Mathematics of the USSR-Izvestiya

UNIPOTENT GROUP SCHEMES OVER INTEGRAL RINGS

Izv. Akad. Nauk SSSR
Ser. Mat. Tom 38 (1974), No. 4

Math. USSR Izvestija
Vol. 8 (1974), No. 4

UNIPOTENT GROUP SCHEMES OVER INTEGRAL RINGS

UDC 519.4

B. Ju. VEĬSFEĬLER AND I. V. DOLGAČËV

Abstract. In this paper we study families of unipotent algebraic groups over integral rings. The main results relate to the geometry of such families. In particular, we prove that, under some hypotheses, the space of such a family is isomorphic to an affine space over the base. We give counterexamples showing that in the case of an arbitrary base ring the basic facts of the theory of unipotent algebraic groups over a field cease to be true. For a certain class of the group schemes that we consider we prove results on cohomology, extensions and deformations.

Introduction

The present paper is devoted to the study of families of unipotent algebraic groups parametrized by an affine integral scheme S (or, more precisely, to the study of unipotent group schemes over S in the sense of (0.8)).* The general theory of group schemes was established in the seminar of Grothendieck and Demazure [2] (SGAD), in which, in addition, families of reductive groups were studied.

The theory of unipotent algebraic groups, and in particular that of commutative unipotent groups, over a field represents a beautifully complete theory (see, for example, [7]). On the other hand, questions about families of unipotent groups arise naturally in the theory of quasielliptic algebraic surfaces [11]. Moreover, unipotent groups play an important role in studying the structure of affine groups over a field, and the same role can be expected of them over arbitrary schemes. It is curious to note also that the study of unipotent group schemes leads to interesting questions in the geometry of affine varieties (see §3.8.5 in particular).

The majority of the results of this paper are based on the assumption that the base scheme is the spectrum of a discrete valuation ring. The examples of §6 show that unipotent group schemes over general integral rings have many pathological properties (which, however, are not surprising in the light of the work of Raynaud [12]).

As is well known, the theory of unipotent groups over a field is only interesting in

---

AMS (MOS) subject classifications (1970). Primary 14L15; Secondary 14M20, 14F20.

**Translator's note.* A study of unipotent algebraic groups by T. Kambayashi, M. Miyanishi and M. Takeuchi has recently been published (Lecture Notes in Math., vol. 414, Springer-Verlag, New York-Heidelberg-Berlin, 1974).

positive characteristic. According to Raynaud's results this also holds in the general case: over schemes of characteristic 0 the theory is trivial.

The main property of unipotent groups over a field consists of the existence of a composition series of elementary groups (i.e. subgroups of the additive group of the field). As the examples of §6 show, the only analogue of this property over general integral rings is a theorem on linear unipotence (§1). If the ground ring is a discrete valuation ring, then one can prove the stronger assertion about the extension of a composition series from the generic fiber to a flat series over the ring (cf. §4).

In §2 we study the coordinate ring of a unipotent group scheme over a discrete valuation ring. The results of this section play the basic role in studying the geometry of such groups. Each such group, under some restrictions on the generic fiber, is given as a complete intersection in affine space. If the ground ring is equicharacteristic and the group is commutative and smooth of period p with connected fibers, then it becomes $\mathbf{A}_S^n$ over some radical extension of the base (Theorem 3.5). This result generalizes the well-known classical result. A discussion of some natural generalizations of this result is given in §3.8.

In §4 we show that smooth connected groups lift from a perfect field of characteristic p to unipotent group schemes over rings of characteristic 0. There we also find extensions of $\mathbf{G}_m$ by $\mathbf{G}_a$. In §5, using a standard cohomological technique, we compute the Grothendieck cohomology groups of commutative unipotent group schemes.

At the present time (i.e. a year after the present work was completed) we are certain that the ideas, methods and results of this paper can also be applied in studying models of tori and semisimple groups. We have a number of examples of such models. The fact that unipotent groups are essential here is clear, for example, for the following reason: if G is a model of a torus (i.e. if G is a torus over the generic fiber), then G degenerates to a unipotent group over some closed set. Preliminary considerations show that the methods of §§2 and 4 can be applied to models of the group $\mathbf{G}_m$ and give analogous results. Moreover, we have succeeded in computing extensions of some models of $\mathbf{G}_m$ by $\mathbf{G}_a$ (cf. §4.7) over equicharacteristic rings.

We thank V. I. Danilov for useful comments.

§0. Notation and review

0.1. Let S be a scheme and (Sch/S) the category of S-schemes. A group object of this category is called a group scheme over S ((SGAD), I, 2.1; see also [9], §11). For any S-scheme T and any S-group scheme G the set $G(T) = \mathrm{Hom}_S(T, G)$ is an abstract group, called the group of T-points of G. The association $T \to G(T)$ defines a contravariant functor from the category Sch/S into the category of groups (Gr). This functor is often identified with the group scheme G.

Group schemes over S form a subcategory of Sch/S, whose morphisms are homomorphisms of group schemes, defined in the natural way.

0.2. As is the case for every S-scheme, the terminology of the theory of schemes is applied for S-group schemes. In particular, one defines such concepts as affine, flat and smooth S-group schemes.

0.3. We recall that if $S = \operatorname{Spec} A$, where A is a field, then any S-scheme is flat. But if A is a one-dimensional regular ring (for example, a discrete valuation ring), then the condition that a scheme X of finite type over S be flat is equivalent to the following ([6], Chapter I, §2.4, Proposition 3):

0.3.1. The A-algebra $\mathcal{O}_{X,x}$ is torsion-free for all $x \in X$.

In the general case, if the base scheme S is regular, then the condition that a scheme X locally of finite type over S be flat is equivalent to the following:

0.3.2. The fibers X_s, $s \in S$, have the same dimension ((EGA) IV, 14.4.4, 15.4.2).

We note that the fibers of a flat morphism $f: X \to S$, where S is connected, have the same dimension.

0.4. In case the base scheme S is locally noetherian, the condition that a scheme X locally of finite type over S be smooth is as follows ((EGA), IV, 17.5.2): X is a flat S-scheme and for all $s \in S$ the fiber X_s is a smooth scheme over the residue field $k(s)$ of the point s.

As is known, that a group scheme over a field k is smooth is equivalent to its being geometrically reduced ([7], Chapter II, §5, Theorem 2.1). By Cartier's theorem ([7], Chapter II, §6, no. 1), if S is a scheme of characteristic zero (i.e. a $\mathbf{Q}$-scheme), then any flat S-group scheme is a smooth S-scheme.

0.5. Let G be an affine S-group scheme. Assume that $S = \operatorname{Spec} A$ is an affine scheme. Then G is also affine, i.e. $G = \operatorname{Spec} B$, where B is an A-algebra.

The ring $B = \Gamma(G, \mathcal{O}_G)$ is denoted by $A[G]$ and is called the coordinate ring of the affine A-group scheme G. The structure of a group scheme on a scheme G is equivalent in this case to giving B an A-algebra structure. The latter is defined by giving three A-algebra homomorphisms:

$$\mu: B \to B \otimes_A B \quad \text{(comultiplication)},$$

$$\iota: B \to B \quad \text{(coinversion)},$$

$$\varepsilon: B \to A \quad \text{(coidentity)},$$

for which the standard axioms hold ((SGAD), I, 4.2; see also [9]).

0.5.1 If $f: G \to S$ is a flat S-group scheme of finite type over S and $f_*(\mathcal{O}_G)$ is a flat $\mathcal{O}_S$-module, then on $G' = \operatorname{Spec}(f^*\mathcal{O}_G))$ there exists a structure of an affine flat S-group scheme for which the canonical homomorphism $u: G \to G'$ is a homomorphism. The scheme G' is called the affinization of the group scheme G. By the results of Raynaud ([12], VII, 3.2), the affinization is defined in case S is regular and $\dim S \leq 2$. Moreover, in this case, if G is quasi-affine, then the homomorphism $u: G \to G'$ is an open immersion ([12], VII, 3.1).

0.5.2. By the results of Raynaud ([12], VII, 2.2), if S is a normal scheme and G is a smooth S-group scheme with connected fibers, whose fibers over the maximal points (generic points of the irreducible components of S) are affine, then G is quasi-affine.

0.6. Let G be a group scheme over a field k and G^0 the connected component of G containing the identity. Then G^0 is geometrically connected ((SGAD), VI_A, 2.1.1).

For any S-group scheme G we denote by G^0 the subset of G that is the union of the connected components of the fibers G_s^0 for $s \in S$. If G^0 is open (for example, when G is smooth over S ((SGAD), VI_A, 3.10), then the corresponding subscheme is denoted by G^0 and is called the connected component of the identity of G. It is an S-group scheme, and for any S-scheme T we have

$$G^0(T) = \{u \in G(T) : \forall t \in T \text{ the image of } u \text{ in } G_t(t) \text{ is contained in } G_t^0(t)\}.$$

Obviously $G = G^0$ if and only if the fibers of G are connected.

0.7. We now recall some definitions and properties of unipotent algebraic groups over a field (here by algebraic groups we mean group schemes of finite type over a field; they are not necessarily smooth).

0.7.1. An algebraic group G over a field k is said to be unipotent if the following equivalent conditions hold:

a) G is affine and in $k[G]$ there exist generators $t_1, \ldots, t_n$, such that $\mu(t_i) = t_i \otimes 1 + 1 \otimes t_i + \Sigma a_{ij} \otimes b_{ij}$, where $a_{ij}, b_{ij} \in k[t_1, \ldots, t_{i-1}]$ (cf. [16], Chapter VII, §1.6, Remark 2).

b) G possesses a composition series whose successive quotients are isomorphic to the subgroups $\mathbf{G}_{a,k}$ (cf. (SGAD), XVII, 3.5, 1.5).

0.7.2. Examples. a) $\mathbf{G}_{a,k}$ is the additive group;

$$k[\mathbf{G}_{a,k}] = k[t], \quad \mu(t) = t \otimes 1 + 1 \otimes t,$$
$$\iota(t) = -t, \quad \varepsilon(t) = 0.$$

b) $\alpha_{q,k}$, where $q = p^r$, $p = \operatorname{char} k > 0$;

$$k[\alpha_{q,k}] = k[t]/(t^q), \quad \mu(t) = t \otimes 1 + 1 \otimes t.$$

c) $(\mathbf{Z}/p\mathbf{Z})_k$, $p = \operatorname{char} k > 0$;

$$k[(\mathbf{Z}/p\mathbf{Z})_k] = k[t]/(t^p - t), \quad \mu(t) = t \otimes 1 + 1 \otimes t.$$

d) Forms of $\mathbf{G}_{a,k}$, $p = \operatorname{char} k > 0$:

$$k[G] = k[t_1, t_2], \quad t_1^{p^n} = a_0 t_2 + a_1 t_2^p + \ldots + a_m t_2^{p^m},$$
$$a_0 \neq 0, \quad a_i \in k, \quad \mu(t_i) = t_i \otimes 1 + 1 \otimes t_i,$$
$$\iota(t_i) = -t_i, \quad \varepsilon(t_i) = 0, \quad i = 1, 2.$$

According to [15] these equations give all the k-forms of $\mathbf{G}_{a,k}$. They are trivial if k is perfect. If $a_0 = 1$, then $k(a_1^{p^{-n}}, \ldots, a_m^{p^{-n}})$ is a minimal (purely inseparable) decomposition field for G.

e) *Two-dimensional smooth connected groups.* We write

$$\Phi_r(x) = \frac{1}{p} \sum_{i=1}^{p^r-1} C_{p^r}^i x^i \otimes x^{p^r-i} \in \mathbf{Z}[x] \otimes \mathbf{Z}[x].$$

We put

$$k[G] = k[t_1, t_2], \quad \mu(t_1) = t_1 \otimes 1 + 1 \otimes t_1,$$
$$\mu(t_2) = t_2 \otimes 1 + 1 \otimes t_2 + \sum a_i \Phi_i(t_1), \quad a_i \in k.$$

Any unipotent two-dimensional connected smooth group is given by such formulas if k is perfect ([16], Chapter VII, §2.7, Proposition 8).

f) If k is a field of characteristic 0 and G a unipotent group scheme over k, then G is a smooth connected group. If $\mathfrak{g}$ is its Lie algebra, then for any k-algebra A the group $G(A)$ is identified with $\mathfrak{g}(A)$ via mapping $\exp: \mathfrak{g}(A) \to G(A)$, where for $x \in \mathfrak{g}(A)$

$$\exp x = \sum_0^\infty (\operatorname{ad} x)^i (i!)^{-1}$$

(this series terminates since $\mathfrak{g}$ is nilpotent), and the multiplication is given by the Campbell-Hausdorff formula ((SGAD), XVII, 3.9 ter). In particular, if G is commutative, then $G \cong \mathbf{G}_{a,k}^n$.

0.7.3. An affine unipotent algebraic group over the field k possesses the following properties (see (SGAD), XVII, 3.9, 4.1.1, 4.1.3):

a) *G has a central composition series whose successive quotients are isomorphic to $\mathbf{G}_{a,k}$ if k is of characteristic 0 (see 0.7.2f)) (respectively to one of the groups $\mathbf{G}_{a,k}$ or $\alpha_{p,k}$, or to a k-form of the group $(\mathbf{Z}/p\mathbf{Z})^r$ if char $k = p > 0$).*

b) If G is connected, then there exists a composition series with quotients isomorphic to $\mathbf{G}_{a,k}$ or to $\alpha_{p,k}$.

c) If G is connected and smooth, then G possesses a central composition series whose successive quotients are k-forms of $\mathbf{G}_a$. In particular, the space G is a form of the affine space $\mathbf{A}_k^n$. If k is perfect, these forms are trivial. In the general case the forms of $\mathbf{G}_{a,k}$ are isomorphic to $\mathbf{G}_{a,k}$ over a suitable radical extension.

0.8. **Definitions.** Let G be a flat group scheme of finite type over S. We say that

a) *G is unipotent if the fibers of G over each point $s \in S$ are unipotent algebraic groups over $k(s)$.*

b) *G is linearly unipotent* if G is affine and there exist sections $t_1, \ldots, t_n$ of the ring $\mathcal{O}_{S,G}$ such that

$$\mu(t_i) = t_i \otimes 1 + 1 \otimes t_i + \sum_j a_{ij} \otimes b_{ij},$$

where $a_{ij}, b_{ij} \in \mathcal{O}_S[t_1, \ldots, t_{i-1}]$.

Remark. The second definition is extremely close to the definition over a field (0.2.1). It is clear that b) $\Rightarrow$ a). Later on we shall show that for certain affine unipotent S-groups G over integral affine bases these definitions are equivalent. The only apparent difference between a) and b) is that in a) we do not require that G be affine and S integral. Example 6.1 shows that over a ring with nilpotents these definitions are not equivalent. On the other hand, Example 6.2 shows that over integral rings there exist unipotent group schemes that are not affine.

0.8.1. (Raynaud [12], XV, 3). Let S be a scheme of characteristic 0, G a unipotent S-group, and $\mathcal{F} = \mathrm{Lie}\, G$ the $\mathcal{O}_S$-Lie algebra of G. Then the exponential map $\exp: W(\mathcal{F}) \to G$ is an isomorphism of S-schemes. Moreover, if we equip $W(\mathcal{F})$ with a group law described by the Campbell-Hausdorff formula, then exp is a group isomorphism. In particular, if $S = \mathrm{Spec}\, A$, then G is linearly unipotent. Moreover, G is a form of $\mathbf{A}^n_S$ in the Zariski topology (0.10.2).

We recall (SGAD) that for any coherent $\mathcal{O}_S$-Module $\mathcal{F}$, $W(\mathcal{F})$ denotes the S-group scheme representing the functor $T \to \Gamma(T, \mathcal{F} \otimes_{\mathcal{O}_S} \mathcal{O}_T)$. Since S is of characteristic 0, the group scheme G is smooth and has connected fibers. In particular, $\mathcal{F} = \mathrm{Lie}\, G$ is a locally free $\mathcal{O}_S$-Module and $W(\mathcal{F})$ is the vector bundle over S corresponding to $\mathcal{F}$ ((SGAD), II.4.11).

0.8.2. According to Grothendieck ((SGAD), X, 8.7, p. 121) a smooth S-group G of finite type is unipotent if and only if its maximal fibers are unipotent. This indicates that the condition of smoothness is perhaps unnecessary.

0.9. Let S be an integral locally noetherian scheme, η its generic points and X_η a scheme of finite type over η. A flat S-scheme of finite type extending X_η will be called a *model* of X_η. In case X_η is a group scheme over η, a *group model* of X_η is a flat S-group scheme G extending X_η.

0.9.1. Examples. a) Every flat S-scheme (respectively S-group scheme) is a model (a group model) of its generic fiber.

b) If S is the spectrum of a discrete valuation ring A and G_η an extension of an abelian variety by a torus, then by the results of Néron and Raynaud [13] there always exists a group model for G_η.

c) If A is the ring of integers of a local field K, then the parahoric subgroups of a semisimple group over K are its smooth group models [19].

