# On linearity of finitely generated $R$-analytic groups *

A. Jaikin-Zapirain

Departamento de Matemáticas Facultad de Ciencias

Universidad Autónoma de Madrid

**Abstract**

In this paper we prove that if $R$ is a commutative Noetherian local pro-$p$ domain of characteristic 0, then every finitely generated $R$-standard group is linear.

## 1 Introduction

Let $R$ be a commutative Noetherian local pro-$p$ ring and $\mathfrak{m}$ its maximal ideal. The group $G$ is called $R$**-standard** if $G$ is equal to $(\mathfrak{m}^l)^{(d)}$ as a set and the group operation is given by a **formal group law**, i.e. a $d$-tuple $\mathbf{F} = (F_1, \dots, F_d)$ of power series over $R$ in $2d$ variables, as follows: for all $\mathbf{x}, \mathbf{y} \in G = (\mathfrak{m}^l)^{(d)}$ we have

$$\mathbf{x} \cdot \mathbf{y} = (F_1(\mathbf{x}, \mathbf{y}), \dots, F_d(\mathbf{x}, \mathbf{y})).$$

The number $d \geq 0$ is the **dimension** of $G$ and $l > 0$ is the **level** of $G$.

The concept of an $R$-standard group is closely related to the notion of an $R$**-analytic group**. Roughly speaking, $R$-analytic groups are Lie groups over $R$ (see [3, Chapter 13] for a more concrete definition). In this paper we understand by an $R$-analytic group a topological group that has an $R$-standard subgroup as an open subgroup. As it is shown in [3, Theorem 13.20] this definition coincides with the general one when $R$ satisfies some additional condition (that the ring $\bigoplus_{i=0}^{\infty} \mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a domain). However the same is true if we only assume that $R$ is domain (see Remark 3.2).

The neutral element of $G$ is $\mathbf{e} = (0, \dots, 0)$. If $I$ is an ideal of $R$, then we write $G(I)$ for $(I)^{(d)} \subseteq G$. Also $G_i$ denotes $G(\mathfrak{m}^i)$, and so $G = G_1 = G(\mathfrak{m})$. From now on, $R$ always denotes a commutative Noetherian local pro-$p$ domain. We

*This work has been partially supported by the FEDER, the MCYT Grants BFM2001-0201, BFM2001-0180 and the Ramón y Cajal Program.

say that a pro-$p$ group is $R$**-linear** if it can be embedded as a closed subgroup into $\mathrm{GL}_n(R)$ for some $n$.

The $\mathbb{Z}_p$-analytic pro-$p$ groups are well-understood (see [8, 3]) and they are linear over $\mathbb{Z}_p$. It was conjectured that $R$-analytic pro-$p$ groups are $R$-linear. Since compact $\mathbb{Z}_p$-analytic groups are finitely generated, it is natural to consider first finitely generated $R$-analytic pro-$p$ groups. In [5] it was shown 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 $\mathbb{Z}_p[[t]]$-perfect groups is shown. Recall that an $R$-standard group of level $l$ is called $R$-perfect if $[G,G]=G_{2l}$. Note that $R$-perfect groups are finitely generated. Without loss of generality we will always assume that the level of $G$ is 1. If $T$ is a ring, we denote by $K\dim T$ the Krull dimension of $T$. The main result of this paper is as follows.

**Theorem 1.1.** *Let $R$ be a commutative Noetherian local pro-p domain of characteristic 0 and $G$ a finitely generated $R$-standard group. Then $G$ is $S$-linear, where $S$ is a commutative Noetherian local pro-p domain of characteristic 0 and same Krull dimension as $R$.*

The layout of the paper is as follows. First 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 standard definition is based on the formal group law of $G$. We introduce another definition coming from the theory of algebraic groups and define $\mathbb{L}$ as the set of left invariant derivations of $\mathbb{A}=R[[x_1,\cdots x_d]]$. We prove that these two definitions are equivalent. In Section 4, assuming that the characteristic of $R$ is 0, we use the Baker-Campbell-Hausdorff formula in order to define on $\mathbf{p}\mathbb{L}$ (here $\mathbf{p}=\mathbf{p}(p)=4$ if $p=2$ and $\mathbf{p}=p$ if $p$ is an odd prime) a group structure. We show that the constructed group is isomorphic to $G(\mathbf{p}R)$. In Section 5 we prove that if an $R$-standard group is finitely generated, then the soluble radical of $\mathbb{L}(G)$ is nilpotent. This allows to use the Weigel result about linearity of some Lie rings which we describe in Section 6. Finally, in Section 7 we prove Theorem 1.1.

