ISRAEL JOURNAL OF MATHEMATICS 85 (1994), 307–337

ON SOME Λ-ANALYTIC PRO-p GROUPS

BY

ALEXANDER LUBOTZKY AND ANER SHALEV

Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: alexlub@vms.huji.ac.il and shalev@math.huji.ac.il

ABSTRACT

This paper is devoted to the first steps towards a systematic study of pro-p groups which are analytic over a commutative Noetherian local pro-p ring Λ, e.g. $\Lambda = \mathbb{F}_p[[t]]$. We restrict our attention to Λ-standard groups, which are pro-p groups arising from a formal group defined over Λ. Under some additional assumptions we show that these groups are of 'intermediate growth' in various senses, strictly between p-adic analytic pro-p groups and free pro-p groups. This suggests a refinement of Lazard's theory which stresses the dichotomy between p-adic analytic pro-p groups and all the others. In the course of the discussion we answer a question posed in [LM1], and settle two conjectures from [Bo].

1. Introduction

Let (Λ, M) be a complete commutative Noetherian local ring whose residue field Λ/M is finite, say $\Lambda/M = \mathbb{F}_q$ where $q = p^e$ (p a prime). The goal of this paper is to present various properties of pro-p groups which are analytic over Λ. Our initial interest was in the case $\Lambda = \mathbb{F}_p[[t]]$. In this case the field of fractions $K = \mathbb{F}_p((t))$ is ultrametric and so basic results on analytic groups over K can be found in Serre [S] and Bourbaki [B]. In particular it is shown in [S] that such groups have open subgroups, called standard, which arise from a formal group defined over $\mathbb{F}_p[[t]]$. This reduces, to some extent, the study of analytic groups over K to the investigation of the standard ones. While carrying out this

Received July 8, 1992 and in revised form June 29, 1993

investigation we realized that almost all our results can be extended to standard groups over general rings Λ. Our results do not require a complete theory of Λ-manifolds and analytic groups over Λ, but they call for the development of such a theory.

There are several motivations for looking at Λ-analytic groups:

1. The special case $\Lambda = \mathbb{Z}_p$ (the ring of the p-adic integers) whose study was initiated by Lazard [La] led to a beautiful theory which turned to have many applications to abstract groups; see [DDMS] and the references therein. In particular, Lazard's solution of Hilbert's 5th problem for p-adic Lie groups led to a characterization of finitely generated linear groups in characteristic zero [Lu2]. It is hoped that a better understanding of Λ-analytic groups, especially in the case $\Lambda = \mathbb{F}_p[[t]]$, would lead to similar applications in positive characteristic.

2. Understanding Λ-analytic groups seems an essential step in developing a reasonable structure theory of pro-p groups. We mention briefly two particular aspects of such a theory. The first is the study of certain growth functions associated with a finitely generated pro-p group G, such as its subgroup growth (see [Se],[LM2],[Sh],[SS]). It is still not known which types of growth a pro-p group can have, and the analysis of Λ-analytic groups is relevant in this context. The second aspect is related to presentations of pro-p groups, and to the derivation of the Golod–Shafarevich inequality for certain types of groups (see [K],[Lu1],[W],[WZ]). In the long run we also aim at classification theorems for pro-p groups, in which the Λ-analytic groups would form an important building block.

3. In [M] and [Bo] Mazur and Boston study deformation spaces of p-adic representations of some pro-p Galois groups. Such a deformation space defines a single representation ρ of G into $\mathrm{GL}_n(\Lambda)$ for a suitable local ring Λ of the type considered here. The image of G is a closed subgroup of $\mathrm{GL}_n(\Lambda)$ (which is Λ-analytic), and thus information on closed subgroups of Λ-analytic groups is relevant in the study of the representation ρ.

Let us now outline the content of this paper.

In section 2 we define Λ-standard groups and study their basic properties. The basic examples are the congruence subgroups $\mathrm{Ker}(\mathrm{SL}_n(\Lambda) \longrightarrow \mathrm{SL}_n(\Lambda/M))$. The main result of section 2 states that, unless Λ is a finitely generated $\mathbb{Z}_p$-module, a Λ-standard group is *not* p-adic analytic.

To every Λ-standard group we associate a Lie algebra, which is our main tool in most of the group-theoretic applications. Our Lie algebra is not the classical Lie algebra associated with the group, but rather a graded version of it. This graded version was defined (in the ultrametric case) in [S],[B] and [La], but it seems that it is put to use here for the first time.

In section 3 we restrict ourselves to an important subclass of standard groups, the class of Λ-perfect groups. While Λ-standard groups may not be finitely generated, the Λ-perfect ones are. We compute the lower central series of a Λ-perfect group G and derive some abstract group-theoretic consequences. A Hilbert–Poincaré series is then associated to G and we relate it to the Hilbert–Poincaré series of the ring Λ, thus deducing the rationality of the first from that of the latter.

Section 4, which contains the main results of this paper, deals with growth functions associated with a Λ-perfect group G. The group-theoretic questions are reduced to Lie-theoretic ones, which are then solved using methods of a combinatorial flavour. The results illustrate that, in the non p-adic analytic case, the Λ-perfect groups form 'medium-sized' pro-p groups – not 'as small' as $\mathbb{Z}_p$-analytic groups, and not 'as large' as (non-abelian) free pro-p groups. This leads to a refinement of the work of Lazard, who stressed the dichotomy between $\mathbb{Z}_p$-analytic pro-p groups and all the rest.

For example, let $a_n = a_n(G)$ denote the number of open subgroups of index n in a pro-p group G. If G is a finitely generated (non-abelian) free pro-p group, then $\{a_n\}$ grows exponentially with n [I]. On the other hand $\{a_n\}$ grows (at most) polynomially for p-adic analytic groups (and this property actually characterizes them [LM2]). In [Sh] it is shown that, if G is not p-adic analytic, then $a_n > n^{c\log_p n}$ for infinitely many values of n, where c is any constant less than $1/8$.

We show in Theorem 4.4 that any Λ-perfect group satisfies $a_n < n^{c\log_p n}$ for all n, where c is a fixed constant (depending on G and Λ). We see that, in a way, Λ-perfect groups have minimal subgroup growth among the non p-adic analytic groups.

A similar phenomenon occurs with respect to another growth function, defined by $g_n = g_n(G) = \max\{d(H) \mid H \subseteq_o G, (G\colon H) = n\}$, where $d(H)$ denotes the (minimal) number of generators of H (as a topological group). Here $\{g_n\}$ is bounded for p-adic analytic groups, grows logarithmically for Λ-perfect groups, and grows linearly for free pro-p groups.

We also study the **lower rank** of a pro-p group G, defined by

$$\liminf\{d(H) \mid H \subseteq_o G\},$$

and show that it is finite in every Λ-perfect group which is defined over the prime subring of Λ. In [LM1] it is asked whether the finiteness of the lower rank already implies that the group is p-adic analytic. Since Λ-perfect groups are usually not p-adic analytic, a negative answer follows at once.

In section 5 we relate presentations of some arithmetic groups Γ over global rings such as $\mathbb{F}_q[t]$ to presentations of some $\mathbb{F}_q[[t]]$-analytic groups G. We use it on the one hand to show that some of these groups G are finitely presented. On the other hand we show, implementing growth results from section 3, that in the Λ-perfect case G satisfies the Golod–Shafarevich inequality, and use this to derive a related inequality for the given arithmetic group Γ. This generalizes results of [Lu1] from characteristic zero to characteristic p.

The last section deals with two conjectures of Boston, made in [Bo]. The first states that a certain pro-p Galois group H does not have a faithful representation into $\mathrm{GL}_2(\Lambda)$ for any Λ. The second asserts that the rate of growth of the number of generators of open subgroups is 'moderate' for closed subgroups of $\mathrm{GL}_2(\Lambda)$. We show that the second conjecture does not hold for arbitrary closed subgroups, though an essentially sharper bound holds for open subgroups. However, applying results of Romanovskii [R] and Zubkov [Zu], we confirm the first conjecture of Boston.

Finally, we would like to draw attention to a number of problems in this area which, to our mind, are of fundamental importance.

1. Various necessary conditions for a pro-p group to have the structure of a Λ-perfect group are given here; but can we find conditions which are also sufficient? namely, can we obtain an abstract characterization of Λ-perfect pro-p groups (or of more general groups with analytic structure over Λ)?

We note that the so-called Nottingham group, namely, the group of normalized automorphisms of $\mathbb{F}_p[[t]]$, shares many properties with $\mathbb{F}_p[[t]]$-perfect groups. For example, it has finite lower rank, and its subgroup growth is of the type $n^{c\log n}$. However, it is easy to see that the Nottingham group is not $\mathbb{F}_p[[t]]$-perfect (see section 3); moreover, since this group is not linear over any field, it is probably not analytic over $\mathbb{F}_p[[t]]$. For these, and other properties of the Nottingham group, see [LGSW].

2. It would be interesting to know whether Λ-standard (or Λ-perfect) groups are always linear. It is not difficult to verify that, if the associated Lie algebra of the group G has trivial center, then the adjoint representation of G on its Lie algebra is faithful, and so the group is linear. But, as in the p-adic case, it may well be that this condition on the Lie algebra is not essential.

3. For various purposes it is important to find out which pro-p groups can be obtained as closed subgroups of Λ-perfect groups. We conjecture here that (non-abelian) free pro-p groups cannot be obtained in this way. This question is related to the notion of pro-p identities in pro-p groups. See [Zu] and section 3 for more details.

We would like to thank the referee for his detailed and helpful comments on an earlier version of this manuscript.

Notation: This is rather standard. For topological groups H, G we write $H \subseteq_c G$ ($H \subseteq_o G$) if H is a closed (open) subgroup of G. Group commutators are denoted by $(x,y) = x^{-1}y^{-1}xy$, to be distinguished from Lie products $[x,y]$. G' stands for the commutator subgroup (the derived subalgebra) of a group (a Lie algebra) G. If G is a topological group, then G' is understood to be closed. For a pro-p group G, $\gamma_n = \gamma_n(G)$ denote its (closed) lower central series, and G^p is the (closed) subgroup generated by all pth powers in G. $D_n = D_n(G)$ is the nth dimension subgroup of G in characteristic p (see [Pa]). $\Phi(G)$ denotes the Frattini subgroup of G, which coincides with $G'G^p$.