0.10. Let S be a scheme. By a Grothendieck topology on the scheme S we mean an arbitrary topologized full subcategory T of the category Sch/S, whose topology is given by the set $\mathrm{Cov}(T)$ of finite surjective families of morphisms $\{U_i \xrightarrow{\phi_i} S'\}_{i \in I}$, $S' \in \mathrm{Ob}(T)$, called covers of S'. Here the finiteness means that the set of indices I is finite, and the surjectivity that $\bigcup_{i \in I} \phi_i(U_i) = S'$.

0.10.1. In what follows we shall come across the following topologies on a noetherian scheme S:

a) The Zariski topology $T = S_{Zar}$. It is formed by the open subschemes of the scheme S, and $\mathrm{Cov}(S_{Zar})$ consists of the families $\{U_i \xrightarrow{\phi_i} S'\}$, where ϕ_i is an open immersion.

b) The étale topology $T = S_{ét}$. It is formed by étale S-schemes, and $\mathrm{Cov}(S_{ét})$ consists of families $\{U_i \xrightarrow{\phi_i} S'\}$ in which ϕ_i is an étale morphism.

c) The fppf-topology $T = S_{fppf}$. It is formed by flat separated quasifinite S-schemes of finite type, and $\mathrm{Cov}(S_{fppf})$ consists of families of flat morphisms.

Here a morphism is called quasifinite if its fibers are finite ((EGA)).

d) The fpqc-topology $T = S_{fpqc}$. It is formed by flat quasicompact S-schemes. $\mathrm{Cov}(S_{fpqc})$ consists of families of flat morphisms.

e) The radical topology $T = S_{rad}$. It is formed by finite flat radical S-schemes. $\mathrm{Cov}(S_{rad})$ consists of families of flat morphisms.

Here a morphism $f: X \to Y$ of schemes is said to be radical if, for all $y \in Y$, $f^{-1}(y)$ consists of the single point x and the corresponding extension of residue fields $k(x)/k(y)$ is radical (i.e. is purely inseparable) ((EGA), 1.3.5.8).

0.10.2. Let S be a scheme and T a Grothendieck topology on S. We will say that an S-scheme X is an *S-form* of an S-scheme Y relative to T if there exists a covering

$$\{U_i \to S\}_{i \in I} \in \mathrm{Cov}(T),$$

such that for all $i \in I$

$$X \times_S U_i \cong Y \times_S U_i.$$

In particular, one can speak about forms in the Zariski topology, fppf-forms, étale forms, radical forms, etc..

§ 1. Linear unipotence

1.0. This subsection is aimed at introducing the notation that will be used.

Let A be an integral ring, K its field of fractions, X an affine model of the affine space $\mathbf{A}^n_K$ over A, and $A[X] = \Gamma(X, \mathcal{O}_X)$. Let $\phi: A[X] \to K[X]$ be the natural imbedding, $K[X] = K[x_1, \ldots, x_n]$.

1.0.1. If $x_1^{t1} \ldots x_n^{tn}$ is a monomial, we shall sometimes write it in the form x^t, interpreting t as the vector $(t_1, \ldots, t_n)$. Let $t \ll m$ denote component-wise comparison of vectors (i.e. $t_i \leq m_i$ for all i). If $m = (m_i)$, then $T(m) = \{t : t \ll m\}$.

The signs $>$ and $<$ will denote lexicographic comparison of vectors (according to the first different component from the right; in particular, $(1, 0, \ldots, 0)$ is the minimal vector with nonnegative integral coefficients); max is always taken relative to this order.

We shall write $t = \deg x^t$. If $f = \Sigma a_t x^t$, then $\deg f = \max(t : a_t \neq 0)$.

1.0.2. For $f \in A[X]$ we put $\deg f = \deg \phi(f)$. Let

$$P_t = \{f \in A[X] : \deg f \leqslant t\},$$

$$P'_t = \{f \in A[X] : \deg f < t\},$$

$$\overline{P}_t = P_t / P'_t.$$

Then the following lemma is obvious.

Lemma. a) *P_t, P'_t and $\overline{P}_t$ are finitely-generated torsion-free A-modules.*

b) $\dim \overline{P}_t \otimes K = 1$.

1.0.3. For each vector t we denote by $z_{1,t}, \ldots, z_{r(t),t}$ the set of elements of P_t whose images in $\overline{P}_t$ are generators of $\overline{P}_t$. Since X is of finite type, there exists a vector $m(X) = (m_1, \ldots, m_n)$ such that $A[X] = A\{z_{ij}, i = 1, \ldots, r(j), j \in T(m(X))\}$.

1.0.4. **Lemma.** *$\phi \otimes \phi$ is an imbedding of $A[X] \otimes A[X]$ into $K[X] \otimes K[X]$.*

Proof. Consider the exact sequence of A-modules

$$0 \to A[X] \xrightarrow{\varphi} K[X].$$

Since $A[X]$ is a flat A-module, the sequence

$$0 \to A[X] \otimes A[X] \xrightarrow{\varphi \otimes 1} K[X] \otimes A[X]$$

is exact. Now it suffices to note that

$$K[X] \otimes A[X] = K[X] \otimes K[X], \quad \varphi \otimes 1 = \varphi \otimes \varphi.$$

1.0.5. For $f = \Sigma a \otimes b \in K[X] \otimes K[X]$ we set

$$\deg f = \max (\deg a + \deg b).$$

Then, in view of 1.0.4, the following lemma is obvious.

Lemma. *Let* $f = \Sigma a_i \otimes b_i \in A[X] \otimes A[X]$. *Then*

$$\deg (\varphi \otimes \varphi)(f) = \max (\deg a_i + \deg b_i).$$

1.1. **Theorem.** *Let G be an affine group model over A of a unipotent group, where the generic fiber of G is isomorphic to $\mathbf{A}^n_K$. Then G is linearly unipotent.*

1.1.1. **Proof.** We adopt the notation of 1.0 for $X = G$. We number the x_i so that x_i will be primitive $\bmod (x_1, \ldots, x_{i-1})$ (see 4.4 below or [7], Chapter IV, §4, Theorem 4.1). We have $A[G] = A[z_{ij},\ i \in [1, r(j)],\ j \in T(m(G))]$. We number the z_{ij}, $j \in T(m(G))$, in succession and so that $\deg z_i < \deg z_j \Rightarrow i < j$.

1.1.2. **Lemma.** *Let* $y \in A[G]$, $\deg y = t$. *Then*

$$\mu(y) = y \otimes 1 + 1 \otimes y + \sum a_l \otimes b_l,$$

where $a_i, b_i \in A[G]$, $\deg a_i < t$, $\deg b_i < t$ *and* $\deg (\Sigma a_i \otimes b_i) \leq t$.

Proof. Let $y = \Sigma d_i x^i$, $d_i \in K$. Then

$$(\mu \otimes K)(y) = y \otimes 1 + 1 \otimes y + \sum_l d_l \sum_{\substack{j<l,\, h<l \\ j+h<l}} c_{ljh}\, x^j \otimes x^h$$

(because of the choice of the order on the x_i). From a comparison of the formulas for $\mu(y)$ and $(\mu \otimes K)(y)$ it follows that $\Sigma a_i \otimes b_i \in P'_t \otimes P'_t \otimes K$, from which in view of 1.0.4 we get $\Sigma a_i \otimes b_i \in P'_t \otimes P'_t$, and, in view of 1.0.5, $\deg (\Sigma a_i \otimes b_i) \leq t$.

1.1.3. We have $A[G] = A[z_1, \ldots, z_N]$, where $i > j \Rightarrow \deg z_i \geq \deg z_j$. Since

$$\mu(z_l) = z_l \otimes 1 + 1 \otimes z_l + \sum a_{lj} \otimes b_{lj},$$

$$\deg a_{lj} < \deg z_l, \quad \deg b_{lj} < \deg z_l,$$

it follows that

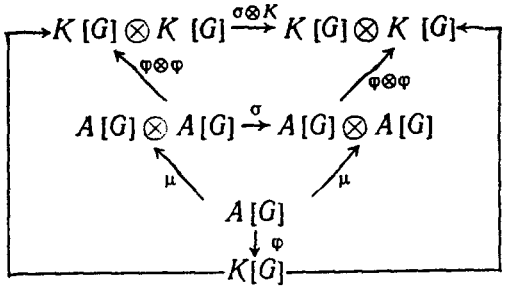
$$a_{ij} = \sum_{m<i} q_{ijm} z_m, \quad b_{ij} = \sum_{m<i} q'_{ijm} z_m, \quad q_{ijm}, q'_{ijm} \in A,$$

from which our assertion also follows.

1.1.4. **Remark.** Applications to the case of a discrete valuation ring are based on the choice of the basis $\{z_i\}$ ("reduced polynomials") and on Lemma 1.1.2.

1.2. **Theorem.** *Let A be an integral ring, and G an affine group model of a commutative group over A. Then G is a commutative group scheme.*

Proof. Let $\sigma: A[G] \otimes A[G] \to A[G] \otimes A[G]$ be the interchange of factors. We have



We know that the outer triangle is commutative as well as all the rectangles on its sides. Since ϕ and $\phi \otimes \phi$ are imbeddings (1.0.4), the inner triangle is commutative.

1.3.1. **Remark.** If 2 is invertible in A, we can symmetrize the formulas for $\mu(y)$. Namely, in view of 1.3,

$$\mu(y) = \sum a_i \otimes b_i = \sum b_i \otimes a_i.$$

Therefore

$$\mu(y) = \sum \frac{1}{2}(a_i \otimes b_i + b_i \otimes a_i).$$

1.3.2. **Corollary.** *Affine group models of commutative unipotent groups are commutative group schemes.*

1.3.3. **Remark.** If the ground ring R has nilpotents, then there exists a group scheme G over R whose generic fiber is commutative, but which is itself not commutative. For example, $R = k[u]/u^2$, k a field, $R[G] = R[x, y, z]$, x, y primitive, and $\mu(z) = z \otimes 1 + 1 \otimes z + uy \otimes x$.

§2. Some technical theorems

2.0. The properties of affine unipotent groups over discrete valuation rings turn out to be rather close to the properties of unipotent groups over fields. To prove the corresponding assertions we need some explicit information about the generators of the ring $A[G]$, which is contained in Theorems 2.3.0, 2.4.0 and 2.5.0 proved below.

2.1. Let A be a discrete valuation ring, π its uniformizing parameter, $k = A/\pi$ the residue field, $p = \operatorname{char} k$, and K the field of fractions of A.

Let X be an affine model of A^n_K over A. We adopt the notation and conventions of 1.0.

2.1.1. Since A is a principal ideal ring, in view of Lemma 1.0.2 we have that $\overline{P}_t$ is a free A-module with a single generator (i.e. $r(t) = 1$ in the notation of 1.0.3). We denote the corresponding element z_{1t} by z_t.

Definition. We set $y_1 = z_{(1,0,\ldots,0)}$, and denote by y_{i+1} the first z_t such that $\deg z_t > \deg y_i$ and $z_t \notin A[y_1, \ldots, y_i]$.

2.1.2. We set

$$\Omega_r = \{j : y_j \in K[x_1, \ldots, x_r]\}, \quad \Omega_0 = \varnothing,$$

$$\overline{\Omega}_r = \Omega_r - \Omega_{r-1}, \quad \Omega_r = [1, t_{r+1} - 1],$$

$$I = \{t_1 = 1, t_2, \ldots, t_n\}, \quad \overline{I} = [1, N] - I, \quad N = t_{n+1} - 1.$$

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

Proposition. a) *If $t \in I$, then*

$$y_t = a_t x_{\omega(t)} + P(y_1, \ldots, y_{t-1}), \quad a_t \in K, \quad a_t \neq 0.$$

b) *If $t \in \overline{I}$, then there exists $d_t \in \mathbb{N}$ such that*

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

Proof. If $t \in I$, then $y_t \in K[x_1, \ldots, x_{\omega(t)}]$, but $y_t \notin K[x_1, \ldots, x_{\omega(t)-1}]$. Therefore $\deg y_t = (i_1, \ldots, i_{\omega(t)}, 0, \ldots, 0)$, $i_{\omega(t)} \neq 0$. Since $\pi^a x_{\omega(t)} \in A[G]$ for sufficiently large a, and since $\deg y_i > \deg y_t$ for $i > t$, and $y_i \in K[x_1, \ldots, x_{\omega(t)-1}]$ for $i < t$, it follows that the images of $\pi^a x_{\omega(t)}$ and y_t in $P_{\deg y_t}$ coincide, i.e. $i_{\omega(t)} = 1$, which proves a).

From a) it follows that $K[x_1, \ldots, x_{\omega(t)}] = K[y_1, \ldots, y_t]$. Therefore for $t \in \overline{I}$ we have $\pi^a y_t \in A[y_1, \ldots, y_{t-1}]$. Choosing a to be minimal with this property, we obtain b).

2.2. In this subsection we introduce some notions and we will prove some assertions that will allow us to establish the main results of this section.

2.2.1. Let $p = \operatorname{char} A/\pi \neq 0$. Let B be an A-algebra with generators u_i, $i \in [1, t]$. We assume that $[1, t] = I \cup \overline{I}$, $1 \in I$, and to each $i \in \overline{I}$ we associate the number $r(i)$. If $P(u_1, \ldots, u_t)$ is a polynomial, then the written form $P = \sum a_i u^i$ will be said to be *reduced* if for $i = (i_1, \ldots, i_t)$ from $a_i \neq 0$ it follows that $i_\alpha < p^{r(\alpha+1)}$ for all $\alpha \in [1, t-1]$ such that $\alpha + 1 \in \overline{I}$.

Furthermore, we require that the algebra B be the quotient algebra of the polynomial algebra $A[u_1, \ldots, u_t]$ modulo the ideal generated by the relations

$$\forall i \in \overline{I} \quad \pi^{d_i} u_i = u_{i-1}^{p^{r(i)}} + \sum_{j < m(i-1, p^{r(i)})} a_{ij} u^j \quad \text{for } a_{ij} \in A \text{ and all } i \in \overline{I},$$

where

$$\sum_{j < m(i-1, p^{r(i)})} a_{ij} u^j$$

is in reduced written form, and $m(s, d) = (0, \ldots, 0, \underset{s}{d}, 0, \ldots, 0)$. We write $P_i(u_1, \ldots, u_{i-1})$ for $u_{i-1}^{p^{r(i)}} + \sum a_{ij} u^j$. We define now Ω_i and $\overline{\Omega}_i$ in the following way:

$$\Omega_i = [1, t_{i+1} - 1],$$

where $|I \cap \Omega_i| = i$, $|I \cap [1, t_{i+1}]| = i + 1$ (by definition $\Omega_{|I|} = [1, t]$ and $\Omega_0 = \varnothing$), and

$$\bar{\Omega}_i = \Omega_i - \Omega_{i-1}.$$

If $i \in [1, t]$, then we put $\omega(i) = r$ for $i \in \bar{\Omega}_r$. Further, we put $m = |I|$.

2.2.2. **Lemma.** *Let $P(u_1, \ldots, u_t) \in B$. Then P has a reduced written form.*

Proof. Let $P(u_1, \ldots, u_t) = \Sigma a_i u^i$ be some written form of the polynomial P. Let $\lambda(i) = \Sigma i_\alpha$. We construct an algorithm $\mathfrak{A}$, which transforms the given written form of polynomials into another. An application of the algorithm $\mathfrak{A}$ to the monomial u^r gives the polynomial $\Sigma d_{rj} u^j$, where

$$\max(\lambda(j) : d_{rj} \neq 0) \leqslant \lambda(r).$$

Moreover, if $\max(\lambda(j) : d_{rj} \neq 0) = \lambda(r)$, then $\mathfrak{A}(u^r) = u^r$; and this happens if and only if u^r is reduced. In view of these remarks the algorithm described below stops after a finite number of steps, and the final result is a reduced polynomial.

We now describe $\mathfrak{A}$. Let $a_r u^r \neq 0$ be a term of highest degree $r = (r_1, \ldots, r_t)$ for which r does not satisfy the condition of being reduced. Let β be the least number for which $\beta + 1 \in \bar{I}$, $\beta + 1 < t$, $r_\beta \geq p^{r(\beta+1)}$. We put

$$\mathfrak{A}\left(\sum a_i u^i\right) = \sum_{i \neq r} a_i u^i + \mathfrak{A}(a_r u^r),$$

$$\mathfrak{A}(a_r u^r) = a_r u_1^{r_1} \ldots u_\beta^{r_\beta} \ldots u_t^{r_t} \cdot u_\beta^{r(\beta)-p^{r(\beta+1)}} (\pi^{d_{\beta+1}} u_{\beta+1} - P_{\beta+1}(u_1, \ldots, u_\beta)).$$

The property of $\mathfrak{A}$ mentioned above is obvious, and the lemma is proved.

