On linearity of finitely generated $R$-analytic groups

A. Jaikin-Zapirain
Departamento de Matemáticas Facultad de Ciencias
Universidad Autónoma de Madrid

Abstract
We prove that if $R$ is a commutative Noetherian local pro-$p$ domain of characteristic 0 then every finitely generated $R$-standard group is $R$-linear.

1 Introduction
Let $R$ be a commutative Noetherian local pro-$p$ domain and $m$ its maximal ideal. The concept of an $R$-analytic group is defined in [3, Chapter 13], where it is shown that if $R$ satisfies some additional technical conditions, then every such group contains an open subgroup which is $R$-standard. To recall what this means, let $G$ be an $R$-standard group. Then the underlying set of $G$ may be “identified” with the cartesian product $(m^l)^{(d)}$ of $d$ copies of $m^l$, for some $l \in \mathbb{N}$. The number $d \geq 0$ is the dimension of $G$ and $l > 0$ is the level of $G$. The group operation is given by a formal group law, i.e. a $d$-tuple $F = (F_1, \ldots, F_d)$ of power series over $R$ in $2d$ variables, as follows: for all $x, y \in G = (m^l)^{(d)}$ we have

$$x \cdot y = (F_1(x, y), \ldots, F_d(x, y)).$$

The neutral element of $G$ is $e = (0, \ldots, 0)$. Without loss of generality we will always assume that the level of $G$ is 1. We shall write $G(I)$ for $(I)^{(d)} \subset G$ and $G_i$ will denote $G(m^i)$. Hence $G = G_1 = G(m)$.

The $Z_p$-analytic pro-$p$ groups are well-understood (see [7, 8]) and they are linear over $Z_p$. It was conjectured that $R$-analytic pro-$p$ groups are $R$-linear. Since compact $Z_p$-analytic groups are finitely generated, it is natural to consider first finitely generated $R$-analytic pro-$p$ groups. In [5] it was proved that just infinite $R$-analytic groups are $R$-linear. As an $R$-analytic group contains an open $R$-standard subgroup, we can restrict our attention to $R$-standard groups. In [2] the linearity of $Z_p[[t]]$-perfect groups is shown. Recall that an $R$-standard

*This work has been partially supported by the FEDER, the MCYT Grants BFM2001-0201, BFM2001-0180 and the Ramón y Cajal Program.
group of level \( l \) is called \( R \)-perfect if \([G, G] = G_{2l}\). Note that \( R \)-perfect groups are finitely generated. In this work we prove:

**Theorem 1.1.** Let \( R \) be commutative Noetherian local pro-\( p \) domain of characteristic 0 and \( G \) a finitely generated \( R \)-standard group. Then \( G \) is \( R \)-linear.

Note that if a pro-\( p \) group is finitely generated and \( R \)-linear, then it is a closed subgroup of \( \text{GL}_n(R) \) for some \( n \). In the following we will use the notion \( R \)-linear only for closed subgroups of \( \text{GL}_n(R) \).

First at all in Section 2 we prove some new results about \( t \)-linear pro-\( p \)-groups. In Section 3 we shall describe the Lie algebra \( \mathbb{L} = \mathbb{L}(G) \) of an \( R \)-standard group \( G \). The typical definition is based on the formal group law of \( G \). We shall introduce another definition coming from the theory of algebraic groups and define \( \mathbb{L} \) as the set of left invariant derivations of \( A = R[[x_1, \ldots, x_d]] \). We shall prove that these two definitions are equivalent (it is a folklore result, however, I do not know any reference for it in the literature). In Section 4 assuming that the characteristic of \( R \) is 0, we use the BCHF to define on \( p\mathbb{L} \) (here \( p = p(p) = 4 \) if \( p = 2 \) and \( p = p \) if \( p \) is an odd prime) a group structure. We show that the obtained group is isomorphic to \( G(pR) \). In Section 5 we show that if an \( R \)-standard group is finitely generated, then the radical of \( \mathbb{L}(G) \) is nilpotent. It will permit us use the Weigel result about linearity of some Lie rings which we describe in Section 6. In Section 7 we finish the proof of Theorem 1.1.

## 2 Some results about \( t \)-linear pro-\( p \) groups

Recall the definition of \( t \)-linear pro-\( p \) groups from [5].

**Definition.** Let \( G \) be a pro-\( p \) group. We shall say that \( G \) is \( t \)-linear if it is a closed subgroup of \( \text{GL}_n(A) \) for some commutative profinite ring \( A \).

In [5 Theorem 4.1] it was shown that if \( G \) is a finitely generated \( t \)-linear pro-\( p \) group, then \( G \) is linear over some commutative Noetherian local pro-\( p \) ring. In this section we extend this result. If \( R \) is a ring, we denote by \( K \dim R \) the Krull dimension of \( R \).

**Theorem 2.1.** Let \( G \) be a finitely generated pro-\( p \) group and suppose that \( G \) is linear over some commutative Noetherian local pro-\( p \) domain \( R \). Then we have

1. If \( \text{char } R = 0 \) and \( K \dim R > 2 \), then \( G \) is linear over every commutative Noetherian local pro-\( p \) domain of characteristic zero and Krull dimension greater than 2.

2. If \( \text{char } R = 0 \) and \( K \dim R \leq 2 \), then \( G \) is linear over every commutative Noetherian local pro-\( p \) domain of characteristic zero and Krull dimension greater or equal than of \( R \).

