Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Algebra 286 (2005) 476–491
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Character degrees of p-groups and pro-p groups

Alireza Salehi Golsefidy

Department of Mathematics, Yale University, New Haven, CT 06520, USA

Received 19 March 2004

Communicated by Efim Zelmanov

Abstract

In the 1970s, Isaacs conjectured that there should be a logarithmic bound for the length of solvability of a p-group G with respect to the number of different irreducible character degrees of G. So far, there are just a few partial results for this conjecture. In this note, we say that a pro-p group G has property (I) if there is a real number $D = D(G)$ that just depends on G such that for any open normal subgroup N, $\mathrm{dl}(G/N) \leqslant \log_2 |\mathrm{cd}(G/N)| + D$. We prove that any p-adic analytic pro-p group has property (I). We also study the first congruence subgroup G of a classical Chevalley group $\mathbb{G}$ with respect to the local ring $\mathbb{F}_p[\![t]\!]$. We show that if $\mathrm{Lie}(\mathbb{G})(\mathbb{F}_p)$ has a non-degenerated Killing form, then G has property (I).

Keywords: Character; Monomial groups; Pro-p groups; Chevalley groups

1. Introduction and statements of results

In 1930s Taketa has shown that if G is a monomial group, then it is solvable and $\mathrm{dl}(G) \leqslant |\mathrm{cd}(G)|$ (see [Is94] or [Hu98]). In the 1970s Isaacs asked two questions regarding this inequality. First, he asked if the same inequality holds for any solvable group. Second, he asked if there is a logarithmic bound for $\mathrm{dl}(G)$ with respect to $|\mathrm{cd}(G)|$ when G is a p-group. Though both of these question are still open, there are more success in the

E-mail address: alireza.salehigolsefidy@yale.edu.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2004.12.013

first one. Gluck [Gl85] has proved that $\mathrm{dl}(G) \leqslant 2|\mathrm{cd}(G)|$ and Berger [Be76] proved the conjecture for groups having odd order. For the second question, it is a common believe that the answer should be affirmative even for any solvable group. A lot of work has recently been done in this direction by T. Keller [K99(I),K99(II),K02], and he has almost shown that if Isaacs' original problem has an affirmative answer, then there is an affirmative answer to the question for any solvable group. However, in the case of p-groups, there are just a few partial results. For instance, M. Slattery [Sl89] improved Taketa's inequality just by 1 when $\mathrm{cd}(G) = \{1, p, \ldots, p^n\}$. A. Moretó [Mo03] has recently studied p-groups whose set of character degrees consists of two parts A and B such that $A = \{1, p, \ldots, p^n\}$ and any element of B is bigger than p^{2n}. He shows that for some absolute constants E_1 and E_2, $\mathrm{dl}(G) \leqslant E_1 \log n + |B| + E_2$. This result gives a logarithmic bound if $|B|$ has an upper bound, and in particular when B is empty. Nevertheless, the general case is far from to be solved.

In this note, we are going to attack this problem via pro-p groups. We say a pro-p group has property (I) if its finite quotients satisfy Isaacs' conjecture, namely if there exists a real number $D = D(G)$ that depends only on G such that for any normal open subgroup N of G,

$$\mathrm{dl}(G/N) \leqslant \log_2 \bigl|\mathrm{cd}(G/N)\bigr| + D.$$

We will prove the following results:

Theorem A. *Any p-adic analytic pro-p group has property* (I).

Theorem B. *Let $G = \ker(\mathbb{G}(\mathbb{F}_p[\![t]\!]) \to \mathbb{G}(\mathbb{F}_p))$, where $\mathbb{G}$ is a classical Chevalley group. Then G has property* (I) *if $p > 2, 3$ does not divide $n+1$ when $\mathbb{G}$ is of type A_n or C_n; $2n-1$ when $\mathbb{G}$ is of type B_n or $n-1$ when $\mathbb{G}$ is of type D_n.*

In order to prove Theorem A, we use Howe's Kirillov theory for compact p-adic analytic groups, and show $\mathrm{dl}(G/G_n) \leqslant \log_2 |\mathrm{cd}(G/G_n)| + 3$ for any uniform group G with dimensional subgroups G_n. Then, in order to get to any open normal subgroup N, we start with uniform groups with $\mathbb{Q}_p$-simple Lie algebra and prove that for these groups, one can find $f = f(G)$ that just depends on G, such that $G_{n+f} \subset N \subseteq G_n$, for some n. This information gives us property (I) for these kind of uniform groups. Then we prove property (I) for "semisimple" case and finally for the general case.

The second part of this note is devoted to the proof of Theorem B. For $\mathbb{F}_p[\![t]\!]$-analytic groups there is no analogue of Kirillov theory, as Howe extensively used Baker–Campbell–Hausdorff formula, which is meaningless in the positive characteristic. So in this case we will work with a finite analogue of the adjoint action, and use Clifford's correspondence to get different irreducible character degrees. We show that $\mathrm{dl}(G/G_n) \leqslant \log_2 |\mathrm{cd}(G/G_n)| + 3$ where G_n is the nth congruence subgroup. Finally by a result of Shalev, we control any open normal subgroup of G, by congruence subgroups, and get the result.

2. Notation and background

2.1. Notation

Throughout this note, we will use the following notation:

$\vert X\vert$:	the number of elements of the set X;
$\mathrm{dl}(G)$:	length of solvability of the solvable group G;
$\mathrm{Irr}(G)$:	the set of continuous irreducible complex characters of G;
$\mathrm{cd}(G)$	$:= \{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}$.

Let G be a group, $N \leqslant G$, $\chi \in \mathrm{Irr}(G)$, and $\nu \in \mathrm{Irr}(N)$.

χ_N:	the restriction of χ on N;
ν^G:	the induced character;
${}^g\nu(x)$	$:= \nu(g^{-1}xg)$ for any $g \in G$ and $x \in N$;
$I_G(\nu)$	$:= \{g \in G \mid {}^g\nu = \nu\}$;
$Z(\chi)$	$:= \{g \in G \mid \vert\chi(g)\vert = \chi(1)\}$.

2.2. Character theory

We will essentially use the following two well-known theorems from the character theory of finite groups.

Theorem 2.1 [Hu98, p. 253]. *Let G be a finite group, $N \trianglelefteq G$, $\nu \in \mathrm{Irr}(N)$, and $\chi \in \mathrm{Irr}(G)$. Assume that $\langle \chi_N, \nu\rangle = e > 0$ and $[G : I_G(\nu)] = m$. Then*

$$\text{(i)}\quad \chi(1) = em\nu(1), \qquad \text{(ii)}\quad e^2m \leqslant |G/N|.$$

Theorem 2.2 [Is94]. *Let G be a finite group, $N \trianglelefteq G$, and $\nu \in \mathrm{Irr}(N)$. Set $A = \{\chi \in \mathrm{Irr}(G) \mid \langle \chi_N, \nu\rangle \neq 0\}$ and $B = \{\psi \in \mathrm{Irr}(I_G(\nu)) \mid \langle \psi_N, \nu\rangle \neq 0\}$, then $\psi \mapsto \psi^G$ is a bijection between B and A.*

2.3. Pro-p groups

In the first half of this note, we will work with p-adic analytic pro-p groups. We recall some of the definitions, interested reader may find [DSMS99] helpful.