2.2.3. We have $\bar{\Omega}_r \cap I = t_r$. We put $v_r = u_{t_r}$, $r \in [1, m]$. For a polynomial $Q(v_1, \ldots, v_m)$ we denote by $\deg Q$ its degree relative to $\{v_i\}$ (cf. 1.0.1).

Lemma. a) *The subring $A[v_1, \ldots, v_m]$ of the ring B is isomorphic to a polynomial ring in m variables.*

b) *Let $P(u_1, \ldots, u_t) \in B$, and let $P = \Sigma a_i u^i$ be reduced written form. Let $\rho = \max(i : a_i \neq 0)$, $\rho = (\rho_1, \ldots, \rho_t)$. Then there exist an $a \in \mathbb{N}$ and a polynomial $Q(v_1, \ldots, v_m)$ such that $\pi^a P = Q$. Here if $\deg Q = (\delta_1, \ldots, \delta_m)$, then*

$$\delta_q = \sum_{\alpha \in \bar{\Omega}_1} \left(\rho_\alpha \prod_{\substack{\beta < \alpha \\ \beta \in \bar{\Omega}_q}} p^{r(\beta)} \right).$$

Proof. a) obviously follows from Definition 2.2.1.

We shall prove b). We put $d = \Sigma_{\alpha \in \bar{I}} d_\alpha$ (cf. 2.2.1). For the written form $\Sigma b_i u^i$, $b_i \in K$, we put

$$\varkappa = \max\left(\sum i_\alpha : b_i \neq 0\right), \quad \sigma = \max(i : b_i \neq 0),$$

$$\tau = \min(q \in \bar{I} : i_\alpha = 0 \quad \forall \alpha \in [q + 1, t] \cap \bar{I}),$$

We now define an algorithm $\mathfrak{B}$ (in some sense a converse to the algorithm $\mathfrak{A}$ of the

proof of Lemma 2.2.2), which acts on the written forms of polynomial of $u_1, \ldots, u_t$. Namely, if $\Sigma b_i u^i$, $b_i \in A$, is some written form, $k = \kappa(\Sigma b_i u^i)$ and $q = r(\Sigma b_i u^i)$, then we put

$$\mathfrak{B}: \sum b_i u^i \to \pi^{d_k} \sum b_i u_1^{i_1} \ldots u_t^{i_t} \to \sum c_i u_1^{i_1} \ldots u_{q-1}^{i_{q-1}} (\pi^d u_q)^{i_q} u_{q+1}^{i_{q+1}} \ldots u_t^{i_t}$$

$$\to \sum c_i u_1^{i_1} \ldots u_{q-1}^{i_{q-1}} (u_{q-1}^{p^{r(q)}} + \sum a_{qj} u^j)^{i_q} u_{q+1}^{i_{q+1}} \ldots u_t^{i_t} .$$

From the choice of k and d it follows that $c_i \in A$. Furthermore, it is obvious that $r(\mathfrak{B}(\Sigma b_i u^i)) < r(\Sigma b_i u^i)$. Therefore $\mathfrak{B}$ stops after $t - |I|$ steps, and the end result will be a polynomial in the u_i, $i \in I$, i.e. in the v_i. It remains to show that this will be a polynomial of the indicated degree. This follows from the fact that

$$\sigma(\mathfrak{B}(u^i)) = (i_1, \ldots, i_{q-r}, i_{q-1} + p^{r(q)} i_q, 0, i_{q+1}, \ldots),$$

and from the following simple fact: if

$$i = (i_1, \ldots, i_t), \quad j = (j_1, \ldots, j_t), \quad i_{q-1} < p^{r(q)},$$

$$j_{q-1} < p^{r(q)}, \quad i > j,$$

then $\sigma(\mathfrak{B}(u^i)) > \sigma(\mathfrak{B}(u^j))$.

In fact it is necessary to show that $i_{q-1} + p^{r(q)} i_q > j_{q-1} + p^{r(q)} j_q$ follows from $(i_{q-1}, i_q) > (j_{q-1}, j_q)$, $i_{q-1} < p^{r(q)}$ and $j_{q-1} < p^{r(q)}$. But if $i_q = j_q$, this is obvious. And if $i_q > j_q$, this follows from the inequalities on i_{q-1} and j_{q-1}.

According to what was said above, a term of maximal degree will always remain a term of maximal degree, from which assertion b) of the lemma follows.

2.2.4. Corollaries. a) *B is a flat A-algebra.*

b) $B \otimes K = K[v_1, \ldots, v_m]$.

c) *The reduced written form is unique.*

d) *Nonproportional reduced monomials have different degree (in the ring $K[v_1, \ldots, v_m]$ and relative to $v_1, \ldots, v_m$).*

Proof. All these assertions are direct consequences of 2.2.3b). For example, here is a proof of a). We must show that B has no A-torsion. Let $P \in B$, and let $\Sigma a_i u^i$ be its reduced written form. If $\pi P = 0$, this means, according to 2.2.3b), that $\sigma(\Sigma a_i u^i) = 0$ (in the notation of the proof of 2.2.3), i.e. $\Sigma a_i u^i = 0$, as was required.

2.2.5. **Remark.** If u^i is a reduced monomial, then each monomial u^j, $i \ll j$, is also reduced.

2.2.6. **Lemma.** *Let $v_i \to v_i' = a v_i + Q_i(v_1, \ldots, v_{i-1})$ be a change of generators in the ring $K[v_1, \ldots, v_m]$. If* deg *and* deg′ *are the degree functions with respect to the first and second systems of generators respectively, then for each polynomial $P \in K[v_1, \ldots, v_m]$ we have* $\deg P = \deg' P$.

The proof is obvious.

2.2.7. Let

$$P \in (B \otimes_A K) \otimes_A (B \otimes_A K),$$

$$P = \sum d_{ij} u^i \otimes u^j, \quad d_{ij} \in K.$$

We will say that this written form is *reduced* if the nonzero monomials $d_{ij}u^i$ and $d_{ij}u^j$ are reduced.

Lemma. *Each polynomial $P \in B \otimes B \otimes K$ possesses a reduced written form, which is then unique.*

This written form will be denoted by $\tilde{\mathfrak{A}}(P)$.

Proof. Let $P = \Sigma b_{ij} u^i \otimes u^j$ be an arbitrary written form. We define an algorithm $\tilde{\mathfrak{A}} = \mathfrak{A} \otimes \mathfrak{A}$ by the formula $\tilde{\mathfrak{A}}(P) = \Sigma b_{ij} \mathfrak{A}(u^i) \otimes \mathfrak{A}(u^j)$, where $\mathfrak{A}$ is the algorithm from the proof of Lemma 2.2.2. As in the proof of Lemma 2.2.2, we obtain $\tilde{\mathfrak{A}}^d(P) = \tilde{\mathfrak{A}}^{d-1}(P)$ for sufficiently large d, and then $\tilde{\mathfrak{A}}^d(P)$ is a reduced written form.

If $P = \Sigma b_{ij} u^i \otimes u^j = \Sigma d_{ij} u^i \otimes u^j$ are two reduced written forms, then

$$0 = \Sigma (b_{ij} - d_{ij}) u^i \otimes u^j.$$

Therefore it suffices to prove that $0 \in B \otimes B \otimes K$ has a unique reduced written form. Let $0 = \Sigma d_{ij} u^i \otimes u^j$, and let

$$t_1 = \max \{i : d_{ij} \neq 0\}, \quad t_2 = \max \{j : d_{t_1 j} \neq 0\}.$$

Then under the inclusion of $B \otimes B \otimes K$ in $K[v_1, \ldots, v_m] \otimes K[v_1, \ldots, v_m]$ the leading term of this expression will be of the form

$$b_{t_1 t_2} v^{\deg u^{t_1}} \otimes v^{\deg u^{t_2}}$$

and is not equal to zero, which contradicts the fact that this is a written form of zero.

2.3. The goal of this subsection is to prove that the generators y_i of the ring $A[G]$, where G is an affine group model of a unipotent group with generic fiber isomorphic to $\mathbf{A}^n_K$, possess the properties indicated in 2.2. We shall use these properties in §§3 and 4.

We apply the notation of §2.1 for $X = G$. In addition we put

$$\eta(x) = \mu(x) - x \otimes 1 - 1 \otimes x, \quad \Phi_a(x) = \frac{1}{p} \sum_{i=1}^{p^a - 1} C_{p_a} x^i \otimes x^{p^a - i}$$

and let $m(i, d)$ denote a vector of arbitrary length whose ith component is equal to d, and the remaining ones to zero. We put $h(i) = \deg y_i$.

2.3.0. Let G be an affine group model of a unipotent group over A whose generic fiber is isomorphic to $\mathbf{A}^n_K$. Let $K[G] = K[x_1, \ldots, x_n]$, where we shall assume ([7], Chapter IV, §4, Theorem 4.1) that x_i is primitive modulo $K[x_1, \ldots, x_{i-1}]$.

Theorem. *Let $p = \operatorname{char} A/\pi \neq 0$. We can choose y_i, $i \in \bar{I}$ (see 2.1), so that*

$$\pi^{d_i} y_i = y_{i-1}^{p^{r(i)}} + \tilde{P}_i(y_1, \ldots, y_{i-1}),$$

where a) $\deg \tilde{P}_i(y_1, \ldots, y_{i-1}) < p^{r(i)} \deg y_{i-1}$, *and* b) $\pi^{d_i} | p$.

2.3.0.1. Remarks. a) The theorem can also be proved when char $A/\pi = 0$. However, in this case, instead of assertion b) of the theorem, we have the condition $\pi^{d_i} | p$ for some prime p, from which it follows that $\bar{I} = \varnothing$ (cf. 0.8.1).

b) If char $K = p$, then assertion b) of the theorem is void, since $p = 0$ in K. This gives us the possibility of proving more precise assertions in characteristic p (cf. 2.4, 2.5).

2.3.0.2. The proof of this theorem can be considered as a detailed carrying out of the proof of the theorem on linear unipotence. We use in an essential way the possibility of canonically choosing a basis in $A[G]$. The apparatus that gives this canonical choice is the reduced polynomials of 2.2.

2.3.1. Before we proceed to the proof, we introduce some notation and definitions.

2.3.1.1. We shall say that y_i, $i \leq t$, are *properly chosen generators* if they satisfy the conclusion of the theorem.

It is clear that the considerations of § 2.2 are applicable to the subalgebra B of $A[G]$ generated by the y_i, $i \leq t$. In particular, one can define "reducedness", and assertions 2.2.2–2.2.7 hold.

2.3.1.2. **Lemma.** *Let* $y_1, \ldots, y_t$ *be properly chosen generators, and let* $t+1 \in \bar{I}$ *and* $\pi^{d_{t+1}} y_{t+1} = \Sigma a_i y^i$, $a_i \in A$, *where* $\Sigma a_i y^i$ *is a reduced written form.*

a) *If* $a_m y^m$, $a_m \neq 0$, *is the highest degree term in this written form, then we may assume that* $a_m = 1$.

b) *If* $a_i \in \pi^{d_{t+1}} A$, *then we may assume that* $a_i = 0$.

Proof. Assume that $a_m = \pi b$, $b \in A$. Then

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

and $\deg z < \deg y_{t+1}$. Hence

$$\pi^{d_{t+1}} y_{t+1} = \pi b y^m + \pi z.$$

But, in view of the flatness of $A[G]$, this contradicts the condition on the choice of d_{t+1} (cf. 2.1.3). Therefore $a_m \in A^*$.

We put $y'_{t+1} = a_m^{-1} y_{t+1}$. It is easy to see that y'_{t+1} satisfies an analogous equation with $a_m = 1$.

Now if $a_i \in \pi^{d_{t+1}} b$, $b \in A$, then we put $y'_{t+1} = y_{t+1} - b y^i$. Then $y'_{t+1} \in A[G]$ and $\pi^{d_{t+1}} y_{t+1} = \Sigma a_\alpha y^\alpha - a_i y^i$, as was required.

2.3.1.3. **Lemma.** *Let* $y_1, \ldots, y_t$ *be a properly chosen system of generators. Let* $t+1 \in I$, *and let*

$$y_{t+1} = \chi_{t+1} x_{\omega(t+1)} + \sum a_i y^i, \qquad a_i,\ \chi_{t+1} \in K,$$

be a reduced written form. If $a_i \in A$, *then we may assume that* $a_i = 0$.

Proof. Let $a_i \in A$. Putting $y'_{t+1} = y_{t+1} - a_i y^i$ we get our assertion.

2.3.2. Let $M = A[G] \otimes A[G]$ and $r = (r_1, \ldots, r_n)$. We denote by M_r the subspace of $M \otimes K$ generated by elements $a \otimes b$ for which $\deg a + \deg b < r$. The function $\deg a \otimes b = \deg a + \deg b$ will be called the global degree.

2.3.2.1. We recall that, according to 1.1.2, for all $y \in A[G]$ we have

$$\eta(y) = \sum a_j \otimes b_j, \quad a_j,\ b_j \in A[G],$$

$$\deg a_j < \deg y, \quad \deg b_j < \deg y, \quad \deg a_j \otimes b_j \leqslant \deg y.$$

We must make this assertion more precise.

2.3.2.2. Let $y = \Sigma a_i y^i$, $a_i \in K$, be a reduced written form. Let $\Lambda = \{j : a_j \neq 0\}$. We number the elements of Λ in increasing order, and write

$$\sum a_i y^i = \sum b_\alpha y^{\lambda_\alpha}, \qquad b_\alpha \in K, \quad \lambda_\alpha \in \Lambda.$$

Let

$$z = \sum_{\alpha \geqslant q} b_\alpha y^{\lambda_\alpha}, \quad \eta(z) = \sum b_{ij} y^i \otimes y_j$$

be reduced written form.

Lemma. *Let* $r = \deg y^{\lambda_{q-1}}$, *and assume that* $b_{ij} \in A$ *if* $\deg y^i \otimes y^j > r$. *For* $\eta(y) \in M$ *it is necessary that*

$$\eta(b_{q-1} y^{\lambda_{q-1}}) + \sum_{\deg y^i \otimes y^j = r} b_{ij} y^i \otimes y^j \in M + \tilde{M}_r.$$

Proof. Reduced monomials form a basis of $A[G]$. The reduced written form for $\eta(y)$ is precisely the expression of $\eta(y)$ by basis elements, which was used in 1.1 to prove linear unipotence. The terms $b_\alpha y^{\lambda_\alpha}$, $\alpha < q - 1$, have smaller degree than $b_{q-1} y^{\lambda_{q-1}}$ (see 2.2.3, 2.2.6). Therefore

$$\eta\left(\sum_{\alpha < q-1} b_\alpha y^{\lambda_\alpha}\right) \in \tilde{M}_r.$$

From this our assertion follows.

2.3.2.3. The preceding assertion is used in the following form.

Corollary. *We adopt the conditions of* 2.3.2.2. *If* $\deg y^i \otimes y^j = m(t_{ij}, p^{a_{ij}})$ *for* $b_{ij} y^i \otimes y^j \notin M + \tilde{M}_r$, *then either* $\lambda_{q-1} = m(t, p^a)$, *or* $\eta(b_{q-1} y^{\lambda_{q-1}}) \in M + \tilde{M}_r$.

Proof. We assume that $\eta(b_{q-1} y^{\lambda_{q-1}}) \in M + \tilde{M}_r$. Then 2.3.2.2 yields $r = m(t, p^a)$. The assertion now follows from 2.2.3 and 2.2.6.

2.3.3. We recall some properties of binomial coefficients and the expressions $\Phi_a(x)$.

2.3.3.1. Let $d = p^a \cdot b$. Then $p^{a-\alpha} | C_d^\beta$ if $p^{\alpha+1} \nmid \beta$.

2.3.3.2. $C_{p^a d}^{p^a} \equiv C_d^a \bmod p$.

2.3.3.3. $\mathrm{GCD}_{\alpha \in [1, d-1]} C_d^\alpha = 1$ if $d \neq p^a$, p prime; and $\mathrm{GCD}_{\alpha \in [1, d-1]} C_d^\alpha = p$ if $d = p^a$, p prime.

2.3.3.4. $\Phi_a(x) \in \mathbf{Z}[x] \otimes \mathbf{Z}[x]$, and $\Phi_a(x^{p^b}) \equiv \Phi_{a+b}(x) \bmod p\, \mathbf{Z}[x] \otimes \mathbf{Z}[x]$.

2.3.4. Now suppose that $y_1, \ldots, y_t$ are properly chosen generators.

2.3.4.1. If $i \in I$, then

$$\eta(y_i) \equiv 0 \bmod \tilde{M}_{h(i)},$$

$$\eta(y_i^{p^a b}) \equiv \sum_{\alpha=1}^{b-1} C_b^\alpha y_i^{p^a \alpha} \otimes y_i^{p^a (d-\alpha)} \bmod pM + \tilde{M}_{h(i)}$$

for $a \geq 1$, and $\eta(y_i^{p^a}) \equiv p\Phi_1(y_i^{p^{a-1}}) \bmod p^2 M + \tilde{M}_{h(i)}$.

