Compositio Mathematica **128:** 1–15, 2001.
© 2001 *Kluwer Academic Publishers. Printed in the Netherlands.*

Finite Flat Group Schemes over Local Artin Rings

RENÉ SCHOOF
Dipartimento di Matematica, 2ª Università di Roma 'Tor Vergata', I-00133 Rome, Italy.
e-mail: schoof@wins.uva.nl

(Received: 18 February 1999; accepted: 23 December 2000)

Abstract: Let R be a local Artin ring with maximal ideal $\mathfrak{m}$ and residue class field of characteristic $p > 0$. We show that every finite flat group scheme over R is annihilated by its rank, whenever $\mathfrak{m}^p = p\mathfrak{m} = 0$. This implies that any finite flat group scheme over an Artin ring the square of whose maximal ideal is zero, is annihilated by its rank.

Mathematics Subject Classifications (2000). Primary 14L15; Secondary 16W30, 13D10.

Key words. group scheme, Hopf algebra, deformations.

1. Introduction

By Lagrange's theorem, every finite group G of order n has the property that $g^n = 1$ for every $g \in G$. One could ask whether a similar theorem is true for a finite locally free group scheme G of rank n over a base scheme X. Let $[n]\colon G \to G$ be the composite of the diagonal and multiplication morphisms $G \to G^n$ and $G^n \to G$.

QUESTION. Is G annihilated by n? In other words, does the morphism $[n]$ factor as $G \to X \xrightarrow{e} G$ where $e\colon X \to G$ is the unit section of G?

P. Deligne showed in 1969 that the answer to the question is affirmative whenever G is a commutative group scheme [8, p. 4] or [9, (3.8)]. His result holds for an arbitrary base X. It is known that a non-commutative group scheme is annihilated by its rank when X is the spectrum of a field or, more generally, when the base scheme X is reduced [4, Exp. VII$_A$ Prop. 8.5]. This is also an easy consequence of our Proposition 2.1. The general problem is still open [8, Remark p. 5] or [9, (3.8)]. "Il serait intéressant de trouver une démonstration dans ce cas général", A. Grothendieck writes in SGA 3 [4, Exp. VIII, Remarque 7.3.1].

In this paper we answer the question in a special case. To explain our result, we note that it suffices to consider the case where the base scheme X is the spectrum of a local ring R. Then $G = \mathrm{Spec}(A)$ where A is a finite free R-algebra of rank n. The group scheme G is determined by the R-Hopf algebra structure of A. Choosing an R-basis for A, this structure can be specified by a finite number of matrices with entries in R. Replacing R by the subring generated by these entries and localizing once again, we may assume that G is a finite free or, equivalently, flat group scheme

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

over a local Noetherian ring R. By Krull's Theorem we may even assume that R is a local Artin ring. This opens the possibility to proceed by induction with respect to the length of R. When the length is one, R is a field and the answer to Grothendieck's question is affirmative.

In this paper we deal with Artin rings of length larger than 1. In particular, we answer the question affirmatively for Artin rings the square of whose maximal ideal is zero. Artin rings of length 2 are a special case. Our main result is the following.

THEOREM 1.1. *Let R be a local Artin ring with maximal ideal $\mathfrak{m}$ and residue field of characteristic $p > 0$. Suppose that $\mathfrak{m}^p = p\mathfrak{m} = 0$. Then every finite flat group scheme over R is annihilated by its rank.*

COROLLARY 1.2. *Let R be a local Artin ring with maximal ideal $\mathfrak{m}$ satisfying $\mathfrak{m}^2 = 0$. Then every finite flat group scheme over R is annihilated by its rank.*

Indeed, if the characteristic of the residue field is positive, the result follows from Theorem 1.1. On the other hand, if the characteristic of the residue field k of R is zero, the reduced group scheme $G \otimes k$, and hence G itself, is necessarily étale [10, 11.4]. By ordinary group theory $G \otimes \bar{k}$ is annihilated by its rank. Therefore so is $G \otimes k$. Since reduction modulo $\mathfrak{m}$ induces an equivalence between the categories of finite étale group schemes over R and k respectively [3, I.6.1], it follows that G is annihilated by its rank as well.

If the characteristic of the ring R itself is equal to $p > 0$, then Theorem 1.1 says the following.

COROLLARY 1.3. *Let R be a local Artin ring of characteristic $p > 0$. If the maximal ideal $\mathfrak{m}$ of R satisfies $\mathfrak{m}^p = 0$, then every finite flat group scheme over R is annihilated by its rank.*

The proof of Theorem 1.1 is given in Section 4. The strategy is as follows. As is explained in Section 4, it suffices to prove the theorem for local group schemes over local Artin rings with algebraically closed residue field k of characteristic $p > 0$. The rank of such group schemes is a power of p. It is not difficult to see that the theorem holds for local group schemes of rank p^n that have the property that their reductions over the residue field k are already annihilated by p^{n-1}. Therefore we study in Section 2 local group schemes over an algebraically closed field k of rank p^n that are *not* annihilated by p^{n-1}. The main result is Proposition 2.3. It is the critical ingredient for the proof of Theorem 1.1. Proposition 2.3 implies that there are only two types of exceptions. In Section 3 we show that the exceptional group schemes only allow trivial flat deformations. Since group schemes over k are annihilated by their ranks, this implies Theorem 1.1.

For the ring $k[\varepsilon]$, $\varepsilon^2 = 0$, a proof of Corollary 1.2 was obtained earlier, jointly with Fabrizio Andreatta. I would like to thank Fabrizio Andreatta, Francesco

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

Baldassarri, Cornelius Greither, Ben Moonen and the referee for their useful remarks concerning this paper.

2. Group Schemes over Fields

In this section we consider finite group schemes over an algebraically closed field of characteristic $p > 0$. The first proposition was explained to me by Bas Edixhoven.