3. If \( \text{char } R = p \) and \( K \dim R \geq 2 \), then \( G \) is linear over every commutative Noetherian local pro-\( p \) domain \( R \) of characteristic \( p \) and Krull dimension greater than 1.
We see that the last theorem reduces the study of linear over pro-$p$ domains pro-$p$ groups to study of $R$-linear pro-$p$ groups, where $R = \mathbb{Z}_p[[t_1, t_2]]$ or $R = \mathbf{F}_p[[t_1, t_2]]$.

One of the main steps in the proof of the previous theorem is the following proposition. We also will use it in the proof of our main result.

**Theorem 2.2.** Let $R$ be a commutative Noetherian local pro-$p$ domain and $W$ a finitely generated $R$-torsion-free $R$-module. Suppose $G \leq \text{Aut}_R(W)$. Then there exists a commutative Noetherian local pro-$p$ domain $S$, satisfying $\text{char} S = \text{char} R$ and $K \text{dim} S = K \text{dim} R$, such that $G$ is $S$-linear. Moreover, if $R$ is regular, then $S = R$.

First we need some auxiliary results. In the following $R$ is always a commutative Noetherian local pro-$p$ domain.

**Lemma 2.3.** Let $a \neq 0, r \in R$ and $T = R[[t]]/(at - r)$. Then the Krull dimensions of $R$ and $T$ are the same.

**Proof.** First note that $K \dim R[[t]] = K \dim R + 1$ and since $R[[t]]$ is domain $K \dim R[[t]]/(at - r)$ is strictly less than $K \dim R[[t]]$. Hence $K \dim R[[t]]/(at - r) \leq K \dim R$.

On the other hand, $K \dim T$ is equal to the number of elements in a system of parameters of $T$ (see [8, p.27]), and this number is at least $K \dim R[[t]] - 1$. This implies $K \dim R[[t]]/(at - r) \geq K \dim R$. \qed

Recall that a (multiplicative non-archimedean) valuation of a field $D$ is a mapping $v: D \to \mathbb{R}_{\geq 0}$ such that for $a, b \in D$.

(i) $v(a) = 0$ if and only if $a = 0$.
(ii) $v(ab) = v(a)v(b)$.
(iii) $v(a + b) \leq \max(v(a), v(b))$.

We need the following proposition:

**Proposition 2.4.** ([8, Proposition 11.9]) Let $R$ be a subring of a field $D$ and $m$ a non-trivial ideal of $R$. Then there exists a valuation $v$ of $D$ such that $v(r) \leq 1$ for every $r \in R$ and $v(m) < 1$ for every $m \in m$.

**Lemma 2.5.** Let $S$ be the integrally closure of $R$. Then $S$ is also a commutative Noetherian local pro-$p$ ring of same characteristic and same Krull dimension as $R$.

**Proof.** First we want to see that $S$ is local. Let $D$ be the quotient field of $R$ and $v$ a valuation from Proposition 2.4. If $s \in S$ then $v(s) \leq 1$, because $s$ is integral over $R$. In order to see that $S$ is local it is enough to show that if $v(s) = 1$ then $s$ is invertible in $S$. Let $f(t) = \sum_{i=0}^{n} a_i t^i$ be a monic irreducible over $R$ polynomial such that $f(s) = 0$. Since $v(s) = 1$, there exists $a_i$, $i < n$, such that...
Proof of Theorem 2.2. Let $a \notin m$. Therefore, since $R$ is a Henselian ring (see [5, Theorem 30.3]), we have that $a_0 \notin m$. Hence $s^{-1} \in S$.

Finally, by [5, Theorem 32.1], $S$ is a finite extension of $R$, whence their Krull dimensions coincide.

**Theorem 2.6.** Let $R$ be a commutative Noetherian local pro-$p$ domain and $a \in R$. Then there are a commutative Noetherian local pro-$p$ domain $S$ and an injective homomorphism $\phi : R \to S$ such that

(i) $\phi(m^k) \subseteq \phi(a)S$ for some $k \in \mathbb{N}$;

(ii) $S$ is integrally closed and its Krull dimension is the same as of $R$.

Moreover, if $R$ is regular, then $S = R$.

**Proof.** Let $D$ be the quotient field of $R$ and $v$ a valuation from Proposition 2.4. Let $\Omega$ be a completion of $D$ respect to $v$. Since $R$ is Noetherian, there exists $s = \max\{v(r) | r \in m\} < 1$ Let $k$ be such that $s^k/v(a) < 1$ and put $S_1 = R[[m^k/a]] \subseteq \Omega$. It is clear that $S_1$ is a local pro-$p$ ring. Moreover, if $t_1, \ldots, t_m$ are generators of $m^k$ as $R$-module, then $S_1 = R[[t_1/a, \ldots, t_m/a]]$. Hence $S_1$ is Noetherian. Applying several times Lemma 2.8, we obtain that its Krull dimension is the same as of $R$. Finally, let $S$ be the integral closure of $S_1$. Theorem follows from Lemma 2.8.

If $R = A[[t_1, \ldots, t_j]]$, where $A$ is equal to $F_q$ or to a finite extension of $\mathbb{Z}_p$, then the homomorphism $\phi : R \to S$ is defined by means of $\phi(t_i) = at_i$. $\square$

**Proof of Theorem 2.9.** Let $D$ be the field of quotients of $R$. Consider the $D$-module $M = D \otimes_R W$. Since $W$ is $R$-torsion-free, we can see $W$ as an $R$-submodule of $M$.