2.3.4.2. Lemma. *Let $i \in \bar{I}$, $m = p^a b$, $b > 1$, $p \nmid b$, $\gamma = m(i, p^a)$, $\delta = m(i, m - p^a)$, and*

$$\eta(y_i^m) = \sum b_{mi\alpha\beta} y^\alpha \otimes y^\beta,$$

where $y^\alpha \otimes y^\beta$ are reduced monomials for $b_{mi\alpha\beta} \neq 0$. Then

$$b_{mi\gamma\delta} \equiv C_{p^a}^m \bmod \pi.$$

Proof. Let

$$\eta(y_i) = \sum b_{i\alpha\beta} y^\alpha \otimes y^\beta \bmod \tilde{M}_{h(i)},$$

where $\deg b_{i\alpha\beta} y^\alpha \otimes y^\beta = h(i)$, $\deg b_{i\alpha\beta} y^\alpha < h(i)$, and $\deg b_{i\alpha\beta} y^\beta < h(i)$ for $b_{i\alpha\beta} \neq 0$. Then

$$\eta(y_i^m) \equiv (y_i \otimes 1 + 1 \otimes y_i + \sum b_{i\alpha\beta} y^\alpha \otimes y^\beta)^m -$$

$$- y_i^m \otimes 1 - 1 \otimes y_i^m \equiv \sum_{\alpha=1}^{m-1} C_m^\alpha y_i^{m-\alpha} \otimes y_i^\alpha + \sum d_{\alpha\beta} y^\alpha \otimes y^\beta \bmod \tilde{M}_{mh(i)}.$$

We note that either y^α or y^β contains y_j, $j < i$, for $\deg d_{\alpha\beta} y^\alpha \otimes y^\beta = mh(i)$ and $\alpha, \beta \neq m(i, d)$. If after putting such a monomial in reduced form we have a term of the form $y_i^\alpha \otimes y_i^\beta$, $\alpha + \beta = m$, then this will be the term of highest degree and thus its coefficient will be a multiple of π, from which our assertion follows.

2.3.4.3. Lemma. *Let $i \in I$ and $m = p^{a+1}$, $a \geq 0$. Let γ, δ and $b_{mi\gamma\delta}$ be as in* 2.3.4.2. *Then $b_{mi\gamma\delta} \equiv C_m^{p^a} \bmod \pi p$.*

Proof. For $\eta(y_i^m)$ we write the same expressions as in the proof of 2.3.4.2. The same method as in the proof of 2.3.4.2 establishes that the terms $d_{\alpha\beta} y^\alpha \otimes y^\beta$, which after reduction give the term $y^\gamma \otimes y^\delta$ with a coefficient that does not lie in πp, are contained in the sum

$$C_p^1 y_i^{p^a} \otimes y_i^{p^a(p-1)} + \sum (b_{i\alpha\beta} y^\alpha \otimes y^\beta)^m$$

(since the remaining terms contain the coefficient p and after reduction they again give π).

Assume that $b^m_{i\alpha\beta} y^{m\alpha} \otimes y^{m\beta}$ after reduction gives $d y_i^{p^a} \otimes y_i^{p^a(p-1)}$. Then for a suitable b we must have

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

Consequently

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

and, in view of 2.2.3, $y^\alpha = y_j^{p^r}$ and $p \cdot \deg y^\alpha = \deg y_i$. But then, since the written form for $\eta(y_i)$ is reduced, from the proof of 2.3.4.2 we will find

$$y^{p\alpha} = d' y_i + Q(\ldots), \quad \deg Q < \deg y_i.$$

From this it follows that $y^\alpha = y_{i-1}^{p^{r(i)-1}}$, and hence

$$y^\beta = y_{i-1}^{p^{r(i)-1}(p-1)}.$$

We assume that the coefficient of such a term lies in $\pi^{-d_i} pA$. Then

$$(b_{i\alpha\beta} y^\alpha \otimes y^\beta)^p \in (\pi^{-d_i} p)^p (\pi^{d_i})^p M + \tilde{M}_{ph(i)},$$

from which our assertion follows.

The proof that $b_{i\alpha\beta} \in \pi^{-d_i} pA$ is carried out by induction. Let $\omega(i) = r$, $i = t_r + j$. If $j = 0$, our assertion is contained in 2.3.4.1. We assume that it is true for $j - 1$ and prove it for j. We have

$$\eta(y_{i-1}) = \pi^{-d_{i-1}} p \tilde{d} \Phi_1 (y_{i-2}^{p^{r(i-1)-1}}) + \ldots, \quad \tilde{d} \in A,$$

$$\eta(y_i) = \pi^{-d_i} (y_i \otimes 1 + 1 \otimes y_i + \pi^{-d_{i-1}} p \tilde{d} \Phi_1 (y_{i-2}^{p^{r(i-1)-1}}) + \ldots)^{p^{r(i)}}$$
$$- \pi^{-d_i} y_i^{p^{r(i)}} - \pi^{-d_i} 1 \otimes y_i^{p^{r(i)}}.$$

Terms of the form $y_i^\alpha \otimes y_i^\beta$ of degree $\deg y_i$ are obtained by different methods, but by virtue of the induction hypothesis and in view of the fact that enough factors of π show up under reduction, we get our assertion.

2.3.5. We proceed to the proof of the theorem. We use induction on i. Assume we have proved that $y_1, \ldots, y_t$ are properly chosen. We shall show that y_{t+1} can be chosen properly. If $t + 1 \in I$, there is nothing to prove (cf. 2.3.1.3). So assume $t + 1 \in \bar{I}$.

2.3.5.1. Let $\pi^{d_{t+1}} y_{t+1} = \Sigma a_i y_i$ be reduced written form, $a_i \in A$. Let $m = \max(i : a_i \neq 0)$. By 2.3.1.2, $a_m = 1$. By 2.3.2.2,

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

We shall show that $m = m(t, p^a)$ and $\pi^{d_t+1} | p$ follow from this.

2.3.5.2. We note that if $m = (m_1, \ldots, m_t, 0, \ldots, 0)$, then $m_t \neq 0$.

In fact, if $m_t = 0$, then, by the reducedness (see 2.2), we will have $\deg y_{t+1} < \deg y_t$, which contradicts the fact that y_{t+1} has been properly chosen.

2.3.5.3. Assume that $m_i \neq 0$ for $i < t$. Then $\eta(y_{t+1})$ contains the term

$$\pi^{-d_{t+1}} y_t^{m_t} \otimes y^{m-m(t,m_t)},$$

which, by 2.3.4, is the unique reduced term of such a form in $\eta(y_{t+1})$ that does not lie in pM. From this it follows that this case is impossible, i.e. $m_i = 0$ for all $i \neq t$.

2.3.5.4. Now let $m_i = 0$, $i \neq t$, $m_t = d$, $d = p^a b$, $p \nmid b$ and $b \neq 1$. By 2.3.4.2 it follows from this that $\pi^{d_t+1} | C_b^\alpha$, $\alpha = 1, \ldots, b-1$. However, this is not possible for $d_{t+1} \geq 1$.

2.3.5.5. Thus $m_t = p^a$, and $m_i = 0$ for all $i \neq t$. By 2.3.4.3 we must then have $\pi^{d_t+1} | C_p^\alpha$ for all $\alpha \in [1, p-1]$. From this it follows that $\pi^{d_t+1} | p$, which, together with the proof of 3.1, which again allows us to use 2.2, completes the induction step.

2.4. Now suppose $\operatorname{char} K = p$. Let $K[G] = K[x_1, \ldots, x_n]$. Assume that $[1, n] = \bigcup_{\alpha=1} J_\alpha$, $J_\alpha \cap J_\beta = \varnothing$ for $\alpha \neq \beta$, and we have that $i > j$ for $\alpha > \beta$ for all $i \in J_\alpha$ and all $j \in J_\beta$. Assume further that for $i \in J_\alpha$ we have

$$\eta(x_i) \equiv 0 \bmod K[x_j, j \in \bigcup_{\beta<\alpha} J_\beta] \otimes K[x_j, j \in \bigcup_{\alpha<\beta} J_\beta].$$

Such a partitioning corresponds to the normal series whose quotients are isomorphic to $G_{a,K}^{|J_\alpha|}$.

We put

$$\widetilde{\Omega}_\alpha = \bigcup_{i \in J_\alpha} \overline{\Omega}_i, \quad \Omega'_\alpha = \Omega_i - \widetilde{\Omega}_\alpha, \quad i \in J_\alpha.$$

If $i \in \widetilde{\Omega}_\alpha$, we put $\widetilde{\omega}(i) = \alpha$.

2.4.0. **Theorem.** *Let* $\operatorname{char} K = p > 0$. *We can choose* y_i, $i \in [1, N]$ (*cf.* 2.1), *so that for* $i \in \overline{I}$ *we have*

$$\pi^{d_i} y_i = \sum_{\substack{j \in \widetilde{\Omega}_{\omega(i)} \\ j<i}} \sum_\alpha a_{ij\alpha} y_j^{p^\alpha} + \widetilde{P}_i(y_j, j_i \in \Omega_{\widetilde{\omega}(i)}), \quad a_{ij\alpha} \in A,$$

and for $i \in I$ *we have*

$$y_i = \chi_i x_{\omega(i)} + \sum_{\substack{j \in \widetilde{\Omega}_{\omega(i)} \\ j<i}} \sum_\alpha a_{ij\alpha} y_j^{p^\alpha} + \widetilde{P}_i(y_j, j \in \Omega'_{\widetilde{\omega}(i)}), \quad \chi_i, a_{ij\alpha} \in K.$$

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

a) $a_{i,i-1,r(i)} = 1$ *for* $i \in \bar{I}$, *and*

b) $a_{ij\alpha} = 0$ *if* $j+1 \in \bar{I}$ *and* $\alpha \geq r(j+1)$.

2.4.0.1. **Remark.** Assertion a) is contained in 2.3.0. Assertion b) means simply that we consider things in reduced written form.

2.4.0.2. The proof of Theorem 2.4.0 is in essence that of Theorem 2.3.0 using the property $p = 0$.

2.4.1. We will now say that $y_1, \ldots, y_t$ are *chosen properly* if they satisfy the conclusion of Theorem 2.4.0. It is clear that all the properties of proper generators that were considered in 2.3 are also preserved in the present situation.

2.4.2. Now let $y_1, \ldots, y_t$ be properly chosen generators. We assume everywhere below that $d_i = 0$ for $i \in I$. Put

$$R_t = M + K[y_j,\ j \in \Omega'_{\omega(t)}] \otimes K[y_j,\ j \in \Omega'_{\omega(t)}].$$

2.4.2.1. For all $i \in [1, t]$

$$\eta(y_t) \equiv 0 \mod R_t,$$

$$\eta(y_i^{p^{a_b}}) \equiv \sum_{\alpha=1}^{b-1} C_b^a y_i^{p^{a_\alpha}} \otimes y_i^{p^{a(b-\alpha)}} \mod R_t.$$

In particular, $\eta(y_i^{p^{a}}) \equiv 0 \mod R_t$.

2.4.3. **Proof of the theorem.** Induction on i. We assume we have shown that $y_1, \ldots, y_t$ are chosen properly. We shall show that we can choose y_{t+1} properly.

2.4.4.1. Let

$$y_{t+1} = \chi_{t+1}\lambda_{\omega(t+1)} + \sum a_i y^i,$$

where $\chi_{t+1} = 0$ if $i \in \bar{I}$, $\Sigma a_i y^i$ is reduced written form, $a_i \in K$ and

$$\deg \Sigma a_i y^i < \deg x_{\omega(t+1)}$$

for $i \in I$. We apply the notation of 2.3.3.2 to $y = \Sigma a_i y^i$. In particular, $\Lambda = \{i;\ a_i \neq 0\}$; having enumerated the elements of Λ in increasing order, we have

$$y = \sum_{\alpha=0}^{|\Lambda|-1} b_\alpha y^{\lambda_\alpha}.$$

If $\lambda_\alpha = m(i, d)$, we put $\rho(\alpha) = i$.

2.4.4.2. **Secondary descending induction on the elements of Λ.** Assume that for $\alpha \geq q$ we have shown that $\lambda_\alpha = m(\rho(\alpha), p^{\nu\alpha})$. Put

$$z = \sum_{\alpha \geq q} b_\alpha y_{\rho(\alpha)}^{p^{\nu_\alpha}}.$$

By 2.4.3.1 we have $\eta(z) \equiv 0 \mod R_{t+1}$.

2.4.4.3. Put $\lambda_{p-1} = m = (m_1, \ldots, m_N)$ and $y^m \notin K[y_i,\ i \in \Omega'_{\omega(t+1)-1}]$. We shall show that if $m \neq m(i, p^d)$, then $b_{q-1} \in A$, and then we apply 2.4.1.1 or 2.3.1.2. By

2.4.2.1 and the property $\eta(z) \equiv 0 \bmod R_{t+1}$ we have

$$\eta(b_{q-1}y^m) \equiv 0 \mod (R_{t+1} + M + \tilde{M}_{\deg y^m}).$$

However, in view of 2.3.2.3 for $m \neq m(i, p^d)$ it follows from this that $b_{q-1} \in A$, as was required (for $m = m(i, p^d)$ we obtain the condition $0 \cdot b_{q-1} \in A$, which cannot occur). This proves the theorem.

2.5. **Corollary.** *Under the assumptions of Theorem 2.4.0, if the generic fiber of G is $G^n_{a,K}$, then y_i, $i \in [1, N]$, can be chosen as in Theorem 2.4.0, where $\tilde{P}_i = 0$ for all $i \in [1, N]$ (since $J_1 = [1, N]$ in this case).*

2.6. **Corollary.** *Under the hypothesis of Corollary 2.5 there exists an exact sequence of groups over A:*

$$1 \to G \to G^N_{a,A} \to G^{N-n}_{a,A} \to 1.$$

Proof. We put $F_i = \pi^{d_i} Y_i - P_i(Y_1, \ldots, Y_{i-1})$, $i \in \bar{I}$. Since the P_i are p-polynomials, the mapping ψ: $A[X_i, i \in \bar{I}] \to A[Y_1, \ldots, Y_N]$, given by the formula

$$\psi(X_i) = F_i(Y_1, \ldots, Y_N),$$

defines a homomorphism $G^N_{a,A} \to G^{|\bar{I}|}_{a,A}$ (if we assume X_i and Y_i to be primitive), whose kernel is the coordinate ring of the group G. It is obviously an epimorphism.

2.7. **Remark.** Apparently, the proof of Theorem 2.4.0 can be extended to the case when the J_α are chosen so that

$$\eta(x_i) \equiv \sum_{j<i} \sum_m a_{ijm} \Phi_m(x_j) \bmod K[x_j, j \in \bigcup_{\beta<\alpha} J_\beta] \otimes K[x_j, j \in \bigcup_{\beta<\alpha} J_\beta].$$

(This corresponds to a series whose factors are commutative.) For this it would be necessary to change the order of the vectors $\deg y^t$, to prove an analogue of 1.1.2 for this new order and to adapt 2.2 to the new situation.

Such a generalization of 2.4 would allow us to prove Theorem 3.5 in the following guise for arbitrary commutative groups: smooth models of unipotent groups with connected fibers over a discrete valuation ring with field of fractions of characteristic p are forms of A^n_S in the radical topology.

§3. The geometry of unipotent groups

3.0.0. In this section A denotes a discrete valuation ring, K its field of fractions, π the uniformizing parameter of A, $k = A/\pi$ the residue field, and p the characteristic of k.

3.0.1. In this section we shall prove that affine unipotent groups over A, since they are models of A^n_K, are complete intersections in A^N_A. Moreover, if the equations defining such a group G are written as p-polynomials (see 3.3.0) (we then say that G is a p-polynomial group), and if the fibers of G are smooth and connected, then $G_{A'} = G_A \otimes_A A' \cong A^n_{A'}$ for some quasi-radical extension $A' \supset A$ (see 3.3.2).

In particular, if $A \supset F_p$, then each smooth commutative group G with $G_K \cong G^n_a$ with connected fibers is p-polynomial, and by the same token we can apply the assertion given above to such a G.

3.0.2. The question of whether every affine unipotent group model of $\mathbf{A}^n_K$ is p-polynomial remains open.

3.0.3. We observe that the assumption that our unipotent A-group scheme is affine is not very restrictive. According to the result announced by Raynaud (cf. [12], IX, 2.2), every flat separable A-group scheme of finite type with affine generic fiber is affine. The condition of separatedness holds for any flat group scheme of finite type with connected fibers ((SGAD), VI_B, 5.5).

We observe that, without using the result of Raynaud mentioned above, we can find that unipotent quasi-affine A-group schemes are affine, if we use [12], VII, 3.1.3.2. In particular, this is true if G is smooth with connected fibers (since in this case G is quasi-affine (see [12], VII, 2.1)).

