic assumption that Γ^J is large.

In Theorem A we use the fact that a soluble group is *amenable*, i.e. admits a finitely additive invariant measure of finite total measure (with respect to which *all* subsets are measurable). As far as we know this is the first use of amenability in proving algebraic results for soluble groups.

We first show, applying suitable results from the theory of infinite soluble groups, that a minimal counterexample to Theorem A is metabelian-by-finite. While we do not necessarily obtain a metabelian counterexample, we are able to construct a metabelian group G admitting a 'nice' measure μ such that $\mu(G^n) > 0$ for some $n \in J$. By replacing G with a minimal quotient which is still not nilpotent-by-finite and analysing its structure, the study of G is reduced to number theoretic questions.

It turns out that the condition $\mu(G^n) > 0$ implies that, for some field k which is a number field or a global field of positive characteristic and some finitely generated

multiplicative subgroup $Q \subset k^*$, the set of solutions to the equation $x + y = 1$ in Q has positive measure.

The final contradiction is now obtained by applying the theory of S-unit equations. Let k be as above and let S be a finite set of primes (valuations) of k. The basic result states that, in the case $\mathrm{char}(k) = 0$, there are only finitely many solutions to the equation $x + y = 1$, where x and y are S-units. See Lang [9] and Evertse [1], [2]. The case $\mathrm{char}(k) = p$ is somewhat different: here $x + y = 1$ implies $x^p + y^p = 1$, so that there are usually infinitely many solutions. This causes some complications in the proof. However, Mason [13] has recently shown that there are only finitely many solutions which are not p^{th}-powers and this turns out to be sufficient for our purposes. The reader is referred to [3] and the books [16], [12] for a detailed account of the interesting theory of S-unit equations and their applications.

In the proof of Theorem B, a different way to measure size of subsets is used. Here, by looking at a minimal counterexample, one can reduce to the case where Γ is a Zariski dense subgroup of $G(R)$ where G is a simply connected simple algebraic group defined over a finitely generated domain R.

Strong approximation results for such linear groups (see Nori [14], Weisfeiler [18] and Hrushovski [8]) imply that there exists a Zariski dense set X of maximal ideals of R such that the image of Γ in $G(R/\pi)$ contains $G^0(R/\pi)$ for all $\pi \in X$, where G^0 is the connected component of G.

Defining the X-topology on $G^0(R)$ as the one generated by the subgroups $G^0(\pi)$ $= \mathrm{Ker}(G(R) \longrightarrow G(R/\pi))$ $(\pi \in X)$, this implies that $\Gamma \cap G^0(R)$ is dense in $G^0(R)$ with respect to that topology. Since $\Gamma = T\Gamma^J$ for some finite set T, we see that $S := G(R)^J \cap G^0(R)$ is dense in some open subset of $G^0(R)$.

On the other hand, using the classification of simple algebraic groups and their automorphisms, we are able to show that S is topologically small; i.e. that S is nowhere dense in $G^0(R)$ with respect to any X-topology. This leads to the desired contradiction, completing the proof of Theorem B.

Finally, we hope that the methods introduced here in studying the set of n^{th}-powers will prove useful in the investigation of other natural subsets of infinite groups.

2. Proof of Theorem A

In all the proofs it is possible to make reductions by passing to a quotient of G, because the hypothesis that G^J is 'large' (in various senses) is inherited by quotients. Since finitely generated nilpotent-by-finite groups are finitely presented, any finitely generated group G which is not nilpotent-by-finite has a just-non-(nilpotent-by-finite) quotient $\overline{G}$; this means that every proper quotient of $\overline{G}$ is nilpotent-by-finite while $\overline{G}$ itself is not.

It is therefore useful to have a description of various types of just-non-nilpotent-by-finite groups, starting with the metabelian case. A very general theory has been developed here (see Robinson and Wilson [15]), and the results we need may be summarised as follows:

Lemma 2.1. *Let G be a finitely generated metabelian group which is just-non-(nilpotent-by-finite). Let A denote the Fitting subgroup of G, and let $Q = G/A$. Then*

(i) *both Q and A are abelian, and $A = C_G(A)$;*

(ii) *either A is torsion-free, or it is an elementary abelian p-group of infinite rank, for some prime p;*

(iii) *if A is torsion-free, then it has finite rank and it possesses a free abelian subgroup A_0 such that A/A_0 is S-torsion for some finite set S of rational primes; if A is an elementary abelian p-group, then it is torsion-free of finite rank qua $\mathbb{F}_p[t]$-module for suitable $t \in Q$, and again it has a free $\mathbb{F}_p[t]$-submodule A_0 such that A/A_0 is S-torsion for a finite set S of primes of $\mathbb{F}_p[t]$.*

(iv) *in both cases the action of Q on A has no unipotent part.*

Moreover, if R denotes $\mathbb{Z}$ in case A is torsion-free, and $\mathbb{F}_p[t]$ in case A is a p-group, and k_0 denotes the field of fractions of R, then

(v) *$k := A \otimes_R k_0$ is a finite field extension of k_0 and G is isomorphic to a subgroup of the split extension of k by k^*, and correspondingly Q is isomorphic to a subgroup of k^*.*

