Normal Subgroup Growth of Linear Groups: the (G_2, F_4, E_8)-Theorem

Michael Larsen and Alexander Lubotzky

Dedicated to M. S. Raghunathan

April 11, 2004

Let Γ be a finitely generated residually finite group. Denote by $s_n(\Gamma)$ (resp. $t_n(\Gamma)$) the number of subgroups (resp. normal subgroups) of Γ of index at most n. In the last two decades the study of the connection between the algebraic structure of Γ and the growth rate of the sequence $\{s_n(\Gamma)\}_{n=1}^{\infty}$ has become a very active area of research under the rubric "subgroup growth" (see [L1], [LS] and the references therein). The subgroup growth rate of a finitely generated group is bounded above by $e^{O(n \log n)}$, which is the growth rate for a finitely generated non-abelian free group. On the other end of the spectrum, the groups with polynomial subgroup growth (PSG-groups for short), i.e., those satisfying $s_n(\Gamma) \leq n^{O(1)}$, were characterized ([LMS]) as the virtually solvable groups of finite rank. This was originally proved for linear groups ([LM]). The linear case was then used to prove the theorem for general residually finite groups.

In recent years, interest has also developed in the *normal* subgroup growth $\{t_n(\Gamma)\}_{n=1}^{\infty}$. In [L3] it was shown that the normal subgroup growth of a non-abelian free group is of type $n^{\log n}$, just a bit faster than polynomial growth. One cannot, therefore, expect that the condition on Γ of being of "polynomial normal subgroup growth" (PNSG, for short) will have the same strong structural implications as that of polynomial subgroup growth. In particular, PNSG-groups (unlike PSG-groups) need not be virtually solvable. In fact, the examples produced in [S, Py] (which, incidentally, show that essentially every rate of subgroup growth between polynomial and factorial can occur) all have sublinear normal subgroup growth and are very far from being solvable.

For linear groups, however, the situation is quite different.

First fix some notations: Let F be an (algebraically closed) field and Γ a finitely generated subgroup of $GL_n(F)$. Let G be the Zariski closure of Γ, $R(G)$ the solvable radical of G, and G°-the connected component of G. Write $\overline{G} = G^\circ/R(G)$ and let $S(\Gamma) = \overline{G}/Z(\overline{G})$ – "the semisimple closure of Γ". So $S(\Gamma) =$

$\prod_{i=1}^{r} S_i$ where each S_i is a simple algebraic group over F.

Theorem A. *Assume Γ is of polynomial normal subgroup growth, and $S(\Gamma) = \prod_{i=1}^{r} S_i$ as above. Then either*

(a) $r = 0$*, in which case Γ is virtually solvable, or*

(b) $r > 0$ *and for each $1 \leq i \leq r$, S_i is a simple algebraic group of type G_2, F_4 or E_8.*

Theorem A is best possible. Indeed, we will see below (Theorem C) that for S-arithmetic subgroups of G_2, F_4 and E_8, the rate of growth of the normal congruence subgroups is polynomial. At least some of these arithmetic groups (and conjecturally all – see [PR]) satisfy the congruence subgroup property. So, they provide examples of Zariski dense subgroups of G_2, F_4 and E_8 with polynomial normal subgroup growth. It should be noted, however, that the normal subgroup growth rate is not determined by the Zariski closure. Every simple algebraic group has a Zariski dense free subgroup and the normal growth of the latter is $n^{\log n}$.

Theorem A is surprising in two ways: First, it shows that linear groups are very different from general residually finite groups; the linear PNSG-groups are "generically" virtually solvable. But even more surprising is the special role played by G_2, F_4 and E_8. This seems to be the first known case in which a growth condition singles out individual simple algebraic groups from all the others.

What is so special about G_2, F_4 and E_8? These are the only simple algebraic groups whose simply connected and adjoint forms are the same, or in other words the only groups whose universal covers have trivial center. Theorem A is therefore equivalent to:

Theorem A'. *Let $\Gamma \leq GL_n(F)$ and $S(\Gamma) = \prod_{i=1}^{r} S_i$ as above. Assume that for some i, $1 \leq i \leq r$, $\mathcal{Z}(\tilde{S}_i) \neq 1$ (i.e., the scheme-theoretic center of the simply connected cover of S_i is non-trivial). Then Γ is not a PNSG-group.*

In fact, our result is much more precise:

Theorem B. *Let $\Gamma \leq GL_n(F)$ and $S(\Gamma) = \prod_{i=1}^{r} S_i$ as above. Denote the characteristic of F by $p \geq 0$. Then,*

(i) *If for some i, $1 \leq i \leq r$, $\mathcal{Z}(\tilde{S}_i) \neq 1$ then the normal subgroup growth rate of Γ is at least $n^{\log n/(\log\log n)^2}$.*

(ii) *If for some i, $1 \leq i \leq r$, $p \big| \, |\mathcal{Z}(\tilde{S}_i)|$ then the normal subgroup growth rate of Γ is $n^{\log n}$.*

It is easy to see that Theorem B implies A(and A'), so we will aim at proving the former. To this end we will prove the following result which may be of independent interest:

Theorem 4.1. *Let A be an integral domain, finitely generated over the prime field of characteristic $p \geq 0$, with fraction field K. Let Γ be a finitely generated subgroup of $GL_n(A)$ whose Zariski closure G in $GL_n(K)$ is connected and absolutely simple. Then there exists a global field k and a ring homomorphism $\phi\colon A \to k$, such that the Zariski closure of $\phi(\Gamma)$ in $GL_n(k)$ is isomorphic to G over some common field extension of K and k.*

Theorem 4.1 will enable us to reduce the proof of Theorem B to the case when Γ sits within $GL_n(k)$, where k is a global field. Being finitely generated, it is even contained in an S-arithmetic group. The Strong Approximation Theorem for linear groups (in the strong version of Pink [P2]) then connects the estimate of $t_n(\Gamma)$ to the counting of normal congruence subgroups in an S-arithmetic group. Here we can prove the following precise result.

Theorem C. *Let k be a global field of characteristic $p \geq 0$, S a non-empty set of valuations of k containing all the archimedean ones, and $\mathcal{O}_S = \{x \in k | v(x) \geq 0, \forall v \notin S\}$. Let $\mathcal{G}$ be a smooth group scheme over $\mathcal{O}_S$ whose generic fiber $\mathcal{G}_\eta$ is connected and simple . Let $\tilde{\mathcal{G}}_\eta$ be the universal cover of $\mathcal{G}_\eta$. Let Δ be the S-arithmetic group $\Delta = \mathcal{G}(\mathcal{O}_S)$. Assume Δ is an infinite group. Let $D_n(\Delta)$ be the number of normal congruence subgroups of index at most n in Δ. Then the growth type of $D_n(\Delta)$ is:*

(i) *n if $\mathcal{G}$ is of type G_2, F_4 or E_8.*

(ii) *$n^{\log n/(\log\log n)^2}$ if $\mathcal{Z}(\tilde{\mathcal{G}}_\eta) \neq 1$ and $p \nmid |\mathcal{Z}(\tilde{\mathcal{G}}_\eta)|$*

(iii) *$n^{\log n}$ if $p \Big| |\mathcal{Z}(\tilde{\mathcal{G}}_\eta)|$*

Note that by $|Z(\tilde{\mathcal{G}}_\eta)|$ we mean the order of the group scheme which is the center of $\tilde{G}_\eta$. This is an invariant which depends only on the root system: If $p \neq 2, 3$, $p \big| |\mathcal{Z}(\tilde{\mathcal{G}}_\eta)|$ if and only if $\mathcal{G}$ is of type A_n and $p|(n+1)$.

It is of interest to compare $D_n(\Delta)$ to $C_n(\Delta)$ when $C_n(\Delta)$ counts the number of all congruence subgroups of Δ of index at most n. The following table summarizes the situation.

	$p=0$	$p>0$
G_2, F_4, E_8	C: $n^{\log n/\log\log n}$ $[L2, GLP]$ D: n $[LL]$	C: $n^{\log n}$ $[N]$ D: n $[LL]$
$\mathcal{Z}(\tilde{\mathcal{G}}_\eta) \neq 1$ and $p \nmid \lvert Z(\tilde{\mathcal{G}}_\eta)\rvert$	C: $n^{\log n/\log\log n}$ $[L2, GLP]$ D: $n^{\log n/(\log\log n)^2}$ $[LL]$	C: $n^{\log n}$ $[N]$ D: $n^{\log n/(\log\log n)^2}$ $[LL]$
$p \big\vert \lvert\mathcal{Z}(\tilde{\mathcal{G}}_\eta)\rvert$	cannot occur	C: $n^{\log n}$ $[N]$ D: $n^{\log n}$ $[LL]$

We only remark, that as of now the results of $[N]$ require the assumption that $\mathcal{G}$ splits. [LL] refers to the current paper.

The proof of Theorem C depends on a careful analysis of the corresponding problem over local fields. Here we have:

Theorem D. *Let k be a non-archimedean local field of characteristic $p \geq 0$, and $\mathcal{O}$ its valuation ring. Let $\mathcal{G}$ be a smooth group scheme over $\mathcal{O}$ whose generic fiber $\mathcal{G}_\eta$ is connected, simply connected and simple. Let $\Delta = \mathcal{G}(\mathcal{O})$ and $t_n(\Delta)$ the number of open normal subgroups of Δ of index at most n. Then the growth type of $t_n(\Delta)$ is:*

(i) $n^{\log n}$ *if* $p \Big\vert \Big\lvert \mathcal{Z}(\mathcal{G}_\eta) \Big\rvert$

(ii) n *if $\mathcal{G}$ is of Ree type, i.e., either $p=2$ and $\mathcal{G}$ is of type F_4 or $p=3$ and $\mathcal{G}$ is of type G_2.*

(iii) $\log n$ *otherwise.*

Theorem D is somewhat surprising in its own right; the groups of Ree type which play a special role appear here for an entirely different reason than G_2, F_4 and E_8 appear in Theorem C. In fact, G_2, F_4 and E_8 appear in Theorem C because their (schematic) center is trivial, while the groups of Ree type appear as exceptions because their adjoint representations are reducible. In all other cases of reducibility, p divides the order of the center; in particular, the groups of Suzuki type are of type (i).

It is also of interest here to compare the growth of $t_n(\Delta)$ to $s_n(\Delta)$, the number of all open subgroups of index at most n. For $s_n(\Delta)$ the result is simple: $s_n(\Delta)$ grows polynomially if $p = 0$ [LM] and as fast as $n^{\log n}$ if $p > 0$ (see [LSh]).

The paper is organized as follows: In §1, we collect some general results on counting normal subgroups and other preliminaries. Special attention is called to Proposition 1.5 which seems to be new and useful. In §2, we treat the local case and prove a stronger version of Theorem D, and in §3 Theorem C is proven. Section 4 deals with the question of specializing groups while preserving their Zariski closures and Theorem 4.1 is proved. All this is collected to deduce Theorem B in §5.