3.1. **Theorem.** *Let G be an affine unipotent group that is a model of $\mathbf{A}^n_K$ over A. Let $y_1, \ldots, y_N$ be generators of the algebra $A[G]$, constructed according to 2.1, and set*

$$\pi^{di} y_i = P_i(y_1, \ldots, y_{i-1}), \quad i \in \bar{I},$$

where P_i is a polynomial of the form indicated in Theorem 2.3.0. Then the relations indicated above are the only relations in $A[G]$.

Proof. We have shown in 2.2.4 that the algebra B constructed by the generators and relations indicated in the theorem is flat. Let $\psi: B \to A[G]$ be the projection of B onto $A[G]$. We have a commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{\psi} & A[G] \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ K[u_i, i \in I] & \to & K[y_i, i \in I] = K[x_1, \ldots, x_n]. \end{array}$$

Since the bottom arrow is an isomorphism, and the vertical arrows are inclusions, it follows that ψ is an isomorphism, which proves the assertion of the theorem.

3.2. **Corollary.** *Let G be an affine unipotent group over A, which is a model of $\mathbf{A}^n_K$. Then G is a complete intersection in $\mathbf{A}^n_A$.*

Proof. We retain the notation of Theorem 3.1. Let $\bar{I} = \{i_1, \ldots, i_r\}$, where $r = N - n$ (cf. 2.1.2) and $i_1 < \cdots < i_r$. Put

$$F_m = \pi^{d_{i_m}} Y_{i_m} - P_{i_m}(Y_1, \ldots, Y_{i_m - 1}).$$

By Theorem 3.1 the scheme G is given by the ideal $I = (F_1, \ldots, F_r)$ in $\mathbf{A}^N_A = \operatorname{Spec} A[Y_1, \ldots, Y_N]$. We must show that the sequence $F_1, \ldots, F_r$ is regular, i.e., setting $B_m = A[Y_1, \ldots, Y_N]/(F_1, \ldots, F_{m-1})$, we must show that F_m is not a zero divisor in B_m. By 3.1.1 the algebra B_i is flat. Therefore B_m is included in $B_m \otimes K$. We have

$$B_m \otimes K = K[Y_j, j \in (I \cap [1, i_m - 1]) \cap [i_m, N]].$$

Let J be an ideal in $B_m \otimes K$ generated by Y_j, $j \in I \cap [1, i_m - 1]$. If F_m is a zero divisor in B_m, then F_m is a zero divisor in $B_m \otimes K$, and hence F_m is a zero divisor in $B_m \otimes K/J$. However, $B_m \otimes K/J = K[Y_j, j \in [i_m, N]]$, and the image of F_m in $B_m \otimes K/J$ is $\pi^{d_{i_m}} Y_{i_m}$. Since Y_{i_m} is not a zero divisor in $K[Y_j, j \in [i_m, N]]$, our assertion is proved.

3.3. We will say that an affine scheme G over A is *p-polynomial* if $A[G] = A[y_1, \ldots, y_N]$, $[1, N] = I \cup \bar{I}$, $I \cap \bar{I} = \emptyset$ and G is given in $\mathbf{A}^N_A$ by the equation

$$\pi^{d_i} y_i = \sum_{j<i} \sum_{\alpha} a_{ij\alpha} y_j^{p^\alpha}, \quad a_{ij\alpha} \in A, \quad \pi^{d_i} \mid p,$$

$$a_{i\,i-1\,r(i)} = 1, \; r(i) = \max(\alpha : a_{i\,i-1\,\alpha} \neq 0) \quad \text{for } i \in I.$$

It is obvious that a p-polynomial A-scheme G is a model of $\mathbf{A}^n_K$.

The goal of this subsection is a proof of the following result.

Theorem. *Let G be a smooth p-polynomial scheme over A with connected fibers of dimension n. Then there exists an unramified extension $A' \supset A$ such that the corresponding extension of residue fields is radical and $G_{A'} = G_A \otimes_A A' \cong \mathbf{A}^n_{A'}$.*

3.3.0. **Definition.** A polynomial of the form

$$P(X_1, \ldots, X_n) = \sum_{i,j} a_{ij} X_i^{p^j} \in A[X_1, \ldots, X_n]$$

is called a *p-polynomial.*

A mapping $f: A[X_1, \ldots, X_n] \to A[T_1, \ldots, T_n]$ is called a *p-polynomial homomorphism* if $f(X_i) = R_i(T_1, \ldots, T_n)$ is a p-polynomial for all $i \in [1, n]$.

If, moreover, f is an isomorphism and f^{-1} is a p-polynomial homomorphism, then f is called a *p-polynomial isomorphism.*

3.3.1. **Lemma.** *If $f: A[X_1, \ldots, X_n] \to A[T_1, \ldots, T_n]$ is a p-polynomial homomorphism, then for any p-polynomial $P(X_1, \ldots, X_n)$*

$$f(P) - P' \in pA[T_1, \ldots, T_n],$$

where $P' = P'(T_1, \ldots, T_n)$ is a p-polynomial.

3.3.2. **Definition.** A discrete valuation ring A' containing A, with uniformizing parameter π' and residue field $k' = A'/\pi'$, is called a *quasi-radical extension* of A if $\pi A' = \pi' A'$ and k'/k is a radical field extension.

We note that if $A \supset \mathbf{F}_p$, then the morphism $\operatorname{Spec} A' \to \operatorname{Spec} A$ is radical in the sense of 0.10.1e).

3.3.3. **Lemma.** *For any invertible element $a \in A$ and any $n > 0$ there exists a quasi-radical extension $A' \supset A$ containing an element $a' \in A'$ such that $a'^{p^n} - a \in \pi A'$.*

Proof. Let $\bar{a}$ be the image of a under the natural homomorphism $A \to k$. We choose a radical extension $k' = k(\sqrt[p^n]{\bar{a}})$ and some finite quasi-radical extension $A' \supset A$ with residue field k' (this can be done because of (EGA), 0_{III}, 10.3.2). Let $a' \in A$ be

mapped into $\sqrt[p^n]{\bar{a}}$ under the natural homomorphism $\phi\colon A' \to A'/\pi = k'$. Obviously

$$\varphi(a'^{p^n}) - \varphi(a) = \varphi(a'^{p^n} - a) = 0$$

and by the same token $a'^{p^n} - a \in \pi A'$, as required.

3.3.4. **Lemma.** *Let $P \in A[X_1, \ldots, X_n]$ be a p-polynomial that is irreducible modulo π and has invertible nonzero coefficients. There exist a quasi-radical extension $A' \supset A$ and a p-polynomial isomorphism $f\colon A'[X_1, \ldots, X_n] \to A'[T_1, \ldots, T_n]$ such that $f(P) - T_1 \in pA'(T_1, \ldots, T_n)$.*

Proof. Let

$$P = \sum_{j=1}^{n} \sum_{i=0}^{m_j} a_{ji} X_j^{p^i}.$$

We apply induction on the maximum of the m_j with $a_{jm_j} \not\equiv 0$. Without loss of generality we may assume that $m_1 = \max(m_j\colon a_{jm_j} \not\equiv 0)$. Assume that $m_1 = 0$. Then, setting

$$R_i(T_1, \ldots, T_n) = T_i, \quad i = 2, \ldots, n,$$

$$R_1(T_1, \ldots, T_n) = a_{10}^{-1}\left(T_1 - \sum_{j=2}^{n} a_{j0} T_j\right),$$

we find that $P(R_1, \ldots, R_n) = T_1$. The homomorphism $X_i \to R_i(T_1, \ldots, T_n)$ obviously defines a p-polynomial isomorphism $A[X_1, \ldots, X_n] \to A[T_1, \ldots, T_n]$. Now let $m_1 > 0$. If all the $a_{jm_j} = 0$ for $j > 2$, then the polynomial $P(X_1, \ldots, X_n) = \sum_{i=0}^{m_1} a_{1i} X_1^{p^i}$ is not irreducible mod π. Thus we may assume that, say, $a_{2m_2} \not\equiv 0$. By assumption $m_1 \geq m_2$.

By 3.3.3 there exists a quasi-radical extension $A' \supset A$ containing the elements $b_i = (a_{1i}/a_{2m_2})^{p^{-m_2}}$, $i = m_2, \ldots, m_1$. Put

$$R_1 = T_1,$$

$$R_i = T_i, \quad i \geqslant 3,$$

$$R_2 = T_2 - b_{m_2} T_1 - \ldots - b_{m_1} T_1^{p^{m_1 - m_2}}.$$

The homomorphism $f\colon X_i \to R_i(T_1, \ldots, T_n)$ obviously defines a p-polynomial isomorphism $A'[X_1, \ldots, X_n] \to A'[T_1, \ldots, T_n]$. We have

$$a_{2m_2} X_2^{p^{m_2}} + a_{1m_2} X_1^{p^{m_2}} + \ldots + a_{1m_1} X_1^{p^{m_1}}$$

$$= a_{2m_2}(X_2 + b_{m_2} X_1 + \ldots + b_{m_1} X_1^{p^{m_1 - m_2}})^{p^{m_2}} + pF(X_1, X_2)$$

and thus

$$P' = P(R_1, \ldots, R_n) = \sum_{i=0}^{m_1 - 1} a'_{1i} T_1^{p^i} + \sum_{i=0}^{m_2} a_{2i} T_2^{p^i} +$$

$$+\sum_{j=3}^{n}\sum_{i=0}^{m_j} a_{ji}T_j^{pi} + pF'(T_1, T_2).$$

Since f is an isomorphism, the polynomial $P'(T_1, \ldots, T_n)$ is irreducible. If $m_1 > m_2$, we lower $\max(m_1, \ldots, m_n)$ and we can use the induction hypothesis. But if $m_1 = m_2$, then we must apply the preceding argument, interchanging T_1 and T_2, and again lower m_2. The proof is complete.

3.3.5. **Lemma.** *Let* $F = \pi^d X_{n+1} - P(X_1, \ldots, X_n) \in A[X_1, \ldots, X_{n+1}]$, *and let* P *have the form* $P = P_0 + \pi P_1 + \ldots + \pi^d P_d$, *where* $P_i \in A[X_1, \ldots, X_n]$, $i = 0, \ldots, d$. *Put*

$$F_i' = \pi Y_i - P_{i-1} - Y_{i-1} \in A[X_1, \ldots, X_n, Y_1, \ldots, Y_d],$$
$$i = 1, \ldots, d, \quad Y_0 = 0.$$

Then there exists an isomorphism

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

Proof. We define a homomorphism $\tilde{f}: A[X_1, \ldots, X_{n+1}] \to A[X_1, \ldots, X_n, Y_1, \ldots, Y_d]$ by setting

$$\tilde{f}(X_i) = X_i \qquad \text{for } i = 1, \ldots, n,$$

$$\tilde{f}(X_{n+1}) = Y_d + P_d(X_1, \ldots, X_n).$$

We have

$$\tilde{f}(F(X_1, \ldots, X_{n+1})) = \tilde{f}\left(\pi^d X_{n+1} - \sum_{i=0}^{d} \pi^i P_i(X_1, \ldots, X_n)\right)$$

$$= \pi^d Y_d + \pi^d P_d - \sum_{i=0}^{d} \pi^i P_i = \pi^d Y_d + \pi^d P_d$$

$$+ \sum_{i=0}^{d-1} \pi^i (F_{i+1}' - \pi Y_{i+1} + Y_i) - \pi^d P_d = \sum_{i=1}^{d} \pi^{i-1} F_i'.$$

Therefore $\tilde{f}$ defines a homomorphism

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

The fact that f is an isomorphism follows easily from the construction of $\tilde{f}$.

3.3.6. **Lemma.** *Let* $F = \pi X_{n+1} - P(X_1, \ldots, X_n) - \pi Q(X_1, \ldots, X_n) \in A[X_1, \ldots, X_{n+1}]$, *where* $P = P(X_1, \ldots, X_n)$ *is a* $\bmod \pi$ *irreducible p-polynomial. Then there exists a quasi-radical extension* $A' \supset A$ *and an isomorphism* f: $A'[X_1, \ldots, X_{n+1}]/(F) \to A'[Y_1, \ldots, Y_n]$ *such that*

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

where the R_i *are p-polynomials.*

Proof. We may obviously assume that the nonzero coefficients of the polynomial P are invertible. Applying Lemma 3.3.4, we find a quasi-radical extension $A' \supset A$ and a p-polynomial isomorphism

$$f_1 : A'[X_1, \ldots, X_{n+1}] \to A'[T_1, \ldots, T_n, X_{n+1}]$$

such that $f_1(F) = \pi X_{n+1} - T_1 - \pi Q'(T_1, \ldots, T_n)$.

We write the polynomial Q' in the form

$$Q'(T_1, \ldots, T_n) = Q_1'(T_2, \ldots, T_n) + T_1 Q_2'(T_1, \ldots, T_n)$$

and consider the isomorphism

$$f_2 : A'[T_1, \ldots, T_n, X_{n+1}] \to A'[T_1, \ldots, T_n, S],$$

defined by the following formula:

$$f_2(T_i) = T_i, \quad i = 1, 2, \ldots, n,$$

$$f_2(X_{n+1}) = S - T_1 Q_2'(T_1, \ldots, T_n).$$

We have

$$f_2 \circ f_1(F) = \pi(S - Q_1'(T_2, \ldots, T_n)) - T_1,$$

from which, by passing to the quotient ring, we obtain an isomorphism

$$f_3 : A'[X_1, \ldots, X_{n+1}]/(F) \to A'[T_1, \ldots, T_n, S]/(\pi(S - Q_1'(T_2, \ldots, T_n)) - T_1).$$

Taking the composition of this isomorphism with the isomorphism

$$A'[T_1, \ldots, T_n, S]/(\pi(S - Q_1'(T_2, \ldots, T_n)) - T_1) \to A'[Y_1, \ldots, Y_n],$$

that is defined by the formulas

$$T_i \mapsto Y_{i-1}, \quad i = 2, \ldots, n,$$

$$S \mapsto Y_n,$$

$$T_1 \mapsto \pi Y_n - \pi Q_2'(Y_1, \ldots, Y_{n-1}),$$

we find an isomorphism $f : A'[X_1, \ldots, X_{n+1}]/(F) \to A'[Y_1, \ldots, Y_n]$.

From the construction of f it easily follows that

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

where the $R_i(Y_1, \ldots, Y_n)$ are p-polynomials.

3.3.7. **Proof of Theorem 3.3.** By definition there exists a subset $\bar{I} = \{i_1, \ldots, i_{N-n}\} \subset [1, N]$ such that $A[G] \cong A[X_1, \ldots, X_N]/(F_1, \ldots, F_{N-n})$, where $F_j = \pi^{d_j} X_{i_j} - P_j(X_1, \ldots, X_{i_j - 1})$, $j = 1, \ldots, N - n$, the P_j are p-polynomials, and $\pi^{d_j} | p$.

a) (Reduction to the case when $d_j = 1$, and the nonzero coefficients of the polynomials P_j are invertible.) We represent the polynomial $P_1(X_1, \ldots, X_{i_1-1})$ in the form

$$P_1 = P_1^{(0)} + \pi P_1^{(1)} + \ldots + \pi^{d_1-1} P_1^{(d_1-1)} + \pi^{d_1} P_1^{(d_1)},$$

where the $P_1^{(i)}$ $(i = 0, \ldots, d_1 - 1)$ are p-polynomials with invertible nonzero coefficients. Applying Lemma 3.3.5, we obtain a homomorphism

$$\begin{aligned} \tilde{f}_1 \colon A[X_1, \ldots, X_N] \to A[Y_1, \ldots, Y_{i_1-1}, Y_{i_1}, \ldots, Y_{i_1+d_1}, \ldots, Y_{N+d_1}] \\ (X_i \mapsto Y_i, \quad 1 \leqslant i < i_1, \\ X_i \mapsto Y_{i+d_1}, \quad i_1 < i \leqslant N, \\ X_{i_1} \mapsto Y_{i_1+d_1} - P_1^{(d_1-1)}(Y_1, \ldots, Y_{i_1-1})), \end{aligned}$$

inducing an isomorphism

$$f_1 \colon A[X_1, \ldots, X_N]/(F) \to A[Y_1, \ldots, Y_{N+d_1}]/(F_1^{(1)}, \ldots, F_1^{(d_1)}),$$

where

$$F_1^{(i)} = \pi Y_{i_1+i-1} - Y_{i_1+i-2} - P_1^{(i-1)}(Y_1, \ldots, Y_{i_1-1}), \quad 2 \leqslant i \leqslant d,$$

$$F_1^{(1)} = \pi Y_{i_1} - P_1^{(0)}(Y_1, \ldots, Y_{i_1-1}).$$

Since $\tilde{f}_1$ is a p-polynomial homomorphism, we have

$$\tilde{f}_1(F_2) = F_2' = \pi^{d_2} Y_{i_2+d_1} - P_2(Y_1, \ldots, Y_{i_2+d_1-1}) - pQ(Y_1, \ldots, Y_{i_2+d_1-1}),$$

where P_2 is a p-polynomial. We represent F_2' in the form

$$F_2' = \pi^{d_2} Y_{i_2+d_1} - P_2^{(0)} - \pi P_2^{(1)} - \ldots - \pi^{d_2}(P_2^{(d_2)} + p\pi^{-d_2} Q),$$

where the nonzero coefficients of the $P_2^{(i)}$ $(0 \leq i \leq d_2 - 1)$ are invertible. Applying Lemma 3.3.5 to F_2', we obtain an isomorphism

$$\begin{aligned} f_2 \colon A[X_1, \ldots, X_n]/(F_1, F_2) \\ \to A[Z_1, \ldots, Z_{N+d_1+d_2}]/(\bar{F}_1^{(1)}, \ldots, \bar{F}_1^{(d_1)}, \bar{F}_2^{(1)}, \ldots, \bar{F}_2^{(d_2)}), \end{aligned}$$

where

$$\bar{F}_1^{(1)} = \pi Z_{i_1} - P_1^{(0)}(Z_1, \ldots, Z_{i_1-1}),$$

$$\bar{F}_1^{(i)} = \pi Z_{i_1+i-1} - Z_{i_1+i-2} - P_1^{(i-1)}(Z_1, \ldots, Z_{i_1-1}), \quad 2 \leqslant i \leqslant d_1,$$

$$\bar{F}_2^{(1)} = \pi Z_{i_2+d_1} - P_2^{(0)}(Z_1, \ldots, Z_{i_2+d_1-1}),$$

$$\bar{F}_2^{(i)} = \pi Z_{i_2+d_1+i-1} - Z_{i_2+d_1+i-2} - P_2^{(i-1)}(Z_1, \ldots, Z_{i_2+d_1-1}), \quad 2 \leqslant i \leqslant d_2$$