Remarks on the proof. The key point not already amply covered in the literature is that the Fitting subgroup A of G is abelian. Now it is known, and easily shown, that the Fitting subgroup of any finitely generated just-non-polycyclic-by-finite group is abelian; the argument depends on the class of polycyclic-by-finite groups being extension closed. Since every nilpotent-by-finite group is polycyclic-by-finite, it follows that either A is abelian or G is polycyclic-by-finite. But, if G is polycyclic-by-finite and A is non-abelian, then G/A' is nilpotent-by-finite and its Fitting subgroup H/A' is nilpotent. Since H/A' and A are both nilpotent, Hall's Theorem [6] implies that H is, whence G is nilpotent-by-finite. This is a contradiction and so A is abelian in any case. The final assertions on the structure of A originate in Hall's fundamental paper [7], and are also discussed in Groves' work [4]. Clearly Q has no unipotent part in its action on A because this would give rise to a nilpotent subgroup larger than A.

Lemma 2.2. *Let G be a group extension of A by Q, with A, Q abelian. For $g \in G$ and $n \geq 2$, set $T(n, g) = \{q \in Q | q^n = \overline{g}\}$, where $\overline{g}$ denotes the image of g in Q. Then there exist elements $x_q \in A$, such that the set $A \cap g^{-1}G^n$ is equal to*

$$\bigcup_{q \in T(n,g)} x_q A^{q^{n-1}+\ldots+q+1}.$$

Remark. If Q is finitely generated abelian (or more generally nilpotent) then this is a boundedly finite union because the set $T(n, g)$ contains at most $|\tau(Q)|$ elements where $\tau(Q)$ is the torsion subgroup of Q.

Proof. The group extension is completely determined by A, Q, the action of Q on A and a factor set $f : Q \times Q \longrightarrow A$. With these data, every element of G can be expressed uniquely in the form $q \cdot a$ with $q \in Q$ and $a \in A$. Multiplication in G is now given by

$$(q \cdot a)(q' \cdot a') = qq' \cdot \left(f(q, q') a^{q'} a' \right).$$

From this formula we have

$$(q \cdot a)^n = q^n \cdot \left(b(q) a^{q^{n-1}+\ldots+q+1} \right),$$

where $b(q) \in A$ depends only on q and not on a. Thus for each $q \in Q$ the set $\{(q \cdot a)^n | a \in A\}$ is a left coset of $A^{q^{n-1}+\ldots+q+1}$. The result now follows by letting q range over $T(n, g)$. □

In what follows we say that a subset X of an amenable group G is *marginal* if it has measure zero under all invariant measures of G. All measures on groups below will be assumed to be invariant.

Lemma 2.3. *Let Q be a finitely generated abelian group and let $X \subseteq Q$. Suppose X is marginal. Then X^n is marginal for all n.*

Proof. Case 1. Q is torsion-free. Let μ be an invariant measure on Q, and let us show that $\mu(X^n) = 0$. Define a new measure μ' by $\mu'(Y) = \mu(Y^n)$. It is easy to see that μ' is invariant. Furthermore, since Q is torsion-free, $Y \cap Z = \varnothing \Longrightarrow Y^n \cap Z^n = \varnothing$ for all $Y, Z \subseteq Q$, and this implies that μ' is finitely additive. Finally since X is marginal, $\mu'(X) = 0$ and hence $\mu(X^n) = 0$.

Case 2. The general case. Write $Q = R \times F$ where R is torsion-free and F is finite. Note that there is an obvious bijection between measures on Q and measures on R. By identifying R with $\overline{Q} := Q/F$ we also obtain a bijection between measures on Q and measures on $\overline{Q}$. Since X is marginal in Q, $\overline{X} = XF/F$ is marginal in $\overline{Q}$ because if $\overline{\mu}, \mu$ are corresponding measures on $\overline{Q}, Q$ respectively then $\overline{\mu}(\overline{X}) = \mu(XF) \leq |F|\mu(X) = 0$. By case 1, $\overline{X}^n$ is marginal in $\overline{Q}$ so that $X^n F$ is marginal in Q. The result follows since $X^n \subseteq X^n F$. □

Lemma 2.4. *Let k be a finite extension of $\mathbb{F}_p(t)$, and let $u \in k$. Suppose that the equations $x^{p^i} - u = 0$ are all soluble in k. The u is a root of unity.*

Proof. Clear. □

Lemma 2.5. *Let k be as above, and let $B \subset k$ be a finite set. Define $C = \{b^{p^i} : b \in B, i \geq 0\}$. Then $C \cap uC$ is finite, provided $u \in k$ is not a root of unity.*

Proof. We have to show that u can be written only in finitely many distinct ways as $u = b_1^{p^i}/b_2^{p^j}$ where $b_1, b_2 \in B$ and $i, j \geq 0$. Since u is not a root of unity, there exists l such that the equation $x^{p^l} - u = 0$ has no solutions in k. This means that if $u = b_1^{p^i}/b_2^{p^j}$, then either $i < l$ or $j < l$. Suppose $i < l$. Then $b_1^{p^i}$ can have only finitely many values, from which it follows that $b_2^{p^j}$ takes only finitely many values. The argument for the case $j < l$ is similar. □