The profinite and pro-p completions of an abstract group Γ are denoted by $\hat{\Gamma}$ and $G_{\hat{p}}$ respectively. Λ_0 denotes the prime subring of Λ, that is, the closed subring generated by 1 in Λ. We shall usually assume that Λ is infinite. The Cartesian product of d copies of a set S is denoted by $S^{(d)}$. We say that a series $\{a_n\}$ grows polynomially if there exists a polynomial P such that $a_n \leq P(n)$ for all n. The lower and upper integral parts of a real number r are denoted by $\lfloor r \rfloor$ and $\lceil r \rceil$ respectively.

The Nottingham group over $\mathbb{F}_p$, which we denote by Nott(p), is the group of automorphisms of the ring $\mathbb{F}_p[[t]]$ acting trivially on $t\mathbb{F}_p[[t]]/t^2\mathbb{F}_p[[t]]$. It may be identified with the group of all power series of the form $t + a_2t^2 + a_3t^3 + \cdots$ ($a_i \in \mathbb{F}_p$) under substitution.

2. Λ-Standard groups

Consider the local ring (Λ, M). Since M is topologically nilpotent, every power series $F \in \Lambda[[X_1, \ldots, X_d]]$ gives rise to a well-defined function $M^{(d)} \longrightarrow \Lambda$, which, by abuse of notation, will be denoted by F. Similarly, if F lies in $\Lambda[[X_1, \ldots, X_d]]^{(k)}$, then it gives rise to a well-defined function $F\colon M^{(d)} \longrightarrow \Lambda^{(k)}$. We shall refer to these functions as functions expressed by power series. Of course, these functions form a subfamily of the set of analytic functions, which are locally expressed by power series.

Recall that a d-dimensional power series $F \in \Lambda[[X_1, \ldots, X_{2d}]]^{(d)}$ is a **formal group**, if it satisfies

$$F(X,0) = F(0,Y) = 0,$$

and

$$F(F(X,Y),Z) = F(X,F(Y,Z)).$$

These conditions imply the existence of an inverse power series $I \in \Lambda[[X_1, \ldots, X_d]]^{(d)}$ satisfying

$$I(X) = -X + \text{non-linear term}$$

and

$$F(I(X),X) = F(X,I(X)) = 0.$$

For background on formal groups, see Hazewinkel [H].

Definition 2.1: A d-dimensional Λ-**standard group** is a pair $(M^{(d)}, F)$ such that F is a d-dimensional formal group defined over Λ.

It is clear that, by identifying F with a function from $M^{(d)} \times M^{(d)}$ to $M^{(d)}$ as above, we obtain a binary operation on $M^{(d)}$ which makes it into a topological group, in which 0 is the identity element. We shall not always distinguish between this group and the pair $(M^{(d)}, F)$. However, it should be emphasized that different standard groups may give rise to isomorphic topological groups (see below). Another point which may need clarification is that, while the dimension d above will usually be positive, the trivial group $\{1\}$ should be considered as a standard group of dimension zero.

The theory of formal groups is particularly developed in the 1-dimensional case, due to work by Dieudonné, Lazard and others. For example, it is known that for a ring Λ without nilpotent torsion elements, every 1-dimensional formal group defined over Λ is commutative [H, p.38]. A similar result follows at once for Λ-standard groups. However, there are usually infinitely many non-isomorphic 1-dimensional formal groups over Λ.

It is shown in [S, p.116] that every Lie group G over an ultrametric field K has an open subgroup which may be identified with a Λ-standard group, where Λ is the valuation ring of K. It is therefore clear that information on $\mathbb{F}_p[[t]]$-standard groups will have immediate applications to the structure of arbitrary analytic groups over $\mathbb{F}_p((t))$.

Example 2.2: (1) The additive group $(M, +)$ is a 1-dimensional standard group.

(2) The multiplicative group $(1 + M, \cdot)$ of normalized units can be identified with the 1-dimensional standard group (M, F) where $F(X, Y) = X + Y + XY$.

(3) Let $\mathrm{SL}^1_m(\Lambda) = \mathrm{Ker}(\mathrm{SL}_m(\Lambda) \longrightarrow \mathrm{SL}_m(\Lambda/M))$ be the first congruence subgroup of $\mathrm{SL}_m(\Lambda)$. Then $\mathrm{SL}^1_m(\Lambda)$ may be given the structure of an $m^2 - 1$-dimensional Λ-standard group. Indeed, given $m^2 - 1$ coordinates $x_{ij} \in M$, where $1 \leq i, j \leq m$ and $(i, j) \neq (m, m)$, there exists a unique matrix $y = (y_{ij}) \in \mathrm{SL}^1_m(\Lambda)$ satisfying $y_{ij} = x_{ij}$ for $i \neq j$, and $y_{ii} = 1 + x_{ii}$ for $i < m$; moreover, all the matrices in $\mathrm{SL}^1_m(\Lambda)$ are obtained in this way. This enables us to identify $\mathrm{SL}^1_m(\Lambda)$ with $M^{(m^2-1)}$. It is then easy to see that multiplication is given by a single $m^2 - 1$-dimensional formal group F, which is defined over the prime subring Λ_0.

Consider the case $\Lambda = \mathbb{F}_p[[t]]$, $M = t\Lambda$. Then $(M^{(2)}, +) \cong (M, +)$ as topological groups; we see that the same topological group can have different standard structures (of different dimensions). This phenomenon, which cannot occur in the p-adic case (where the dimension is determined by the group structure [La]), indicates an inherent difficulty of the subject.

For a closed subring N of M and a standard group $G = (M^{(d)}, F)$, we let $G(N)$ denote the subset $N^{(d)}$ of G. Note that, if either F is defined over the prime subring Λ_0, or N is an ideal of Λ, then $G(N)$ is in fact a closed subgroup of the topological group G. More generally, if R is any ring such that F gives rise to a well-defined function $R^{(2d)} \longrightarrow R^{(d)}$ we let $G(R)$ denote the group $(R^{(d)}, F)$.

The next result is just a slight extension of results from [S] and [B], dealing with the case where Λ is a discrete valuation ring. We need some notation. Given a (d-dimensional) formal group F, let $C(X, Y)$ be the (d-dimensional) power series expressing commutation, namely

$$C(X, Y) = F(I(X), F(I(Y), F(X, Y))),$$

where $I(X)$ is the inverse power series. Similarly, we let $P_i(X)$ be the power series corresponding to taking ith powers. It follows from the definition of a formal group that

$$C(X,0) = C(0,Y) = 0 \quad \text{and} \quad P_i(P_j(X)) = P_j(P_i(X)) = P_{ij}(X).$$

Note that, over certain rings Λ commutation (or taking ith powers) in the standard group $(M^{(d)}, F)$ may also be expressed by some other power series, but for our purpose here this does not really matter.

LEMMA 2.3: *Let I, J be proper ideals of Λ.*

(1) $G(I) \lhd G$.
(2) *If $J \subseteq I$ then* $G(I)/G(J) \cong G(I/J)$.
(3) $(G(I), G(J)) \subseteq G(IJ)$.
(4) $G(I)^p \subseteq G(I^p + pI)$.

Proof: Parts (1),(2) are easily verified. For part (3), consider the power series $C(X,Y)$. It follows from the above remarks that each monomial occuring in $C(X,Y)$ involves some X_i and some Y_j, so (3) easily follows.

Let us prove (4). Consider the power series $P = P_p(X)$, which corresponds to the power map $g \mapsto g^p$ in G. In order to prove (4) it suffices to show that every monomial in P whose coefficient is not divisible by p has (total) degree at least p. Consider $P_i(X)$ for $0 < i < p$. Note that $P_i(X) = iX + \delta_i(X)$ where δ_i consists of non-linear terms. Since $P(P_i(X)) = P_i(P(X))$ we have

$$P(iX + \delta_i(X)) = iP(X) + \delta_i(P(X)).$$

Now, among the monomials in P whose coefficients are not divisible by p, choose one, say Z, with minimal degree. Looking at the coefficients of Z in both sides of the above equation, we obtain $i^k \equiv i \bmod p$, where $k = \deg(Z)$. Taking i to be a primitive element modulo p we deduce that $k \geq p$, as required. ∎

The following filtration associated with a Λ-standard group G will be of some use in what follows.

Definition 2.4: For a standard group $G = (M^{(d)}, F)$, set $G_n = G(M^n)$ $(n \geq 1)$.

The basic properties of $\{G_n\}$ are summarized below.

LEMMA 2.5: *For positive integers n, m we have:*

(1) $G_n \lhd G$.

(2) G_n/G_{n+1} *is a finite elementary abelian p-group.*

(3) $(G_n, G_m) \subseteq G_{n+m}$.

(4) *If* $p\Lambda = 0$ *then* $(G_n)^p \subseteq G_{pn}$.

(5) $G = \varprojlim G/G_n$.

The proof is an easy application of 2.3.

COROLLARY 2.6: *Every Λ-standard group is a pro-p group.*

Since $\{G_n\}$ is a central series, we have $G_n \supseteq \gamma_n(G)$ for all n. The case of equality is discussed in the next section. If Λ has characteristic p then $\{G_n\}$ is an N_p-series (in the sense of [Pa, Chapter 3]), and consequently $G_n \supseteq D_n(G)$, the nth dimension subgroup of G over $\mathbb{F}_p$.

We can now prove the first significant result of this section; it shows that Λ-standard groups are not p-adic analytic, unless Λ is finitely generated as a p-adic module.