PROPOSITION 2.1. *Let $G = \mathrm{Spec}(A)$ be a finite free group scheme over a ring R. Let $I \subset A$ denote the augmentation ideal of A. Let p be a prime and let $[p]\colon A \to A$ denote the algebra morphism corresponding to the morphism $[p]\colon G \to G$. Then $[p](I) \subset pI + I^p$.*

Proof. Since $pI = pA \cap I$ we may replace R by the ring R/pR and show that $[p](I) \subset I^p$. Let q denote the rank of G. Consider the closed immersion of G into the linear group GL_q that is induced by the action of G on its Hopf algebra A via left translations [10, 3.4]. Let $B = R[Y_{11}, \ldots, Y_{1q}, \ldots, Y_{q1}, \ldots, Y_{qq}, 1/\det(Y_{ij})]$, equipped with the obvious comultiplication morphism, be the Hopf algebra of the group scheme GL_q and let $\varphi\colon B \to A$ be the surjective morphism of Hopf algebras corresponding to the immersion $G \hookrightarrow \mathrm{GL}_q$. Let σ be the $q \times q$-matrix given by

$$\sigma = \begin{pmatrix} Y_{11} & \cdots & Y_{1q} \\ \vdots & & \vdots \\ Y_{q1} & \cdots & Y_{qq} \end{pmatrix}.$$

The entries of the matrix $\sigma - \mathrm{id}$ generate the augmentation ideal I' of B and, hence, the entries of $\sigma^p - \mathrm{id} = (\sigma - \mathrm{id})^p$ generate $[p](I')$. This means that $[p](I') \subset I'^p$. Applying φ we find that $[p](I) \subset I^p$ as required.

The following well-known fact is an easy corollary:

COROLLARY 2.2. *Finite group schemes over fields are annihilated by their ranks.*

Proof. It suffices to show this when the ground field is algebraically closed. Then there is for any finite group scheme G an exact sequence of group schemes

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0,$$

where G^0 denotes the connected component of G and $G^{\text{ét}}$ its largest étale quotient. By ordinary group theory, $G^{\text{ét}}$ is annihilated by its rank. Therefore it suffices to show that any local group scheme $G = \mathrm{Spec}(A)$ over an algebraically closed field k of characteristic $p > 0$ is annihilated by its rank. By [10, 14.4], the Hopf algebra A of such a group scheme is a local Artin k-algebra of dimension a power of p. Let p^n denote the rank of G. Then the augmentation ideal I of A satisfies $I^{p^n} = 0$. Proposition 2.1 then implies that $[p^n](I) = 0$. Therefore the morphism $[p^n]\colon A \to A]$ factors through $A/I = k$ and so G is killed by p^n, as required.

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

In the remainder of this section we study finite *local* group schemes of rank p^n over an algebraically closed field k of characteristic p. By Corollary 2.2, such group schemes are killed by p^n. The next proposition determines all finite local group schemes that are not annihilated by any smaller power of p.

PROPOSITION 2.3. *Let k be an algebraically closed field of characteristic p. Suppose G is a local group scheme over k of rank p^n that is not annihilated by p^{n-1}. Then G is isomorphic to one of the following group schemes.*

(i) μ_{p^n}, *its Hopf algebra being isomorphic to* $k[X]/(X^{p^n})$;
(ii) *the closed subgroup of* GL_2 *given by*

$$\left\{\begin{pmatrix} 1 & X \\ 0 & 1+Y \end{pmatrix} : X^p = 0 \quad \text{and} \quad Y^{p^{n-1}} = 0\right\};$$

in this case there is an exact sequence

$$0 \to \alpha_p \to G \to \mu_{p^{n-1}} \to 0$$

and the Hopf algebra of G is isomorphic to $k[X, Y]/(X^p, Y^{p^{n-1}})$.

Proof. Case: $n = 1$. The proposition is true, because, up to isomorphism, the only local group schemes of order p over k are μ_p and α_p.

Case: $n = 2$. We claim that G is an extension of one group scheme of order p by another. Indeed, by [10, 14.4] the Hopf algebra of G is isomorphic to either $k[X]/(X^{p^2})$ or $k[X, Y]/(X^p, Y^p)$. In the first case the kernel of the Frobenius morphism is a normal finite subgroup scheme of G of rank p. In the second case, we consider the p-Lie algebra L corresponding to G. It has dimension 2. If L is commutative, the operation $x \mapsto x^{(p)}$ is p-linear. Therefore there is an eigenvector and this eigenvector and this eigenvector generates a one-dimensional p-Lie ideal of L. If L is not commutative, then we can choose a k-basis $\mathbf{e}_1$, $\mathbf{e}_2$ of L so that $[\mathbf{e}_1, \mathbf{e}_2] = \mathbf{e}_1$. In the notation of [4, Chap. VII$_A$, 5], let $\mathbf{e}_1^{(p)} = \lambda\mathbf{e}_1 + \mu\mathbf{e}_2$ for certain $\lambda, \mu \in k$. Then

$$\mu\mathbf{e}_1 = [\mathbf{e}_1, \lambda\mathbf{e}_1 + \mu\mathbf{e}_2] = [\mathbf{e}_1, \mathbf{e}_1^{(p)}] = [\mathbf{e}_1, \mathbf{e}_1]^{(p)} = 0.$$

This shows that $\mathbf{e}_1^{(p)} \in k\mathbf{e}_1$ and, hence, that $\mathbf{e}_1$ generates a one-dimensional p-Lie ideal of L. By [2, II,7.4.3.e] the one-dimensional p-Lie ideal corresponds in either case to a normal subgroup scheme of G of order p.

It follows that G is an extension of one group scheme of rank p by another. Since k is algebraically closed, the only local group schemes of rank p are, up to isomorphism, μ_p and α_p. We discuss all four possibilities:

(i) $0 \to \mu_p \to G \to \alpha_p \to 0$,
(ii) $0 \to \mu_p \to G \to \mu_p \to 0$,
(iii) $0 \to \alpha_p \to G \to \alpha_p \to 0$,

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

(iv) $0 \to \alpha_p \to G \to \mu_p \to 0$.