In preparing for the proof of Theorem B a subtle difficulty has to be confronted: with subgroup growth, one can pass without restricting generality to a finite index subgroup and so one can always assume that the Zariski closure G of Γ is connected. On the other hand, normal subgroup growth may be sensitive to such a change. We must therefore handle also the non-connected case. So Theorem C and Theorem D are proven also for the case where G is not necessarily connected.

Raghunathan has made fundamental contributions to the study of congruence subgroups (cf. [R1] [R2] and [R3]). We are pleased to dedicate this paper, which counts congruence subgroups, as a tribute to him.

Notations and conventions

If $g, f\colon \mathbb{N} \to \mathbb{R}$ are functions, we say that g grows at least as fast as f and write $g \succeq f$ if there exists a constant $0 < a \in \mathbb{R}$ such that $g(n) \geq f(n)^a$ for every large n. We say that g and f have the same growth type if $g \succeq f$ and $f \succeq g$, or equivalently if $\log f(n) \approx \log g(n)$.

Algebraic groups are geometrically reduced, possibly disconnected affine group scheme of finite type over a field. They are generally written in italics. We use calligraphic letters for groups schemes to emphasize that they are *schemes*, either because the base is not a field or because we wish to allow non-reduced groups. The superscript $^\circ$ denotes identity component and $\tilde{X}$ is the universal covering group of X. Semisimple groups are connected, but simple groups may have a finite center.

If Δ is a discrete (resp. profinite) group we denote by $T_n(\Delta)$ the set of normal (resp. normal open) subgroups of Δ of index at most n and $t_n(\Delta) = |T_n(\Delta)|$.

1 Counting normal subgroups and preliminaries

In this short section we assemble few propositions mainly about counting normal subgroups in finitely generated (discrete or profinite) groups, that will be used in the following sections.

Proposition 1.1. *Let Γ be a finitely generated group and K a finite normal subgroup of Γ. Then the normal subgroup growth type of Γ is the same as that of $\Delta = \Gamma/K$.*

Proof. Clearly $t_n(\Gamma) \geq t_n(\Delta)$. On the other hand, every $N \in T_n(\Gamma)$ gives rise to a subgroup NK/K of Δ of index at most n. So the map $N \to NK/K$ is a surjective map from $T_n(\Gamma)$ onto $T_n(\Delta)$. If it is not true that $t_n(\Delta) \succeq t_n(\Gamma)$, then for infinitely many values of n, $t_n(\Delta) \leq t_n(\Gamma)^{1/2}$. For such an n, the fiber of at least one element in $T_n(\Delta)$ is of order at least $s = \left[t_n(\Gamma)^{1/2}\right]$, i.e., there exist $N_1, \ldots, N_s \in T_n(\Gamma)$ such that all N_iK are equal to each other – say to $\overline{N}$. There are only a bounded number c_1 of possibilities for $N_i \cap K \lhd K$, hence by replacing s by $\left[\frac{s}{c_1}\right]$ we can assume that all the groups N_i have the same intersection K_1 with K. Thus $\overline{N}/K_1 \simeq N_i/K_1 \times K/K_1$ for every i. As there are $\left[\frac{s}{c_1}\right]$ different N_i/K_1, it follows that $\overline{N}/K_1$ has at least $\left[\frac{s}{c_1}\right]$ different Γ-homomorphisms to K/K_1. The number of endomorphisms of K/K_1 is bounded by c_2, so $N_i/K_1 \simeq \overline{N}/K$ has at least $\left[\frac{s}{c_1c_2}\right]$ different Γ-homomorphisms to K/K_1. This shows that $\overline{N}/K$ has at least $\left[\frac{s}{c_1c_2c_3}\right]$ subgroups which are normal in Γ/K and their index in $\overline{N}$ is at most $|K/K_1|$, so their index in Γ is at most $[\Gamma\colon \overline{N}] \cdot |K/K_1| \leq \frac{n}{|K/K_1|} \cdot |K/K_1| = n$. Thus $t_n(\Delta) \geq \left[\frac{s}{c_1c_2c_3}\right]$ and Δ has the same growth as of Γ. ☐

Proposition 1.2. *Let Γ be a finitely generated group and Δ a finite index normal subgroup of Γ. Then there exists two constants c_1 and c_2 such that*

$$t_n(\Gamma) \leq c_1 n^{c_2} t_n(\Delta)$$

Remark. We do not know a useful upper bound on $t_n(\Delta)$ in terms of $t_n(\Gamma)$. Such a bound could save us the trouble of treating non-connected algebraic groups.

Proof. If $N \in T_n(\Gamma)$ then $D = N \cap \Delta \in T_n(\Delta)$ and $K = N\Delta$ is normal in Γ containing Δ. Given D and K as above, the number of $N \lhd \Gamma$ with $N \cap \Delta = D$ and $N \cdot \triangle = K$ is bounded by n^c for a suitable constant c. Indeed, N/D should be a normal complement to the normal subgroup Δ/D in K/D. The number of such complements is bounded by the number of possible $\Gamma-$ homomorphisms from K/D to Δ/D. The latter is at most $|\Delta/D|^{d_\Gamma(K)}$ where $d_\Gamma(K)$ denotes the number of Γ-generators of K. The proposition now follows with c_1 equals the number of normal subgroups K of Γ containing Δ and c_2 the maximum of $d_\Gamma(K)$ over these possible K. ☐

Lemma 1.3. *Let $G = A \times B$ be a product of two groups and $N \lhd G$. Let $A_1 = N \cap A, B_1 = N \cap B, A_2 = \pi_A(N)$ and $B_2 = \pi_B(N)$ where π_A and π_B are the projections to A and B, respectively. Then*

(i) *A_2/A_1 (resp. B_2/B_1) is central in A/A_1 (resp. B/B_1).*

(ii) *There exists an isomorphism $\varphi\colon A_2/A_1 \to B_2/B_1$ such that $N/(A_1 \times B_1)$ is the graph of φ.*

Proof. Clearly $A_2/A_1 \xleftarrow{\sim} N/(A_1 \times B_1) \xrightarrow{\sim} B_2/B_1$, and this defines φ satisfying (ii). We claim that A_1/A_2 is central in A/A_1. Indeed, for all $x \in A$

$$(xA_1, B_1)^{-1}\,(aA_1, \varphi(aA_1))\,(xA_1, B_1) = \big(x^{-1}axA_1, \varphi(aA_1)\big).$$

As φ is an isomorphism, this implies $x^{-1}axA_1 = aA_1$, i.e., aA_1 commutes with xA_1. By symmetry B_2/B_1 is central in B/B_1 and (i) is proved. □

Corollary 1.4. *Let $G = A \times B$ as above. If for every (finite index) normal subgroup $M \lhd A, Z(A/M) = \{1\}$, then every (finite index) normal subgroup $N \lhd G$ is of the form $N = (N \cap A) \times (N \cap B)$.* □

Proposition 1.5. *Let $G = A \times B$ be a product of two groups. Then:*

$$t_n(G) \le t_n(A)^2 \cdot t_n(B)^2 \cdot z_n(A)^{\delta_n(A)}$$

where

$$z_n(A) = \max\{|Z(A/N)| \,\big|\, N \lhd A \ \text{ and } \ [A\colon N] \le n\}$$

and

$$\delta_n(A) = \max\{d\big(Z(A/N)\big) | N \lhd A \ \text{ and } \ [A\colon N] \le n\}$$

(when $d(X)$ denotes the number of generators of X).

Proof. Apply Lemma 1.3. The two pairs of normal subgroups $A_1 \le A_2$ in A and $B_1 \le B_2$ in B (so that A_2/A_1 (resp. B_2/B_1) is central in A/A_1 (resp. B/B_1)) together with the isomorphism $\varphi\colon A_2/A_1 \to B_2/B_1$ determine N. This proves that

$$t_n(G) \le t_n(A)^2 \cdot t_n(B)^2 \cdot h_n$$

where h_n is the maximum possible number of isomorphisms from A_2/A_1 to B_2/B_1 as above, or equivalently, h_n is an upper bound on the number of automorphisms of A_2/A_1 when $A_1 \le A_2$ are normal subgroups of index at most n in A, such that A_2/A_1 is central in A/A_1. Clearly $h_n \le z_n(A)^{\delta_n(A)}$ (note that as A_2/A_1 is abelian and central in A/A_1, $d(A_2/A_1) \le d\big(Z(A/A_1)\big)$. The proposition is therefore proved. □

Proposition 1.6. *If Γ is a finitely generated discrete or profinite group, then $t_n(\Gamma) \preceq n^{\log n}$.*

Proof. This is proved in [L3] for the free groups; it therefore follows for every group. $\square$

Remark 1.7. While the proof of the general result in [L3] requires the classification of the finite simple groups (CFSG), this is not always needed for a given profinite or discrete group. The CFSG has been used in [L3] via the result of Holt [Ho] which implies that for every finite simple group G, every prime p and every simple $\mathbb{F}_p[G]$-module $M, \dim H^2(G, M) = O(\log |G|) \dim M$. Now, if Γ is a profinite group whose finite composition factors satisfy Holt's inequality (for every p and every M) then Proposition 1.6 holds for Γ. Now, the proof of Holt in [Ho] for the *known* simple groups is still valid, even if one does not assume the CFSG. In our papers, all the relevant profinite groups are such that almost all their composition factors are known, so Proposition 1.6 holds for them. It is worth mentioning that we also use [P2] later, which not only improves [W] but also frees it from CFSG. Our paper is therefore classification free!

Proposition 1.8. *Let G be a simple algebraic group defined over an algebraically closed field F of characteristic $p \geq 0$. Let $\tilde{G}$ be the universal cover of G and $\mathcal{Z}(\tilde{G})$ its scheme-theoretic center. Assume $p \nmid |\mathcal{Z}(\tilde{G})|$ and that the action of G on $L = Lie(G)$ is not irreducible. Then either (i) $p = 2$ and G is of type F_4 or (ii) $p = 3$ and G is of type G_2. In either case L has an ideal $I \triangleleft L$ such that L/I is isomorphic to I (as a Lie algebra and as G-module). In case (i), I is of type D_4 and in case (ii) of type A_2.*

Proof. See [H]. $\square$

Throughout the paper if we are in either case (i) or (ii), we say that G is a group of **Ree type**.

2 The local case

Let k be a local (non-archimedean) field of characteristic $p \geq 0$, and G an algebraic group defined over k, with a semisimple connected component G°, whose universal cover we denote $\widetilde{G^\circ}$. Let $\mathcal{Z}$ be the scheme-theoretic center of $\widetilde{G^\circ}$. It is a finite group scheme of order $z = |\mathcal{Z}|$. In other words z is the dimension of the coordinate ring of $\mathcal{Z}$ as a vector space over k. Another way to think about z is as the index of the lattice generated by the absolute roots of G° in the lattice of weights.