THEOREM 2.7: *Let* $G \neq \{1\}$ *be a Λ-standard group. Then G is p-adic analytic if and only if* $\Lambda/p\Lambda$ *is finite.*

Proof: If $\Lambda/p\Lambda$ is finite, then Λ is finitely generated as a $\mathbb{Z}_p$-module by Nakayama's Lemma [AM, pp.21–22], and this implies that G is p-adic analytic. So let us prove the other direction.

Suppose G is p-adic analytic. Then so is $G/G(p\Lambda) \cong G(M/p\Lambda)$. Thus we may assume $p\Lambda$=0, and have to show that Λ is finite.

Suppose not, and consider the sections G_n/G_{2n} $(n \geq 1)$. By 2.5 they are all elementary abelian. Since Λ is infinite and the quotients Λ/M^n are all finite, we see that M is not nilpotent. Therefore the series $\{M^i\}$ is strictly decreasing. This yields

$$|G_n/G_{2n}| = \prod_{i=n}^{2n-1} |G_i/G_{i+1}| = \prod_{i=n}^{2n-1} |M^i/M^{i+1}|^d \geq p^{dn}.$$

Since $\Phi(G_n) \subseteq G_{2n}$ we see that $d(G) \geq dn$ for all n, so in particular $d(G_n) \longrightarrow \infty$ with n. Therefore G has infinite rank. Applying [LM1] we see that G is not p-adic analytic. ∎

COROLLARY 2.8: *If a topological group G is analytic both over* $\mathbb{Z}_p$ *and over* $\mathbb{F}_p[[t]]$, *then it is discrete (hence finite in the compact case).*

Proof: G has an open subgroup H which is a standard $\mathbb{F}_p[[t]]$-group. H is p-adic analytic, since it is an open subgroup of the p-adic analytic group G. Applying 2.7 we obtain a contradiction, unless $H = \{1\}$. We conclude that $\{1\}$ is open in G, and so the topology of G is discrete. ∎

We now construct, following [S, I Chap. II, Prop. 2.3 (4)] and [B, III section 7.4], a Lie algebra associated with a Λ-standard group G. It should be stressed that, in general, this is not the usual Lie algebra associated to G, but rather a certain graded version of it. This graded Lie algebra will serve as an important tool in studying the group-theoretic properties of G.

Definition 2.9: Let G be a Λ-standard group, and let $\{G_n\}$ be the filtration associated with it. Let $L_n = L_n(G) = G_n/G_{n+1}$ considered as an $\mathbb{F}_q$-space, and let $L = L(G) = \prod_{n\geq 1} L_n$ be the Cartesian product of these spaces. For $x \in G_n, y \in G_m$ set

$$[xG_{n+1}, yG_{m+1}] = (x,y)G_{n+m+1}.$$

Extend $[\,,\,]$ to non-homogeneous elements by linearity. Using property 2.5(3) of $\{G_n\}$, it follows that this definition makes sense, and that L is a Lie algebra. We clearly have $[L_n, L_m] \subseteq L_{n+m}$, so L is graded over the natural numbers. If Λ has characteristic p, we may define a formal pth power in L by

$$(xG_{n+1})^{[p]} = x^p G_{pn+1},$$

where $x \in G_n$ (see 2.5(4)). Then L becomes a restricted Lie algebra satisfying $L_n^{[p]} \subseteq L_{pn}$ (see [J] for a background on restricted Lie algebras).

Remark 2.10:

(1) Note that $L(G)$ is a Lie algebra over the finite residue field $\mathbb{F}_q = \Lambda/M$ of characteristic p, even when Λ has characteristic zero. As an $\mathbb{F}_q$-Lie algebra $L(G)$ is infinite-dimensional if $|\Lambda| = \infty$.

(2) Let $\mathrm{gr}(\Lambda) = \prod_{n\geq 0} \mathrm{gr}_n(\Lambda) = \prod_{n\geq 0} M^n/M^{n+1}$ be the complete graded ring associated with Λ, and let $\mathrm{gr}(M) = \prod_{n\geq 1} M^n/M^{n+1}$ be its maximal ideal. Then $L(G)$ has a natural structure of a $\mathrm{gr}(\Lambda)$-module. Moreover, as a $\mathrm{gr}(M)$-module, $L(G)$ is free of rank $d = \dim(G)$, that is $L(G) \cong \mathrm{gr}(M)^{(d)}$.

(3) Let $C(X,Y)$ be the commutation power series as before. Then C gives rise to a well-defined binary operation on $\mathrm{gr}(M)^{(d)}$ which we denote by $\mathrm{gr}(C)$. By definition, $\mathrm{gr}(C)$ is a graded operation, i.e. it sends $\mathrm{gr}_n(\Lambda)^{(d)} \times \mathrm{gr}_m(\Lambda)^{(d)}$ to

$\mathrm{gr}_{n+m}(\Lambda)^{(d)}$. From our definition of $L(G)$ it follows that this operation coincides with the Lie product in $L(G)$. Therefore

$$L(G) \cong (\mathrm{gr}(M)^{(d)}, +, \mathrm{gr}(C)).$$

(4) It follows from previous remarks that $C(X,Y)$ has no linear terms, and that its quadratic part is bilinear in X, Y. Let $C_2(X,Y)$ be the reduction of that quadratic part modulo M. Then $C_2(X,Y)$ is a bilinear form defined over $\mathbb{F}_q$. Observe that monomials of degree greater than 2 in $C(X,Y)$, and monomials whose coefficients belong to M will not effect the binary operation $\mathrm{gr}(C)$. Thus $\mathrm{gr}(C)$ coincides with the binary operation defined by C_2 on $\mathrm{gr}(M)^{(d)}$.

We see that $L(G) \cong (\mathrm{gr}(M)^{(d)}, +, C_2)$. In particular, $L(G)$ has the structure of a Lie algebra over $\mathrm{gr}(\Lambda)$ (or $\mathrm{gr}(M)$).

(5) Let $L_0 = L_0(G) = (\mathrm{gr}_0(\Lambda)^{(d)}, +, C_2) = (\mathbb{F}_q^{(d)}, +, C_2)$. Then L_0 is a d-dimensional Lie algebra over $\mathbb{F}_q$, and we have

$$L(G) \cong L_0(G) \otimes \mathrm{gr}(M).$$

The finite Lie algebra $L_0(G)$ constructed above will play an important role in what follows.

It is easy to verify that our construction of $L(G)$ is compatible with that of [H, pp.79–81]. More precisely, it is shown in [H] that, if $F(X,Y)$ is a formal group law and $F_2(X,Y)$ is its quadratic part, then the bilinear form $[X,Y] = F_2(X,Y) - F_2(Y,X)$ satisfies the Jacobi identity. Now, the Lie algebra $L(G)$ is obtained by applying that form to $\mathrm{gr}(M)^{(d)}$.

Example 2.11: (1) Let $\Lambda = \mathbb{F}_p[[t]]$, $M = t\Lambda$, and let $G = \mathrm{SL}_m^1(\Lambda)$. Then it is easy to verify that $L(G) \cong \mathfrak{sl}_m(M) \cong \mathfrak{sl}_m(p) \otimes M$.

(2) If $\Lambda = \mathbb{Z}_p$ then $\mathrm{gr}(\Lambda) \cong \mathbb{F}_p[[t]]$. The Lie algebra associated with $\mathrm{SL}_m(\mathbb{Z}_p)$ is therefore isomorphic to that of $\mathrm{SL}_m^1(\mathbb{F}_p[[t]])$ (without the restricted structure), since $L_0(G)$ coincide for these two groups.

We now define the Lie subalgebra of $L(G)$ associated with a closed subgroup $H \subseteq G$.

Definition 2.12: For a Λ-standard group G and a closed subgroup H, set $K(H) = \prod_{n\geq 1} K_n(H)$, where $K_n(H) = (H \cap G_n)G_{n+1}/G_{n+1} \subseteq L_n(G)$. Observe that, in general, $K(H)$ is an $\mathbb{F}_p$-space, but not a $\mathrm{gr}(\Lambda)$-module (it may not even be an $\mathbb{F}_q$-space if $q \neq p$).

The following properties are easily verified.

LEMMA 2.13:

(1) *$K(H)$ is a graded Lie subalgebra of $L(G)$, considered as a Lie algebra over $\mathbb{F}_p$.*
(2) *If $p\Lambda=0$ then $K(H)$ is a restricted subalgebra.*
(3) *If $H \lhd G$ then $K(H)$ is a Lie ideal in $L(G)$.*
(4) *$K(G) = L(G)$ and $K(H_1) \supseteq K(H_2)$ if $H_1 \supseteq H_2$.*
(5) *$K((H_1, H_2)) \supseteq [K(H_1), K(H_2)]$.*
(6) *If $p\Lambda = 0$ then $K(H^p) \supseteq K(H)^{[p]}$.*
(7) *If $H_1 \supseteq H_2$ then $(K(H_1)\colon K(H_2)) = (H_1\colon H_2)$ (where both sides may be infinite). In particular, $(G\colon H)$ is finite if and only if $K(H)$ has finite co-dimension in $L(G)$.*

3. Λ-Perfect groups

In this section we restrict our attention to a subclass of Λ-standard groups, which we call Λ-perfect. Unlike general Λ-standard groups, the Λ-perfect ones are always finitely generated, and their structure turns out to be rather rigid.

Definition 3.1: Let G be a Λ-standard group, and let $L_0 = L_0(G)$ be the finite Lie algebra associated with it (see 2.10). We say that G is a **Λ-perfect group** if L_0 is a perfect Lie algebra (i.e. $L_0' = L_0$).

Since $L(G) = \prod L_n \cong L_0 \otimes \mathrm{gr}(M)$, where L_n corresponds to $L_0 \otimes M^n/M^{n+1}$, we see that G is perfect if and only if $[L_n, L_m] = L_{n+m}$ for all $n, m \geq 1$. For example, note that the Λ-standard groups $\mathrm{SL}_m^1(\Lambda)$ are all perfect, unless $p = m = 2$.

While the filtration $\{G_n\}$ cannot always be described group-theoretically, we do have such a description in the Λ-perfect case.

