UNIPOTENT GROUPS OVER A DISCRETE VALUATION RING (AFTER DOLGACHEV-WEISFEILER)

Jilong Tong

Contents

Introduction

The theory of unipotent algebraic groups, and in particular that of commutative unipotent algebraic groups, over a field represents a very beautiful theory (see for example [**3**] [**10**] [**14**] [**16**]), which plays also an important role of in the study of algebraic groups over a field. Hence we can also expect that over a general base scheme, a study of unipotent group scheme can give applications in the study of family of algebraic groups. On the other hand, family of unipotent group arises also naturally in practice, and leads to interesting questions of affine schemes.

In Exposé XVII of [**5**], a general theory of unipotent groups over a field or over a general base scheme is given. Besides of this, one can still find in Exposé XXVI of [**6**] some studies of family of unipotent groups, but only in a very special case, namely, the unipotent radical of a parabolic subgroup of some reductive group. In [**20**], Dolgachev and Weisfeiler proposed a theory of

Key words and phrases. — unipotent group scheme, p-polynomial scheme, models.

unipotent groups in a more general setting. More precisely, the authors of *loc. cit.* considered affine unipotent group schemes G flat over an affine integral scheme $S = \mathrm{Spec}(R)$ such that the generic fiber is isomorphic to an affine space as scheme, and they got many interesting properties about such group schemes. For example, if R is a discrete valuation ring, the authors were able to find a family of good generators of the affine ring $R[G]$ of G/S and determined all the relations between these generators. When R is of equal characteristic $p > 0$ and if $G_K \simeq \mathbb{G}_{a,K}^n$, they proved that the group scheme G/S is a so-called p-polynomial S-scheme. With this result and suppose moreover that G/S has smooth connected fibers, together with some computations with the p-polynomials, the authors proved that the groups scheme G/S is isomorphic to $\mathbb{G}_{a,S}^n$ after an eventual extension of discrete valuation rings of R. Besides of these, one finds in *loc. cit.* also many results concerning deformations and cohomology of such group schemes.

The present report is then an attempt to understand the papers [**20**] of Dolgachev-Weisfeiler. Since the majority of the results in *loc. cit.* are based on the assumption that the base scheme S is the spectrum of a discrete valuation ring, in this report, we will work mainly over such a base. This report contains *no* original result, and every statement in this report is contained in [**20**] (or [**3**], [**11**]), though in some places, the treatments given here are slightly different from the original ones in [**20**]. But of course, I am responsible for any error in this report.

This is the expanded version of a talk given in the summer school in Luminy organized in the occasion of the reprint of SGA3. The author wants to thank P. Gille for the kind invitation. During the preparation of this notes, the author benefits from the communications with M. Raynaud, Q. Liu and D. Tossici, he thanks them sincerely.

1. Notations and reviews

1.1. Notations and conventions. —

1.1.1. Unless mentioned explicitly, in this report, the letter R denotes always a discrete valuation ring, with K its fraction field and k it residue field. Moreover, we note by S the spectrum of R.

1.1.2. Let X_K be a scheme of finite type over K. In this report, a *model* of X_K over S will be a *flat* S-morphism of finite type X/S whose generic fiber is X_K.

1.1.3. For $m, n \in \mathbb{Z}$ tow integers such that $m \leq n$, we will denote by $[m, n]$ the set $\{m, m+1, \cdots, n\} \subset \mathbb{Z}$.

1.1.4. Let $i \in [1, n]$, and for any $r \in \mathbb{Z}_{\geq 0}$, we will denote by

$$m(i,r) = (0, \cdots, 0, r, 0, \cdots, 0) \in \mathbb{Z}^n_{\geq 0}$$

where the integer r is located in the i-th component.

1.1.5. For G an affine group scheme over an affine scheme $\mathrm{Spec}(A)$, we denote by $A[G]$ the function ring of G, and by

$$\mu : A[G] \to A[G] \otimes_A A[G]$$

its map of comultiplication. Moreover, we denote by $\eta : A[G] \to A[G] \otimes_A A[G]$ the morphism obtained by

$$x \mapsto \mu(x) - x \otimes 1 - 1 \otimes x.$$

1.2. Unipotent groups over a field: definitions and examples. —

1.2.1. Let k be a *algebraically closed* field, and G be a group scheme over k. Recall that the group scheme G is *unipotent* if it verifies one of the following two equivalent conditions:

- G has a central composition series of the form
$$0 = H_0 \subset H_1 \subset \cdots H_{r-1} \subset H_r = G$$
whose successive quotients H_i/H_{i-1} for $i = 1, 2, \cdots, r$ are isomorphic to an algebraic subgroup of $\mathbb{G}_{a,k}$ ([**5**] Exposé XVII, Définition 1.1).
- G is affine, and in its function ring $k[G]$, there exist generators $t_1, \cdots, t_n$ of $k[G]$ as k-algebra such that the comultiplication map μ verifies
$$\mu(t_i) = t_i \otimes 1 + 1 \otimes t_i + \sum_j a_{ij} \otimes b_{ij}, \quad \forall i = 1, \cdots, n$$
with $a_{ij}, b_{ij} \in k[t_1, \cdots, t_{i-1}]$ ([**15**] Chap. VII § 1.6, Remarque 2).

1.2.2. More generally, until the end of §1.2, let k be an arbitrary field, with $\bar{k}$ an algebraic closure of k. A group scheme G/k is called *unipotent* if the $\bar{k}$-group scheme $G_{\bar{k}} := G \times_{\mathrm{Spec}(k)} \mathrm{Spec}(\bar{k})$ is unipotent in the sense of § 1.2.1. When the group scheme G/k is smooth and connected group scheme, then the condition that G/k is unipotent is also equivalent to the following condition ([**5**] Exposé XVII, Proposition 4.1.1):

- G has a composition series whose successive quotients are forms of $\mathbb{G}_{a,k}$.

In particular, once the base field k is *perfect*, since there is no non trivial form of $\mathbb{G}_{a,k}$ over k (*loc. cit.,* Lemme 2.3 bis), G has a composition series whose successive quotients are isomorphic to $\mathbb{G}_{a,k}$. As a result, its underlying scheme is isomorphic to some affine space $\mathbb{A}^n_k$. More generally, without the perfectness of the field k, we have the following result due to Lazard.

Proposition 1.1 **(Lazard [3] IV § 4 n° 4, Théorème 4.1)**

Let G/k be an affine k-group scheme. The following three assertions are equivalents:

- *There is an isomorphism of k-*schemes *$G \simeq \mathbb{A}_k^n$ with $n = \dim(G)$;*
- *G has a composition series with successive quotients isomorphic to $\mathbb{G}_{a,k}$;*
- *G is reduced and solvable. Moreover, there exists integer $N \geq 1$ and a dominant morphism of k-schemes $\mathbb{A}_k^N \to G$.*

Definition 1.2 **([17] Chapter IV Definition 4.1.2)**

A connected k-unipotent group scheme G/k is call *k-split* (or *split over k*), if G/k verifies one of the three equivalent conditions in Proposition 1.1.

Hence, for G/k *split* over k of dimension n, one can find generators $x_1, \cdots, x_n$ of $k[G]$ such that the comultiplication map satisfies

$$\mu(x_i) = x_i \otimes 1 + 1 \otimes x_i + \sum_{ij} a_{ij} \otimes b_{ij}$$

with $a_{ij}, b_{ij} \in k[x_1, \cdots, x_{i-1}]$. In the following, such a family of generators of $k[G]$ will be called *primitive*. In this report, we are mainly interested in such unipotent groups and their affine models over a discrete valuation ring.

1.2.3. Some examples of unipotent groups. — Let G be a smooth connected unipotent group over a field k of characteristic $p > 0$.

1. If G is of one dimensional, then G is a form of the additive group $\mathbb{G}_{a,k}$. Hence if k is perfect, $G \simeq \mathbb{G}_{a,k}$. But over an imperfect field, there exists non trivial form of $\mathbb{G}_{a,k}$. For example, let $a \in k - k^p$, and consider the following closed subgroup scheme of $\mathbb{G}_k^2 = \mathrm{Spec}(k[x,y])$ defined by the following equation
$$x + x^p + ay^p = 0$$
which can be trivialized by the inseparable extension $k \subset k(a^{1/p})$.
2. For $r \in \mathbb{Z}_{\geq 1}$, let
$$\Phi_r(X) = \frac{1}{p} \sum_{i=1}^{p^r-1} \binom{p^r}{i} X^i \otimes X^{p^r-i} \in \mathbb{Z}[X] \otimes \mathbb{Z}[X].$$
We consider the k-algebra of polynomials in two variables $k[x,y]$, and define the following map $\mu : k[x,y] \to k[x,y] \otimes k[x,y]$ by:
$$\mu(x) = x \otimes 1 + 1 \otimes x, \quad \mu(y) = y \otimes 1 + 1 \otimes y + \sum_{r \geq 1} a_r \Phi_r(x)$$
for $a_r \in k$ such that $a_r = 0$ for almost all r. We verify that this gives a structure of Hopf algebra on $k[x,y]$, and the group scheme obtained in this way is an extension of $\mathrm{Spec}(k[x]) = \mathbb{G}_{a,k}$ by $\mathrm{Spec}(k[x,y]/(x)) = \mathbb{G}_{a,k}$, which is also commutative. Conversely, any k-split two dimensional

(connected) commutative unipotent group is given by such formulas ([**3**] II § 3 4.6 théorème).

Finally, we refer to [**10**] for a detail discussion of unipotent groups over general fields. See also [**3**] [**14**] and [**16**].

1.3. Characteristic zero case. — Let S be an arbitrary noetherian base scheme, and G/S be a *flat* S-group scheme of finite type. Recall that G/S is *unipotent* if the geometric fibers of G/S are unipotent groups in the sense of §1.2. In this section, we will briefly review the results of unipotent group schemes when the base S is of characteristic *zero*, *i.e.,* is a scheme over $\mathbb{Q}$. Under this assumption, according to a result of Cartier, the group scheme G/S has smooth fibers, and hence G/S is smooth by the flatness of G/S. Moreover, over an algebraically closed field of characteristic zero, the only subgroup scheme of $\mathbb{G}_a$ is (0) and $\mathbb{G}_a$ itself ([**5**] Exposé XVII Proposition 1.5), the group scheme G/S has hence connected fibers. As a result, the group scheme G/S is separated ([**4**] Exposé VI Corollaire 5.5).

1.3.1. Exponential maps. — Let S be a noetherian scheme of characteristic *zero*, and G be a group scheme *flat* of finite type over S. Let $\mathrm{Spec}(R)$ be an affine scheme over S, we will denote by an element of $G(R[[T]])$ (*resp.* of $G(R[T])$) by the functional symbol like $f(T)$. For any complete linear topology R-algebra A (*resp.* any R-algebra A), and any element $t \in A$ which is topologically nilpotent (*resp.* any element $t \in A$), we denote by $f(t) \in G(A)$ the image of $f(T) \in G(R[[T]])$ in $G(A)$ (*resp.* of $f(T) \in G(R[T])$ in $G(A)$) by the canonical map $G(R[[T]]) \to G(A)$, which is induced by $R[[T]] \to A$ sending T to $t \in A$ (*resp.* by $R[T] \to R$ sending T to $t \in A$).

Proposition 1.3 **([3] II § 6 n° 3).** — 1. *Pour each* $x \in \mathrm{Lie}(G_R) = \ker(G(R[\varepsilon]) \to G(R))$*, there exists a unique element* $e^{Tx} \in G(R[[T]])$ *such that*

- $e^{\varepsilon x} = x \in G(R[\varepsilon])$;
- $e^{(T+T')x} = e^{Tx} \cdot e^{T'x} \in G(R[[T, T']])$.

Moreover, let $x, y \in \mathrm{Lie}(G_R)$ *be two elements verifying* $[x, y] = 0$*, then*

$$e^{T(x+y)} = e^{Tx} \cdot e^{Ty}.$$

2. *Let* V *be a vector bundle on* S*, and* $G = \mathrm{GL}(V)$*. Then for any element* $x \in \mathrm{Lie}(G_R) = \mathrm{End}_R(V \otimes_{\mathcal{O}_S} R)$*, we have*

$$e^{Tx} = \sum_{i \geq 0} \frac{T^i x^i}{i!} \in \mathrm{GL}(V \otimes_{\mathcal{O}_S} R[[T]])$$

In particular, if $x \in \mathrm{End}_R(V \otimes_{\mathcal{O}_S} R)$ *is* nilpotent*, we have* $e^{Tx} \in G(R[T])$.

Corollary 1.4 **([3] II § 6 n° 3 Corollaire 3.5)**. — *Let $\rho\colon G \hookrightarrow \mathrm{GL}_n(V)$ be a faithful representation of G on a vector bundle V of finite rank over S. If $x \in \mathrm{Lie}(G_R) \subset \mathrm{End}(V_R)$ is nilpotent. Then $e^{Tx} \in G(R[T]) \subset G(R[[T]])$.*

Let G/S be a unipotent group scheme which can be realized as subgroup scheme of some $\mathrm{GL}(V)$ for some vector bundle V on S by the morphism $\rho\colon G \to \mathrm{GL}(V)$. This latter morphism induces a morphism between their Lie-algebras:

$$\mathrm{Lie}(\rho)\colon \mathrm{Lie}(G) \to \mathrm{Lie}(\mathrm{GL}(V)) = \mathrm{End}(V)$$

Since G/S has unipotent fibers and the base S is noetherian, the image of the previous map $\mathrm{Lie}(\rho)$ is contained in the set of nilpotent endomorphisms of V. In particular, we can apply the construction that we sketched here. Hence, for any affine scheme $\mathrm{Spec}(R)$ over S, and for any $x \in \mathrm{Lie}(G_R)$, we have $e^{Tx} \in G(R[T])$. Now, we consider the morphism of R-algebras $R[T] \to R$ sending T to $1 \in R$, and the inducing morphism of groups

$$G(R[T]) \to G(R)$$

we get hence an element $e^x := e^{x\cdot 1} \in G(R)$, and hence a map $\mathrm{Lie}(G_R) \to G(R)$. More generally, we get in such a way a morphism of S-schemes (called the *exponential map* of the unipotent group scheme G/S):

$$\exp\colon \mathbb{W}(\mathrm{Lie}(G)) \to G, \quad x \mapsto e^x. \tag{1}$$

whose geometric fibers are isomorphisms of schemes ([3] IV § 2 n° 4 Proposition 4.1). Since the two S-schemes are smooth of finite type, this implies then the exponential map (1) is an isomorphism of S-schemes.

1.3.2. Exponential map over a normal base. — With the help of [11], it is possible to extend the construction of exponential map in the previous § to unipotent group schemes over a general normal base scheme. Recall that S of characteristic zero, and for G/S a (flat) unipotent group scheme, its Lie-algebra $\mathrm{Lie}(G)$ is nilpotent. Hence, by using the Baker-Campbell-Hausdorff formula, $\mathbb{W}(\mathrm{Lie}(G))$ becomes an S-group scheme which is in general not commutative (see for example [2] Chapter II § 6.5 Remark (3)).

Proposition 1.5. — *Let S be a noetherian normal scheme of characteristic zero, and G/S be a flat unipotent group. Then there is a unique morphism of S-schemes*

$$\exp\colon \mathbb{W}(\mathrm{Lie}(G)) \to G$$

which can be characterized by the following condtions:

(a) $\exp$ *sends the zero section of* $\mathbb{W}(\mathrm{Lie}(G))$ *to the neutral element e of G/S;*
(b) $\exp(n \cdot x) = \exp(x)^n \in G$ *for any local section x of* $\mathbb{W}(\mathrm{Lie}(G))$*;*

(c) *The induced map of* exp *between the tangent spaces*

$$\mathrm{T}_0(\exp)\colon \mathrm{Lie}(G) \simeq \mathrm{T}_0(\mathbb{W}(\mathrm{Lie}(G))) \to \mathrm{T}_e(G) = \mathrm{Lie}(G)$$

is identity.

Moreover, if we impose the group scheme structure on $\mathbb{W}(\mathrm{Lie}(G))$ *given by the Baker-Campbell-Hausdorff formula as in* [**2**] *(Chapter II § 6.5), the exponential map above is an isomorphism of* S*-group schemes.*

Proof. — Since G/S is separated and $\mathbb{W}(\mathrm{Lie}(G))$ is flat over S, to prove the uniqueness, we only need to verify the corresponding statement over the generic point of S. Hence, we are reduced to the case where $S = \mathrm{Spec}(K)$ is the spectrum of a field of characteristic zero. By Galois descent, we can even assume that K is algebraically closed. Let f, g two morphism of S-schemes verifying the three properties (a)-(c) of the proposition. Since K is algebraically closed, we only need to show that $f(x) = g(x)$ for for any $x \in \mathrm{Lie}(G) = \mathbb{W}(\mathrm{Lie}(G))(K)$. Let $\mathfrak{g} = K \cdot x \subset \mathrm{Lie}(G)$ be the linear subspace generated by such a $x \in \mathrm{Lie}(G)$. This gives a Lie-subalgebra of $\mathrm{Lie}(G)$. We consider then the compositions f', g' of f, g with the following canonical map

$$\mathbb{W}(\mathfrak{g}) \to \mathbb{W}(\mathrm{Lie}(G)).$$

According to our assumption on f and g, the two maps f' and g' induces the same morphisms between the tangent spaces on 0, and also verify

$$f'(ny) = f'(y)^n, \quad g'(ny) = g'(y)^n \quad \forall y \in \mathbb{W}(\mathfrak{g}).$$

As a result, both maps are morphisms of groups schemes over S. Hence, the kernel H of the double morphism

$$\begin{tikzcd} \mathbb{W}(\mathfrak{g}) \arrow[r, shift left, "f'"] \arrow[r, shift right, "g'"'] & G \end{tikzcd}$$

is an algebraic subgroup of $\mathbb{W}(\mathfrak{g})$. On the other hand, since f', g' have the same induced map bwtween the tangent spaces, this implies that $\mathrm{Lie}(H) = \mathrm{Lie}(\mathbb{W}(\mathfrak{g})) = \mathfrak{g}$. Since K is of characteristic zero, we get $H = \mathbb{W}(\mathfrak{g})$. Hence $f' = g'$. In particular, $f(x) = g(x)$, as is required.

It remains to prove the existence of such a morphism under our assumption on the base. Recall that by the Baker-Campbell-Hausdorff formula, $\mathbb{W}(\mathrm{Lie}(G))$ becomes a smooth group scheme over S with connected fibers. We will first construct the exponential map when the base S is local normal of dimension one. In this case, on applying the Lemma IX 2.2 of [**11**], G/S can be realized as a closed subgroup scheme of GL_n for some integer n. Hence one can construct the exponential map as in § 1.3.1

$$\exp\colon \mathbb{W}(\mathrm{Lie}(G)) \to G.$$

By the Proposition 1.3, the morphism of schemes exp verifies the properties (a)-(c) of the proposition. To see that exp is a morphism of groups, since our group scheme G/S is separated and $\mathbb{W}(\mathrm{Lie}(G))$ is flat over S, we are reduced to show the similar result between the generic fibers, which is then well-known ([**3**] IV § 2, 4.3). Finally, we proceed to the general case. According to the Corollary IX 1.4 of [**11**] and the fact that $\mathbb{W}(\mathrm{Lie}(G))/S$ is smooth with connected fibers, we only need to construct the morphism exp over an open subset $W \subset S$ contain every point of S of depth ≤ 1. Hence, we are reduced to prove that for any point $s \in S$ of depth ≤ 1, there exists some open subset $V \subset S$ containing s, and a morphism $\mathbb{W}(\mathrm{Lie}(G_W)) \to G_W$ inducing the usual exponential map on the generic fibers. Hence, up to replace S by its localization at $s \in S$, we are reduced to the previous case. This finishes the proof. □

2. Generators of the R-algebra $R[G]$

In this part, $S = \mathrm{Spec}(R)$ is the spectrum of a discrete valuation ring. Let G be a flat affine group scheme of finite type over S such that its generic fiber G_K is *K-split* in the sense of Definition 1.2. The aim of this section is to explain the existence of good generators of $R[G]$ as an R-algebra. Let us begin with some preparations on the lexicographic order defined on the ring of polynomials.