A pro-p group is called k-powerful if $[G, G] \subseteq G^{p^k}$ where G^{p^k} is the group generated by g^{p^k}. A torsion free k-powerful pro-p group is called k-uniform and a uniform group is a 1-uniform if $p \neq 2$ and 2-uniform if $p = 2$. It is well known that if G is a uniform group, we can associate a $\mathbb{Z}_p$-Lie algebra L_G with G. In fact, this algebra can be identified by G as a set and the Lie operations are defined by

$$g + h := \lim_{n\to\infty} \bigl(g^{p^n} h^{p^n}\bigr)^{p^{-n}}, \qquad [g, h] := \lim_{n\to\infty} \bigl(g^{p^n}, h^{p^n}\bigr)^{p^{-2n}}.$$

Similarly, a $\mathbb{Z}_p$-Lie algebra L is called k-powerful if $[L, L] \subseteq p^k L$, and is called powerful if it is 1-powerful (2-powerful) when $p \neq 2$ ($p = 2$).

Let G be a pro-p group and $H \leqslant G$. One says that H is powerfully embedded in G if $[G, H] \subseteq H^{p^{k+1}}$ where $k = 0$ ($k = 1$) when $p \neq 2$ ($p = 2$). If G is a uniform group, then $G_n = G^{p^{n-1}} = \{g^{p^{n-1}} \mid g \in G\}$ is p.e. in G. We are going to need the following theorems:

Theorem 2.3 [DSMS99, p. 151]. *Let G be a uniform pro-p group, and N be a $\mathbb{Z}_p$-Lie subalgebra of L_G such that L_G/N is torsion free. Then*

(i) *N is a closed uniform subgroup of G;*
(ii) *if N is an ideal of L_G then N is normal in G and G/N is uniform and $L_{G/N}$ is isomorphic to L_G/N as a $\mathbb{Z}_p$-Lie algebra.*

Theorem 2.4 [DSMS99, p. 51]. *Let G be a finite rank pro-p group. Then G has a powerful characteristic subgroup W such that any $N \leqslant W$ which is a normal open subgroup of G is p.e. in W.*

Theorem 2.5 [DSMS99, p. 152]. *Let G be a uniform group. Then G is solvable as a group if and only if L_G is solvable as a Lie algebra.*

In the second part of this note, we will work with $\mathbb{F}_p[\![t]\!]$-analytic pro-p groups, and we use the following terminology and result of Shalev [Sh95]: a sequence of open normal subgroups $\{G_n\}_{n=1}^{\infty}$ of a pro-p group G is called an N-sequence if $G = G_1$ and for any positive integers m and n, $[G_n, G_m] \subseteq G_{m+n}$.

Theorem 2.6 [Sh95]. *Let G be a pro-p group, and $\{G_n\}_{n=1}^{\infty}$ be an N-sequence. If $\bigoplus_{n=1}^{\infty} G_n/G_{n+1}$ is isomorphic to $\mathfrak{g} \otimes_{\mathbb{F}_p} t\mathbb{F}_p[t]$ as a graded Lie algebra where $\mathfrak{g}$ is a finite simple Lie algebra, then there exists a real number $f = f(G)$ that just depends on G such that for any normal open subgroup N of G, there is a natural number n:*

$$G_{n+f} \subset N \subseteq G_n.$$

2.4. Howe's Kirillov theory

In the 1970s, R. Howe [Ho77] developed Kirillov theory of compact p-adic analytic groups. He did not go to details for the case of characteristic 2. Recently, A. Jaikin-Zapirain [JZ04] used Howe's correspondence to study the zeta function of irreducible characters of a FAb compact p-adic analytic group. He also studied the case of characteristic two. We follow his work.

If G is a uniform group, as we saw L_G can be identified by G as a set, and so G can act on L_G by group conjugation. We call it adjoint action of G. G also acts on $\mathrm{Irr}(L_G)$ via the adjoint action. If $\Omega \subseteq G$, we define

$$\Phi_\Omega(g) = |\Omega|^{-1/2} \sum_{\omega \in \Omega} \omega(g).$$

Lemma 2.7 [Ho77]. *Let G be a uniform group and $\omega \in \mathrm{Irr}(G)$; then*

$$\mathrm{St}_G(\omega) = \{x \in L_G \mid \omega([x, L_G]) = 1\}.$$

Theorem 2.8 [Ho77]. *Let G be a uniform pro-p group with $p > 2$ and Ω be a G-orbit in $\mathrm{Irr}(L_G)$. Then $\Phi_\Omega \in \mathrm{Irr}(G)$ and all irreducible characters of G have this form.*

Theorem 2.9 [JZ04]. *Let G be a uniform pro-2 group. Then there exists a bijection f between $\mathrm{Irr}(G)$ and $\{\Phi_\Omega \mid \Omega$ is a G-orbit in $\mathrm{Irr}(G)\}$ such that for any $\chi \in \mathrm{Irr}(G)$, $f(\chi)_{G^2} = \chi_{G^2}$.*

Combining these two theorems, we have the following corollary:

Corollary 2.10. *Let G be a uniform group and $G_n = G^{p^{n-1}}$. Then*

$$\mathrm{cd}(G/G_n) = \{|\Omega|^{1/2} \mid \Omega \textit{ is a } G\textit{-orbit in } \mathrm{Irr}(L_G/p^n L_G)\}.$$

3. Uniform groups with simple $\mathbb{Q}_p$-Lie algebras

We shall start with uniform groups. One can easily see the following remark.

Remark 3.1.

(i) $\mathrm{dl}(G/G_n) \leqslant \log_2(n) + 1$ if G is a finitely generated pro-p group and $\{G_n\}$ is an N-sequence.

(ii) If G is a uniform group with simple $\mathbb{Q}_p$-Lie algebra and $G_n = G^{p^{n-1}}$ for any natural number n, then

$$\log_2(n) + 1 - \log_2 s \leqslant \mathrm{dl}(G/G_n) \leqslant \log_2(n) + 1, \quad \text{where } G_s \subseteq [G, G].$$

The lower bound in the second part of the remark is a consequence of Shalev's result [Sh93] about powerful groups, which says if M and N are powerfully embedded in G, then $[N^{p^m}, M^{p^n}] = [N, M]^{p^{m+n}}$.