As in [2, III] we write $\tilde{\mathrm{Ex}}^1(H, A)$ for the group of extensions of an fppf sheaf of groups H by an fppf sheaf A of H-modules. We remark that any such extension is an A-torsor over H. Therefore, if H and A are represented by group schemes and H is affine, any such extension is represented by an a group scheme as well [2, III, Prop. 4.1.9].

(i) Since the automorphism group of μ_p is étale, the group scheme α_p acts trivially on μ_p. By [2, Chap. III, 6.8.6], the extension group $\tilde{\mathrm{Ex}}^1(\alpha_p, \mu_p)$ is isomorphic to the additive group k/k^p which is trivial because k is algebraically closed. We conclude that every finite flat group scheme that is an extension of α_p by μ_p, is necessarily a direct product and hence killed by p.

(ii) Since k is algebraically closed, any group scheme that admits a filtration with normal subgroup schemes with successive quotients isomorphic to μ_p, is commutative and is isomorphic to a direct product of group schemes of the form μ_{p^m}, $m \geqslant 1$. See [2, Chap. III, 1.4.5 and 6.8.7] for this fact. Therefore, we have $G \cong \mu_p \times \mu_p$ or $G \cong \mu_{p^2}$.

(iii) In this case G is an extension of α_p by α_p. By [2, Chap. III, 6.7.7], the extension group $\tilde{\mathrm{Ex}}^1(\alpha_p, \alpha_p)$ is a k-vector space of dimension 2. The Hopf algebra of the corresponding extensions are isomorphic to $k[X, Y]/(Y^p - aX, X^p)$ with group law

$$(X, Y) + (X', Y') = (X + X', Y + Y' + bW(X, X')), \quad (a, b \in k).$$

Here $W(X, X') \in \mathbf{Z}[X, X']$ denotes the polynomial

$$W(X, X') = \frac{(X + X')^p - X^p - X'^p}{p}.$$

Since $[m](X, Y) = (mX, mY)$ for each $m \in \mathbf{Z}$, each extension is annihilated by p.

(iv) Finally we consider extensions of μ_p by α_p. It is just as easy and more convenient to consider, more generally, extensions of μ_{p^m} by α_p for arbitrary $m \geqslant 1$. We write $\alpha_p = \mathrm{Spec}(k[X]/(X^p))$ with the additive group law and $\mu_{p^m} = \mathrm{Spec}(k[Y]/(Y^{p^m}))$ with the group law given by the formula $Y + Y' + YY'$. The possible actions of μ_{p^m} on α_p correspond to the algebra homomorphisms $k[X]/(X^p) \to k[X, Y]/(X^p, Y^{p^m})$ given by $X \mapsto (1 + Y)^\lambda X$ for some unique $\lambda \in \mathbf{Z}/p^m\mathbf{Z}$. By [2, III, 6.7.8] the extension group $\tilde{\mathrm{Ex}}^1(\mu_{p^m}, \alpha_p)$ is trivial for any of these actions. Therefore any extension G of μ_{p^m} by α_p has its Hopf algebra isomorphic to $k[X, Y]/(X^p, Y^{p^m})$ with group law

$$(X, Y) + (X', Y') = (X'(1 + Y)^\lambda + X, Y + Y' + YY'),$$

for some unique $\lambda \in \mathbf{Z}/p^m\mathbf{Z}$. Thus

$$[p^l](X, Y) = \left(X \frac{(1 + Y^{p^l})^\lambda - 1}{(1 + Y)^\lambda - 1}, Y^{p^l} \right)$$

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

for any $l \geqslant 1$. So we have that

$$[p^m](X, Y) = (uT^{p^{m+i}-p^i}X, 0),$$

while $[p^{m+1}](X, Y) = (0, 0)$. Here p^i is the exact power of p dividing λ and u is some unit in the ring $k[Y]/(Y^{p^m})$. Since $p^{m+i} - p^i \geqslant p^m$ when $i \geqslant 1$, we see that $[p^m]$ kills G whenever p divides λ. So, if we insist that p^m not kill G, we must take $\lambda \in (\mathbf{Z}/p^m\mathbf{Z})^*$. All group schemes with $\lambda \in (\mathbf{Z}/p^m\mathbf{Z})^*$ are isomorphic, so we may take $\lambda = 1$. Finally, since

$$\begin{pmatrix} 1 & X \\ 0 & 1+Y \end{pmatrix}\begin{pmatrix} 1 & X' \\ 0 & 1+Y' \end{pmatrix} = \begin{pmatrix} 1 & X+X'+X'Y \\ 0 & 1+Y+Y'+YY' \end{pmatrix}$$

we see that G is isomorphic to the matrix group scheme described in the statement of the Proposition.

This proves the proposition for $n = 2$.

Case: $n > 2$. By [10, 14.4], there are exponents $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_t \geqslant 1$ so that the Hopf algebra of G is isomorphic to $k[X_1, \ldots, X_t]/(X_1^{p^{e_1}}, \ldots, X_t^{p^{e_t}})$. The rank of G is p^n with $n = e_1 + \cdots + e_t$. If $t \geqslant 3$ or if $t = 2$ and $e_1, e_2 \geqslant 2$, we have $\sum_{i=1}^{t}(p^{e_i} - 1) \leqslant p^{n-1} - 1$. This implies that every monomial of degree p^{n-1} is zero and hence that the p^{n-1}-th power of the augmentation ideal I vanishes. By Proposition 2.1 this implies that $[p^{n-1}](I) \subset I^{p^{n-1}} = 0$. Therefore either $t = 1$ or $t = 2$ and one of e_1, e_2 is equal to 1. This means that the Hopf algebra of G is isomorphic to either $k[X]/(X^{p^n})$ or $k[X, Y]/(X^p, Y^{p^{n-1}})$.