2.1. Lexicographic orders. — Let $n > 0$ be an integer, we consider the ring $K[x_1, x_2, \cdots, x_n]$ of polynomials in n variables with coefficients in K. To denote a monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, we will use the usual abbreviation x^n, where $x = (x_1, \cdots, x_n)$ and $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. For any $\alpha, \alpha' \in \mathbb{Z}_{\geq 0}^n$, we introduce the so-called *lexicographic order*: $\alpha > \alpha'$ if there is some integer $i \in [1, n]$ such that $\alpha_i > \alpha_i'$ and that $\alpha_j = \alpha_j'$ for any $j \in [i+1, n]$. In particular, this gives a *total* order on $\mathbb{Z}_{\geq 0}^n$, and $(1, 0, \cdots, 0)$ is the minimal element different from $0 = (0, 0, \cdots, 0)$ in $\mathbb{Z}_{\geq 0}^n$. In this report, the maximum "max" is always taken relative to this order.

Lemma 2.1. — *The lexicographic order of $\mathbb{Z}_{\geq 0}^n$ satisfies the decreasing chain condition: for $\alpha_i \in \mathbb{Z}_{\geq 0}^n$ such that*

$$\alpha_0 \geq \alpha_1 \geq \cdots \geq \alpha_i \geq \alpha_{i+1} \geq \cdots, \tag{2}$$

there exists some $i_0 \in \mathbb{Z}_{\geq 0}$ sufficiently large such that $\alpha_i = \alpha_{i_0}$ for any $i \geq i_0$.

Proof. — Let $\alpha_i = (a_{i,1}, a_{i,2}, \cdots, a_{i,n})$. According to the definition of lexicographic order, we must have the following descending sequence of non negative integers:

$$a_{1,n} \geq a_{2,n} \geq \cdots \geq a_{i,n} \geq \cdots$$

As a result, for some $i_0 \gg 0$, and for any $i \geq i_0$, we must have $a_{i,n} = a_{i_0,n}$. Up to remove all the first i_0 terms of the sequence (2), we may assume that $a_{i,n} = a_{1,n}$ for all $i \geq 0$. Hence, one must have

$$a_{1,n-1} \geq a_{2,n-1} \geq \cdots \geq a_{i,n-1} \geq \cdots$$

The same argument shows that up to remove again finitely many first terms in the sequence (2), we may assume further more that $a_{i,n-1} = a_{1,n-1}$ for all $i \geq 0$. After at most n repetitions of this argument, and up to remove finitely many terms of the sequence (2), we find that $\alpha_i = \alpha_0$ for any $i \geq 0$. This gives the lemma. □

Corollary 2.2. — *Any non empty subset of $\mathbb{Z}^n_{\geq 0}$ has a minimal element relative to the lexicographic order.*

Definition 2.3. — For any polynomial $f = \sum_\alpha a_\alpha x^\alpha \in K[x_1, \cdots, x_n]$, we define its *degree*, denoted by $\deg(f)$, by the element of $\mathbb{Z}^n_{\geq 0}$ given by the following formula

$$\deg(f) = \max\{\alpha \mid a_\alpha \neq 0\}.$$

Now, let X be an affine model (1.1.2) of the affine space

$$\mathbb{A}^n_K = \mathrm{Spec}(K[x_1, x_2, \cdots, x_n]),$$

with $R[X]$ its affine ring, which is an R-algebra of finite type. From the flatness of $R[G]$ over R, we can view $R[G]$ naturally as an R subalgebra of $K[x_1, x_2, \cdots, x_n]$. Hence, for any $f \in R[X]$, we have the well-defined notion $\deg(f)$. Following [**20**], for any $\alpha \in \mathbb{Z}^n_{\geq 0}$, we define

$$P_\alpha = \{f \in R[X] \mid \deg(f) \leq \alpha\}, \qquad \text{and} \quad P'_\alpha = \{f \in R[X] \mid \deg(f) < \alpha\}.$$

We have $P'_\alpha \subset P_\alpha$, its cokernel will be denoted by $\overline{P_\alpha}$.

Lemma 2.4. —

1. *These three R-modules are torsion free.*
2. $\dim_K(\overline{P}_\alpha \otimes_A K) = 1$.
3. *Suppose that the origin $o_K = (0, 0, \cdots, 0) \in \mathbb{A}^n_K$ can be extended to a S-section of X/S. Then the R-module $\overline{P_\alpha}$ is also of finite type. In particular, the R-module $\overline{P_\alpha}$ is free of rank 1 over R.*

Proof. — Only the third statement needs a verification. We will introduce some notations for this proof: for any $\alpha = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq}$, we put

$$|\alpha| = \sum_{i=1}^n \alpha_i.$$

and define $d(f) = \min\{|\alpha| \ : \ a_\alpha \neq 0\}$ for a polynomial f. In particular, $d(f) \geq 0$ with equality holds if and only if the polynomial f has non zero constant term.

Now, let us begin the proof. Since $R[X]$ is an R-algebra of finite type, there exist $f_1, f_2, \cdots, f_m \in K[x_1, \cdots, x_n]$ such that $R[X] = R[f_1, \cdots, f_m]$. We claim that the constant term of each f_i is contained in R. According to our assumption, the origin o_K of $X_K = \mathbb{A}^n_K$ can be extended to an S-section of X/S, hence there exists an epimorphism of R-algebras $\rho : R[X] \to R$, such that its induced map on the generic fiber is the epimorphism of K-algebras given by

$$\rho_K : K[x_1, x_2, \cdots, x_n] \to K, \qquad x_i \mapsto 0.$$

If we write $f_i = c_i + f_i'$ such that $c_i \in K$ and $f_i' \in (x_1, x_2, \cdots, x_n)$, we find that $\rho_K(f_i) = \rho_K(c_i) = c_i$. On the other hand, since $\rho_K(f_i) = \rho(f_i) \in R \subset K$, we must have $c_i \in R$. Hence, up to modify f_i by $f_i - c_i$, we may assume that each f_i has zero constant term. In particular, $d(f_i) > 0$.

Now as an R-modules, $R[X]$ is generated by the elements $f^t := f_1^{t_1} f_2^{t_2} \cdots f_m^{t_m}$ for $f = (f_1, \cdots, f_m)$ and $t = (t_1, \cdots, t_m) \in \mathbb{Z}^m_{\geq 0}$. For each $t \in \mathbb{Z}^m_{\geq 0}$, let λ_t be the coefficient of the term x^α of the polynomial $f^t \in K[x_1, \cdots, x_n]$, et $\Lambda \subset K$ be the R-submodule generated by these coefficients. Then Λ is also the set of coefficients of the term x^α of the elements in $R[G]$. Since $d(f^t) = \sum_{i=1}^m d(f_i) \cdot t_i$, we find that $\lambda_t = 0$ once the following inequality is satisfied:

$$\sum_{i=1}^m t_i \cdot d(f_i) > |\alpha|.$$

Since the complement of the elements $t \in \mathbb{Z}^m_{\geq 0}$ verifying the inequality above is *finite* (because $d(f_i) > 0$ for all i), there is only finitely many $t \in \mathbb{Z}^m_{\geq 0}$ such that $\lambda_t \neq 0$. As a result, the R-module Λ is of finite type over R. Now we consider the subset Λ' of K formed by the element $\lambda \in K$ such that, there exist an element $g \in P_\alpha$ with λ as its coefficient of the term x^α. This is a R-submodule of K, which is also contained in Λ. Hence Λ' is also of finite type over R, this means exactly that the R-module $\overline{P_\alpha}$ is of finite type. This finishes the proof. □

2.2. Linear unipotence of affine group models of a unipotent group. —

2.2.1. Let G/S be an affine flat group scheme of finite type over S, such that its generic fiber is *split* (Definition 1.2). In particular, we can find $x_1, \cdots, x_n \in K[G_K]$ such that $K[G_K] = K[x_1, x_2, \cdots, x_n]$ and that

$$\mu(x_i) = x_i \otimes 1 + 1 \otimes x_i + \sum_j a_{ij} \otimes b_{ij} \tag{3}$$

with μ the comultiplication map, and $a_{ij}, b_{ij} \in K[x_1, \cdots, x_{i-1}]$. In the following, we will fix once for all such a primitive family of generators of $K[G_K]$.

Since G/S is a affine group scheme and because of the choice of the primitive family $\{x_1, \cdots, x_n\}$, the zero section of $G_K = \mathrm{Spec}(K[x_1, \cdots, x_n])$ can be extended to a section of G over S (*i.e.*, the neutral element of G/S), the S-scheme satisfies hence the assumption of Lemma 2.4 (3). In particular, for each $\alpha \in \mathbb{Z}^n_{\geq 0}$, the corresponding R-module $\overline{P_\alpha}$ is free of rank 1. For each $\alpha \in \mathbb{Z}^n_{\geq 0}$, let $z_\alpha \in P_\alpha$ an element whose image in $\overline{P_\alpha}$ gives a basis over R. Then $R[G]$ is a free R-module with a basis given by the family $\{z_\alpha : \alpha \in \mathbb{Z}^n_{\geq 0}\}$. Moreover, as an R-module, $R[G] \otimes_R R[G]$ is free with a basis given by $\{z_\alpha \otimes z_\beta : \alpha, \beta \in \mathbb{Z}^n_{\geq 0}\}$. This family gives also a basis of $K[G_K] \otimes K[G_K]$ over K, and an element

$$\sum_{\alpha,\beta} a_{\alpha,\beta} z_\alpha \otimes z_\beta \in K[G_K] \otimes K[G_K], \quad a_{\alpha,\beta} \in K$$

is contained in $R[G] \otimes R[G] \subset K[G_K] \otimes K[G_K]$ if and only if the coefficients $a_{\alpha,\beta} \in R$ for any $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. In the following, to simplify the presentation, we will use the following notations: let $\alpha \in \mathbb{Z}^n_{\geq 0}$, we put

- $M := R[G] \otimes_R R[G]$, $M_K = M \otimes_R K = K[x_1, \cdots, x_n] \otimes_K K[x_1, \cdots, x_n]$;
- $M_{K,\alpha} \subset M_K$ (resp. $\widetilde{M_{K,\alpha}}$) the subspace generated over K by the elements $a \otimes b$ verifying the following properties:

$$\begin{gathered} \deg(a) < \alpha, \quad \deg(b) < \alpha, \quad \text{and} \\ \deg(a) + \deg(b) \leq \alpha \;\; (\text{resp. } \deg(a) + \deg(b) < \alpha). \end{gathered}$$

- $M_\alpha := M_{K,\alpha} \cap M$, and $\widetilde{M_\alpha} := \widetilde{M_{K,\alpha}} \cap M$.

For any $a \otimes b \in M_K$, we define $\deg(a \otimes b) := \deg(a) + \deg(b)$.

Lemma 2.5. — *Let $\mu : R[G] \to R[G] \otimes R[G]$ the comultiplication map of the group scheme G/S. Then for any $y \in R[G]$, we have*

$$\mu(y) \equiv y \otimes 1 + 1 \otimes y \mod M_{\deg(y)}.$$

Proof. — Let $\alpha_0 = \deg(y)$. According to the formula (3), we have

$$\mu(y) - (y \otimes 1 + 1 \otimes y) = \sum_\ell a_\ell \otimes b_\ell \in K[x_1, \cdots, x_n] \otimes K[x_1, \cdots, x_n].$$

such that the following two conditions are satisfied: (1) $\deg(a_\ell) < \alpha_0$, $\deg(b_\ell) < \alpha_0$; (2) $\deg(a_\ell) + \deg(b_\ell) \leq \alpha_0$. Since $z_\alpha \in P_\alpha$ which generates also $\overline{P_\alpha} \otimes_R K$ over K, there exist $c_{\alpha,\beta} \in K$ such the following equality holds:

$$\sum_\ell a_\ell \otimes b_\ell = \sum_{\substack{\alpha<\alpha_0, \beta<\alpha_0 \\ \alpha+\beta\leq\alpha_0}} c_{\alpha,\beta} z_\alpha \otimes z_\beta$$

On the other hand, since $y \in R[G]$, $\mu(y) - y \otimes 1 - 1 \otimes y \in R[G] \otimes R[G]$. Moreover, since the family $\{z_\alpha \otimes z_\beta : \alpha, \beta \in \mathbb{Z}^n_{\geq 0}\}$ is a basis of the free R-module $R[G] \otimes R[G]$, the coefficients $c_{\alpha,\beta}$ in the previous equality must lie in R. From this, we get the conclusion. □

Corollary 2.6. — *Let $\alpha = (t_1, t_2, \cdots, t_s, 0, \cdots, 0)$, $\beta = (0, \cdots, 0, t_{s+1}, \cdots t_n)$ two elements in $\mathbb{Z}^n_{\geq 0}$. Then the image of $z_\alpha \cdot z_\beta \in P_{\alpha+\beta}$ in $\overline{P}_{\alpha+\beta}$ gives also a basis of this free R-module of rank* 1.

Proof. — By the Lemma 2.4 (iii), there exists $a \in R$ such that $az_{\alpha+\beta} - z_\alpha z_\beta \in P'_{\alpha+\beta} \subset R[G]$. We only need to prove that $a \in R^*$. According to the previous Lemma 2.5, we have $\eta(az_{\alpha+\beta} - z_\alpha z_\beta) \in \widetilde{M}_{\alpha+\beta}$. On the other hand, since $z_{\alpha+\beta} \in R[G]$, it follows that $\eta(z_{\alpha+\beta}) \in R[G] \otimes R[G] = M$, hence

$$\frac{1}{a}\eta\left(z_\alpha z_\beta\right) = \eta(z_{\alpha+\beta}) + \frac{1}{a}\eta(z_\alpha z_\beta - az_{\alpha+\beta}) \in M + \widetilde{M}_{K,\alpha+\beta}.$$

Now

$$\begin{aligned} \eta(z_\alpha z_\beta) &= \mu(z_\alpha)\mu(z_\beta) - z_\alpha z_\beta \otimes 1 - 1 \otimes z_\alpha z_\beta \\ &= (z_\alpha \otimes 1 + 1 \otimes z_\alpha + \eta(z_\alpha)) \cdot (z_\beta \otimes 1 + 1 \otimes z_\beta + \eta(z_\beta)) \\ &\quad - z_\alpha z_\beta \otimes 1 - 1 \otimes z_\alpha z_\beta \\ &= z_\alpha \otimes z_\beta + z_\beta \otimes z_\alpha + (z_\alpha \otimes 1 + 1 \otimes z_\alpha) \cdot \eta(z_\beta) \\ &\quad + (z_\beta \otimes 1 + 1 \otimes z_\beta) \cdot \eta(\alpha) + \eta(\alpha) \cdot \eta(\beta). \end{aligned}$$

By the assumptions on α and β, for any $\alpha' \leq \alpha$, and any $\beta' < \beta$, we have $\alpha' + \beta' < \beta$, and since $\eta(z_\alpha) \in M_\alpha$ $\eta(z_\beta) \in M_\beta$, the following sum

$$(z_\alpha \otimes 1 + 1 \otimes z_\alpha) \cdot \eta(z_\beta) + (z_\beta \otimes 1 + 1 \otimes z_\beta) \cdot \eta(\alpha) + \eta(\alpha) \cdot \eta(\beta).$$

does not contain the term $z_\alpha \otimes z_\beta$. As a result, the coefficient of the term $z_\alpha \otimes z_\beta$ in $\eta(z_\alpha z_\beta)$ is equal to 1. Hence, in order that $\frac{1}{a}\eta(z_{\alpha z_\beta}) \in M + \widetilde{M}_{K,\alpha+\beta}$, it is necessary that $\frac{1}{a} \in R$. This proves that $a \in R$ is a unit. □

2.2.2. Since $R[G]$ is finitely generated as an R-algebra, there exist finitely many $\alpha_1, \cdots, \alpha_t$ such that $R[G]$ is generated by these z_{α_i} $(1 \leq i \leq t)$ as an R-algebra. In fact, we can do better here.

Definition 2.7. — We define by induction a family of element $\{y_i\} \subset R[G]$ verifying the following two properties: (i) $y_1 = z_{(1,0,\cdots,0)}$; (ii) for $i \geq 1$, y_{i+1} is the first z_α such that $\deg(z_\alpha) > \deg(y_i)$ and $z_\alpha \notin R[y_1, y_2, \cdots, y_i]$ (here if such a z_α does not exist, then we stop and get a finite family).

Lemma 2.8. — *The construction in 2.7 stops after finitely many steps.*

In order to prove this lemma, we need some preparations. Recall that we have chosen $\{x_1, \cdots, x_n\}$ is a primitive family of generators of $K[G_K]/K$, hence for any integer $r \in [1, n]$, the K-scheme $H_K = \mathrm{Spec}(K[x_1, \cdots, x_r])$ has a group scheme structure. Moreover, the canonical injection $K[x_1, \cdots, x_r] \subset K[x_1, \cdots, x_n]$ gives us a surjective morphism of K-algebraic groups:

$$G_K \to H_K.$$

Its kernel is the subgroup scheme F_K of G_K defined by the ideal $(x_1, x_2, \cdots, x_r) \subset K[x_1, \cdots, x_n]$. Let F be the schematic closure of F_K in G, which is a flat finite type subgroup scheme of G_K.

Lemma 2.9. — *With the notations as above.*

1. *The quotient G/F is representable by a group scheme H flat affine of finite type over S, and its generic fiber is $H_K = \mathrm{Spec}(K[x_1, \cdots, x_r])$.*
2. *If we identify $R[H]$ as a subalgebra of $K[H_K]$ which itself is contained in $K[x_1, \cdots, x_n]$, then*

$$R[H] = R[G] \cap K[x_1, \cdots, x_r].$$

In particular, the last intersection is of finite type over R as an R-algebra.

Proof. — The first assertion (1) follows from the general result of Artin and Raynaud. More precisely, according to 8.4/9 of [**1**], the fppf quotient $H = G/F$ is representable by an algebraic space over S. Since $F \hookrightarrow G$ is a closed subgroup scheme over S, it follows that the quotient H is separated. By by a theorem of Raynaud (Théorème 3.3.1 of [**12**]), this algebraic space is representable by an S-group scheme, necessarily flat and of finite type over S. Since our basis S is normal of dimension 1, the affineness of H/S follows then from the Lemma IX 2.2 of [**11**] since the generic fiber H_K, being a quotient of an affine K-group scheme G_K, is affine.

For (2), since $H = G/F$, H is the cokernel of the double morphism

$$\begin{tikzcd} F \times G \arrow[r, shift left, "\mathrm{pr}_2"] \arrow[r, shift right, "m"'] & G \end{tikzcd}$$

where $\mathrm{pr}_2 : F \times G \to G$ is the projection to the second factor, and $m : F \times G \to G$ is the multiplication map. As a result, a morphism $h : G \to \mathbb{A}^1_S$ can factor through the surjection $G \to F$ if and only if $h \circ \mathrm{pr}_2 = h \circ m$. Since G/S is separated, the last condition is equivalent to the corresponding equality in the generic fiber: $h_K \circ \mathrm{pr}_{2,K} = h_K \circ m_K$, which is again equivalent to the fact that $h_K : G_K \to \mathbb{A}^1_K$ can factor through H_K. Hence, if we identify $K[H_K]$ and $R[G]$ as subset of $K[G_K] = K[x_1, \cdots, x_n]$, $h \in K[G_K]$ lies in $R[H]$ if and only if $h \in R[G] \cap K[H_K]$. This last statement means exactly $R[H] = R[G] \cap K[H_K]$, and hence finishes the proof of the lemma. □

Proof of Lemma 2.8. — Let $\{y_1, y_2, \cdots\}$ be a family (finite or infinite) produced by the construction in Definition 2.7. Since $R[G]$ is finitely generated over R, to prove the lemma, we only need to verify that $R[G] = R[y_1, y_2, \cdots]$. This follows that there exists some integer N such that $R[G] = R[y_1, \cdots, y_N]$, hence the construction in Definition 2.7 must stop after finitely steps.

