The density of representation degrees

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ
England

Dan Segal
All Souls College
Oxford OX1 4AL
England

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904
Israel

Abstract

For a group G and a positive real number x, define $d_G(x)$ to be the number of integers less than x which are dimensions of irreducible complex representations of G. We study the asymptotics of $d_G(x)$ for algebraic groups, arithmetic groups and finitely generated linear groups. In particular we prove an "alternative" for finitely generated linear groups G in characteristic zero, showing that either there exists $\alpha > 0$ such that $d_G(x) > x^\alpha$ for all large x, or G is virtually abelian (in which case $d_G(x)$ is bounded).

The second author acknowledges the support of an EPSRC Visiting Fellowship at Imperial College London, and a grant from the Israel Science Foundation

2000 *Mathematics Subject Classification:* 20C15, 20G15, 20G05

1 Introduction

In this paper we study some asymptotic questions concerning the dimensions of irreducible complex representations of various groups. These include complex algebraic groups, p-adic groups, arithmetic groups, finitely generated soluble groups and finitely generated linear groups. One of our main results (Theorem 4) constitutes an "alternative" for finitely generated linear groups in characteristic zero – either they have many representation degrees, or they are virtually abelian.

For a group G, define D_G to be the set of (finite) degrees of irreducible complex representations of G; when G is complex algebraic or profinite, we allow only rational representations and continuous representations (i.e. representations that factor through a quotient by an open normal subgroup), respectively, in this definition. For a real number x, define

$$D_G(x) = \{n \in D_G \,:\, n \leq x\},$$

and

$$d_G(x) = |D_G(x)|.$$

While we are not aware of any previous systematic study (or indeed definition) of this function, there are various related results in the literature, mainly for finite groups. Perhaps the first is the theorem of Isaacs and Passman [8], bounding the index of an abelian subgroup of a finite group G in terms of $\max(n \,:\, n \in D_G)$. Another is the result of Isaacs [7] bounding the derived length of a finite soluble group in terms of $\max(d_G)$. Related results for finite simple groups can be found in [13], [14].

A related active field of study is representation growth, where one counts the number $r_n(G)$ of irreducible representations of G of dimension n – see [11] and the references therein.

In this paper we study the asymptotics of the density function $d_G(x)$ for various infinite groups G. Our results form an interesting contrast with those in [11], particularly for the case of arithmetic groups (see Theorem 3). The analogous notion of the density of subgroup indices is studied in [20].

We begin with complex simple algebraic groups. For these, we include only rational representations in our definition of D_G.

Theorem 1 *Let $G = G(\mathbb{C})$ be a simply connected simple algebraic group of rank r over $\mathbb{C}$, and let u be the number of positive roots in the root system of G. Then there is a constant c depending only on G such that*

$$x^{r/u - c/\log\log x} \leq d_G(x) \leq x^{r/u + (r-1)/\log\log x}.$$

In particular

$$d_G(x) = x^{r/u + o(1)}.$$

The final statement of Theorem 1 can also be deduced from [11, 5.1].

For p-adic groups, $d_G(x)$ is much smaller. Let G be an absolutely simple, simply connected algebraic k-group, where k is an algebraic number field. For each prime ideal $\mathfrak{p}$ of the ring of integers O of k, let $O_\mathfrak{p}$ be the corresponding discrete valuation ring and $G(O_\mathfrak{p})$ the group of $O_\mathfrak{p}$-rational points in G. If p is the characteristic of $O/\mathfrak{p}$, then $G(O_\mathfrak{p})$ is virtually pro-p. Hence, letting b be the index of the maximal normal pro-p subgroup, we have

$$D_{G(O_\mathfrak{p})} \subseteq \{ap^i \,:\, 1 \le a \le b,\, i \ge 0\},$$

where $D_{G(O_\mathfrak{p})}$ is the set of degrees of complex irreducible finite representations of $G(O_\mathfrak{p})$. It follows that there is a constant c such that

$$d_{G(O_\mathfrak{p})}(x) \le c \log_p x. \tag{1}$$

We shall need to deal with products of the groups $G(O_\mathfrak{p})$ for different primes $\mathfrak{p}$.

Theorem 2 *Let G and k be as above, and define $R = R(G)$ as in Table 1. Let $H = \prod G(O_\mathfrak{p})$, where $\mathfrak{p}$ ranges over all but finitely many primes of O. Then*

$$d_H(x) = x^{1/R + o(1)}.$$

Table 1

G	A_r	B_r	C_r	D_r	G_2	F_4	E_6	E_7	E_8
$R(G)$	r	$2r-2$	r	$2r-3$	3	8	11	17	29

The numbers $R(G)$ are the degrees of the polynomials in p expressing the minimal dimensions of complex irreducible representations of the groups $G(\mathbb{F}_p)$ (see [10], [15]).

The next theorem combines the above results to study $d_G(x)$ for arithmetic groups.

Theorem 3 *Let k be a algebraic number field, let G be an absolutely simple, simply connected k-group, and let $\Gamma = G(O_S)$ where S is a finite set of primes of k and O_S is the ring of S-integers. Assume that Γ has the congruence subgroup property. Then*

$$d_\Gamma(x) = x^{r/u + o(1)},$$

where r is the rank of G and u is the number of positive roots in the root system of G.

The congruence subgroup property means that the profinite completion of Γ is isomorphic (modulo a finite normal subgroup) to a group H as in Theorem 2, hence the density of degrees of finite representations of Γ is given by Theorem 2. The above theorems show that asymptotically the function $d_{G(O_S)}$ is similar to $d_{G(\mathbb{C})}$, and is at least (and often larger than) d_H, since $r/u \geq 1/R$. In other words, the main contribution to $D_{G(O_S)}$ comes from rational representations rather than finite representations. This is in sharp contrast to a result of Larsen and Lubotzky [11, 8.1], showing that in large rank, $G(O_S)$ has many more finite representations than rational representations.

We note that it was believed for some time that arithmetic groups as in Theorem 3 have $x^{r/u+o(1)}$ irreducible representations of degree at most x; this is refuted in [11], and the precise representation growth of arithmetic groups is still unknown. Theorem 3 above shows that the suggested estimate above holds if instead of counting irreducible representations we count their degrees.

The above results are a major ingredient in the proof of the following "alternative" for linear groups in characteristic zero.

Theorem 4 *Let G be a finitely generated linear group in characteristic zero. Then one of the following holds:*

(i) *there exists $\alpha > 0$ such that $d_G(x) > x^\alpha$ for all sufficiently large x;*

(ii) *there exists $c > 0$ such that $d_G(x) < c$ for all x, and G is virtually abelian.*

The proof of Theorem 4 uses a version of the "Lubotzky Alternative" ([16, Window 9]) and the previous theorems to reduce to the case where G is virtually soluble. It is well known ([22, 4.7]) that finitely generated linear groups in characteristic zero are virtually residually p for almost all primes p. In Theorem 6.12 we prove that every finitely generated virtually soluble group with this property satisfies either (i) or (ii) of Theorem 4, thereby completing the proof of Theorem 4. The proof of this involves both analytic and algebraic number theory (see Subsections 6.2 and 6.3). We are grateful to Roger Heath-Brown for some useful discussions relating to sieve theory and Subsection 6.3.