Let $m_1, \ldots, m_r$ be a $D$-basis of $M$ lying in $W$. Put $N = \sum Rm_i$. It is clear that $N$ is a free $R$-module. Let $a \neq 0$ be such that $aW \subseteq N$. By the previous result, there are a commutative Noetherian local pro-$p$ ring $S$ and an injective homomorphism $\phi : R \to S$ such that $\phi(m^k) \subseteq \phi(a)S$ for some $k \in \mathbb{N}$. Moreover, if $R$ is regular, then $S = R$.

Put $W_1 = m^k W$ and $G_1 = \{g \in G | gw \equiv w \pmod{W_1} \text{ for every } w \in W\}$. It is clear that $G_1$ is of finite index in $G$ and $G$ acts faithfully on $W_1$. Define $L = S \otimes_R N$. We have $L$ is a free $S$-module.

Now we embed $W_1$ in $L$ in the following way. Let $w \in W_1$. Then $w = \sum_{i=1}^r a^{-1}k_im_i$, where $k_i \in m^k$. Define $\psi(w) = \sum_{i=1}^r \phi(a)^{-1}\phi(k_i) \otimes m_i$ (since $S$ is domain and $\phi(m^k) \subseteq \phi(a)S$, we can speak about $\phi(a)^{-1}\phi(k_i) \in S$). The map $\psi$ is an $R$-homomorphism. So we can see $W_1$ as $R$-submodule of $L$.

Now, we explain how we can extend the action of $G_1$ on $L$. Let $g \in G_1$ and $l = \sum_{i=1}^r s_im_i$. Define $gl = \sum_{i=1}^r s_igm_i$. Note that, since $g \in G_1$, $gm_i \in W_1 + N$, so the definition is correct. This action gives an embedding $G_1 \leq \text{Aut}_S(L) \cong \text{GL}_r(S)$. Since $G_1$ is of finite index in $G$, $G$ is also $S$-linear. $\square$
Proof of Theorem 2.1. By the structure theorem of complete local rings (see [8, Corollary 31.6]), $R$ is a finite extension of a regular ring $T = \mathbb{Z}_p[[t_1, \ldots, t_k]]$ or $T = \mathbb{F}_p[[t_1, \ldots, t_k]]$ for some $k$. Hence, $G \in \text{Aut}_T(R^n)$ for some $n$, and Theorem 2.2 implies that $G$ is $T$-linear. Note that the Krull dimensions of $R$ and $T$ are the same.

1. If $\text{char } T = 0$ and $K \dim T > 2$, then by Remark VII.10.4 of [11], we can embed $T = \mathbb{Z}_p[[t_1, \ldots, t_k]]$ into $\mathbb{Z}_p[[s_1, s_2]]$. On the other hand $\mathbb{Z}_p[[s_1, s_2]]$ can be embedded into every commutative Noetherian local pro-$p$ domain $S$ of characteristic zero and Krull dimension greater than 2, and so $G$ is also $S$-linear.

The proofs of 2. and 3. follow the same ideas.

3 Lie algebra of an $R$-standard group

We use the notation of Section 1. So $G$ is an $R$-standard group of level 1. The law $F$ can be written in the form

$$F(x, y) = x + y + B(x, y) + O'(3),$$

where $B$ is the sum of the all polynomials in $x$ and $y$ of degree 2 and the expression $O'(n)$ stands for any power series in which every term has total degree at least $n$ and has degree at least 1 in each variable. We know, see, for example, [9, p.26], that if $C(x, y) = B(x, y) - B(y, x)$, then $(R^{(d)}, +, C)$ is a Lie $R$-algebra, and we shall denote this Lie algebra by $L = L(G)$.

Now, let $A = R[[x_1, \ldots, x_d]]$. Since $G$ is identified with $m^{(d)}$, $A$ can be considered as a subring of the ring of functions from $G$ to $R$. Note that since $R$ is domain, two different elements from $A$ give us two different functions. Define two actions of $G$ on $A$ via left and right translation:

$$(\lambda_x f)(y) = f(x^{-1}y), \quad (\rho_x f)(y) = f(yx),$$

where $f \in A$, $x, y \in G$. Since the multiplication in $G$ is given by an analytic function, we have that if $f \in A$ then $\lambda_x f$ and $\rho_x f$ also belong to $A$.

The bracket of two $R$-derivations of $A$ is again a derivation. Therefore, Der $A$ is a Lie algebra. So is the subspace of left invariant derivations Der$_l A = \{ w \in \text{Der } A \mid w\lambda_x = \lambda_x w \text{ for all } x \in G \}$, since the bracket of two derivations which commute with $\lambda_x$ obviously does likewise. The next theorem is the main result of this section:

**Theorem 3.1.** The Lie $R$-algebras $L$ and Der$_l A$ are isomorphic.

Before the proof of the theorem we need to do some preliminary work.
Lemma 3.2. Let $w_1, w_2 \in \text{Der}_l A$ and $f \in A$. Then we have

$$w_1(f)(y) = \sum_{i=1}^{d} \frac{\partial f(yx)}{\partial x_i} \bigg|_{x=e} w_1(x_i)(e),$$

$$w_2(w_1(f))(z) = \sum_{i,j=1}^{d} \frac{\partial^2 f(zyx)}{\partial x_i \partial y_j} \bigg|_{(x,y)=(e,e)} w_1(x_i)(e)w_2(x_j)(e).$$

Proof. We prove only the first equality, because the second one is obtained applying two times the first.