In either case there exists a filtration

$$0 = N_0 \subset N_1 \subset \cdots \subset N_n = G$$

with finite closed subgroup schemes that are normal in G and with successive quotients N_{k+1}/N_k of rank p. To see this, we consider the subgroup schemes that are defined by the kernels of the powers of the Frobenius morphism. These give at once the required filtration when A is isomorphic to $k[X]/(X^{p^n})$. In the case $A \cong k[X, Y]/(X^p, Y^{p^{n-1}})$, however, the first step is the kernel of Frobenius and this is a normal subgroup scheme $H \hookrightarrow G$ of rank p^2. Its Hopf algebra is isomorphic to $k[X, Y]/(X^p, Y^p)$. Since p^{n-1} does not kill G, the group scheme H is not killed by p. By the discussion of the case $n = 2$ above, this means that H is isomorphic to the matrix group of order p^2 described in part (iv) of the proof for the case $n = 2$:

$$H \cong \left\{ \begin{pmatrix} 1 & X \\ 0 & 1+Y \end{pmatrix} : X^p = 0 \quad \text{and} \quad Y^{p^{n-1}} = 0 \right\}.$$

The subgroup scheme K of H given by the equation $Y = 0$ is isomorphic to α_p. It is a normal subgroup scheme of H. Actually, somewhat more is true.

CLAIM. *The group scheme K is normal in G.*

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

Proof. Let R be a finite local k-algebra and consider the exact sequence

$$0 \longrightarrow \mathrm{Hom}_R((K/H) \otimes R, \mathbf{G}_m \otimes R)$$
$$\longrightarrow \mathrm{Hom}_R(H \otimes R, \mathbf{G}_m \otimes R) \xrightarrow{g} \mathrm{Hom}_R(K \otimes R, \mathbf{G}_m \otimes R).$$

Here all tensor products are taken with respect to k. The map g is trivial. Indeed, let $\chi\colon H \otimes R \to \mathbf{G}_m \otimes R$ be a homomorphism and let $h(X, Y)$ be the corresponding unit in the Hopf algebra $R[X, Y]/(X^p, Y^p)$ of $H \otimes R$. Then $h(X, 0) \in (R[X]/(X^p))^*$ is the unit corresponding to $g(\chi)$. We have that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1+Y \end{pmatrix}^{-1} \begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1+Y \end{pmatrix} = \begin{pmatrix} 1 & X(1+Y) \\ 0 & 1 \end{pmatrix}$$

and, hence, since $\mathbf{G}_m$ is commutative,

$$h(X(1+Y), Y) = h(X, Y), \quad \text{in } R[X, Y]/(X^p, Y^p).$$

Reducing this relation modulo Y^2 shows that the derivative of $h(X, 0)$ vanishes. This implies that $h(X, 0)$ is a polynomial in X^p. Therefore it is constant and hence 1.

This means that every homomorphism $\chi\colon H \otimes R \to \mathbf{G}_m \otimes R$ factors through $(H/K) \otimes R$. Since $H/K \cong \mu_p$, every such homomorphism is therefore given by

$$\chi\colon \begin{pmatrix} 1 & X \\ 0 & 1+Y \end{pmatrix} \mapsto (1+Y)^i, \quad \text{for some } i \in \mathbf{Z}/p\mathbf{Z}.$$

The non-constant homomorphisms all have kernel $K \otimes R$. Since any automorphism of $H \otimes R$ permutes the non-constant homomorphisms $H \otimes R \to \mathbf{G}_m \otimes R$, the subgroup scheme $K \otimes R$ is stable under automorphisms. Since this is so for every finite local k-algebra R, the same is true for every finitely generated k-algebra R and this means that K is normal in G. It follows that $0 \subset K \subset H \subset \cdots \subset G$ is a filtration of G of the required form.

Therefore there exists in either case a filtration

$$0 = N_0 \subset N_1 \subset \cdots \subset N_n = G$$

with normal subgroup schemes N_k and with N_{k+1}/N_k of rank p. Since p^{n-1} does not annihilate G, no extension of any two successive steps in this filtration is annihilated by p. By case (i) of the discussion of the case $n = 2$ above, we conclude that there is an exact sequence

$$0 \to H_1 \to G \to H_2 \to 0,$$

where H_1 can be filtered with α_p's and H_2 can be filtered with μ_p's. Moreover, by (iii) above, the filtration of H_1 consists of at most one step. Therefore by (ii) above and [2, IV.1.4.5], either H_1 is trivial and H_2 is isomorphic to μ_{p^n}, or $H_1 \cong \alpha_p$ and $H_2 \cong \mu_{p^{n-1}}$ and G is isomorphic to the matrix group described in case (iv) above.

This proves the proposition.

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

3. A Matrix Group Scheme

Let k be a field of characteristic $p > 0$. In this section the field k needs *not* be algebraically closed. We study a rather special matrix group scheme, or rather a family of such group schemes. It shows up in the proof of Theorem 1.1. Let $m \geqslant 1$ and let G_0 be the matrix group scheme over k given by

$$\left\{ \begin{pmatrix} 1 & X \\ 0 & 1+Y \end{pmatrix} : X^p = 0 \quad \text{and} \quad Y^{p^m} = 0 \right\}.$$

The Hopf algebra A_0 of G_0 is isomorphic to $k[X, Y]/(X^p, Y^{p^m})$. This group scheme occurs in Proposition 2.3(ii). We show that the group scheme G_0 cannot be non-trivially deformed. More precisely, we show that after a faithfully flat extension, every deformation to a local Artin ring R is a base change of G_0 itself. For $m = 1$, the group scheme G_0 has rank p^2 and is discussed in [7, Example $-B$]. Our Proposition 3.3 makes the statements there more precise. Moreover, for $m = 1$ our proof also shows that the deformation of G_0 to R itself is already trivial; it is not necessary to make the faithfully flat extension.