Now, we are going to find different irreducible character degrees of G/G_n. By Corollary 2.10, we know that in order to get different character degrees, we need to find different orbit sizes in $\mathrm{Irr}(L_G/p^n L_G)$. The following remark tells us when an orbit in $\mathrm{Irr}(L_G)$ is interesting for us.

Remark 3.2.

(i) In the above setting, $\ker(\Phi_\Omega) = \bigcap_{\omega \in \Omega} \ker(\omega)$.

(ii) $p^n L_G \subseteq \ker(\omega)$ if and only if $\omega(u) = \theta^{a(u)}$, where θ is a p^n-th root of unity and a is in L_G^*.

(iii) $\Phi_\Omega(1) = |\Omega|^{1/2} = [G : \mathrm{St}_G(\omega)]$.

In fact, using Remark 3.2, $G_n \subseteq \ker(\Phi_\Omega)$ if and only if Ω is a G-orbit of a character in the form $\theta^{a(u)}$, where θ is a p^{n-1}-th root of unity and a is in L_G^*. Hence $\mathrm{Irr}(L_G)$ has an element of order p^{n-1}, say ω, whose G-orbit gives us an irreducible character of G/G_n.

Lemma 3.3. *Let G be a uniform group, $\omega \in \mathrm{Irr}(L_G)$. If $\mathrm{St}_G(\omega)$ is a proper subgroup of G, then it is also a proper subgroup of $\mathrm{St}_G(\omega^p)$.*

Proof. By Lemma 2.7, $\mathrm{St}_G(\omega) = \{x \in L_G \mid \omega([x, L_G]) = 1\}$. On the other hand, one can find a p^n-th root of unity θ and $a \in L_G^*$ such that $\omega(x) = \theta^{a(x)}$. Thus $\mathrm{St}_G(\omega) = \{x \in L_G \mid a([x, L_G]) \in p^n\mathbb{Z}_p\}$ is a proper subset of L_G. Let x be an element of L_G outside of $\mathrm{St}_G(\omega)$, and s be the largest integer for which $p^s\mathbb{Z}_p$ contains $a([x, L_G])$. Hence $p^{n-1-s}a([x, L_G])$ is contained in $p^{n-1}\mathbb{Z}_p$ and not in $p^n\mathbb{Z}_p$. Therefore $p^{n-1-s}x$ is in $\mathrm{St}_G(\omega^p)$ and not in $\mathrm{St}_G(\omega)$. □

Using Remark 3.2 and Lemma 3.3, one can get the following corollary.

Corollary 3.4. *Let G be a uniform group. Then for any natural number n,*

$$\mathrm{dl}(G/G_n) \leqslant \log_2\bigl|\mathrm{cd}(G/G_n)\bigr| + 3.$$

Proof. Let s be the largest natural number for which $p^s L_G$ contains $[L_G, L_G]$. Choose $a \in L_G^*$ such that $a([L_G, L_G])$ would not be a subset of $p^{s+1}\mathbb{Z}_p$, and let $\omega(x) = \theta^{a(x)}$ where θ is a primitive p^{n-1}-th root of unity. Thus by the Lemmas 3.3 and 2.7, if $n > s - 1$,

$$\mathrm{St}_G(\omega) \subsetneq \mathrm{St}_G(\omega^p) \subsetneq \cdots \subsetneq \mathrm{St}_G\bigl(\omega^{p^{n-2-s}}\bigr) \subsetneq G.$$

Hence if $n > s - 1$, then by Remark 3.2, $n - s - 1 \leqslant |\mathrm{cd}(G/G_n)|$, and if $n \leqslant s - 1$ then G/G_n is Abelian and therefore $|\mathrm{cd}(G/G_n) = 1|$.

On the other hand, since $[G, G] \subseteq G_{s+1}$, it can easily be seen that

$$\mathrm{dl}(G/G_n) \leqslant \log_2(n) - \log_2(s + 1) + 2$$

if $n > s + 1$, and $\mathrm{dl}(G/G_n) = 1$ otherwise. So in any case, we have

$$\mathrm{dl}(G/G_n) \leqslant \log_2\bigl|\mathrm{cd}(G/G_n)\bigr| + 3. \qquad \square$$

By the above corollary, we have a good understanding about the quotients of G by the dimensional subgroups. So if one controls any normal open subgroup of G by the dimensional subgroups, we can get property (I).

We show that one has such a control if $L_G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a simple Lie algebra. It is a known result. It can be seen as a corollary of [KLGP97, Theorem III.12] and [LGM, Exercise 12.1(4)]. However, we could not find the following setting in the literature. Even Y. Barnea and R. Guralnick [BG02] showed this for $G = SL_n^1(\mathbb{Z}_p)$ for odd prime p or $n > 2$, and asked for a proof depending on powerful subgroups which also works for the remaining case. Since our proof is different and fairly short, we will write it here:

Lemma 3.5. *Let F be a non-Archimedean local field, $\mathcal{O}$ be its valuation ring, and π be a uniformizing element. If L is an $\mathcal{O}$-Lie algebra such that $L_F = L \otimes_{\mathcal{O}} F$ is a simple Lie algebra, then*

$$\sup\bigl\{\bigl|L/\mathrm{ideal}(a)\bigr| \bigm| a \in L \setminus \pi L\bigr\}$$

is finite.

Proof. (This short proof is suggested to us by the referee.) By the contrary, assume that for any i we may find $a_i \in L \setminus \pi L$ such that $|L/\mathrm{ideal}(a_i)| > i$. Since $L \setminus \pi L$ is compact, without lose of generality, we may assume that a_i converges to $a \in L \setminus \pi L$. Because of the simpleness of L_F, $L/\mathrm{ideal}(a)$ is finite. Hence $\mathrm{ideal}(a)$ contains $\pi^k L$ for some k. On the other hand, $a \equiv a_i \pmod{\pi^{k+1} L}$, for large enough i, say $i > i_0$. Thus $\pi^k L \subseteq \mathrm{ideal}(a) = \mathrm{ideal}(a_i) + \pi^{k+1} L$ for $i > i_0$. Now by induction on s, it is easy to see that $\pi^k L \subseteq \mathrm{ideal}(a_i) + \pi^s L$ for any natural number s. Therefore $\mathrm{ideal}(a_i)$ contains $\pi^k L$ for $i > i_0$, which is a contradiction by the choice of a_i's. $\square$

Lemma 3.6. *Let G be a uniform group with simple $\mathbb{Q}_p$-Lie algebra. Then there is a constant $f = f(G)$ such that, for any normal open subgroup N of G, there exists n such that $G_{n+f} \subset N \subseteq G_n$.*