Proposition 2.6. *Let Q, k be as in Lemma* 2.1. *Let S be a finite set of primes in the ring $\mathcal{O}$ of integers of k. Let $f(X)$ be a polynomial over k with S-unit coefficients, and satisfying $f(0) = 1$. Set*

$$Q_1 := \{q \in Q | \det(f(q)) \text{ is an } S\text{-unit } \},$$

where det *is taken with respect to the embedding of Q in* $\mathrm{End}_{k_0}(k)$. *Then*

(i) *If* $\mathrm{char}\, k = 0$, *then Q_1 is finite; and*

(ii) *if* $\mathrm{char}\, k = p > 0$, *then Q_1 is marginal.*

Proof. Replacing k by a finite extension, if necessary, we may assume that f splits in k. Furthermore by enlarging S we may also assume that the eigenvalues of elements of Q and the roots of f are S-units. Let $\lambda : Q \longrightarrow k^*$ be the monomorphism as in

Lemma 2.1. Clearly $\det f(q) = N_{k/k_0}(f(\lambda(q)))$. We conclude that if $q \in Q_1$, then $f(\lambda(q))$ is an S-unit. Let ω be a root of f. Since $\omega - X$ divides $f(X)$, it follows that $u(q) := \omega - \lambda(q)$ is an S-unit. We therefore have

$$\lambda(q)/\omega + u(q)/\omega = 1 \qquad (1 \le i \le m,\ q \in Q_1). \tag{2}$$

Case 1. $\operatorname{char} k = 0$. By the S-unit theorem equation (2) has only finitely many solutions, so there are only finitely many possibilities for $\lambda(q)$. Since $\lambda(q)$ determines q, we conclude that Q_1 is finite.

Case 2. $\operatorname{char} k = p > 0$. Then the S-unit equation (2) has only finitely many basic solutions, i.e. solutions which are not p^{th}-powers. Let B be a list of these basic solutions. Then for each $q \in Q_1$, $\lambda(q)$ is of the form ωb^{p^i} for some $b \in B$ and some integer $i \ge 0$.

Let T be any transversal to the torsion subgroup in Q. Then we claim that $tQ_1 \cap t'Q_1$ is finite whenever $t,\ t'$ are distinct elements of T. To see this it is sufficient to show that $\lambda(t)\lambda(Q_1) \cap \lambda(t')\lambda(Q_1)$ is finite, which is equivalent to $\lambda(Q_1) \cap \lambda(t^{-1}t')\lambda(Q_1)$ being finite. Since $\lambda(t^{-1}t')$ is not a root of unity, this is a consequence of Lemma 2.5. This proves the claim. Finally since Q_1 has infinitely many almost disjoint translations it is marginal in Q. □

In order to formulate the next result we need some definitions. Let G be an amenable group and let $N \lhd G$. Clearly every measure μ_G on G gives rise to a unique measure $\mu_{G/N}$ on G/N (defined by $\mu_{G/N}(X/N) = \mu_G(X)$ for $N \subseteq X \subseteq G$).

Now, suppose we are given measures μ_N, μ_Q on N and on $Q = G/N$ respectively. Then we can define a measure μ_G on G by the formula

$$\mu_G(X) = \int_Q \mu_N(N \cap g_q^{-1}X)\mu_Q(dq)$$

where $(g_q | q \in Q)$ is a transversal to N in G, (i.e. $\overline{g_q} = q$). Measures on G which are obtained in this manner will be called *N-induced*.

The following properties are easily verified.

Lemma 2.7. *Let G be an amenable group, and let $N \lhd G$. Then*

(i) *If μ is an N-induced measure on G and $\overline{G}$ is a quotient of G, then the corresponding measure $\overline{\mu}$ on $\overline{G}$ is $\overline{N}$-induced, where $\overline{N}$ is the image of N in $\overline{G}$.*

(ii) *If G/N is finite, then every measure on G is N-induced.*

(iii) *If N is finite, then every measure on G is N-induced.*

(iv) *Let $M \lhd G$ and suppose M and N are commensurable. Then a measure on G is M-induced if and only if it is N-induced.*

Lemma 2.8. *Let G be a finitely generated metabelian group which is just-non-(nilpotent-by-finite). Let $A = F(G)$ be the Fitting subgroup of G and let $n \ge 2$. Then $\mu(G^n) = 0$ for every A-induced measure μ on G.*

Proof. The precise structure of G is given in Lemma 2.1 whose notation we adopt. Fix an A-induced probability measure μ on G, and let μ_A, μ_Q be the corresponding probability measures on A, Q respectively. Suppose, by contradiction, that

$$\mu(G^n) > 0.$$

Then there exist $\epsilon > 0$ and $Q_0 \subseteq Q$ with $\mu_Q(Q_0) > 0$ and $\mu_A(A \cap g_{q_0}^{-1}G^n) \geq \epsilon$ for all $q_0 \in Q_0$. Now, by Lemma 2.2 and the subsequent remark, there exists an l independent of q_0, such that $A \cap g_{q_0}^{-1}G^n$ is a union of at most l cosets of the form $b(q)A^{q^{n-1}+\ldots+q+1}$ (where q satisfies $q^n = q_0$). Thus, if $d(q)$ denotes the index of $A^{q^{n-1}+\ldots+q+1}$ in A, then we have $\mu_A(A \cap g_{q_0}^{-1}G^n) \leq \sum_{q^n=q_0} 1/d(q)$.