We will prove the last statement by induction on n. The case where $n = 1$ is clear. Supposons now the lemma has been proven for the integer $n - 1 \geq 1$. We consider the subalgebra $R[G] \cap K[x_1, \cdots, x_{n-1}]$. According to Lemma 2.9, this subalgebra is finitely generated with generic fiber $K[x_1, \cdots, x_{n-1}]$, which is also the affine ring of the unipotent group H/S. Moreover, $H_K \simeq \mathbb{A}_K^{n-1}$. Hence the construction in Definition 2.7 applying to this subalgebra, together with induction hypothesis, yield finitely many elements $y_1, y_2, \cdots, y_s \in R[G] \cap K[x_1, \cdots, x_{n-1}]$ such that $R[y_1, \cdots, y_s] = R[G] \cap K[x_1, \cdots, x_{n-1}]$. The next element $y_{s+1} \in \{y_1, y_2, \cdots\}$ given by the contruction is then of degree $(0, \cdots, 0, 1)$. We will prove by induction that the elements $y_{s+1}, y_{s+2}, \cdots$ (if exist) are all of the form $(0, \cdots, 0, *)$. Suppose that we have shown this assertion for y_i with $i \geq s + 1$. If $R[y_1, y_2, \cdots, y_i] = R[G]$, then there is nothing to prove. So we suppose in the following that $R[y_1, y_2, \cdots, y_i] \neq R[G]$. Now let $r \in \mathbb{Z}_{\geq 2}$ be the first integer such that $z_{(0,\cdots,0,r)} \notin R[y_1, \cdots, y_s, \cdots y_i]$. We claim that, for $\alpha = (t_1, \cdots, t_{n-1}, t_n) < (0, 0, \cdots, r)$, we have $P_\alpha \subset R[y_1, \cdots, y_i]$. Indeed, let $\beta = (t_1, \cdots, t_{n-1}, 0)$, then $\alpha - \beta = (0, \cdots, 0, t_n)$ with $t_n < r$. Hence $z_\beta \in R[G] \cap K[x_1, \cdots, x_{n-1}] = R[y_1, \cdots, y_s]$, and $z_{\alpha-\beta} \in R[y_1, \cdots, y_s, \cdots y_i]$ (since $t_n < r$). Moreover, according to Corollary 2.6, the image of $z_\beta z_{\alpha-\beta}$ in $\overline{P_\alpha}$ generates the R-module $\overline{P_\alpha}$. Hence, for any $f \in P_\alpha$, there exists $a \in R$ such that $f - az_{\alpha-\beta}z_\beta \in P'_\alpha$ with $az_{\alpha-\beta}z_\beta \in R[y_1, \cdots, y_i]$. Now by repeating this argument and taking account Lemma 2.1, we find that $f \in R[y_1, \cdots, y_i]$. Hence $z_{(0,\cdots,0,r)}$ is the first $z_\alpha \notin R[y_1, \cdots, y_i]$, and we have $y_{i+1} = z_{(0,\cdots,0,r)}$. Finally, because of this and for the reason of degree, we find $R[G] = R[y_1, \cdots, y_s, y_{s+1}, \cdots]$. This finishes the proof. □

Corollary 2.10. — *One can find a finite family $\{y_1, y_2, \cdots, y_N\} \subset R[G]$ verifying the following properties:*

1. $R[G] = R[y_1, \cdots, y_N]$*;*
2. $\deg(y_1) < \deg(y_2) < \cdots < \deg(y_N)$*;*
3. *For each $i \geq 0$ $P'_{\deg(y_i)} \subset R[y_1, \cdots, y_{i-1}]$ (here, by convention, let $y_{-1} = 0$).*

Remark 2.11. — In the following, a family of generators in Corollary 2.10 is said to be a family of *good generators*. Clearly, good generators are not unique. For example, let $\{y_i : 1 \leq i \leq N\}$ a family of good generators, and let

$$y'_i = \lambda_i y_i + f_i, \quad \text{for } i = 1, \cdots, N,$$

with $\lambda_i \in R^*$ and $f_i \in R[y_1, \cdots, y_{i-1}]$, then $\{y_i' : 1 \leq i \leq N\}$ is still a family of good generators. Conversely, any two families of good generators can be related in the previous way.

Recall that an affine group scheme U/S is called *linearly unipotent* if there exist generators $u_1, \cdots, u_s$ of $R[U]/R$ such that

$$\mu(u_i) = u_i \otimes 1 + 1 \otimes u_i + \sum_j \lambda_{ij} a_{ij} \otimes b_{ij}$$

with $a_{ij}, b_{ij} \in R[u_1, \cdots, u_{i-1}]$. With this terminology, we have

Theorem 2.12. — *Let G be an affine group model over R of a unipotent group, where the generic fiber of G is* split *over K (Definition 1.2). Then G is linearly unipotent. In particular, G/S is a unipotent group scheme.*

Proof. — We consider a family of good generators $\{y_1, \cdots, y_N\}$ given in Corollary 2.10. For each y_i, according to Lemma 2.5, we have

$$\mu(y_i) = y_i \otimes 1 + 1 \otimes y_i + \sum a_{ij} \otimes b_{ij} \in R[G] \otimes R[G],$$

with $\deg(a_{ij}) < \deg(y_i)$ and $\deg(b_{ij}) < \deg(y_i)$. Hence by the properties of the generators $\{y_1, \cdots, y_N\}$, we find that $a_{ij}, b_{ij} \in R[y_1, \cdots, y_{i-1}]$. This implies exactly that G/S is linearly unipotent. □

2.3. Relations between the good generators. —

2.3.1. Statement of the main result. — We use the notations as in the previous §. Moreover, for $r \in [1, N]$, we set

$$\Omega_r = \{j : y_j \in K[x_1, \cdots, x_r]\}, \quad \Omega_0 = \emptyset,$$
$$\overline{\Omega_r} = \Omega_r - \Omega_{r-1}, \quad \Omega_r = [1, t_{r+1} - 1]$$
$$I = \{t_1 = 1, t_2, \cdots, t_n\}, \quad \overline{I} = [1, N] - I, \quad N = t_{n+1} - 1.$$

If $t \in \overline{\Omega_i}$, then we put $\omega(t) = i$.

Proposition 2.13. — *Keeping the notations as above.*

1. *If $t \in I$, then there exist $a_t \in K - \{0\}$, and an element $f_t \in K[y_1, \cdots, y_{t-1}]$ such that*

$$y_t = a_t x_{\omega(t)} + f_t.$$

2. *If $t \in \overline{I}$, then there exists $d_t \in \mathbb{Z}_{\geq 1}$ such that*

$$\pi^{d_t} y_t \in R[y_1, \cdots, y_{t-1}], \quad \pi^{d_t - 1} y_t \notin R[y_1, \cdots, y_{t-1}].$$

Proof. — If $t \in I$, y_t is then the first among the family $\{y_1, \cdots, y_N\}$ which is contained in $K[x_1, \cdots, x_{\omega(t)}]$. Hence, its degree must be $m(\omega(t), 1)$. Let $a_t \in K$ be the leading coefficient of y_t, then $y_t - a_t x_{\omega(t)} \in K[x_1, \cdots, x_{\omega(t)-1}]$. Now we only need to use the fact that $R[y_1, \cdots, y_{t-1}] \otimes_B K = K[x_1, \cdots, x_{\omega(t)-1}]$ to get the assertion (1). Suppose now $t \in \bar{I}$, let $r \in I$ be the biggest integer such that $r < t$. Then we have

$$R[y_1, \cdots, y_r] \subset R[y_1, \cdots, y_{t-1}] \subset R[y_1, \cdots, y_t].$$

Moreover, by the first assertion, the generic fibers of these three R-algebras are all equal to $K[x_1, \cdots, x_{\omega(t)}]$. In particular,

$$R[y_1, \cdots, y_{t-1}] \otimes_R K = R[y_1, \cdots, y_t] \otimes_R K.$$

As a result, for some integer $d \gg 0$, we have $\pi^d \cdot y_t \in R[y_1, \cdots, y_{t-1}]$. The integer d_t that we need in the second statement is then the minimal non negative integer d with this property. Moreover, since $R[y_1, \cdots, y_{t-1}] \neq R[y_1, \cdots, y_t]$, we find $d_t \geq 1$. This finishes the proof. □

The main result of this section can be stated as follows:

Theorem 2.14. — *Keeping the notations as before, and let $p = \mathrm{char}(R/\pi) \neq 0$. Then we can find a family of good generators $\{y_1, \cdots, y_N\}$ such that*

$$\pi^{d_i} y_i = y_{i-1}^{p^{r(i)}} + \sum_{\alpha < m(i-1, p^{r(i)})} a_{i,\alpha} y^\alpha, \quad \forall i \in \bar{I}$$

with the following two properties:

(a) $r(i) \in \mathbb{Z}_{\geq 1}$ *for all* $i \in \bar{I}$;

(b) *The sum*

$$\sum_{\alpha < m(i-1, p^{r(i)})} a_{i,\alpha} y^\alpha$$

has coefficients $a_{i,\alpha} \in R$, and it is reduced with respect to the integers $r(i)$ ($\forall i \in \bar{I}$) in the sense of the Definition 2.15 below.

(c) $\pi^{d_i} | p$, *where $d_i \in \mathbb{Z}$ is the integer in Proposition 2.13.*

Moreover, these relations are the only ones between these good generators.

2.3.2. Preliminary of the proof: reduced written forms. — The notion of *reduced written form* is used to produce some nice basis of the free R-modules $R[G]$ and $R[G] \otimes_R R[G]$. In this §, let B be an R-algebra of finite type with generators u_i ($i \in [1, t]$). We assume that $[1, t] = I \cup \bar{I}$ with $1 \in I$. For each $i \in \bar{I}$, we associate it with a number $r(i) \in \mathbb{Z}_{\geq 1}$.

Definition 2.15. — With the notations as before. A written form of an element $b \in B$

$$b = \sum_{\alpha \in \mathbb{Z}^t_{\geq 0}} a_\alpha u^\alpha$$

is called *reduced* (with respect to the integers $r(i)$ for $i \in \bar{I}$) if for $\alpha = (\alpha_1, \cdots, \alpha_t)$ from $a_\alpha \neq 0$, it follows that

$$\alpha_i < p^{r(i+1)}$$

for all $i \in [1, t-1]$ such that $i + 1 \in \bar{I}$.

Suppose further more that B is the quotient of the polynomial algebra $R[U_1, \cdots, U_t]$ modulo the ideal generated by the following elements

$$\pi^{d_i} U_i - \left(U_{i-1}^{p^{r(i)}} + \sum_{\beta < m(i-1, p^{r(i)})} a_{i\beta} U^\beta \right), \quad \text{for } i \in \bar{I}$$

where $a_{i\beta} \in R$, and the sum

$$\sum_{\beta < m(i-1, p^{r(i)})} a_{i\beta} U^\beta \in R[U_1, \cdots, U_{i-1}]$$

is *reduced* in the sense of Definition 2.15 with respect to the integers $r(i)$ (for $i \in \bar{I}$), and we will denote by u_i the image of U_i in the quotient B.

Lemma 2.16. — *Write $I = \{1 = i_1 < i_2 < \cdots < i_r\}$, let $v_j = u_{i_j}$.*

(i) *The generic fiber $B_K := B \otimes_R K$ of B is the polynomial ring in r variables $v_1, v_2, \cdots, v_r$ with coefficients in K.*

(ii) *Let $b = u^\alpha \in B$ be a monomial with $\alpha = (\alpha_1, \cdots, \alpha_t)$. Let b_K be its image in B_K, and $\deg(a_K) = (\delta_1, \cdots, \delta_r)$ the degree of b_K with respect to the variables $v_1, \cdots, v_r$. Then we have*

$$\delta_q = \sum_{i_q \leq i < i_{q+1}} \left(\alpha_i \prod_{i_q < j \leq i} p^{r(j)} \right)$$

(iii) *Let $a = u^\alpha$ and $b = u^\beta$ be two* reduced *monomials in $B = R[u_1, \cdots, u_t]$. Then if $\alpha < \beta$, we have $\deg(a_K) < \deg(b_K)$.*

Proof. — The first assertion is clear from the definition of B. In order to prove (ii), without loss of generality, we may assume that $I = \{1\} \subset [1, t]$. Let u^α be a monomial, or more generally, we consider a polynomial

$$\sum_\beta a_\beta u^\beta \tag{4}$$

satisfying the following two properties:

(a) $\alpha := \max\{\beta : a_\beta \neq 0\} = (\alpha_1, \cdots, \alpha_t + p^r a)$ for some $a \geq 0$ $r \geq 0$, and $(\alpha_1, \cdots, \alpha_t) \in \mathbb{Z}^t_{\geq 0}$;

(b) For each $\beta = (\beta_1, \cdots, \beta_t)$ such that $a_\beta \neq 0$, there exist integers $b_1, \cdots, b_t \geq 0$ verifying $b_1 + \cdots + b_t = a$, and such that

$$\beta \ll (\alpha_1 + b_1 p^{r(2)}, \cdots, \alpha_{t-1} + b_{t-1} p^{r(t)}, \alpha_t + b_t p^r)^{(1)}$$

We only need to reduce the sum (4) into a polynomial in u_1, and compute its degree. To do this, we will first reduce the sum (4) into an expression which involves only $u_1, \cdots u_{t-1}$ by replacing in (4) the variable u_t by

$$\pi^{-d_t} u_{t-1}^{p^{r(t)}} - \pi^{-d_t} \cdot \sum_{\delta < m(t-1, p^{r(t)})} a_{t\delta} u^\delta$$

Now we claim that after this reduction, the new sum in $u_1, \cdots, u_{t-1}$ satisfies again the similar properties (a) and (b). More precisely, let u^γ be a monomial appearing after applying the reduction to u^β for $\beta = (\beta_1, \beta_2, \cdots, \beta_t)$, then since the sum

$$\sum_{\delta < m(t-1, p^{r(t)})} a_{t\delta} u^\delta$$

is reduced, there exist $c_1, \cdots, c_{t-1}$ such that $\sum_{i=1}^{t-1} c_i = \beta_t$, and that

$$\gamma \ll (\beta_1 + c_1 p^{r(2)}, \beta_2 + c_2 p^{r(3)}, \cdots, \beta_{t-1} + c_{t-1} p^{r(t)}, 0)$$

Hence,

$$\gamma \ll (\alpha_1 + (c_1 + b_1) p^{r(2)}, \cdots, \alpha_{t-1} + (c_{t-1} + b_{t-1}) p^{r(t)}, 0)$$

The highest term of the new sum is of degree

$$\left(\alpha_1, \cdots, \alpha_{t-2}, \alpha_{t-1} + (\alpha_t + ap^r)\, p^{r(t)}, 0\right)$$

Hence, to finish the proof, we only need to show that

$$\sum_{j=1}^{t-1} (b_i + c_i) \leq \alpha_t + a \cdot p^r$$

But, since

$$\sum_{j=1}^{t} b_j = a, \quad \text{and} \sum_{j=1}^{t-1} c_j = \beta_t \leq \alpha_t + b_t p^r$$

we find

$$\sum_{j=1}^{t-1} (b_j + c_j) \leq a - b_t + \alpha_t + b_t p^r$$

[1] For $\gamma = (\gamma_1, \cdots, \gamma_n), \delta = (\delta_1, \cdots, \delta_n) \in \mathbb{Z}^n_{\geq 0}$, we define $\gamma \ll \delta$ if $\gamma_i \leq \delta_i$ for all $i \in [1, n]$.

So, we are reduced to show that

$$\alpha_t + b_t p^r + a - b_t \leq \alpha_t + a p^r$$

or equivalently

$$a - b_t \leq (a - b_t) p^r$$

which is clear. Hence, after repeating this reduction $t-1$ times to the monomial u^α, we get a polynomial in u_1 with degree given by the formula

$$\sum_{i=1}^{t} \alpha_i \left(\prod_{2 \leq j \leq t} p^{r(j)} \right)$$

As is required. Now the proof of (iii) is immediate from the degree formula. Indeed, let u^α and u^β be two reduced written form. Let $i \in [1, t]$ such that $\alpha_i > \beta_i$, and $\alpha_j = \beta_j$ for all $j \geq i$. Moreover, suppose $i_q \leq i < i_{q+1}$. Let δ and γ be the degree of u^α and u^β. We claim that we have

$$\delta_q > \gamma_q, \qquad \text{and} \quad \delta_{q'} = \gamma_{q'} \quad \forall q' > q.$$

According to the degree formula, for $q' > q$, the number $\delta_{q'}$ (respectively for $\gamma_{q'}$) only involves α_j (respectively β_j) for $j \geq i_{q'} > i$, hence according to the definition of the integer i, on must have $\delta_{q'} = \gamma_{q'}$. We only need to show $\delta_q > \gamma_q$. Since $\alpha_i > \beta_i$, and the monomials u^α u^β are reduced, hence

$$\begin{array}{rcl}
\delta_q - \gamma_q & = & \displaystyle\sum_{i_q \leq j < i_{q+1}} (\alpha_j - \beta_j) \left(\prod_{i_q < j' \leq j} p^{r(j')} \right) \\
& = & \displaystyle\sum_{i_q \leq j \leq i} (\alpha_j - \beta_j) \left(\prod_{i_q < j' \leq j} p^{r(j')} \right) \\
& \geq & \displaystyle\prod_{i_q < j \leq i} p^{r(j)} - \sum_{i_q \leq j < i} (p^{r(j+1)} - 1) \left(\prod_{i_q < j' \leq j} p^{r(j')} \right) \\
& = & \displaystyle\sum_{i_q \leq j \leq i} \left(\prod_{i_q < j' \leq j} p^{r(j')} \right) - \sum_{i_q + 1 \leq j \leq i} \left(\prod_{i_q < j' \leq j} p^{r(j')} \right) \\
& = & 1 > 0
\end{array}$$

Hence $\delta_q < \gamma_q$, this proves (iii).

□

Proposition 2.17. — *With the notations as before.*

1. *Any element $b \in B$ has a unique* reduced *written form in B.*
2. *B is a flat R-algebra.*

Proof. — We only need to show the existence of the reduced written form for any element $b \in B$. Indeed, let $b \in B$ with two reduced written form

$$b = \sum_{\alpha} a_{\alpha} u^{\alpha} \qquad \text{and} \quad b = \sum_{\alpha} a'_{\alpha} u^{\alpha}$$

Define

$$\alpha_0 = \max\{\alpha : a_{\alpha} \neq 0\}, \quad \text{and} \quad \alpha'_0 = \max\{\alpha : a_{\alpha} \neq 0\}.$$

According to Lemma 2.16 (iii), we have $\deg(b_K) = \deg(u_K^{\alpha_0})$, and $\deg(b_K) = \deg(u_K^{\alpha'_0})$. Applying again Lemma 2.16 (iii), we find $\alpha_0 = \alpha'_0$. Now, we consider the element $b - a'_{\alpha_0} u^{\alpha_0}$, it has then the following two reduced written form

$$b - a'_{\alpha_0} u^{\beta_0} = \sum_{\alpha < \alpha_0} a_{\alpha} u^{\alpha} + (a_{\alpha_0} - a'_{\alpha_0}) u^{\alpha_0} = \sum_{\alpha < \alpha_0} a'_{\alpha} u^{\alpha}.$$

Hence the same argument applying to the element $b - b_{\beta_0} u^{\beta}$, we find that $a_{\alpha_0} = b_{\beta_0}$. Now we continue the proof with the element $b - a_{\alpha} u^{\alpha}$, we find finally that $a_{\alpha} = a'_{\alpha}$, hence the two reduced written form are the same.