$$w_1(f)(y) = (\lambda_y^{-1} w_1(f(x)))(e) = w_1(\lambda_y^{-1} f(x))(e) = w_1(f(yx))(e)$$

$$= \sum_{i=1}^{d} \frac{\partial f(yx)}{\partial x_i} \bigg|_{x=e} w_1(x_i)(e).$$

Proof of Theorem 3.1. Define an $R$-homomorphism $\phi : \text{Der}_l A \rightarrow L$ as follows

$$\phi(w) = (w(x_1)(e), \ldots, w(x_d)(e)), w \in \text{Der}_l A.$$ 

First we will show that $\phi$ is a bijective map. Fix $(a_1, \ldots, a_d) \in L$ and define $w \in \text{End}_R(A)$ by means of

$$w(f)(y) = \sum_{i=1}^{d} \frac{\partial f(yx)}{\partial x_i} \bigg|_{x=e} a_i, f \in A.$$ 

If $f_1, f_2 \in A$, then

$$w(f_1f_2)(y) = \sum_{i=1}^{d} \frac{\partial f_1(yx)f_2(yx)}{\partial x_i} \bigg|_{x=e} a_i$$

$$= \sum_{i=1}^{d} \frac{\partial f_1(yx)}{\partial x_i} \bigg|_{x=e} f_2(y) a_i + \sum_{i=1}^{d} \frac{\partial f_2(yx)}{\partial x_i} \bigg|_{x=e} f_1(y) a_i$$

$$= w(f_1)(y)f_2(y) + f_1(y)w(f_2)(y).$$

This implies that $w$ is a derivation of $A$. Now, if $z \in G$, then

$$w(\lambda_z f)(y) = \sum_{i=1}^{d} \frac{\partial (\lambda_z f)(yx)}{\partial x_i} \bigg|_{x=e} a_i$$

$$= w(f)(z^{-1}y) = (\lambda_z w(f))(y).$$

Hence, we obtain that $w$ is really a left invariant derivation. Define the constructed map from $L$ to $\text{Der}_l(A)$ by $\psi$. Note that if $w \in \text{Der}_l(A)$, then we
have
\[
\psi(\phi(w))(f)(y) = \psi(w(x_1)(e), \ldots, w(x_d)(e))(f)(y)
\]
\[
= \sum_{i=1}^d \frac{\partial f(yx)}{\partial x_i} \bigg|_{x=e} w(x_i)(e)
\]
\[
= w(\lambda_{y-1} f)(e) = \lambda_{y-1} w(f)(e) = w(f)(y).
\]

On the other hand if \(a = (a_1, \ldots, a_d) \in L\), then
\[
\phi(\psi(a)) = (b_1, \ldots, b_d),
\]
where \(b_k = \sum_{i=1}^d \frac{\partial F_k(y, x)}{\partial x_i} \bigg|_{x=e} a_i = a_k\). Hence \(\psi(\phi(a)) = a\). We conclude that \(\phi\) is a bijection.

We shall see now that \(\phi\) is also a homomorphism of Lie rings.

Let \(w_1, w_2 \in \text{Der}_l(A)\). From the previous lemma, we obtain that
\[
\phi([w_1, w_2]) = (c_1, \ldots, c_d),
\]
where
\[
c_k = \sum_{i,j=1}^d \frac{\partial^2 F_k(y, x)}{\partial x_i \partial y_j} \bigg|_{(x, y) = (e, e)} (w_2(x_i)(e)w_1(x_j)(e) - w_1(x_i)(e)w_2(x_j)(e)).
\]

We conclude that \(\phi([w_1, w_2]) = C(\phi(w_1), \phi(w_2))\). \(\square\)

Remark 3.3. Note that the previous proof also gives an identification of \(\text{Der}_l(A)\) with \((I/I^2)^* = \text{End}_R(I/I^2, R)\). The derivation \(w\) is identified with the map \(f \rightarrow w(f)(e)\).

In the rest of the work we shall use the letter \(L\) for \(\text{Der}_l(A)\).

4 An application of the Baker-Campbell-Hausdorff Formula

The Baker-Campbell-Hausdorff Formula (BCHF) is \(H(x_1, x_2) = \log(e^{x_1}e^{x_2})\) regarded as a formal power series in two non-commuting variables. Equivalently, this is a formal power series \(H(x_1, x_2)\) such that
\[
e^{H(x_1, x_2)} = e^{x_1}e^{x_2}.
\]

The homogeneous component of \(H(x_1, x_2)\) of degree \(n\) is denoted by \(H_n(x_1, x_2)\), so that \(H(x_1, x_2) = \sum_{n=1} H_n(x_1, x_2)\). The main fact about the BCHF is that \(H_n(x_1, x_2)\) is a Lie word in \(x_1\) and \(x_2\) (see, for example, [5, Theorem 9.11]).

Let \(\{e_i\}\) be a \(\mathbb{Z}\)-basis of the free Lie algebra generated by \(x_1\) and \(x_2\), consisting of simple commutators. Then we can express \(H_n\) as \(H_n = \sum \lambda_{k,n} e_k\), for some
\( \lambda_{k,n} \in \mathbb{Q} \). We need the following fact about the coefficients \( \lambda_{k,n} \) (Proposition II.8.1):

\[
v_p(\lambda_{k,n}) \geq -(n-1)/(p-1),
\]

where \( v_p(ap^s) = s \) if \((a,p) = 1\).