Choose q_1 so that $q_1^n = q_0$ and $d(q_1) = \min\{d(q) | q^n = q_0\}$. Then we have $\mu_A(A \cap g_{q_0}^{-1}G^n) \leq l/d(q_1)$, and hence

$$d(q_1) \leq l/\epsilon. \tag{3}$$

Let Q_1 be the set of all q_1 arising as above; note that the map $x \mapsto x^n$ defines a bijection $Q_1 \longrightarrow Q_0$. We now make use of Lemma 2.1. If A is torsion-free of finite rank, then there is a finite set S of rational primes such that $d(q)$ is greater than or equal to the S'-part of $\det(q^{n-1} + \ldots + q + 1)$, this S-prime part being a rational S-integer. If A is an elementary abelian p-group, then essentially the same holds for a suitable finite set S of primes of $\mathbb{F}_p[t]$, but in this case the S'-part of $\det(q^{n-1} + \ldots + q + 1)$ is a polynomial in t and $d(q)$ is bounded below by its degree. In view of (2) we can thus assume, by enlarging S if necessary, that $\det(q^{n-1} + \ldots + q + 1)$ is an S-unit for all q in Q_1.

By Proposition 2.6, Q_1 is marginal. Now applying Lemma 2.3 we see that $Q_0 = Q_1^n$ is also marginal. But this contradicts the choice of Q_0. □

We can now derive our main result for metabelian groups.

Proposition 2.9. *Let G be a finitely generated metabelian group which is not nilpotent-by-finite, and let $n \geq 2$. Then $\mu(G^n) = 0$ for every G'-induced measure μ on G.*

Proof. Let $\overline{G}$ be a just-non-nilpotent-by-finite quotient of G, and let $\overline{\mu}$ be the corresponding measure on $\overline{G}$. Note that $\overline{\mu}$ is $\overline{G}'$-induced (by 2.7).

Now, $\overline{G}'$ is a non-trivial abelian normal subgroup of $\overline{G}$, so it must have finite index in the Fitting subgroup $F(\overline{G})$; this follows from the fact that $F(\overline{G})$ is a just-infinite $\overline{G}$-module. Applying part (iv) of Lemma 2.7 we conclude that $\overline{\mu}$ is $F(\overline{G})$-induced.

Since the conditions of Lemma 2.8 are satisfied we obtain $\overline{\mu}(\overline{G}^n) = 0$. This clearly implies $\mu(G^n) = 0$.

The proposition is proved. □

Let us now prove Theorem A.

Let G be a finitely generated soluble-by-finite group and let J be a finite set of integers greater than 1. Suppose G^J contains a finite index subgroup. We may assume, as usual, that G is just-non-(nilpotent-by-finite).

Every finitely generated soluble-by-finite group which is just-non-nilpotent-by-finite is metabelian-by-finite; this follows from Groves [4]. Hence we may assume that G is metabelian-by-finite. Choose a metabelian normal subgroup H of G of finite index such that $G^J \supseteq H$.

Let $A = H'$, the derived subgroup of H. Then A is normal in G and A and H/A are abelian. Furthermore, A is just-infinite as a G-module. Define a subgroup G_0 by $G_0/A = FC(G/A)$, the FC-center of G/A. Note that

$$G_0 = \{g \in G | \ |H/A : C_{H/A}(g)| < \infty\},$$

so in particular $G_0 \supseteq H$. Thus $(G : G_0) < \infty$ and G_0 is finitely generated.

Let H_0 be the subgroup of G defined by

$$H_0/A := C_{H/A}(G_0).$$

The fact that G_0 is finitely generated shows that H_0 has finite index in H. Note that G_0 and H_0 are normal in G. Since H_0' is a non-trivial G-invariant subgroup of $A = H'$, we have $(A : H_0') < \infty$.

We claim that $H_0 \setminus G_0^J$ is marginal. To show this, let T be a transversal to H in G. Then

$$G^J = \bigcup_{n\in J}\bigcup_{g\in T}(gH)^n = \bigcup_{n\in J}\bigcup_{g\in T} g^n H^{g^{n-1}+\ldots+1}.$$

Setting $T_n = \{g \in T | g^n \in H\}$ we see that

$$H \cap G^n = \bigcup_{n\in J}\bigcup_{g\in T_n} g^n H^{g^{n-1}+\ldots+1}. \tag{4}$$

Fix $n \in J$ and $g \in T_n$. Since g^n belongs to H, it centralizes H/A. A straightforward calculation now shows that

$$g^n H^{g^{n-1}+\ldots+1} A/A \subseteq C_{H/A}(g).$$

Note that if $g \notin G_0$, then $C_{H/A}(g)$ has infinite index in H/A. Thus

$$g^n H^{g^{n-1}+\ldots+1} \text{ is marginal for all } g \notin G_0. \tag{5}$$

Set $S_n = T_n \cap G_0$. Recall that we assume $H \subseteq G^J$, and hence

$$H \subseteq \bigcup_{n\in J}\bigcup_{g\in T_n} g^n H^{g^{n-1}+\ldots+1}.$$

In view of (5) we see that

$$H \setminus \bigcup_{n\in J}\bigcup_{g\in S_n} g^n H^{g^{n-1}+\ldots+1}$$

is marginal. Thus $H \setminus G_0^J$ is marginal, and so is $H_0 \setminus G_0^J$.