Now, we proceed to the proof of the existence of reduced written form. This will be done by induction on t. First we consider the case where $t = 1$. Recall that $1 \in I$, hence in this case, B is the polynomial ring in one variable u_1 with coefficients in R. Hence, any polynomial $\sum_r u_1^r$ is already in its reduced written form. Now suppose $t \geq 2$, and the existence of reduced written form is proven for $B' = R[u_1, \cdots, u_{t-1}]$ with respect to the relations

$$\pi^{d_i} u_i = u_{i-1}^{p^{r(i)}} + \sum_{\alpha < m(i-1, p^{r(i)})} a_{i\alpha} u^{\alpha}, \quad \text{for all } i \in [1, t-1] \cap \bar{I}$$

Let now $u^{\alpha} = u_1^{\alpha_1} \cdot u_{t-1}^{\alpha_{t-1}} u_t^{\alpha_t}$ be a monomial in B, by induction hypothesis, we may assume that the monomial $u_1^{\alpha_1} \cdots u_{t-1}^{\alpha_{t-1}}$ is reduced as element in B'. We only need to find a reduced written for u^{α}. Clearly, if $t \in I$, then there is nothing to prove since u^{α} is already reduced in B in this case. Hence, from now on, we suppose that $t \in \bar{I}$. We will describe in the following an algorithm acting on u^{α} as follows:

1. If u^{α} is *reduced*, *i.e.*, $\alpha_{t-1} < p^{r(t)}$, then the algorithm stops, and the monomial u^{α} is reduced.
2. If not, *i.e.*, $\alpha_{t-1} \geq p^{r(t)}$. We replace u^{α} by the following

$$u_1^{\alpha_1} \cdots u_{t-2}^{\alpha_{t-2}} \cdot u_{t-1}^{\alpha_{t-1} - p^{r(t)}} \cdot u_t^{\alpha_t} \cdot \left(\pi^{d_t} u_t - \sum_{\alpha < m(t-1, p^{r(t)})} a_{i\alpha} u^{\alpha} \right)$$

Then for each term $u^{\beta} = u_1^{\beta_1} \cdots u_{t-1}^{\beta_{t-1}} u_t^{\beta_t}$ appearing in the previous expression, replace the monomial $u_1^{\beta_1} \cdots u_{t-1}^{\beta_{t-1}}$ by its reduced written form in $R[u_1, \cdots, u_{t-1}]$ (here, we apply our induction hypothesis). Then for *each* monomial appeared in the new expression after this reduction, we return to step 1.

To finish the proof, we must show that this algorithm stops after finitely many iterations. Indeed, we only need to show that each monomial $u_1^{\gamma_1}\cdots u_{t-1}^{\gamma_{t-1}}u_t^{\gamma_t}$ in the new expression of step 2 verifies the following inequality:

$$(\gamma_1,\cdots,\gamma_{t-1})<(\alpha_1,\cdots,\alpha_{t-1}). \tag{5}$$

Then, apply Lemma 2.1, we find that this algorithm stops after finitely many steps. To prove our statement, we claim that for any two *reduced* monomials u^α and u^β of $R[u_1,\cdots,u_{t-1}]$ such that $\alpha<m(t-1,p^{r(t)})$ and $\beta_{t-1}\geq p^{r(t)}$, each monomial of the reduced written form in $R[u_1,\cdots,u_{t-1}]$ of the product

$$u^{\beta-m(t-1,p^{r(t)})}\cdot u^\alpha\in R[t_1,\cdots,u_{t-1}] \tag{6}$$

is of degree $<\beta$. But note that

$$\deg(u^{\beta-m(t-1,p^{r(t)})}\cdot u^\alpha)=\deg(u^\beta)-\deg(u_{t-1}^{p^{r(t)}})+\deg(u^\alpha)<\deg(u^\beta)$$

where the last inequality follows from the fact that $\deg(u_{t-1}^{p^{r(t)}})>\deg(u^\alpha)$ since both the monomials $u_{t-1}^{r(t)}$ and u^α are reduced in $B'=R[u_1,\cdots,u_{t-1}]$ and we have $\alpha<m(t-1,p^{r(t)})$. Hence by Lemma 2.16 (iii), for each monomial u^γ in the reduced form of the product (6), one must have $\gamma<\beta$. In this way, the inequality (5) is verified, and this finishes the proof.

Now, once we show the existence and the uniqueness of the reduced written form, the flatness of B over R follows. In fact, we only need to show that B has no π-torsion. Let $b\in B$ such that $\pi b=0$. Let

$$b=\sum_\alpha a_\alpha u^\alpha$$

be its reduced written form. Hence

$$\sum_\alpha \pi a_\alpha u^\alpha$$

is the reduced written form of πb. The fact that $\pi b=0$ implies then $\pi a_\alpha=0$ by the uniqueness of reduced written form. As a result, we find $b=0$. □

Remark 2.18. — Keeping the notations as before.

1. By using Proposition 2.17, we find that the set of reduced monomials gives a basis of the free R-module B over R.
2. The notion of reduced form still has a sense in B_K. In particular, the set of reduced monomials gives also a basis of the K-space B_K.
3. Let
$$P=\sum_{i,j}d_{ij}u^i\otimes u^j\in B_K\otimes_K B_K,\quad d_{ij}\in K.$$

We say that this written form is *reduced* if the for $d_{ij} \neq 0$, the monomials u^i and u^j are reduced. By using Proposition 2.17, one shows that any element $P \in B_K \otimes B_K$ has a unique reduced written form. Moreover, if $P \in B \otimes_R B \subset B_K \otimes_K B_K$, we may require that its reduced written form has coefficients in R. In particular, $B \otimes_R B$ is free over R, with a basis given by the family

$$\{u^i \otimes u^j \ : \ u^i, u^j \text{ reduced }\}.$$

2.3.3. A reformulation of Lemma 2.5. — The proof of the Theorem 2.14 can be seen as a more careful examination of the linear unipotence established in Theorem 2.12. Hence, before coming into the details of the proof, we will first reformulate lemma 2.5 in a more precise way.

In the following, we suppose that the (part of the) generators $\{y_1, \cdots, y_t\}$ is *properly chosen*, namely, these generators $\{y_1, \cdots, y_t\}$ satisfy the properties of the Theorem 2.14. In particular, the notion of *reduced written form* (in $R[y_1, \cdots, y_t]$) can be applied. Moreover, because of Proposition 2.13, the degree function with respect to the variables u_i ($i \in I$) in the ring $R[G] \otimes_R K = K[G_K]$ is the same as the degree function with respect to the variables x_i as is considered in § 2.1.

Proposition 2.19. — *Keeping the notations as before. Let $m \in \mathbb{Z}^t_{\geq 0}$ a multi-index. Let*

$$\eta(y^m) = \sum_{\alpha,\beta} c_{\alpha,\beta} y^\alpha \otimes y^\beta \tag{7}$$

be the reduced written form of $\eta(y^m)$.

1. *Suppose $m = m(i, r)$ with $i \in [1, t]$ and $r \in \mathbb{Z}_{\geq 1}$. If $i + 1 \in \bar{I} \cap [1, t]$, suppose further more that $r \leq p^{r(i+1)}$. In particular, for any $j \in [1, r-1]$, the monomial $y_i^j \otimes y_i^{r-j}$ is reduced.*
   (a) *If $i \in I$. Then for any $j \in [1, r-1]$, we have*
   $$c_{m(i,j),m(i,r-j)} = \binom{r}{j}.$$
   (b) *If $i \in \bar{I}$. Then for any $j \in [1, r-1]$, we have*
   $$c_{m(i,j),m(i,r-j)} \equiv \binom{r}{j} \mod \pi.$$
   (c) *If $i \in \bar{I}$ and $r = p^{a+1}$ for some integer $a \geq 0$. Then*
   $$c_{m(i,p^a),m(i,(p-1)p^a)} \equiv p \mod \pi p.$$

2. *Suppose $m = m' + m(i,r)$ with $r > 0$ and $m' < m(i,1)$ a multi-index different from zero. Moreover, suppose that y^m is* reduced. *Then*
$$c_{m',m(i,r)} \equiv 1 \mod \pi.$$

Proof. — (1) Suppose first of all $i \in I$. With the notations of Proposition 2.13, we have
$$y_t = a_i x_{\omega(i)} + f_t(x_1, \cdots, x_{\omega(i)-1})$$
with $a_i \in K$, and $f_i \in K[x_1, \cdots, x_{\omega(i)-1}]$. As a result,
$$\eta(y_i) = a_i \eta(x_{\omega(i)}) + \eta(P(x_1, \cdots, x_{\omega(i)-1})) \in K[x_1, \cdots, x_{\omega(i)-1}].$$
by the definition of the *primitive* generators $x_1, \cdots x_n$ of $K[G_K]$. Hence
$$\eta(y_i) \equiv 0 \mod \widetilde{M}_{m(\omega(i),1)} = \widetilde{M}_{\deg(y_i)}.$$
As a result, we find
$$\begin{aligned}\eta(y_i^r) &\equiv (y_i \otimes 1 + 1 \otimes y_i)^r - y_i^r \otimes 1 - 1 \otimes y_i^r \mod \widetilde{M}_{\deg(y_i^r)} \\ &\equiv \sum_{j=1}^{r-1} \binom{r}{j} y_i^j \otimes y_i^{r-j} \mod \widetilde{M}_{\deg(y_i^r)}.\end{aligned}$$
By our assumption on $m = m(i,r)$, each monomial $y_i^j \otimes y_i^{r-j}$ in the previous sum is reduced. By comparing the coefficient with (7), we find
$$c_{m(i,j),m(i,r-j)} = \binom{r}{i}.$$
This finishes the proof of (1.a).

Next, suppose $i \in \bar{I}$. Let
$$\eta(y_i) = \sum_{\alpha,\beta} a_{\alpha,\beta} y^\alpha \otimes y^\beta \mod \widetilde{M}_{\deg(y_i)}$$
be the reduced written form for $\eta(y_i)$, such that for those $a_{\alpha,\beta} \neq 0$, we have
$$\deg(y^\alpha) < \deg(y_i), \quad \deg(y^\beta) < \deg(y_i) \quad \text{and} \quad \deg(y^\alpha \otimes y^\beta) = \deg(y_i).$$
hence we must have $\alpha, \beta < m(i,1)$ since all the monomials y^α, y^β, y_i are reduced (Lemma 2.16 (iii)). In particular, the monomial y^α (resp. y^β) contains a factor y_ℓ for some $\ell < i$ (resp. a factor $y_{\ell'}$ for some $\ell' < i$). On the other hand,
$$\begin{aligned}\eta(y_i^r) &\equiv \left(1 \otimes y_i + y_i \otimes 1 + \sum_{\alpha,\beta} a_{\alpha,\beta} y^\alpha \otimes y^\beta\right)^r - y_i^r \otimes 1 - 1 \otimes y_i^r \mod \widetilde{M}_{\deg(y_i^r)} \\ &\equiv \sum_{j=1}^{r-1} \binom{r}{j} y_i^j \otimes y_i^{r-j} + \sum_{\gamma,\delta} b_{\gamma,\delta} y^\gamma \otimes y^\delta \mod \widetilde{M}_{\deg(y_i^r)}\end{aligned}$$

where for $b_{\gamma,\delta} \neq 0$, we have either y^γ or y^δ contain a factor y_ℓ for some $\ell < i$. Hence, after we replace $y^\gamma \otimes y^\delta$ by its reduced written form, once a term of the form $y_i^j \otimes y_i^{r-j}$ appears, the coefficient of the term $y_i^j \otimes y_i^{r-j}$ must be a multiple of π. As a result, in the reduced written form of $\eta(y_i^r)$, the coefficient of $y_i^j \otimes y_i^{r-j}$ is equal to $\binom{r}{j}$ modulo π. This gives (1.b).

To get (1.c), we need a more careful examination of the coefficients of (7). First of all, since for any integer $j \in [1, p^{a+1}]$, the binomial coefficient $\binom{p^{a+1}}{j}$ is divisible by p, the arguments before shows that the form $y^\gamma \otimes y^\delta$ whose reduced form gives the term $y_i^{p^a} \otimes y_i^{r-p^a}$ with coefficient not contained in πp must be contained in the following sum

$$y_i^{p^a} \otimes y_i^{r-p^a} + \sum_{\alpha,\beta} a^r_{\alpha,\beta} y^{r\alpha} \otimes y^{r\beta} \tag{8}$$

Now, suppose $y^{r\alpha} \otimes y^{r\beta}$ after reduction gives $y_i^{p^a} \otimes y_i^{r-p^a}$, we claim that we have

$$\alpha = m(i-1, p^{r(i)-1}).$$

Indeed, by Proposition 2.13, and since the family $\{y_1, \cdots, y_t\}$ is properly chosen, for each $y_j \in \{y_1, \cdots, y_t\}$, its degree is of the form $m(\omega(j), p^*)$. It follows that

$$\deg(y^{r\alpha}) = \deg(y_i^{p^a}) = m(\omega(i), p^b)$$

for some integer $b > 0$. Hence

$$\deg(y^\alpha) = m(\omega(i), p^{b-a-1}).$$

Hence, according to the degree formula (Lemma 2.16 (ii)), there exists some $j < i$, such that $y^\alpha = y_j^{p^c}$ for some integer c. Since $p\deg(y^\alpha) = \deg(y^{p\alpha}) = m(\omega(i), p^{b-a}) = \deg(y_i)$, and since y^α is reduced, we find that $y^\alpha = y_{i-1}^{p^{r(i)-1}}$. As a result,

$$y^\alpha \otimes y^\beta = y_{i-1}^{p^{r(i)-1}} \otimes y_{i-1}^{(p-1)p^{r(i)-1}} \tag{9}$$

For simplicity, we put

$$\lambda_i := a_{m(i-1,p^{r(i)-1}),m(i-1,(p-1)p^{r(i)-1})}$$

We will prove (1.c) by induction on the integer $i - i_{\omega(i)}$ the following two statements:

(I) $\lambda_i \in \pi^{-d_i} pR$

(II) The conclusion (1.c) holds for the index i.

We claim first that for an index i, the statement (I) implies (II). Indeed, if we compute the coefficient of the term $y_i^{p^a} \otimes y_i^{r-p^a}$ of the reduced written of the term

$$\lambda_i^r \cdot y_{i-1}^{rp^{r(i)-1}} \otimes y_{i-1}^{r(p-1)p^{r(i)-1}}$$

in (8), by (I), this coefficient is divisible by

$$(\pi^{-d_t}p)^r \cdot \pi^{d_t \cdot p^a} \cdot \pi^{d_t \cdot (p^a(p-1))} = p^r$$

Since $r = p^{a+1} \geq p \geq 2$, this gives

$$c_{m(i,p^a),m(i,r-p^a)} \equiv 1 \mod \pi p.$$

and hence the conclusion of (1.c) holds for the index i. That is (II) is verified once (I) is proven.

Suppose first that $i - i_\omega = 1$, hence $i - 1 = i_{\omega(i)} \in I$. Moreover, the family $\{y_1, \cdots, y_t\}$ is properly chosen, this implies that

$$\pi^{d_i} y_i = y_{i-1}^{p^{r(i)}} - \sum_{\alpha < m(i-1, p^{r(i)})} a_{i,\alpha} y^\alpha$$

Hence

$$\pi^{d_i}\eta(y_i) \quad \equiv \quad \eta(y_{t-1}^{p(i)}) \mod \widetilde{M}_{\deg(y_i)}$$

Hence, according to (1.a), the coefficient λ_i of the term

$$y_{i-1}^{p^{r(i)-1}} \otimes y_{i-1}^{p^{r(i)} - p^{r(i)-1}}$$

in the reduced form of $\eta(y_i)$ is equal to

$$\pi^{-d_i}\binom{p^{r(i)}}{p^{r(i)-1}}$$

In particular, we get $\lambda_i \in \pi^{-d_i}pR$. As a result, the statement (I) is proven for i, and so (II) for the same index i.

Suppose now $i - i_{\omega(i)} \geq 2$, and suppose that (I) and hence (II) have been shown for the index $i - 1$. We must show that the statement (I) holds for i. Indeed, since $\{y_1, \cdots, y_t\}$ is properly chosen, we have

$$\pi^{d_i} y_i = y_{i-1}^{p^{r(i)}} + \sum_{\alpha < m(i-1, p^{r(i)})} a_{i,\alpha} y^\alpha$$

we find

$$\pi^{d_i}\eta(y_i) \equiv \eta(y_{i-1}^{r(i)}) \mod \widetilde{M}_{\deg(y_{i-1}^{p^{r(i)}})}.$$

Now applying the statement (II) for the index $i-1$, we find that the coefficient of $y_{i-1}^{p^{r(i)-1}} \otimes y_{i-1}^{(p-1)p^{r(i)-1}}$ of the reduced form of $\eta(y_{i-1}^{p^{r(i)}})$ is congruent to p modulo πp. Hence we have

$$\lambda_i \equiv \frac{p}{\pi^{d_i}} \mod \frac{\pi p}{\pi^{d_i}}.$$

Hence we get finally $\lambda_i \in \pi^{-d_i}pR$. This proves (I) for i, and hence finishes the proof of (1.c)

The proof of (2) is similar to that of (1.b) Since $y^m = y^{m'} \cdot y_i^r$, we have

$$\begin{aligned}
\mu(y^m) &= \mu(y^{m'}) \cdot \mu(y_i)^r \\
&= \left(y^{m'} \otimes 1 + 1 \otimes y^{m'} + \eta(y^{m'})\right) \cdot (y_i^r \otimes 1 + 1 \otimes y_i^r + \eta(y_i^r)) \\
&= y^m \otimes 1 + 1 \otimes y^m + y_i^r \otimes y^{m'} + y^{m'} \otimes y_i^r + (y^{m'} \otimes 1 + 1 \otimes y^{m'})\eta(y_i^r) \\
&\quad +(y_i^r \otimes 1 + 1 \otimes y_i^r)\eta(y^{m'}) + \eta(y^{m'})\eta(y_i^r).
\end{aligned}$$

Hence

$$\begin{aligned}
\eta(y^m) &= y_i^r \otimes y^{m'} + y^{m'} \otimes y_i^r + (y^{m'} \otimes 1 + 1 \otimes y^{m'})\eta(y_i^r) \\
&\quad +(y_i^r \otimes 1 + 1 \otimes y_i^r)\eta(y^{m'}) + \eta(y^{m'})\eta(y_i^r).
\end{aligned}$$

Let

$$\eta(y_i^r) = \sum_{\alpha,\beta} a_{\alpha\beta} y^\alpha \otimes y^\beta \bmod \widetilde{M}_{\deg(y_i^r)}, \quad \text{and} \quad \eta(y^{m'}) = \sum_{\alpha',\beta'} b_{\alpha'\beta'} y^{\alpha'} \otimes y^{\beta'} \bmod \widetilde{M}_{\deg(y^m)}$$

be their reduced written forms, such that $\deg(y^\alpha \otimes y^\beta) = \deg(y_i^r)$ for $a_{\alpha\beta} \neq 0$, and that $\deg(y^{\alpha'} \otimes y^{\beta'}) = \deg(y^{m'})$ for $b_{\alpha'\beta'} \neq 0$. We find

$$\begin{aligned}
\eta(y^m) &\equiv y^{m'} \otimes y_i^r + y_i^r \otimes y^{m'} + \sum_{\alpha,\beta} a_{\alpha\beta} \left(y^{\alpha+m'} \otimes y^\beta + y^\alpha \otimes y^{\beta+m'}\right) \\
&\quad + \sum_{\alpha',\beta'} b_{\alpha'\beta'} \left(y^{\alpha'} y_i^r \otimes y^{\beta'} + y^{\alpha'} \otimes y^{\beta'} y_i^r\right) \\
&\quad + \sum_{\alpha,\beta,\alpha',\beta'} a_{\alpha\beta} b_{\alpha'\beta'} y^{\alpha+\alpha'} \otimes y^{\beta+\beta'} \quad \bmod \widetilde{M}_{\deg(y^m)}.
\end{aligned}$$

Now let $y^\gamma \otimes y^\delta$ be any monomial in the previous sum, which is neither $y_i^r \otimes y^{m'}$ nor $y^{m'} \otimes y_i^r$, then we have either $\gamma < m(i,r)$, or $\delta < m'$. Hence, once a monomial of the form $y_i^r \otimes y^{m'}$ appears in its reduced written form, its coefficient must be a multiple of π. This gives (2). □

2.3.4. Proof of the main result. — Let us now begin the proof of the theorem. Let $\{y_i : 1 \leq i \leq N\}$ be an arbitrary family of good generators, we will prove by induction on the integer $t \geq 0$ that up to modify these generators, we can assume that the generators $\{y_i : 1 \leq i \leq t\}$ verify the properties required by the theorem (*i.e.*, the family $\{y_1, \cdots, y_t\}$ is *properly chosen*).