## 2 Some results about t-linear pro-$p$ groups

Recall the definition of a t-linear pro-$p$ group 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 $\mathrm{GL}_n(A)$ 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. The aim of this section is to prove the following result.

**Theorem 2.1.** *Let $R$ be a commutative Noetherian local pro-p domain and $W$ a finitely generated $R$-torsion-free $R$-module. Suppose that $G\leq \mathrm{Aut}_R(W)$.*

*Then there exists a commutative Noetherian local pro-$p$ domain $S$, satisfying* $\operatorname{char} S = \operatorname{char} R$ *and* $K \dim S = K \dim R$*, such that $G$ is $S$-linear.*

First we need to prove some auxiliary results.

**Lemma 2.2.** *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 [9, p.27]), and this number is at least $K \dim R[[t]] - 1$. This implies that $K \dim R[[t]]/(at - r) \geq K \dim R$. $\square$

Recall that a **(multiplicative non-archimedean) valuation** of a field $D$ is a mapping $v \colon D \to \mathbb{R}_{\geq 0}$ 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 2.3.** *([9, Proposition 11.9]) Let $R$ be a subring of a field $D$ and $\mathfrak{m}$ 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 $m \in \mathfrak{m}$.*

**Lemma 2.4.** *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 see that $S$ is local. Let $D$ be the quotient field of $R$ and $v$ a valuation from Proposition 2.3. If $s \in S$, then $v(s) \leq 1$, because $s$ is integral over $R$. Thus, 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 $f(t) = t^n + \sum_{i=0}^{n-1} a_i t^i$ be a monic, irreducible over $R$, polynomial such that $f(s) = 0$. Let $k$ be the smallest $i$ such that $a_i \notin \mathfrak{m}$. Since $v(s) = 1$, $i$ must be less than $n$. We show that $k = 0$. Indeed, if $k > 0$, then $f \equiv t^k g(t) \pmod{\mathfrak{m}}$ for some $g \in R[t]$. Since $R$ is a Henselian ring (see [9, Theorem 30.3]), we obtain that $f$ is not irreducible. Hence $k = 0$, and so $s^{-1} \in S$.

Finally, by [9, Theorem 32.1], $S$ is a finite extension of $R$, whence their Krull dimensions coincide. $\square$

We need also the following lemma.

**Lemma 2.5.** *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 $\phi\colon R \to S$ such that*

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

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

*Proof.* Let $D$ be the quotient field of $R$ and $v$ a valuation from Proposition 2.3. Let $\Omega$ be a completion of $D$ respect to $v$. Since $R$ is Noetherian, there exists $s = \max\{v(r) | r \in \mathfrak{m}\} < 1$ Let $k$ be such that $s^k/v(a) < 1$ and put $S_1 = R[[\mathfrak{m}^k/a]] \subset \Omega$. It is clear that $S_1$ is a local pro-$p$ ring. Moreover, if $t_1, \dots, t_m$ are generators of $\mathfrak{m}^k$ as $R$-module, then $S_1 = R[[t_1/a, \dots, t_m/a]]$. Hence $S_1$ is Noetherian. Applying several times Lemma 2.2, we obtain that its Krull dimension is the same as of $R$. Finally, let $S$ be the integral closure of $S_1$. Then Theorem follows from Lemma 2.4. □

*Proof of Theorem 2.1.* 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 $m_1, \cdots, m_r$ 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 an element of $R$ such that $aW \leq N$. By Lemma 2.5, there are a commutative Noetherian local pro-$p$ ring $S$ and an injective homomorphism $\phi\colon R \to S$ such that $\phi(\mathfrak{m}^k) \subseteq \phi(a)S$ for some $k \in \mathbb{N}$.

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

Now we embed $W_1$ in $L$ in the following way. Let $w \in W_1$. Since $aW_1 \leq a\mathfrak{m}^k W \leq \mathfrak{m}^k N$ and $m_i$ are free $R$-generators of $N$, there are unique $k_i \in \mathfrak{m}^k$ such that $w = \sum_{i=1}^r a^{-1}k_i m_i$. Define $\psi(w) = \sum_{i=1}^r \phi(a)^{-1}\phi(k_i) \otimes m_i$ (since $S$ is domain and $\phi(\mathfrak{m}^k) \subseteq \phi(a)S$, we can speak about $\phi(a)^{-1}\phi(k_i) \in S$). Then the map $\psi$ is an $R$-homomorphism. Therefore, we can see $W_1$ as an $R$-submodule of $L$.