We can now state the main result of this section.

Theorem 2.1. *Let G be as above and M a (topologically) finitely generated Zariski-dense compact subgroup of $G(k)$. Then the normal subgroup growth rate of M is:*

(i) $n^{\log n}$ *if* $p \Big| \; |\mathcal{Z}|$

(ii) n *if* $p \nmid |\mathcal{Z}|$ *and* G° *has a simple factor of Ree type*

(iii) $\log n$ *otherwise.*

Let us start with an example which is also treated in [BG].

Example 2.2. Let $M = SL_d(\mathbb{F}_p[[t]])$. If $p \nmid d$ then for every open normal subgroup N of M, there exists $r \in \mathbb{N}$ such that $Q_r \subseteq N \subseteq Z_r$ where

$$Q_r = Ker(SL_d(\mathbb{F}_p[[t]]) \to SL_d(\mathbb{F}_p[[t]]/(t^r))$$

and Z_r is the preimage in M of the center of $\overline{M}(r) = SL_d(\mathbb{F}_p[[t]]/(t^r))$. Such N is of index approximately $p^{(d^2-1)r}$ and Z_r/Q_r is of order bounded independently of r, so there are only a bounded number of possibilities for such N. Hence $t_n(M)$ grows like $\log n$.

On the other hand, if $p|d$, then for every r, the group $\overline{M}(pr)$ has a large center: it consists of all the scalar matrices of the form $(1+y)I_d$ where $y \in (t^r)/(t^{pr})$. Note that $(1+y)^p = 1$ in the ring $\mathbb{F}_p[[t]]/(t^{pr})$, so $det\big((1+y)I_d\big) = 1$. Now, $|(t^r)/(t^{pr})| = p^{(p-1)r}$ and so $\overline{M}(pr)$ has a p-elementary abelian central subgroup of rank $(p-1)r$. Hence, it has at least $p^{\frac{1}{4}(p-1)^2r^2}$ normal subgroups of index at most $|M(pr)| \approx p^{(d^2-1)pr}$. Therefore $t_n(M)$ grows at least as fast as $n^{\log n}$. By (1.6), this is the largest normal subgroup growth possible.

The proof of Theorem 2.1 will depend on a careful analysis of principal congruence subgroups.

Let $\mathcal{O}$ be the discrete valuation ring of k, π a uniformizer and $\mathbb{F}$ the residue field. Let $\mathcal{G}/\mathcal{O}$ denote a smooth group scheme. In particular, if G is a semisimple algebraic group over k and X the associated Bruhat-Tits building, then for every point x of X, the stabilizer of x in $G(k)$ is equal to $\mathcal{G}(\mathcal{O})$ for some such $\mathcal{G}$ [BT, 5.1.9]. For each positive integer n, $\mathcal{G}(\mathcal{O}/\pi^n\mathcal{O})$ is finite and the reduction map $\mathcal{G}(\mathcal{O}) \to \mathcal{G}(\mathcal{O}/\pi^n\mathcal{O})$ is surjective (since $\mathcal{G}$ is smooth). The kernel Q_n is called the n-th *principal congruence subgroup.* These subgroups are closely related to the Lie algebra $\mathcal{L} = Lie(\mathcal{G}/\mathcal{O})$, which is by definition the dual of the pull-back of the relative cotangent bundle $\Omega^1_{\mathcal{G}/\mathcal{O}}$ by the identity section. As $\mathcal{O}$-module, $\mathcal{L}$ is free of rank equal to the relative dimension of $\mathcal{G}/\mathcal{O}$. This construction commutes with base change [SGA3, II 4.11]; in particular, $\mathcal{L} \otimes k$ and $\mathcal{L} \otimes \mathbb{F}$ are the Lie algebras of the generic and special fiber, respectively. In the case that $\mathcal{G}$ is Chevalley, i.e. split semisimple, and $\mathcal{O} \simeq \mathbb{F}[[\pi]]$ then $\mathcal{L}$ is isomorphic to $(\mathcal{L} \otimes \mathbb{F})[[\pi]]$. If $a, b, \in \mathbb{N}$ with $a \leq b \leq 2a$, there exists a canonical isomorphism

$$\log_{(\pi^a)/(\pi^b)}\colon Q_a/Q_b \to (\pi^a\mathcal{O}/\pi^b\mathcal{O}) \otimes \mathcal{L}$$

(see [P1, 6.2]). If $c, d \in \mathbb{N}$ and $c \leq d \leq 2c$ the square

$$\begin{array}{ccc} Q_a/Q_b \times Q_c/Q_d & \xrightarrow{[\ ,\ ]} & Q_{a+c}/Q_{a+d} \cdot Q_{b+c} \\ {\scriptstyle \log}\big\downarrow & & \big\downarrow{\scriptstyle \log} \\ \pi^a L/\pi^b L \times \pi^c L/\pi^d L & \xrightarrow{[\ ,\ ]} & \pi^{a+c} L/(\pi^{a+d} L + \pi^{b+c} L). \end{array}$$

commutes.

We can now begin the proof of Theorem 2.1, starting with the lower bounds. One can easily see that the principal congruence subgroups (with respect to any fixed faithful representation of G into GL_n) described above assure that the normal subgroup growth is always at least logarithmic.

The cases of interest for lower bounds are when either $p \big| |\mathcal{Z}|$ or G is of Ree type.

The reader should note that these lower bounds arguments are complicated by the difficulty mentioned in the introduction (see also (1.2)) that obliges us to consider non-connected groups.

We will use the notation and terminology of [P1]. Replacing G by a quotient we may assume that G° is a product of isomorphic adjoint simple groups $G_i, i = 1, \ldots, r$, that G/G° acts transitively on the factors G_i, and that $Cent_G(G^\circ)$ is trivial. Let $F = k^r$, $M^\circ = M \cap G^\circ(k)$ and $\mathcal{G}^\circ$ be the adjoint simple group scheme over F such that $\mathcal{G}^\circ(F) = G(k)$. Let $(E, \mathcal{H}^\circ, \varphi)$ be the minimal quasi-model of $(F, \mathcal{G}^\circ, M^\circ)$. Thus $\mathcal{H}^\circ$ is adjoint simple, E is a closed subalgebra of F, which is a product of local fields, M° can be regarded as a Zariski dense subgroup of $\mathcal{H}^\circ(E)$ and $\varphi : \mathcal{H}^\circ \underset{E}{\times} F \to \mathcal{G}^\circ$ is an isogeny, which induces an isomorphism on the embeddings of M°. By the (essential) uniqueness of the minimal quasi-model [P1, 3.6] and the transitivity of the action of M/M° on the factors of F, we conclude that M/M° acts transitively on the factors of E. Furthermore, E has the same number of factors as F since M° is Zariski dense in G°. So we write $E = k'^r$ where k' is a (local) subfield of k. The restriction of scalars of $\mathcal{H}^\circ$ to k' is a product H° of isomorphic adjoint simple factors H_i, $i = 1, \ldots, r$ and φ is a product of identical isogenies φ_i: $H_i \underset{k'}{\times} k \to G_i$. Let $H^{out} = H^\circ \rtimes Out(H^\circ)$, $\widetilde{H^{out}} = \widetilde{H^\circ} \rtimes Out(H^0)$, and $G^{out} = G^\circ \rtimes Out(G^\circ)$. Note that $Out(G^\circ)$ and $Out(H^\circ)$ are canonically isomorphic. In fact G° and H° have the same root system except possibly in characteristic 2 where there exist isogenies between groups of type B_n and C_n. Even though G need not map to G^{out}, if $\overline{k}$ is an algebraic closure of k, $G(\overline{k})$ is naturally a finite index subgroup of $G^{out}(\overline{k})$, and we regard M as a subgroup of the latter. We extend φ to φ^{out}: $H^{out} \underset{k'}{\times} k \to G^{out}$ to identify $G^{out}(\overline{k})$ with $H^{out}(\overline{k})$. Finally, we pull back by the natural map $\widetilde{H^{out}} \to H^{out}$ to obtain a group $\tilde{M} \leq \widetilde{H^{out}}(\overline{k})$. As M is a quotient of $\tilde{M}$ by a finite normal subgroup, it suffices by (1.1) to give a lower bound for $t_n(\tilde{M})$.

Let $\tilde{M}^\circ = \tilde{M} \cap \tilde{H}^\circ(k')$. By [P1, 0.2], $\tilde{M}^\circ$ is an open subgroup of $\tilde{H}^\circ(k')$. Let π denote the universal cover map $\tilde{H}^\circ \to H^\circ$. Then $H^\circ(k')/\pi\big(\tilde{H}^\circ(k')\big)$ is an abelian torsion group. As $\tilde{M}$ is finitely generated, the image of $\tilde{M} \cap \tilde{H}^\circ(\overline{k})$ in this quotient is finite, so $\tilde{M}^\circ$ is a finite index subgroup of $\tilde{M} \cap \tilde{H}^\circ(\overline{k})$ and therefore of $\tilde{M}^\circ$. As M normalizes M°, a Zariski dense subgroup of H°, it normalizes H° itself and likewise $H^\circ(k')$; by the same argument $\tilde{M}$ normalizes $\tilde{H}^\circ(k')$. We conclude that $\tilde{M}^\circ$ is normal in $\tilde{M}$.

As $\tilde{M}$ is compact, its conjugation action fixes a point x in the Bruhat-Tits building of $\widetilde{H^\circ}(k')$. Let $\mathcal{F}$ be the smooth group scheme over $\mathcal{O}$ corresponding to x. As $\tilde{M}$ fixes x, conjugation by any element of $\tilde{M}$ gives an automorphism of $\mathcal{F}$. Let Q_n denote the n-th principal congruence subgroup of $\mathcal{F}(\mathcal{O})$. By construction, it is normalized by $\tilde{M}$.

Let $\mathcal{Z}$ denote the identity component of the scheme theoretic center of $\widetilde{H^\circ}$ and $\mathcal{Z}_\mathcal{F}$ the Zariski closure of $\mathcal{Z}$ in $\mathcal{F}$. Note that for any $\mathcal{O}$-algebra R, $\mathcal{Z}_\mathcal{F}(R)$ lies in the center of $\mathcal{F}(R)$.