Continuing this process, we eventually obtain an isomorphism

$$A[X_1, \ldots, X_N]/(F_1, \ldots, F_{N-n}) \to A[T_1, \ldots, T_{N+d}]/(F_1', \ldots, F_{N-n+d}'),$$

where $d = d_1 + \ldots + d_{N-n}$, and for some subset $I' = \{i_1, \ldots, i_{N-n+d}\} \subset [1, N]$ we have that $F_j' = \pi T_{i_j} - P_j(T_1, \ldots, T_{i_j-1})$ and the P_j are p-polynomials whose nonzero coefficients are invertible. Therefore we may assume that $d_j = 1$ and the nonzero coefficients of P_j are invertible.

b) Since the closed fiber G_0 of the scheme G is integral, the k-algebra $k[G_0]$ is also integral. We have

$$k[G_0] = k[X_1, \ldots, X_N]/(\overline{P}_1, \ldots, \overline{P}_{N-n}),$$

where the $\overline{P}_i$ are the images of the polynomials P_i under the reduction homomorphism $A[X_1, \ldots, X_N] \to k[X_1, \ldots, X_N]$. In particular, the polynomials $\overline{P}_i(X_1, \ldots, X_N)$ are irreducible.

c) *(end of the proof).* Let

$$B_j = A[X_1, \ldots, X_{i_j}](F_1, \ldots, F_j), \quad j = 1, \ldots, N-n.$$

By Lemma 3.3.6 there exists a quasi-radical extension $A' \supset A$ and an isomorphism

$$f_1 : B_1' = B_1 \otimes_A A' \to A'[Y_1, \ldots, Y_{i_1-1}]$$

such that

$$f_1(X_i) = R_i(Y_1, \ldots, Y_{i_1-1}) + \pi\Phi_i(Y_1, \ldots, Y_{i_1-1}), \quad 1 \leqslant i \leqslant i_1,$$

where the $R_i(Y_1, \ldots, Y_{i1-1})$ are p-polynomials. We extend the isomorphism f_1 to an isomorphism

$$\tilde{f}_1 : B_2' = B_2 \otimes_A A' = B_1'[X_{i_1+1}, \ldots, X_{i_2}]/(\pi X_{i_2} - P_2(X_1, \ldots, X_{i_2-1})),$$
$$\to A'[Y_1, \ldots, Y_{i_1-1}, Y_{i_1}, \ldots, Y_{i_2-1}]/(\pi Y_{i_2-1} - P_2'(Y_1, \ldots, Y_{i_2-2}) - \pi Q(Y_1, \ldots, Y_{i_1-2})),$$

by setting

$$\tilde{f}_1(X_i) = f_1(X_i), \quad 1 \leqslant i \leqslant i_1,$$
$$\tilde{f}_1(X_i) = Y_{i-1}, \quad i_1 < i \leqslant i_2.$$

Obviously $P_2'(Y_1, \ldots, Y_{i_2-2})$ is an irreducible p-polynomial. Thus we can again apply Lemma 3.3.6 and continue with an analogous argument. Finally, we obtain for some quasi-radical extension $\tilde{A} \supset A$ the desired isomorphism

$$\tilde{f} : \tilde{A}[G] = B_{N-n} \otimes_A \tilde{A} \to \tilde{A}[Z_1, \ldots, Z_n]$$

and thus we have proved Theorem 3.3.

3.4. **Corollary.** *Under the hypotheses of Theorem* 3.3 *we assume that the residue field k is perfect. Then* $G \cong \mathbf{A}_A^n$.

In fact, since k is perfect, the extension $A' \supset A$ of the assertion of Theorem 3.3 necessarily coincides with A.

3.5. The application of Theorem 3.3 to unipotent groups is based on 2.4.0 and 3.1.

Theorem. *Let S be a locally noetherian regular integral scheme of dimension ≤ 1 over a field k of characteristic p. Let G be a commutative smooth unipotent S-group scheme with generic fiber of period p and with connected fibers of dimension n. Then G is a form of $\mathbf{A}^n_S$ relative to the radical topology (cf. 0.10.2).*

Proof. If $\dim S = 0$, the assertion is well known (0.7.3c)). Assume that $\dim S = 1$. Using the standard technique of passing to the projective limit ((EGA), IV.8.5), we may assume that $S = \operatorname{Spec} A$, where A is a discrete valuation ring. Let K be the field of fractions of A. In view of 0.7.3c) there exists a radical extension K'/K such that $G_K \otimes_K K' \cong \mathbf{G}^n_{a,K'}$. Let S' be the normalization of S in K'. Then $S' = \operatorname{Spec} A'$, where A' is a discrete valuation ring, and the canonical morphism $\operatorname{Spec} A' \to \operatorname{Spec} A$ is radical. Now taking instead of G the group scheme $G' = G \times_A S'$, we find ourselves, because of 0.7.3c), in the situation of 2.5. Therefore G' is a p-polynomial A'-scheme. Since the conditions of smoothness and connectedness of the fibers are preserved under flat base change, we can apply Theorem 3.3 to G'. As a result we obtain a quasi-radical extension $A'' \supset A'$ such that $G' \otimes_{A'} A'' \cong \mathbf{A}^n_{A''}$. Since $A' \supset \mathbf{F}_p$, the morphism $\operatorname{Spec} A'' \to \operatorname{Spec} A'$ is radical (cf. 3.3.2), and therefore the composition $S'' = \operatorname{Spec} A'' \to \operatorname{Spec} A' \to \operatorname{Spec} A$ is also radical.

3.6. **Corollary.** *In addition to the hypotheses of Theorem 3.5 assume that the generic fiber G_η is isomorphic to $\mathbf{G}^n_{a,\eta}$ and that the residue fields of the closed points of S are perfect. Then G is a form of $\mathbf{G}^n_{a,S}$ in the Zariski topology.*

This follows immediately from 3.4 and the proof of 3.5.

3.7. **Proposition.** *Let S be a locally noetherian regular integral scheme of dimension ≤ 1. Every smooth group model of $\mathbf{G}_{a,\eta}$ over S with connected fibers is a form of $\mathbf{G}_{a,S}$ in the Zariski topology.*

The proof of this proposition is precisely analogous to the proof of Theorem 3.5 and Corollary 3.6, in which instead of Theorem 3.3 we use the following

Lemma. *Let G be a smooth model of $\mathbf{G}_{a,K}$ over A with connected fibers. Then $G \cong \mathbf{G}_{a,A}$.*

Proof. According to 2.3.0, $A[G] = A[y_1, \ldots, y_N]$, where $\bar{I} = [2, N]$ in our case. We shall show that $\bar{I} = \varnothing$.

Assume that $\bar{I} \neq \varnothing$. Then $A[G]$ is given by the relations

$$\pi^{a_i} y_i = y_{i-1}^{p^{r(i)}} + P_i(y_1, \ldots, y_{i-1}), \quad i = 2, \ldots, N,$$

where $\deg P_i < \deg y_i$. We consider $k[G] = k[y_1, \ldots, y_N]$,

$$y_{i-1}^{p^{r(i)}} + \bar{P}_i(y_1, \ldots, y_{i-1}) = 0, \quad i = 2, \ldots, N.$$

We put $B = k[y_1, y_2] \subset k[G]$. The inclusion $B \to k[G]$ defines an epimorphism $G \to \operatorname{Spec} B$.

(That Spec B has a group structure follows from the linear unipotence of G.) From this we see that Spec B must be a one-dimensional smooth connected unipotent group scheme. However,

$$B = k[X_1, X_2]/(X_1^{p^{r(2)}} - \overline{P}_1(X_1)), \quad \deg \overline{P}_1(X_1) < p^{r(2)},$$

and is not a geometrically integral ring. Therefore $\overline{I} = \varnothing$ and $A[G] = A[y_1]$, as required.

3.8. In this subsection we offer some comments on the results of this section.

3.8.1. The proof of Theorem 3.3 is considerably simpler if the ring A is equicharacteristic. In fact, Lemma 3.3.1 shows that the image of a p-polynomial with respect to a p-polynomial homomorphism is again a p-polynomial. This fact allows us to considerably simplify Lemma 3.3.6, and along with this yields a proof of the theorem.

3.8.2. It appears that Corollary 3.4 can be strengthened if instead of requiring that the residue field be perfect we require the existence of the isomorphism $G_0 \cong \mathbf{A}_k^n$ for the closed fiber. For this it is necessary to show that Lemma 3.3.4 holds in this case, with $A' = A$.

3.8.3. The results of 2.3.0 and 3.3–3.6 make the following conjecture plausible.

Conjecture 1. *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 $\mathbf{A}_S^n$ with respect to the* fppf*-topology. If in addition S is an equicharacteristic scheme, then the same is true with respect to the radical topology.*

We observe that the condition of affineness in Conjecture 1 is essential (cf. Example 6.2). If S is a scheme of characteristic zero, then Conjecture 1 is true by virtue of 0.8.1.

3.8.4. If $\dim S = 1$, the preceding conjecture would follow from Theorem 3.3 and the following conjecture.

Conjecture 2. *Let A be a discrete valuation ring. Every unipotent group model of affine space is a p-polynomial A-scheme.*

3.8.5. Conjecture 1 is obviously a special case of an assertion of the following form:

Let S be as in Conjecture 1, and X an affine S-scheme such that the fiber $X_s \cong \mathbf{A}_S^n$ for all $s \in S$. Then X is a form of $\mathbf{A}_S^n$ in the Zariski topology.

It has been shown by V. I. Danilov (unpublished) that this assertion is true if $n = 1$ (cf. 3.7). The preceding assertion is closely connected with a result of Bryński [5].

§4. Composition series

The notation is the same as in 3.0.0.

4.1. Theorem. *Let G be a unipotent group model of $\mathbf{A}_K^n$ over A. Let $\widetilde{H}$ be a normal subgroup of the group G_K; H is isomorphic to $\mathbf{A}_K^m$. Then there exists an affine group model H, normal in G, such that $H_K = \widetilde{H}$. The quotient G/H exists and is a group model of the group $G_K/\widetilde{H}$.*

Proof. Let $K[G] = K[x_1, \ldots, x_n]$ and $K[G_K/\widetilde{H}] = K[x_1, \ldots, x_{n-m-1}]$ (here we have used a theorem from [7], IV, §4, 4.1). We will moreover assume that x_i is

primitive modulo $x_1, \ldots, x_{i-1}$ (see [7], IV, §4, 4.1). Put $B = A[G] \cap K[x_1, \ldots, x_{n-m-1}]$. The kernel of the homomorphism $G \to \operatorname{Spec} B$ has the ring $A[G]/(y_i,\ i \in \Omega_{n-m-1})$ as its ring (cf. 2.2.1). The kernel is flat by 2.2.4a); denote it by H. By the above G, $\operatorname{Spec} B$, H and the homomorphisms $H \to G$ and $G \to \operatorname{Spec} B$ are flat. By construction $H_K = H$, as required.

4.2. Let G be as in 4.1. The series of group models

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_l \supseteq \ldots$$

is called a *model* of the series $G_K = G_{0,K} \supseteq G_{1,K} \supseteq \ldots \supseteq G_{i,K} \supseteq \ldots$, if the quotients G_i/G_{i+j} exist.

Theorem. *Let G be a unipotent group model of $\mathbf{A}^n$ over A. Then G contains models of the following series:*

a) *the composition series whose quotients are $\mathbf{G}_{a,K}$;*

b) *the upper and lower central series;*

c) *the characteristic composition series whose quotients are models of $\mathbf{G}^n_{a,K}$.*

The proof is achieved by applying Theorem 4.1, taking into account [7], Chapter IV, §4, Theorem 4.1 and also 0.7.3c).

4.2.1. Examples 6.3 and 6.7.5 show that a smooth unipotent group model with connected fibers may not have a series of smooth group schemes with connected fibers.

4.3. Theorem 4.2 is a special case of the following general assertion, whose proof is based on the deep results of Raynaud and Anantharaman on the existence of quotients of flat group schemes over one-dimensional bases ([4], [14]).

Theorem. *Let G be a flat S-group scheme of finite type over a locally noetherian one-dimensional regular integral scheme S. Let η be a generic point of S, and let $G_\eta = \tilde{G}_0 \supseteq \tilde{G}_1 \supseteq \ldots \supseteq \tilde{G}_n = 0$ be a composition series of the generic fiber G_η. Then there exists a composition series of the group G which is a model of this series.*

Proof. By (EGA), IV.2.8.5, the scheme-theoretic closures G_i of the subgroups $\tilde{G}_i$ will be flat S-group schemes. It remains to use the results of [4] on the existence and those of [18] on the affineness of the quotients G_i/G_{i+1}.

4.4. We put

$$\Phi_a(x) = \frac{1}{p} \sum_{\alpha=1}^{p^a-1} C^\alpha_{p^a} x^\alpha \otimes x^{p^a-\alpha}.$$

Note that in characteristic p we have

$$\Phi_a(x) = \Phi_1(x^{p^{a-1}}).$$

Lemma. *Let L be a field of characteristic p and G a commutative unipotent group that is isomorphic as a scheme to $\mathbf{A}^n_L$. Then we can choose generators $x_1, \ldots, x_n$ of the ring $L[G]$ such that*

$$\eta(x_i) = \sum_{j<i} \sum_{\alpha} a_{ij\alpha}\Phi_\alpha(x_j). \qquad (*)$$

Proof. By [7], Chapter IV, § 4, Theorem 4.1, the group G has a composition series of the groups $\mathbf{G}_{a,L}$. By [7], Chapter II, § 3, 4.6 and Chapter III, § 4, Corollary 6.6, G is given by such formulas if $n = 2$. Apply induction on n. We assume that the assertion is true for $n \leq t$ and prove it for $n = t + 1$. We have

$$1 \to \mathbf{G}_a \to G \to H \to 1,$$

dim $H = t$, $L[H] = L[x_1, \ldots, x_t]$, and formula (*) holds for $\eta(x_i)$, $i \leq t$. Put $H_1 = \operatorname{Spec} L[x_1, \ldots, x_{t-1}]$. Then we have the exact sequence

$$1 \to H_2 \xrightarrow{\varphi} H \xrightarrow{\psi} H_1 \to 1,$$

where $H_2 \cong \mathbf{G}_a$.

The group G is determined by a cocycle $\alpha \in H^2(\mathbf{G}_a, H)$ (cf. [7], II, § 3, 4.6). We have

$$H^2(\mathbf{G}_a, H_2) \xrightarrow{\varphi_*} H^2(\mathbf{G}_a, H) \xrightarrow{\psi_*} H^2(\mathbf{G}_a, H_1)$$

(exact at the middle term). $\psi_*(\alpha)$ corresponds to formulas of the form (*) by the induction hypothesis, so we may assume that $\psi_*(\alpha) = 0$. But then $\alpha \in \operatorname{Im} \phi_*$, and hence α is again given by formulas of the form (*), as required.