First, since $1 \notin \bar{I}$, hence we can keep y_1. Suppose now that the family $\{y_1, \cdots, y_t\}$ has been properly chosen with $t < N$. To finish the induction, we only need to modify y_{t+1} by $y_{t+1} + f$ with $f \in R[y_1, \cdots, y_t]$ such that with this new y_{t+1}, the family $\{y_1, \cdots, y_t, y_{t+1}\}$ satisfies again the property of the theorem. If $t + 1 \in I$, then there is nothing to do. Hence, in the following, we may assume that $t+1 \in \bar{I}$. In particular, according to 2.13, we have

$$\pi^{d_{t+1}} y_{t+1} = \sum_i a_i y^i \in R[y_1, \cdots, y_t]$$

Moreover, we may assume that the sum

$$\sum_i a_i y^i$$

is reduced (Proposition 2.17).

Lemma 2.20. — *Keeping the notations as above. Then $a_m \in R^*$.*

Proof. — Assume that $a_m = \pi \cdot b$ with $b \in A$, and let

$$z = \pi^{d_{t+1}-1} y_{t+1} - b y_m \in R[G]$$

Then $\deg(z) < \deg(y_{t+1})$, which implies $z \in R[y_1, \cdots, y_t]$ by the definition of good generators. Hence $\pi^{d_{t+1}} y_{t+1} = \pi b y^m + \pi z$, and we get

$$\pi^{d_{t+1}-1} y_{t+1} = b y^m + z \in R[y_1, \cdots, y_t]$$

in view of the flatness of $A[G]$. But this equality contradicts the definition of the integer d_{t+1}. Therefore $a_m \in R^*$.

□

According to this lemma, up to replace y_{t+1} by $a_m^{-1} y_{t+1}$, we may assume that $a_m = 1$, and that $a_i \notin \pi^{d_{t+1}} A$ for any $i < m$.

Lemma 2.21. — *With the notations as before. We have*

$$\pi^{-d_{t+1}} \eta(y^m) \in M + \widetilde{M}_{K, \deg(y^m)}.$$

Proof. — By Lemma 2.16, we have

$$\begin{aligned} \pi^{d_{t+1}} \eta(y_{t+1}) &= \eta(\pi^{d_{t+1}} y_{t+1}) = \eta(y^m) + \sum_{\alpha < m} a_\alpha \eta(y^\alpha) \\ &\equiv \eta(y^m) \mod \widetilde{M}_{\deg(y^m)}. \end{aligned}$$

Hence

$$\pi^{-d_{t+1}} \eta(y^m) \equiv \eta(y_{t+1}) \quad \widetilde{M}_{K, \deg(y^m)}.$$

Hence the lemma follows once we remark that $\eta(y_{t+1}) \in M = R[G] \otimes R[G]$ since $y_{t+1} \in R[G]$. □

Let $m = (m_1, \cdots, m_t, 0 \cdots, 0)$, and

$$\eta(y^m) = \sum_{\alpha, \beta} a_{\alpha\beta} y^\alpha \otimes y^\beta$$

be its reduced written form. According to Lemma 2.21, for those (α, β) such that $\deg(y^\alpha \otimes y^\beta) = \deg(y^m) = \deg(y_{t+1})$, we must have

$$\pi^{-d_{t+1}} | a_{\alpha\beta}. \tag{10}$$

In the following, we will show that $m = m(t, p^\alpha)$, and $\pi^{d_{t+1}} | p$.

First of all, we claim that $m_t \neq 0$. Indeed, otherwise $m < m(t, 1)$, and we find the following contradiction with the construction of good generators (Corollary 2.10)

$$\deg(y_{t+1}) = \deg(y^m) < \deg(y^{m(t,1)}) = \deg(y_t)$$

where the inequality follows from the fact that the two monomials y^m and $y^{m(t,1)}$ are reduced, and that $m < m(t,1)$ (Lemma 2.19). Hence, we find $m_t \neq 0$. Next, we claim that $m_i = 0$ for any $i < t$. Otherwise, let $m' = (m_1, \cdots, m_{t-1}, 0, \cdots, 0)$, then we have $m' \neq 0$, and

$$y^m = y^{m'} \cdot y^{m(t,m_t)} = y^{m'} y_t^{m_t}$$

According to Proposition 2.19 (2), we have

$$a_{m(t,m_t),m'} \equiv 1 \mod \pi.$$

In particular, $\pi^{d_{t+1}} \nmid a_{m(t,m_t),m'}$. This gives us a contradiction with the divisibility condition (10). Hence we must have $m' = 0$.

Now, we will show that m_t must be a power of p. Otherwise, let $m_t = p^a \cdot b$ with $b > 1$ prime to p. Let $\delta = m(t, m_t - p^a)$, and $\gamma = m(t, p^a)$. According to Proposition 2.19 (1.b), we must have

$$a_{\gamma,\delta} \equiv \binom{p^a b}{p^a} \mod \pi.$$

Since, the binomial coefficient above is prime to p, we find $\pi^{d_{t+1}} \nmid a_{\gamma,\delta}$. Thus, this gives us a contradiction with (10). Hence m_t must be a power of p. Let $m_t = p^{a+1}$, with $a \geq 0$. To finish the proof, we only need to show $\pi^{d_{t+1}} | p$. We consider again $\gamma = m(t, m_t - p^a)$, and $\delta = m(t, p^a)$. According to Proposition 2.19 (1.c), we have

$$a_{\gamma,\delta} \equiv p \mod p\pi.$$

Hence the divisibility condition (10) implies

$$\pi^{d_{t+1}} | p.$$

This shows the existence of y_{t+1} such that the family $\{y_1, \cdots, y_t, y_{t+1}\}$ satisfies the relations as indicated in the theorem for all $i \in \bar{I} \cap [1, t+1]$.

Now to complete the proof of Theorem 2.14, it remains to show that these relations are the only ones verified by $y_1, \cdots, y_{t+1}$. Let B be the quotient of the polynomial ring $R[Y_1, \cdots, Y_{t+1}]$ by the ideal generated by the relations indicated in the theorem for $i \in \bar{I} \cap [1, t+1]$. Then by Proposition 2.17 (1), we note that B is flat over R. The previous arguments show that there exists a surjective morphism of R-algebras

$$B \to R[y_1, \cdots, y_{t+1}], \quad \text{class of } Y_i \mapsto y_i.$$

Since both of this two R-algebras are flat, with the same generic fiber $K[x_1, \cdots, x_{\omega(t+1)}]$, this surjection must be an isomorphism of R-algebras. This completes then the proof of the theorem.

2.3.5. Variants and applications of the main result. — Let $\{y_1, \cdots, y_N\}$ a family of good generators with the properties in Theorem 2.14, this allows us to realize G as a closed subscheme of $\mathbb{A}^N_S$. The proof of the following corollary can be found in **[20]** (Corollary 3.2).

Corollary 2.22. — *The subscheme $G \hookrightarrow \mathbb{A}^N_S$ is a complete intersection.*

Once the discrete valuation ring is of equal characteristic $p > 0$, because of the following fundamental property in characteristic p:

$$(X+Y)^p = X^p + Y^p$$

it is possible to get some more precise information on the generators of $R[G]$. To avoid some further notations, we will assume that $G_K \simeq \mathbb{G}^n_{a,K}$, and refer to **[20]** Theorem 2.4.0 for a more general statement.

Theorem 2.23. — *Suppose* $\mathrm{Char}(K) = p > 0$, *and $G_K \simeq \mathbb{G}^n_{a,K}$. Then there exists a family of good generators $\{y_1, \cdots, y_N\}$ such that for each $i \in \bar{I}$ we have*

$$\pi^{d_i} y_i = \sum_{j<i} \sum_{\alpha} a_{ij\alpha} y_j^{p^\alpha} \tag{11}$$

for some $a_{ij\alpha} \in R$, and for $i \in I$ we have

$$y_i = a_i x_{\omega(i)} + \sum_{j<i} \sum_{\alpha} b_{ij\alpha} y_j^{p^\alpha} \tag{12}$$

for $b_{ij\alpha} \in K$. Here, setting $r(i) = \max\{\alpha : a_{i,i-1,\alpha} \neq 0\}$ for $i \in \bar{I}$, we have

- *$a_{i,i-1,r(i)} = 1$ for $i \in \bar{I}$;*
- *The following two sums in* (11) *and* (12)

$$\sum_{j<i} \sum_{\alpha} a_{ij\alpha} y_j^{p^\alpha}, \quad \textit{and} \quad \sum_{j<i} \sum_{\alpha} b_{ij\alpha} y_j^{p^\alpha}$$

are reduced.

Proof. — In this proof, we say that the family $\{y_1, \cdots, y_t\}$ is properly chosen, if it satisfies the properties of this theorem. As before, we proceed by induction.

We begin with the case $t = 1$. Hence $t \in I$. On can find $a_1 \in K - \{0\}$ such that

$$y_1 = a_1 x_1 + b, \quad a_1, b \in K$$

As proved in the proof of the Lemma 2.4, we have $b \in R$. Hence up to replace y_1 by $y_1 - b \in R[G]$, we may assume that $b = 0$. Hence, $\{y_1\}$ is properly chosen. Suppose now for an integer $t < N$, the family $\{y_1, \cdots, y_t\}$ has been properly chosen. In particular, one finds that each y_i are of the form

$$y_i = \sum_{\ell \leq \omega(i)} \sum_{\alpha} b_{i\ell\alpha} x_\ell^{p^\alpha}, \quad b_{i\ell\alpha} \in K \quad \forall i \in [1, t].$$

In particular, we find $\eta(y_i) = 0$ for *any* $i \in [1, t]$ by our assumption. We want to modify y_{t+1} so that the new family $\{y_1, \cdots, y_{t+1}\}$ satisfies again the conclusion of the theorem. Let

$$y_{t+1} = a_t x_{\omega(t+1)} + \sum_{\alpha} c_\alpha y^\alpha, \quad a_t \in K, c_\alpha \in K, \tag{13}$$

where we put $a_t = 0$ if $t + 1 \in I$, and the sum

$$\sum_{\alpha} c_\alpha y^\alpha \in K[y_1, \cdots, y_t]$$

is reduced (but with coefficients in K). We enumerate increasingly the following finite set

$$\{\alpha : c_\alpha \neq 0\} = \{\lambda_1 < \lambda_2 \cdots\}$$

and we suppose that for an integer $q \geq 1$, we have shown that

$$\sum_{i > q} c_{\lambda_i} y^{\lambda_i} = \sum_{j \leq t} \sum_{\beta} b_{j\beta} y_j^{p^\beta}$$

We claim that if λ_q is not of the form $m(j, p^a)$ for some $j \leq t$ and some integer $a \geq 0$, then $a_{\lambda_q} \in R$. Indeed, from (13), we find

$$\eta\left(\sum_{i<q} c_{\lambda_i y^{\lambda_i}}\right) + \eta\left(c_{\lambda_q} y^{\lambda_q}\right) + \eta\left(\sum_{i>q} c_{\lambda_i y^{\lambda_i}}\right) = \eta(y_{t+1}) \in M.$$

Together with the property $\eta(y_i) = 0$ for all $i \in [1, t]$, we find

$$\eta\left(c_{\lambda_q} y^{\lambda_q}\right) \in M + \widetilde{M}_{\deg(y^{\lambda_q})}$$

Now a similar argument as in the proof of Theorem 2.14 (with the help of Proposition 2.19), we see that if λ_q is not of the form of $m(j, p^a)$ for some $j \in [1, t]$ and some integer $a \geq 0$, we must have $c_{\lambda_q} \in R$. Now up to replace y_{t+1} by $y_{t+1} - c_{\lambda_q} y^{\lambda_q} \in R[G]$, we may remove the term $c_{\lambda_q} y^{\lambda_q}$ in the sum

$$\sum_{i} c_{\lambda_i} y^{\lambda_i}.$$

After repeating finitely many times of this argument, we find finally that

$$\sum_i c_{\lambda_i} y^{\lambda_i} = \sum_{j\geq t} \sum_{\alpha} a_{tj\alpha} y^{p^\alpha}.$$

In particular, the family $\{y_1, \cdots, y_{t+1}\}$ is properly chosen. This finishes then the proof. □

Corollary 2.24. — *Under the assumption of Theorem 2.23, there exists a sequence of commutative group schemes over S:*

$$0 \to G \to \mathbb{G}_{a,S}^N \to \mathbb{G}_{a,S}^{N-n} \to 0. \tag{14}$$

which is exact for the fppf-topology.

Proof. — For each $i \in \bar{I}$, let

$$F_i = \pi^{d_i} Y_i - \sum_{j<i} \sum_{\alpha} a_{ij\alpha} Y_j^{p^\alpha} \in R[Y_1, \cdots, Y_N].$$

This is a p-polynomial. Consider now the following morphism of S-schemes given by the $N - n = \sharp(\bar{I})$ polynomials F_i $(\forall \bar{I})$:

$$f : \mathbb{G}_{a,S}^N \to \mathbb{G}_{a,S}^{N-n}.$$

Since the polynomials F_i $(i \in \bar{I})$ are all p-polynomial, the morphism f is a morphism of S-group schemes. Moreover, we have $\ker(f) \simeq G$. It remains to show that f is a flat morphism. Indeed, we only need to verify this assertion over thie special fibers $f_s : \mathbb{G}_{a,s}^N \to \mathbb{G}_{a,s}^{N-n}$. After reduction by modulo π, we get

$$\overline{F_i} = -\sum_{j<i} \sum_{\alpha} \overline{a_{ij\alpha}} \cdot Y_j^{p^\alpha} \in k[Y_1, \cdots, Y_N]$$

Moreover, we have $a_{i,i-1,p^{r(i)}} = 1$, this implies then f_s is an epimorphism. As is required. □

Corollary 2.25. — *Suppose* $\mathrm{Char}(K) = p > 0$*, and G/S is an affine flat* commutative *group scheme of finite type such that $G_K \simeq \mathbb{A}_K^n$. Let $\tau \in \{fpqc, fppf\}$ be one of these two Grothendieck topologies, and we denote by H_τ^i the corresponding τ-cohomology. Then we have $\mathrm{H}_\tau^i(S, G) = 0$ for $i \geq 2$. If further more the residue field k of R is algebraically closed, then we have moreover* $\mathrm{H}_\tau^1(S, G) = 0$.

Proof. — By Lazard's theorem (Theorem 1.1), G_K admits a composition series

$$0 = G_{K,0} \subset \cdots, G_{K,n-1} \subset G_{K,n} = G_K$$

whose successive quotients are isomorphic to $\mathbb{G}_{a,K}$. Let G_i be the schematic closure of $G_{K,i}$ in G. As shown in the proof of Lemma 2.9 (1), the fppf-quotient $H_i = G_i/G_{i-1}$ is representable by a flat affine S-group scheme of finite type with generic fiber $\simeq \mathbb{G}_{a,K}$. Now, in order to prove the corollary for G/S, we only need to prove the corollary for each H_i for $i \in [1, n]$. Hence, up to replace G/S by H_i/S, we are reduced to the case where $G_K = \mathbb{G}_{a,K}$. Hence our unipotent group scheme G/S satisfies the assumption of Corollary 2.24. Now the first part of this corollary follows directly from the short exact sequence (14) and the fact that $\mathrm{H}^i_{\tau}(S, \mathbb{G}_{a,S}) = 0$ for any $i > 0$. To get the second statement, it remains to show that the morphism

$$f(S) : \mathbb{G}_{a,S}^N(S) \to \mathbb{G}_{a,S}^{N-n}(S)$$

is surjective when the residue field k of R is algebraically closed. Indeed, for any $(a_1, \cdots, a_{N-n}) \in \mathbb{G}_{a,S}^{N-n}(S)$, since k is algebraically closed, we can find $b = (b_1, \cdots, b_N) \in R^N$ such that

$$F_i(b_1, \cdots, b_N) \equiv a_i \mod \pi.$$

Moreover, if we replace, for $i \in I$, each b_i by $b_i + \pi^{e_i}$ for some integer e_i sufficiently large, and then modify accordingly the value of b_i $(i \in \bar{I})$ by some $b_i + \pi^{f_i}$ for some suitable f_i, we may find $\widetilde{b_i}$ such that

$$F_i(\widetilde{b_1}, \cdots, \widetilde{b_N}) = a_i$$

This gives the corollary. □

3. Geometry of unipotent groups

3.1. The main result. — In § 3, R is a discrete valuation of residue characteristic $p > 0$.

Definition 3.1. — An affine S-scheme X/S is called *p-polynomial* if there exist some integer $N \geq 1$, and $I \subset [1, N]$ with $1 \in I$ such that X is the subscheme of $\mathbb{A}_S^N$ given by the equations:

$$\pi^{d_i} y_i = \sum_{j<i} \sum_{\alpha} a_{ij\alpha} y_j^{p^\alpha}, \qquad \forall i \in \bar{I} := [1, N] - I, \tag{15}$$

where

- $a_{ij\alpha} \in R$ such that $a_{i,i-1,r(i)} = 1$ where $r(i) := \max(\alpha : a_{i,i-1,\alpha} \neq 0)$;
- $d_i > 0$ is an integer such that $\pi^{d_i} | p$.

Remark 3.2. — With the notations as before.

1. Let $n = \sharp(I)$, then the generic fiber X_K of X is isomorphic to $\mathbb{A}_K^n$.
2. Suppose $\mathrm{Char}(K) = p > 0$, and let G/S be an affine unipotent groups flat over S such that $G_K \simeq \mathbb{G}_{a,K}^n$. Then according to Theorem 2.23, the scheme G/S is p-polynomial.

Theorem 3.3. — *Let X/S be a smooth p-polynomial S-scheme with connected fibers of dimension n. Then there exists a sequence of finite extensions of discrete valuation rings:*

$$R = R_0 \subset \cdots \subset R_i \subset R_{i+1} \subset \cdots \subset R_n = R',$$

such that

- *For each i, the extension $R_i \subset R_{i+1}$ is defined by an equation of the form $x^p = a$ for some element $a \in R_i$ whose reduction $\bar{a}$ in the residue field is not a p-th power.*
- *$X_{S'} := X \times_S S' \simeq \mathbb{A}^n_{S'}$ as S'-scheme with $S' = \operatorname{Spec}(R')$.*

In particular, if the residue field of R is perfect, we have $X \simeq \mathbb{A}^n_S$.

Corollary 3.4. — *Suppose that K is of characteristic $p > 0$. Let G/S be a smooth group scheme G/S with connected fibers such that $G_K \simeq \mathbb{G}^n_{a,K}$. Then there exists an extension $R \subset R'$ of discrete valuation rings as indicated in Theorem 3.3 such that $G_{S'} \simeq \mathbb{G}^n_{a,S'}$ with $S' = \operatorname{Spec}(R')$. In particular, if R has perfect residue field, then $G \simeq \mathbb{G}^n_{a,S}$.*

From these last two results, we can show the corresponding global analogue (namely, over a locally regular integral scheme of dimension ≤ 1 *of characteristic p*), we refer to **[20]** 3.5 and 3.6 for the precise statements. The rest of this § is then devoted to the proof of Theorem 3.3 and its corollary.

3.2. Some preliminaries of the proof.

— In this §, we suppose that the residue field of the discrete valuation ring R is *perfect*. In particular, for any element $a \in R$, one can find an element $a' \in R$ such that $a'^{p^n} - a \in \pi R$.

Definition 3.5. — Let A be any ring.