Theorem 4 is not true for finitely generated linear groups in positive characteristic, as is shown for example by the group $SL_d(\mathbb{F}_p[t])$. However there is a weaker alternative that holds in this case, where (i) is replaced by $d_G(x) > \frac{c \log x}{\log \log x}$. For finitely generated residually finite groups that are neither linear nor soluble, the function $d_G(x)$ can grow arbitrarily slowly. Details will appear in a future paper.

2 Preliminaries

For a natural number n and a group G, let $r_n(G)$ denote the number of irreducible complex representations of G of dimension n, and define $R_n(G) = \sum_{m=1}^{n} r_m(G)$. The following is clear.

Lemma 2.1 *For any group G,*

$$\frac{R_n(G)}{max(r_m(G) : m \leq n)} \leq d_G(n) \leq R_n(G).$$

For any group G, define a "zeta function" $\delta_G : \mathbb{R} \to \mathbb{R} \cup \{\infty\}$ by

$$\delta_G(s) = \sum_{n \in D_G} n^{-s}.$$

Lemma 2.2 *Let I be countable set, and for each $i \in I$ let G_i be a group. Let $G = \prod_{i \in I} G_i$ be their Cartesian product. Then*

$$\delta_G(s) \leq \prod_{i \in I} \delta_{G_i}(s)$$

for every $s \in \mathbb{R}$.

Proof. We are only counting representations whose kernel contains all but finitely many of the factors in the product. The result then follows easily from the fact that every finite-dimensional irreducible representation of a finite product of the G_i is a tensor product of irreducible representations of the G_i. ∎

Lemma 2.3 *Let G be a group and s a positive real number.*

(i) *If $\delta_G(s) < \infty$, then $d_G(x) = O(x^s)$.*

(ii) *If $d_G(x) = O(x^s)$, then for any $t > s$ we have $\delta_G(t) < \infty$.*

Proof. (i) Fix $x > 0$, and for $i \geq 0$ define

$$D_i = \{n \in D_G : 2^{-(i+1)}x < n \leq 2^{-i}x\}.$$

Observe that

$$d_G(x) = \sum_{i \geq 0} |D_i|. \tag{2}$$

Now

$$\delta_G(s) \geq \sum_{n \in D_i} n^{-s} \geq (2^{-i}x)^{-s}|D_i| = 2^{is}x^{-s}|D_i|.$$

Therefore

$$|D_i| \leq \delta_G(s) \cdot 2^{-is} \cdot x^s,$$

and so by (2),

$$d_G(x) \leq \delta_G(s) \cdot x^s \sum_{i \geq 0} 2^{-is} = O(x^s),$$

as required.

(ii) This is quite similar. For $i \geq 0$ define $C_i = \{n \in D_G : 2^i \leq n < 2^{i+1}\}$, and for $t > s$ define

$$\delta_i(t) = \sum_{n \in C_i} n^{-t}.$$

Then $\delta_i(t) \leq |C_i| \cdot (2^i)^{-t} \leq d_G(2^{i+1}) \cdot 2^{-it}$. By our assumption, $d_G(2^{i+1}) \leq c \cdot (2^{i+1})^s$. Hence $\delta_i(t) \leq c \cdot 2^{s-i(t-s)}$. Consequently

$$\delta_G(t) = \sum_{i \geq 0} \delta_i(t) \leq c \sum_{i \geq 0} 2^{s-i(t-s)},$$

which is finite. ∎

The next result shows that the function d_G does not change much when passing to a subgroup of finite index. In the statement, $d(m)$ denotes the number of positive divisors of m.

Lemma 2.4 *Let G be a group and let H be a normal subgroup of finite index m in G. Then*

(i) $d_G(x) \geq \frac{1}{d(m)} d_H(x/m)$;

(ii) $d_H(x) \geq \frac{1}{d(m)} d_G(x)$.

Proof. (i) For each $n \in D_H(x/m)$, choose an irreducible representation ρ of H of dimension n, and an irreducible constituent ρ' of the induced representation $\rho \uparrow G$. Then ρ is a constituent of $\rho' \downarrow H$ by Frobenius Reciprocity, so by [6, 11.29], $\dim \rho' / \dim \rho$ is an integer dividing m. Let $n' = \dim \rho'$. Then $n' \in D_G(x)$ and $n' = ni$ for some divisor i of m. This defines a (non-canonical) map from $D_H(x/m)$ to $D_G(x)$ which is at most $d(m)$ to 1. The result follows.

(ii) For each $n \in D_G(x)$, choose an irreducible representation ρ of G of dimension n, and an irreducible constituent ρ' of $\rho \downarrow H$. Then $\dim \rho / \dim \rho'$ is an integer dividing m, by [6, 11.29]. Let $n' = \dim \rho'$. Then $n' \in D_H(x)$ and $n' = n/i$ for some divisor i of m. This defines a (non-canonical) map from $D_G(x)$ to $D_H(x)$ which is at most $d(m)$ to 1. The result follows. ∎

We remark that if H is a finite index subgroup of G (not necessarily normal), then by considering its core, we see that the conclusions of 2.4 hold with m replaced by $m!$. The next result follows immediately.

Corollary 2.5 *Let G be a group and let H be a subgroup of finite index in G.*

(i) *Suppose $d_H(x) \geq cx^s$ for all $x \geq 1$, where $c, s > 0$. Then there is a positive constant c' (depending on c and $|G : H|$) such that $d_G(x) \geq c'x^s$.*

(ii) *Suppose $d_G(x) \geq cx^s$ for all $x \geq 1$, where $c, s > 0$. Then there is a positive constant c' (depending on c and $|G : H|$) such that $d_H(x) \geq c'x^s$.*

For any finite group G, let $m(G)$ be the smallest dimension of a nontrivial complex representation of G. For a Lie type X, we denote by $X^\epsilon(q)$ ($\epsilon \in \{1, 2, 3\}$) a possibly twisted group of type X (and unspecified isogeny type) over the finite field $\mathbb{F}_q$, where $\epsilon = 1$ indicates the untwisted group, $\epsilon = 2$ indicates the twisted groups ${}^2A_n$, ${}^2D_n$, ${}^2E_6$, and $\epsilon = 3$ indicates ${}^3D_4$. (Note that we are excluding the Suzuki and Ree groups, as these do not arise in any proofs in the paper.)

Lemma 2.6 *Fix a type G of simply connected simple algebraic group, and define $R = R(G)$ as in Table 1. There there are positive absolute constants c_1, c_2 such that for any prime $p > 3$ and any power q of p,*

$$c_1 q^R < m(G^\epsilon(\mathbb{F}_q)) < c_2 q^R.$$

Moreover, for $p > 3$ and $G \neq G_2$, $m(G^\epsilon(\mathbb{F}_q))$ is given by a polynomial in q of degree R which depends only on the type of G (and the twisted type G^ϵ); for $G = G_2$ it is given by one of two polynomials, depending on the congruence class of q modulo 6.