Proof. Since G is a finite rank pro-p group, by Theorem 2.4, there is a characteristic subgroup W such that any $N \leqslant W$ which is a normal open subgroup of G is powerfully embedded in W. Therefore $N \cap W$ p.e. in W, for any $N \lhd_o G$. Since G is torsion free, $N \cap W$ and W are uniform, and $L_{N\cap W}$ and L_W are finite index $\mathbb{Z}_p$-Lie algebras of L_G. Hence $L_W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a simple Lie algebra. On the other hand, for any $n \in L_{N\cap W}$ and $w \in L_W$, $[n, w] = \lim_{k\to\infty} (n^{p^k}, w^{p^k})^{p^{-2k}}$ and by the result of Shalev [Sh93] which I mentioned above, $[(N \cap W)^{p^k}, W^{p^k}] = [N \cap W, W]^{p^{2k}}$. Thus for any k, $(n^{p^k}, w^{p^k})^{p^{-2k}} \in [N \cap W, W] \subseteq N \cap W$ and so $[n, w] \in L_{N\cap W}$, which means that $L_{N\cap W}$ is an ideal of L_W. Let n be the largest non-negative integer such that $L_{N\cap W} \subseteq p^n L_W$. Therefore $p^{-n} L_{N\cap W} \lhd L_W$ and $p^{-n} L_{N\cap W} \cap (L_W \setminus pL_W)$ is non-empty. Therefore by Lemma 3.5, $|L_W / p^{-n} L_{N\cap W}| \leqslant C$ where C is independent of N. So there is $c = c(W)$ such that $p^c L_W \subseteq p^{-n} L_{N\cap W} \subseteq L_W$. Thus $W^{p^{n+c}} \subseteq N \cap W \subseteq W^{p^n}$. On the other hand, $W \lhd_o G$ and so there is an integer s such that $G^{p^s} \subseteq W$. Thus $N^{p^s} = \langle n^{p^s} \mid n \in N\rangle \subseteq N \cap W \subseteq W^{p^n} \subseteq G^{p^n}$ and $G^{p^{n+c+s}} \subseteq N \subseteq G^{p^{n-s}}$ and $-n + s + (n + c + s) = c + 2s = f(G)$ just depends on G. $\square$

Lemma 3.7. *Let G be a uniform group with simple $\mathbb{Q}_p$-Lie algebra; then G has property* (I).

Proof. By Lemma 3.6, there is $f = f(G)$ such that for any normal open subgroup N of G, we can find n such that $G_{n+f} \subset N \subseteq G_n$. Thus by Lemma 3.3,

$$\begin{aligned}\mathrm{dl}(G/N) &\leqslant \mathrm{dl}(G/G_{n+f}) \leqslant \mathrm{dl}(G/G_n) + \mathrm{dl}(G_n/G_{n+f}) \leqslant \mathrm{dl}(G/G_n) + 1\\ &\leqslant \log_2\bigl|\mathrm{cd}(G/G_n)\bigr| + 4 \leqslant \log_2\bigl|\mathrm{cd}(G/N)\bigr| + 4, \quad \text{for any } f \leqslant n.\end{aligned}$$

Set $D = 4 + \mathrm{dl}(G/G_f)$. Therefore

$$\mathrm{dl}(G/N) \leqslant \log_2 \bigl|\mathrm{cd}(G/N)\bigr| + D,$$

as we wanted. □

4. Proof of Theorem A

Lemma 4.1. *Let G be a pro-p group and H be an open subgroup of it. Then G has property* (I) *if H has.*

Proof. First, we prove the lemma when H is an open normal subgroup; let N be an open normal subgroup of G. Then $N \cap H$ is an open normal subgroup of H, so

$$\mathrm{dl}(H/N \cap H) \leqslant \log_2 \bigl|\mathrm{cd}(H/N \cap H)\bigr| + D_H.$$

On the other hand, $\mathrm{dl}(G/N) \leqslant \mathrm{dl}(G/H) + \mathrm{dl}(H/N \cap H)$. Therefore

$$\mathrm{dl}(G/N) \leqslant \log_2 \bigl|\mathrm{cd}(H/N \cap H)\bigr| + D_H + \mathrm{dl}(G/H).$$

Using Theorem 2.1,

$$\bigl|\mathrm{cd}(NH/N)| \leqslant |\mathrm{cd}(G/N)\bigr| \cdot [G : H]^{3/2}.$$

Thus

$$\mathrm{dl}(G/N) \leqslant \log_2 \bigl|\mathrm{cd}(G/N)\bigr| + 3/2 \log_2 [G : H] + \mathrm{dl}(G/H) + D_H,$$

which finishes the proof in this case. For an arbitrary open subgroup, it suffices to note that any such subgroup is subnormal. □

Lemma 4.2. *Let $G_1, \ldots, G_k$ be pro-p groups with property* (I). *Then $G = G_1 \times G_2 \times \cdots \times G_k$ has property* (I).

Proof. Let N be an open normal subgroup of G. Before going to the proof, it is worth mentioning a few general remarks:

Remark 4.3.

(i) Since G/N has a faithful fully reducible representation,

$$N = \bigcap_{\substack{\rho \in \mathrm{Irr}(G) \\ N \subseteq \ker(\rho)}} \ker(\rho).$$

(ii) $\rho \in \mathrm{Irr}(G)$ if and only if $\rho = \rho_1 \otimes \cdots \otimes \rho_k$ where $\rho_i \in \mathrm{Irr}(G_i)$.
(iii) $\bigoplus_{i=1}^k \ker(\rho_i) \subseteq \ker(\rho_1 \otimes \cdots \otimes \rho_k) \subseteq \bigoplus_{i=1}^k Z(\rho_i)$.

Using three parts of the above remark,

$$\bigoplus_{i=1}^k N_i^l \subseteq N \subseteq \bigoplus_{i=1}^k N_i^u, \quad \text{where}$$
$$N_i^l = \bigcap_{\rho_i \in A_i} \ker(\rho_i), \qquad N_i^u = \bigcap_{\rho_i \in A_i} Z(\rho_i), \quad \text{and}$$
$$A_i = \bigl\{ v_i \in \mathrm{Irr}(G_i) \bigm| \exists v_j \in \mathrm{Irr}(G_j) \text{ for any } 1 \leqslant j \leqslant k \text{ and } j \neq i \text{ such that } N \subseteq \ker(v_1 \otimes \cdots \otimes v_k) \bigr\}.$$

Clearly N_i^u / N_i^l is an Abelian group. Therefore

$$\mathrm{dl}(G/N) \leqslant \mathrm{dl}\bigl(G/N_i^l\bigr) \leqslant \mathrm{dl}\bigl(G/N_i^u\bigr) + 1 = \max_{1\leqslant i\leqslant k} \bigl(\mathrm{dl}\bigl(G_i/N_i^u\bigr)\bigr) + 1.$$

On the other hand G_i has property (I) for any $1 \leqslant i \leqslant k$. Thus

$$\begin{aligned}
\mathrm{dl}(G/N) &\leqslant \max_{1\leqslant i\leqslant k} \bigl(\log_2 \bigl|\mathrm{cd}\bigl(G_i/N_i^u\bigr)\bigr| + D_i\bigr) + 1 \\
&\leqslant \log_2 \left| \mathrm{cd}\left(G/\bigoplus_{1\leqslant i\leqslant k} N_i^u \right) \right| + 1 + \max_{1\leqslant i\leqslant k} \{D_i\} \\
&\leqslant \log_2 \bigl|\mathrm{cd}(G/N)\bigr| + D. \qquad \square
\end{aligned}$$

Lemma 4.4. *Let G be a uniform group with semisimple $\mathbb{Q}_p$-Lie algebra. Then G has property* (I).