**Theorem 4.1.** Let \( M \) be a Lie \( \mathbb{Z}_p \)-algebra without \( \mathbb{Z}_p \)-torsion and suppose that \( \cap_{i=0}^\infty p^i M = 0 \). If \( M \) is complete in the topology induced by the filtration \( p^i M \), then

(i) If \( a, b \in pM \), then \( H_n(a, b) \in pM \) and \( \lim_{n \to \infty} H_n(a, b) = 0 \) (in particular, we can compute \( H(a, b) \));

(ii) \((pM, H)\) is a group.

**Proof.** The first proposition of the theorem follows directly from the formula (1).

Since \( H(a, 0) = H(0, a) = a \) and \( H(a, -a) = 0 \) for any \( a \in pM \), then in order to prove the second statement, we only need to show that the operation \( H(x_1, x_2) \) is associative.

Let \( F \) be the \( \mathbb{Q}_p \)-algebra of formal power series in the non-commuting variables \( x_1, x_2, x_3 \). Then we have the following equalities in \( F \):

\[
H(H(x_1, x_2), x_3) = \log(e^{H(x_1, x_2) e^{x_3}}) = \log(e^{x_1 e^{x_2 e^{x_3}}}) = \log(e^{x_1 e^{H(x_2, x_3)} H(x_1, H(x_2, x_3)))}.
\]

In particular, we obtain

\[
H(H(p x_1, p x_2), p x_3) = H(p x_1, H(p x_2, p x_3)).
\]

Let \( L \) be the Lie \( \mathbb{Z}_p \)-subalgebra of \( F^{(-)} \), generated by \( x_1, x_2, x_3 \). It is clear that \( L \) is a free Lie \( \mathbb{Z}_p \)-algebra. Let \( \{ \lambda_k, k \in \mathbb{N} \} \) be a \( \mathbb{Z}_p \)-basis of \( L \) and \( \bar{L} \) be the Lie \( \mathbb{Z}_p \)-subalgebra of \( F^{(-)} \), consisting from the formal power series \( \sum \lambda_k e_k \) with \( \lambda_k \in \mathbb{Z}_p \) and \( \lim_{k \to \infty} (\lambda_k) = +\infty \). We have that \( \bar{L} \) is the completion of \( L \) in the topology induced by the filtration \( p^i L \). By (1), if \( y_1, y_2 \in p\bar{L} \), then \( H(p y_1, p y_2) \in p\bar{L} \).

Now, let \( a, b, c \in M \) and \( \phi : L \to M \) be a Lie \( \mathbb{Z}_p \)-algebra homomorphism defined by means of \( \phi(x_1) = a, \phi(x_2) = b, \phi(x_3) = c \). Since \( M \) is complete in the topology induced by the filtration \( p^i M \), this homomorphism can be extended to \( \phi : L \to M \). Furthermore, \( \phi \) is a continuous map. Then

\[
H(H(pa, pb), pc) = H(H(\phi(p x_1), \phi(p x_2)), \phi(p x_3)) = \phi(H(H(p x_1, p x_2), p x_3)) = H(H(p x_1, H(p x_2, p x_3))).
\]

We conclude that the operation \( H(x_1, x_2) \) is associative and, so, \((pM, H)\) is a group.

We will denote the group \((pM, H)\) by \( \Gamma(pM) \).
There exists $\log \phi$ in the topology induced by the filtration $p^i D$. If $M$ is a closed Lie $\mathbb{Z}_p$-subalgebra of $D^{(-1)}$, then

(i) If $a \in pD$, then $a^n/n! \in pD$ for $n \geq 1$ and $\lim_{n \to \infty} a^n/n! = 0$ (in particular, we can compute $e^a \in 1 + pD$ and $\log(1 + a) \in pD$);

(ii) If $a \in pD$, then $\log(e^a) = a$ and $e^{\log(1+a)} = 1 + a$ (in particular, $e^a = 1$ if and only if $a = 0$);

(iii) $\{e^a | a \in pM\}$ is a group (with multiplication of $D$) isomorphic to $\Gamma(pM)$.

**Proof.** The first statement follows from the fact that $v_p(n!) \leq (n - 1)/(p - 1)$ (see [1, Lemma II.8.1]).

Let $P$ be the subring of $\mathbb{Z}_p[[t]]$, consisting of the series

$$
\sum_i \alpha_i t^i \text{ with } \lim_{i \to \infty} v_p(\alpha_i) = +\infty.
$$

Suppose $f \in tP$. Since $v_p(n!) \leq (n - 1)/(p - 1)$, $e^f \in P$ and $\log(1 + f) \in P$. Let $a = pb$. Define a homomorphism of $\mathbb{Z}_p$-algebras $\phi : \mathbb{Z}_p[t] \to D$, by means of $\phi(t) = b$. Since $P$ is isomorphic to the completion of $\mathbb{Z}_p[t]$ in the topology induced by $p^k\mathbb{Z}_p[t]$, we can extend $\phi$ on $P$. Note that in $P$, the equality $pt = \log(e^{pt})$ holds. Since $\phi$ is continuous, we have

$$
a = \phi(pt) = \phi(\log(e^{pt})) = \log(e^a).
$$

Analogically, $e^{\log(1+a)} = a$. This proves the second proposition.

Since $M$ satisfies the hypothesis of the previous theorem, in order to prove the third statement we have to show that $e^a e^b = e^{H(a,b)}$, for any $a, b \in pM$. The proof of this equality is analogical of the proof of Theorem [1, Lemma II.8.1] and we omit it.