Proof. This follows from [21, 1.1] for classical groups, and from [15] for exceptional types. ∎

3 The complex case

In this section we prove Theorem 1. Let $G = G(\mathbb{C})$ be a simply connected simple algebraic group of rank r over $\mathbb{C}$. Let Φ be the root system of G, with fundamental roots $\alpha_1, \ldots, \alpha_r$, and let $\lambda_1, \ldots, \lambda_r$ be corresponding fundamental dominant weights. Let $u = |\Phi^+|$. For λ a dominant weight, let $V(\lambda)$ be the Weyl module for G of highest weight λ. The Weyl character formula (see for example [5, p.139]) states that

$$\dim V(\lambda) = \frac{\prod_{\alpha \in \Phi^+} \langle \lambda + \delta, \alpha \rangle}{\prod_{\alpha \in \Phi^+} \langle \delta, \alpha \rangle}, \tag{3}$$

where δ is half the sum of the positive roots, and $\langle \lambda + \delta, \alpha \rangle$ is defined as $(\lambda+\delta, \alpha^v)$ with $\alpha^v = 2\alpha/(\alpha, \alpha)$, the dual root. Write $N(\lambda)$ for the numerator and l for the denominator in (3) – that is,

$$N(\lambda) = \prod_{\alpha \in \Phi^+} \langle \lambda + \delta, \alpha \rangle, \quad l = \prod_{\alpha \in \Phi^+} \langle \delta, \alpha \rangle.$$

We refer to [1, p.250] for descriptions of root systems.

Lemma 3.1 *We have*

$$r_n(G) \leq d(ln)^u \leq n^{c/\log\log n} \leq n^{o(1)},$$

where $d(m)$ is the number of divisors of m, and $c = c(r)$.

Proof. Each irreducible complex representation of G is afforded by a Weyl module $V(\lambda)$ for some λ. By (3), we therefore have to count the number of weights λ for which $N(\lambda) = ln$. For such λ, $N(\lambda)$ is a product of u natural numbers $\langle \lambda + \delta, \alpha \rangle$ which are all divisors of ln. Hence there are at most $d(ln)^u$ possibilities for these u numbers $\langle \lambda + \delta, \alpha \rangle$. Since these numbers determine λ uniquely, it follows that $r_n(G) \leq d(ln)^u$. Finally, it is well known that $d(m) \leq m^{c/\log\log m}$, proving the second inequality. ∎

The following proposition is our main tool for proving the upper bound in Theorem 1.

Proposition 3.2 *Write $\lambda = \sum_1^l m_i \lambda_i$, and let $u = |\Phi^+|$, the number of positive roots. Then*

$$N(\lambda) \geq \prod_1^l (m_i + 1)^{u/r}.$$

Proof. Since $\delta = \sum_1^l \lambda_i$, we have

$$N(\lambda) = \prod_{\alpha \in \Phi^+} \langle \sum_1^r (m_i + 1)\lambda_i, \alpha \rangle. \tag{4}$$

We begin by considering G of type A_r (i.e. $G = SL_{r+1}(\mathbb{C})$). The positive roots take the form $\alpha_{st} = \alpha_s + \cdots + \alpha_t$ $(s \leq t)$, and

$$\langle \sum_1^r (m_i + 1)\lambda_i, \alpha_{st} \rangle = m_s + \cdots + m_t + t - s + 1.$$

Write $m_{st} = m_s + \cdots + m_t + t - s + 1$. Then

$$N(\lambda) = \prod_{1 \leq s \leq t \leq l} m_{st}.$$

Hence

$$N(\lambda)^2 = \prod_{s=1}^{r}(\prod_{t\geq s} m_{st} \prod_{t\leq s} m_{ts}).$$

Since $m_{st} \geq m_s + 1$ and $m_{ts} \geq m_s + 1$, it follows that

$$N(\lambda)^2 \geq \prod_{s=1}^{r}(m_s+1)^{r+1} = \prod_{s=1}^{r}(m_s+1)^{2u/r},$$

as required.

Next consider G of type B_r. The positive roots are

$$\begin{array}{l}\alpha_{sr} = \alpha_s + \cdots + \alpha_r \ (s \leq r), \text{ and} \\ \alpha_{st} = \alpha_s + \cdots + \alpha_t, \ \beta_{st} = \alpha_s + \cdots + \alpha_t + 2(\alpha_{t+1} + \cdots + \alpha_r) \ \ (s \leq t < r)\end{array}$$

and we have $\alpha^v_{sr} = 2\alpha_{sr}$, while $\alpha^v_{st} = \alpha_{st}, \beta^v_{st} = \beta_{st}$ for $s \leq t < r$. It follows by (4) that

$$N(\lambda) = \prod_{s\leq r} k_{sr} \prod_{s\leq t<r} m_{st}n_{st},$$

where

$$\begin{array}{l}k_{sr} = 2m_s + \cdots + 2m_{r-1} + m_r + 2r - 2s + 1, \\ m_{st} = m_s + \cdots + m_t + t - s + 1, \\ n_{st} = m_s + \cdots + m_t + 2m_{t+1} + \cdots + 2m_{r-1} + m_r + 2r - s - t.\end{array}$$

Hence $N(\lambda) \geq \prod_{s\leq r} k_{sr} \prod_{s\leq t<r} m^2_{st}$, and by the type A case applied for A_{r-1}, the second product is at least $\prod_{s<r}(m_s+1)^r$. As $k_{sr} \geq m_r + 1$, it follows that

$$N(\lambda) \geq \prod_{s\leq r}(m_s+1)^r = \prod_{s=1}^{r}(m_s+1)^{u/r},$$

giving the result for type B.

The proof for G of type C_r is very similar to that for B_r. Type D_r is not very different: here the positive roots are

$$\begin{array}{l}\alpha_{st} = \alpha_s + \cdots + \alpha_t \ (s \leq t \leq r-1), \\ \alpha_{sr} = \alpha_s + \cdots + \alpha_{r-2} + \alpha_r \ (s \neq r-1) \\ \beta_{st} = \alpha_s + \cdots + \alpha_t + 2(\alpha_{t+1} + \cdots + \alpha_{r-2}) + \alpha_{r-1} + \alpha_r \ (s \leq t \leq r-2)\end{array}$$

Hence, defining m_{st} as above for $s \leq t \leq r-1$, and $m_{sr} = m_s + \cdots + m_{r-2} + m_r + 1$, we have

$$N(\lambda) \geq \prod_{s\leq t\leq r-2} m^2_{st} \prod_{s\leq r-1} m_{s,r-1} \prod_{s\leq r-2} m_{s,r} \cdot (m_r+1).$$

By the A_{r-2} case, the first product is at least $\prod_{s\le r-2}(m_s+1)^{r-1}$, and hence

$$N(\lambda) \ge \prod_{s\le r}(m_s+1)^{r-1} = \prod_{s=1}^{r}(m_s+1)^{u/r},$$

giving the result for type D.

The exceptional types are straightforward. First consider G of type E_6. The positive roots α with α_2-coefficient 0 are in an A_5 subsystem, so by the A_l case, these contribute at least $\prod_{s\ne 2}(m_s+1)^3$ to the expression (4) for $N(\lambda)$. Next the 6 roots 010000, 010100, 011100, 111100, 010110, 010111 contribute at least $(m_2+1)^6$. It is easy to list the remaining 15 positive roots (using [1, p.260]) and to see that these contribute at least $\prod_{s\ne 2}(m_s+1)^3$. Hence $N(\lambda) \ge \prod_1^6(m_s+1)^6$, giving the result for E_6.