Now, we explain how we can extend the action of $H$ on $L$. Let $g \in H$. Since $L$ is a free $S$-module any element $l \in L$ can be uniquely expressed as the sum $\sum_{i=1}^r s_i m_i$, where $s_i \in S$. We define $gl = \sum_{i=1}^r s_i g m_i$. Note that, since $g \in H$, $gm_i \in W_1 + N$, and so $\sum_{i=1}^r s_i g m_i \in L$. Thus, we have constructed an embedding of $H$ into $\mathrm{Aut}_S(L) \cong \mathrm{GL}_r(S)$. Since $H$ is of finite index in $G$, $G$ is also $S$-linear. □

We finish this section posing the following natural question.

**Question 1.** Let $R$ and $S$ be commutative Noetherian local pro-$p$ domains of characteristic 0, having same Krull dimensions, and $G$ a pro-$p$ group. Is it true that $G$ is $R$-linear if and only if $G$ is $S$-linear?

We say that a commutative local pro-$p$ ring $R$ is **regular** if $R \cong R_0[[x_1, \ldots, x_d]]$, where $R_0$ is a finite extension of $\mathbb{Z}_p$ or it is isomorphic to $\mathbf{F}_q$. The fundamental structure theorem of I. S. Cohen (see [9, Corollary 31.6]) shows that any commutative local pro-$p$ domain $S$ contains a regular commutative local pro-$p$ ring $R$ such that $S$ is a finitely generated $R$-module. Hence we can assume in the previous question that $R$ is regular and $S$ is a finite extension of $R$.

# 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 $\mathbf{F}$ can be written in the form

$$\mathbf{F}(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y} + \mathbf{B}(\mathbf{x}, \mathbf{y}) + O'(3),$$

where $\mathbf{B}$ is the sum of the all polynomials in $\mathbf{x}$ and $\mathbf{y}$ 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, [10, p.26], that if $\mathbf{C}(\mathbf{x}, \mathbf{y}) = \mathbf{B}(\mathbf{x}, \mathbf{y}) - \mathbf{B}(\mathbf{y}, \mathbf{x})$, then $(R^{(d)}, +, \mathbf{C})$ is a Lie $R$-algebra, and we shall denote this Lie algebra by $\mathbb{L} = \mathbb{L}(G)$. In this section we give another description of $\mathbb{L}$.

**Lemma 3.1.** *Let $R$ be a commutative local pro-$p$ domain and $F \in R[[x_1, \ldots, x_d]]$. Suppose $F(\boldsymbol{x}) = 0$ for any $\boldsymbol{x} \in \mathfrak{m}^{(d)}$. Then $F = 0$.*

*Proof.* Suppose that $F \neq 0$. Then there exists a coefficient $a \in R$ of $F$ different from zero. Consider an ideal $J$ of $R$ which does not intersect $\{a^k, k \in \mathbb{N}\}$ and maximal respect to this property. It is well-known that $J$ is a prime ideal of $R$. Put $S = R/J$. The ring $S$ satisfies the following property: every ideal of $S$ contains a power of some fixed element (in our case the element $a + J$). Rings with this property are known to have Krull dimension 1 (see [6, Theorem 146]). On the other hand $S$ is a local pro-$p$ ring. Let $S_0 \leq S$ be isomorphic to $\mathbb{Z}_p$ if the characteristic of $R$ is zero or $\mathbf{F}_p[[t]]$ if the characteristic of $S$ is $p$. Then $S$ is a finitely generated free $S_0$-module. Let $s_1, \cdots, s_l$ be a system of free $S_0$-generators of $S$. Denote by $H$ the image of $F$ in $S[[x_1, \ldots, x_d]]$. We can write $H$ as $H = \sum_i s_i H_i$ where $H_i$ are power series over $S_0$. Since $H \neq 0$, without loss of generality we can suppose that $H_1 \neq 0$. Let $\pi$ be a generator of maximal ideal of $S_0$. By [3, Proposition 6.49], there exist an element $\mathbf{x} \in (\pi S_0)^{(d)}$ such that $H_1(\mathbf{x}) \neq 0$. Hence $H(\mathbf{x}) \neq 0$, and so there exists $\mathbf{y} \in (\mathfrak{m})^{(d)}$ such that $F(\mathbf{y}) \notin J$. We obtain a contradiction. $\square$

**Remark 3.2.** By a remark on the page 323 of [3], the previous lemma allows to change the condition $\bigoplus_{i=0}^{\infty} \mathfrak{m}^i/\mathfrak{m}^{i+1}$ is domain by $R$ is domain in [3, Theorem 13.20].

Now, let $\mathbb{A} = R[[x_1, \ldots, x_d]]$. Since $G$ is equal to $\mathfrak{m}^{(d)}$, by the previous lemma, $\mathbb{A}$ can be considered as a subring of the ring of functions from $G$ to $R$.