PROPOSITION 3.2: *Let G be a Λ-perfect group. Then,*

(1) *$(G_n, G_m) = G_{n+m}$ for all n, m.*
(2) *$\{G_n\}$ coincides with the lower central series $\{\gamma_n\}$ of G.*
(3) *If $p\Lambda=0$ then $G_n = D_n(G)$, the nth dimension subgroup of G over $\mathbb{F}_p$.*

Proof: (1) Let $L(G) = \prod L_n$. Then $[L_n, L_m] = L_{n+m}$, from which it follows that, $(G_n, G_m)G_{n+m+1} = G_{n+m}$ for all n, m. We argue, by induction on $k \geq 1$, that $(G_n, G_m)G_{n+m+k} = G_{n+m}$ for all n, m, the case $k = 1$ having already been established. Assuming this for k we get

$$\begin{aligned}(G_n, G_m)G_{n+m+k+1} &= (G_n, G_m)(G_n, G_{m+1})G_{n+(m+1)+k} \\ &= (G_n, G_m)G_{n+(m+1)} = G_{n+m},\end{aligned}$$

as required.

Since (G_n, G_m) is closed (by definition), it follows that $(G_n, G_m) = G_{n+m}$.

(2) Follows from (1).

(3) We always have $D_n \supseteq \gamma_n$, so applying (2) we get $D_n \supseteq G_n$. On the other hand, $\{G_n\}$ is an N_p-series (by 2.5), and $\{D_n\}$ is the minimal N_p-series in G (see [Pa, Chapter 3]). Therefore we have equality. ∎

Remark 3.3: It is easy to see that the equality $G_2 = \gamma_2$ already implies Λ-perfectness in standard groups. Therefore $\{G_n\}$ coincides with $\{\gamma_n\}$ if and only if G is Λ-perfect.

The following result provides some necessary group-theoretic conditions for a pro-p groups to have the structure of a Λ-perfect group.

COROLLARY 3.4: *Let G be a Λ-perfect group.*

(1) *G is finitely generated; in fact $d(G) = \dim(G)\dim_{\mathbb{F}_p}(M/M^2)$.*

(2) *$(\gamma_n, \gamma_m) = \gamma_{n+m}$ for all n, m.*

(3) *The sections γ_n/γ_{n+1} are elementary abelian finite p-groups.*

(4) *If $p\Lambda = 0$ then γ_n/γ_{pn} has exponent p, and $\gamma_n = D_n(G)$ for all n.*

Proof: Parts (2)–(4) follow immediately from 2.5 and 3.2, so we only have to prove (1). Note that $G_2 \supseteq \Phi(G) = \gamma_2(G)$ (as G/G_2 is elementary abelian). However, $G_2 = \gamma_2$ by 3.2. Hence $G_2 = \Phi(G)$.

Setting $d = \dim(G)$ we conclude that

$$\begin{aligned}d(G) &= \dim_{\mathbb{F}_p}(G/\Phi(G)) = \dim_{\mathbb{F}_p}(G_1/G_2) \\ &= \dim_{\mathbb{F}_p}((M/M^2)^{(d)}) = d \cdot \dim_{\mathbb{F}_p}(M/M^2),\end{aligned}$$

as required. ∎

We now turn to the study of some arithmetic invariants associated with a Λ-perfect group G. We need some notation. Set,

$$c_n = \dim_{\mathbb{F}_p}(\gamma_n/\gamma_{n+1}), \quad d_n = \dim_{\mathbb{F}_p}(D_n/D_{n+1}).$$

Let $f_G(z) = \sum_{n\geq 1} c_n z^n$ be the generating function of $\{c_n\}$. Let Δ be the augmentation ideal of the group ring $\mathbb{F}_p G$, and put

$$r_n = \dim_{\mathbb{F}_p}(\Delta^n/\Delta^{n+1}).$$

Jennings' theory relates the series $\{d_n\}$ and $\{r_n\}$ as follows:

$$\sum_{n\geq 0} r_n z^n = \prod_{n\geq 1}(1 + z^n + z^{2n} + \cdots + z^{(p-1)n})^{d_n}.$$

Cf. [Pa, Chapter 3]. Turning to the underlying ring Λ, we let

$$s_n = \dim_{\Lambda/M}(M^n/M^{n+1})$$

be the Hilbert–Poincaré series of $\mathrm{gr}(\Lambda)$. Denote its generating function by $f_\Lambda(z) = \sum_{n\geq 0} s_n z^n$. Recall that $\Lambda/M = \mathbb{F}_q$ where $q = p^e$.

THEOREM 3.5: *Let G be a Λ-perfect group, and let $d = \dim(G)$.*

(1) $f_G(z) = de(f_\Lambda(z) - 1)$.

(2) *$f_G(z)$ is a rational function.*

(3) *The series $\{c_n\}$ grows polynomially with n.*

(4) *The series $\{d_n\}$ grows polynomially with n.*

Proof: For $n \geq 1$ we have

$$\begin{aligned} c_n &= \dim_{\mathbb{F}_p}((M^n/M^{n+1})^{(d)}) = d \cdot \dim_{\mathbb{F}_p}(M^n/M^{n+1}) \\ &= de \cdot \dim_{\mathbb{F}_q}(M^n/M^{n+1}) = de \cdot s_n. \end{aligned}$$

This proves the first part.

The second follows from Hilbert–Serre Theorem [AM, p.117], showing that f_Λ is a rational function of z. Similarly, since $\{s_n\}$ grows polynomially [AM, p.119], the same holds for $\{c_n\}$. Finally, we always have $D_{n+1} \supseteq \gamma_{n+1}$, and this implies

$$d_n \leq \sum_{i\leq n} d_i \leq \sum_{i\leq n} c_i$$

for all n. Since the right-hand side grows polynomially we are done. ∎

It is clear from 3.2(3) that if G is a Λ-perfect group and Λ has characteristic p, then the generating function $\sum d_n z^n$ is also rational. However, this is not true without the restriction of the characteristic; for example, for $G = \mathbb{Z}_p$ we have $\sum d_n z^n = \sum_{i\geq 0} z^{p^i}$ which is not a rational function.

Note that, unless $p = m = 2$, the group $G = \mathrm{SL}_m^1(\Lambda)$ is Λ-perfect, and thus $d_n(G)$ grows polynomially by 3.5. In fact it can be shown that $d_n(G)$ grows polynomially for every finite index pro-p subgroup of $\mathrm{GL}_m(\Lambda)$, without any restriction on p, m, Λ.

It follows from part 1 of Theorem 3.5 that, if G is an $\mathbb{F}_p[[t]]$-perfect group, then $|\gamma_n/\gamma_{n+1}| = p^d$ for all n, where $d = \dim(G) = d(G)$. Therefore the Nottingham group $G = \mathrm{Nott}(p)$ cannot be $\mathbb{F}_p[[t]]$-perfect: indeed, its lower central factors have orders p and p^2 [Y].

We now draw conclusions concerning the growth of the series $\{r_n\}$ defined above. Jennings' formula enables one to compute $\{r_n\}$ in terms of $\{d_n\}$. However, polynomial growth of $\{d_n\}$ does not imply polynomial growth of $\{r_n\}$. Still, applying a result of Bereznyi [Be], we shall establish subexponential growth of $\{r_n\}$.

PROPOSITION 3.6: *For every pro-p group G we have*

$$\limsup \frac{1}{n} \ln(r_n(G)) = \limsup \frac{1}{n} \ln(d_n(G)).$$

Proof: Let α, β be the left and right hand side respectively. The section D_n/D_{n+1} may be identified with a subspace of the $\mathbb{F}_p$-linear space Δ^n/Δ^{n+1}. Hence $r_n \geq d_n$ for all n, so $\alpha \geq \beta$.

On the other hand, Bereznyi [Be, Lemma 1, p.572] shows that if $\{r_n\}$ and $\{d_n\}$ are any sequences of non-negative integers satisfying $\sum r_n z^n \leq \prod(1-z^n)^{-d_n}$ (that is, the inequality holds for each coefficient), then

$$\limsup \frac{1}{n} \ln(r_n) \leq \limsup \frac{1}{n} \ln(d_n).$$

In our case we have,

$$\sum r_n z^n = \prod_{n\geq 1} \Big(\sum_{0\leq i<p} z^{in} \Big)^{d_n} \leq \prod_{n\geq 1} \Big(\sum_{i\geq 0} z^{in} \Big)^{d_n} = \prod_{n\geq 1} (1-z^n)^{-d_n}.$$

Hence $\alpha \leq \beta$ by Bereznyi's lemma, and the proposition is proved. ∎

The proposition implies that $\{r_n\}$ grows subexponentially (i.e. $\alpha = 0$) if and only if $\{d_n\}$ grows subexponentially ($\beta = 0$). In view of Theorem 3.5(4) we therefore have:

COROLLARY 3.7: *Let G be a Λ-perfect group and let $r_n = r_n(G)$. Then $\{r_n\}$ has subexponential growth.*

This corollary will be rather useful in section 5.

We close this section with a short discussion on the relation between the growth of $d_n(G)$ and the growth of $d_n(H)$ for a finitely generated subgroup H of G.

In Lemma 2 of [Be] it is claimed that, for any finitely generated group G, subexponential growth of $d_n(G)$ implies subexponential growth of $d_n(H)$. However, the following provides a counter-example to this lemma. Take $G = \mathrm{Ker}(\mathrm{SL}_3(\mathbb{Z}) \longrightarrow \mathrm{SL}_3(\mathbb{F}_p))$. By the affirmative solution to the congruence subgroup problem $d_n(G)$ is bounded; but G contains a 2-generated free subgroup H, and $d_n(H)$ grows exponentially. It might still be true that [Be, Lemma 2] holds for pro-p groups, but the proof given there is erroneous.