Proof. By our assumption $\mathcal{L} = L_G \otimes_{\mathbb{Z}_p} \mathbb{Q}_P$ is semisimple and L_G is powerful. Therefore $\mathcal{L} = \mathcal{L}_1 \oplus \cdots \oplus \mathcal{L}_k$ where $\mathcal{L}_i$'s are simple $\mathbb{Q}_p$-Lie algebra. Thus certainly $L_i = p^2(L_G \cap \mathcal{L}_i)$ is a powerful Lie subalgebra of L_G and also $L_1 \oplus \cdots \oplus L_k$ is a finite index additive subgroup of L_G. By Baker–Campbell–Hausdorff formula, we get an open subgroup of G in the form $G_1 \times \cdots \times G_k$ where G_i is a uniform group with L_i as its $\mathbb{Z}_p$-Lie algebra. By Lemma 3.7, G_i has property (I), for any $1 \leqslant i \leqslant k$. So by Lemma 4.2, $G_1 \times \cdots \times G_k$ has property (I), and therefore by Lemma 4.1, G has property (I). $\square$

Lemma 4.5. *Let G be a uniform group. Then G has property* (I).

Proof. Set $\mathcal{L} = L_G \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $r = \mathrm{Rad}(\mathcal{L}) \cap L_G$, where $\mathrm{Rad}(\mathcal{L})$ is the radical of the Lie algebra $\mathcal{L}$. Clearly r is an ideal of L_G and L_G/r is torsion free. Therefore by Theorem 2.3, G has an open normal uniform subgroup R such that $L_R = r$ and $L_{G/R} \simeq L_G/r$. Thus $L_{G/R} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \mathcal{L}/\mathrm{Rad}(\mathcal{L})$ is semisimple. So G/R satisfies conditions of Lemma 4.4 and we conclude that it has property (I). On the other hand, by Theorem 2.5, R is solvable. Over all we can see that for any open normal subgroup N of G:

$$\begin{aligned}\mathrm{dl}(G/N) &\leqslant \mathrm{dl}(RN/N) + \mathrm{dl}(G/RN) \leqslant \mathrm{dl}(R) + \log_2\bigl|\mathrm{cd}(G/RN)\bigr| + D_{G/R}\\ &\leqslant \log_2\bigl|\mathrm{cd}(G/N)\bigr| + D_{G/R} + \mathrm{dl}(R),\end{aligned}$$

as we claimed. □

Proof of Theorem A. By Lemmas 4.1 and 4.5, and the fact that any finite-rank pro-p group has an open uniform group, we can conclude the result. □

5. Proof of Theorem B

In this chapter, we are going to prove that the first congruence subgroup of a classical Chevalley groups over $\mathbb{F}_p[\![t]\!]$ in most of the cases has property (I). In this section p is always a prime number, and we will use the following embedding (†) of classical Chevalley groups and their Lie algebras:

(A_l) $\{g \in \mathbb{GL}_{l+1} \mid \det(g) = 1\}$ and its Lie algebra is $\{x \in \mathfrak{gl}_{l+1} \mid \mathrm{tr}(x) = 0\}$.
(B_l) $\{g \in \mathbb{GL}_{2l+1} \mid gsg^t = s\}$ and its Lie algebra is $\{x \in \mathfrak{gl}_{2l+1} \mid xs = -sx^t\}$, where

$$s = \begin{bmatrix} 1 & 0 & 0\\ 0 & 0 & I_l\\ 0 & I_l & 0\end{bmatrix}.$$

(C_l) $\{g \in \mathbb{GL}_{2l} \mid gsg^t = s\}$ and its Lie algebra is $\{x \in \mathfrak{gl}_{2l} \mid xs = -sx^t\}$, where

$$s = \begin{bmatrix} 0 & I_l\\ -I_l & 0\end{bmatrix}.$$

(D_l) $\{g \in \mathbb{GL}_{2l} \mid gsg^t = s\}$ and its Lie algebra is $\{x \in \mathfrak{gl}_{2l} \mid xs = -sx^t\}$, where

$$s = \begin{bmatrix} 0 & I_l\\ I_l & 0\end{bmatrix}.$$

Let us set a few notations. Let $\mathcal{O} = \mathbb{F}_p[\![t]\!]$ and $G_k = \ker(\mathbb{G}(\mathcal{O}) \to \mathbb{G}(\mathcal{O}/(t^k)))$ be the kth congruence subgroup. $G = G_1$ acts on:

- G_n/G_{2n} by conjugation, i.e., ${}^g hG_{2n} = ghg^{-1}G_{2n}$;
- $\mathrm{Irr}(G_n/G_{2n}) \equiv \mathrm{Hom}(G_n/G_{2n}, \mathbb{F}_p)$ by the action induced by conjugation, i.e., ${}^g\nu(x) = \nu({}^{g^{-1}}x)$;
- $\mathfrak{g}(\mathcal{O}) = \mathrm{Lie}(\mathbb{G})(\mathcal{O})$ by adjoint action $\mathrm{Ad}(g)$;
- $\mathfrak{g}(\mathcal{O})/t^n\mathfrak{g}(\mathcal{O})$ by the action induced by the adjoint action (we will denote it again by $\mathrm{Ad}(g)$); and

- $\mathfrak{g}(\mathcal{O})^* = \mathrm{Hom}_{\mathcal{O}}(\mathfrak{g}(\mathcal{O}), \mathcal{O})$ by the action induced by the adjoint action, i.e., for any $f \in \mathfrak{g}(\mathcal{O})^*$ and $x \in \mathfrak{g}(\mathcal{O})$, $\mathrm{Ad}(g)^*(f)(x) = f(\mathrm{Ad}(g^{-1})(x))$.

Now, let us recall a few well-known or easy statements as a remark.

Remark 5.1.