4.5. **Theorem.** *Let $\tilde{G}$ be a unipotent group over $k = A/\pi$, isomorphic to $\mathbf{A}^n_k$. Then there exists an unipotent group scheme G over A such that $G_k \cong \tilde{G}$, and also $G \cong \mathbf{A}^n_A$. In particular, if the field is perfect, then any smooth connected group over this field lifts to characteristic 0.*

Proof. Let $k[\tilde{G}] = k[x_1, \ldots, x_n]$ and

$$\eta(x_i) = \sum_{j<i} \sum_{\alpha} \bar{a}_{ij\alpha}\Phi_\alpha(x_j), \quad \bar{a}_{ij\alpha} \in k.$$

We also choose $a_{ij\alpha} \in A$ such that the reduction of $a_{ij\alpha}$ is equal to $\bar{a}_{ij\alpha}$. We put $A[G] = A[y_1, \ldots, y_n]$ and

$$\eta(y_i) = \sum_{j<i} \sum_{\alpha} a_{ij\alpha}\Phi_\alpha(y_j).$$

It is clear that then the reduction of $A[G]$ is $\tilde{G}$, and it is only necessary to check that these formulas give a group law. It is also clear that it suffices to check these formulas for $n = 2$, $\eta(y_1) = 0$ and $\eta(y_2) = \Phi_\alpha(y_1)$. This is immediate.

4.6. **Remark.** The hypotheses of Theorem 4.5 are essential. For example, nontrivial forms of the group $\mathbf{G}_a$ (see 0.7.2d) if A/π is not perfect) do not lift to unipotent groups in characteristic 0.

In fact, if char $K = 0$ and dim $G = 1$, then $G_K \cong \mathbf{G}_{a,K}$ and thus Proposition 3.7 is applicable.

4.7. **Theorem.** *Extensions of $\mathbf{G}_{a,A}$ by $\mathbf{G}_{a,A}$ over the ring A have coordinate ring*

$A[y_1, y_2]$ *with the composition law*

$$\eta(y_1) = 0, \quad \eta(y_2) = \sum_i a_i \Phi_i(y_1), \quad a_i \in A.$$

In particular, the set of extensions is isomorphic to a free module over the noncommutative ring $(A/p)[F]$, *where* F *is the Frobenius operator (in* A/p).

Proof. We shall first show that the second assertion of the theorem follows from the first. In fact, $y_1 \to y_1$, $y_2 \to y_2 + P(y_1)$ are the only changes of coordinates that do not change the extension (in case it is nontrivial). For such changes to preserve the shape of our formulas it is necessary that $P(y_1)$ be a p-polynomial, $P(y_1) = \Sigma b_i y_1^{p^i}$. But then in the new coordinates we have

$$\eta(y_1) = 0, \ \eta(y_2) = \sum (a_i + pb_i)\, \Phi_i(y_1).$$

Since, moreover, $\Phi_{i+j}(y) = (\Phi_j(y))^{p^j}$ in A/p, our assertion is proved.

Let G be an extension of $G_{a,A}$ by $G_{a,A}$. Then $G \cong A_A^2$, i.e. $A[G] = A[y_1, y_2]$. We may assume that the imbedding $A[y_1] \to A[G]$ corresponds to a projection of our extension. Then we have $\eta(y_1) = 0$. Automatically $\eta(y_2) \in A[y_1] \otimes A[y_1]$.

We consider the cases char $K = 0$ and char $K = p > 0$ separately.

4.7.1. First suppose that char $K = 0$. Then $K[G] = K[x_1, x_2]$ and $\eta(x_1) = \eta(x_2) = 0$. We may assume that $x_1 = y_1$. In this case $y_2 = Q(x_1, x_2)$, and in view of the conditions $\eta(y_2) \in A[y_1] \otimes A[y_1]$ and $\eta(x_1) = \eta(x_2) = 0$ we have $y_2 = bx_2 + P(x_1)$. We will show that by admissible changes of variables $P(x_1)$ reduces to the form $P(x_1) = \Sigma r_i x_1^{p^i}$ and $pr_i \in A$. The assertion of the theorem will follow from this with $a_i = pr_i$. Let $P(x_1) = \Sigma b_i x_1^i$. Assume that for $i \geq q$ we have proved that $pb_i \in A$ and that we may assume the validity of the equality

$$\sum_{i \geqslant q} b_i x_1^i = \sum r_i x_1^{p^i}.$$

We shall show that if $\deg b_{q-1} x_1^{q-1} \neq p^a$, then $b_{q-1} \in A$; then, applying 2.3.1.3, we may assume that $b_{q-1} = 0$. In fact, setting $z = \Sigma_{i \geq q} b_i x_1^i$, we have

$$\eta(z) = \sum pr_i \Phi_i(x_1), \quad pr_i \in A.$$

Applying 2.3.3 to $\eta(b_{q-1} x_1^{q-1})$, we find that $b_{q-1} C_{q-1}^i \in A$ for all $i \in [1, q-2]$.

If $q - 1 \neq p^a$, it follows from this that $b_{q-1} \in A$, as required. If $q - 1 = p^a$, then from 2.3.3.3 we find $b_{q-1} \cdot p \in A$, which completes the induction step.

4.7.2. Now if char $K = p$, then $K[G] = K[x_1, x_2]$, $x_1 = y_1$, $\eta(x_2) = \Sigma \tilde{a}_i \Phi_i(x_1)$ and $\tilde{a}_i \in K$ (cf. [7], Chapter II, § 3.4.6 and Chapter III, § 4, Corollary 6.6). We have $y_2 = bx_2 + \Sigma b_i x_1^i$. Replacing x_2 by bx_2, we obtain $b = 1$ and $\eta(x_2) = \Sigma a_i \Phi_i(x_1)$. Carrying out the induction as above, we find that (cf. 2.3.2.3) $\Sigma b_i x_1^i = \Sigma r_i x_1^{p^i}$, whence $\eta(y_2) = \Sigma a_i \Phi_i(x_1)$, as required.

4.7.3. **Remark.** The proof of 4.7.1 actually does not use the condition that A is

an equicharacteristic discrete valuation ring. Namely, let A *be a local ring and* K *its* field of fractions, char $K = 0$. Let B be the integral closure of $\mathbf{Z}$ in A. Then B is a discrete valuation ring. Let π be the uniformizing parameter of B, $p = \operatorname{char} B/\pi$, and $D = A \otimes \mathbf{Q}$, and let G be an extension of $\mathbf{G}_{a,A}$ by $\mathbf{G}_{a,A}$. Then, according to 0.8.1, $G_D \cong \mathbf{G}_{a,D}^2$. Since $A[G] = A[y_1, y_2]$, $\eta(y_1) = 0$ and $\eta(y_2) \in A[y_1] \otimes A[y_1]$, we have $y_2 = bx_2 + P(x_1)$, where $b \in \overline{\mathbf{Q}}$ and $P(x_1) \in D[x_1]$. In particular, $\pi P(x_1) \in A[x_1]$ for suitable a.

After these remarks, the proof of 4.7.1 goes through without change and leads to the following result.

Theorem. *Let* A *be a local integral ring with field of fractions of characteristic* 0 *and residue field of characteristic* $p > 0$. *The conclusions of Theorem* 4.7 *hold over* A.

§5. Cohomology of commutative unipotent groups

5.0. The notation is that of 3.0.0. In addition, let $S = \operatorname{Spec} A$, and let η be the generic point of A and s the closed point of A. In this section we compute the cohomology of commutative unipotent groups G over A. The cohomology $H^i_\alpha(X, G)$ is considered with respect to the fpqc-topology ($\alpha = 1$), the fppf-topology ($\alpha = 2$), and the étale topology ($\alpha = 3$) on the scheme X.

All the group schemes considered in this section are assumed to be commutative.

5.1. The following results relate to the "comparison theorems" for cohomology with respect to the various topologies:

5.1.1 (Grothendieck [8]). If G is a smooth group scheme over an arbitrary scheme X, then $H^i_2(X, G) \cong H^i_3(X, G)$, $i \geq 0$.

5.1.2 (Miyanishi [10]). For any X-group scheme G, $H^1_1(X, G) \cong H^1_2(X, G)$.

5.2. We recall the standard computation of the cohomology of "elementary" unipotent groups over a field k of characteristic $p > 0$.

5.2.0. The following exact sequences are basic for these computations:

$$0 \to \alpha_p \to \mathbf{G}_a \xrightarrow{F} \mathbf{G}_a \to 0, \tag{*}$$

$$0 \to (\mathbf{Z}/p\mathbf{Z})_k \to \mathbf{G}_a \xrightarrow{\wp} \mathbf{G}_a \to 0. \tag{**}$$

Here $F: x \to x^p$ and $\wp: x \to x^p - x$. The first of these sequences is exact only in the fpqc- and fppf-topologies: the second is also exact in the étale topology.

5.2.1. By 5.1.1 and (SGAA), IX.4.3, for any affine base X

$$H^i(X, \mathbf{G}_{a,X}) = 0, \quad i \geq 0.$$

5.2.2. Applying the exact sequences of cohomology groups to sequence (*) of 5.2.0, from 5.2.1 we obtain

$$H^i_\alpha(k, \alpha_p) = \begin{cases} k^+/k^{+p}, & i = 1, \\ 0, & i \neq 1 \end{cases} \quad (\alpha = 1, 2).$$

Since the restriction of the sheaf α_p to $S_{\text{ét}}$ equals zero, then

$$H^i_3(k, \alpha_p) = 0, \quad i \geq 0.$$

5.2.3. Analogously, using 5.2.1 and the sequence (**) of 5.2.0, we find that

$$H^i_\alpha(k, (\mathbf{Z}/p\mathbf{Z})_k) = \begin{cases} \mathbf{Z}/p\mathbf{Z}, & i = 0, \\ k^+/\mathfrak{p}(k^+), & i = 1 \\ 0, & i > 1 \end{cases}$$

$$(\alpha = 1, 2, 3).$$

By Witt's theorem (cf. [17], p. 447), if k is a local field, then

$$k^+/\mathfrak{p}(k^+) \cong \mathrm{Hom}(k^*/k^{*p}, \mathbf{Q}/\mathbf{Z}).$$

5.2.4. Now if G is an étale k-form of $(\mathbf{Z}/p\mathbf{Z})_k$, then it is trivialized on some separable extension k'/k of degree dividing $p-1$. By (SGAA), IX, 5.2, it follows from this that

$$0 = H^i_3(k', (\mathbf{Z}/p\mathbf{Z})_{k'}) \Rightarrow H^i_3(k, G) = 0.$$

Since G is smooth, $H^i_\alpha(k, G) = H^i_3(k, G)$ for $\alpha = 1, 2$.

5.2.5. Collecting together the results of 5.2.1–5.2.4, we obtain the following assertion:

Lemma. *Let $G = \mathbf{G}_{a,X}$, α_p or an étale k-form of $\mathbf{Z}/p\mathbf{Z}$. Then for $\alpha = 1, 2$ and 3 we have $H^i_\alpha(k, G) = 0$ for $i \geq 2$. Furthermore, if G is connected and k is perfect, then $H^1_\alpha(k, G) = 0$ for $i \geq 1$ $(\alpha = 1, 2, 3)$.*

5.3. The computation of the cohomology of arbitrary unipotent groups over k is based on the existence of a composition series of elementary groups (0.7.3) for such groups.

In particular, we obtain the following

Proposition. *Let G be a unipotent k-group. Then $H^i_\alpha(k, G) = 0$ for $i \geq 2$ $(\alpha = 1, 2, 3)$. If, in addition, G is connected and k is perfect, then $H^i_\alpha(k, G) = 0$ for $i \geq 1$ $(\alpha = 1, 2, 3)$. If G is connected, then $H^i_3(k, G) = 0$, $i \geq 1$, for any field k. Moreover, if k is algebraically closed, then $H^i_\alpha(k, G) = 0$ for $i \geq 1$ and $\alpha = 1, 2, 3$.*

5.4. In this subsection we shall prove the following result.

Theorem. *Let G be a unipotent S-group. Assume that S is equicharacteristic and $G_\eta \simeq \mathbf{A}^n_\eta$. Then $H^i_\alpha(S, G) = 0$ for $i \geq 2$ and $\alpha = 1, 2, 3$. If k is algebraically closed, then this is also true for $i \geq 1$.*

Proof. By 4.3 it suffices to prove the theorem while assuming that G is a group model of $\mathbf{G}_{a,\eta}$. Applying Lemma 2.6 and 5.2.1, we obtain $H^i_\alpha(S, G) = 0$ for $i \geq 2$ and all α. Moreover, $H^1_\alpha(S, G)$ is the cokernel of the homomorphism $A^N \to A^{N-1}$ defined by the formula

$$(a_1, \ldots, a_N) \to (F_2(a_1, a_2), \ldots, F_N(a_1, \ldots, a_N)),$$

where the F_i are the p-polynomials of 2.6. If k is algebraically closed, this mapping is obviously surjective. Thus in this case $H^1_\alpha(S, G) = 0$, as required.

5.5. **Corollary.** *Let G be a unipotent S-group scheme. Assume that* char $K = p > 0$ *and that the generic fiber G_η is smooth and connected. Then for $\alpha = 3$ we have $H^i_\alpha(S, G) = 0$ for $i \geq 2$. This is also true for $\alpha = 1$ and 2 if G is smooth.*

Proof. Let K'/K be a radical extension such that $G_\eta \otimes K' \cong \mathbf{A}^n_{K'}$ (0.7), and let S' be the normalization of S in K'. Then $S' \to S$ is a radical integral surjective morphism, from which it follows that $H^i_3(S, G) \cong H^i_3(S', G_{S'})$ for $i \geq 0$ (SGAA, VIII, 1.2). It remains to apply Theorem 5.4 and Assertion 5.1.1.

§6. Examples and counterexamples

In this section we give examples, mostly showing the limits at which one or another classical assertion or an assertion of the present paper ceases to be true. We also have examples showing that the conditions imposed in the definitions and theorems are essential.

Below $\mathbf{Z}_p$ denotes the ring of p-adic integers, $\mathbf{Z}_p[\![t]\!]$ the ring of formal power series over $\mathbf{Z}_p$. If A is a ring, then K is its field of fractions.

We let

$$\eta(a) = \mu(a) - 1 \otimes a - a \otimes 1, \quad \Phi_t(a) = \frac{1}{p} \sum_{\alpha=1}^{p^t-1} C^\alpha_{p^t} a^\alpha \otimes a^{p^t-\alpha}.$$

6.1. **An example of a group that is unipotent but not linearly unipotent over a non-reduced ring.** Let $A = \mathbf{Z}_2[u]/u^2$, $A[G] = A[x]$, $\eta(x) = ux \otimes x$, $\iota(x) = -x + ux^2$ and $\epsilon(x) = 0$. The unique fiber of this group is unipotent. In order to get rid of the term $ux \otimes x$, we can only use the substitution $x \to ax + uP(x)$, $a \in A^*$. However, such substitutions have no influence over $ux \otimes x$, i.e. the group is not linearly unipotent.

6.2. **An example of a unipotent group over $\mathbf{Z}_p[\![t]\!]$ that is quasi-affine but not affine** (due to Raynaud [12], VII, 3). Let $A = \mathbf{Z}_p[\![t]\!]$, $A[G] = A[x, y, z]/pz = ty + x + x^p$, $\eta(x) = \eta(y) = 0$ and $\eta(z) = \Phi_1(x)$. Then G is a smooth A-group. Over $A_{(p)} = \mathbf{Q}_p[\![t]\!]$ it is isomorphic to $\mathbf{G}^2_a = \operatorname{Spec} A_{(p)}[x, y]$ (cf. 0.7.2f)). Over $A_{(t)}$ it is isomorphic to $\operatorname{Spec} A_{(t)}[x, z]$ (since $y = (pz - x^p - x)/t$) and is an extension of $\mathbf{G}_a = \operatorname{Spec} A_{(t)}[x, y]/(x)$ by $\mathbf{G}_a = \operatorname{Spec} A_{(t)}[x]$.

Let $s = (p, t)$. We have $G_s = \operatorname{Spec} \mathbf{F}_p[x, y, z]/(x^p + x)$. In particular, G_s is not connected. The connected component G^0 of the identity of G is a smooth quasi-affine group ((SGAD), VI_B, 3.10) with connected fibers. Since $\operatorname{prof}_{G-G^0}(G) = 2$, it follows that $\Gamma(G) \to \Gamma(G^0)$ is bijective (cf. [12], VII.3), and since $G \neq G^0$, G^0 is not affine. We note that here all the fibers of G^0 are affine spaces $\mathbf{A}^2$.

6.3. **An example of a smooth group with connected fibers over $\mathbf{Z}_2$ that does not have a composition series consisting of smooth connected group schemes.** Take

$$A = \mathbf{Z}_2, \quad A[G] = A[x, y, z]/2z = x^4 + y^2 + y,$$

$$\eta(x) = \eta(y) = 0, \quad \eta(z) = \Phi_2(x) + \Phi_1(y).$$

We have $\mathbf{F}_2[G] = \mathbf{F}_2[v, w]$, where $v = x^2 + x + y$, $w = z + v^6$, $\eta(v) = 0$ and $\eta(w) = \Phi_2(v)$. From this we see that for G to be an extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ over $\mathbf{Z}_2$ it is necessary that $A[G]$ contain an element $\bar{v} \equiv x^2 + x + y \bmod 2 \cdot A[G]$ such that $\bar{v} = \alpha x + \beta y$. But

such an element does not exist and thus G does not have a series of G_a's (cf. 4.7, 6.7.5).