Lemma 2.3. *Let $\mathcal{O} = \mathbb{F}[[\pi]]$, Δ a finite group and B a commutative $\mathcal{O}[\Delta]$-algebra which is finite as a module. Suppose that the nil radial I of $B \underset{\mathcal{O}}{\otimes} k$ is non-trivial and* $\dim_k(B \underset{\mathcal{O}}{\otimes} k)/I = 1$. *Then there exists a non-trivial $\mathbb{F}[\Delta]$-module T and a positive integer γ such that for every $n \in \mathbb{N}$, $Hom_{ring}(B, \mathcal{O}/\pi^{2\gamma n}\mathcal{O})$ contains T^n as a submodule.*

We apply the lemma in the case B is the coordinate ring of $\mathcal{Z}_\mathcal{F}$ and $\Delta = \tilde{M}/(\widetilde{H^\circ}(k') \cap \tilde{M})$; note that $Hom_{ring}(B, \mathcal{O}/\pi^{2\gamma n}\mathcal{O})$ and hence T^n sits as a subgroup of $\tilde{M}/Q_{2\gamma n}$ for n sufficiently large. Now, as $T^n \simeq T \otimes (\mathcal{O}/(\pi))^n$ as Δ-modules, we can deduce that $\tilde{M}$ has at least $p^{\frac{1}{4}n^2}$ normal subgroups of index at most $\left|\tilde{M}/Q_{2\gamma n}\right| \sim c_0^{2\gamma n}$ for some constant c_0. This finishes the proof of the lower bound modulo the lemma.

Proof of Lemma 2.3 Let J be the nil radical of B and $S = \bigcup_{r=1}^{\infty} \{x \in B \big| \pi^r x \in J\}$ its π-saturation. Then B/S is a finitely generated torsion free $\mathcal{O}$-module, hence free over $\mathcal{O}$, and the codimension condition on $I = S \underset{\mathcal{O}}{\otimes} k$ implies that the rank of B/S is 1. Thus $B = \mathcal{O} \oplus S$ as $\mathcal{O}$-module. Any $\mathcal{O}$-linear map from S/S^2 to $\pi^{\gamma n}\mathcal{O}/\pi^{2\gamma n}\mathcal{O}$ gives an $\mathcal{O}$-algebra homomorphism $B \to \mathcal{O}/\pi^{2\gamma n}\mathcal{O}$. By Nakayama's Lemma, $(S/S^2) \underset{\mathcal{O}}{\otimes} k = I/I^2 \neq (0)$, so the free $\mathcal{O}$-module $(S/S^2)/(S/S^2)_{tor}$ is a non-zero $\mathcal{O}[\Delta]$-module and $N = Hom_\mathcal{O}(S/S^2, \mathcal{O})$ is a non-zero $\mathcal{O}[\Delta]$-module which is $\mathcal{O}$-free. It suffices to find an $\mathbb{F}[\Delta]$-module appearing with multiplicity at least n in $N/\pi^{\gamma n}N$. Choose $v \in N \backslash \pi N$ and then choose γ such that $\mathbb{F}[\Delta]v \backslash \{0\} \subseteq N \backslash \pi^\gamma N$. Then

$$\mathbb{F}[\Delta]\{v, \pi^\gamma v, \ldots, \pi^{\gamma(n-1)}v\} \simeq \bigoplus_{i=0}^{n-1} \mathbb{F}[\Delta]\pi^{i\gamma} v \simeq \bigoplus_{i=0}^{n-1} \mathbb{F}[\Delta]v.$$

This proves the lemma with $T = \mathbb{F}[\Delta]v$. □

We turn now to proving the lower bound for the Ree cases.

Lemma 2.4. *Assume $char(k) = 2$ (resp. 3) and G° has at least one factor of type F_4 (resp. G_2). If M is a compact open subgroup of $G(k)$ then $t_n(M)$ has growth rate at least n.*

Proof. Without loss of generality we may assume that G° is isotypic and $M/M \cap G^\circ(k)$ acts transitively on the factors. We claim that every k-automorphism of a simple group H which is both adjoint and simply connected is an inner automorphism by an element of $H(k)$. Indeed, Dynkin diagrams of adjoint simply connected simple groups have no symmetries, so every automorphism is of the form $ad(x)$ for $x \in H(\bar{k})$; as $ad(x)$ is a k-automorphism of the Lie algebra of H and the adjoint representation is faithful, this implies $x \in H(k) \subset GL_{\dim(H)}(k)$. We can therefore write $G = G^\circ \rtimes M/M^\circ$.

As before we may assume that the image Δ of M in $Out(G^\circ)$ acts transitively on the factors. The projection of $M \cap G^\circ(k)$ to each factor is then the same: a compact open subgroup C of $F_4(k)$ (resp. $G_2(k)$). Let $\mathcal{H}$ denote a smooth group scheme over $\mathcal{O}$ such that C lies in $\mathcal{H}(\mathcal{O})$ as an open subgroup. Thus M is contained in $\mathcal{H}(\mathcal{O})^r \rtimes G/G^\circ$ and by Propositions 1.1 and 1.2, we can assume $M = \mathcal{H}(\mathcal{O})^r \rtimes \Delta$. If $N \in T_n\big(\mathcal{H}(\mathcal{O})\big)$, then N^r is an open normal subgroup of M of index $\leq |\Delta| n^r$, so without loss of generality we may assume that $G = G^\circ$ is simple and $M = \mathcal{H}(\mathcal{O})$. Let $\mathcal{L} = Lie(\mathcal{H}/\mathcal{O})$. By [1.8], $\mathcal{L} \otimes k$ has a unique proper ideal I, and $(\mathcal{L} \otimes k)/I$ is isomorphic as $\mathcal{L} \otimes k$ module to I. We fix an isomorphism $\psi \colon (\mathcal{L} \otimes k)/I \to I$ such that $\psi(\mathcal{L}/I \cap \mathcal{L}) \subseteq \mathcal{L}$.

Let d be a positive integer and $q(x)$ a polynomial of degree less than d with coefficients in the field of constants of k. Let

$$N_{d,q} = \{\pi^{2d}\psi(\alpha) + \pi^{3d}q(\pi)\alpha \big| \alpha \in \mathcal{L}/\pi^{2d}\mathcal{L}\} \subseteq \pi^{2d}\mathcal{L}/\pi^{4d}\mathcal{L}$$

For fixed d and varying q, we obtain a family of pairwise distinct $\mathcal{L}$-submodules of $\pi^{2d}\mathcal{L}/\pi^{4d}\mathcal{L}$ of cardinality exponential in d. Pulling back by the map $\log_{(\pi^{2d})/(\pi^{4d})}$ we obtain subgroups of Q_{2d}/Q_{4d} and therefore open subgroups of M. By [P1, 6.2(c)] these subgroups are normal. So we have exhibited c_1^d normal open subgroups of M of index at most $[M \colon Q_{4d}] \sim c_2^d$. This finishes the proof of the proposition. We have therefore proved the lower bounds in all cases of Theorem 2.1. □

We turn now to the proof of the upper bounds. First note that the upper bound for case (i) follows immediately from (1.6), as $n^{\log n}$ is the maximal normal subgroup growth rate possible for finitely generated groups.

We now turn to the proof of the upper bound in the remaining cases. We have already seen that without loss of generality we may assume that M contains an open subgroup which is also an open subgroup of the k-points of a connected, simply connected semisimple group. For upper bounds, we are free to pass to subgroups of finite index (see 1.2)), so we can assume from now on that M is open in $G(k)$. Let us start with the generic case.

Proposition 2.5. *Let G/k be a simple algebraic group not of Ree type and for which $p \nmid |\mathcal{Z}(\tilde{G})|$. Let $M \leq G(k)$ be a compact open subgroup. Then*

(i) *there exists a constant c such that for every N open and normal in M, $|Z(M/N)| < c$;*

(ii) $t_n(M) \preceq \log n$.

Proof. Let $\mathcal{G}/\mathcal{O}$ be a smooth group scheme with generic fiber G and $M \subseteq \mathcal{G}(\mathcal{O})$. Let $\mathcal{L} = Lie(\mathcal{G}/\mathcal{O})$. By (1.8), $L = \mathcal{L} \otimes k$ is a simple Lie algebra, so there exists $\ell \in \mathbb{N}$ such that the ℓ-th iterated Lie bracket $[L, [L, [\ldots, [L, x]] = L$ for all non-zero $x \in L$. Thus $[\mathcal{L}, [\mathcal{L}, [\ldots, [\mathcal{L}, x]]$ contains an open neighborhood $\pi^{n_x}\mathcal{L}$ of zero for all $x \in \mathcal{L} \setminus \{0\}$. By compactness, there is a uniform upper bound n on n_x as x ranges over $\mathcal{L} \setminus \pi\mathcal{L}$.

Replacing M if necessary by a finite index subgroup, we may assume $M = Q_m$, for some $m > n$. If $\mathbb{N} \ni r \geq m$ and $x \in \pi^r\mathcal{L} \setminus \pi^{r+1}\mathcal{L}$ then for every $i \in \mathbb{N}$,

$$[\pi^i\mathcal{T}, [\mathcal{T}, \ldots, [\mathcal{T}, \overline{x}] \ldots] \supseteq \pi^{i+\ell m+r+n}\mathcal{L}/\pi^{(i+\ell+1)m+r}\mathcal{L}$$

where $\overline{x}$ is the projection of x to $\pi^r\mathcal{L}/\pi^{r+m}\mathcal{L}$, $\mathcal{T} = \pi^m\mathcal{L}/\pi^{2m}\mathcal{L}$ and the bracket is taken ℓ times. (We are using the diagram, introduced earlier, computing brackets of quotients of principal congruence subgroups). Thus the topological normal closure of every element $y \in Q_r \setminus Q_{r+1}$ contains representatives of every class in $Q_{i+(\ell+1)m+r-1}/Q_{i+(\ell+1)m+r}$. So this normal subgroup contains $Q_{(\ell+1)m+r-1}$.

This shows that if N is a normal open subgroup of M containing an element outside Q_{r+1}, then N contains $Q_{(\ell+1)m+r-1}$. As ℓ and m are constants, this shows that there exists a constant c' such that for every normal subgroup N of M, there exists $n \in \mathbb{N}$, $n = O(\log[M\colon N])$, such that $Q_n \subseteq N \subseteq Q_{n-c'}$. The order of $Q_{n-c'}/Q_n$ is bounded, so for every n, there are only finitely many such possibilities for N. This proves that the normal subgroup growth of M is at most logarithmic. We also see that the center of Q_m/N is included in $Q_{n-c'-m}/N$, so its order is bounded. $\square$

Before passing to the semisimple case, let us first consider the Ree case for simple groups. We can then treat the semisimple case uniformly.

Proposition 2.6. *Let G/k be a simple group of Ree type and $M \subset G(k)$ an open compact subgroup. Then*

(i) *There exists a constant c such that for every open normal subgroup N of M, $|Z(M/N)| < c$.*

(ii) $t_n(M) \preccurlyeq n$.