Define two actions of $G$ on $\mathbb{A}$ via the left and the right translations:

$$(\lambda_{\mathbf{x}} f)(\mathbf{y}) = f(\mathbf{x}^{-1}\mathbf{y}),\ (\rho_{\mathbf{x}} f)(\mathbf{y}) = f(\mathbf{y}\mathbf{x}),\ \text{where}\ \ f \in \mathbb{A}, \mathbf{x} \in G, \mathbf{y} \in G.$$

Since the multiplication in $G$ is given by an analytic function, we have that if $f \in \mathbb{A}$ then $\lambda_{\mathbf{x}} f$ and $\rho_{\mathbf{x}} f$ also belong to $\mathbb{A}$.

The bracket of two $R$-derivations of $\mathbb{A}$ is again a derivation. Therefore, $\operatorname{Der} \mathbb{A}$ is a Lie algebra. So is the subspace of left invariant derivations

$$\operatorname{Der}_l \mathbb{A} = \{w \in \operatorname{Der} \mathbb{A} \mid w\lambda_{\mathbf{x}} = \lambda_{\mathbf{x}} w \text{ for all } \mathbf{x} \in G\},$$

since the bracket of two derivations which commute with $\lambda_{\mathbf{x}}$ obviously does likewise. The next theorem is the main result of this section:

**Theorem 3.3.** *The Lie $R$-algebras $\mathbb{L}$ and $\operatorname{Der}_l \mathbb{A}$ are isomorphic.*

First we prove several auxiliary results. If $f \in \mathbb{A}$ and $\mathbf{x}, \mathbf{y}, \mathbf{z} \in G$ then $f(\mathbf{zyx})$ can be regarded as an element of $R[[x_1, \cdots, x_d, y_1, \cdots, y_d, z_1, \cdots, z_d]]$. Then $\frac{\partial f(\mathbf{yx})}{\partial x_i}$ and $\frac{\partial^2 f(\mathbf{zyx})}{\partial x_i \partial y_j}$ are formal partial derivations respect to $x_i$ and $y_j$ in the ring $R[[x_1, \cdots, x_d, y_1, \cdots, y_d, z_1, \cdots, z_d]]$.

**Lemma 3.4.** *Let $w_1, w_2 \in \operatorname{Der}_l \mathbb{A}$ and $f \in \mathbb{A}$. Then we have*

$$\begin{aligned} w_1(f)(\boldsymbol{y}) &= \sum_{i=1}^{d} \left.\frac{\partial f(\boldsymbol{yx})}{\partial x_i}\right|_{\boldsymbol{x}=\boldsymbol{e}} w_1(x_i)(\boldsymbol{e}), \\ w_2(w_1(f))(\boldsymbol{z}) &= \sum_{i,j=1}^{d} \left.\frac{\partial^2 f(\boldsymbol{zyx})}{\partial x_i \partial y_j}\right|_{(\boldsymbol{x},\boldsymbol{y})=(\boldsymbol{e},\boldsymbol{e})} w_1(x_i)(\boldsymbol{e}) w_2(x_j)(\boldsymbol{e}). \end{aligned}$$

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

$$\begin{aligned} w_1(f)(\mathbf{y}) &= (\lambda_{\mathbf{y}^{-1}} w_1(f))(\mathbf{e}) = w_1(\lambda_{\mathbf{y}^{-1}} f)(\mathbf{e}) \\ &= \sum_{i=1}^{d} \frac{\partial(\lambda_{\mathbf{y}^{-1}} f)}{\partial x_i}(\mathbf{e}) w_1(x_i)(\mathbf{e}) = \sum_{i=1}^{d} \left.\frac{\partial f(\mathbf{yx})}{\partial x_i}\right|_{\mathbf{x}=\mathbf{e}} w_1(x_i)(\mathbf{e}). \end{aligned}$$

$\square$

*Proof of Theorem 3.3.* Define an $R$-homomorphism $\phi\colon \operatorname{Der}_l(A) \to \mathbb{L}$ as follows

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

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

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

If $f_1, f_2 \in A$, then

$$\begin{aligned} w(f_1 f_2)(\mathbf{y}) &= \sum_{i=1}^{d} \frac{\partial f_1(\mathbf{yx}) f_2(\mathbf{yx})}{\partial x_i}\bigg|_{\mathbf{x}=\mathbf{e}} a_i \\ &= \sum_{i=1}^{d} \frac{\partial f_1(\mathbf{yx})}{\partial x_i}\bigg|_{\mathbf{x}=\mathbf{e}} f_2(\mathbf{y}) a_i + \sum_{i=1}^{d} f_1(\mathbf{y}) \frac{\partial f_2(\mathbf{yx})}{\partial x_i}\bigg|_{\mathbf{x}=\mathbf{e}} a_i \\ &= w(f_1)(\mathbf{y}) f_2(\mathbf{y}) + f_1(\mathbf{y}) w(f_2)(\mathbf{y}). \end{aligned}$$