However, the embedding $A[x] \to A[G]$ defines a homomorphism whose kernel is Spec $A[y, z]/(2z = y^2 + y)$. It is nonconnected, although it is smooth. On the other hand, the embedding $A[y] \to A[G]$ defines a homomorphism whose kernel is

$$\operatorname{Spec} A[x, z]/2z = x^4.$$

Its fibers are connected, but it is not smooth.

6.4. **An example of a smooth affine unipotent group with connected fibers over $A = \mathbf{Z}_2[\![t]\!]$, for which there does not exist a model (cf. 4.2) of the upper and lower central series.** Take

$$A[G] = A[x, y, z, u]/2u = tz^2 + x^2 + y,$$

$$\eta(x) = \eta(y) = 0, \quad \eta(z) = 2x \otimes y,$$

$$\eta(u) = tz \otimes z + 2tx \otimes zy + 2tzx \otimes y + 2tx^2 \otimes y^2 + x \otimes x.$$

G is a connected smooth A-group, and $G \otimes \mathbf{Q}$ is isomorphic to the group of unipotent matrices of order three. The imbedding $K[x, y] \to K[G]$ defines a homomorphism of $G \otimes K$ into $G^2_{a,K}$ (quotient modulo the center).

We will show that a model of the lower (upper) central series of G (cf. 4.2) contains no flat groups. In fact, such a series must be defined by the embedding $K[x, y] \cap A[G] \to A[G]$. The kernel of the corresponding homomorphism is Spec $A[z, u]/(2u = tz^2)$. This group is not flat (on the line $t = 0$) (see 0.3.2).

6.5. **An example of a flat affine commutative unipotent group over the ring $A = \mathbf{F}_2[\![t]\!]$, which does not have a composition series consisting of flat one-dimensional groups.** We take

$$A[G] = A[x, y, z]/t_1 z = t_2 y^2 + x^2 + ax,$$

$$\eta(x) = 0, \quad \eta(y) = t_1 \Phi_1(x), \quad \eta(z) = t_1 \Phi_2(x).$$

This group is flat. It is smooth (but not connected) for $a = 1$, and its fibers are connected for $a = 0$. Over $\mathbf{F}_2[\![t_2]\!]((t_1))$ it is isomorphic to a Witt group. Every homomorphism of the Witt group G_K in $G_{a,K}$ is given by an embedding $K[f(x)] \to K[G] = K[x, y]$, where $f(x)$ is a p-polynomial. The kernel of this homomorphism is Spec $K[x, y]/(f(x))$.

Assume that G has a composition series of one-dimensional groups over A. Then, by what has been mentioned above, the projection of this series is given by an embedding $A[G] \otimes K[f(x)] \to A[G]$. The kernel of this homomorphism is

$$A[x, y, z]/(f(x), t_1 z - t_2 y^2 - x^2 - ax).$$

This last scheme has dimension 2 at the point (t_1, t_2) and thus is not flat (see 0.3.2).

6.6. **An example of a smooth connected affine commutative unipotent group over $A = \mathbf{Z}_2[\sqrt{2}][\![t]\!]$ that does not have a composition series consisting of flat groups.** We take

$$A[G] = A[x, y, z, u]/\sqrt{2}z = x + ty^2, \quad \sqrt{2}u = y + tz^2,$$

$$\eta(x) = \eta(y) = 0, \quad \eta(z) = \sqrt{2}ty \otimes y,$$

$$\eta(u) = \sqrt{2}tz \otimes z + 2t^2zy \otimes y + 2t^2y \otimes zy + \sqrt{2}t^3y^2 \otimes y^2.$$

Over K the homomorphism of projection is defined by an embedding of $K[ax + by]$ into $K[G] = K[x, y]$, $a, b \in K$. Therefore over A the homomorphism of projection must be defined by an embedding of $M = K[ax + by] \cap A[G]$ in $A[G]$. We may obviously assume that $a, b \in A$.

We assert that over the line $t = 0$ the kernel of any such homomorphism is not flat. In fact, $A/(t)[G] = A[z, u]$, $x = 2z$, $y = 2u$. Therefore $M \otimes A/(t) \subset 2A/(t)[G]$, from which it follows that the kernel is not flat (see 0.3.2).

6.7. Some models of G_a^2 over a discrete valuation ring A with field of fractions of characteristic zero. We consider affine group models of G_a^2 over A, where A is a discrete valuation ring, char $K = 0$ and char $A/\pi = p \neq 0$. We have

$$A[G] = A[x, y, z]/\pi^{d+1}z = \sum_{i=0}^{m} a_i x^{p^i} + \sum_{i=0}^{n} b_i y^{p^i}, \quad a_i, b_i \in A,$$

$$\pi^{d+1} \mid p, \quad (a_m, b_n) = A,$$

$$\eta(x) = \eta(y) = 0,$$

$$\eta(z) = \pi^{-d-1} \cdot p\left[\sum_{i=1}^{m} a_i \Phi_i(x) + \sum_{i=1}^{n} b_i \Phi_i(y)\right].$$

The set of such groups is denoted by $\mathfrak{G}$. We will call the numbers d, a_i for $i \in [0, m]$ and b_j for $j \in [0, n]$ the parameters of the group G.

6.7.1. Let $A_d = A/\pi^{d+1}$, and let $A_d^2[F]$ be the additive group of noncommutative polynomials of F whose coefficients lie in A_d^2, where $Fa = a^pF$, $a \in A_d$.

Furthermore, let $\Pi_d = (d, A_d^2[F])$. We associate a set of parameters d, (a_i), (b_i) to an element of Π_d according to the rule: let α_i be a vector with coordinates (a_i, b_i), taken mod π^{d+1}. Then to our set we associate $(d, \Sigma\alpha_i F^i) \in \Pi_d$.

Lemma. *If $\{d, (a_i), (b_i)\}$ and $\{d, (a_i'), (b_i')\}$ are two sets of parameters that correspond to the same element of the set Π_d, then these sets yield isomorphic A-groups.*

Proof. We have $a_i' = a_i + c_i\pi^{d+1}$ and $b_i' = b_i + d_i\pi^{d+1}$. The substitution

$$z \to z - \sum c_i x^{p^i} - \sum d_i y^{p^i}$$

takes one group into the other.

We will denote by G_ω, where $\omega \in \Pi_d$, any A-group whose parameters are reduced in ω.

6.7.2. The group $\mathfrak{S}_d = GL_1(A_d) \times GL_2(A_d)$ acts on Π_d according to the formula

$$(\lambda, D)\left(d, \sum r_i \mathbf{F}^i\right) = \left(d, \sum \lambda D^{p^i} r_i \mathbf{F}^i\right)$$

(GL_1 acts on the left and GL_2 on the right).

Lemma. *Let $\phi, \omega \in \Pi_d$. The groups G_ω and G_ϕ are isomorphic if and only if $g\omega = \phi$ for suitable $g \in \mathfrak{G}_d$.*

Proof. The A-module $Ax + Ay$ is uniquely isolated in $A[G]$ as the A-module of primitive elements. Therefore x and y are determined up to the substitution $x \to \alpha x + \beta y$, $y \to \gamma x + \delta y$, $\det\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in A^*$. We denote this matrix by D. Since $\pi^{d+1} | p$, and since

$$(\alpha x + \beta y)^{p^a} \equiv \alpha^{p^a} x^{p^a} + \beta^{p^a} y^{p^a} \bmod p,$$

$$(\gamma x + \delta y)^{p^a} \equiv (\gamma^{p^a} x^{p^a} + \delta^{p^a} y^{p^a}) \bmod p,$$

in view of Lemma 6.7.1 we can define an action of $GL_2(A_d)$ on Π_d that agrees with the one described above.

In order to preserve the shape of the formulas, we can only admit for z the substitution

$$z \to \lambda z + \sum c_i x^{p^i} + \sum d_i y^{p^i},$$

which in view of Lemma 6.7.1 reduces to replacing the parameters a_i and b_i (modulo π^{d+1}) by λa_i and λb_i. This gives an action of GL_1 which coincides with the one described above.

Now if two groups G_ω and G_ϕ are isomorphic, then by what was mentioned above there must exist a substitution

$$x \to \alpha x + \beta y,\ y \to \gamma x + \delta y,\ z \to \lambda z + \sum c_i x^{p^i} + \sum d_i y^{p^i}$$

that takes one set of parameters into the other, which proves our assertion.

6.7.3. Let $\mathcal{H}_d$ be the group of automorphisms of the group G_a^2 over A_d. $\mathcal{H}_d$ is generated by transformations from $GL_2(A_d)$ and transformations of D:

$$x \to x + d_0 \pi \sum \alpha_i x^{p^i},$$

$$y \to y + d_0 \pi \sum \beta_i y^{p^i} + \sum \gamma_i x^{p^i}$$

(where $d_0 = 0$ if $d = 0$; $d_0 = 1$ if $d \neq 0$).

Put $\tilde{\mathcal{H}}_d = GL_1 \times \mathcal{H}_d$ and define an action of D on Π_d by the formula

$$\left(d, \sum r_i \mathbf{F}^i\right) \to \left(d, \sum \tilde{r}_i \mathbf{F}^i\right),$$

where

$$r_i = (r_i', r_i''), \quad \tilde{r}_i = (\tilde{r}_i', \tilde{r}_i''), \quad \tilde{r}_i'' = \sum_{\alpha+\beta=i} r_\alpha'' (\pi d \beta_\beta)^{p^\alpha},$$

$$\tilde{r}_i' = r_i' + \sum_{s+t=i} r_s' (\pi d\beta_t)^{p^s} + \sum_{s+t=i} r_s'' \gamma_t^{p^s}.$$

This action extends to an action of $\tilde{\mathcal{H}}_d$ on Π_d.

Lemma. *Let $\phi, \omega \in \Pi_d$. The groups $G_\omega \otimes A_d$ and $G_\phi \otimes A_d$ are isomorphic over A_d if and only if $h\omega = \phi$ for suitable $h \in \tilde{\mathcal{H}}_d$.*

The proof is different from the proof of the preceding assertion only in that the module of primitive elements now consists of the p-polynomials $\Sigma d_i' x^{p^i} + \Sigma d_i'' y^{p^i}$ in x and y; and $\mathcal{H}_d$ is precisely the group that preserves this module.

6.7.4. Corollary. *Let $\omega \in \Pi_d$. The isomorphism classes over A of the A-groups belonging to G which over A_d are isomorphic to $G_\omega \otimes A_d$ are parametrized by the homogeneous space $\mathrm{GL}_2(A_d)\backslash\mathcal{H}_d$. In particular, this set is infinite (and even infinite-dimensional).*

6.7.5. Corollary. *Let the field $k = A_0$ be perfect, and let $\pi^m = p$. Then for each smooth connected group over k there exist $\mathrm{GL}_2(k)\backslash\mathcal{H}_{m-1}$ nonisomorphic A-groups that reduce to the same group. Only one of these groups (up to isomorphism) admits a smooth composition series.*

Proof. It suffices to construct such a group. It is given by one of the sets $d = m - 1$, $a_0 = 1$, $a_i = 0$, $i > 0$, $b_i \in A$ (cf. 4.7). Now apply the preceding assertion.

6.7.6. Suppose k is not perfect. The forms of $\mathbf{G}_a$ over k are enumerated in 0.7.2d).

Corollary. *For any k-form $\tilde{G}$ of the group $\mathbf{G}_{a,k}$ there exist infinitely many smooth affine group models of $\mathbf{G}_{a,K}^2$ with connected fibers over A, which over k have the series*

$$0 \to \mathbf{G}_{a,k} \to G \otimes k \to \tilde{G} \to 0.$$

If p is ramified in A, then there exist an infinite number of models of $\mathbf{G}_{a,K}^2$ over A such that $G_K \cong \mathbf{G}_{a,K} \times \tilde{G}$.

Proof. That there are infinitely many follows from 6.7.4. Suppose $\tilde{G}$ is given by the equation

$$y^{p^n} = \sum_{i=0}^{m} a_i x^{p^i}, \quad a_0 \neq 0, \quad a_i \in k$$

(cf. 0.7.2d)). Put $\omega = (0, \Sigma r_i \mathbf{F}^i)$, where $r_i = (\tilde{a}_i, 0)$ for $i \neq n$, $r_n = (\tilde{a}_n, -1)$ and $\tilde{a}_i \equiv a_i \bmod \pi$. Then $\omega \in \Pi_0$ and

$$G_{\omega,k} = \operatorname{Spec} k[x, y, z]/\left(y^{p^n} - \sum a_i x^{p^i}\right).$$

The mapping $k[\tilde{x}, \tilde{y}]/(y^{p^n} - \Sigma a_i x^{p^i}) \to k[G_\omega]$ defines a homomorphism $G_{\omega,k} \to \tilde{G}$. Its

kernel is Spec $k[z] = G_{a,k}$. If $\pi^{-1}p \notin A^*$, then $G_{\omega,k} = \tilde{G} \times G_{a,k}$ (in view of formula 6.7).

Received 8/MAY/73

BIBLIOGRAPHY

1. A. Grothendieck, *Éléments de géométrie algébrique*, Inst. Hautes Études Sci. Publ. Math. Nos. 8 (1961); 24 (1965); 28 (1964). MR 33 #7330; 36 #177b, 178. (EGA)

2. M. Demazure and A. Grothendieck, editors, *Schémas en groupes*. I, II, III, Séminaire de Géométrie Algébrique du Bois Marie 1972/64, Lecture Notes in Math., vols. 151–153, Springer-Verlag, Berlin and New York, 1970. MR 43 #223a, b, c. (SGAD)

3. M. Artin, A. Grothendieck et al., editors, *Théorie des topos et cohomologie étale des schémas*. I, II, Séminaire de Géométrie Algébrique du Bois Marie 1963/64, Lecture Notes in Math., vols. 269, 270, Springer-Verlag, Berlin and New York, 1972. (SGAA)

4. S. Anantharaman, *Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension* 1, Bull. Soc. Math. France. Mém. 33 (1973), 5–79.

5. M. Bryński, *Forms of the rings* $R[X]$ *and* $R[X, Y]$, Glasgow Math. J. 13 (1972), 91–97.

6. N. Bourbaki, *Algèbre commutative*, Chap. 1, Actualités Sci. Indust., no. 1290, Hermann, Paris, 1961. MR 36 #146.

7. M. Demazure and P. Gabriel, *Groupes algébriques*. Tome I: *Géométrie algébrique, généralités, groupes commutatifs*, Masson, Paris; North-Holland, Amsterdam, 1970. MR 46 #1800.

8. A. Grothendieck, *Le groupe de Brauer*. III: *Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, Masson, Paris; North-Holland, Amsterdam, 1968, pp. 88–188. MR 39 #5586c.

9. Ju. I. Manin, *Lectures on algebraic geometry*. Part I: *Affine schemes*, Izdat. Moskov. Univ., Moscow, 1970. (Russian) MR 44 #1661.

10. M. Miyanishi, *On the cohomologies of commutative affine group schemes*, J. Math. Kyoto Univ. 8 (1968), 1–39. MR 38 #158.

11. D. Mumford, *Enriques' classification of surfaces in* char *p*. I, Global Analysis (Papers in Honor of K. Kodaira), Univ. Tokyo Press, Tokyo, 1969, pp. 325–339. MR 40 #7266.

12. 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. MR 41 #5381.

13. ———, *Modèles de Néron*, C. R. Acad. Sci. Paris Sér. A–B 262 (1966), A345–A347. MR 33 #2631.

14. ———, *Spécialisation du foncteur de Picard*, Inst. Hautes Études Sci. Publ. Math. No. 38 (1970), 27–76. MR 44 #227.

15. P. Russell, *Forms of the affine line and its additive group*, Pacific J. Math. 32 (1970), 527–539. MR 42 #277.

16. J.-P. Serre, *Groupes algébriques et corps de classes*, Publ. Inst. Math. Univ. Nancago, VII, Actualités Sci. Indust., no. 1264, Hermann, Paris, 1959. MR 21 #1973; errata, 30, 1200.

17. S. S. Shatz, *Cohomology of Artinian group schemes over local fields*, Ann. of Math. (2) 79 (1964), 411–449. MR 33 #1314.

18. Anne-Marie Simon, *Un théorème d'affinité de schéma en groupes quotient*, Acad. Roy. Belg. Bull. Cl. Sci. 58 (1972), 1325–1337. MR 47 #8558.

19. F. Bruhat and J. Tits, *Groupes algébriques simples sur un corps local*, C. R. Acad. Sci. Paris Sér. A–B 263 (1966), A822–A825. MR 39 #4162.

Translated by J. S. JOEL