Let μ be an A-induced measure on G. Then the above discussion shows that $\mu(H_0 \cap G_0^J) = \mu(H_0) > 0$, and so there exists $n \in J$ and $g_0 \in G_0$ (depending on μ) such that $g_0^n \in H_0$ and $\mu((g_0H_0)^n) > 0$. Define $K := \langle H_0, g_0\rangle$. Since $g_0 \in G_0$, it centralises H_0/A. Hence K/A is abelian, and K is metabelian. Since $(G : K) < \infty$ it follows that K is finitely generated and not nilpotent-by-finite. Note that $H_0' \subseteq K' \subseteq A$ and so by previous remarks we have $(A : K') \leq (A : H_0') < \infty$. Since μ is A-induced, we conclude (using 2.7(iv)) that the measure μ restricted to K is K'-induced. Finally, by the choice of n and g_0 we have

$$\mu(K^n) \geq \mu((g_0H_0)^n) > 0.$$

This violates Proposition 2.9.

The theorem is proved.

3. Proof of Theorem B

Let R be a finitely generated integral domain of characteristic $p \geq 0$. Let $Y(R)$ be the set of primes $\pi \in \mathrm{Spec}(R)$ such that R/π is a finite field, which is required to be prime if $p = 0$.

Our main tool in this section is the following Strong Approximation Theorem for linear groups over R. The characteristic zero case follows from Nori [14], while Weisfeiler's work [18] settles the case $p > 3$. The version used here for arbitrary characteristic is due to Hrushovski [8].

A subset X of maximal ideals of R is Zariski dense if R embeds into $\prod_{\pi \in X} R/\pi$.

Theorem 3.1. *Let G be a connected, simply connected semisimple algebraic group, and let Γ be a finitely generated Zariski dense subgroup of $G(K)$ (K an algebraically closed field). Then there exists a conjugate Γ_1 of Γ and a finitely generated ring $R \subseteq K$ with the following properties:*

(i) $\Gamma_1 \subseteq G(R)$.

(ii) *If R_1 is a finitely generated ring satisfying $R \subseteq R_1 \subseteq K$, then Γ_1 is mapped onto $G(R_1/\pi)$ for densely many maximal ideals π of R_1.*

Remarks. (i) This follows from a much more precise result, describing the image of Γ in $G(R/\pi)$ for all but finitely many π. The image lies between S and $N_{G(R/\pi)}(S)$, where S is a certain quasi-simple subgroup of $G(R/\pi)$. The possibilities for S include twisted Chevalley groups. The weaker version of 3.1 suffices for our purposes, and exempts us from dealing with twisted groups in the present paper.

(ii) The group S above is obtained by 'twisting': $S = \{x \in G(R/\pi) : h(x) = f(x)\}$, where f is a rational group homomorphism from G to G, and h is a field automorphism arising from one of a finite number of ring automorphisms of R. By the Čebotarev density theorem, there are many primes π that do not respect any of the given ring automorphisms; for these primes no twisting occurs, and we are reduced to Theorem 3.1. For the same reason one may consider in the statement arbitrary finitely generated extension rings R_1 (they will be collapsed into R by many primes), which adds to the flexibility.

We now reformulate Theorem 3.1 in topological terms. Given a Zariski dense subset $X \subseteq Y(R)$, define the X-topology on $G(R)$ to be the one generated by the subgroups $G(\pi) = \mathrm{Ker}(G(R) \longrightarrow G(R/\pi))$ ($\pi \in X$). Such a topology on $G(R)$ will be called *admissible*.

Let G, Γ, Γ_1 be as above. Choose X such that Γ_1 is mapped onto $G(R/\pi)$ for all $\pi \in X$, and such that, for two distinct π and π' in X, $G(R/\pi)$ and $G(R/\pi')$ have no common simple quotient. This way Γ_1 is mapped onto $G(R/I)$ where I is any intersection of finitely many primes in X. This means that Γ_1 is dense in $G(R)$ with respect to some admissible topology (namely, the X-topology).

We shall also need the following well-known result.

Lemma 3.2. *Let G be a connected, simply connected semisimple algebraic group. Then the group $\mathrm{Aut}(G)$ of automorphisms of G as an algebraic group is a split extension of $\mathrm{Inn}(G)$ by a finite group D of automorphisms of the Dynkin diagram.*

Lemma 3.3. *Let G be a connected semisimple algebraic group, $\widetilde{G}$ its universal cover, and suppose $G = \widetilde{G}/N$. Then every automorphism of G lifts uniquely to an automorphism of $\widetilde{G}$ respecting N.*

Proof. Let h be an automorphism of G, considered as a subgroup of $G \times G$. Let $\widetilde{h}$ be the connected component of the inverse image of h in $\widetilde{G} \times \widetilde{G}$. Then $\widetilde{h}$ is a group, and the projections to $\widetilde{G}$ make it a finite cover of $\widetilde{G}$. Since $\widetilde{G}$ is simply connected, these projections must be injective. Thus $\widetilde{h}$ defines an automorphism of $\widetilde{G}$. If $x \in N$, $(x, y) \in \widetilde{h}$, then $(xN, yN) \in h$, so $yN = N$ (the identity of $\widetilde{G}/N$) and $y \in N$. Thus $\widetilde{h}$ preserves N.