(iii) *There exists a universal constant γ, independent of k, such that if M is hyperspecial, then for every normal subgroup N of M, $Z(M/N) = \{1\}$ and $t_n(M) \leq n^\gamma$ for every n.*

Proof. By [Ti], as k is local non-archimedean, G splits over k. There is therefore a split simple group scheme $\mathcal{G}/\mathcal{O}$ with generic fiber G, so that M is commensurable to $\mathcal{G}(\mathcal{O}) \subseteq \mathcal{G}(k) = G(k)$. By Proposition 1.2 we can replace M by any of its open subgroups, in particular by a principal congruence subgroup Q_m of $\mathcal{G}(\mathcal{O})$ when m is sufficiently large. Fix such an m and take $M = Q_m$. If m is hyperspecial, we take $m = 0$.

Let $\mathcal{L} = Lie(\mathcal{G}/\mathcal{O})$, $\overline{L} = \mathcal{L} \otimes \mathbb{F}$ and so $\mathcal{L} = \overline{L}[[\pi]]$. Let I denote the unique non-trivial ideal of $\overline{L}$. For every normal subgroup N of M, and for $r \in \mathbb{N}$, we denote by $gr_r N$ the quotient $(Q_r \cap N)/(Q_{r+1} \cap N) \subseteq \overline{L}$. Starting with a subset $Y \subseteq \overline{L}$, the iterative process $Y \mapsto [\overline{L}, Y]$ stabilizes after a bounded number ℓ of steps to $C(Y)$, the minimal ideal containing Y, i.e., either $0, I$ or $\overline{L}$. For all $r \in \mathbb{N}$ and $t \geq r + \ell m$

$$gr_t N \geq C(gr_r N).$$

Thus there exists integers a and b, $m \leq a \leq b$, such that

$$(*) \qquad gr_r N = \begin{cases} 0 & \text{if } r < a - \ell m \\ I & \text{if } a \leq r < b \\ \overline{L} & \text{if } r \geq b + \ell m. \end{cases}$$

One can also easily see that a and b or $O(\log[M\colon N])$. At this point part (i) follows by the same argument as (i) of Proposition 2.5. In the hyperspecial case, moreover, the center M/N is trivial.

It follows that

$$gr_r(Q_a \cap Q_b N) = \begin{cases} 0 & \text{if } r < a \\ I & \text{if } a \leq r < b \\ \overline{L} & \text{if } r \geq b. \end{cases}$$

We claim that for a fixed N satisfying $(*)$, the set of open normal subgroups $N' \subset M$ satisfying $(*)$ for the same constant a and b, with $Q_a \cap Q_b N' = Q_a \cap Q_b N$ is bounded by a polynomial in $|M/N|$. Indeed, $N' \supseteq Q_{b+\ell m}$ and $Q_b N'/Q_{b+\ell m}$ is generated by $(Q_a \cap Q_b N)/Q_{b+\ell m}$ and a bounded number of other elements of $Q_{a-\ell m}/Q_{b+\ell m}$, so the number of possibilities for $Q_b N'$ is bounded by $p^{c'b}$, hence polynomially in $|M/N|$. Now, as $N' \triangleleft Q_b N'$ is of bounded index, $N'/Q_{b+\ell m}$ is the kernel of a homomorphism from $Q_b N'/Q_{b+\ell m}$ to a group of bounded order. The number of generators of a group is logarithmic in its order, so the number of such homomorphism is again bounded polynomially in $|M/N|$. If $m = 0, N = Q_a \cap Q_b N$, so the number of possibilities for N' is 1, i.e., $N' = N$.

It therefore remains to fix (a, b) and count the number of normal open subgroups N of M with

$$(**) \qquad gr_r N = \begin{cases} 0 & \text{if } r < a \\ I & \text{if } a \le r < b \\ \overline{L} & \text{if } r \ge b. \end{cases}$$

At this point, if M is hyperspecial, it will be more convenient to reset m to 1. We now prove by induction that the number of possibilities for N satisfying $(**)$ is bounded above by $|\mathbb{F}|^{c_1(b-a)m}$ where c_1 is an absolute constant. For $b - a < 2m$ the claim is trivial. Suppose $b - a \ge 2m$. Let N_1 and N_2 denote two groups in this collection. Now, for $i \in \{1, 2\}$,

$$[Q_m, Q_{b-m}N_i] = [Q_m, Q_a \cap Q_{b-m}N_i] \subseteq Q_{a+m} \cap Q_b N_i = Q_{a+m} \cap N_i$$

At the associated graded level

$$gr_r[Q_m, Q_{b-m}N_i] = gr_r(Q_{a+m} \cap N_i) = \begin{cases} 0 & \text{if } r < a + m \\ I & \text{if } a + m \le r < b \\ \overline{L} & \text{if } r \ge b. \end{cases}$$

So $[Q_m, Q_{b-m}N_i] = Q_{a+m} \cap N_i$. By the induction hypothesis, the number of possibilities for $Q_{b-m}N_i$ is at most $|\mathbb{F}|^{c_1(b-a-m)m}$. We fix one, so

$$Q_{b-m}N_1 = Q_{b-m}N_2$$

and

$$Q_{a+m} \cap N_1 = Q_{a+m} \cap N_2.$$

We have a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
 & Q_{b-m}/Q_b \arrow[r, equal] \arrow[d] & Q_{b-m}/Q_b \arrow[d] & & \\
0 \arrow[r] & Q_{a+m}/Q_b \arrow[r] \arrow[d] & Q_a/Q_b \arrow[r] \arrow[d] & Q_a/Q_{a+m} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & Q_{a+m}/Q_{b-m} \arrow[r] \arrow[d] & Q_a/Q_{b-m} \arrow[r] \arrow[d] & Q_a/Q_{a+m} \arrow[r] & 0 \\
 & 0 & 0 & &
\end{tikzcd}$$

where the two columns are central extensions (as $(a+m)+(b-m)\geq b$ and $a+(b-m)\geq b$). Now, N_1/Q_b and N_2/Q_b are subgroups of Q_a/Q_b whose images in Q_a/Q_{b-m} and intersections with Q_{a+m}/Q_b coincide. Suppose their intersections with Q_{b-m}/Q_b are both equal to R/Q_b for some $R\supset Q_b$. The discrepancy between the groups N_i/Q_b is encoded by a homomorphism $N_1/Q_{b-m}\to Q_{b-m}/R$ which is trivial on $(N_1\cap Q_{a+m})/Q_{b-m}$, i.e., a homomorphism from a subgroup of Q_a/Q_{a+m} to a quotient group of Q_{b-m}/Q_b. The number of such homomorphisms is bounded by $||\mathbb{F}|^{c_2m^2}$ and the same applies to the number of possibilities R. Thus parts (ii) of the proposition are also proved. $\square$

We can now finish the proof of the upper bounds in Theorem 2.1. The only thing left is to extend Propositions 2.5 and 2.6, to the case that G is not necessarily simple. So let G be as in Theorem 2.1 parts (ii) and (iii). By passing to an open subgroup of M, which is permissible by (1.2), we can assume that M is a product $\prod_{i=1}^{r} M_i$ where M_i is an open compact subgroup of $S_i(k)$ and where S_i is a simple k-algebraic group.

We can now apply Proposition 1.5, with Propositions 2.5 and 2.6 to finish the proof. $\square$

Proof of Theorem D. Theorem D is a special case of Theorem 2.1; the only point to note is that since $\mathcal{G}_\eta$ is simply connected, $\Delta=\mathcal{G}(\mathcal{O})$ is finitely generated [BL]. $\square$

3 The global case

In this section we prove first the following Theorem 3.1, from which Theorem C is deduced. We then prove a variant of it, Proposition 3.2 below, to be used in the proof of Theorem B.

Theorem 3.1. *Let k be a global field of characteristic $p\geq 0$, S a non-empty set of valuations of k containing all the archimedean ones and*

$$\mathcal{O}_S=\{x\in k|v(x)\geq 0,\forall v\notin s\}.$$

Let $\mathcal{G}$ be a smooth group scheme over $\mathcal{O}_S$, whose generic fiber $\mathcal{G}_\eta$ is connected, simple and simply connected. Let H be the profinite group $\mathcal{G}(\hat{\mathcal{O}}_S)$. Then the growth type of $t_n(H)$ is:

(i) *n if $\mathcal{G}$ is of type G_2, F_4 or E_8.*

(ii) *$n^{\log n/(\log\log n)^2}$ if $\mathcal{Z}(\mathcal{G}_\eta)\neq 1$ and $p\nmid|\mathcal{Z}(\mathcal{G}_\eta)|$*

(iii) *$n^{\log n}$ if $p\Big||\mathcal{Z}(\mathcal{G}_\eta)|$.*

Proof. We remark first that $H = \mathcal{G}(\hat{\mathcal{O}}_S)$ is indeed a finitely generated group. This can be proved by analyzing the Frattini subgroup of $\mathcal{G}(\hat{\mathcal{O}}_S) = \prod\limits_{v \notin S} \mathcal{G}(\mathcal{O}_v)$, or, alternatively, as follows: for sufficiently large $S' \supset S$, the S'-arithmetic group $\mathcal{G}(\mathcal{O}_{S'})$ is finitely generated [Be] and dense in $\mathcal{G}(\hat{\mathcal{O}}_{S'})$ [PR], and $\mathcal{G}(\hat{\mathcal{O}}_S) = \mathcal{G}(\hat{\mathcal{O}}_{S'}) \times \prod\limits_{v \in S' \setminus S} \mathcal{G}(\mathcal{O}_v)$. As each of $\mathcal{G}(\mathcal{O}_v)$ is finitely generated [BL], so is $\mathcal{G}(\hat{\mathcal{O}}_S)$.

Case (iii) follows easily from Theorem 2.1, i.e., already the projection to one local factor gives growth type at least $n^{\log n}$. This, in turn, is the maximal possible normal subgroup growth type of finitely generated profinite groups by (1.6).

We first prove the lower bounds of (i) and (ii). For (i): $\mathcal{O}_S$ (and hence $\hat{\mathcal{O}}_S$) has at least cn ideals of index at most n, for some fixed $c > 0$ (depending on $\mathcal{O}_S$) and n sufficiently large. Each such ideal I gives rise to a principal congruence subgroup

$$Q(I) = Ker\big(\mathcal{G}(\hat{\mathcal{O}}_S) \to \mathcal{G}(\hat{\mathcal{O}}_S/I)\big)$$

of index at most n^d for some constant d. This shows that the growth type of $t_n(H)$ is at least n.

(ii) Let k' be a finite Galois extension of k, in which $\mathcal{Z} = \mathcal{Z}(\mathcal{G}_\eta)$ splits. In particular $\mathcal{Z}(k')$ is a finite group of order say z, and by our assumption in (ii), $p \nmid z$. Let $\mathcal{P}_1$ be the set of primes in k which splits completely in k' and $\mathcal{P} = \mathcal{P}_1 \setminus S$. By the Cebotarev density theorem, $\mathcal{P}_1$ (and as S is finite, also $\mathcal{P}$) has positive density.