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

$$\begin{aligned} w(\lambda_{\mathbf{z}} f)(\mathbf{y}) &= \sum_{i=1}^{d} \frac{\partial (\lambda_{\mathbf{z}} f)(\mathbf{yx})}{\partial x_i}\bigg|_{\mathbf{x}=\mathbf{e}} a_i \\ &= w(f)(\mathbf{z}^{-1}\mathbf{y}) = (\lambda_{\mathbf{z}} w(f))(\mathbf{y}). \end{aligned}$$

Hence, we obtain that $w$ is also left invariant. Define the constructed map from $\mathbb{L}$ to $\mathrm{Der}_l(A)$ by $\psi$. Note that if $w \in \mathrm{Der}_l(A)$, then we have

$$\begin{aligned} \psi(\phi(w))(f)(\mathbf{y}) &= \psi(w(x_1)(\mathbf{e}), \ldots, w(x_d)(\mathbf{e}))(f)(\mathbf{y}) \\ &= \sum_{i=1}^{d} \frac{\partial f(\mathbf{yx})}{\partial x_i}\bigg|_{\mathbf{x}=\mathbf{e}} w(x_i)(\mathbf{e}) \\ &= w(\lambda_{\mathbf{y}^{-1}} f)(\mathbf{e}) = \lambda_{\mathbf{y}^{-1}} w(f)(\mathbf{e}) = w(f)(\mathbf{y}). \end{aligned}$$

On the other hand if $a = (a_1, \ldots, a_d) \in \mathbb{L}$, then

$$\phi(\psi(a)) = (b_1, \ldots, b_d),$$

where $b_k = \sum_{i=1}^{d} \frac{\partial F_k(\mathbf{y},\mathbf{x})}{\partial x_i}\Big|_{\mathbf{x}=\mathbf{e}} a_i = a_k$. 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 $w_1, w_2 \in \mathrm{Der}_l(A)$. From the previous lemma, we obtain that

$$\phi([w_1, w_2]) = (c_1, \ldots, c_d),$$

where

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

We conclude that $\phi([w_1, w_2]) = \mathbf{C}(\phi(w_1), \phi(w_2))$. □

**Remark 3.5.** Note that the previous proof also gives an identification of $\mathrm{Der}_l(A)$ with $(\mathbb{I}/\mathbb{I}^2)^* = \mathrm{End}_R(\mathbb{I}/\mathbb{I}^2, R)$, where $\mathbb{I}$ is the ideal of $\mathbb{A}$ generated by $x_1, \cdots, x_d$. The derivation $w$ is identified with the map $f \to w(f)(\mathbf{e})$.

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

# 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 $H(x_1, x_2) = \sum_{n=1}^{\infty} H_n(x_1, x_2)$. 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, [7, Theorem 9.11]). Let $\{e_k\}$ 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 $\lambda_{k,n}$ ([1, Proposition II.8.1]):

$$v_p(\lambda_{k,n}) \geq -(n-1)/(p-1), \tag{1}$$

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 $\cap_i p^i M = 0$. If $M$ is complete in the topology induced by the filtration $p^i M$, then*

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

(ii) *$(\boldsymbol{p}M, H)$ is a group.*

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

Since $H(a,0) = H(0,a) = a$ and $H(a,-a) = 0$ for any $a \in \mathbf{p}M$, then in order to prove the second part, 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 $F$:

$$\begin{aligned} H(H(x_1,x_2),x_3) &= \log(e^{H(x_1,x_2)} e^{x_3}) = \log(e^{x_1} e^{x_2} e^{x_3}) \\ &= \log(e^{x_1} e^{H(x_2,x_3)}) = H(x_1, H(x_2, x_3)). \end{aligned}$$

In particular, we obtain

$$H(H(\mathbf{p}x_1, \mathbf{p}x_2), \mathbf{p}x_3) = H(\mathbf{p}x_1, H(\mathbf{p}x_2, \mathbf{p}x_3)). \tag{2}$$

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$\{e_k, k \in \mathbb{N}\}$ 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 $y_1, y_2 \in \mathbf{p}\bar{L}$, then $H(\mathbf{p}y_1, \mathbf{p}y_2) \in \mathbf{p}\bar{L}$.