**Lemma 4.3.** Let $D$ be an associative $\mathbb{Z}_p$-algebra without $\mathbb{Z}_p$-torsion and suppose that $\cap_i p^i D = 0$. Assume that $D$ is complete in the topology induced by the filtration $p^i D$. Let $\phi$ be a $\mathbb{Z}_p$-automorphism of $D$ and suppose $(\phi - 1)D \in pD$. Then $\log \phi \in p \text{End}_{\mathbb{Z}_p}(D)$ is well-defined and it is a derivation of $D$.

**Proof.** From the hypothesis on $\phi$ it follows that $\phi \in 1 + p \text{End}_{\mathbb{Z}_p}(D)$. Since $D$ is complete in the topology induced by the filtration $p^i D$, $\text{End}_{\mathbb{Z}_p}(D)$ is complete in the topology induced by the filtration $p^i \text{End}_{\mathbb{Z}_p}(D)$. By the previous theorem there exists $\log \phi$.

Let

$$
f_n(t) = \sum_{i=1}^n \frac{(-1)^{i+1}(t-1)^i}{i} = \sum_i \alpha_i t^i.
$$

Define $d_n = f_n(\phi)$. Note that $\log \phi = \lim_{n \to \infty} d_n$. Then

$$
d_n(ab) = \sum_i \alpha_i \phi^i(a) \phi^i(b) = \sum_{j,k} \beta_{j,k}(\phi - 1)^j(a)(\phi - 1)^k(b),
$$

9
where $\beta_{j,k}$ are coefficients obtained from the following equality:

$$f_n(ts) = \sum_{j,k} \beta_{j,k}(t-1)^j(s-1)^k.$$  

From the definition of $f_n$, it follows that

$$f_n(ts) - f_n(t) - f_n(s) = \sum_{j+k>n} \beta_{j,k}(t-1)^j(s-1)^k.$$  

Hence

$$d_n(ab) - d_n(a)b - ad_n(b) = \sum_{j+k>n} \beta_{j,k}(\phi-1)^j(a)(\phi-1)^k(b)$$

and so

$$(\log \phi)(ab) - (\log \phi)(a)b - a(\log \phi)(b) = \lim_{n \to \infty} d_n(ab) - d_n(a)b - d_n(a)b = 0.$$  

Hence $\log \phi$ is a derivation.  

Using the similar argument we can prove the next lemma

**Lemma 4.4.** Let $D$ be an associative $\mathbb{Z}_p$-algebra without $\mathbb{Z}_p$-torsion and suppose that $\bigcap_i p^iD = 0$. Assume that $D$ is complete in the topology induced by the filtration $p^iD$. Let $\phi$ be a $\mathbb{Z}_p$-derivation of $D$ and suppose $\phi(D) \in pD$. Then $\exp(\phi) \in 1 + p\text{End}_{\mathbb{Z}_p}(D)$ is well-defined and it is an automorphism of $D$.

Let $R$ be a commutative Noetherian local pro-$p$ domain of characteristic 0. We use the notation of the previous section. Suppose that $x \in G(pR)$. Then it is clear that the automorphism $\rho_x$ satisfies the condition: $(\rho_x - 1)A \in pA$, whence $\rho_x \in 1 + p\text{End}_R(A)$. By Lemma 4.3 we have the well-defined derivation $\log(\rho_x) \in p\text{End}_R(A)$. Since $\lambda_y$ and $\rho_x$ commute, $\log(\rho_x) \in pL = p\text{Der}_l(A)$.

From the equality $\exp(\log(\rho_x)) = \rho_x$, we obtain, using Theorem 4.2(iii), that $G(pR)$ can be embedded into $\Gamma(pL)$. In fact, we can prove more:

**Theorem 4.5.** The groups $\{\rho_x|x \in G(pR)\}$ and group $\{e^a|a \in pL\}$ coincide. In particular, $G(pR) \cong \Gamma(pL)$.

**Proof.** Let $V$ be the group of $R$-automorphisms of $A$, commuting with all $\lambda_x$, $x \in G$. We will show that $V = \{\rho_x|x \in G\}$.

Let $v \in V$ and put $x = (v(x_1)(e), \ldots, v(x_n)(e))$. It is easy to see that if $f \in A$, then $v(f)(e) = f(x) = \rho_x f(e)$. Hence if $y \in G$, we have

$$v(f)(y) = \lambda_{y^{-1}} \circ v(f)(e) = v \circ \lambda_{y^{-1}}(f)(e) = \rho_x \circ \lambda_{y^{-1}}(f)(e) = \rho_x(f)(y).$$

It implies that $v = \rho_x$.

Now, if $w \in pL$, then by Lemma 4.4, $e^w$ is an automorphism of $A$. It is clear that $e^w \in V$. Since $e^w(x_i) \in x_i + pA$, we obtain from the previous paragraph that $e^w = \rho_x$ for some $x \in G(pR)$. This finishes the proof.  

\[10\]
Corollary 4.6. If the Lie $R$-algebra $\mathbb{L} = \mathbb{L}(G)$ can be embedded in $\text{End}_R(W)^{(-)}$ for some finitely generated $R$-torsion-free $R$-module $W$, then $G(pR)$ can be embedded as a closed subgroup in $\text{Aut}_R(W)$.

Proof. Suppose $\mathbb{L}$ is a $R$-subalgebra of $\text{End}_R(W)^{(-)}$. By Theorem 1.2 $H = \{e^a | a \in p\mathbb{L}\}$ is a group isomorphic to $\Gamma(p\mathbb{L})$ and, whence, by the previous theorem to $G(pR)$. Note that $H$ is a closed subgroup of $\text{Aut}_R(W)$ because the exponential map is continuous on $p\text{End}_R(W)$ and $p\mathbb{L}$ is compact. 