The proof of Proposition 3.3 is based on the computation of the Hochschild cohomology groups $H^i(G_0, V)$ of certain representations V of G_0. To compute these, we use the exact sequence

$$0 \to \alpha_p \to G_0 \to \mu_{p^m} \to 0).$$

See [6, 4.14] or [2, II.3.1.1] for the definition of the Hochschild cohomology groups. We recall that for any G_0-representation V, the Hochschild cohomology groups $H^i(\alpha_p, V)$ of the normal subgroup scheme α_p are themselves representations of μ_{p^m}.

LEMMA 3.1. *For each G_0-representation V the restriction maps*

$$H^i(G_0, V) \xrightarrow{\cong} H^i(\alpha_p, V)^{\mu_{p^m}}$$

are isomorphisms for all $i \geqslant 0$.

Proof. Since μ_{p^m} is diagonalizable, the required isomorphisms are provided by [6, Cor.6.9]. Indeed, the isomorphisms there are the edge maps of the degenerating Hochschild-Serre spectral sequence and by [6, Remark on p. 99] these coincide with the restriction maps.

Next we compute certain Hochschild cohomology groups of two 2-dimensional representations of G_0. We let V denote the adjoint representation. This is a 2-dimensional representation, dual to the representation I/I^2. Here I denotes the augmentation ideal of the Hopf algebra of G_0.

One easily checks that, with respect to a suitable basis, the matrix $\left(\begin{smallmatrix} 1 & X \\ 0 & 1+Y \end{smallmatrix}\right)$ acts on V as $\left(\begin{smallmatrix} (1+Y)^{-1} & X(1+Y)^{-1} \\ 0 & 1 \end{smallmatrix}\right)$. On the other hand, $V^{(p)}$ denotes the two-dimensional representation for which the action is given by $\left(\begin{smallmatrix} 1+Y^p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$. Finally, one checks that

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

the action by conjugation on the normal subgroup scheme α_p is by multiplication by $(1+Y)^{-1}$.

LEMMA 3.2. *We have the following:*

(i) $H^1(G_0, V^{(p)}) = 0$;
(ii) $H^1(G_0, V) = H^2(G_0, V) = 0$.

Proof. (i) The representation $V^{(p)}$ is a sum of a 1-dimensional representation k with trivial action and of $k^{(p)}$ which has a 'twisted' action. We show that both groups $H^1(G_0, k)$ and $H^1(G_0, k^{(p)})$ vanish.

The cohomology group $H^1(\alpha_p, k)$ is the k-vector space generated by the natural inclusion $\alpha_p \hookrightarrow \mathbf{G}_a$. The action of μ_{p^m} on α_p via conjugation is a morphism $\mu_{p^m} \times \alpha_p \to \alpha_p$. The corresponding k-algebra homomorphism $k[X]/(X^p) \to k[X, Y]/(X^p, Y^{p^m})$ is given by $X \mapsto X(1+Y)^{-1}$. The action of μ_{p^m} on k and $k^{(p)}$ are morphisms $\mu_{p^m} \times \mathbf{G}_a \to \mathbf{G}_a$ with corresponding k-algebra homomorphisms $k[X] \to k[X, Y]/(Y^{p^m})$ given by $X \mapsto X$ and $X \mapsto X(1+Y^p)^{-1}$ respectively.

A 1-cocycle of α_p with values in k or $k^{(p)}$ is invariant under the action of μ_{p^m} if and only if it is compatible with the actions of G_0 on α_p and on k and $k^{(p)}$, respectively. Since $XY \neq 0$ and $XY \neq XY^p$ in the ring $k[X, Y]/(X^p, Y^{p^m})$ and since all 1-coboundaries are zero, we see that the generator of $H^1(\alpha_p, k)$ is not invariant in either case. Part (i) now follows from Lemma 3.1.

(ii) For the proof of Proposition 3.3 we only use the fact that $H^2(G_0, V)$ vanishes. Therefore we leave the easier proof that $H^1(G_0, V) = 0$ to the reader. We have the following exact sequence of G_0-representations

$$0 \to k^{(1)} \to V \to k \to 0.$$

Here $k^{(1)}$ denotes the one-dimensional representation of G with action $G \times \mathbf{G}_a \to \mathbf{G}_a$ corresponding to the morphism $k[T] \to k[T, X, Y]/(X^p, Y^{p^m})$ given by $T \mapsto (1+Y)^{-1}T$. Using Lemma 3.1 and the long cohomology sequence of G_0-cohomology groups, we obtain the following exact sequence

$$\cdots \to H^2(\alpha_p, k^{(1)})^{\mu_{p^m}} \to H^2(G_0, V) \to H^2(\alpha_p, k)^{\mu_{p^m}} \xrightarrow{\partial} H^3(\alpha_p, k^{(1)})^{\mu_{p^m}} \to \cdots$$

The cohomology group $H^2(\alpha_p, k^{(1)})$ is a one-dimensional k-vector space generated by the 2-cocycle $\alpha_p \times \alpha_p \to \mathbf{G}_a$ given by $(X, X') \mapsto W(X, X')$ where W denotes the polynomial introductedin Section 2. See [2, Chap. II, 3.4.8]. The action of μ_{p^m} on $\alpha_p \times \alpha_p$ corresponds to the k-algebra homomorphism $k[X, X']/(X^p, X'^p) \to k[X, X', Y]/(X^p, X'^p, Y^{p^m})$ given by $(X, X') \mapsto ((1+Y)^{-1}X, (1+Y)^{-1}X')$. It maps $W(X, X')$ to $(1+Y^p)^{-1}W(X, X')$. On the other hand, the action of μ_{p^m} on $k^{(1)}$ corresponds to the k-algebra homomorphism $k[T] \to k[T, Y]/(Y^{p^m})$ given by $T \mapsto (1+Y)^{-1}T$. Since $W(X, X')Y \neq W(X, X')Y^p$ in $H^2(\alpha_p, k^{(1)}) \otimes k[Y]/(Y^{p^m})$, the actions are incompatible and $H^2(\alpha_p, k^{(1)})^{\mu_{p^m}} = 0$.