To prove uniqueness, let $\sigma \in \mathrm{Aut}(\widetilde{G})$ induce the identity on G. Then $\sigma(x) = xz(x)$ where $z(x) \in N \subseteq Z(\widetilde{G})$, and one sees easily that z is a homomorphism from $\widetilde{G}$ to N. Since $\widetilde{G}$ is connected, z must be trivial. □

We need the following result.

Lemma 3.4. *Let G be a connected semisimple algebraic group defined over R, and let $K \supset R$ be an algebraically closed field. Let $\sigma \in \mathrm{Aut}(G)$. Then there exists $\sigma' \in \mathrm{Aut}(G)$ which is congruent to σ modulo $\mathrm{Inn}(G)$, such that the centralizer $C_{G(K)}(\sigma')$ contains elements of any given prime order.*

Proof. First notice that it suffices to prove the lemma for simple groups; this is because σ stabilizes a simple subgroup, namely the diagonal subgroup of any given orbit of the action of σ on the set of simple components.

So suppose G is simple. We apply the classification of simple algebraic groups.

It suffices to show that, for a suitable choice of σ', the centralizer $C_{G(K)}(\sigma')$ contains both the multiplicative group and the additive group of K. Indeed, K^* has elements of any prime order $q \neq p$, while the additive group K has elements of order p (if $p > 0$).

If σ is inner we may take $\sigma' = 1$ and use the fact that $G(K)$ contains a torus and a root subgroup, and hence contains the multiplicative and the additive group of K.

If σ is not inner, then automatically $G \neq A_1, B_n, C_n, E_7, E_8, G_2$ or F_4, as these groups do not have non-trivial (separable) Dynkin diagram automorphisms.

It remains to distinguish between the following cases.

Case I. $G = A_n$ $(n \geq 2)$.

Then σ is congruent (modulo $\mathrm{Inn}(G)$) to the unique non-trivial graph automorphism σ' given by $x^{\sigma'} = (x^{-1})^t$. Its centralizer in $G(K)$ is the group $SO_{n+1}(K)$, which contains both the multiplicative group and the additive group of K (since K is algebraically closed).

Case II. $G = D_n$ $(n \geq 3)$ or E_6.

By the structure of the associated graph, we see that there is a root, say r_0, which is fixed under all graph automorphisms. Now, given σ, we can multiply it by an inner automorphism and assume that σ keeps invariant a Borel subgroup B and a torus $T \subseteq B$. Let

$$T_1 = \{x \in T | r(x) = 1 \text{ for all fundamental roots } r \neq r_0\}.$$

Then T_1 is a 1-dimensional torus; it is invariant under σ, since for $r \neq r_0$ and $x \in T_1$ we have $r(x^\sigma) = r^\sigma(x) = 1$ (as $r^\sigma \neq r_0$).

We claim that σ centralizes T_1. To see this, let $x \in T_1$. Then $r_0(x^\sigma) = {r_0}^\sigma(x) = r_0(x)$ so $r_0(x^{-1}x^\sigma) = 1$. Since $x^{-1}x^\sigma \in T_1$ it follows that $r(x^{-1}x^\sigma) = 1$ for all fundamental roots r, so $x^{-1}x^\sigma = 1$. We conclude that $C_{G(K)}(\sigma)$ contains $T_1 \cong K^*$.

Now, let $A \subseteq B$ be a root subgroup for r_0. Multiplying σ by a suitable inner automorphism induced by an element of T we obtain an automorphism σ' centralizing A (and T_1). Since A is isomorphic to the additive group of K, the proof is complete. □

Given $n \geq 2$ and an automorphism $\sigma \in \mathrm{Aut}(G)$, consider the map

$$\phi_{n,\sigma} : x \mapsto x^{\sigma^{n-1}} \cdots x^{\sigma} x.$$

Note that, in $\mathrm{Aut}(G)$ we have

$$(\sigma x)^n = \sigma^n \phi_{n,\sigma}(x).$$

This implies that, if $\sigma, \sigma' \in \mathrm{Aut}(G)$ are congruent modulo $\mathrm{Inn}(G)$, then, as maps defined on $G(K)$, $\phi_{n,\sigma}$ is injective if and only if $\phi_{n,\sigma'}$ is injective.

In what follows we say that a subset of $Y(R)$ contains almost all primes there if it consists of all the primes not containing a single element $a \in R$.

Corollary 3.5. *Let G be a connected semisimple algebraic group defined over R; if p does not divide n, suppose R contains a primitive n^{th} root of unity. Let $\sigma \in \mathrm{Aut}(G)$. Then*

(i) *The map $\phi_{n,\sigma}$ defined on $G(R)$ is not injective.*

(ii) *For almost all primes $\pi \in Y(R)$ the map $\phi_{n,\sigma}$ defined on $G(R/\pi)$ is not injective.*

(iii) *For almost all primes $\pi \in Y(R)$ the map $\phi_{n,\sigma}$ defined on $G(R/\pi)$ is not surjective.*

Proof. Let q be a prime divisor of n; if p divides n, suppose $q = p$. Choose σ' as in the preceding result. Then, by the assumption on R there exists an element $x \in G(R)$ of order q such that $x^{\sigma'} = x$. Thus $\phi_{n,\sigma'}(x) = x^n = 1 = \phi_{n,\sigma'}(1)$ while $x \neq 1$. We see that $\phi_{n,\sigma'}$ is not injective, so by a previous remark $\phi_{n,\sigma}$ is not injective. This proves part (i). Now, part (ii) follows from part (i), and (iii) is a consequence of (ii), since the groups $G(R/\pi)$ are finite. □

We can now prove the main result of this section, from which Theorem B will be shown to follow.