5 Soluble radical of a finitely generated $R$-standard group

Let $R$ be a noetherian commutative domain, $D$ its field of fractions and $\mathbb{L}$ an $R$-Lie algebra which is a finitely generated free $R$-module. We call $\mathbb{L}$ for short an $R$-lattice. Put $\mathbb{L}_D = D \otimes_R \mathbb{L}$. $\mathbb{L}_D$ is a finite dimensional $D$-Lie algebra. In the following $R_n(\mathbb{L}_D)$ will denote the soluble radical of $\mathbb{L}_D$ and $R_n(z(\mathbb{L}_D))$ will denote the nilpotent radical of $\mathbb{L}_D$. The purpose of this section is the next result:

Theorem 5.1. Let $R$ be a commutative Noetherian local pro-$p$ domain of characteristic 0 and Krull dimension greater than 1 and $D$ its field of quotients. Let $G$ be a finitely generated $R$-standard group and $\mathbb{L} = \mathbb{L}(G)$ its Lie algebra. Then $R_n(\mathbb{L}_D)$ is nilpotent.

We use the notation of the previous section. From Theorem 1.5 we know that if $x \in G(pR)$, then $\rho_x = e^a$ for some $a \in p\mathbb{L}(G)$. Recall that $I$ is an ideal of $A$ generated by $x_1, \ldots, x_d$. The conjugation by $x$ which send $f(y) \in I$ to $f(x^{-1}yx) \in I$ is the map $\lambda_x \circ \rho_x$. We need an auxiliary lemma.

Lemma 5.2. Let $G$ be a finitely generated $R$-standard group and $x \in G(pR)$. Let $a \in p\mathbb{L}(G)$ be such that $\rho_x = e^a$. Suppose $\lambda_x \circ \rho_x$ acts as an unipotent automorphism on $(I/I^2)$. Then $a \in R_n(\mathbb{L}(G)_D)$.

Proof. Let $f \in I$ and $w \in \mathbb{L} = \mathbb{L}(G)$. We have

$$(\rho_x^{-1} \circ w \circ \rho_x)(f)(e) = (w \circ \rho_x)(f)(x^{-1}) = (w \circ \lambda_x \circ \rho_x)(f)(e).$$

Note that if a linear automorphism acts unipotently on $V$, it acts also unipotently on $V^*$. Since $\mathbb{L}$ can be identified with $(I/I^2)^*$ (see Remark 3.2), we have that the automorphism of $\mathbb{L}_D$ defined as $\tau(w) = \rho_x^{-1} \circ w \circ \rho_x$ is unipotent.

In order to prove that $ad a$ is nilpotent, we should to show that every $ad a$-invariant subspace $W$ of $\mathbb{L}_D$ has a nonzero element $w$ such that $ad a(w) = 0$. So, let $W$ be an $ad a$-invariant subspace of $\mathbb{L}_D$. Since we have

$$\tau(w) = \rho_x^{-1} \circ w \circ \rho_x = e^{-a} \circ w \circ e^a = \sum_{i=0}^{\infty} \frac{(ad a)^i(w)}{i!} = e^{a(ad a)(w)},$$

$W$ is also $\tau$-invariant. Hence there exists $0 \neq w \in W$ such that $\tau(w) = w$. Then $ad a(w) = 0$. We conclude that $ad a$ is nilpotent. 

11
Proof of Theorem 5.1. We suppose the contrary. If \( v \in R_n(L_D) \setminus R_n(L_D^0) \), then \( Dv \cap R_n(L_D^0) = \{0\} \). Put \( T = pL \cap R_n(L_D^0) \) and \( T_1 = pL \cap Dv \). As in the previous section we see the elements from \( L(G) \) as left invariant derivations of \( A \), and the elements from \( G \) as left invariant automorphisms of \( A \) (so \( G \) coincides with \( \{\rho_x | x \in G\} \)).

Put \( H = \{ e^a | a \in T \} \) and \( H_1 = \{ e^a | a \in T_1 \} \). By Theorem 6.1, these two sets are subsets of \( L(G) = \{\rho_x | x \in G(pL)\} = \{e^a | a \in pL(G)\} \). Note also that \( H \) and \( H_1 \) are subgroups of \( G \).

If \( h = e^a \in H \) and \( g \in G \), then \( h^g = (e^{\text{Ad}(a)}) \). Hence \( H \) is a normal subgroup of \( G \). On the other hand since \( T \) is soluble, \( H \) is soluble.

In [5, Proposition 5.1] we proved that for some \( k \) the kernel of the action by conjugation on \( I/I^k \) is \( Z(G) \). If \( \Omega \) is the algebraic closure of \( D \), we can consider \( G/Z(G) \) as a subgroup of \( \text{GL}_m(\Omega) \), where \( m \) is the rank of \( I/I^k \) as \( R \)-module. Let \( \bar{G} \) and \( \bar{H} \) be the Zariski closures of \( G/Z(G) \) and \( HZ(G)/Z(G) \) respectively in \( \text{GL}_m(\Omega) \). Then \( \bar{H} \) is a normal soluble subgroup of \( \bar{G} \). By [4, Lemma 19.5], \( [\bar{G}^0, \bar{G}^0] \cap \bar{H} \) is virtually unipotent.