Types E_7 and E_8 are similar. For E_7 we note that by the E_6 case, the positive roots α with α_7-coefficient 0 contribute at least $\prod_{s\le 6}(m_s+1)^6$ to (4), and one can list the remaining positive roots to see that they contribute at least $(m_7+1)^9\prod_{s\le 6}(m_s+1)^3$. For E_8, the E_7 case shows that the roots with α_8-coefficient 0 contribute at least $\prod_{s\le 7}(m_s+1)^9$, and the rest contribute at least $(m_8+1)^{15}\prod_{s\le 7}(m_s+1)^6$. Finally, types F_4 and G_2 are similar and easier, and we leave them to the reader.

This completes the proof of the proposition. ∎

Proposition 3.3 *We have*

$$b_1 x^{r/u} \le R_x(G) \le b_2 x^{r/u}(\log x)^{r-1},$$

where b_1, b_2 are positive constants. In particular,

$$R_x(G) = x^{\frac{r}{u}+o(1)}.$$

The final statement of this proposition also follows from [11, Theorem 5.1], with a somewhat different proof to ours.

Proof of 3.3 First we obtain the upper bound for $R_x(G)$. Let $c = \prod_{\alpha\in\Phi^+}\langle\delta,\alpha\rangle$, the denominator in (3). Let $\lambda = \sum m_i\lambda_i$ as above, and assume $\dim V(\lambda) \le x$, so that $N(\lambda) \le cx$. By Proposition 3.2, $\prod_1^r(m_i+1)^{u/r} \le cx$, and hence

$$\prod_1^r(m_i+1) \le c_1 x^{r/u} \tag{5}$$

(where $c_1 = c^{r/u}$). We claim that the number $f(r,x)$ of r-tuples $(a_1,\dots,a_r)$ of natural numbers satisfying $a_1\cdots a_r \le x$ is at most $c_2 x\,(\log x)^{r-1}$. This is

easily proved by induction on r: observe that $f(r,x) \leq \sum_{a_r=1}^{x} f(r-1, x/a_r)$, so by induction we have

$$f(r,x) \leq c_3 \frac{x}{a_r} (\log(x/a_r)^{r-2} \leq c_3 x (\log x)^{r-2} \sum_{1}^{x} a_r^{-1} \leq c_2 x \, (\log x)^{r-1}.$$

By the claim and (5), the number of possibilities for $\lambda = \sum m_i \lambda_i$ with $N(\lambda) \leq cx$ is at most $c_3 x^{r/u} \, (\log x)^{r-1}$, and hence this is an upper bound for $R_x(G)$.

For the lower bound, let $\lambda = \sum_1^r m_i \lambda_i$, and for each $\alpha \in \Phi^+$, define $l_\alpha = \langle \lambda + \delta, \alpha \rangle$. Choose $\epsilon > 0$ such that for any choice of $m_1, \ldots, m_r \leq \epsilon x^{1/u}$, we have $l_\alpha \leq (cx)^{1/u}$ for all $\alpha \in \Phi^+$. So for all such m_i we have

$$\dim V(\lambda) = \frac{\prod_{\alpha \in \Phi^+} l_\alpha}{c} \leq x.$$

The number of choices of $(m_1, \ldots, m_r)$ with all $m_i \leq \epsilon x^{1/u}$ is at least $\epsilon^r x^{r/u}$, and hence $R_x(G) \geq b_1 x^{r/u}$ for some positive constant b_1. ∎

Theorem 1 follows from Proposition 3.3 and Lemma 3.1, together with Lemma 2.1.

4 Products of p-adic groups

In this section we prove Theorem 2. Let G be an absolutely simple, simply connected k-group, where k is an algebraic number field. Define $R = R(G)$ as in Table 1, let $c_1 > 0$ be as in Lemma 2.6, and recall the $G^\epsilon(q)$ notation in that lemma.

Lemma 4.1 *For almost all primes $\mathfrak{p}$ of O, the dimension of any nontrivial irreducible complex finite representation ρ of $G(O_\mathfrak{p})$ satisfies*

$$\dim \rho = a p^i$$

for some $a, i \in \mathbb{N}$ such that $a \geq c_1 q^R$, where $q = p^f = N(\mathfrak{p})$, and a divides $|G^\epsilon(\mathbb{F}_q)|$ for some ϵ.

Proof. We may assume that p is sufficiently large so that good reduction holds (see [18, Section 3]). Let $\bar{G} = G(O_\mathfrak{p})/\ker \rho$. Then $\bar{G}$ is a finite group which is an extension of a p-group V by some $G^\epsilon(\mathbb{F}_q)$. If $V = 1$ the result follows from Lemma 2.6.

Now assume that $V \neq 1$. It is well known (see [23, 5.2]) that the successive congruence quotients of $G(O_\mathfrak{p})$ have the structure of adjoint modules

for $G^\epsilon(\mathbb{F}_q)$. Assuming (as we may) that $p > \mathrm{rank}(G)+1$, the adjoint module is irreducible for $G^\epsilon(\mathbb{F}_q)$. It follows that if W is a minimal normal subgroup of $\bar{G}$ contained in $Z(V)$, then $G^\epsilon(\mathbb{F}_q)$ fixes no nonzero element of $Z(V)^*$. By Clifford's theorem, $\rho \downarrow W = e\sum_{i\in\Delta}\theta_i$, where $e \in \mathbb{N}$ and the sum is over a $\bar{G}$-orbit Δ of irreducible representations θ_i of W. By the previous remark, we have $|\Delta| > 1$, and hence $|\Delta|$ is the index of a proper subgroup of $G^\epsilon(\mathbb{F}_q)$. Clearly such an index is at least $m(G^\epsilon(\mathbb{F}_q))$, hence at least $c_1 q^R$. Finally, $\dim\rho = e|\Delta|$ divides $|\bar{G}|$. The result follows, defining $a = e_{p'}|\Delta|$, where $e_{p'}$ is the p'-part of e. ∎

Now let $\mathfrak{p}$ and $q = N(\mathfrak{p})$ be as in Lemma 4.1, and define $\delta_\mathfrak{p}$ to be the zeta function $\delta_{G(O_\mathfrak{p})}$. Let

$$A_\mathfrak{p} = \{a \in \mathbb{N} : a \geq c_1 q^R \text{ and } a \text{ divides } |G^\epsilon(\mathbb{F}_q)| \text{ for some } \epsilon\}.$$

For each $a \in A_\mathfrak{p}$ and $s \in \mathbb{R}$, define

$$\delta_{\mathfrak{p},a}(s) = \sum_{i\geq 0}(ap^i)^{-s} = \frac{a^{-s}}{1-p^{-s}}.$$

Then by Lemma 4.1,

$$\delta_\mathfrak{p}(s) \leq 1 + \sum_{a\in A_\mathfrak{p}} \delta_{\mathfrak{p},a}(s) \tag{6}$$

where the first term 1 accounts for the trivial representation. Hence for $s > 0$,

$$\delta_\mathfrak{p}(s) \leq 1 + \sum_{a\in A_\mathfrak{p}} \frac{a^{-s}}{1-p^{-s}}. \tag{7}$$

In particular, for $s > 0$, $\delta_\mathfrak{p}(s)$ is finite.