1. A polynomial $P \in \mathsf{A}[X_1, \cdots, X_n]$ is called a *p-polynomial*, if it can be written of the form
$$P(X_1, \cdots, X_n) = \sum_{i,j} a_{ij} X_i^{p^j} \in \mathsf{A}[X_1, \cdots, X_n].$$
2. A morphism of A-algebras $f : \mathsf{A}[X_1, \cdots, X_n] \to \mathsf{A}[T_1, \cdots, T_m]$ is called *a p-polynomial morphism* if $f(X_i) \in \mathsf{A}[T_1, \cdots, T_m]$ is a p-polynomial for all $i \in [1, n]$. If moreover f is an isomorphism with f^{-1} also a p-polynomial morphism, then f is called a *p-polynomial isomorphism.*

Note that in general, the composition of two p-polynomial morphisms is not necessarily still p-polynomial. But because of the following well-known congruence relation

$$(X + Y)^{p^r} \equiv X^{p^r} + Y^{p^r} \pmod{p}$$

the *reduction modulo* p of the composition of two p-polynomial morphisms are again p-polynomial.

Lemma 3.6. — *If* $P \in R[X_1, \cdots, X_n]$ *is a polynomial such that its reduction modulo* π *is irreducible (hence non zero) and p-polynomial. Then there exists an isomorphism of* R*-algebras* $f : R[X_1, \cdots, X_n] \to R[T_1, \cdots, T_n]$ *such that* f *is a composition of some p-polynomial isomorphisms, and that* $f(P) - T_1 \in \pi R[T_1, \cdots, T_n]$.

Proof. — Remark first that if $P(X) = P_1(X) + \pi Q(X)$ with P_1, Q two polynomials, then P and P_1 have the same reduction modulo π, and if the conclusion of the lemma holds for P_1, the same happens for P. Hence to prove the lemma here, we may assume that P is p-polynomial such that all the non zero coefficients of P are invertible. Let p^{m_i} be the degree of the $\bar{P}$ of P with respect to the variable T_i if T_i appears in the expression of P. Up to renumbering the variables X_i, we may assume that P can be written as:

$$P(X) = \sum_{i=1}^{r} \sum_{j=0}^{m_i} a_{ij} X_i^{p^j},$$

such that (i) $a_{ij} \in R$ are either 0 or invertible, with $a_{i,m_i} \neq 0$; (ii) $m_1 \geq m_2 \cdots \geq m_r \geq 0$. Note that since the reduction modulo π of P is non zeron, we have necessarily $r \geq 1$. We will prove this lemma by induction on the integer $m := \sum_{i=1}^{r} m_i \geq 0$.

If $m = 0$, then we must have $m_1 = \cdots = m_r = 0$, hence the polynomial P is of the form

$$P(X) = a_{10}X_1 + a_{20}X_2 + \cdots a_{r0}X_r$$

We consider the following p-polynomial isomorphism (note that $a_{10} \in R$ is invertible):

$$\begin{array}{rcl} f : R[X_1, \cdots, X_n] & \to & R[T_1, \cdots, T_n], \\ X_1 & \mapsto & a_{10}^{-1}(T_1 - \sum_{j=2}^{r} a_{i0}T_j), \\ X_i & \mapsto & T_i \text{ for all } i \geq 2. \end{array}$$

Then $f(P) = T_1$, as required. This finishes the proof when $m = 0$.

Suppose next $m > 0$. Since $\overline{P} \in k[X_1, \cdots, X_n]$ is irreducible, we must have $r \geq 2$. Since R has perfect residue field, one can find $b_i \in R$ such that

$$b_i^{p^{m_2}} - \frac{a_{1i}}{a_{2m_2}} \in \pi R$$

for each $i \in [m_2, m_1]$. Now define the following p-polynomial isomorphism

$$\begin{array}{rcl} f' : R[X_1, \cdots, X_n] & \to & R[T_1, \cdots, T_n] \\ X_i & \mapsto & T_i \text{ for } i = 1 \text{ or } i \geq 3, \\ X_2 & \mapsto & T_2 - b_{m_2} T_1 - \cdots - b_{m_1} T_1^{p^{m_1 - m_2}} \end{array}$$

Since

$$\begin{array}{rl} & \left(T_2 - b_{m_2} T_1 - \cdots - b_{m_1} T_1^{p^{m_1 - m_2}} \right)^{p^{m_2}} \\ \equiv & T_2^{p^{m_2}} - b_{m_2}^{p^{m_2}} T_1^{p^{m_2}} - \cdots - b_{m_1}^{p^{m_2}} T_1^{p^{m_1}} \pmod{p} \\ \equiv & a_{2,m_2}^{-1} \left(a_{2,m_2} T_2^{p^{m_2}} - a_{1,m_2} T_1^{p^{m_2}} - \cdots - a_{1,m_1} T_1^{p^{m_1}} \right) \pmod{\pi} \end{array}$$

Hence we find

$$P' := f(P) \equiv \sum_{i=0}^{m_1 - 1} a'_{1,i} T_1^{p^i} + \sum_{j=2}^{r} \sum_{i=0}^{m_2} a_{j,i} T_j^{p^i} \pmod{\pi}$$

Note that the polynomial $P' \in R[T_1, \cdots, T_n]$ has irreducible reduction modulo π since f' is an isomorphism of R-algebras. Moreover, if we look at the degree m'_1 of P' with respect to the variable T_1, we have either the variable T_1 does not appear, or $m'_1 \leq m_1 - 1$. Since

$$m'_1 + \sum_{i=2}^{r} m_i \leq -1 + \sum_{i=1}^{r} m_i < \sum_{i=1}^{r} m_i = m$$

Finally, the reduction modulo π of P' is again p-polynomial since f' is a p-polynomial isomorphism. Hence we can apply our induction hypothesis to the polynomial P', and we find an isomorphism of R-algebras $f'' : R[T_1, \cdots, T_n] \to R[S_1, \cdots, S_n]$, which is a composition of p-polynomial isomorphisms, such that

$$f''(P') - S_1 \in \pi R[S_1, \cdots, S_n]$$

Now, we put $f = f'' \circ f' \colon R[X_1, \cdots, X_n] \to R[S_1, \cdots, S_n]$. The morphism f is then a composition of p-polynomial isomorphisms such that

$$f(P) - S_1 = f''(P') - S_1 \in \pi R[S_1, \cdots, S_n],$$

as desired. □

Lemma 3.7. — *Let*

$$F = \pi^d X_{n+1} - (P_0 + \pi P_1 + \cdots \pi^d P_d) \in R[X_1, \cdots, X_{n+1}]$$

be a polynomial with each $P_i \in R[X_1, \cdots, X_n]$. Let $Y_0 = 0$, and

$$F'_i := \pi Y_i - P_{i-1} - Y_{i-1} \in R[X_1, \cdots, X_n, Y_1, \cdots, Y_d]$$

for $i \in [1, d]$. Then there is an isomorphism

$$f : R[X_1, \cdots, X_{n+1}]/(F) \to R[X_1, \cdots, X_n, Y_1, \cdots, Y_d]/(F'_1, \cdots, F'_d).$$

Proof. — This isomorphism can be defined directly as follows: we first define

$$\begin{array}{rcl} \widetilde{f}: R[X_1,\cdots,X_{n+1}] & \to & R[X_1,\cdots,X_n,Y_1,\cdots,Y_d] \\ X_i & \mapsto & X_i, \quad \text{for } i\in[1,n] \\ X_{n+1} & \mapsto & Y_d+P_d(X_1,\cdots,X_n). \end{array}$$

Then

$$\begin{array}{rcl} \widetilde{f}(F) & = & \pi^d(Y_d+P_d)-(P_0+\pi P_1+\cdots+\pi^dP_d) \\ & = & \pi^dY_d-(P_0+\pi P_1+\cdots+\pi^{d-1}P_{d-1}) \\ & = & \sum_{i=1}^d \left(\pi^{i-1}(\pi Y_i-P_{i-1}-Y_{i-1})\right) \\ & = & \sum_{i=1}^d \pi^{i-1}F_i' \end{array}$$

Hence the morphism $\widetilde{f}$ induces a morphism of R-algebras:

$$f: R[X_1,\cdots,X_{n+1}]\to R[X_1,\cdots,X_n,Y_1,\cdots,Y_d]/(F_1',\cdots,F_d'),$$

which is an isomorphism. □

Lemma 3.8. — *Let*

$$F=\pi X_{n+1}-P(X_1,\cdots,X_n)-\pi Q(X_1,\cdots,X_n)\in R[X_1,\cdots,X_{n+1}]$$

a polynomial, where $P=P(X_1,\cdots,X_n)\in R[X_1,\cdots,X_n]$ a p-polynomial such that its reduction modulo π is irreducible. There exists an isomorphism

$$f: R[X_1,\cdots,X_{n+1}]/(F)\to R[Y_1,\cdots,Y_n]$$

such that

$$f(X_i)=R_i(Y_1,\cdots,Y_n)+\pi\Phi_i(Y_1,\cdots,Y_n)$$

with R_i a p-polynomial.

Proof. — Since $P\in R[X_1,\cdots,X_n]$ is a p-polynomial with irreducible reduction modulo p and the residue field of R is perfect, there exists an isomorphism

$$\widetilde{f}: R[X_1,\cdots,X_n]\to R[T_1,\cdots,T_n]$$

such that $\widetilde{f}(P)-T_1\in\pi R[T_1,\cdots,T_n]$. Since $\widetilde{f}$ is a composition of p-polynomial isomorphism, its reduction modulo π is a p-polynomial isomorphism. Hence for each X_i, $\widetilde{f}(X_i)$ is of the form

$$\widetilde{f}(X_i)=\widetilde{R}_i(T_1,\cdots,T_n)+\pi\widetilde{\Phi}_i(T_1,\cdots,T_n)$$

with $\widetilde{R}_i$ some p-polynomials and $\widetilde{\Phi}_i\in R[T_1,\cdots,T_n]$. The isomorphism $\widetilde{f}$ can be extended to another isomorphism

$$\begin{array}{rcl} f_1: R[X_1,\cdots,X_{n+1}] & \to & R[T_1,\cdots,T_n,X_{n+1}] \\ X_i & \mapsto & \widetilde{f}(X_i) \quad \text{for } i\in[1,n]; \\ X_{n+1} & \mapsto & X_{n+1.} \end{array}$$

Hence $f_1(F) = \pi X_{n+1} - T_1 - \pi Q'(T_1, \cdots, T_n)$ for some $Q' \in R[T_1, \cdots, T_n]$. Let us write the polynomial Q' under the form of

$$Q'(T_1, \cdots, T_n) = Q'_1(T_2, \cdots, T_n) + T_1 Q'_2(T_1, \cdots, T_n)$$

and consider the following isomorphism:

$$\begin{array}{rcl} f_2 : R[T_1, \cdots, T_n, X_{n+1}] & \to & R[T_1, \cdots, T_n, S] \\ T_i & \mapsto & T_i \text{ for } i \in [1, n]; \\ X_{n+1} & \mapsto & S - T_1 Q'_2(T_1, \cdots, T_n). \end{array}$$

Then

$$f_2 \circ f_1(F) = f_2(\pi X_{n+1} - T_1 - \pi Q'(T_1, \cdots, T_n)) = \pi(S - Q'_1(T_2, \cdots, T_n)) - T_1 =: F_2.$$

Hence we obtain an isomorphism, denoted by f':

$$f' : R[X_1, \cdots, X_{n+1}]/(F) \to R[T_1, \cdots, T_n, S]/(F_2).$$

Next, we consider the morphism

$$\begin{array}{rcl} f_3 \colon R[T_1, \cdots, T_n, S] & \to & R[Y_1, \cdots, Y_n] \\ T_i & \mapsto & Y_{i-1} \text{ for } i \in [2, n]; \\ S & \mapsto & Y_n; \\ T_1 & \mapsto & \pi Y_n - \pi Q'_1(Y_1, \cdots, Y_{n-1}). \end{array}$$

Then

$$f_3(F_2) = \pi(Y_n - Q_1(Y_1, \cdots, Y_{n-1})) - (\pi Y_n - \pi Q'_1(Y_1, \cdots, Y_{n-1})) = 0.$$

Hence it induces a map

$$f'' : R[T_1, \cdots, T_n, S]/(F_2) \to R[Y_1, \cdots, Y_n].$$

which is also an isomorphism. Finally, let $f = f'' \circ f'$, then this is an isomorphism of R-algebras. Moreover, for $i \in [1, n]$,

$$\begin{array}{rcl} f(X_i) & = & f_3 \circ f_2 \circ f_1(X_i) \\ & = & f_3(f_2(\widetilde{R}_i(T_1, \cdots, T_n) + \pi \widetilde{\Phi}_i(T_1, \cdots, T_n))) \\ & = & f_3(\widetilde{R}_i(T_1, \cdots, T_n) + \pi \widetilde{\Phi}_i(T_1, \cdots, T_n)) \\ & = & R_i(Y_1, \cdots, Y_{n-1}) + \pi \Phi_i(Y_1, \cdots, Y_n) \end{array}$$

with R_i a p-polynomial, and for $f(X_{n+1})$, we have

$$\begin{array}{rcl} f(X_{n+1}) & = & f_3 \circ f_2 \circ f_1(X_{n+1}) \\ & = & f_3(f_2(X_{n+1})) \\ & = & f_3(S - T_1 Q'_2(T_1, \cdots, T_n)) \\ & = & Y_n + \pi \Phi_{n+1}(Y_1, \cdots, Y_n) \end{array}$$

with $\Phi_{n+1} \in R[Y_1, \cdots, Y_n]$. This finishes then the proof. □

Remark 3.9. — In this remark, we suppose that K is of characteristic $p > 0$. As a result, the composition of two p-polynomial morphisms with coefficients in K is again p-polynomial.

1. In Lemma 3.6, suppose further more that P is a p-polynomial. Let $f\colon R[X_1, \cdots, X_n] \to R[T_1, \cdots, T_n]$ be the isomorphism in *loc. cit.,* then f is a p-morphism. In particular, $f(P)$ is again a p-polynomial.
2. In Lemma 3.7, if we suppose moreover that F is a p-polynomial. Then the isomorphism f given in *loc. cit.* is p-polynomial, and the F_i' are all p-polynomials.
3. In Lemma 3.8, suppose further more that F is a p-polynomial. Then the isomorphism f in *loc. cit.* is p-polynomial.

3.3. Proof of the Theorem 3.3 and its corollary. —

3.3.1. We use the same notation as in § 3.1. We suppose first of all that the residue field of R is *perfect.* Let $\bar{I} = \{i_1 < i_2 < \cdots < i_{N-n}\} \subset [1, N]$. By using 3.7, we will first reduce to the case where $d_{i_j} = 1$, and the non zero coefficients $a_{ij\alpha}$ in (15) are invertible. More precisely, for each $j \in [1, N-n]$, let $P_j \in R[X_1, \cdots, X_{i_j - 1}]$ be the p-polynomial appeared in the equality (15), and we note

$$F_j = \pi^{d_{i_j}} X_{i_j} - P_j(X_1, \cdots, X_{i_j-1}) \in R[X_1, \cdots, X_{i_j}, \cdots, X_N].$$

We represent first the polynomial P_1 in the form

$$P_1 = P_1^{(0)} + \pi P_1^{(1)} + \cdots + \pi^{d_{i_1}-1} P_1^{d_{i_1}-1} + \pi^{d_{i_1}} P_1^{(d_{i_1})}$$

where the $P_1^{(i)}$ (for $i \in [0, d_1 - 1]$) are all p-polynomials with invertible nonzero coefficients. Applying Lemma 3.7, we obtain a morphism

$$\begin{aligned}
\widetilde{f_1} : R[X_1, \cdots, X_N] &\to R[Y_1, \cdots, Y_{i_1-1}, Y_{i_1}, \cdots, Y_{i_1+d_{i_1}}, \cdots, Y_{N+d_{i_1}}] \\
X_i &\mapsto Y_i \qquad \text{for } 1 \leq i < i_1; \\
X_i &\mapsto Y_{i+d_{i_1}} \quad \text{for } i_1 < i \leq N; \\
X_{i_1} &\mapsto Y_{i_1+d_{i_1}} + P^{(d_{i_1})}(Y_1, \cdots, Y_{i_1-1}).
\end{aligned}$$

inducing an isomorphism

$$f_1\colon R[X_1, X_N]/(F_1) \to R[Y_1, \cdots, Y_{N+d_1}]/(F_1^{(1)}, \cdots, F_1^{(d_{i_1})})$$

where by definition,

$$\begin{aligned}
F_1^{(i)} &= \pi Y_{i+i_1-1} - Y_{i+i_1-2} - P_1^{(i-1)}(Y_1, \cdots, Y_{i_1-1}) \quad 2 \leq i \leq d_{i_1}; \\
F_1^{(1)} &= \pi Y_{i_1} - P_1^{(0)}(Y_1, \cdots, Y_{i_1-1}).
\end{aligned}$$

By definition, $\widetilde{f_1}$ is a p-polynomial morphism, hence for $i \geq 2$, we have

$$\begin{aligned} F'_j : &= \widetilde{f_1}(F_j) \\ &= \pi^{d_{i_j}} Y_{i_j+d_{i_1}} - P_j(Y_1, \cdots, Y_{i_1-1}, Y_{i_1+d_1} - P_1^{(d_{i_1}-1)}(Y_1, \cdots, Y_{i_1-1}), Y_{i_1+1+d_{i_1}}, \cdots, Y_{i_j+d_{i_1}-1}) \\ &= \pi^{d_j} Y_{i_j+d_{i_1}} - P'_j(Y_1, \cdots, Y_{i_j+d_{i_1}-1}) - pQ'_j(Y_1, \cdots, Y_{i_j+d_{i_1}-1}) \end{aligned}$$

for some p-polynomial $P'_j \in R[Y_1, \cdots, Y_{i_j+d_{i_1}-1}]$, and some polynomial $Q'_j \in R[Y_1, \cdots, Y_{i_j+d_{i_1}-1}]$. By Definition 3.1, we have $\pi^{d_{i_j}}|p$, hence F'_j can be written again as

$$F'_j = \pi^{d_j} Y_{i_j+d_{i_1}} - P'_j - \pi^{d_{i_j}} R'_j$$

with $R'_j \in R[Y_1, \cdots, Y_{i_j+d_{i_1}-1}]$. Now, we write

$$P'_2 = P_2^{(0)} + \pi P_2^{(1)} + \cdots + \pi^{d_{i_2}} P_2^{d_{i_2}}$$

such that $P_2^{(j)}$ are p-polynomials for $j \in [0, d_{i_2}]$, moreover for those $j < d_{i_2}$, the nonzero coefficients of $P_2^{(j)}$ are all invertible. In this way

$$F'_2 = \pi^{d_{i_2}} Y_{i_2+d_{i_1}} - \left(\sum_{j=0}^{d_{i_2}-1} \pi^j P_2^{(j)} \right) - \pi^{d_{i_2}} \left(P^{(d_{i_2})} + R'_2 \right)$$

Now, we consider

$$\begin{aligned} \widetilde{f_2} : R[Y_1, \cdots, Y_{N+d_{i_1}}] &\to R[Z_1, \cdots, Z_{N+d_{i_1}+d_{i_2}}] \\ Y_i &\mapsto Z_i \qquad \text{for } 1 \leq i < d_{i_1} + i_2; \\ Y_i &\mapsto Z_{i+d_{i_2}} \quad \text{for } d_{i_1} + i_2 < i \leq N; \\ Y_{d_{i_1}+i_2} &\mapsto Z_{d_{i_1}+i_2+d_{i_2}} + P_2^{(d_{i_2})}(Z_1, \cdots, Z_{d_{i_1}+i_2-1}). \end{aligned}$$

which induces an isomorphism

$$R[Y_1, Y_2, \cdots, Y_{N+d_{i_1}}]/(F'_2) \to R[Z_1, \to Z_{N+d_{i_1}+d_{i_2}}]/(F_2^{(1)}, \cdots, F_2^{(d_{i_2})})$$

where

$$\begin{aligned} F_2^{(d_{i_2})} &= \pi Z_{i_2+d_{i_1}+d_{i_2}} - Z_{i_1+d_{i_1}+d_{i_2}-1} - P_2^{(d_{i_2}-1)} - \pi R'_2 \\ F_2^{(j)} &= \pi Z_{i_2+d_{i_1}+j} - Z_{i_1+d_{i_1}+(j-1)} - P_2^{(j-1)}, \quad j \in [2, d_{i_2}-1]; \\ F_2^{(1)} &= \pi Z_{i_2+d_{i_1}+1} - P_2^{(0)} \end{aligned}$$

Hence by considering the composition $f_2 \circ f_1$, we get an isomorphism

$$\frac{R[X_1, \cdots, X_N]}{(F_1, F_2)} \longrightarrow \frac{R[Z_1, \cdots, Z_{N+d_{i_1}+d_{i_2}}]}{\left(F_1^{(1)}, \cdots, F_1^{(d_{i_1})}, F_2^{(1)}, \cdots, F_2^{(d_{i_2})}\right)}$$

Moreover, since f_2 is a p-polynomial morphism, for each $j \geq 3$, $f_2(F'_j)$ is of the following form:

$$\pi^{d_{i_j}} Z_{i_j+d_{i_1}+d_{i_2}} - P''_j - pQ''_j$$

with $P''_j, Q''_j \in R[Z_1, \cdots, Z_{i_j+d_{i_1}+d_{i_2}-1}]$ such that P''_j is p-polynomial. Hence, if we continue this process, we eventually obtain an isomorphism

$$R[X_1, \cdots, X_N]/(F_1, \cdots, F_{N-n}) \to R[T_1, \cdots, T_{N+d}]/(F'_1, F'_2, \cdots, F'_{N-d+d}),$$

where $d = d_{i_1} + d_{i_2} + \cdots + d_{i_{N-n}}$, and for some

$$\bar{I} = \{i'_1 < i'_2 < \cdots < i'_{N-n+d}\} \subset [1, N+d]$$

we have

$$F'_j = \pi T_{i'_j} - P'_j(T_1, \cdots, T_{i'_j-1}) - \pi Q'_j(T_1, \cdots, T_{i'_j-1}). \tag{16}$$

and the P'_j are p-polynomials whose non zero coefficient are invertible. Therefore, we are reduced to the case where $d_{i_j} = 1$, and the F_j are of the form (16) such that the nonzero coefficients of the p-polynomial P_j are invertible.