Suppose \( h = e^a \), \( a \in pL \) acts as an unipotent automorphism on \( I/I^k \). Then by the previous lemma, \( a \in R_n(L) \). This implies that \( H_1 Z(G)/Z(G) \) does not have non-trivial unipotent elements and so \( [\bar{G}^0, \bar{G}^0] \cap H_1 Z(G)/Z(G) \) is finite. Since \( Dv \cap R_n(L_D^0) = \{0\} \), we have \( H_1 \cap Z(G) = \{1\} \), whence \( [\bar{G}^0, \bar{G}^0] \cap H_1 \) is finite.

On the other hand, since \( G \) is finitely generated, \( G^0 = G \cap \bar{G}^0 \) is finitely generated and so \( H_1 / ([G^0, G^0] \cap H_1) \) is abelian of finite rank. We obtain that \( H_1 \) has finite rank. We have a contradiction because \( (R, +) \) can be embedded in \( H_1 \) and it is not of finite rank. \( \square \)

6 The Weigel theorem

Let \( R \) be a noetherian commutative domain, \( K \) its field of fractions and \( L \) an \( R \)-Lie algebra which is a finitely generated free \( R \)-module. \( L_K \) is a finite dimensional \( K \)-Lie algebra. The Ado-Iwasawa theorem states that \( L_K \) has a finite dimensional linear representation. The next result shows that if the soluble radical of \( L_K \) is nilpotent, then this representation can satisfy some additional nice properties.

Theorem 6.1. ([T. Weigel, Lemma 4.3, Proposition 4.4]) Let \( R \) be an integrally closed noetherian commutative domain and \( K \) its field of fractions. Assume that \( L \) is an \( R \)-lattice and that soluble radical of \( L_K \) is nilpotent. Then there exist a finitely generated \( R \)-torsion-free \( R \)-module \( W \) and a faithful \( R \)-linear representation \( \psi : L \to \text{End}_R(W) \).

7 Linearity of groups

In this section we finish the proof of Theorem 6.1.
Theorem 7.1. Let $R$ be a commutative Noetherian local pro-$p$ ring of characteristic 0 and $G$ be a finitely generated $R$-standard group. Then $G$ is $R$-linear.

Proof. The theorem is known in the case when $K \dim R = 1$. So we suppose that $K \dim R > 1$. Let $F = F(x, y) (x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n))$ be the formal law associated with $G$ and $\phi: R \to S$ a homomorphism from Theorem 2.6 when $a = p$. Then we can extend this homomorphism to

$$\phi: R[[x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n]] \to S[[x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n]]$$

in obvious way. Put $H(x, y) = \phi(F(x, y))$. We have

$$H(H(x, y), z) = \phi(F(F(x, y), z)) = \phi(F(x, F(y, z))) = H(x, H(y, z)).$$

Hence $H$ is also a formal group law. Let $H$ be an $S$-standard group associated with $H$.

Let $D$ be the ring of quotients of $R$. By Theorem 6.1 the radical of $D \otimes_R L(G)$ is nilpotent. Let $E$ be the field of quotients of $S$. Then we have

$$E \otimes_S L(H) = E \otimes_S (S \otimes_R L(G)),$$

which clearly implies that the radical of $E \otimes_S L(H)$ is also nilpotent.

Applying $\phi$, $G(m^k)$ is embedded as a closed subgroup into $H(pS)$:

$$(x_1, \ldots, x_d) \mapsto (\phi(x_1), \ldots, \phi(x_d)).$$

By Theorem 6.1, $L(H)$ acts faithfully on a finitely generated $S$-torsion-free module $W$. Hence, by Corollary 5.6 $G(m^k) \leq H(pS)$ acts faithfully on $W$. By Theorem 2.2 $G(m^k)$ is linear over some commutative Noetherian local pro-$p$ domain $T$ of characteristic 0 and same Krull dimension as $R$. By Theorem 2.1 $G(m^k)$ is $R$-linear. Finally, since the index of $G(m^k)$ in $G$ is finite, $G$ is also $R$-linear.

References

[1] N. Bourbaki, Lie groups and Lie algebras, Springer-Verlag, 1989.
[2] R. Camina, M du Sautoy, Linearity of $\mathbb{Z}_p[[\ell]]$-perfect groups, preprint.
[3] J. Dixon, M. du Sautoy, A. Mann, Y D. Segal, Analytic pro-$p$ groups, 2nd ed., Cambridge University Press, Cambridge, 1999.
[4] J. Humphreys, Linear algebraic groups, Graduate Texts in Mathematics, No. 21, Springer-Verlag, New York-Heidelberg, 1975.
[5] A. Jaikin Zapirain, On linear just infinite pro-$p$ groups, J. Algebra 255 (2002), 392–404.
[6] E. I. Khukhro, *p-Automorphisms of Finite p-groups*, Cambridge University Press, Cambridge, 1998.

[7] M. Lazard, Groupes analytiques *p*-adiques, *Publ. Math. I.H.E.S.* 71(1968), 389–603.

[8] M. Nagata, *Local Rings*, R.E. Krieger Publishing Company, Huntington, New York, 1975.

[9] *New Horizons in pro-*p* Groups*, M. du Sautoy, D. Segal, A. Shalev (editors), Birkhauser 2000.

[10] T. Weigel, The Ado-Iwasawa Theorem, *J. Algebra* 212(1999), 613-625.

[11] O. Zariski, P. Samuel, *Commutative Algebra*, D. van Nostrand Company, Princeton, New Jersey, Toronto, London, 1967.