However, it is easy to see that, if G is a finitely generated pro-p group such that $d_n(G)$ grows polynomially, and $H \subseteq_o G$, then $d_n(H)$ grows polynomially. To show this let $N \lhd G$ be an open normal subgroup of G contained in H. Then G/N is a finite p-group, so the augmentation ideal $\Delta(G/N)$ is nilpotent. This means that

$$\Delta(G)^c \subseteq \Delta(N)\mathbb{F}_p G,$$

so $\Delta(G)^{cn} \subseteq \Delta(N)^n \mathbb{F}_p G$ for all n. This implies that

$$D_{cn}(G) \subseteq D_n(N) \subseteq D_n(H) \quad \text{for all } n.$$

The polynomial growth of $\{d_n(H)\}$ now easily follows.

It would be extremely useful to know that, for a finitely generated pro-p group G, subexponential (or even polynomial) growth of $d_n(G)$ implies subexponential growth of $d_n(H)$ for finitely generated closed subgroups H. In view of Theorem 3.5 and the remarks thereafter, this would imply the following:

CONJECTURE 3.8:

(1) *A (non-abelian) free pro-p group cannot be embedded in* $\mathrm{GL}_m(\Lambda)$.

(2) *Every pro-p subgroup of* $\mathrm{GL}_m(\Lambda)$ *satisfies some non-trivial pro-p identity.*

We note that assertions (1) and (2) are actually equivalent. For more details and some interesting partial results, see Zubkov [Zu].

4. Growth functions

In this section we examine certain growth functions associated with a Λ-perfect group, such as its subgroup growth, and the growth of the number of generators of open subgroups. It will turn out that, up to certain constants, the growth behaviour of a Λ-perfect group G does not depend on G or on the underlying ring Λ, as long as $\Lambda/p\Lambda$ is infinite, i.e. G is not p-adic analytic.

Given a finitely generated pro-p group G, let

$$a_n = a_n(G) = |\{H \subseteq_o G \mid (G\colon H) = n\}|,$$

and

$$g_n = g_n(G) = \max\{d(H) \mid H \subseteq_o G,\ (G\colon H) = n\},$$

as in the introduction.

If G is p-adic analytic, then $\{g_n\}$ is bounded and $\{a_n\}$ grows polynomially with n [LM1, LM2]. In free (non-abelian) pro-p groups, $\{g_n\}$ grows linearly (according to the Schreier formula), and $\{a_n\}$ grows exponentially [I].

In general, we have the following simple relation between $\{a_n\}$ and $\{g_n\}$.

LEMMA 4.1: *With the above notation we have*

$$a_{p^k} \leq \prod_{i=0}^{k-1} \frac{p^{g_{p^i}} - 1}{p-1} \leq p^{g_1 + g_p + \cdots + g_{p^{k-1}}}.$$

Proof: It suffices to show that, for $k \geq 1$ we have

$$a_{p^k} \leq a_{p^{k-1}} \cdot \frac{p^{g_{p^{k-1}}} - 1}{p-1}.$$

Indeed, any open subgroup H of index p^k in G is a maximal subgroup of some subgroup H_1, whose index is p^{k-1}. There are $a_{p^{k-1}}$ possibilities for the choice of H_1. Fixing H_1 , there are $(p^{d(H_1)}-1)/(p-1)$ ways to choose a maximal subgroup $H \subset H_1$. Since $d(H_1) \leq g_{p^{k-1}}$, the result follows. ∎

The following Lie-theoretic result is the key to our analysis of the growth behaviour of Λ-perfect groups.

PROPOSITION 4.2: *Let L_0 be a finite-dimensional perfect Lie algebra over $\mathbb{F}_p$, and let $L = L_0 \otimes \mathrm{gr}(M)$. Then there exists a constant c such that, for every proper open Lie $\mathbb{F}_p$-subalgebra K of L we have*

$$\dim(K/K') \leq c \cdot \dim(L/K).$$

Proof: We may assume, for simplicity, that $\Lambda/M \cong \mathbb{F}_p$. Let $d = \dim(L_0)$. Note that $K \supseteq L_n$ for all sufficiently large n. Since L_0 is perfect this implies that $K' \supseteq L_n$ for all sufficiently large n. In particular K/K' is finite-dimensional.

Given a certain subset A of K whose image in K/K' forms a basis for K/K', we shall construct a subset B of L, linearly independent modulo K, such that $|A| \leq c_1|B| + c_2$ for some fixed constants c_1, c_2 (independent of K). This will show that

$$\dim(K/K') = |A| \leq c_1|B| + c_2 \leq c_1 \dim(L/K) + c_2 \leq c \cdot \dim(L/K),$$

where $c = c_1 + c_2$ (recall that K is a proper subalgebra of L).

This construction, which is of a combinatorial nature, consists of several stages.

1. Let $\{X_1, \ldots, X_r\}$ be a basis for $\mathrm{gr}_1(\Lambda) = M/M^2$. Then there exists a collection C of monomials in $X_1, \ldots, X_r$ satisfying:

(i) For each $n \geq 0$, the subset C_n of monomials of degree n in C forms a basis for $\mathrm{gr}_n(\Lambda) = M^n/M^{n+1}$.

(ii) C is an order ideal of monomials, namely, if $X \in C$ and Y divides X, then $Y \in C$.

The construction of C is rather standard; see, e.g., [St, p.59].

2. Clearly, every element a of $L = L_0 \otimes \mathrm{gr}(M)$ may be uniquely expressed as $a = \sum_X a_X \otimes X$, where X ranges over C and $a_X \in L_0$ (note that $a_1 = 0$). Consider the lexicographic ordering $<$ on C, and define the **leading term** of a by $\mathrm{lt}(a) = a_X \otimes X$, where X is the minimal monomial in C for which $a_X \neq 0$. The **leading monomial** of a is then defined by $\mathrm{lm}(a) = X$.

3. Call a subset $A \subseteq K$ forming a basis for K modulo K' **maximal** if one cannot replace an element $a \in A$ by an element a' satisfying $\mathrm{lm}(a') > \mathrm{lm}(a)$, thus obtaining another basis for K/K'. It is easy to verify that each basis for K/K' can be deformed in finitely many steps to a maximal basis.

4. Let $A \subseteq K$ be a maximal basis for K modulo K'. Then:

(i) If $a \neq b$ in A, then $\mathrm{lt}(a) \neq \mathrm{lt}(b)$. For otherwise we can replace a by $a' = a - b$, which satisfies $\mathrm{lm}(a') > \mathrm{lm}(a)$, contradicting the maximality of A.

(ii) For each monomial $X \in C$ there exist at most d elements $a \in A$ with $\mathrm{lm}(a) = X$. This is because $d+1$ elements of the form $a_X \in L_0$ are linearly dependent (over $\mathbb{F}_p$); thus if $\mathrm{lm}(a) = X$ for $d+1$ elements of A then it would be possible to increase $\mathrm{lm}(a)$ for some a.

(iii) If $a \in A$ then $\mathrm{lt}(a)$ does not lie in $\mathrm{lt}(K') = \{\mathrm{lt}(b)\colon b \in K'\}$. Indeed, $\mathrm{lt}(a) = \mathrm{lt}(b)$ for $b \in K'$ enables one to replace a by $a - b$, contradicting the maximality of A.

5. Let A be as above and let $a \in A$. Suppose $\mathrm{lt}(a) = a_X \otimes X$, and let $Y, Z \in C$ be monomials such that $X = YZ$. Since L_0 is perfect there exist (non-zero) elements $b_i, c_i \in L_0$ such that $a_X = \sum[b_i, c_i]$. Therefore $\mathrm{lt}(a) = \sum[b_i \otimes Y, c_i \otimes Z]$. Note that, if $b_i \otimes Y, c_i \otimes Z \in \mathrm{lt}(K)$ for all i, then there exist elements g_i, h_i consisting of monomials greater than Y, Z respectively such that $b_i \otimes Y + g_i, c_i \otimes Z + h_i \in K$. This shows that

$$\mathrm{lt}(a) + f = \sum[b_i \otimes Y + g_i, c_i \otimes Z + h_i] \in K',$$

where f consists of monomials greater than X. Thus $\mathrm{lt}(a) \in \mathrm{lt}(K')$, contradicting a previous claim.

We conclude that, if $X \in \mathrm{lm}(A)$, then any factorization $X = YZ$ gives rise to an element $b \otimes W \notin \mathrm{lt}(K)$, where $0 \neq b \in L_0$ and $W \in \{Y, Z\}$.

6. Let $S = \mathrm{lm}(A)$, the set of leading monomials of elements of A. Then $|A| \leq d|S|$ by property (ii) in part 4. Define a metric ρ on C by

$$\rho(\prod X_i^{n_i}, \prod X_i^{m_i}) = \max\{|n_i - m_i| \colon 1 \leq i \leq r\}.$$

Let T be a maximal subset of S satisfying

(i) $\deg(X) > r$ for all $X \in T$.

(ii) $\rho(X, Y) \geq 2$ for all distinct $X, Y \in T$.

In order to estimate the cardinality of T, note that the union of all closed balls of radius 1 around elements of T, together with all the $\binom{2r}{r}$ monomials of degree at most r in $X_1, \ldots, X_r$ covers S (otherwise T may be enlarged). Since a ball of radius 1 (with respect to ρ) has at most 3^r elements, we conclude that

$$|S| \leq |T| 3^r + \binom{2r}{r}.$$

Thus

$$|A| \leq d|S| \leq c_1|T| + c_2,$$

where $c_1 = d3^r$ and $c_2 = d\binom{2r}{r}$.

7. Given a monomial $X = \prod X_i^{n_i} \in T$, define

$$X^+ = \prod X_i^{\lceil n_i/2 \rceil}, \quad X^- = \prod X_i^{\lfloor n_i/2 \rfloor}.$$

Note that $\deg(X^+), \deg(X^-) > 0$ (as $\deg(X) > r$), and $X = X^+ \cdot X^-$. Furthermore, if X, Y are distinct monomials in T, then the sets $\{X^+, X^-\}$, $\{Y^+, Y^-\}$ are disjoint (as $\rho(X, Y) > 1$).