(i) For any positive numbers m and n, $[G_m, G_n] \subseteq G_{m+n}$ and $G_n^p \subseteq G_{np}$.
(ii) If $1 + g_k t^k + g_{k+1} t^{k+1} + \cdots \in G_k$, then $g_i \in \mathfrak{g}(\mathbb{F}_p)$ for $k \leqslant i \leqslant 2k-1$.
(iii) The Killing form of $\mathfrak{g}(\mathbb{F}_p)$ is non-degenerated if $p > 2, 3$ does not divide $n+1$ when $\mathfrak{g}$ is of type A_n or C_n; $2n-1$ when $\mathfrak{g}$ is of type B_n or $n-1$ when $\mathfrak{g}$ is of type D_n [Se67, p. 47].
(iv) $\bigoplus_{n=1}^{\infty} G_n/G_{n+1} \simeq \mathfrak{g}(\mathbb{F}_p) \otimes_{\mathbb{F}_p} t\mathbb{F}_p[t]$ as graded Lie algebras.
(v) $G_n/G_{2n} \simeq \mathfrak{g}(\mathcal{O})/t^n \mathfrak{g}(\mathcal{O})$ as G-modules.
(vi) $\mathrm{Irr}(G_n/G_{2n}) \simeq \mathrm{Hom}_{\mathbb{F}_p}(\mathfrak{g}(\mathcal{O})/t^n \mathfrak{g}(\mathcal{O}), \mathbb{F}_p)$ as G-modules.
(vii) $\mathfrak{g}(\mathcal{O}) \simeq \mathfrak{g}(\mathcal{O})^*$ as G-modules, whenever $\mathfrak{g}(\mathbb{F}_p)$ is a simple Lie algebra.

Quick look at some of the items. Items (i), (iii), and (iv) are well-known. Item (ii) can be shown directly from the definition of Lie algebra of an affine algebraic group. Using (ii), one can get the following map:

$$\left(1 + g_n t^n + g_{n+1} t^{n+1} + \cdots\right) G_{2n} \mapsto \left(g_n + \cdots + g_{2n-1} t^{n-1}\right) + t^n \mathfrak{g}(\mathcal{O})$$

between G_n/G_{2n} and $\mathfrak{g}(\mathcal{O})/t^n \mathfrak{g}(\mathcal{O})$, which is clearly a G-module isomorphism. Item (vi) is an easy consequence of (v). Proof of item (vii) is based on the fact that Killing form of $\mathfrak{g}(\mathbb{F}_p)$ is non-degenerated. Let k be the Killing form of $\mathfrak{g}(\mathbb{F}_p)$. For any $x \in \mathfrak{g}(\mathbb{F}_p)$, let x^* be an element of $\mathfrak{g}(\mathbb{F}_p)^*$ defined by $x^*(y) = k(x, y)$. Since k is non-degenerated, the map which sends x to x^* is a bijective map from $\mathfrak{g}(\mathbb{F}_p)$ to $\mathfrak{g}(\mathbb{F}_p)^*$. On the other hand, $\mathfrak{g}(\mathcal{O}) \simeq \mathfrak{g}(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathcal{O}$ and $\mathfrak{g}(\mathcal{O})^* \simeq \mathfrak{g}(\mathbb{F}_p)^* \otimes_{\mathbb{F}_p} \mathcal{O}$, so * can be extended to a map from $\mathfrak{g}(\mathcal{O})$ to $\mathfrak{g}(\mathcal{O})^*$. And because the Killing form is invariant under the action of G, * is a G-module isomorphism. □

Lemma 5.2. *Let $\mathfrak{g}$ be a classical Chevalley Lie algebra which is embedded in $\mathfrak{gl}_k(\mathbb{F}_p)$ according to* (†). *Then there is an element $x \in \mathfrak{g}(\mathbb{F}_p)$ such that x has different eigenvalues, if either $\mathfrak{g}$ is of type A and $p \nmid \mathrm{rank}(\mathfrak{g}) + 1$ or $\mathfrak{g}$ is of type B, C, or D and p is an odd prime number.*

Proof. Let us start with setting a notation. To any monic polynomial of degree n, say $q(T) = T^n + a_{n-1} T^{n-1} + \cdots + a_0$, we relate the n by n matrix

$$A_q = \begin{bmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & \cdots & 0 & -a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

From elementary linear algebra, the characteristic polynomial of A_q is equal to q.

Now we provide the x claimed in the lemma for each type separately.

Type A_n: $q(T)=T^{n+1}-1$ has different roots since $p\nmid n+1$, and so $x=A_q$ provides our claim.

Type B_n: For this type we need a polynomial $q(T)$ which has different non-zero roots and does not have a common root with $q(-T)$.

We know that $\mathbb{F}_{p^n}^*$ the multiplicative group of the finite field $\mathbb{F}_{p^n}$ is a cyclic group. Let α be a generator of $\mathbb{F}_{p^n}^*$. It is a well-known fact that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group generated by the Frobenius map $a\mapsto a^p$. Hence $q(T)=(T-\alpha)\times(T-\alpha^p)(T-\alpha^{p^2})\cdots(T-\alpha^{p^{n-1}})$ is a polynomial with coefficients in $\mathbb{F}_p$. It is easy to see that $q(T)$ has the properties we are interested in. Now,

$$x=\begin{bmatrix} 0 & 0_{1\times n} & 0_{1\times n}\\ 0_{n\times 1} & A_q & 0_{n\times n}\\ 0_{n\times 1} & 0_{n\times n} & -A_q^t \end{bmatrix}$$

provides the claim of the lemma.

Types C_n *or* D_n: with

$$x=\begin{bmatrix} A_q & 0\\ 0 & -A_q^t \end{bmatrix}$$

and q the same as for type B, we have the claim. □

Corollary 5.3. *Let $\mathbb{G}$ be a classical Chevalley group of rank n, which is embedded as (†) in $\mathbb{GL}_k$. If $\mathfrak{g}(\mathbb{F}_p)$ is a simple Lie algebra, then there is $x\in\mathfrak{g}(\mathbb{F}_p)$ such that $C_{\mathbb{G}}(x)=\{g\in\mathbb{G}\mid \mathrm{Ad}(g)(x)=x\}$ is an $\mathbb{F}_p$-torus which splits over $\mathbb{F}_{p^n}$, and so $k(y_1,y_2)=0$ for any $y_1,y_2\in C_{\mathfrak{g}}(x)=\{y\in\mathfrak{g}\mid [y,x]=0\}$ where k is the Killing form of $\mathfrak{g}$.*