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

Part (ii) would now follow if the group $H^2(\alpha_p, k)^{\mu_{p^m}}$ were also zero. Since this is only true for $m \geqslant 2$, we show below instead that the connecting homomorphism $\partial H^2(\alpha_p, k) \to H^3(\alpha_p, k^{(1)})$ is injective. To see the effect of ∂, let $F(X, X')$ be a 2-cocycle in $H^2(\alpha_p, k)$ and lift it to the morphism

$$\begin{pmatrix} 0 \\ F(X, X') \end{pmatrix} : \alpha_p \to V.$$

Since the action of α_p on V is via the matrix $\left(\begin{smallmatrix} 1 & X \\ 0 & 1 \end{smallmatrix}\right)$, the 3-cocycle $\partial F(X, X')$ in $H^3(\alpha_p, k^{(1)})$ is the first coordinate of

$$\begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ F(X', X'') \end{pmatrix} - \begin{pmatrix} 0 \\ F(X + X', X'') \end{pmatrix} + \begin{pmatrix} 0 \\ F(X, X' + X'') \end{pmatrix} - \begin{pmatrix} 0 \\ F(X', X'') \end{pmatrix}$$

which is simply $XF(X', X'')$. Since $H^2(\alpha_p, k)$ is a one-dimensional vector space generated by $W(X, X')$, the map ∂ is injective if and only if $\partial W \neq 0$. Suppose therefore that $\partial W(X, X', X'') = XW(X', X'') = 0$ in $H^3(\alpha_p, k^{(1)})$. This means that for some polynomial f we have that

$$XW(X', X'') = f(X', X'') - f(X + X', X'') + f(X, X' + X'') - f(X, X')$$

in the ring $k[X, X', X'']/(X^p, X'^p, X''^p)$. We replace f by its homogenous degree $p + 1$ part. Since $X^p = X'^p = 0$, this means that $f = 0$ when $p = 2$. Since $XW(X', X'') = XX'X'' \neq 0$ we see that ∂ is injective in this case. When $p \neq 2$, we have that $f(X, X') = a_{p-1}X^{p-1}X'^2 + \cdots + a_2X^2X'^{p-1}$ for certain coefficients $a_i \in k$. We differentiate the relation with respect to X and substitute $X = 0$. This gives

$$W(X', X'') = -f_x(X', X'') + f_x(0, X' + X'') - f_x(0, X'')$$

and, hence, since

$$f_x(X, X') = (p - 1)a_{p-1}X^{p-2}X'^2 + \cdots + 2a_2XX'^{p-1},$$

we find that

$$-W(X', X'') = (p - 1)a_{p-1}X'^{p-2}X''^2 + \cdots + 2a_2X'X''^{p-1}.$$

But this is impossible since the $X'^{p-1}X''$ term of $W(X', X'')$ is missing on the right hand side. This shows that $\partial W \neq 0$ and hence that ∂ is injective.

Lemma 3.1 now implies that $H^2(G_0, V) = 0$ and part (ii) follows.

The main result of this section says that, after a finite faithfully flat extension, any flat deformation of G_0 is a base change of the k-group scheme G_0. In particular, G_0 can only be deformed to rings of characteristic p.

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

PROPOSITION 3.3. *Let R be a local Artin ring with maximal ideal $\mathfrak{m}$ and residue field k of characteristic p. Let $G = \mathrm{Spec}(A)$ be a finite flat group scheme over R for which $G \otimes_R k$ is isomorphic to the group scheme G_0. Then*

(i) *the characteristic of R is p;*
(ii) *for some R-algebra S of the form $R[T_1, \ldots, T_r]/(T_1^p - \varphi_1, \ldots, T_r^p - \varphi_r)$ with polynomials $\varphi_i \in R[T_1, \ldots, T_r]$ having coefficients in $\mathfrak{m}$, the S-group scheme $G \otimes_R S$ is isomorphic to $G_0 \otimes_k S$.*

Proof. We proceed by induction with respect to the length of R. If the length of R is 1, we take $S = R = k$ and everything is trivially true. Suppose the length is at least 2. Then we can pick a non-zero element $\pi \in \mathrm{Ann}(\mathfrak{m})$. Applying the induction hypothesis to $R/\pi R$ we find that

(i) $p = \gamma\pi$ for some $\gamma \in R$;
(ii) there is an $R/\pi R$-algebra $S' = (R/\pi R)[T_1, \ldots, T_r]/(T_1^p - \varphi_1', \ldots, T_r^p - \varphi_r')$ with polynomials φ_i' that have their coefficients in $\mathfrak{m}$, for which the S'-group scheme $G \otimes_R S'$ is isomorphic to $G_0 \otimes_k S'$.

We lift the polynomials $\varphi_i' \in (R/\pi R)/[T_1, \ldots, T_r]$ to polynomials $\varphi_i \in R[T_1, \ldots, T_r]$ by lifting the coefficients to R. Let S be the R-algebra given by $S = R[T_1, \ldots T_r]/(T_1^p - \varphi_1, \ldots, T_r^p - \varphi_r)$. It is easy to see that S is a finite free local R-algebra. By construction, $S/\pi S \cong S'$ and hence $(A \otimes_R S)/\pi(A \otimes_R S) \cong A \otimes_R S'$. It follows by induction that

$$A \otimes_R S \cong S[X, Y]/(X^p - \pi f(X, Y), Y^{p^m} - \pi g(X, Y))$$

for certain $X, Y \in A \otimes_R S$ that lift the variables X and Y in A_0 and certain polynomials $f, g \in (S/\mathfrak{m}S)[X, Y]$. Since $\pi^2 = 0$, we may assume that f and g have degree less than p in X and less that p^m in Y. Moreover, the group law of $G \otimes_R S$ is given by