Proposition 3.6. *Let G be a connected, simply connected semisimple algebraic group defined over R. Let J be a finite set of integers greater than 1, and suppose that for each $n \in J$ which is not divisible by p, R has a primitive n^{th} root of unity. Let D be a finite set of automorphisms of the Dynkin diagram of G, and define*

$$P = \{\phi_{n,\sigma}(x) | x \in G(R), n \in J, \sigma \in D\}.$$

Then P is nowhere dense in $G(R)$ with respect to any admissible topology.

Proof. P is the union of the finitely many sets of the form $\phi_{n,\sigma}(G(R))$ $(n \in J, \sigma \in D)$ so it suffices to show that each of these sets is nowhere dense.

Suppose, by contradiction, that for some $n \in J$, $\sigma \in D$ and a dense subset $X \subseteq Y(R)$, $Q := \phi_{n,\sigma}(G(R))$ is dense in some open subset of $G(R)$ with respect to the X-topology. This implies that, for almost all primes $\pi \in X$, Q is mapped onto $G(R/\pi)$. Thus $\phi_{n,\sigma}(G(R/\pi)) = G(R/\pi)$ for densely many primes $\pi \in Y(R)$. This contradicts part (iii) of Corollary 3.5. □

Corollary 3.7. *Let G, R and P be as in* 3.6. *Then, for any finite subset $T \subset G(R)$, TP is nowhere dense in $G(R)$ with respect to any admissible topology.*

Proof. It is clear that, if a subset $S \subseteq G(R)$ is nowhere dense, then so is any of its translations gS (where $g \in G(R)$). Since the union of finitely many nowhere dense subsets is nowhere dense, the result follows. □

Let us now prove Theorem B. The proof is by contradiction. Recall that the property that Γ^J has finite index in Γ is inherited by quotients. Now, among all counterexamples $\Gamma \subseteq G(R)$ where G is a linear algebraic group defined over some finitely generated domain R, choose one for which $\dim(G)$ is minimal. Then Γ is Zariski dense in $G(R)$ (otherwise its Zariski closure will be an algebraic group of lower dimension).

Let G^0 be the connected component of G (having finite index in G), and let S be the soluble radical of G^0. Set $\overline{G} = G/S$, $\overline{\Gamma} = \Gamma/(\Gamma \cap S)$. Then $\overline{\Gamma}$ is still not soluble-by-finite. Thus, if $S \neq 1$, then $\overline{\Gamma} \subseteq \overline{G}$ would be a counterexample of smaller dimension. We conclude that $S = 1$ and G is semisimple.

We may divide by the (finite) centralizer $C_G(G^0)$ and assume $G \subseteq \mathrm{Aut}(G^0)$.

Let $\widetilde{G^0}$ be the simply connected covering group of G^0. By Lemmas 3.2 and 3.3 $\mathrm{Aut}(\widetilde{G^0})$ is a split extension of the group of inner automorphisms by a finite group D of graph automorphisms, and there exists an epimorphism $f : \mathrm{Aut}(\widetilde{G^0}) \longrightarrow \mathrm{Aut}(G^0)$. Recall that $\Gamma \subseteq \mathrm{Aut}(G^0)$. Let $\widetilde{\Gamma} \subseteq \mathrm{Aut}(\widetilde{G^0})$ denote the inverse image of Γ under f. Then finitely many translations of $Z(\widetilde{G^0})\widetilde{\Gamma}^J$ cover $\widetilde{\Gamma}$. Since $Z(\widetilde{G^0})$ is finite, it follows that $\widetilde{\Gamma}^J$ has finite index in $\widetilde{\Gamma}$, say $\widetilde{\Gamma} = T\widetilde{\Gamma}^J$ for a finite set T.

We now apply Theorem 3.1. Replacing Γ by Γ_1 (see 3.1) we may assume that $\widetilde{\Gamma}^0 := \widetilde{\Gamma} \cap \widetilde{G^0}(R)$ is dense in $\widetilde{G}^0(R)$ with respect to some admissible topology. But every element of $\widetilde{\Gamma}^0$ has the form $t\phi_{n,\sigma}(x)$ for some $t \in T, x \in \widetilde{G^0}(R), n \in J$ and $\sigma \in D$. This contradicts Corollary 3.7.

Theorem B is proved.

4. A concluding example

We give an example of a finitely generated soluble linear group G such that for any integer $n \geq 2$ which is coprime to 3,

$$G^n \text{ contains a coset of a subgroup of finite index,}$$

and yet G is not nilpotent-by-finite. The idea is to construct a polycyclic group G so that there are a subgroup H of finite index and an element $g \in G$ such that

$$\forall\, x \in gH, \quad x^9 = 1,$$

for then

$$G^n \supseteq \{x^n | x \in gH\} = gH.$$

Plainly there is nothing special about the number 3 here: we leave the reader to construct variations on this example.