Lemma 4.2 *For any $s > \frac{1}{R}$, there exists $t > 1$ such that $\delta_\mathfrak{p}(s) \leq 1 + cq^{-t}$, where $q = N(\mathfrak{p})$ and c depends only on the rank of G.*

Proof. We may assume that $\mathfrak{p}$ satisfies the conclusion of Lemma 4.1. Since $a \geq c_1 q^R$ for $a \in A_\mathfrak{p}$, it follows from (7) that

$$\delta_\mathfrak{p}(s) \leq 1 + |A_\mathfrak{p}|\,(c_1 q^R)^{-s}\frac{1}{1-p^{-s}}. \tag{8}$$

Now $|A_\mathfrak{p}| \leq \sum_\epsilon d(|G^\epsilon(\mathbb{F}_q)|)$, where G^ϵ are the possible twisted types, and $d(n)$ is the number of divisors of n. Since $|G^\epsilon(\mathbb{F}_q)| < q^{4r^2}$ and $d(n) = n^{o(1)}$, it follows that $|A_\mathfrak{p}| = q^{o(1)}$: in other words, for every $\epsilon > 0$,

$$|A_\mathfrak{p}| \leq q^\epsilon \text{ provided } q > f(\epsilon). \tag{9}$$

Take f such that also $c_1 q^R > q^{R-\epsilon}$ for $q > f(\epsilon)$. Since $s > 1/R$, we may choose $\epsilon > 0$ such that $t := s(R-\epsilon) - \epsilon > 1$. Then for $q > f(\epsilon)$, we have by (8) and (9),

$$\delta_{\mathfrak{p}}(s) \leq 1 + q^{\epsilon} \cdot q^{-(R-\epsilon)s} \cdot \frac{1}{1 - p^{-1/R}} \leq 1 + cq^{-t},$$

where $c = \frac{1}{1-2^{-1/R}}$. ∎

Now define $H = \prod_{\mathfrak{p}} G(O_{\mathfrak{p}})$, where $\mathfrak{p}$ ranges over all but finitely many primes of O.

Lemma 4.3 *If $s > \frac{1}{R}$, then $\delta_H(s) < \infty$.*

Proof. By Lemma 2.2, $\delta_H(s) \leq \prod_{\mathfrak{p}} \delta_{\mathfrak{p}}(s)$, and so by Lemma 4.2,

$$\delta_H(s) \leq \prod_{\mathfrak{p}} (1 + cN(\mathfrak{p})^{-t}).$$

This converges for $t > 1$ by the convergence of the Dedekind zeta function $\zeta_O(t) = \sum N(I)^{-t}$, where I ranges over all nonzero ideals of O. ∎

Lemma 4.4 *There is a set P of rational primes of positive density such that for each $p \in P$, H maps epimorphically onto $G(\mathbb{F}_p)$.*

Proof. Choose a finite Galois extension k' of k over which G is split, and let P be the set of rational primes that split completely in k' and are sufficiently large for G to have good reduction. The Cebotarev density theorem shows that P has positive density.

Now let $\mathfrak{P}$ be a prime of k' dividing $p \in P$ and set $\mathfrak{p} = \mathfrak{P} \cap O_k$. Then $G(O_{\mathfrak{p}})$ maps onto

$$G(O_{\mathfrak{p}}/\mathfrak{p}) \cong G(O_{k'}/\mathfrak{P}) \cong G(\mathbb{F}_p).$$

∎

Lemma 4.5 *Let L be a group which maps onto $G(\mathbb{F}_p)$ for all $p \in P$, where P is a set of rational primes of positive density. Then*

$$d_L(x) \geq x^{1/R + o(1)},$$

where $R = R(G)$.

Proof. Clearly D_L contains the numbers $m(G(\mathbb{F}_p))$ for all primes $p \in P$. By Lemma 2.6, we have $m(G(\mathbb{F}_p)) < c_2 p^R$. Given x, let P_x be the set of primes $p \in P$ with $p > 3$ and $c_2 p^R \leq x$. Since P has positive density, there exists $b > 0$ such that

$$|P_x| \geq \frac{bx^{1/R}}{\log x} = x^{1/R+o(1)}.$$

For $p \in P_x$ we have $m(G(\mathbb{F}_p)) \leq x$, and by Lemma 2.6, $m(G(\mathbb{F}_p))$ is given by a polynomial in p of degree R (two polynomials if $G = G_2$). This implies that each number in the sequence $(m(G(\mathbb{F}_p)) : p \in P_x)$ occurs at most $2R$ times, and hence

$$d_L(x) \geq \frac{|P_x|}{2R} = x^{1/R+o(1)}.$$

■

Proof of Theorem 2

It follows from Lemmas 2.3(i) and 4.3 that $d_H(x) = O(x^s)$ for any $s > \frac{1}{R}$. Hence $d_H(x) \leq x^{\frac{1}{R}+o(1)}$, giving the upper bound in Theorem 2. The lower bound follows from the two preceding lemmas.

5 Arithmetic groups

In this section we prove Theorem 3. Let k be a algebraic number field, let G be an absolutely simple, simply connected k-group, and let $\Gamma = G(O_S)$ where S is a finite set of primes of k. Assume that Γ has the congruence subgroup property. By [11, 3.3], Γ has a finite index subgroup Γ_0 such that the proalgebraic completion $A(\Gamma_0)$ satisfies

$$A(\Gamma_0) = G(\mathbb{C})^j \times \prod_{\mathfrak{p} \notin S} L_{\mathfrak{p}}$$

where j is the number of infinite places of k and $L_{\mathfrak{p}}$ is an open subgroup of $G(O_{\mathfrak{p}})$, equal to it for almost all $\mathfrak{p}$. In view of Corollary 2.5, we may assume that $\Gamma = \Gamma_0$. As explained in [11, Section 2], we then have

$$D_\Gamma = D_{G(\mathbb{C})^j \times H},$$

where $H = \prod_{\mathfrak{p} \notin S} L_{\mathfrak{p}}$. Note that H has finite index in $H_1 = \prod_{\mathfrak{p} \notin S} G(O_{\mathfrak{p}})$.

Fix $s > r/u$. Then $\delta_{G(\mathbb{C})}(s) < \infty$ by Theorem 1 and Lemma 2.3(ii). Hence $\delta_{G(\mathbb{C})^j}(s) < \infty$ by Lemma 2.2. Now we consider $\delta_H(s)$. By inspection we have $r/u \geq 1/R$, where $R = R(G)$ is as defined in Table 1 in the Introduction. Since $s > r/u$, it follows that $s > 1/R$, and so Lemma 4.3 (applied to H_1) implies that $\delta_H(s) < \infty$. Consequently Lemma 2.2 implies that

$$\delta_{G(\mathbb{C})^j \times H}(s) \leq \delta_{G(\mathbb{C})^j}(s)\, \delta_H(s) < \infty.$$

Now Lemma 2.3(i) yields $\delta_{G(\mathbb{C})^j \times H}(x) = O(x^s)$. Hence

$$d_\Gamma(x) = d_{G(\mathbb{C})^j \times H}(x) \leq x^{r/u+o(1)},$$

giving the upper bound in Theorem 3. For the lower bound, observe that $d_\Gamma(x) \geq d_{G(\mathbb{C})}(x) \geq x^{r/u+o(1)}$ by Theorem 1. This completes the proof of Theorem 3.

6 Linear groups

In this section we prove Theorem 4. First we quickly reduce to the case where the linear group G is virtually soluble.

6.1 Reduction to soluble groups

The key to the reduction is the following version of the "Lubotzky alternative" (see [17, Corollary 6.3]).