8. Recall that $T \subseteq S = \mathrm{lm}(A)$. Thus, given $X \in T$, we may choose an element $a \in A$ with $X = \mathrm{lm}(a)$. Apply part 5 above with $Y = X^+$ and $Z = X^-$ to obtain an element of the form $b \otimes W \notin \mathrm{lt}(K)$, where $b \in L_0$ and $W \in \{X^+, X^-\}$. The element $b \otimes W$ obtained in this way depends on X, so let us write $b = b_X, W = W_X$.

9. We can now construct the required subset $B \subseteq L$:

$$B = \{b_X \otimes W_X : X \in T\}.$$

It is clear from the construction of B that B and $\mathrm{lt}(K)$ are disjoint. Using part 7 it follows that the map $X \mapsto W_X$ defined on T is injective. This implies, in particular, that $|B| = |T|$, so

$$|A| \leq c_1|B| + c_2,$$

by part 6.

It remains to be shown that B is linearly independent modulo K. Suppose not. Then for some non-zero scalars $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_p$ and for distinct elements $b_1 \otimes W_1, \ldots, b_k \otimes W_k$ of B we have $\sum_{i=1}^k \lambda_i b_i \otimes W_i \in K$.

Without loss of generality we may assume that $W_1 < W_2 < \cdots < W_k$. Thus

$$b_1 \otimes W_1 = \mathrm{lt}(\lambda_1^{-1} \sum \lambda_i b_i \otimes W_i) \in \mathrm{lt}(K),$$

a contradiction.

The proposition is proved. ∎

THEOREM 4.3: *Let G be a Λ-perfect group. Then $g_n(G) \leq C \log_p n$ for all $n > 1$, where C is a fixed constant (depending on G).*

Proof: Let $H \subset_o G$ be an open subgroup of index $n = p^k$ in G $(k > 0)$. Consider $L = L(G) = L_0 \otimes \mathrm{gr}(M)$ and $K = K(H) \subset L$ (see 2.10,2.12). By 2.13 we have $(L: K) = (G: H) = p^k$, so $\dim(L/K) = k$ (where all dimensions are computed over $\mathbb{F}_p$). Applying the above proposition we conclude that $\dim(K/K') \leq ck$. Since $K(H') \supseteq K(H)' = K'$ (see 2.13), we have $\dim(K(H)/K(H')) \leq ck$, and this yields

$$(H: H') = (K(H): K(H')) \leq p^{ck}.$$

Finally $p^{d(H)} = |H/\Phi(H)| \leq |H/H'| \leq p^{ck}$, so $d(H) \leq ck = c \log_p n$.

Thus the result follows (with $C = c$). ∎

Note that we have actually shown rather more, namely, that

$$(H\colon H') \le (G\colon H)^C$$

for every (proper) open subgroup H of G.

We can now determine the subgroup growth of Λ-perfect groups.

THEOREM 4.4: *Let G be a Λ-perfect group. Then, for a fixed constant c we have $a_n(G) \le n^{c\log_p n}$ for all $n \ge 1$.*

Proof: We may assume $n = p^k$ for some k (otherwise $a_n = 0$). Applying 4.1 and 4.3 we obtain ,

$$a_n \le p^{g_1+g_p+\cdots+g_{p^{k-1}}} \le p^{d+C(1+2+\cdots+k-1)} \le p^{ck^2} = n^{c\log_p n}$$

for a suitable constant c (depending on d and C).

The result follows. ∎

As for examples, it is shown in [Sh] (using a slightly different method) that the subgroup growth of $\mathrm{SL}_2^1(\mathbb{F}_p[[t]])$ $(p > 2)$ is at most $2n^{2\log_p n}$.

It is rather intriguing that the Nottingham group has a similar type of growth, although it is not $\mathbb{F}_p[[t]]$-perfect. Indeed, by [LGSW], if $p \ge 5$ and $a_n = a_n(\mathrm{Nott}(p))$, then

$$a_n \le 2n^{(1+\frac{2}{p-1})\log_p n}$$

for all n.

We now turn to the study of certain limits related to numbers of generators of open subgroups. Following [LM1] we set

$$\underline{L}_d = \liminf\{d(H) \mid H \subseteq_o G\},$$

$$\overline{L}_d = \limsup\{d(H) \mid H \subseteq_o G\},$$

$$\underline{NL}_d = \liminf\{d(H) \mid H \lhd_o G\},$$

and

$$\overline{NL}_d = \limsup\{d(H) \mid H \lhd_o G\}.$$

It is shown in [LM1] that, for an arbitrary pro-p group G, three of these limits coincide, i.e. $\overline{L}_d(G) = \overline{NL}_d(G) = \underline{NL}_d(G)$; moreover, their common value is finite if and only if G is p-adic analytic. In that case we have $\overline{L}_d(G) = \dim(G)$, while $\underline{L}_d(G)$ coincides with the number of generators of the p-adic Lie algebra of

G. Thus $\underline{L}_d(G)$ is usually smaller than $\overline{L}_d(G)$. We refer to $\underline{L}_d(G)$ as the **lower rank** of G.

The following question is then posed in [LM1]: can $\underline{L}_d(G)$ be finite while $\overline{L}_d(G)$ is infinite? In other words, is there a pro-p group of finite lower rank which is not p-adic analytic?

We shall now settle this problem in the affirmative, by showing that $\underline{L}_d(G)$ is finite for every Λ-perfect group whose formal group law F is defined over Λ_0. We need the following combinatorial result.

LEMMA 4.5: *Let Γ be the free commutative semigroup on $X_1, \ldots, X_r$. Given $n \geq 1$ let*

$$T_n = \{X_1^n, \ldots, X_r^n\} \cup \{X_i X_j^n \mid 1 \leq i, j \leq r\},$$

and let Γ_n be the sub-semigroup generated by T_n. Then Γ_n is co-finite in Γ.

Proof: Regard elements of Γ as monomials $X = X_1^{n_1} \cdots X_r^{n_r}$ $(n_i \geq 0)$. Let $f = r^2 n^2 (n+1)$. We shall show that every monomial X whose (total) degree is greater than f lies in Γ_n. Obviously, this would imply that $\Gamma \setminus \Gamma_n$ is finite, as asserted.

First observe that, since $X_i^n, X_i^{n+1} \in T_n$, we have $X_i^N \in \Gamma_n$ for all $N \geq n(n+1)$. Thus, if for all i we have $n_i = 0$ or $n_i \geq n(n+1)$, then

$$X = X_1^{n_1} \cdots X_r^{n_r} \in \Gamma_n.$$

So suppose this is not the case. Assuming $\deg(X) > f$ it follows that $n_i > rn^2(n+1)$ for some i. Without loss of generality we may therefore write

$$n_1 \leq n_2 \leq \cdots \leq n_k < n(n+1) \leq n_{k+1} \leq \cdots \leq n_r,$$

where $1 \leq k < r$ and $n_r \geq rn^2(n+1)$. Consider the monomial

$$Y = \prod_{i=1}^{k} (X_i X_r^n)^{n_i} = (\prod_{i=1}^{k} X_i^{n_i}) X_r^m,$$

where $m = n(n_1 + \cdots + n_k) \leq nkn(n+1) \leq (r-1)n^2(n+1)$.

It is clear that $Y \in \Gamma_n$. Let

$$Z = X_{k+1}^{n_{k+1}} \cdots X_{r-1}^{n_{r-1}} \cdot X_r^{n_r - m}.$$

Note that $n_{k+1}, \ldots, n_r \geq n(n+1)$ and that $n_r - m \geq n^2(n+1)$. Therefore $Z \in \Gamma_n$ by previous arguments. Finally, $X = YZ \in \Gamma_n$.

The result follows. ∎

The main point of this construction is that $\{\Gamma_n\}$ is a series of d-generated cofinite sub-semigroups of Γ where $d = r^2 + r$, with the property that $\Gamma_n \subseteq \Gamma^n$. In fact it can be shown that no such series exists with $d < r^2 + r$. Thus, under a suitable terminology, the free commutative semigroup $\Gamma = \langle X_1, \ldots, X_r \rangle$ has finite lower rank (which is equal to $r^2 + r$).

As a consequence we see that any commutative affine algebra $k[a_1, \ldots, a_r]$ has a series of d-generated subalgebras R_n (without 1) of finite co-dimension, such that $R_n \subseteq (a_1, \ldots, a_r)^n$, where again $d = r^2 + r$.

We can now prove:

THEOREM 4.6: *Let G be a Λ-perfect group defined over Λ_0. Then G has finite lower rank, i.e. $\underline{L}_d(G) < \infty$.*

Proof: There exists r such that Λ is an epimorphic image of $\Delta = \Lambda_0[[X_1, \ldots, X_r]]$. Let N be the maximal ideal of Δ. Since the formal group law F is defined over Λ_0, it gives rise to a Δ-perfect group $H = (N^{(d)}, F)$ where $d = \dim(G)$. Now, N is mapped onto M, so G is an epimorphic image of H (see 2.3). It therefore suffices to show that H has finite lower rank. Thus we may assume that $G = H$ and $\Lambda = \Lambda_0[[X_1, \ldots, X_r]]$.

Note that the maximal ideal M of Λ is generated by $X_1, \ldots, X_r$ and $p = p \cdot 1$ (which may be 0). If p is non-zero in Λ, we set $X_{r+1} = p$ and increase r by 1. This ensures that $X_1, \ldots, X_r$ generate M.

We shall now show that, in this situation, the lower rank of G is at most $d(r^2 + r)$.

Let $L = L(G) = L_0 \otimes \mathrm{gr}(M)$. For a monomial X in $X_1, \ldots, X_r$, define $L_X = L_0 \otimes X$. By abuse of notation we shall also regard every such monomial as an element of the semigroup Γ defined in Lemma 4.5.

Then L_X $(X \in \Gamma)$ are linear subspaces of L, and L is spanned by these subspaces. Since L_0 is perfect, we have

$$[L_X, L_Y] = [L_0 \otimes X, L_0 \otimes Y] = [L_0, L_0] \otimes XY = L_{XY}$$

for all $X, Y \in \Gamma$.