Now, let $a, b, c \in M$ and $\phi\colon L \to M$ 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 $\phi\colon \bar{L} \to M$. Furthermore, $\phi$ is a continuous map. Then

$$\begin{aligned} H(H(\mathbf{p}a, \mathbf{p}b), \mathbf{p}c) &= H(H(\phi(\mathbf{p}x_1), \phi(\mathbf{p}x_2)), \phi(\mathbf{p}x_3)) \\ &= \phi(H(H(\mathbf{p}x_1, \mathbf{p}x_2), \mathbf{p}x_3)) = \phi(H(\mathbf{p}x_1, H(\mathbf{p}x_2, \mathbf{p}x_3))) \\ &= H(\mathbf{p}a, H(\mathbf{p}b, \mathbf{p}c)). \end{aligned}$$

We conclude that the operation $H(x_1, x_2)$ is associative and, so, $(\mathbf{p}M, H)$ is a group. □

We will denote the group $(\mathbf{p}M, H)$ by $\Gamma(\mathbf{p}M)$.

**Theorem 4.2.** *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 $p^i D$. If $M$ is a closed Lie $\mathbb{Z}_p$-subalgebra of $D^{(-)}$,then*

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

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

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

*Proof.* By [1, Lemma II.8.1], $v_p(n!) \leq (n-1)/(p-1)$. Hence we obtain the first part of the theorem.

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 $f \in t\mathbf{p}P$. Since $v_p(n!) \leq (n-1)/(p-1)$, $e^f \in P$ and $\log(1+f) \in P$. Let $a = \mathbf{p}b$. 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 $\mathbf{p}t = \log(e^{\mathbf{p}t})$ holds. Since $\phi$ is continuous, we have

$$a = \phi(\mathbf{p}t) = \phi(\log(e^{\mathbf{p}t})) = \log(e^a).$$

In the same way we obtain that $e^{\log(1+a)} = a$. This proves the second part of the theorem.

Since $M$ satisfies the hypothesis of the previous theorem, in order to prove the third part we have to show that $e^a e^b = e^{H(a,b)}$ for all $a, b \in \mathbf{p}M$. The proof of this equality is similar to the proof of Theorem 4.1 and therefore 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 $(\phi - 1)D \in \mathbf{p}D$. Then $\log \phi \in \mathbf{p}\operatorname{End}_{\mathbb{Z}_p}(D)$ is well-defined and it is a derivation of $D$.*

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

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

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

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

Hence $\log \phi$ is a derivation. $\square$

Using a similar argument we can prove the following lemma.

**Lemma 4.4.** *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 $\mathbb{Z}_p$-derivation of $D$ and suppose $\phi(D) \in \mathbf{p}D$. Then $\exp(\phi) \in 1 + \mathbf{p}\operatorname{End}_{\mathbb{Z}_p}(D)$ 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 $\mathbf{x} \in G(\mathbf{p}R)$. Then it is clear that the automorphism $\rho_{\mathbf{x}}$ satisfies the condition: $(\rho_{\mathbf{x}} - 1)A \in \mathbf{p}A$, whence $\rho_{\mathbf{x}} \in 1 + \mathbf{p}\,\mathrm{End}_R(A)$. By Lemma 4.3, we have a well-defined derivation $\log(\rho_{\mathbf{x}}) \in \mathbf{p}\,\mathrm{End}_R(A)$. Since $\lambda_{\mathbf{y}}$ and $\rho_{\mathbf{x}}$ commute, $\log(\rho_{\mathbf{x}}) \in \mathbf{p}\mathbb{L} = \mathbf{p}\,\mathrm{Der}_l(A)$.

From the equality $\exp(\log(\rho_x)) = \rho_x$, we obtain, using Theorem 4.2(iii), that $G(\mathbf{p}R)$ can be embedded into $\Gamma(\mathbf{p}\mathbb{L})$. In fact, we can prove more:

**Theorem 4.5.** *The groups $\{\rho_{\boldsymbol{x}} | \boldsymbol{x} \in G(\boldsymbol{p}R)\}$ and group $\{e^a | a \in \boldsymbol{p}\mathbb{L}\}$ coincide. In particular, $G(\boldsymbol{p}R) \cong \Gamma(\boldsymbol{p}\mathbb{L})$.*

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

Indeed, let $v \in V$ and put $\mathbf{x} = (v(x_1)(\mathbf{e}), \dots, v(x_n)(\mathbf{e}))$. It is easy to see that if $f \in A$, then $v(f)(\mathbf{e}) = f(\mathbf{x}) = \rho_{\mathbf{x}} f(e)$. Hence if $\mathbf{y} \in G$, we have

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

It implies that $v = \rho_{\mathbf{x}}$.