Proposition 6.1 *Let G be a finitely generated linear group in characteristic zero, and suppose that G is not virtually soluble. Then there exist a subgroup L of finite index in G, a fixed (untwisted) Lie type X, and a set P of primes of positive density, such that L maps onto $X(\mathbb{F}_p)$ for each $p \in P$.*

Corollary 6.2 *If G is as in Proposition 6.1, then there exists $\alpha > 0$ such that $d_G(x) > x^\alpha$ for all sufficiently large x.*

Proof. This follows from the Proposition together with Lemma 4.5. ■

The rest of the proof concerns the soluble case. This has a strong number-theoretic flavour, and we begin with some preparations for this.

6.2 Some number theory, I: number fields

Let k be an algebraic number field. To each prime $\mathfrak{p}$ of k is associated a finite residue field $k(\mathfrak{p}) = O/\mathfrak{p}$. Let $\mathcal{F}_k$ denote the set of residue fields $k(\mathfrak{p})$ for primes $\mathfrak{p}$ of k. The following is elementary algebraic number theory.

Lemma 6.3 *If $(K : \mathbb{Q}) = f$ then for every (rational) prime p there exists s with $1 \leq s \leq f$ such that $\mathbb{F}_{p^s} \in \mathcal{F}_k$.*

A subring R of k will be called *full* if R is finitely generated as a ring and k is its field of fractions. In this case, there is a finite set S of primes

of k such that each prime $\mathfrak{p} \notin S$ corresponds to a maximal ideal P of R with $R/P \cong k(\mathfrak{p})$. We write $\pi_\mathfrak{p} : R \to k(\mathfrak{p})$ for the associated epimorphism. Let Δ be a finitely generated subgroup of k^* such that the additive span $R = R(\Delta)$ of Δ is a full subring of k. Then the following is immediate from Lemma 6.3:

Lemma 6.4 *There exist natural numbers f and N such that for every prime $p \geq N$ there is a prime $\mathfrak{p}$ of k such that $R(\Delta)\pi_\mathfrak{p} = \mathbb{F}_{p^s}$ with $1 \leq s \leq f$.*

If $\pi : R(\Delta) \to \mathbb{F}_{p^s}$ is an epimorphism then $\Delta\pi$ is cyclic, and a generator is a primitive element for $\mathbb{F}_{p^s}$; hence

$$s \leq |\Delta\pi| \mid p^s - 1. \tag{10}$$

Now let $\mathcal{N}(\Delta)$ denote the set of numbers $|\Delta\pi_\mathfrak{p}|$ with $\mathfrak{p}$ as in the preceding lemma.

The key to our argument is the following sieve-theoretic result.

Theorem 6.5 *Let $h \in \mathbb{N}$. Then there exist $d = d(h) \in \mathbb{N}$ and $c = c(h) > 0$ such that for all sufficiently large x, there is a set of primes Q_x with the following properties:*

$$\begin{gathered} p^h < x \text{ for all } p \in Q_x, \\ (p^h - 1, q^h - 1) \mid d \text{ for all } p \neq q \in Q_x, \\ |Q_x| > x^c. \end{gathered}$$

This will be proved in the next subsection. Now we use it to deduce

Proposition 6.6 *Suppose that Δ is infinite. Then there exists $c > 0$ such that*

$$|\mathcal{N}(\Delta) \cap [1, x]| \geq x^c$$

for all sufficiently large x.

Proof. Put $h = f!$. Then Lemma 6.4, with (10), shows that for every sufficiently large prime p, the set $\mathcal{N}(\Delta)$ contains a number $n_p = |\Delta\pi_\mathfrak{p}|$ which divides $p^h - 1$. If $n_p \mid d = d(h)$ then $\Delta^d - 1 \subseteq \ker \pi_p$; as the intersection of any infinite set of prime ideals in R is zero, while Δ is infinite, this can occur for at most finitely many p. Hence if p and q are sufficiently large distinct primes and $n_p = n_q$ then $(p^h - 1, q^h - 1)$ does not divide d.

Let $\mathcal{Q}$ denote the finite set of insufficiently large primes in the above sense, and let x be a large real number. The preceding observations show that $p \mapsto n_p$ maps $Q_x \setminus \mathcal{Q}$ injectively into the set $\mathcal{N}(\Delta) \cap [1, x]$. The result now follows from Theorem 6.5, on replacing c by any slightly smaller positive number. ∎

6.3 Some number theory, II: a sieve result

Here we prove Theorem 6.5.

The proof depends on the following result.

Lemma 6.7 *Fix an integer $h \geq 1$, and let x be a sufficiently large real number. Then there is a set Q_1 of primes $p \leq x$, a constant $a > 0$, a positive real number $c_1(h)$, and a positive integer $d_1(h)$, with the following properties:*

(i) $|Q_1| > ax(\log x)^{-h}$

(ii) *for all $p \in Q_1$, $d_1(h)$ divides $p^h - 1$ properly*

(iii) *for all $p \in Q_1$, all prime factors of $(p^h - 1)/d_1(h)$ are greater than $x^{c_1(h)}$.*

Proof. This follows from [3, Theorem 2.6] (taking $u = 1/c_1(h)$ large enough for the first error term in (8.4) to be at most $\frac{1}{2}$). ∎

We now prove Theorem 6.5. Let $y = x^{1/h}$; then $p^h - 1 < x$ for $p < y$. Apply Lemma 6.7 with y replacing x, giving $Q_1, c_1(h), d_1(h)$. Define $d(h) = d_1(h)$, and choose a maximal subset Q of Q_1 satisfying the second condition of Theorem 6.5.

Let $p \in Q$, and write $p^h - 1 = d(h)p_1 \cdots p_b$ where the p_i are primes. As $p \in Q_1$, we have $p_i > y^{c_1(h)}$ for all i. Hence

$$x = y^h > p^h - 1 > y^{c_1(h)b}.$$

It follows that $h > c_1(h)b$, so $b < b(h) := h/c_1(h)$.

We claim that for each i, the number of primes $q \in Q_1$ such that p_i divides $q^h - 1$ is at most hy/p_i. Indeed, $q^h - 1$ is a polynomial in q which has at most h roots in $\mathbb{F}_{p_i}$. For each such root α, there are at most y/p_i numbers up to y which are congruent to α mod p_i. This proves the claim.

Since $p_i > y^{c_1(h)}$, it follows that the number of primes $q \in Q_1$ such that p_i divides $q^h - 1$ is at most $hy^{1-c_1(h)}$. Therefore the number of primes $q \in Q_1$ with $\gcd((p^h - 1)/d(h), (q^h - 1)/d(h)) > 1$ is at most $b(h)hy^{1-c_1(h)}$. Letting $p \in Q$ vary, we conclude that the number of $q \in Q_1$ satisfying $\gcd((p^h - 1)/d(h), (q^h - 1)/d(h)) > 1$ for some $p \in Q$ is at most

$$|Q|b(h)hy^{1-c_1(h)}.$$

By the maximality of Q, this number must be at least $|Q_1|$, giving

$$|Q|b(h)hy^{1-c_1(h)} \geq |Q_1| \geq ay(\log y)^{-h}.$$

This yields

$$|Q| > ab(h)^{-1}h^{-2}(\log y)^{-h}y^{c_1(h)}.$$

This is greater than $x^{c(h)}$ for any $c(h) < c_1(h)/h$.

This completes the proof of Theorem 6.5.