$$(X, Y) + (X', Y') = (X + X' + XY' + \pi h_1(X, X', Y, Y'), \\ Y + Y' + YY' + \pi h_2(X, X', Y, Y'))$$

for certain polynomials $h_1, h_2 \in (S/\mathfrak{m}S)[X, Y, X', Y']/(X^p, Y^{p^m}, X'^p, Y'^{p^m})$. Since the comultiplication is an R-algebra homomorphism and since $p \in (\pi) \subset \mathrm{Ann}(\mathfrak{m})$, we find that

$$\begin{aligned} &(X + X' + XY')^p - \pi f(X + X' + XY', Y + Y' + XY') = 0, \\ &(Y + Y' + YY')^{p^m} - \pi g(X + X' + XY', Y + Y' + YY') = 0 \end{aligned} \qquad (*)$$

in the ring $A \otimes_R A \otimes_R S$. We subtract the equations $(X^p - \pi f(X, Y))(1 + Y')^p = 0$ and $X'^p - \pi f(X', Y') = 0$ from the first equation. In this way we obtain a relation all of whose coefficients are contained in πS. Dividing by π in the flat R-algebra

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

S we find the following relation

$$\gamma W(X + XY', X') = f(X + X' + XY', Y + Y' + YY') - f(X, Y) - f(X', Y') - Y'^p f(X, Y)$$

in the k-algebra $(S/\mathfrak{m}S)[X, Y, X', Y']/(X^p, Y^{p^m}, X'^p, Y'^{p^m})$. Next we put $Y = Y' = 0$ and we obtain the following relation in the ring $(S/\mathfrak{m}S)[X, X']/(X^p, X'^p)$:

$$\gamma W(X, X') = f(X + X', 0) - f(X, 0) - f(X', 0).$$

Since $f(X, 0)$ has degree at most $p - 1$, the term $X'X^{p-1}$ does not occur on the right hand side. since it occurs on the left with coefficient γ, we conclude that $\gamma = 0$ in $S/\mathfrak{m}S$ and hence that $p = \gamma\pi = 0$ in S. Since S is free over R, this implies that the characteristic of R is equal to p as well. This proves (i).

We now have

$$f(X + X' + XY', Y + Y' + YY') = f(X, Y) + f(X', Y') + Y'^p f(X, Y),$$
$$g(X + X' + XY', Y + Y' + YY') = g(X, Y) + g(X', Y'),$$

in the k-algebra $(S/\mathfrak{m}S)[X, Y, X', Y']/(X^p, Y^{p^m}, X'^p, Y'^{p^m})$. The first formula follows from the fact that $\gamma = 0$. The second follows from $(*)$ and the relation $(Y + Y' + YY')^{p^m} = Y^{p^m} + Y'^{p^m} + Y^{p^m} Y'^{p^m} = \pi g(X, Y) + \pi g(X', Y')$. These two formulas express the fact that

$$F(X, Y) = \begin{pmatrix} 1 + Y^p & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} f(X, Y) \\ g(X, Y) \end{pmatrix}$$

is a 1-cocycle $G_0 \to V^{(p)}$, where $V^{(p)}$ denotes the rank 2 module of Lemma 3.2. By part (i) of this Lemma, $H^1(G_0 \otimes + kS/\mathfrak{m}S, V^{(p)} \otimes_k S/\mathfrak{m}S) \cong H^1(G_0, V^{(p)}) \otimes_k S/\mathfrak{m}S = 0$. Therefore this cocycle is a coboundary. In other words, $g(X, Y) = 0$ and $f(X, Y) = cY^p$ for some $c \in S/\mathfrak{m}S$.

We conclude that

$$A \otimes_R S \cong S[X, Y]/(X^p - c\pi Y^p, Y^{p^m}).$$

If $m = 1$ we have that $Y^p = 0$ and hence $A \otimes_R S \cong S[X, Y]/(X^p, Y^p)$. When $m > 1$, we replace S by the faithfully flat S-algebra $S[T]/(T^p - c\pi)$. This algebra is of the form described in condition (ii) and, replacing X by $X - TY$, we see that

$$A \otimes_R S \cong S[X, Y]/(X^p, Y^{p^m}) \cong A_0 \otimes_k S.$$

Therefore, in either case the underlying scheme of $G \otimes_R S$ is isomorphic to $\mathrm{Spec}(A_0 \otimes_k S)$.

By [4, III, Théorème 3.5] with $\underline{I} = \mathfrak{m}$ and $\underline{J} = \pi R$, the set of group scheme structures on $S \otimes_k A_0$ modulo automorphisms that induce the identity modulo π, form a principal homogeneous space over $H^2(G_0, V)$ where V is the adjoint representation of G_0. By Lemma 3.2 (ii) this Hochschild cohomology group vanishes. This shows that the group scheme G is isomorphic to the group scheme $G_0 \otimes_k S$.

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

This proves the proposition.

Note that for $m = 1$ we do not replace S by a faithfully flat extension in the induction step. It follows that for $m = 1$ the Proposition is true with $S = R$. In other words, G itself is already a trivial deformation of G_0.

Remark 3.4. By refining the proof of Proposition 3.3 one can obtain deformation results for the k-subgroup schemes G_0 of GL_2 given by

$$G_0 = \begin{pmatrix} 1 & \alpha_{p^m} \\ 0 & \mu_{p^n} \end{pmatrix}, \quad m, n \geqslant 1.$$

We mention the following result without proof.

THEOREM. *Let R be an local Artin ring with maximal ideal $\mathfrak{m}$ and residue field k of characteristic p. Let G be a flat deformation of G_0 to R. Then*

(i) *the characteristic of R is p;*
(ii) *there is a faithfully flat finite local R-algebra S such that*

$$G \otimes_R S \cong \begin{pmatrix} 1 & N \\ 0 & \mu_{p^n} \end{pmatrix},$$

where N is a flat deformation of α_{p^m}. It is a closed flat subgroup scheme of $\mathbf{G}_a$ given by $H(X) = X^{p^m} + \sum_{i=n}^{m-1} b_i X^{p^i} = 0$ for certain $b_i \in \mathfrak{m}S$.