Now, if $w \in \mathbf{p}\mathbb{L}$, then by Lemma 4.4, $e^w$ is an automorphism of $A$. It is clear that $e^w \in V$. Since $e^w(x_i) \in x_i + \mathbf{p}A$, we obtain from the previous paragraph that $e^w = \rho_{\mathbf{x}}$ for some $\mathbf{x} \in G(\mathbf{p}R)$. This finishes the proof. □

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

*Proof.* Let $\phi \colon \mathbb{L} \to \mathrm{End}_R(W)^{(-)}$ be the embedding and let $M = \phi(\mathbb{L})$ be the image of $\mathbb{L}$ . By Theorem 4.2, $H = \{e^a | a \in \mathbf{p}M\}$ is a group isomorphic to $\Gamma(\mathbf{p}\mathbb{L})$ and, whence, by the previous theorem, it is isomorphic to $G(\mathbf{p}R)$. Note that $H$ is a closed subgroup of $\mathrm{Aut}_R(W)$ because the exponential map is continuous on $\mathbf{p}\,\mathrm{End}_R(W)$ and $\mathbf{p}M$ is compact. □

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

Let $T$ be a noetherian commutative domain, $D$ its field of fractions and $M$ an $T$-Lie algebra which is a finitely generated free $T$-module. We call such $M$ a an **$R$-lattice**. Put $M_D = D \otimes_T M$. Then $M_D$ is a finite dimensional $D$-Lie algebra. In the following $R_s(M_D)$ will denote the soluble radical of $M_D$ and $R_n(M_D)$ will denote the nilpotent radical of $M_D$. The purpose of this section is to prove the following 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 $R_s(\mathbb{L}_D)$ is nilpotent.*

We use the notation of the previous section. From Theorem 4.5 we know that if $\mathbf{x} \in G(\mathbf{p}R)$, then $\rho_{\mathbf{x}} = e^a$ for some $a \in \mathbf{p}\mathbb{L}(G) = \mathbf{p}\,\mathrm{Der}_l\,\mathbb{A}$. Recall that $\mathbb{I}$ is an ideal of $\mathbb{A}$ generated by $x_1, \cdots, x_d$. The conjugation by $\mathbf{x}$ which send $f(\mathbf{y}) \in \mathbb{I}$ to $f(\mathbf{x}^{-1}\mathbf{y}\mathbf{x}) \in \mathbb{I}$ is the map $\lambda_{\mathbf{x}} \circ \rho_{\mathbf{x}}$. We need an auxiliary lemma.

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

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

$$(\rho_{\mathbf{x}}^{-1} \circ w \circ \rho_{\mathbf{x}})(f)(\mathbf{e}) = (w \circ \rho_{\mathbf{x}})(f)(\mathbf{x}^{-1}) = (w \circ \lambda_{\mathbf{x}} \circ \rho_{\mathbf{x}})(f)(e).$$

Note that if a linear automorphism acts unipotently on $V$, it acts also unipotently on $V^*$. Since $\mathbb{L}$ can be identified with $(\mathbb{I}/\mathbb{I}^2)^*$ (see Remark 3.5), we have that the automorphism of $\mathbb{L}_D$ defined as $\tau(w) = \rho_{\mathbf{x}}^{-1} \circ w \circ \rho_{\mathbf{x}}$ is unipotent.

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

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

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

*Proof of Theorem 5.1.* We prove the theorem by way of contradiction. If $v \in R_s(\mathbb{L}_D) \setminus R_n(\mathbb{L}_D)$, then $Dv \cap R_n(\mathbb{L}_D) = \{0\}$. Put $T = \mathbf{p}\mathbb{L} \cap R_s(\mathbb{L}_D)$ and $T_1 = \mathbf{p}\mathbb{L} \cap Dv$. As in the previous section we see the elements from $\mathbb{L}(G)$ as left invariant derivations of $A$, and the elements from $G$ as left invariant automorphisms of $A$ (so $G$ coincides with $\{\rho_{\mathbf{x}} | \mathbf{x} \in G\}$).

Put $H = \{e^a | a \in T\}$ and $H_1 = \{e^a | a \in T_1\}$. By Theorem 4.5, these two sets are subsets of $G(\mathbf{p}R) = \{\rho_{\mathbf{x}} | \mathbf{x} \in G(\mathbf{p}R)\} = \{e^a | a \in \mathbf{p}\mathbb{L}(G)\}$. Note also that $H$ and $H_1$ are subgroups of $G$.