6.4 Soluble groups

For a finite field F, let $A(F)$ denote the 1-dimensional affine group $F_+ \rtimes F^*$. We call a subgroup H of $A(F)$ *full* if $H = F_+ \rtimes U$, where $1 < U \leq F^*$ and U spans F additively; this holds if and only if F_+ is irreducible and non-trivial as a U-module.

Proposition 6.8 *Let G be a torsion free finitely generated metabelian group, and suppose that G is not virtually nilpotent. Then there exist an algebraic number field k and a homomorphism $\phi : G \to k^*$ such that:*

(i) *$G\phi$ is infinite and spans a full subring R of k;*

(ii) *for almost all primes $\mathfrak{p}$ of k, there is a homomorphism $\theta_\mathfrak{p} : G \to A(k(\mathfrak{p}))$ such that the diagram*

$$\begin{array}{ccc} G & \stackrel{\phi}{\longrightarrow} & R^* \\ \theta_\mathfrak{p} \downarrow & & \downarrow \pi_\mathfrak{p} \\ A(k(\mathfrak{p})) & \hookleftarrow & k(\mathfrak{p})^* \end{array} \tag{11}$$

commutes, and $G\theta_\mathfrak{p}$ is a full subgroup of $A(k(\mathfrak{p}))$.

Proof. Set $A = G'$ and consider A as an additively-written module for $\Gamma = G/A$. Put $S = \mathbb{Z}\Gamma$. Then S is a finitely generated $\mathbb{Z}$-algebra and A is a finitely generated, hence Noetherian, S-module (cf. [12, 11.1.1]). Let

$$0 = A_1 \cap \ldots \cap A_t$$

be a primary decomposition of zero in the S-module A; say A/A_i is P_i-primary where $P_1, \ldots, P_t$ are prime ideals of S, $\mathrm{char}(S/P_i) = 0$ for $i = 1, \ldots, r$ and $\mathrm{char}(S/P_i) = q_i \neq 0$ for $i = r+1, \ldots, t$. There exists $s \in \mathbb{N}$ such that $AP_i^s \leq A_i$ for each i. Put $q = \prod_{i=r+1}^t q_i^s$. Then

$$q(A_1 \cap \ldots \cap A_r) \leq A_1 \cap \ldots \cap A_r \cap AP_{r+1}^s \cap \ldots \cap AP_t^s = 0.$$

Since G is torsion-free, it follows that $A_1 \cap \ldots \cap A_r = 0$.

For each n there exists $i \leq r$ such that $\Gamma^{n!}$ does not act nilpotently on A/A_i. At least one value of i occurs infinitely often, say $i = m$. Then no subgroup of finite index in Γ acts nilpotently on A/A_m. Replacing G by G/A_m, we may as well assume henceforth that A is a P-primary S-module, where P is a prime ideal such that $|\Gamma : \Gamma \cap (1+P)| = \infty$ and $\mathrm{char}(S/P) = 0$.

Now S/P is a finitely generated infinite integral domain. According to [2, Theorem A], there exist an algebraic number field k and a homomorphism $\theta : S \to k$, with $P \leq \ker\theta = Q$ say, such that θ induces an injective homomorphism from the group of units $(S/P)^*$ into k^*. We may take k to be the field of fractions of $S\theta = R$, and put $\Delta = \Gamma\theta \leq R^*$. Then

$$\Delta \cong \Gamma/(\Gamma \cap (1+Q)) = \Gamma/(\Gamma \cap (1+P))$$

is an infinite group.

Now let

$$\phi : G \to \Gamma \to k^*$$

be the map induced by θ. Then $G\phi = \Delta$ is an infinite subgroup of k^*, and Δ spans the full subring R of k.

Since A is a P-primary S-module, there exists $a \in A$ with $\mathrm{ann}_S(a) = P$. Then

$$aS/aQ \cong S/Q.$$

Let $K \geq aQ$ be an S-submodule of A maximal subject to A/K containing a copy of S/Q. Using the Artin-Rees Lemma it is easy to see that $AQ \leq K$ and A/K is torsion-free of rank one as an S/Q-module. Replacing G by G/K, we may suppose that A itself is torsion-free of rank one as an S/Q-module. Then A contains a free cyclic S/Q-submodule B such that $As \leq B$ for some $s \in S \setminus Q$, and $A/AL \cong S/L$ for every maximal ideal L of S with $L \geq Q$ and $s \notin L$.

Let $\mathfrak{p}$ be a prime of k corresponding to a maximal ideal $P_\mathfrak{p}$ of R, and put $L = P_\mathfrak{p}\theta^{-1}$, so L is a maximal ideal of S containing Q and $S/L \cong k(\mathfrak{p}) := F$. Let us assume that $s \notin L$ and that $\Delta - 1 \not\subseteq P_\mathfrak{p}$: this excludes only finitely many possibilities for $\mathfrak{p}$. Then $A/AL \cong S/L \cong F$, the action of $g \in G$ on A/AL corresponding to multiplication by $g\phi\pi_\mathfrak{p} \in F$, and $U := G\phi\pi_\mathfrak{p} \neq 1$. In particular, A/AL is simple and non-trivial as a G-module.

Put $C = \mathrm{C}_G(A/AL) = \ker(\phi\pi_\mathfrak{p})$ and set $Z/AL = \mathrm{Z}(G/AL)$. Then C/Z embeds in $\mathrm{Hom}(G/A, A/AL)$, so C/Z is an elementary abelian p-group where $p = \mathrm{char}(F)$; on the other hand, $G/C \cong U \leq F^*$, a p'-group. It follows that $C/Z = T/Z \times Y/Z$ where $Y/Z = \mathrm{C}_{C/Z}(G)$ and

$$T/Z = [C,G]Z/Z = AZ/Z \cong A/(A \cap Z) = A/AL.$$

As $(|G/C|, |C/Y|) = 1$ this now implies that

$$G/Y \cong (TY/Y) \rtimes (G/C) \cong (A/AL) \rtimes (G/C) \cong F_+ \rtimes U,$$

a full subgroup of $A(F)$; a suitable epimorphism $\theta_\mathfrak{p} : G \to G/Y \to F_+ \rtimes U$ then makes the diagram (11) commute. ∎

For a full subgroup $H = F_+ \rtimes U$ of $A(F)$, write $n(H) = |U|$; this is the p'-part of $|H|$ where $p = \mathrm{char}(F)$.

Proposition 6.9 *Let H be a full subgroup of $A(\mathbb{F}_{p^f})$. Then the irreducible character degrees of H are 1 and $n(H)$.*

Proof. This is a special case of [6, 12.3]. ∎

Now let $\phi : G \to G\phi = \Delta \leq k^*$ be as in Proposition 6.8. Then for almost all primes $\mathfrak{p}$ of k we have

$$G\theta_{\mathfrak{p}} \cong k(\mathfrak{p})_+ \rtimes \Delta\pi_{\mathfrak{p}}$$

so G has a character of degree $n(G\theta_{\mathfrak{p}}) = |\Delta\pi_{\mathfrak{p}}|$. Thus

$$D_G \supseteq \mathcal{N}(\Delta) \smallsetminus T \tag{12}$$

for some finite set T. The results of section 6.2 therefore imply lower bounds for the growth of D_G, and for any group that maps onto G. We will exploit these.