Proof. Let x be the regular element provided by Lemma 5.2. Then clearly $C_{\mathbb{G}}(x)$ is defined over $\mathbb{F}_p$ (see [Bo97, p. 130]), and x is diagonalizable over $\mathbb{F}_{p^n}$. Since x has different eigenvalues, $C_{M_k(R)}(\bar{x})=\{g\in M_k(R)\mid \mathrm{Ad}(g)(\bar{x})=\bar{x}\}$ is the set of diagonal elements over R, where R is any $\mathbb{F}_{p^n}$-algebra, and $\bar{x}$ is a conjugate of x which is diagonal. Thus $C_{\mathfrak{g}}(x)$ is a Cartan subalgebra of $\mathfrak{g}$. On the other hand, since x is semisimple, $\mathrm{Lie}(C_{\mathbb{G}}(x))=C_{\mathfrak{g}}(x)$ (see [Bo97, p. 130]). Hence $C_{\mathbb{G}}(x)$ contains a maximal torus. Therefore $C_{\mathbb{G}}(x)$ is a maximal torus since in a reductive group $C_{\mathbb{G}}(\mathbb{T})=(\mathbb{T})$ where $\mathbb{T}$ is a maximal torus. Also by the previous argument, it is $\mathbb{F}_{p^n}$-isomorphic to a subgroup of $\mathbb{D}_k$, which means it is $\mathbb{F}_{p^n}$-split.

In order to see the second part, it is enough to write the root system of $\mathfrak{g}$ with respect to $C_{\mathfrak{g}}(x)$ and note that if α is a root, so is $-\alpha$. □

Now let us recall that there is a quite generalization of Hensel's lemma for schemes which can be found in the work of Nèron [Ne64]. We need a very easy case of it which can be proved with the same method as the Hensel's lemma itself.

Corollary 5.4. *If X is a smooth affine $\mathbb{F}_q$-variety, then the congruence map from $X(\mathbb{F}_q[\![t]\!])$ to $X(\mathbb{F}_q[\![t]\!]/(t^k))$ is surjective.*

Before going to the proof of Theorem B in the general case, we will show it for quotients of G by the congruence subgroups G_n's.

Theorem 5.5. *For any natural number n, $\mathrm{dl}(G/G_n) \leqslant \log_2(|\mathrm{cd}(G/G_n)|) + 3$, if $p > 2, 3$ does not divide $l+1$ when $\mathbb{G}$ is of type A_l or C_l; $2l-1$ when $\mathbb{G}$ is of type B_l or $l-1$ when $\mathbb{G}$ is of type D_l.*

Proof. Lemma 5.3 provides us $x \in \mathfrak{g}(\mathbb{F}_p)$ for which $C_{\mathbb{G}}(x)$ is an $\mathbb{F}_p$-torus. Let $\bar{x}$ be an $\mathbb{F}_p$-linear map from $\mathfrak{g}(\mathcal{O})/t^n\mathfrak{g}(\mathcal{O})$ to $\mathbb{F}_p$ defined by

$$\bar{x}\big(\big(g_0 + g_1 t^1 + \cdots + g_{n-1}t^{n-1}\big) + t^n \mathfrak{g}(\mathcal{O})\big) = \sum_{k=0}^{n-1} x^*(g_k).$$

By Remark 5.1(vi), we can get $\nu \in \mathrm{Irr}(G_n/G_{2n})$ which is corresponded to $\bar{x}$.

First Step. ${}^g\nu = \nu$ *if and only if* $\mathrm{Ad}(g)^*(x^*) \equiv x^* \pmod{t^n}$.

Proof. By Remark 5.1(vi) and the way we chose ν, ${}^g\nu = \nu$ if and only if $\mathrm{Ad}(g)^*(\bar{x}) = \bar{x}$. Now let $\mathrm{Ad}(g)(a) = T_g^0(a) + T_g^1(a)t + \cdots$ for $a \in \mathfrak{g}(\mathbb{F}_p)$. If $g \in G$, then $T_g^0 = \mathrm{id}$ and $T_g^k(\mathfrak{g}(\mathbb{F}_p)) \subseteq \mathfrak{g}(\mathbb{F}_p)$ and all of them are $\mathbb{F}_p$-linear maps. Thus

$$\begin{aligned}
\mathrm{Ad}(g)^*(\bar{x})\left(\overline{\sum_{i=0}^{n-1} y_i t^i}\right) &= \bar{x}\left(\mathrm{Ad}\big(g^{-1}\big)\left(\overline{\sum_{i=0}^{n-1} y_i t^i}\right)\right) = \bar{x}\left(\overline{\sum_{i=0}^{n-1} \mathrm{Ad}\big(g^{-1}\big)(y_i)t^i}\right) \\
&= \bar{x}\left(\overline{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} T_{g^{-1}}^j(y_i)t^{i+j}}\right) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-i-1} x^*\big(T_{g^{-1}}^j(y_i)\big) \\
&= \sum_{i=0}^{n-1} x^*(y_i) + \sum_{i=0}^{n-1}\sum_{j=1}^{n-i-1} x^*\big(T_{g^{-1}}^j(y_i)\big) \\
&= \bar{x}\left(\overline{\sum_{i=0}^{n-1} y_i t^i}\right) + \sum_{i=0}^{n-1}\sum_{j=1}^{n-i-1} x^*\big(T_{g^{-1}}^j(y_i)\big)
\end{aligned}$$

where $\bar{\ }: \mathfrak{g}(\mathcal{O}) \to \mathfrak{g}(\mathcal{O})/t^n\mathfrak{g}(\mathcal{O})$ is the natural epimorphism. Hence overall we get that $\mathrm{Ad}(g)^*(\bar{x}) = \bar{x}$ if and only if, for any $y_0, \ldots, y_{n-1}$ in $\mathfrak{g}(\mathbb{F}_p)$,

$$\sum_{i=0}^{n-1}\sum_{j=1}^{n-i-1} x^*\big(T_{g^{-1}}^j(y_i)\big) = 0.$$

Now, for any i, set $y_0 = \cdots = y_{i-1} = y_{i+1} = \cdots = y_{n-1} = 0$ and $y_i = y$, so

$$\sum_{j=1}^{n-i-1} x^*\bigl(T_{g^{-1}}^{j}(y)\bigr) = \sum_{j=1}^{n-i-1} {T_{g^{-1}}^{j}}^*(x^*)(y) = 0.$$

Therefore $\sum_{j=1}^{i} {T_{g^{-1}}^{j}}^*(x^*) = 0$, for any $0 \leqslant i \leqslant n-1$, and so ${T_{g^{-1}}^{j}}^*(x^*) = 0$, for any $0 \leqslant i \leqslant n-1$. On the other hand,

$$\begin{aligned}\mathrm{Ad}(g)^*(x^*)(y) &= x^*\bigl(\mathrm{Ad}\bigl(g^{-1}\bigr)y\bigr) = x^*\left(\sum_{i=0}^{\infty} T_{g^{-1}}^{i}(y)t^i\right) = \sum_{i=0}^{\infty} x^*\bigl(T_{g^{-1}}^{i}(y)\bigr)t^i \\ &= x^*(y) + \sum_{i=1}^{\infty} x^*\bigl(T_{g^{-1}}^{i}(y)\bigr)t^i = x^*(y) + \sum_{i=1}^{\infty} {T_{g^{-1}}^{i}}^*(x^*)(y)t^i\end{aligned}$$

which completes the proof of the first step. □

Second Step. $I_{G/G_{2n}}(\nu) = C_G(x)G_n/G_{2n}$.