If $h = e^a \in H$ and $g \in G$, then $h^g = (e^{\mathrm{Ad}\, g(a)})$. 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 $\mathbb{I}/\mathbb{I}^k$ is $Z(G)$. If $\Omega$ is the algebraic closure of $D$, we can consider $G/Z(G)$ as a subgroup of $\mathrm{GL}_m(\Omega)$, where $m$ is the rank of $\mathbb{I}/\mathbb{I}^k$ as $R$-module. Let $\bar{G}$ and $\bar{H}$ be the Zariski closures of $G/Z(G)$ and $HZ(G)/Z(G)$ respectively in $\mathrm{GL}_m(\Omega)$. Then $\bar{H}$ is a normal soluble subgroup of $\bar{G}$. Let $\bar{G}^\circ$ be the connected component of 1 in $\bar{G}$. Since $H$ is normal and soluble $\bar{H}$ is contained in the soluble radical of $\bar{G}$. Thus, by [4, Lemma 19.5], $[\bar{G}^\circ, \bar{G}^\circ] \cap \bar{H}$ is virtually unipotent.

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

Let $G^\circ$ be a subgroup of $G$ containing $Z(G)$ such that $G^\circ/Z(G) = (G/Z(G)) \cap \bar{G}^\circ$. It is clear that $G^\circ$ is a subgroup of finite index in $G$. Since $G$ is finitely generated, $G^\circ$ is finitely generated and so $H_1/([G^\circ, G^\circ] \cap H_1)$ 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. □

# 6 The Weigel theorem

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

**Theorem 6.1.** *(T. Weigel,[11, Lemma 4.3,Proposition 4.4]) Let $T$ be an integrally closed noetherian commutative domain and $D$ its field of fractions. Assume that $M$ is an $T$-lattice and that soluble radical of $M_D$ is nilpotent. Then there exist a finitely generated $T$-torsion-free $T$-module $W$ and a faithful $T$-linear representation $\psi\colon M \to \mathrm{End}_T(W)$.*

# 7 Linearity of $R$-standard groups

In this section we finish the proof of Theorem 1.1.

**Theorem 7.1.** *Let $R$ be a Noetherian local pro-$p$ domain of characteristic 0 and $G$ be a finitely generated $R$-standard group. Then $G$ is $S$-linear, where $S$ is a commutative Noetherian local pro-$p$ domain of characteristic 0 and same Krull dimension as $R$.*

*Proof.* The theorem is known in the case when $K\dim R = 1$. So we suppose that $K\dim R > 1$. Let $\mathbf{F} = \mathbf{F}(\mathbf{x}, \mathbf{y})$ ($\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n)$) be the formal law associated with $G$. By Lemma 2.5 there are a commutative Noetherian local pro-$p$ domain $T$ and an injective homomorphism $\phi\colon R \to T$ such that

(i) $\phi(\mathfrak{m}^k) \subseteq \phi(\mathbf{p})T$ for some $k \in \mathbb{N}$;

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

We can extend this homomorphism to

$$\phi\colon R[[x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n]] \to T[[x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_n]]$$

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

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

Hence $\mathbf{H}$ is also a formal group law. Let $H$ be an $T$-standard group associated with $\mathbf{H}$.

Let $D$ be the ring of quotients of $R$. By Theorem 5.1, the radical of $D\otimes_R \mathbb{L}(G)$ is nilpotent. Let $E$ be the field of quotients of $T$. Then we have

$$E\otimes_T \mathbb{L}(H)=E\otimes_T (T\otimes_R \mathbb{L}(G)),$$

which clearly implies that the radical of $E\otimes_T \mathbb{L}(H)$ is also nilpotent.

Applying $\phi$, $G(\mathfrak{m}^k)$ is embedded as a closed subgroup into $H(\mathbf{p}T)$:

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

By Theorem 6.1, $\mathbb{L}(H)$ acts faithfully on a finitely generated $T$-torsion-free T-module $W$. Hence, by Corollary 4.6, $G(\mathfrak{m}^k)\leq H(\mathbf{p}T)$ acts faithfully on $W$. By Theorem 2.1, $G(\mathfrak{m}^k)$ is linear over some commutative Noetherian local pro-$p$ domain $S$ of characteristic 0 and same Krull dimension as $R$. □

# References


[1] N. Bourbaki, *Lie groups and Lie algebras*, Spinger-Verlag, 1989.

[2] R. Camina, M du Sautoy, Linearity of $\mathbb{Z}_p[[t]]$-perfect groups, to apper in Geom. Ded.

[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] I. Kaplansky, "Commutative Rings", Allyan and Bacon, Inc., Boston, 1970.

[7] E. I. Khukhro, *p-Automorphisms of Finite p-groups*, Cambridge University Press, Cambridge, 1998.

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

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

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

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

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