In particular, the group schemes G_0 cannot be deformed to rings that do not have characteristic p. Note that μ_{p^n} acts on the subgroup scheme N of part (ii) and that $N \cong \alpha_{p^m}$ whenever $m \leqslant n$. If $m = n$, the proof actually shows that one can take $R = S$ in (ii): in this case, the only deformation of G_0 is $G \cong G_0 \otimes_k R$.

4. Proof of the Theorem

In this section we prove Theorem 1.1. Let G be a finite flat group scheme over a local Artin ring R with residue class field k of characteristic p and maximal ideal $\mathfrak{m}$ satisfying $\mathfrak{m}^p = p\mathfrak{m} = 0$.

By [5, III, Ch. 0, 10.3.1] and [1, II, 3.2, Cor. 2] there exists a local faithfully flat R-algebra whose maximal ideal is generated by $\mathfrak{m}$ and whose residue field is algebraically closed. In order to prove the theorem, we may replace R by this algebra and hence we may assume that k is algebraically closed. Then R is strictly Henselian and there is an exact sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0$$

where G^0 denotes the connected component of G and $G^{\text{ét}}$ its largest étale quotient. By ordinary group theory, $G^{\text{ét}} \otimes k$ is annihilate by its rank. Since reducing modulo $\mathfrak{m}$

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

induces an equivalence of the categories of étale group schemes over k and over R respectively [3, I.6.1], we see that $G^{\text{ét}}$ itself is also annihilated by its rank. Since ranks are multiplicative in exact sequences, we may assume that G is a local group scheme.

Let therefore $G = \mathrm{Spec}(A)$ be a finite flat local group scheme of rank p^n over R. Let I denote the augmentation ideal of A. We want to show that G is annihilated by its rank. This amounts to showing that $[p^n](I) = 0$. First we study the group scheme $G \otimes_R k$. By Corollary 2.2. $G \otimes_R k$ is annihilated by p^n. If it happens to be already annihilated by p^{n-1}, then $[p^{n-1}]$ maps the augmentation ideal I of G into $\mathfrak{m}A \cap I = \mathfrak{m}I$ and Proposition 2.1 implies that

$$[p^n](I) = [p^{n-1}]([p](I)) \subset [p^{n-1}](pI + I^p) \subset p\mathfrak{m}I + (\mathfrak{m}I)^p.$$

Since $p\mathfrak{m} = \mathfrak{m}^p = 0$, this implies that p^n annihilates G over R and we are done.

Therefore we may assume that $G \otimes_R k$ is not annihilated by p^{n-1}. Since k is algebraically closed, there are by Proposition 2.3 only two possibilities for $G \otimes_R k$:

Case I. $G \otimes_R k$ is isomorphic to μ_{p^n}. This group scheme cannot be deformed non-trivially. More precisely, by [4, Exp. X, Corollaries 2.3 and 2.4], the group scheme G is a multiplicative iso-trivial group scheme over R. Since k is algebraically closed, R is strictly Henselian and we see that G is actually diagonalizable. Therefore $G \cong \mu_{p^n}$ over R. In particular, G is annihilated by p^n.

Case II. $G \otimes_R k$ is isomorphic to the matrix group scheme over k of Proposition 2.3 (ii) with Hopf algebra $k[X, Y]/(X^p, Y^{p^{n-1}})$.

If $n = 1$, this is the group scheme α_p. In this case $G \otimes_R k$ has rank p and so does G over R. This implies that G is commutative [8, Lemma 1]. It follows then from Deligne's result [8, p. 4] that G is annihilated by p.

Suppose now that $n > 1$. In this case we apply Proposition 3.3 to $G_0 = G \otimes_R k$. It follows that after a finite faithfully flat extension S of R, the group scheme G is isomorphic to a base change of G_0. Since the k-group scheme G_0 is annihilate by its rank, the same is true for the S-group scheme $G_0 \otimes_k S \cong G \otimes_R S$. By the faithful flatness of the R-algebra S it follows that G is annihilated by its rank. This completes the proof of Theorem 1.1.

References

1. Bourbaki, N.: *Commutative Algebra* I–VII, Hermann, Paris, 1972.
2. Demazure, M. and Gabriel, P.: *Groupes algébriques* I, Masson, Paris, 1970.
3. Grothendieck, A.: Revêtements étales et groupe fondamental, In: *Sem. de géometrie algébrique du Bois Marie* (1960/61) SGA 1, Lecture Notes in Math. 224, Springer, New York, 1971.
4. Demazure, M. and Grothendieck, A.: Schémas en groups, In: *Sem. de géometrie algébrique du Bois Marie* (1962/64) SGA 3, vols. I, II and III, Lecture Notes in Math. 151, 152 and 153, Springer, New York, 1970.
5. Grothendieck, A. and Dieudonné, J.: Étude cohomologique des faisceaux cohérents, éléments de géometrie algébrique III, *Publ. Math. IHES* **11** (1961), **17** (1963).

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press

6. Jantzen, J. C.: *Representations of Algebraic Groups*, Academic Press, Orlando, 1987.
7. Oort, F. and Mumford, D.: Deformations and liftings of finite commutative group schemes, *Invent. Math.* **5** (1968), 317–334.
8. Tate, J. and Oort, F.: Group schemes of prime order, *Ann. Sci. École Norm. Sup.* **3** (1970), 1–21.
9. Tate, J.: Finite flat group schemes, In: G. Cornell, J. Silverman and G. Stevens (eds), *Modular Forms and Fermat's Last Theorem*, Springer, New York, 1997.
10. Waterhouse, W.: *Introduction to Affine Group Schemes*, Grad. Texts in Math. 66, Springer, New York, 1979.

https://doi.org/10.1023/A:1017560215203 Published online by Cambridge University Press