Proof.

$$\begin{aligned}I_{G/G_{2n}}(\nu) &= \bigl\{gG_{2n} \in G/G_{2n} \mid {}^g\nu = \nu\bigr\} \\ &= \bigl\{gG_{2n} \in G/G_{2n} \mid \mathrm{Ad}(g)^*(x^*) \equiv x^* \pmod{t^n}\bigr\} \quad \text{(First Step)} \\ &= \bigl\{gG_{2n} \in G/G_{2n} \mid \mathrm{Ad}(g)(x) \equiv x \pmod{t^n}\bigr\} \quad \text{(Remark 5.1(vii))} \\ &= C_G(x)G_n/G_{2n} \quad \text{(by Corollaries 5.4 and 5.3).} \qquad \square\end{aligned}$$

Third Step. *ν can be extended to $I_{G/G_{2n}}(\nu)$.*

Proof. It is clear that $(C_G(x) \cap G_n)G_{2n}/G_{2n} \subseteq \ker(\nu)$, using the second part of Corollary 5.3. Hence $\psi(agG_{2n}) = \nu(gG_{2n})$ is a well-defined map where a and g are any elements of $A = C_G(x)$ and G_n, respectively. And clearly ψ is a homomorphism, which shows the claim. □

Final Step. By Clifford's correspondence, $\psi^{G/G_{2n}}$ is an irreducible character of G/G_{2n} and $\psi^{G/G_{2n}}(1) = [G : AG_n]$ since $\psi(1) = 1$. Hence $\{[G : AG_k] \mid 1 \leqslant k \leqslant n\} \subseteq \mathrm{cd}(G/G_{2n})$. On the other hand, $AG_{k+1} \subsetneq AG_k$ since $\mathfrak{g}(\mathbb{F}_p)$ is centerless. Therefore $|\mathrm{cd}(G/G_{2n})| \geqslant n$. Thus by Remarks 5.1 and 3.1,

$$\mathrm{dl}(G/G_n) \leqslant \log_2(n) + 1 < \log_2\lfloor n/2\rfloor + 3 \leqslant \log_2\bigl|\mathrm{cd}(G/G_n)\bigr| + 3. \qquad \square$$

Proof of Theorem B. Let N be an open normal subgroup of G, then by Theorem 2.6 and Remark 5.1(iv), $G_{n+f} \subseteq N \subseteq G_n$, for some n, where $f = f(G)$ just depends on G. Therefore for $n \geqslant f$,

$$\begin{aligned}\mathrm{dl}(G/N) &\leqslant \mathrm{dl}(G/G_{n+f}) \leqslant \mathrm{dl}(G/G_n) + 1\\ &\leqslant \log_2\bigl|\mathrm{cd}(G/G_n)\bigr| + 4 \quad \text{(by Theorem 5.5)}\\ &\leqslant \log_2\bigl|\mathrm{cd}(G/N)\bigr| + 4.\end{aligned}$$

Hence for any normal open subgroup N of G,

$$\mathrm{dl}(G/N) \leqslant \log_2\bigl|\mathrm{cd}(G/N)\bigr| + \log_2(f) + 5. \qquad \square$$

Acknowledgments

I thank E. Zelmanov for introducing me pro-p groups, A. Lubotzky for letting me know about character growth of pro-p groups and his continuous encouragement, and G. Margulis for all his helpful advices. I also thank the referee for very useful remarks, without that length of this paper would have been twice!

References

[Be76] T.R. Berger, Characters and derived length in groups of odd order, J. Algebra 39 (1976) 199–207.
[BG02] Y. Barnea, R. Guralnick, Subgroup growth in some pro-p groups, Proc. Amer. Math. Soc. 130 (2002) 653–659.
[Bo97] A. Borel, Linear Algebraic Groups, 2nd ed., Springer-Verlag, New York, 1997.
[DSMS99] J. Dixon, M.Du Sautoy, A. Mann, D. Segal, Analytic Pro-p Groups, Cambridge University Press, Cambridge, 1999.
[Gl85] D. Gluck, Bounding the number of character degrees of a solvable group, J. London Math. Soc. 31 (2) (1985) 457–462.
[Ho77] R. Howe, Kirillov theory for compact p-adic groups, Pacific J. Math. 73 (1977) 365–381.
[Hu98] B. Huppert, Character Theory of Finite Groups, de Gruyter, Berlin, 1998.
[Is94] I.M. Isaacs, Character Theory of Finite Groups, Dover, New York, 1994.
[JZ04] A. Jaikin-Zapirain, Zeta function of representations of compact p-adic analytic groups, 2004, preprint.
[K99(I)] T.M. Keller, Orbit sizes and character degrees, Pacific J. Math. 187 (1999) 317–332.
[K99(II)] T.M. Keller, Orbit sizes and character degrees II, J. Reine Angew. Math. 516 (1999) 27–114.
[K02] T.M. Keller, Orbit sizes and character degrees III, J. Reine Angew. Math. 545 (2002) 1–17.
[KLGP97] G. Klass, C.R. Leedham-Green, W. Plesken, Linear Pro-p Groups of Finite Width, Springer-Verlag, Berlin, 1997.
[LGM] C.R. Leedham-Green, S. McKay, The Structure of Groups of Prime Power Order, Oxford University Press, New York, 2002.
[Mo03] A. Moretó, Derived length and character degrees of solvable groups, Proc. Amer. Math. Soc. 132 (6) (2003) 1599–1604.
[Ne64] A. Nèron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. Inst. Hautes Études Sci. 21 (1964) 5–128.
[Se67] G.B. Seligman, Modular Lie Algebras, Springer-Verlag, Berlin, 1967.
[Sh93] A. Shalev, Polynomial identities in graded group rings, restricted algebras and p-adic analytic groups, Trans. Amer. Math. Soc. 337 (1993) 451–462.
[Sh95] A. Shalev, Finite p-groups, in: B. Hartley, et al. (Eds.), Finite and Locally Finite Groups, Istanbul, Turkey, 1994, NATO ASI Ser., vol. 471, Kluwer Academic, Dordrecht, 1995, pp. 401–450.
[Sl89] M.C. Slattery, Character degrees and derived length in p-groups, Glasgow Math. J. 30 (1989) 221–230.

Further reading

N. Jacobson, Lie Algebras, Dover, New York, 1979.