Let us say that a group G is *strongly torsion-free* if there exist disjoint sets of primes π and σ such that G is residually a π-group and residually a σ-group. As noted in the Introduction, finitely generated linear groups in characteristic zero are virtually strongly torsion-free; so are torsion-free finitely generated abelian-by-polycyclic groups ([19]). Strongly torsion-free groups are evidently torsion free; they also have many natural torsion-free quotients, as exemplified in

Lemma 6.10 *If G is strongly torsion-free and A is maximal among abelian normal subgroups of G then G/A is strongly torsion-free.*

Proof. Let $\mathcal{X}$ denote the set of $N \lhd G$ such that G/N is a π-group. Then

$$\left[\bigcap_{N\in\mathcal{X}} NA, \bigcap_{N\in\mathcal{X}} NA\right] \leq \bigcap_{N\in\mathcal{X}} N = 1,$$

so $\bigcap_{N\in\mathcal{X}} NA = A$. Thus G/A is residually a π-group, and similarly with σ in place of π. ∎

Proposition 6.11 *Let G be a finitely generated virtually nilpotent group that is not virtually abelian. Then there exists $\alpha > 0$ such that $d_G(x) > x^\alpha$ for all large x.*

Proof. By 2.5, we may assume that G is nilpotent. Since G has a maximal normal subgroup N such that G/N is not virtually abelian, we may further assume that G is just non-virtually abelian (i.e. every proper quotient is virtually abelian). We have $Z(G) \neq 1$, and hence $G/Z(G)$ is

virtually abelian, so G is virtually of class 2. So we may assume G is of class 2. Replacing G by a subgroup of finite index, we may also assume that G is torsion-free. For a prime p, define $G_p = G/G^p$. This a finite p-group of exponent p, generated by $d = d(G)$ elements. Hence $|G_p| \leq p^b$, where $b = d + \binom{d}{2}$.

We claim that for all sufficiently large primes p, G_p is non-abelian. Indeed, if this is not the case, then there is an infinite set P of primes p such that $G' \subseteq G^p$ for all $p \in P$. However, according to a result of Higman [4], we have $\bigcap_{p\in P} G^p = 1$, which is a contradiction.

Say G_p is non-abelian for all $p > c$. Then for all $p > c$, G_p has an irreducible character χ_p of degree p^{i_p}, where $1 \leq i_p \leq b/2$. This shows that

$$D_G \supseteq \{p^{i_p} \,:\, p > c\},$$

which gives $d_G(x) \geq x^\alpha$ for any $\alpha < 2/b$ and large enough x. ∎

Theorem 6.12 *Let G be a finitely generated virtually soluble group, and assume that G is virtually strongly torsion free. Then exactly one of the following holds:*

(a) *G is virtually abelian, and $d_G(x)$ is bounded for all x;*

(b) *there exists $\alpha > 0$ such that $d_G(x) > x^\alpha$ for all large x.*

Proof. If G has an abelian normal subgroup of index m then $d_G(x) \leq m$ for all x, by Lemma 2.4. Assume now that G is not virtually abelian. If G has a non-(virtually abelian) quotient that is virtually nilpotent the result follows from Proposition 6.11, so we shall assume further that every virtually nilpotent quotient of G is virtually abelian.

We claim that G has normal subgroups $G_0 > N$ such that G/G_0 is finite and G_0/N is torsion-free and metabelian. Accepting the claim for now, we apply Proposition 6.8 to the group G_0/N. With (12) and Proposition 6.6 this shows that $d_{G_0/N}(x)$ satisfies the inequality specified in (**b**). The result follows by Lemma 2.4.

The claim is proved by induction on $l(G)$, the least derived length of any soluble subgroup of finite index in G. If $l(G) \leq 2$ then $l(G) = 2$ and we take $N = 1$. Suppose that $l(G) = l \geq 3$, and let G_1 be a strongly torsion-free soluble normal subgroup of finite index in G having derived length l. Let A_1 be maximal among abelian normal subgroups of G_1 containing $G_1^{(l-1)}$, and put $A = \mathrm{core}_G(A_1)$. Then G/A is not virtually abelian since $l(G) \geq 3$, and G_1/A_1 is strongly torsion-free by Lemma 6.10, and hence so is G_1/A. As the derived length of G_1/A is $l - 1$, the claim now follows on applying the inductive hypothesis to G/A. ∎

Proof of Theorem 4

Let G be a finitely generated linear group over a field of characteristic zero, and assume that G is not virtually abelian. By Corollary 6.2 we may assume that G is virtually soluble. Now G is virtually strongly torsion-free by [22, Theorem 4.7]. The conclusion follows by Theorem 6.12.

References

[1] N. Bourbaki, *Groupes et Algebres de Lie* (Chapters 4,5,6), Hermann, Paris, 1968.

[2] F. Grunewald and D. Segal, Remarks on injective specializations, *J. Algebra* **61** (1979), 538-547.

[3] H. Halberstam and H. Richert, *Sieve methods*, London Math. Soc. Monographs, No. 4, Academic Press 1974.

[4] G. Higman, A remark on finitely generated nilpotent groups, *Proc. Amer. Math. Soc.* **6** (1955), 284–285.

[5] J.E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, 1972.

[6] I.M. Isaacs, *Character theory of finite groups*, Pure and Applied Mathematics, No. 69, Academic Press, 1976.

[7] I.M. Isaacs, Character degrees and derived length of a solvable group, Canad. J. Math. 27 (1975), 146–151.

[8] I.M. Isaacs and D.S. Passman, Groups with representations of bounded degree, *Canad. J. Math.* **16** (1964), 299–309.

[9] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series **129**, Cambridge University Press, Cambridge, 1990.

[10] V. Landazuri and G.M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418-443.

[11] M. Larsen and A. Lubotzky, Representation growth for linear groups, *J. Eur. Math. Soc.* **10** (2008), 351–390.

[12] J. C. Lennox and D. J. S. Robinson, *The theory of infinite soluble groups,* Clarendon Press, Oxford, 2004.

[13] M.W. Liebeck and A. Shalev, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc.* **90** (2005), 61-86.

[14] M.W. Liebeck and A. Shalev, The sparsity of dimensions of irreducible representations of finite simple groups, *Bull. London Math. Soc.* **39** (2007), 467–472.

[15] F. Lübeck, Smallest degrees of representations of exceptional groups of Lie type, *Comm. Algebra* **29** (2001), 2147–2169.

[16] A. Lubotzky and D. Segal, *Subgroup growth*, Progress in Mathematics, 212, Birkhauser Verlag, Basel, 2003.

[17] N. Nikolov, Strong approximation methods in group theory, LMS/EPSRC Short course lecture notes, arXiv:0803.4165

[18] V. P. Platonov and A. Rapinchuk, *Algebraic groups and number theory,* Academic Press, New York, 1994.

[19] D. Segal, On abelian-by-polycyclic groups, *J. London Math. Soc.* **11** (1975), 445-452.

[20] A. Shalev, The density of subgroup indices, *J. Aust. Math. Soc.* **85** (2008), 257–267.

[21] P.H. Tiep and A.E. Zalesskii, Minimal characters of the finite classical groups, *Comm. Algebra* **24** (1996), 2093–2167.

[22] B. A. F. Wehrfritz, *Infinite linear groups,* Springer-Verlag, Berlin, 1973.

[23] B. Weisfeiler, Strong approximation for Zariski-dense subgroups of semisimple algebraic groups, *Annals of Math.* **120** (1984), 271–315.