Given a monomial $X \in \Gamma$, let $M_X \subseteq M$ be the closed subring (without 1) it generates in Λ. Let $G_X = G(M_X)$ be the corresponding subgroup (note that we need the assumption that F is defined over Λ_0 to conclude that G_X is a subgroup).

Now, since M is mapped onto M_X (in various ways), G_X is an epimorphic image of G. This yields

$$d(G_X) \leq d(G) = d \quad \text{for all } X \in \Gamma.$$

Let $\Gamma_n = \langle T_n \rangle$ be as in Lemma 4.5. Given $n \geq 1$ define a (closed) subgroup $H_n \subseteq_c G$ by

$$H_n = \langle G_X \colon X \in T_n \rangle.$$

Clearly, $|T_n| = r^2 + r$, so

$$d(H_n) \leq \sum_{X \in T_n} d(G_X) \leq d(r^2 + r).$$

Note also that $H_n \subseteq G_n$ for all n, so $H_n \longrightarrow 1$ in the topology of G.

To prove the theorem it remains to establish the following:

Claim: H_n is open in G for all n.

To show this fix n and let $K = K(H_n)$ be the Lie subalgebra associated to H_n. It suffices to show that L/K is finite-dimensional (over $\mathbb{F}_p$), as this implies $(G \colon H_n) < \infty$.

Let

$$\Gamma^* = \{X \in \Gamma \colon L_X \subseteq K\}.$$

First observe that, if $X \in T_n$, then $H_n \supseteq G_X$, so $K(H_n) \supseteq K(G_X) \supseteq L_X$. Therefore $T_n \subseteq \Gamma^*$. Next, assuming $X, Y \in \Gamma^*$ we obtain

$$L_{XY} = [L_X, L_Y] \subseteq [K, K] \subseteq K,$$

and thus $XY \in \Gamma^*$. It follows that Γ^* is a sub-semigroup of Γ containing T_n. Hence $\Gamma^* \supseteq \langle T_n \rangle = \Gamma_n$.

Applying Lemma 4.5 we conclude that Γ^* is cofinite in Γ, and this implies that $\dim(L/K) < \infty$, as required. ∎

The simplest example of a pro-p group of infinite rank and finite lower rank obtained in this manner is $G = \mathrm{SL}_2^1(\mathbb{F}_p[[t]])$. Our proof gives $\underline{L}_d(G) \leq 6$ in this case. However, by a more delicate analysis we can show that $\underline{L}_d(G) \leq 3$. It is not clear whether the lower rank is 2 or 3 in this case (in fact the two authors have conflicting views on this matter).

Nevertheless, non p-adic analytic pro-p groups of lower rank 2 do exist: it is shown in [LGSW] that, for $p \geq 5$, the Nottingham group $\mathrm{Nott}(p)$ has lower rank 2.

5. Golod–Shafarevich inequalities

In this section we consider presentations of Λ-perfect groups. We do not know whether they are always finitely presented, but we show that, for $\Lambda = \mathbb{F}_p[[t]]$, this is the case in some typical situations. We also show that Λ-perfect groups always satisfy the Golod–Shafarevich inequality.

A key to this section is the interplay between presentations of pro-p groups and of abstract groups, particularly arithmetic groups over a global field of characteristic p. This interplay is in both directions: we use results on arithmetic groups to deduce finite presentability of certain Λ-perfect groups; and we apply our results on the growth of pro-p groups to deduce the Golod–Shafarevich inequality for certain arithmetic groups.

The connection between presentations of pro-p groups and abstract groups is based on the following easy but crucial lemma from [Lu1].

LEMMA 5.1: *Let Γ be an abstract group with a presentation $\langle X; R\rangle$ where X is a finite set of generators, and R is a set of relations. Let $\Gamma_{\hat{p}}$ be the pro-p completion of Γ.*

1. *$\langle X; R\rangle$ is a presentation of $\Gamma_{\hat{p}}$ in the category of pro-p groups.*
2. *If $d(\Gamma_{\hat{p}}) < |X|$, then $\Gamma_{\hat{p}}$ has a presentation with $d(\Gamma_{\hat{p}})$ generators and $|R| - (|X| - d(\Gamma_{\hat{p}}))$ relations.*

Let G be a simply connected simple Chevalley group and let k be a global field of characteristic p. Let S be a finite set of primes (i.e. valuations) of k. Set

$$\mathcal{O}_S = \{x \in k\colon v(x) \geq 0 \text{ for every } v \in S\}.$$

Given $q = p^e$, choose S and a fixed valuation v_0 such that $|S| \geq 3$, $v_0 \notin S$, and the residue field of v_0 is $\mathbb{F}_q$. Let K be the completion of k with respect to v_0. Then K is isomorphic to $\mathbb{F}_q((t))$, and the completion $(\mathcal{O}_S)_{v_0}$ of $\mathcal{O}_S$ with respect to v_0 is isomorphic to $\mathbb{F}_q[[t]]$.

Let $\Gamma = G(\mathcal{O}_S)$. Since $|S| \geq 3$ it follows from results of Behr [B1,B2] that Γ is finitely presented. Γ is dense in $G((\mathcal{O}_S)_{v_0}) \cong G(\mathbb{F}_q[[t]])$.

Denote

$$G^1 = \operatorname{Ker}(G(\mathbb{F}_q[[t]]) \longrightarrow G(\mathbb{F}_q)),$$

and

$$\Gamma^1 = \Gamma \cap G^1.$$

Now, $G(\mathcal{O}_S)$ has the strong approximation property [Pr] and satisfies the congruence subgroup property [Ra]. Hence

$$\widehat{G(\mathcal{O}_S)} \cong G(\widehat{\mathcal{O}_S}) \cong \prod_{v \notin S} G((\mathcal{O}_S)_v).$$

Then

$$\widehat{\Gamma^1} = \prod_{v \notin S \cup \{v_0\}} G((\mathcal{O}_S)_v) \times G^1((\mathcal{O}_S)_{v_0}).$$

Note that $G^1((\mathcal{O}_S)_{v_0})$ is a pro-p group; in fact in most cases (see [We, Lemma 5.2]) $G^1((\mathcal{O}_S)_{v_0})$ is a Λ-perfect group, where $\Lambda = \mathbb{F}_q[[t]]$.

On the other hand, $G((\mathcal{O}_S)_v)$ has no pro-p quotient for almost every v, for otherwise C_p^∞ would be a quotient of $G(\mathcal{O}_S)$, which is impossible (as $G(\mathcal{O}_S)$ is finitely generated).

Now, the pro-p completion $\Gamma^1_{\hat{p}}$ of Γ^1 is the maximal pro-p quotient of $\widehat{\Gamma^1}$. The above decomposition of $\widehat{\Gamma^1}$ therefore implies that

$$\Gamma^1_{\hat{p}} = G^1((\mathcal{O}_S)_{v_0}) \times B,$$

where B is a finitely generated pro-p group (in most cases B is finite or even trivial).

As mentioned above, Γ – and hence Γ^1 – is a finitely presented abstract group. Thus $\Gamma^1_{\hat{p}}$ is a finitely presented pro-p group (see 5.1). Since

$$G^1(\mathbb{F}_q[[t]]) \cong G^1((\mathcal{O}_S)_{v_0}) \cong \Gamma^1_{\hat{p}}/B$$

and B is finitely generated, we see that $G^1(\mathbb{F}_q[[t]])$ is finitely presented as a pro-p group.

Without aiming at the most general result, we can now deduce:

PROPOSITION 5.2: *Let G be a Chevalley group scheme (e.g. $G = \mathrm{SL}_m$), and $G^1 = \mathrm{Ker}(G(\mathbb{F}_q[[t]]) \longrightarrow G(\mathbb{F}_q))$. Then G^1 is a finitely presented pro-p group.*

Remark 5.3: G^1 above is an $\mathbb{F}_q[[t]]$-standard group; as such it is $\mathbb{F}_q[[t]]$-perfect, except when $q = 2^e$ and $G = A_1$ or C_n.

We do not know whether Proposition 5.2 holds also for rings Λ of Krull dimension larger than 1.

We now turn to the Golod–Shafarevich inequality, established originally for finite p-groups, and then for wider classes of pro-p groups. It is now known for p-adic analytic pro-p groups (see [K],[Lu1]), for soluble pro-p groups (Wilson [W]), and for pro-p groups which do not have non-abelian free abstract subgroups (Wilson and Zelmanov [WZ]). The following result establishes the Golod–Shafarevich inequality for a new class of pro-p groups.

PROPOSITION 5.4: *Let G be a Λ-perfect group and $\langle X; R\rangle$ a minimal pro-p presenation of G (i.e. $|X| = d(G)$). Then $|R| \geq |X|^2/4$.*

Proof: Let $r_n = r_n(G)$ be as in section 3. It follows from [Lu1] that the convergence of $\sum r_n z^n$ for $0 \leq z < 1$ already implies the Golod–Shafarevich inequality for G. In particular, subexponential growth of $\{r_n\}$ suffices. The desired conclusion now follows from Corollary 3.7. ∎

A Golod-Shafarevich inequality for a pro-p completion of an abstract group Γ implies a similar inequality for Γ, as shown in [Lu1]. By combining the current discussion with the arguments from [Lu1], it is easy to deduce the following corollary for abstract groups. Define $d_{ab}(\Gamma) = d(\Gamma^{ab}) = d(\Gamma/\Gamma')$, and $\mathrm{def}(\Gamma) = \sup\{|X| - |R|\}$ where $\langle X; R\rangle$ ranges over all presentations of Γ.