For a large real number x, let $\mathcal{P}_x$ be the set of all primes in $\mathcal{P}$ of norm at most x (where a norm $|P|$ of a prime P is its index in $\mathcal{O}_S$). By the Prime Number Theorem and the positive density of $\mathcal{P}$, we have: $\pi(x)/\frac{x}{\log x}$ and $\psi(x)/x$ are both bounded away from zero and infinity when $\pi(x) = |\mathcal{P}_x|$ and $\psi(x) = \sum\limits_{P \in \mathcal{P}_x} \log |P|$.

Let $m(x) = \prod\limits_{P \in \mathcal{P}_x} P$ and let $Q\big(m(x)\big)$ denote, as before, the principal congruence subgroup $\big(\bmod\ m(x)\big)$. It follows that $|\mathcal{O}_S/m(x)| \approx c_1^x$ for some constant c_1. Fix now a prime q dividing z. Now:

$$H/Q\big(m(x)\big) \simeq \mathcal{G}\big(\mathcal{O}_S/m(x)\big) = \prod_{P \in \mathcal{P}_x} \mathcal{G}(\mathcal{O}_S/P).$$

This shows that $Q\big(m(x)\big)$ is of index at most c_2^x for some constant c_2. On the other hand, for each $P \in \mathcal{P}_x$, the finite group $\mathcal{G}(\mathcal{O}_S/P)$ has a central subgroup of order z, and hence also a central cyclic subgroup of order q. Hence $H/Q\big(m(x)\big)$ has a central subgroup which is a q-elementary abelian group of rank $\pi(x)$. This shows that $H/Q\big(m(x)\big)$ has at least $q^{\frac{1}{4}\pi(x)^2}$ central subgroups and hence H has at least $q^{\frac{1}{4}\pi(x)^2} \geq q^{\frac{1}{4c^2} \cdot \frac{x^2}{(\log x)^2}}$ normal subgroups of index at most c_2^x. This proves that the normal subgroup growth rate of H is at least $n^{\log n/(\log\log n)^2}$.

We turn now to the proof of the upper bound. We start with both cases, (i) and (ii), together. We assume without loss of generality that G is connected (see (1.2)).

We have to prove an upper bound for $t_n\big(\mathcal{G}(\hat{\mathcal{O}}_S)\big)$. Note that $\mathcal{G}(\hat{\mathcal{O}}_S) = \prod_{v \notin S} \mathcal{G}(\mathcal{O}_v)$. Let $\mathcal{P}$ denote the set of all primes of k which are not in S. Let $\mathcal{P}_1$ be the set of all $v \in \mathcal{P}$ such that:

(a) $\mathcal{G}(\mathbb{F}_v)$ is an almost simple group, where $\mathbb{F}_v = \mathcal{O}_v/m_v$ and m_v is the maximal ideal of $\mathcal{O}_v$.

(b) If $Q_v(r) = Ker(\mathcal{G}(\mathcal{O}_v) \to \mathcal{G}\big(\mathcal{O}_v/m_v^r)\big)$ then $[Q_v(1), Q_v(i)] = Q_v(i+1)$ for every $i \geq 1$.

(c) The elementary abelian p-group $Q_v(1)/Q_v(2)$ is a simple $\mathcal{G}(F_v)$-module, and

(d) If $p = 0,\ v \nmid |\mathcal{Z}(\mathcal{G})|$

Now, unless $\mathcal{G}_\eta$ is of Ree type $\mathcal{P}_1$ contains almost all primes in $\mathcal{P}$. By [SGA 3, XIX 2.5] all but finitely many fibers of $\mathcal{G}$ are simple. This implies (a). For (b) we use (1.8) and the logarithm map discussed in Section 2. For (c), we note that every composition factor of the adjoint representation of the special fiber is $|\mathbb{F}_v|$-restricted except if $|\mathbb{F}_v| = 2$ and $\mathcal{G}_\eta$ is a form of SL_2. By Steinberg's theorem [St], any restricted irreducible representation is irreducible over $\mathcal{G}(\mathbb{F}_v)$. As $\mathcal{G}_\eta$ is not of Ree type and $p \nmid z$, the irreducibility of the adjoint representation follows from (1.8). Part (d) is clear.

Leaving aside for now the two exceptional cases, consider $S_1 = S \cup \{v | v \notin \mathcal{P}_1\}$ and $H_1 = \mathcal{G}(\hat{\mathcal{O}}_{S_1}) = \prod_{v \in \mathcal{P}_1} \mathcal{G}(\mathcal{O}_v)$. One proves by induction that for every open normal subgroup N of H_1, there exists an ideal I in $\mathcal{O}_{S_1}$ such that $Q_1(I) \subseteq N \subseteq Z_1(I)$ when

$$Q_1(I) = Ker\big(\mathcal{G}(\hat{\mathcal{O}}_{S_1}) \to \mathcal{G}(\hat{\mathcal{O}}_{S_1}/I)\big)$$

and $Z_1(I)$ is the preimage in H_1 of the center of $\mathcal{G}(\hat{\mathcal{O}}_{S_1}/I)$. It now follows, by a similar computation to the one carried out above for the lower bound, that the normal subgroup growth rate of H_1 is n in case (i) and $n^{\log n/(\log\log n)^2}$ in case (ii).

Now $H = H_1 \times H_2$ where $H_2 = \prod_{v \notin \mathcal{P}_1 \cup S} \mathcal{G}(\mathcal{O}_v)$. This is a product of finitely many groups. The normal subgroup growth rate of H_2 is at most polynomial by Theorem 2.1, Proposition 1.5 and Proposition 2.5.

We can now finish the proof with the help of Proposition 1.5: In case (i), note that the only open normal subgroups of H_1 are the principal congruence subgroups $Q_1(I)$, and $H_1/Q_1(I)$ has no center. So $t_n\big(\mathcal{G}(\hat{\mathcal{O}}_S)\big) \leq t_n(H_1)^2 \cdot t_n(H_2)^2$, and so it is polynomially bounded. In case (ii), the normal subgroups of H_1 lie between $Q_1(I)$ and $Z_1(I)$. Note that if I is an ideal of index n^ε, which is a product of m prime powers then $m \leq c\frac{\log n}{\log\log n}$ (by the prime number theorem). So the center $Z_1(I)/Q_1(I)$ is of order at most $z^{c\log n/\log\log n}$ and its number of generators is at most $c' \log n/\log\log n$ (in fact $c' \leq 2c$). This shows that $z_n(H_1) \leq z^{c\log n/\log\log n}$ and $\delta_n(H_1) \leq c' \log n/\log\log n$ where z_n and δ_n are as in (1.6). Thus

$t_n(H) \leq t_n(H_1)^2 t_n(H_2)^2 \cdot z^{cc'(\log n/\log\log n)^2}$. As z is a constant, we have finished the proof except for groups of Ree type.

For these two cases, let us make the following remarks. As before we decompose $H = H_1 \times H_2$ where $H_1 = \prod_{v \in \mathcal{P}_1} \mathcal{G}(\mathcal{O}_v)$ and $\mathcal{P}_1$ is the set of all primes v for which $\mathcal{G}(\mathcal{O}_v)$ is hyperspecial. By [SGA3, XIX 2.5], for almost all primes $\mathcal{G}_{\mathbb{F}_v}$ is simple and this implies that $\mathcal{G}(\mathcal{O}_v)$ is hyperspecial. As before H_2 is a finite product of local groups, and in this case the factors are of Ree type. By Theorem 2.1(ii), $t_n(H_2)$ is polynomially bounded. By Proposition 1.5, $t_n(H) \leq t_n(H_1)^2 t_n(H_2)^2 z_n(H_1)^{\delta_n(H_1)}$. As H_1 is a product of hyperspecial factors, its quotient by any open normal subgroup has trivial center by Proposition 2.6(iii). It suffices, therefore, to prove that $t_n(H_1)$ is polynomially bounded.

Let $N \in T_n(H_1)$. Then there exists an ideal I such that $N \supset Q_1(I)$. We claim that I can be chosen to be so that $Q_1(I)$ has index at most n^{c_1} for some constant c_1. Indeed choose first $I = \prod_{i=1}^{r} P_i^{e_i}$ to be some ideal so that $N \supset Q_1(I)$. So $N/Q_1(I)$ is a normal subgroup of $S = \prod_{i=1}^{r} \mathcal{G}(\mathcal{O}_{P_i}/P_i^{e_i})$. Now, as the centers of all the quotients of S are trivial, we deduce from (1.4) that N is a product of its intersections with the factors. In the proof of Proposition 2.6 we have analyzed the normal subgroups of hyperspecial groups of Ree type, and we implicitly showed that every normal subgroup of index r contains a principal congruence subgroup whose index in the first principal congruence subgroup is at most r^2. This shows that N contains a principal congruence subgroup of index at most n^3. For each $I = \prod_{i=1}^{r} P_i^{e_i}$, the numbers of normal subgroups of H_1 containing $Q_1(I)$ is the product over i of the number of normal subgroups of $H_i/Q_1(P_i^{e_i})$ which is at the number of most $|H_1/Q_1(P_i^{e_i})|^{\gamma} \leq |P_i^{e_i}|^{\gamma'}$ for a constant γ'. Thus $t_n(H_1) \leq \sum_{\{I \,\big|\, |I| \leq n^c\}} |I|^{\gamma'}$ and this is polynomially bounded. Theorem 3.1 follows. $\square$

For use in §5, let us put on record the following Proposition, whose proof is quite similar to the proof of the lower bound of case (ii) of Theorem 3.1.