Let η be a primitive 9^{th} root of unity, and let $\mathcal{O}$ be the ring of integers in a number field containing η. Let B be the subgroup of $GL_3(\mathcal{O})$ comprising the

diagonal matrices of determinant 1, and let Q be the subgroup generated by B together with

$$\phi := \begin{pmatrix} 0 & \eta & 0 \\ 0 & 0 & 1 \\ \eta^2 & 0 & 0 \end{pmatrix}.$$

Thus Q is a group of automorphisms of $A := \mathcal{O} \oplus \mathcal{O} \oplus \mathcal{O}$. Since ϕ^3 is the scalar matrix with diagonal entries η^3, it is easy to check that for any $\delta \in B$, the following identities hold in the endomorphism ring of A:

$$\delta^{\phi^2}\delta^{\phi}\delta = 1,$$

$$\delta^{\phi^6} + \delta^{\phi^3} + \delta = 0.$$

Now let G be the split extension of A by Q. The subgroup $H := BA$ has index 3, and from the above identities, it is easily seen that the coset ϕH consists entirely of elements of order 9: indeed, for a typical element $\delta \cdot a$ of H, we have

$$\begin{aligned}(\phi\delta \cdot a)^9 =&(\phi^9\delta^{\phi^8}\delta^{\phi^7}\delta^{\phi^6}\delta^{\phi^5}\delta^{\phi^4}\delta^{\phi^3}\delta^{\phi^2}\delta^{\phi}\delta) \\ &\cdot a(\delta^{\phi^8} + \delta^{\phi^7} + \delta^{\phi^6} + \delta^{\phi^5} + \delta^{\phi^4} + \delta^{\phi^3} + \delta^{\phi^2} + \delta^{\phi} + \delta) = 1.\end{aligned}$$

References

1. J. H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), 561–584. MR **85f:**11048
2. J. H. Evertse, K. Győry, C.L. Stewart, and R. Tijdeman, *On S-unit equations in two unknowns*, Invent. Math. **92** (1988), 461–477. MR **89g:**11028
3. J.-H. Evertse, K. Győry, C. L. Stewart, and R. Tijdeman, *S-unit equations and their applications*, New Advances in Transcendence Theory (Proceedings of the Symposium on Transcendental Number Theory at Durham, 1986) (A. Baker, ed.), Cambridge Univ. Press, Cambridge, 1988, pp. 110–174. MR **89j:**11028
4. J. R. J. Groves, *Soluble groups with every proper quotient polycyclic*, Illinois J. Math. **22** (1978), 90–95. MR **80b:**20035
5. V. S. Guba, *Finitely generated divisible groups*, Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), 883–924. MR **88e:**20034
6. P. Hall, *Some sufficient conditions for a group to be nilpotent*, Illinois J. Math. **2** (1958), 787–801. MR **21:**4183
7. ———, *On the finiteness of certain soluble groups*, Proc. London Math. Soc. **9** (1959), 595–622. MR **22:**1618
8. E. Hrushovski, *Strong approximation for linear groups in arbitrary characteristic*, in preparation.
9. S. Lang, *Integral points on curves*, Publ. Math. I.H.E.S. **6** (1960), 27–43. MR **24:**A86
10. John C. Lennox and James Wiegold, *Converse of a theorem of Mal′cev on nilpotent groups*, Math. Z. **139** (1974), 85–86. MR **50:**13280
11. A. I. Mal′cev, *Homomorphisms onto finite groups*, Ivanov. Gos. Ped. Inst. Uchen. Zap. Fiz.-Mat. Nauki **8** (1958), 49–60.
12. R. C. Mason, *Diophantine equations over function fields*, London Math. Soc. Lecture Note Series, vol. 96, Cambridge Univ. Press, Cambridge, 1984. MR **86b:**11026
13. ———, *Normal form equations.* III: *positive characteristic*, Math. Proc. Cambridge Philos. Soc. **99** (1986), 409–423. MR **90e:**11048a
14. M. Nori, *On subgroups of $GL_n(\mathbb{F}_p)$*, Invent. Math. **88** (1987), 257–275. MR **88d:**20068
15. D. J. S. Robinson and J. S. Wilson, *Soluble groups with many polycyclic quotients*, Proc. London Math. Soc. **48** (1984), 193–229. MR **85k:**20115
16. T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge Tracts in Math., vol. 87, Cambridge Univ. Press, Cambridge, 1986. MR **88h:**11002

17. S. Wagon, *The Banach-Tarski paradox*, Encyclopedia Math. Appl., vol. 24, Cambridge Univ. Press, Cambridge, 1985. MR **87e:**04007
18. B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups*, Ann. of Math. (2) **120** (1984), 271–315. MR **86m:**20053

(E. Hrushovski, A. Lubotzky and A. Shalev) Department of Mathematics, Hebrew University, Jerusalem 91904, Israel

(P.H. Kropholler) School of Mathematical Sciences, Queen Mary & Westfield College, Mile End Road, London E1 4NS, United Kingdom