PROPOSITION 5.5: *Let G be a Chevalley group scheme, and let $k, \mathcal{O}_S$ be as before. Suppose $\sum_{v\in S} \mathrm{rank}(G(k_v)) \geq 2$, and that if $\mathrm{char}(k) = 2$ then $G \neq A_1, C_n$. Let Γ be a finite index subgroup of $G(\mathcal{O}_S)$.*

(1) *If $\langle X; R\rangle$ is a presentation of Γ, then*

$$|R| \geq d_{ab}(\Gamma)^2/4 + |X| - d_{ab}(\Gamma).$$

(2)

$$\liminf\{\mathrm{def}(\Delta)\colon \Delta \textit{ a finite index subgroup of } \Gamma\} = -\infty.$$

This extends Theorem 4.2 of [Lu1], dealing with the characteristic 0 case. We omit the detailed proof, and instead make two remarks. The first is that the pro-p completion of Γ in the proposition is not necessarily an $\mathbb{F}_q[[t]]$-standard group, but it is commensurable with such. Using arguments from the end of section 3 it is easy to show that subexponential growth of $\{r_n\}$ is inherited by commensurable groups. Consequently, a group which is commensurable to a Λ-perfect group will also satisfy the Golod–Shafarevich inequality. The second remark is that the exclusion of $p = 2$ and $G = A_1, C_n$ is very likely not needed. To cover this case one needs to generalize the theory developed in section 3 in order to deal with Λ-standard groups which are not Λ-perfect, but are 'nearly

Λ-perfect' in some sense (e.g. finitely generated). Some preliminary results in this direction were recently obtained by Inga Levich.

6. Deformations of Galois representations

Let S be a finite set of rational primes, and $G = G_{\mathbb{Q},S}$ the Galois group over $\mathbb{Q}$ of a maximal algebraic extension of $\mathbb{Q}$ unramified outside S. In [M] Mazur (following some ideas of Hida) initiated a systematic study of the collection of p-adic representations $\rho: G \longrightarrow \mathrm{GL}_n(\mathbb{Z}_p)$ lifting a given representation $\overline{\rho}: G \longrightarrow \mathrm{GL}_n(\mathbb{F}_p)$. In particular he showed the existence of a universal lift $\widetilde{\rho}: G \longrightarrow \mathrm{GL}_n(\Lambda)$ where Λ is a complete Noetherian local ring of the type discussed here.

In [Bo] Boston considers the case $n = 2, p > 2$ and S containing p. He denotes by K the fixed field of $\mathrm{Ker}\rho$ and by L the maximal pro-p extension of K unramified outside the places above S. As $\mathrm{Ker}(\mathrm{GL}_2(\Lambda) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p))$ is a pro-p group, it follows that the universal representation $\widetilde{\rho}$ factors through $\mathrm{Gal}(L/\mathbb{Q})$. Boston posed the following:

Conjecture A (non-injectivity) [Bo,p.186]. The universal deformation $\widetilde{\rho}: \mathrm{Gal}(L/Q) \longrightarrow \mathrm{GL}_2(\Lambda)$ is never injective.

As a method to prove the conjecture he posed a second one which implies the first:

Conjecture B [Bo,p.187]. If P is a finitely generated pro-p subgroup of $\mathrm{GL}_2(\Lambda)$, where Λ has Krull dimension r, then there is a constant C (depending on P) such that

$$d(U) \leq C(P: U)^{\frac{r-1}{r}}$$

for all subgroups $U \subseteq_o P$.

In other words, this means that $g_n(P) \leq Cn^{(r-1)/r}$ for all n.

Let us first consider conjecture B, starting with the case $r = 1$. While it is certainly true in characteristic zero (as observed in [Bo]), it is false in characteristic p, since $\mathbb{F}_p[[t]]$-standard groups have infinite rank (see 2.7,2.8).

In the general case, if P is an open subgroup of a Λ-perfect group, then Theorem 4.3 provides a logarithmic bound on $g_n(P)$, which is obviously sharper than the bound appearing in conjecture B whenever $r > 1$. On the other hand, the following example shows that for arbitrary closed subgroups no bound better than the trivial linear one exists.

Example 6.1: Let $\Lambda = \mathbb{F}_p[[t]]$ and let P be the closed subgroup of $\mathrm{GL}_2(\Lambda)$ generated by the matrices

$$\begin{pmatrix} 1+t & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

It is straightforward to verify that

$$P \cong C_p \wr \mathbb{Z}_p = \varprojlim C_p \wr C_{p^m}.$$

Let $K_m = \mathrm{Ker}(P \longrightarrow C_{p^m})$. Then $(P\colon K_m) = p^m$ and $d(K_m) = p^m$. Thus $g_n(P) \geq n$ for all pth powers n.

We note that this construction can be immitated over any ring Λ which is not a finitely generated p-adic module; indeed, factoring out $p\Lambda$ we may assume that Λ is an infinite complete local ring of characteristic p, so it has a subring isomorphic to $\mathbb{F}_p[[t]]$.

The next result settles conjecture A of Boston in the affirmative.

PROPOSITION 6.2: *The universal representation $\widetilde{\rho}$: $\mathrm{Gal}(L/K) \longrightarrow \mathrm{GL}_2(\Lambda)$ is not injective.*

Proof: Let $P = \mathrm{Ker}(\mathrm{Gal}(L/K) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p))$. Then P is a pro-p group; as shown in [Bo] (see Proposition 3.1 there, or remark 3 on p.187) $\mathrm{def}(P) \geq 2$, i.e. P has a representation with at least two more generators than relators. By a theorem of Romanovskii [R] this implies that two of the generators of P generate a free (non-abelian) pro-p group F. By a result of Zubkov [Zu] such a group F cannot be embedded in $\mathrm{GL}_2(\Lambda)$. Since $F \subseteq \mathrm{Gal}(L/K)$, the map $\widetilde{\rho}$ cannot be injective. ∎

As mentioned in section 3, we conjecture that non-abelian free pro-p groups cannot be embedded in $\mathrm{GL}_n(\Lambda)$ for any n and Λ. This would extend the above proposition for n-dimensional representations.

References

[AM] M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Massachusetts, 1969.

[B1] H. Behr, *Finite presentability of arithmetic groups over global function fields*, Proc. Edinburgh Math. Soc. **30** (1987), 23–39.

[B2] H. Behr, *Arithmetic groups over function fields*, preprint.

[Be] A.E. Bereznyi, *Discrete subexponential groups*, J. Soviet Math. **28** (1985), 570–579.

[Bo] N. Boston, *Explicit deformation of Galois representations*, Invent. Math. **103** (1991), 181–196.

[B] N. Bourbaki, *Lie Groups and Lie Algebras*, Chapters 1–3, Springer, Berlin, 1980.

[DDMS] J. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, London Math. Soc. Lecture Note Series 157, Cambridge University Press, Cambridge, 1991.

[G] R.I. Grigorchuk, *On the Hilbert–Poincaré series of graded algebras associated with groups*, Math. USSR Sbornik **66** (1990), 211–229.

[H] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.

[I] I. Ilani, *Counting finite index subgroups and the P. Hall enumeration principle*, Israel J. Math. **68** (1989), 18–26.

[J] N. Jacobson, *Lie Algebras*, Wiley-Interscience, New York, 1962.

[K] Koch, *Zum Satz von Golod–Safarevic*, Math. Nachr. **42** (1969), 321–333.

[La] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. I.H.E.S. **26** (1965), 389–603.

[LGSW] C.R. Leedham-Green, A. Shalev and A. Weiss, *Reflections on the Nottingham group*, in preparation.

[Lu1] A. Lubotzky, *Groups presentations, p-adic analytic groups and lattices in* $SL_2(\mathbb{C})$, Ann. Math. **118** (1983), 115–130.

[Lu2] A. Lubotzky, *A group theoretic characterization of linear groups*, J. Algebra **113** (1988), 207–214.

[LM1] A. Lubotzky and A. Mann, *Powerful p-groups. I,II.*, J. Algebra **105** (1987), 484–505 and 506–515.

[LM2] A. Lubotzky and A. Mann, *On groups of polynomial subgroup growth*, Invent. Math. **104** (1991), 521–533.

[M] B. Mazur, *Deforming Galois representations*, in *Galois Groups over* $\mathbb{Q}$, MSRI Publ. no. 16 (Y. Ihara, K. Ribet and J.-P. Serre, eds.), 1989, pp. 385–437.

[Pa] D.S. Passman, *The Algebraic Structure of Group Rings* (new edition), Wiley-Interscience, New York, 1985.

[Pr] G. Prasad, *Strong approximation for semi-simple groups over function fields,* Ann. Math. **105** (1977), 553-572.

[Ra] M.S. Raghunathan, *On the congruence subgroup problem,* Publ. Math. I.H.E.S. **46** (1976), 107–161.

[R] N.S. Romanovskii, *A generalized theorem on freedom for pro-p groups,* Sib. Math. J. **27** (1986), 267–280.

[Se] D. Segal, *Subgroups of finite index in soluble groups I,* in *Proc. Groups — St Andrews 1985*, London Math. Soc. Lecture Note Series No. 121, pp. 307–314, Cambridge University Press, Cambridge, 1986.

[SS] D.Segal and A. Shalev, *Groups with fractionally exponential subgroup growth,* J. Pure Appl. Algebra, to appear.

[S] J.-P. Serre, *Lie groups and Lie algebras* (new edition), Lecture Notes in Math. 1500, Springer, Berlin, 1991.

[Sh] A. Shalev, *Growth functions, p-adic analytic groups, and groups of finite coclass,* J. London Math. Soc. **46** (1992), 111–122.

[St] R.P. Stanley, *Hilbert functions of graded algebras,* Adv. in Math. **28** (1978), 57–83.

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

[W] J.S. Wilson, *Finite presentations of pro-p groups and discrete groups,* Invent. Math. **105** (1991), 177–183.

[WZ] J.S. Wilson and E.I. Zelmanov, *Identities for Lie algebras of pro-p groups,* J. Pure Appl. Algebra **81** (1992), 103–109.

[Y] I.O. York, *The ring of formal power series under substitution,* Ph.D. thesis, Nottingham University, 1990.

[Zu] A. Zubkov, *Non-abelian free pro-p groups cannot be represented by 2-by-2 matrices,* Sib. Math. J. **28** (1987), 742–747.