Proposition 3.2. *Let $k' \subset k$ an extension of global field, S a finite set of primes in k (containing all the archimedean ones) and S' the corresponding induced primes of k'. Let $\mathcal{O}_S$ (resp. $\mathcal{O}_{S'}$) be the ring of S-integers in k (resp. S'-integers in k'). Let $\mathcal{G}$ be a smooth group scheme defined over $\mathcal{O}_S$ and $\mathcal{G}'$ a connected smooth group scheme defined over $\mathcal{O}_{S'}$, such that $\mathcal{G}' \underset{\mathcal{O}_{S'}}{\times} \mathcal{O}_S = \mathcal{G}^\circ$. Assume the generic fiber $\mathcal{G}'_\eta$ is simply connected, $\mathcal{Z}(\mathcal{G}'_\eta) \neq \{1\}$ and $p \nmid |\mathcal{Z}(\mathcal{G}'_\eta)|$. Assume H is a subgroup of $\mathcal{G}(\hat{\mathcal{O}}_S)$ containing $\mathcal{G}'(\hat{\mathcal{O}}_{S'})$ as a normal open subgroup. Then $t_n(H) \succcurlyeq n^{\log n/(\log\log n)^2}$.*

Proof. By Theorem 3.1, $t_n(\mathcal{G}'(\hat{\mathcal{O}}_{S'})) \succcurlyeq n^{\log n/(\log\log n)^2}$. Recall that we have shown there that for suitable choices of product of primes of $\mathcal{O}_{S'}$, $m(x) = \prod_{P \in \mathcal{P}_x} P$, there is a sufficiently large q-elementary abelian central subgroup $V = \prod_{P \in \mathcal{P}_x} C_P$ in $\mathcal{G}'\big(\mathcal{O}_{S'}/m(x)\big)$ where C_P is the q-part of the center of $\mathcal{G}'(\mathcal{O}_{S'}/P)$. These provide enough normal subgroups to ensure that growth. The principal congruence subgroups of $\mathcal{G}'(\hat{\mathcal{O}}_{S'})$ are intersections of principal congruence subgroups of $\mathcal{G}(\hat{\mathcal{O}}_S)$ with $\mathcal{G}'(\hat{\mathcal{O}}_{S'})$ and are therefore normalized by H. H also normalizes the individual factors $\mathcal{G}'(\mathcal{O}_v)$ for $v \in S'$. Hence it preserves C_P for every $P \in \mathcal{P}_x$. All the factors C_P are isomorphic and $\mathcal{G}'(\hat{\mathcal{O}}_{S'})$ acts trivially. There are finitely many possible homomorphisms from $H/\mathcal{G}'(\hat{\mathcal{O}}_{S'})$ to $Aut(C_P)$. Hence the action is diagonal on a sufficiently large subset of $\mathcal{P}_x$. This gives the desired lower bound for H as well. □

We finally note:

Proof of Theorem C. Theorem C is an immediate corollary of Theorem 3.1. Indeed, Δ is infinite so the classical strong approximation theorem [PR] implies that $\Delta = \mathcal{G}(\mathcal{O}_S)$ is dense in the profinite group $\mathcal{G}(\hat{\mathcal{O}}_S)$ and the profinite topology of $\mathcal{G}(\hat{\mathcal{O}}_S)$ induces on Δ the congruence topology, so $D_n(\Delta) = t_n\big(\mathcal{G}(\hat{\mathcal{O}}_S)\big)$. □

4 Specializing while preserving the Zariski closure

This section is devoted to the following question: Let A be an integral domain with fraction field K and Γ a finitely generated subgroup of $GL_n(A)$ with Zariski closure G in $GL_{n,K}$. Is there a specialization $\phi : A \to k$, where k is a global field, such that the Zariski closure of $\phi(\Gamma)$ is $\overline{K}$-isomorphic to G?

Of course, we cannot expect this to be true for every Γ. For example, if G (as an algebraic group over an algebraic closure $\overline{K}$ of K) is not isomorphic to a group defined over some global field, then the Zariski closure of $\varphi(\Gamma)$ cannot be isomorphic to G. Recall, for example, that there are uncountably many $\mathbb{C}$-isomorphism classes of unipotent algebraic groups, so most of them are clearly not isomorphic to groups defined over global fields. For our purposes, it suffices to consider the case where G is connected and (absolutely) simple. In this case, as is well known, G is $\overline{K}$-isomorphic to a group defined over the prime field, so potentially our question may have a positive answer. This is exactly what we prove in the following theorem. In fact, a similar result holds for semisimple groups and even for reductive groups, but the proof for the simple case is considerably easier and sufficient for our needs.

Theorem 4.1. *Let A be an integral domain, finitely generated over the prime field of characteristic $p \geq 0$, with fraction field K. Let $\Gamma \leq GL_n(A)$ denote a finitely generated subgroup whose Zariski closure in $GL_{n,K}$ is a connected absolutely simple group G. Then there exists a global field k and a ring homomorphism $\phi\colon A \to k$ such that the Zariski closure of $\phi(\Gamma)$ in $GL_{n,k}$ is $\overline{K}$-isomorphic to G.*

Remark. Note that we assert that the groups are isomorphic, but we do not claim that the ambient representations of the Zariski closures are isomorphic (i.e., we do not claim that they are conjugate in $GL_n(\overline{K})$). This is because in characteristic $p > 0$, representations of a simple algebraic group need not be rigid.

We begin with a few general remarks about Zariski closure. If $Y \to S$ is a morphism of schemes, $X \subset Y(S)$ is a set of sections and s is a point of S, the closure of $X \cap Y_s$ in the fiber Y_s is contained in $\overline{X} \cap Y_s$ since the latter is closed in Y_s. If S is irreducible and $s \in S$ is the generic point, then closure commutes with restriction to Y_s. Indeed, any closed set in Y containing x_s for x an element of $Y(S)$ contains all of x and therefore any closed set in Y containing $X \cap Y_s$ contains $\overline{X}$.

A second remark is that if $Y \to S$ is a morphism of schemes, X is a subset of $Y(S)$ and $T \to S$ is an open morphism, then the Zariski closure of $X \underset{S}{\times} T$ in $Y \underset{S}{\times} T$ equals $(\overline{X} \underset{S}{\times} T)^{red}$, i.e., set-theoretically, the Zariski closure commutes with open base change ([EGA IV, 2.4.11]).

In particular this is the case when $T \to S$ is étale as well as the case when T is obtained from S by tensoring by an arbitrary field extension [EGA IV, 2.4.10].

We break the proof into several lemmas, in which we keep the notations of Theorem 4.1. Let $\mathcal{G}$ be the Zariski closure of Γ in $GL_{n,A}$. Note that the generic fiber of $\mathcal{G}$ is G.

Lemma 4.2. *There exists an étale A-algebra B such that the Zariski closure $\mathcal{G}_B$ of Γ in $GL_{n,B}$ is a split simple group scheme.*

Proof. By construction, $\mathcal{G}$ is affine and finitely presented. By [EGA IV, 9.7.7], after inverting some element of A, we may assume the fibers are geometrically integral, and by generic flatness, we may also assume that $\mathcal{G}$ is flat. By [SGA3, XIX 2.5], by inverting an additional element, we may further assume that $\mathcal{G}$ is a simple group scheme; and by [EGA IV, 6.12.6, 6.13.5], we may assume A is integrally closed. Thus, by [SGA3, XXII 2.3], there exists an étale A-algebra B such that $\mathcal{G} \underset{A}{\times} B$ is a split simple group scheme. So by the remark preceding the lemma, $\mathcal{G}_B = (\mathcal{G} \underset{A}{\times} B)^{red} = \mathcal{G} \underset{A}{\times} B$. ◻

Note that an étale extension of a normal integral domain is a direct sum of integral domains [SGA1, I 9.2]. Replacing A by any summand of B, we obtain an algebra satisfying the hypotheses of Theorem 4.1 and in addition we can assume from now on that $\mathcal{G}$ is split.

Lemma 4.3. *Given a simple algebraic group H over an algebraically closed field, there exists a finite set of proper subgroups $H_1, \ldots, H_r$ such that every positive-dimensional proper subgroup of H is conjugate to a subgroup of H_i for some $i = 1, \ldots, r$.*

Proof. See Liebeck-Seitz [LS1, LS2, LS3]. $\square$

Lemma 4.4. *There exists an open subset of Spec(A) such that for every point s of the subset, the closure of Γ in $\mathcal{G}(\Bbbk_s)$ is either finite or all of $\mathcal{G}_s$ (By $\Bbbk_s$ we mean the residue field of Spec(A) at s).*

Proof. Let Y denote the disjoint union of r copies of $G \underset{K}{\times} \overline{K}$, where r is the number of conjugacy classes of maximal positive dimensional subgroups as in Lemma 4.3. Y can be thought of as parametrizing the maximal positive dimensional subgroups of G. Let $Z \subset G \underset{K}{\times} Y$ denote the Y-subgroup scheme such that $Z_y \subset G$ is the subgroup parametrized by $y \in Y$. Let $\tau_1, \ldots, \tau_\ell$ denote a finite set of generators for Γ, which we regard as morphisms from $Spec(A)$ to G and hence also as sections of $G \underset{K}{\times} Spec(A) \to Spec(A)$.

Let p_i, $i = 1, 2, 3$ denote the projection map from $G \underset{K}{\times} Spec(A) \underset{K}{\times} Y$ to the product in which the i-th factor is omitted. The intersection

$$W = \bigcap_{j=1}^{\ell} p_1\left(p_2^{-1}(Z) \cap p_3^{-1}\left(\tau_j(SpecA)\right)\right)$$

as a subset of $Spec(A) \underset{K}{\times} Y$ is the set of "bad points", i.e., the set of pairs (ϕ, y), $\phi \in Spec(A)$ and $y \in Y$ such that $\phi(\Gamma) \subseteq Z_y$. By Chevalley's theorem, W is a constructible set. The same is true for its projection $\overline{W}$ to $Spec(A)$. Now, $\overline{W}$ omits the generic point (as Γ is dense in G_K) and hence it omits a non-empty affine open set U in $Spec(A)$. This proves the lemma. $\square$

¿From now on, we will replace A by the coordinate ring of U. Let $\mathbb{F}$ be the field of constants in A, i.e., the algebraic closure of the prime field in A. Let us fix an (absolutely) irreducible (almost faithful) representation ρ of $G \hookrightarrow GL_m$ defined over A. (Such a representation exists over the prime field and can then be extended to A). We define a character $\chi\colon \Gamma \to A$ by $\chi(\gamma) = tr\rho(\gamma), \gamma \in \Gamma$. By Burnside's Lemma [CR, 36.1], $\chi(\Gamma)$ is infinite. Now, if $\chi(\Gamma) \subset \mathbb{F}$, since specialization is injective on constants, for any specialization, $\phi(\Gamma)$ contains elements with infinitely many different character values, so $\phi(\Gamma)$ cannot lie within a finite group. Therefore by Lemma 4.4, it is dense in G. Otherwise, fix γ such that $\chi(\gamma) \in A$ is non-constant. If $p = 0$, as A is finitely generated over $\mathbb{Q}$, $\chi(\gamma) - r$ is not invertible in A for sufficiently large $r \in \mathbb{N}$. We choose large $r > m$ and a specialization ϕ such that $\phi(\chi(\gamma)) = r$. A sum of m roots of unity cannot equal r, so $\phi(\gamma)$ is of infinite order. Thus $\phi(\Gamma)$ is not finite and again we finish by Lemma 4.4. Let now $p > 0$: In this case we regard χ as a dominant morphism from $Spec(A)$ to $\mathbb{A}^1$. Let C be a quasi-section [EGA IV, 17.16.1], i.e., a curve in $Spec(A)$ such that $\chi|_C$ is still dominant. Let k be the function field of C and ϕ the specialization from A to k. By construction, $\phi(\chi(\gamma))$ is not constant, and we are done by Lemma 4.4. Theorem 4.1 is therefore proved. $\square$

5 Proof of Theorem B

We are now ready to reap the fruits of our labor and prove Theorem B. We will use the notation of the introduction.