3.3.2. We claim that for the p-polynomial P_j, its reduction $\overline{P_j}$ modulo π is irreducible. Indeed, let X_0 be the special fiber of the affine S-scheme X, then its affine ring

$$k[X_0] \simeq k[X_1, \cdots, X_N]/(\overline{P_1}, \cdots, \overline{P}_{N-n}).$$

But by our assumption, X_0 is integral and smooth of dimension n over k, hence all these $\overline{P}_j$ must be irreducible.

3.3.3. Since the reduction modulo π of P_1 is irreducible, there exists an isomorphism

$$f_1\colon = R[X_1, \cdots, X_{i_1}]/(F_1) \to R[Y_1, \cdots, Y_{i_1-1}]$$

such that

$$f_1(X_i) = R_i(Y_1, \cdots, Y_{i_1-1}) + \pi\Phi_i(Y_1, \cdots, Y_{i_1-1}), \quad 1 \leq i \leq i_1. \tag{17}$$

where the $R_i(Y_1, \cdots, Y_{i_1-1})$ are p-polynomials. Next, we extends f_1 to be an isomorphism

$$\begin{array}{rcl} \widetilde{f_1} : R[X_1, \cdots, X_{i_1}, X_{i_1+1}, \cdots, X_N]/(F_1) & \to & R[Y_1 \cdots, Y_{N-1}] \\ X_i & \mapsto & f_1(X_i) \quad 1 \leq i \leq i_1; \\ X_i & \mapsto & X_{i-1} \quad i > i_1. \end{array}$$

Moreover for $j \geq 2$,

$$\begin{array}{rcl} F'_j = \widetilde{f_1}(F_j) & = & \pi Y_{i_j-1} - P_1(f_1(X_1), \cdots, f_1(X_{i_1}), Y_{i_1}, \cdots, Y_{i_j-2}) \\ & & -\pi Q_j(f_1(X_1), \cdots, f_1(X_{i_1}), Y_{i_1}, \cdots, Y_{i_j-2}) \end{array}$$

Now using the equality (17), there exist a p-polynomial $P'_j \in R[Y_1, \cdots, Y_{i_j-2}]$, and a polynomial $Q_j \in R[Y_1, \cdots, Y_{i_j-2}]$ such that

$$F'_j = \pi Y_{i_j-1} - P_j(Y_1, \cdots, Y_{i_j-2}) - \pi Q_j(Y_1, \cdots, Y_{i_j-2})$$

hence

$$R[X_1, \cdots, X_N]/(F_1, \cdots, F_{N-n}) \simeq R[Y_1, \cdots, Y_{N-1}]/(F'_2, \cdots, F'_{N-n}).$$

Hence the theorem follows by induction on $N - n$. This finishes the proof of Theorem 3.3 when R has *perfect* residue field.

3.3.4. To treat the general case of Theorem 3.3, by **[7]** (Chapitre 0_{III} 10.3.1), there exists an extension $R \subset \widetilde{R}$ of discrete valuation rings such that $\widetilde{R}/R$ is integral (but in general, this extension is not finite) and that $\widetilde{R}$ has perfect residue field. Moreover $\widetilde{R}/R$ is obtained as the direct limit of some inductive system whose transition maps are extensions of the form indicated in the statement of Theorem 3.3. Now, according to what we have shown, there exists an isomorphism of $\widetilde{S} := \mathrm{Spec}(\widetilde{R})$-schemes $X_{\widetilde{S}} \to \mathbb{A}^n_{\widetilde{S}}$. Since both schemes are of finite presentation over $\widetilde{S}$, the general case of Theorem 3.3 follows by a limit argument.

3.3.5. It remains to prove the Corollary 3.4. Indeed, by Remark 3.9, all the isomorphisms in the proof of Theorem 3.3 in § 3.3.1-§ 3.3.4 are p-polynomial. As a result, what we obtain finally is an isomorphism of S-groups $\mathbb{G}^{N-n}_{a,S} \to G$. This gives Corollary 3.4.

3.4. Remarks. — In G/S is of one dimensional, it is possible to prove a more general statement.

Proposition 3.10. — *Let T be a locally noetherian normal integral scheme with $\eta \in T$ its generic point. Then every smooth group model of $\mathbb{G}_{a,\eta}$ over T with connected fibers is a form of $\mathbb{G}_{a,T}$ in the Zariski topology.*

The key point in the proof of the proposition is the following lemma, which treats the local version of the previous proposition. See also **[18]** (Theorem 2.2) for another proof of the following lemma by using the notion of Néron blow-ups (or dilatation).

Lemma 3.11. — *Let $S = \mathrm{Spec(R)}$ with R a discrete valuation ring. Let G be a smooth model of $\mathbb{G}_{a,K}$ over R with connected fibers. Then $G \simeq \mathbb{G}_{a,S}$.*

Proof. — Remark first that since G/S is flat of finite presentation with connected fibers, it follows that G/S is separated ([**4**] Exposé VI Corollaire 5.5). Further more, G/S is smooth with connected fibers such that G_K is affine, hence G/S is quasi-affine ([**11**] VII 2.2). Finally, by applying [**11**] IX 2.2, we find that G/S is affine. From now on, we will use the notations of § 2.3. Hence let $R[G] = R[y_1, \cdots, y_N]$ be its coordinate ring. Since $G_K = \mathbb{G}_{a,K}$ is of one dimensional, we have $\bar{I} = [2, N]$. We only need to show $\bar{I} = \emptyset$. Assume that $\bar{I} \neq \emptyset$. Then $R[G]$ is given by the relations

$$\pi^{d_i} y_i = y_{i-1}^{p^{r(i)}} + P_i(y_1, \cdots, y_{i-1}), \quad i \in [2, N] \tag{18}$$

where

$$P_i(y_1, \cdots, y_{i-1}) = \sum_{\beta < m(i-1, p^{r(i)})} a_{i\beta} y^{\beta}$$

is in reduced form. Moreover, by the choice $\{y_i\}$, the S-scheme $\mathrm{Spec}(R[y_1, y_2])$ has a group scheme structure. Let $\overline{y}_i \in k[G_k] = R[G]/\pi$ be the reduction modulo π of y_i, and we put $B = k[\overline{y}_1] \subset k[G_k]$. Then $H := \mathrm{Spec}(B)$ is a k-group scheme, and the canonical morphism of k-algebras $k[\overline{y}_1] \to R[G]/\pi = k[G_k]$ gives an epimorphism of k-group schemes:

$$G_0 \to H.$$

Now, according to (18), $\overline{y}_1$ satisfies only the the relation

$$y_1^{p^{r(2)}} - \overline{P}_2(y_1) = 0$$

with $\overline{P}_2(Y_1) \in k[Y_1]$ a polynomial of degree $< p^{r(2)}$. In particular, $k[y_1] = k[Y_1]/(Y_1^{p^{r(2)}} - \overline{P}_2(Y_1))$ is not integral. But since G_0 is smooth and integral, the group scheme H, being a quotient of G_0, must be integral. This gives us a contradiction. Hence $\bar{I} = \emptyset$. Hence $R[G] = R[y_1]$. Moreover, by the definition of y_1, we have $y_1 = \lambda x$ for some $\lambda \in K - \{0\}$, hence

$$\mu(y_1) = y_1 \otimes 1 + 1 \otimes y_1.$$

We find in this way an isomorphism of S-group schemes $G \simeq \mathbb{G}_{a,S}$. □

Proof of Proposition 3.10. — This is a local question, hence we may assume T noetherian regular and local. Let $\xi \in T$ any point of codimension 1 in T, and $T_\xi = \mathrm{Spec}(\mathcal{O}_{T,\xi})$. Then Lemma 3.11 implies that $G \times_T T_\xi \simeq \mathbb{G}_{a,T_\xi}$. Hence, there exists some neighborhood U of ξ, and an isomorphism of U-group schemes $f_U : G|_U \to \mathbb{G}_{a,U} = \mathrm{Spec}(\mathcal{O}_U[Y])$. By considering the same construction for each points of codimension 1 of Y, we can find a family of open subsets $\{U_\alpha : \alpha\}$ of T, such that its union $U = \cup_\alpha U_\alpha$ contains all the points of codimension 1 of T. Moreover, for each α, there exists an isomorphism of U_α-group schemes

$$f_\alpha : G|_{U_\alpha} \to \mathbb{G}_{a,U_\alpha} = \mathrm{Spec}(\mathcal{O}_{U_\alpha}[Y])$$

By consider the restriction

$$f_\alpha|_{U_\alpha \cap U_\beta} \circ \left(f_\beta|_{U_\beta \cap U_\alpha}\right)^{-1} : \mathbb{G}_{a,U_\alpha \cap U_\beta} \to \mathbb{G}_{a,U_\alpha \cap U_\beta}$$

is then given as the multiplication by an element $\mu_{\alpha\beta} \in \Gamma(U_\alpha \cap U_\beta, \mathcal{O}_T^*)$ (since the base scheme is regular). The datum $\{U_{\alpha\beta}, \mu_{\alpha\beta}\}$ gives us then a 1-cocycle of the multiplicative group, and hence an element of $\mathrm{H}^1(U, \mathcal{O}_U^*) = \mathrm{Pic}(U)$. On the other hand, we claim that the canonical map

$$\mathrm{Pic}(T) \to \mathrm{Pic}(U)$$

is surjective. Indeed, the scheme T being regular, and $T - U$ of codimension ≥ 2 in T, any Cartier divisor of U can be extended, by taking the schematic closure, to a unique Cartier divisor in T. In particular, the map above is surjective. Now, using the fact that T is local, hence $\mathrm{Pic}(T) = 0$, so is $\mathrm{Pic}(U)$. In particular, the 1-cocycle $\{U_\alpha, \mu_{\alpha\beta}\}$ is then actually a 1-coboundary. From this, there exist $\mu_\alpha \in \Gamma(U_\alpha, \mathcal{O}_T^*)$ such that $\mu_\alpha \mu_\beta^{-1} = \mu_{\alpha\beta}$. Now we define

$$g_\alpha = \mu_\alpha^{-1} \cdot f_\alpha \colon G|_{U_\alpha} \to \mathbb{G}_{a,U_\alpha}, \quad a \mapsto \mu_\alpha^{-1} \cdot f_\alpha(a)$$

we have then $g_\alpha|_{U_\alpha \cap U_\beta} = g_\beta|_{U_\alpha \cap U_\beta}$. Hence the isomorphisms g_α can be glued to a morphism of U-group schemes $g : G|_U \to \mathbb{G}_{a,U}$. Now we apply the Corollaire IX 1.4 of **[11]** to see that this isomorphism can be extended to an isomorphism of groups schemes $G \to \mathbb{G}_{a,T}$. This finishes the proof. □

To finish this section, we state the following conjectures given in **[20]**, which are still open, thought some special cases are known (see for example **[19]** **[8]** **[9]** **[13]**).

Conjecture 3.12. — *Let S be a normal locally noetherian integral scheme and G a smooth affine unipotent S-group scheme with connected fibers. Then G is a form of $\mathbb{A}_S^n$ with respect to the fppf topology. If in addition S is of characteristic p, then same holds with respect to the radical topology.*

Conjecture 3.13. — *Let R be a discrete valuation ring. Then every unipotent group model of affine space is a p-polynomial R-scheme.*

Note that the Conjecture 3.12 is also a special case of the following more general one

Conjecture 3.14. — *Let S as in the Conjecture 3.12 and X/S be a flat affine S-scheme such that the fiber $X_s \simeq \mathbb{A}_s^n$ for all $s \in S$. Then X/S is a form of $\mathbb{A}_S^n$ for the Zariski topology.*

4. Some explicit models of $\mathbb{G}_{a,K}^2$

In this section, we will construct some affine S-models of a unipotent group G_K such that $G_K \simeq \mathbb{A}_K^2$.

4.1. Extension of $\mathbb{G}_a$ by $\mathbb{G}_a$. — In § 1.2.3, we have seen that how to describe the extension of $\mathbb{G}_a$ by $\mathbb{G}_a$ over a field. We will prove a similar result over S. Recall that $S = \mathrm{Spec}(R)$ is the spectrum of a discrete valuation ring. Moreover, for a ring A of characteristic $p > 0$, we will denote by $A[F]$ the non commutative A-algebra generated by one element F with respect to the usual relations:

$$F \cdot a = a^p \cdot F, \quad \text{for any } a \in A.$$

Theorem 4.1. — *Let G be a* commutative *extension of $\mathbb{G}_{a,S}$ by $\mathbb{G}_{a,S}$. Then one can find $x, y \in R[G]$ such that $R[G] = R[x,y]$, and such that the comultiplication map is given*

$$\mu(x) = x \otimes 1 + 1 \otimes x, \quad \mu(y) = y \otimes 1 + 1 \otimes y + \sum_i a_i \Phi_i(x).$$

with $a_i \in R$. In particular, there exists an isomorphism of groups

$$R/p[F] \to \mathrm{Ext}^1_S(\mathbb{G}_{a,S}, \mathbb{G}_{a,S})$$

where the $\mathrm{Ext}^1_S(-,-)$ is taken in the category of abelian fppf-sheaves on S.

Proof. — Let G be an extension of $\mathbb{G}_{a,S}$ by $\mathbb{G}_{a,S}$. Since $\mathbb{G}_{a,S}$ is an affine scheme, we have $\mathrm{H}^1(\mathbb{G}^1_{a,S}, \mathcal{O}_{\mathbb{G}_{a,S}}) = 0$. In particular, $G \simeq \mathbb{A}^2_S$ as S-schemes. Hence there exist generators $x, y \in R[G]$ such that $R[G] = R[x,y]$, and the comultiplication on $R[G]$ is given by

$$\mu(x) = x \otimes 1 + 1 \otimes x, \quad \mu(y) = y \otimes 1 + 1 \otimes y + \eta(x) \tag{19}$$

which $\eta(x) \in R[x] \otimes_R R[x]$. In the following, we consider the case $\mathrm{Char}(K) = 0$ and the case $\mathrm{Char}(K) = p > 0$ separately.

First suppose that $\mathrm{Char}(K) = 0$. Then $G_K \simeq \mathbb{G}^2_{a,K}$, and hence one can find generator $u, v \in K[G_K]$ such that $u = x$, and that

$$\mu(u) = u \otimes 1 + 1 \otimes 1, \quad \mu(v) = v \otimes 1 + 1 \otimes v.$$

Since $y \in R[G] \subset K[G_K] = K[u,v]$, there exists some two variable polynomial such that $y = Q(u,v)$. Because of the formula (19), one must have $Q(u,v) = \lambda u + P(v)$ with P a polynomial in v, and $\lambda \in K$. We will show that up to replace y by some element of the form $y - \sum_r a_r x^r$ with $a_r \in R$, we may assume that

$$P(v) = \sum_i r_i v^{p^i} \in K[v]$$

such that $p \cdot r_i \in R$. The proof of this statement is similar to that of Theorem 2.23. Assume that we have proved that

$$\sum_{i \geq q} b_i x^i = \sum_i r_i x^{p^i}$$

such that $p \cdot r_i \in R$ (to start with, we can take $q \gg 0$ so that $\sum_{i \geq q} b_i x^i = 0$). We claim first that if $q-1$ is not a power of p, then $b_{q-1} \in A$. Indeed, let

$$z = \sum_{i \geq q} b_i x^i = \sum_i r_i x^{p^i},$$

then we have

$$\mu(z) = z \otimes 1 + 1 \otimes z + \sum_i p r_i \Phi_i(x)$$

Hence, we have

$$\begin{aligned} \eta(y) &= \eta\left(bv + \sum_{i<q-1} b_i x^i + b_{q-1}x^{q-1} + z\right) \\ &= \sum_{i<q-1} b_i \left((x \otimes 1 + 1 \otimes 1)^i - x^i \otimes 1 - 1 \otimes x^i\right) \\ &\quad + b_{q-1}\left((x \otimes 1 + 1 \otimes x)^{q-1} - x^{q-1} \otimes 1 - 1 \otimes x^{q-1}\right) + \sum_i p r_i \Phi_i(x). \end{aligned}$$

Since $\eta(y) \in R[G] \otimes R[G]$, we find for the reason of degree that

$$b_{q-1}\left(x \otimes 1 + 1 \otimes x\right)^{q-1} - x^{q-1} \otimes 1 - 1 \otimes x^{q-1} \in R[G] \otimes R[G].$$

Hence, we must have

$$b_{q-1}\binom{q-1}{j} \in \mathbb{Z}, \quad j = 1, 2, \cdots, q-2. \tag{20}$$

If $q-1$ is not a power of p, there exists some j such that $\binom{q-1}{j}$ is prime to p. From this, we must have $b_{q-1} \in R$. Up to modify y by $y - b_{q-1}x^{q-1}$, we may assume that $b_{q-1} = 0$ in this case. To complete the proof, it remains to show that if $q - 1 = p^{a+1}$ is a power of p for some $a \geq 0$, then $pb_{q-1} \in R$. Indeed, by using again the condition (20), we have in particular $b_{q-1}\binom{q-1}{p^a} \in R$. Since this binomial coefficient is congruent to p modulo p^2, we get finally $pb_{q-1} \in R$. Hence

$$\sum_{i \geq q-1} b_q x^q = \sum_i r_i' x^{p^{r_i}}$$

This finishes the proof when $\mathrm{Char}(K) = 0$.