So let $\Gamma \leq GL_n(F)$ be a finitely generated group Zariski dense in G, $S(\Gamma) = \overline{G}/Z(\overline{G})$ and $S(\Gamma) = \prod_{i=1}^{r} S_i$. If $r = 0$, G and Γ are virtually solvable and we are done. Assume thus that $r > 0$ and some S_i, say S_1, of type X, satisfies $\mathcal{Z}(\tilde{S}_1) \neq \{1\}$. Replacing G by a suitable quotient if needed (which may also entail changing n), we can assume that G° itself is a product $\prod_{i=1}^{r} S_i$, all the factors S_i are adjoint and isomorphic to one another, all of type X, and that G/G° acts transitively on the set of factors. So now Γ and G are subgroups of $G^\circ \rtimes Out(G^\circ)$. Pulling back to $\widetilde{G^\circ} \rtimes Out(G^\circ)$, replacing Γ by $\tilde{\Gamma}$, we can assume that each S_i is simply connected. Let $\Gamma^\circ = \Gamma \cap G^\circ$ and let Γ^1 be the projection of Γ° to S_1. Note that S_1 can also be regarded as a subgroup of G° and therefore of GL_n. As Γ° is of finite index in Γ, Γ^1 is also a finitely generated group. There is therefore an integral domain A in F which is finitely generated over the prime field such that both Γ and Γ_1 are inside $GL_n(A)$. The Zariski closure of Γ_1 is the connected absolutely simple group S_1. By Theorem 4.1, there exists a global field k and a ring homomorphism $\phi\colon A \to k$ such that the Zariski closure of $\phi(\Gamma_1)$ in $GL_{n,k}$ is F-isomorphic to S_1. The specialization ϕ induces also a homomorphism from Γ to $GL_n(k)$. Let H be the Zariski closure of $\phi(\Gamma)$ in $GL_{n,k}$, and H° the connected component of H. It follows that $H^\circ = \prod_{j=1}^{s} R_j$ where $1 \leq s \leq r$ and for every j, $1 \leq j \leq s$, R_j is isomorphic to S_1. Moreover, H/H° acts transitively on the set $\{R_j\}_{j=1}^{s}$.

Replacing Γ by a suitable quotient we may assume it is contained in $GL_n(k)$ and its Zariski closure G satisfies $G^\circ = \prod_{i=1}^{r} S_i$, each S_i is a simply connected group of type X and G/G° acts transitively on $\{S_i\}_{i=1}^{r}$.

Now, as Γ is finitely generated, there exists a finite set of primes S in k (containing all the archimedean ones) such that Γ is in $GL_n(\mathcal{O}_S)$. Let $\mathcal{G}$ be the Zariski closure of Γ in $GL_{n,\mathcal{O}_S}$. Thus $\Gamma \subset \mathcal{G}(\mathcal{O}_S)$ and $\mathcal{G}_\eta = G$. Assume now that we are in case (ii) of Theorem B, i.e., $p \mid |\mathcal{Z}(S_i)|$ for some i. Let v be a prime outside S, so Γ is in $\mathcal{G}(\mathcal{O}_v)$ and is Zariski dense in $\mathcal{G}_{k_v}$. Let M be the closure of Γ in the profinite group $\mathcal{G}(\mathcal{O}_v)$. We can apply Theorem 2.1 to deduce that the normal subgroup growth of M is at least $n^{\log n}$. It follows that the same applies to Γ. Now, by (1.6), this is the maximal possible normal subgroup growth type; hence Theorem B(ii) is proved.

To prove (i), we continue as follows: By [P2] we can find a global subfield k' of k and a semisimple, connected, simply connected algebraic group G' over k' such that $G' \underset{k'}{\times} k$ is isogenous to G° and $[\Gamma^\circ, \Gamma^\circ]$ is contained as a Zariski dense subgroup of $G'(k')$ satisfying strong approximation. As $p \nmid |\mathcal{Z}(G^\circ)|$, the isogeny is an isomorphism. Let $\mathcal{G}'$ be a smooth group scheme defined over the S'-integers of k' for some finite set S' of primes of k', such that $\mathcal{G}'_\eta = G'$. As $\mathcal{G}' \underset{\mathcal{O}_{S'}}{\times} \mathcal{O}_S$ and $\mathcal{G}^\circ$ have isomorphic generic fibers, after enlarging S and S' we may assume these group schemes are isomorphic and S' is the restriction of S to k'. Let H be the closure of Γ in $\mathcal{G}(\hat{\mathcal{O}}_S)$. By strong approximation, and by further enlarging S and S' if needed, we can assume that $[\Gamma^\circ, \Gamma^\circ]$ is dense in $\mathcal{G}'(\hat{\mathcal{O}}_{S'}) \subseteq \mathcal{G}(\hat{\mathcal{O}}_S)$. We claim $[H\colon \mathcal{G}'(\hat{\mathcal{O}}_{S'})]$ is finite, or equivalently, $[\Gamma^\circ\colon \Gamma^\circ \cap \mathcal{G}'(k')]$ is finite. Indeed, let $G' = \mathcal{G}'_\eta$, $G'^{ad} = G'/\mathcal{Z}(G')$ and $\pi\colon G' \to G'^{ad}$ the universal cover map. Again by [P2], $\pi(\Gamma^\circ) \subset G'^{ad}(k')$. As Γ_0 is finitely generated and $G'^{ad}(k')/\pi\big(G'(k')\big)$ is a torsion abelian group, the image of the former in the latter is finite. By Proposition 3.2, $t_n(H) \succcurlyeq n^{\log n/(\log\log n)^2}$ and hence the same is true for Γ. $\square$

Acknowledgement. The authors are indebted to D. Hold, E. Hrushovski, A. Rapinchuk, D. Segal and V.N. Venkataramana for some helpful discussions. Some of this work was done during visits to Yale University, University of Chicago and The Hebrew University. Their hospitality and support are gratefully acknowledged, as well as the support of the NSF and the US-Israel Binational Science Foundation.

References

[BG] Y. Barnea and R. Guralnick, *Subgroup growth in some pro-p groups*, Proc. AMS **130**(2002) 653–659.

[BL] Y. Barnea and M. Larsen, *Random generation in semisimple algebraic groups over local fields*, to appear.

[Be] H. Behr, *Arithmetic groups over function fields I. A complete characterization of finitely generated and finitely presented arithmetic subgroups of reductive algebraic groups*, J. Reine Angew. Math. **495**(1998) 79–118.

[BT] F. Bruhat and J. Tits, *Groupes réductifs sur un corps local II. Schémas en groupes. Existence d'une donné radicielle valué*, Publ. Math. IHES **60**(1984) 197–376.

[CR] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley & Sons, N.Y. 1962.

[SGA3] M. Demazure and A. Grothendieck, *Schémas en Groupes I, II, III*, Lecture Notes in Math. 151–153, Springer Verlag, Berlin 1970.

[GLP] D. Goldfeld, A. Lubotzky and L. Pyber, *Counting congruence subgroups*, in preparation.

[SGA1] A. Grothendieck, *Reveêtements Etales et Groupe Fondamental*, Lecture Notes in Math. 224, Springer-Verlag, Berlin 1971.

[EGA IV] A. Grothendieck, *Elements de Géométrie Algébriques IV*, Publ. Math. IHES **20**(1964), **24**(1965), **28**(1966), **32**(1967).

[H] G.M.D. Hogeweij, *Almost-classical Lie algebras, I*, Nederl. Akad. Wetensch. Indag. Math. **44**(1982) 441-452.

[Ho] D.F. Holt, *On the second cohomology group of a finite group*, Proc. Lond. Math. Soc. **55**(1987) 22–36.

[LS1] M.W. Liebeck and G.M. Seitz, *Maximal subgroups of exceptional groups of Lie type, finite and algebraic*, Geom. Dedicata **35**(1990) 353–387.

[LS2] M.W. Liebeck and G.M. Seitz, *On the subgroup structure of classical groups*, Invent. Math. **134**(1998) 435–453.

[LS3] M.W. Liebeck and G.M. Seitz, *The maximal subgroups of positive dimension in exceptional algebraic groups*, in preparation.

[L1] A. Lubotzky, *Subgroup Growth*, Proc. of the ICM, Zürich 1994, pp. 309–317.

[L2] A. Lubotzky, *Subgroup growth and congruence subgroups*, Invent. Math. **119**(1995) 267–295.

[L3] A. Lubotzky, *Enumerating boundedly generated finite groups*, J. of Algebra **238**(2001) 194–199.

[LM] A. Lubotzky and A. Mann, *On groups of polynomial subgroup growth*, Invent. Math. **104**(1991) 521–533.

[LMS] A. Lubotzky, A. Mann and D. Segal, *Finitely generated groups of polynomial subgroup growth*, Israel J. of Math. **82**(1993) 363–371.

[LS] A. Lubotzky and D. Segal, *Subgroup Growth*, a book in preparation.

[LSh] A. Lubotzky and A. Shalev, *On* Λ*-analytic pro-p groups*, Israel J. Math. **85**(1994) 307–337.

[M] A. Mann, *Enumerating finite groups and their defining relations*, J. Group Theory **1**(1998) 59–64.

[N] N. Nikolov, *Subgroup growth of* $\mathbb{F}_p[[t]]$ *– analytic Chevalley groups*, in preparation.

[No] M. Nori, *On subgroups of* $GL_n(F)$, Invent. Math. **88**(1987) 257–275.

[P1] R. Pink, *Compact subgroups of linear algebraic groups*, J. of Algebra **206**(1998) 438–504.

[P2] R. Pink, *Strong approximation for Zariski dense subgroups over arbitrary global fields*, Comment. Math. Helv **75**(2000) 608–643.

[PR] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure and Applied Math. 139, Academic Press 1994.

[Py] L. Pyber, in preparation.

[R1] M.S. Raghunathan, *On the congruence subgroup problem*, IHES Math. **46**(1976) 107–161.

[R2] M.S. Raghunathan, *On the congruence subgroup problem. II.* Invent. Math. **85**(1986), no. 1, 73–117.

[R3] M.S. Raghunathan, *The congruence subgroup problem*, Proceedings of the Hyderabad Conference on Algebraic Groups (Hyderabad, 1989), 465–494, Manoj Prakashan, Madras, 1991.

[S] D. Segal, *The finite images of finitely generated groups*, Proc. Lond. Math. Soc. **82**(2001) 597–613.

[St] R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22**(1963), 33–56.

[Ti] J. Tits, *Reductive groups over local fields*, in *Automorphic Forms, representations and L-functions*, Proc. Symp. Pure Math. 33, Part 1, pp. 29–69, AMS 1979.

[We] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups*, Ann. of Math. **120**(1984) 271–315.

Michael Larsen
Department of Mathematics
Indiana University
Bloomington, Indiana 47405 USA
larsen@math.indiana.edu

Alexander Lubotzky
Institute of Mathematics
The Hebrew University
Jerusalem 91904, Israel
alexlub@math.huji.ac.il