For the case $\mathrm{Char}(K) = p$. One can find generater $u, v \in K[G_K]$ such that $u = x$, and that

$$\mu(v) = 1 \otimes v + v \otimes 1 + \sum_i a_i \Phi_i(x), \quad a_i \in K$$

We have similarly $y = bv + P(u)$ with $P(u) = \sum_i b_i u^i \in K[u]$ a polynomial. Up to replace v by bv, we may assume $b = 1$. By the same induction, we get that up to change y by some element of the form $y - \sum_i a_i x^i$ with $a_i \in R$, we may assume that

$$\sum_i b_i x^i = \sum_i r_i x^{p^{r_i}}.$$

Hence

$$\mu(y) = \mu(v) = \sum_i a_i \Phi_i(x) \in R[G] \otimes R[G]$$

Hence $a_i \in R$, and the formula of Theorem is proved.

To finish the proof of the theorem, we need to establish a bijection between the group $R/p[F]$ and the group $\mathrm{Ext}^1_S(\mathbb{G}_{a,S}, \mathbb{G}_{a,S})$. Now, as in **[3]** II § 3, 4.6, this group of extensions can be described by the following (symmetric) Hochschild cohomology group:

$$\mathrm{H}^2_s(\mathbb{G}_{a,S}, \mathbb{G}_{a,S}) = \frac{\left\{ f(X,Y) \in R[X,Y] : \begin{array}{c} f(Y,Z) - f(X+Y,Z) + f(X,Y+Z) - f(X,Y) = 0 \\ f(X,Y) = f(Y,X) \end{array} \right\}}{\{\ P(X+Y) - P(X) - P(Y) \in R[X,Y] \ \ : \ \ P \in R[X] \ \}}$$

The previous proof shows that this cohomology group is generated over R by the classes of the polynomials

$$W_r(X,Y) := \frac{1}{p}\left((X+Y)^{p^r} - X^{p^r} - Y^{p^r}\right), \quad r = 1, 2, \cdots$$

Since more over $pW_r = P(X+Y) - P(X) - P(Y)$ with $P = X^{p^r} \in R[X]$, the R-module $\mathrm{H}^2_s(\mathbb{G}_{a,S}, \mathbb{G}_{a,S})$ is killed by p. Hence, it is naturally a R/p-module, which is free with a basis given by the family $\{\overline{W_r} : r = 1, 2, \cdots\}$. On can also define an action of Frobenius F on this R/p-module by the following formula:

$$F \cdot \left(\sum_r a_r \overline{W_r}\right) := \left(\sum_r a_r \overline{W_r}\right)^p = \sum_r a_r^p \overline{W_r^p}, \qquad a_r \in R/p.$$

Hence $\mathrm{H}^2_s(\mathbb{G}_{a,S}, \mathbb{G}_{a,S})$ becomes an $R/p[F]$-module. Since

$$W_r^p \equiv W_{r+1} \mod p$$

we find $F \cdot \overline{W_r} = \overline{W_{r+1}}$. In this way, we get that $\mathrm{H}^2_s(\mathbb{G}_{a,S}, \mathbb{G}_{a,S})$ is an $R/p[F]$-module free of rank 1, with a basis given by $\{\overline{W_1}\}$. This completes the proof. □

4.2. More explicit models of $\mathbb{G}_a^2$ in mixed characteristic. — In this section, let R be a discrete valuation ring of mixed characteristic $(0, p)$.

Definition 4.2. — Let $a = (a_i : i \in \mathbb{Z}_{\geq 0})$ and $b = (b_i : i \in \mathbb{Z}_{\geq 0})$ be two series of elements in R, such that at least one of the elements a_i, b_j $(i, j \in \mathbb{Z}_{\geq 0})$ is invertible. Let $d \geq 0$ be an integer such that $\pi^{d+1}|p$. We define G/S to be the affine group scheme $\mathrm{Spec}(R[G])$ with

$$R[G] = R[X,Y,Z]/(\pi^{d+1}Z - \sum_{i\geq 0} a_i X^{p^i} - \sum_{i\geq 0} b_i Y^{p^i})$$

where the comultiplication given by (here, we denote by x, y, z the image of X, Y, Z in R[G])

$$\eta(x) = \eta(y) = 0, \quad \eta(z) = \pi^{-d-1}\cdot p \cdot \left(\sum_{i\geq 1} a_i \Phi_i(x) + \sum_{i\geq 1} b_i \Phi_i(y)\right)$$

Such a group scheme will be denoted by $G_{d,a,b}$.

Remark 4.3. — These models can also be constructed by using successive dilatations on $\mathbb{G}^2_{a,S}$. For example, we consider first $G = \mathbb{G}^2_{a,S} = \mathrm{Spec}(R[X,Y])$, and the closed group subscheme $H \subset G_k$ defined by the ideal

$$\left(\pi, \sum_i a_i X^{p^i} + \sum_i b_i Y^{p^i}\right) \subset R[X,Y]$$

Then $G_{0,a,b}$ is the dilatation of G along H.

Lemma 4.4. — *Let $\{a = (a_i), b = (b_i)\}$ and $\{a' = (a'_i), b' = (b'_i)\}$ be two pairs of series as in Definition 4.2. If*

$$a_i \equiv a'_i \mod \pi^{d+1}, \quad \textit{and} \quad b_i \equiv b'_i \mod \pi^{d+1}, \qquad i = 0, 1, 2, \cdots$$

Then $G_{d,a,b} \simeq G_{d,a',b'}$.

Proof. — Let $a_i - a'_i = \pi^{d+1}\cdot c_i$ and $b_i - b'_i = \pi^{d+1}\cdot d_i$. We define the isomorphism $R[G_{d,a,b}] = R[x,y,z] \to R[G_{d,a',b'}] = R[x',y',z']$ by

$$x \mapsto x', \quad y \mapsto y', \quad z \mapsto z' + \sum_i c_i x'^{p^i} + \sum_i d_i y'^{p^i}.$$

□

Let $R_d = R/\pi^{d+1}$, and $R^2_d[F]$ be the additive group of noncommutative polynomials of F with coefficient in R^2_d. Hence, an element of $R^2_d[F]$ can be written as

$$\sum_{i\geq 0} r_i \cdot F^i, \quad \text{with } r_i \in R^2_d.$$

Finally, let $\Pi_d \subset R^2_d[F]$ be the pre-image of $k^2[F] - \{0\}$ by the canonical map $R^2_d[F] \to k^2[F]$. As a result of the previous lemma, for any group $G_{d,a,b}$ in Definition 4.2, let

$$\omega_{a,b} := \sum_i r_i F^i \in \Pi_d, \quad \text{with } r_i = (\overline{a_i}, \overline{b_i}) \in R^2_d$$

Then any group schemes $G_{d,a,b}$ with the same element $\omega = \omega_{a,b} \in \Pi_d$ are isomorphic. Hence, for any element $\omega \in \Pi_d$, we will denote by G_ω the corresponding isomorphic class.

Definition 4.5. — Let $\mathrm{Aut}_{R_d}(R_d[X,Y])$ be the group of automorphisms of the R_d-algebra $R_d[X,Y]$. We define $\mathcal{H}_d \subset \mathrm{Aut}_{R_d}(R_d[X,Y])$ be the subgroup generated by the following two kinds of automorphisms

(i) $\phi_D \colon R_d[X,Y] \to R_d[X,Y]$ such that

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto D \cdot \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} \alpha X + \beta Y \\ \gamma X + \delta Y \end{pmatrix}, \quad \text{with } D = \left(\begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right) \in \mathrm{GL}_2(R_d).$$

(ii) $\psi \colon R_d[X,Y] \to R_d[X,Y]$ such that

$$X \mapsto X + \pi \sum_i \alpha_i X^{p^i}, \quad \alpha_i \in R_d$$

$$Y \mapsto Y + \pi \sum_i \beta_i Y^{p^i} + \sum_i \gamma_i X^{p^i}, \quad \beta_i\ \gamma_i \in R_d$$

We will denote by $\mathcal{H}'_d \subset \mathcal{H}_d$ the subgroup of $\mathcal{H}_d$ generated by the automorphisms ϕ_D in (i). In particular, $\mathcal{H}'_d \simeq \mathrm{GL}_2(R_d)$

Remark 4.6. — If we consider $\mathbb{G}^2_{a,S_d} = \mathrm{Spec}(R_d[X,Y])$, then the group $\mathcal{H}_d$ considered in the Definition 4.5 is precisely the group of automorphisms of this group scheme over S_d.

We define an action of $R_d^* \times \mathcal{H}_d$ on $R_d^2[F]$ by the following formula:

– For $\lambda \in R_d^*$, and $D \in \mathrm{GL}_2(R_d)$, define

$$(\lambda, \phi_D) \cdot \left(\sum_i r_i F^i \right) = \sum_i \lambda^{-1} \cdot (r_i \cdot D'^{p^i}) \cdot F^i;$$

– For $\lambda \in R_d^*$, and ψ an automorphism of second kind as given in Definition 4.5, then

$$(\lambda, \psi) \cdot \left(\sum_i r_i F^i \right) = \sum_i \widetilde{r}_i F^i$$

where if we write $r_i = (r'_i, r''_i)$, and $\widetilde{r}_i = (\widetilde{r}'_i, \widetilde{r}''_i)$, then

$$\widetilde{r}'_i = \lambda^{-1} \cdot \left(r'_i + \sum_{s+t=i} r'_s (\pi\beta_t)^{p^s} + \sum_{s+t=i} r''_s \gamma_t^{p^s} \right);$$

$$\widetilde{r}''_i = \lambda^{-1} \left(r''_i + \sum_{s+t=i} r''_s (\pi\beta_t)^{p^s} \right).$$

One verifies that these formulas give an action of $R_d^* \times \mathcal{H}_d$ on $R_d^2[F]$, inducing an action of this group on Π_d.

Proposition 4.7. — *For any two elements $\omega, \omega' \in \Pi_d$.*

1. *The groups G_ω and $G_{\omega'}$ are isomorphic if and only if there exist (λ, ϕ_D) for some $D \in \mathrm{GL}_2(R_d)$ such that $(\lambda, \phi_D) \cdot \omega = \omega'$.*
2. *If $g \cdot \omega = \omega'$ for some $g \in R_d^* \times \mathcal{H}_d$. Then there is an isomorphism of group schemes over S_d*
$$G_\omega \otimes R_d \simeq G_{\omega'} \otimes R_d.$$

Proof. — Put $\omega = \omega_{a,b}$ and $\omega' = \omega_{a',b'}$ with (a,b) and (a',b') two pairs of series as in the Definition 4.2. Since K is of characteristic zero, the only primitives elements in $R[G_\omega]$ (*i.e.,* the elements $u \in R[G_\omega]$ such that $\eta(u) = 0$) are those contained in $Rx + Ry \in R[G_\omega]$. Hence any isomorphism $\phi : G_\omega \to G_{\omega'}$ must be given by a substitution of the following form:

$$x \mapsto \alpha x + \beta y, \quad y \mapsto \gamma x + \delta y, \quad z = \lambda z + P(x,y),$$

with

$$D = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(R), \quad \lambda \in R^*, \quad P \in R[x,y].$$

In order that this map can gives an isomorphism between $R[G_\omega]$ and $R[G_{\omega'}]$, we must have the following equality

$$\begin{array}{rl} & \pi^{d+1} \cdot (\lambda z + P(x,y)) - \sum_i \left(a_i(\alpha x + \beta y)^{p^i} + b_i(\gamma x + \delta y)^{p^i} \right) \\ = & \lambda' \cdot \left(\pi^{d+1} z - \sum_i \left(a_i' x^{p^i} + b_i' y^{p^i} \right) \right). \end{array} \tag{21}$$

for some $\lambda \in R^*$. As a result, we find $\lambda' = \lambda$ and

$$\lambda a_i' \equiv a_i \alpha^{p^i} + b_i \gamma^{p^i} \mod \pi^{d+1}, \quad \lambda b_i' = a_i \beta^{p^i} + b_i \delta^{p^i} \mod \pi^{d+1}.$$

Hence $\omega' = (\overline{\lambda}, \phi_{\overline{D}}) \cdot \omega$, with $\overline{\lambda} \in R_d$ (*resp.* $\overline{D} \in \mathrm{GL}_2(R_d)$) the image of λ (*resp.* D) in R_d (*resp.* in $\mathrm{GL}_2(R_d)$). Conversely, if $\omega' = (\overline{\lambda}, \phi_{\overline{D}}) \cdot \omega$ for some matrix

$$D = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(R) \quad \text{and } \lambda \in R.$$

We define then an isomorphism $R[G_\omega] \to R[G_{\omega'}]$ given by

$$x \mapsto \alpha x + \beta y, \quad y \mapsto \gamma x + \delta y, \quad z \mapsto z + P(x,y) \tag{22}$$

with $P(X,Y) \in K[X,Y]$ the polynomial defined by the equality (21)

$$P(X,Y) = \pi^{-d-1} \cdot \left(\sum_i \left(a_i(\alpha X + \beta Y)^{p^i} + b_i(\gamma X + \delta Y)^{p^i} \right) - \sum_i (a_i' X^{p^i} + b_i' Y^{p^i}) \right).$$

Since $(\overline{\lambda}, \phi_{\overline{D}}) \cdot \omega = \omega'$, and $\pi^{d+1} | p$, we find $P \in R[X,Y]$. Hence the morphism (22) is well-defined, and gives indeed an isomorphism between $R[G_\omega]$ and $R[G_{\omega'}]$. This finishes the proof of (1). To prove (2), suppose that $g \cdot \omega = \omega'$

with $g \in R_d^* \times \mathcal{H}_d$, we need to construct an isomorphism of Hopf-algebras over R_d:

$$R_d[G_\omega] \to R_d[G_{\omega'}].$$

By the proof of (1), we only need to consider the case of $g = (1, \psi)$ with ψ the isomorphism given in the second case of Definition 4.5. We put

$$f(X,Y) = X + \pi \sum_i \widetilde{\alpha}_i X^{p^i}, \quad g(X,Y) = Y + \pi \sum_i \widetilde{\beta}_i Y^{p^i} + \sum_i \widetilde{\gamma}_i X^{p^i}$$

with $\widetilde{\alpha}_i, \widetilde{\beta}_i, \widetilde{\gamma}_i$ be any lifting of $\alpha_i, \beta_i, \gamma_i$, and define

$$P(X,Y) := \pi^{-d-1} \cdot \left(\sum_i \left(a_i (f(X,Y))^{p^i} + b_i (g(X,Y))^{p^i} \right) - \sum_i (a_i' X^{p^i} + b_i' Y^{p^i}) \right).$$

Since $p^{d+1}|p$ and since $(1, \psi) \cdot \omega = \omega'$, the polynomial $P(X,Y)$ has coefficients in R. Finally, we put $\widetilde{P}(X,Y)$ the reduction of $P \in R[X,Y]$ modulo π^{d+1}, and we define the morphism $R_d[G_\omega] \to R_d[G_{\omega'}]$ by

$$x \mapsto f(x,y), \quad y \mapsto g(x,y) \quad z \mapsto z + \widetilde{P}(x,y).$$

One verifies that this gives an isomorphism of groups schemes over S_d between $G_\omega \otimes R_d$ and $G_{\omega'} \otimes R_d$. This finishes then the proof. □

Corollary 4.8. — *Let $\omega \in \Pi_d$. There exists infinitely many isomorphism classes over S of the family of S-groups $\{G_{d,a,b}\}$ which over S_d are isomorphic to $G_\omega \otimes R_d$.*

As an application of these computations, suppose the residue field k of R is *perfect* and $p = \pi^e u$ with $u \in R^*$. Let $\underline{G}$ be a smooth commutative connected two dimensional unipotent over k. Then there exist coordinates of G such that $G = \mathrm{Spec}k[U,V]$ such that the comultiplication is given by

$$\mu(U) = U \otimes 1 + 1 \otimes U, \quad \mu(V) = V \otimes 1 + 1 \otimes V + \sum_i \bar{a}_i \Phi_i(U)$$

For each i such that $\bar{a}_i \neq 0$, let $a_i \in R$ be a lifting of $\bar{a}_i$. Let $b = (1, 0, \cdots)$. Then $G_{e-1,a,b}$ is a lifting of $\underline{G}$ over S. Hence, there is infinitely many non isomorphic unipotent groups G_ω such that $G_\omega \otimes R_{e-1} \simeq G_{e-1,a,b} \otimes R_{e-1}$. Moreover, inside these non isomorphic groups, there is exactly one G_{ω_0} which admits a composition series with quotients isomorphic to $\mathbb{G}_{a,S}$.

References

[1] S. Bosch. W. Lütkebohmert. M. Raynaud. — *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **21**. Springer-Verlag, Berlin, 1990.

[2] N. Bourbaki. *Lie groups and Lie algebras: chapters 1-3.* Elements of Mathematics, Springer-Verlag. 1989.

[3] M. Demazure. P. Gabriel. — *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commuattifs.* Masson, Paris; North-Holland, Amsterdam, 1970.

[4] M. Demazure. A. Grothendieck. — *Schémas en groupes. Tome I: Propriétés générales des schémas en groupes.* Lecture Notes in Mathematics, Vol. **151**. Springer-Verlag, 1970.

[5] M. Demazure. A. Grothendieck. — *Schémas en groupes. Tome II: Groupes de Type Multiplicatif, et Structure des Schemas en Groupes Generaux.* Lecture notes in Mathematics, Vol. **152**. Springer-Verlag, 1970.

[6] M. Demazure. A. Grothendieck. — *Schémas en groupes. Tome III: Structure des Schemas en Groupes Reductifs.* Lecture Notes in Mathematics, Vol. **153**. Springer-Verlag, 1970.

[7] A. Grothendieck. — *Éléments de géométrie algébrique: III Étude cohomologique des faisceaux cohérents, Première partie.* rédigé avec la collaboration de J. Dieudonné. Inst. Hautes Études Sci. Publ. Math. No. **11** 1961 5-167.

[8] T. Kambayashi. *On one-parameter family of affine planes.* Invent. Math. **52** (1979), no. 3, 275-281.

[9] T. Kambayashi. M. Miyanishi. *On flat fibrations by the affine line.* Illinois J. Math. **22** (1978), no. 4, 662-671.

[10] T. Kambayashi. M. Miyanishi. M. Takeuchi. — *Unipotent algebraic groups.* Lecture Notes in Math., Vol. **414**, Springer-Verlag, Berlin, Heidelberg, and New York, 1974.

[11] M. Raynaud. — *Faisceaux amples sur les schémas en groupes et les espaces homogènes.* Lecture Notes in Math., Vol. **119**, Springer-Verlag, Berlin and New York, 1970.

[12] M. Raynaud. — *Spécialisation du foncteur de Picard.* Inst. Hautes Études Sci. Publ. Math. No. **38** 1970 27-76.

[13] A. Sathaye. — *Polynomial ring in two variables over a D.V.R.: a criterion.* Invent. Math. **74**, 159-168 (1983).

[14] C. Schoeller. — *Groupes affines, commutatifs, unipotents sur un corps non parfait.* Bull. Soc. Math. France 100 (1972), 241-300.

[15] J. -P. Serre. — *Groupes algébriques et corps de classes.* Reprint of the second edition. Publications de l'Institut Mathématique de l'Université de Nancago, 7. Actualités Scientifiques et Industrielles, 1264. Hermann, Paris, 1984.

[16] M. Takeuchi. — *On the structure of commutative affine group schemes over a non-perfect field.* Manuscrripta Math. **16**, 101-136 (1975).

[17] J. Tits. — *Lectures on algebraic groups.* Yale Univ., New Haven, 1967.

[18] W. Waterhause. B. Weisfeiler — *One dimensional affine group schemes.* J. Algebra **66** (1980), no. 2, 550-568.

[19] W. Waterhause. — *Polynomial group laws over valuation rings.* Illinois J. Math. **26** (1982), no. 2, 252-256.

[20] B. Weisfeiler. I. Dolgacev. — *Unipotent group schemes over integral rings.* Izv. Akad. Nauk SSSR Ser. Mat. Tom **38** (1974), No. 4.

JILONG TONG, Université de Bordeaux 1, Institut de Mathématiques de Bordeaux, 33405 Talence France • *E-mail :* `jilong.tong@math.u-bordeaux1.fr`