Preliminary version
December 9, 2017

II Università degli
Studi di Roma

TOR VERGATA

Is a finite locally free group scheme killed by its order?

René Schoof

Dipartimento di Matematica
2ª Università di Roma "Tor Vergata"
I-00133 Roma ITALY
Email: schoof@mat.uniroma2.it

1. Introduction.

Lagrange's Theorem implies that every finite group G of order m has the property that $g^m = 1$ for every $g \in G$. One could ask whether a similar result is true for a finite locally free group scheme G of order m over a base scheme X. Let $[m] : G \longrightarrow G$ be the composite of the diagonal and multiplication morphisms $G \longrightarrow G^m$ and $G^m \longrightarrow G$.

Question. *Is G annihilated by m? In other words, does the morphism $[m]$ factor as $G \longrightarrow X \xrightarrow{e} G$ where $e : X \longrightarrow G$ is the unit section of G?*

Grothendieck wrote in SGA 3 [1, Exp. VIII Remarque 7.3.1]: "*Il serait intéressant de trouver une démonstration dans ce cas général*". The question has been answered affirmatively in two important cases.

In SGA 3 itself one finds a proof of the fact that over a field, any finite group scheme, commutative or not, is annihilated by its order [1, Exp. VII$_A$ Prop.8.5]. This easily implies that the same is true for finite locally free group schemes over a reduced base scheme X. See also [5, (3.8)] and [4, Cor. 2.2]. Pierre Deligne showed in 1969 that the answer to the question is affirmative whenever the group scheme G is commutative [3, p.4] or [5, (3.8)]. His result holds for an arbitrary base X.

The question remains unanswered in general. See [3, Remark p.5] or [5, (3.8)]. An affirmative answer would follow from an affirmative answer in the following special case.

Question'. *Let R be a local Artin ring with residue field of characteristic $p > 0$. Is every finite free local group scheme G over R killed by its order?*

Indeed, in order to answer the first question affirmatively, it suffices to do so for base schemes X that are the spectra of a local rings R. Then $G = \mathrm{Spec}(A)$ where A is a finite free R-algebra. The rank of A is the order of G. The group scheme G is determined by the structure of the R-Hopf algebra A. The Hopf algebra structure of A is given by the multiplication, comultiplication, inverse, unit, coinverse and counit homomorphisms. These are R-linear maps between R, A and $A \otimes_R A$. Choosing an R-basis for A, the group scheme G is determined by the entries of the matrices that correspond to these maps. Replacing R by the subring generated by the entries of the matrices and localizing once again, we may assume that G is a finite free or, equivalently, finite flat group scheme over a local Noetherian ring R. By Krull's Theorem we may even assume that R is a local Artin ring.

Then there is for any finite group scheme G an exact sequence of group schemes

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

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 order.

Since finite group schemes in characteristic zero are étale, we may assume that the characteristic of the residue field of R is $p > 0$, and that G is a local group scheme, as required.

If the maximal ideal $\mathfrak{m}$ of the Artin ring R in the second question is zero, R is a field and the answer is affirmative by the SGA 3 result mentioned above. In [4] it is shown that if

$$\mathfrak{m}^p = p\mathfrak{m} = 0,$$

then every finite free group scheme G over R is also killed by its order. This happens in particular when the maximal ideal $\mathfrak{m}$ satisfies $\mathfrak{m}^2 = 0$.

In this note we give proofs of the two main results mentioned above. In section 2 we prove that finite group schemes over fields are killed by their orders and in section 3 we present Deligne's proof of the fact that finite commutative locally free group schemes are killed by their orders. Finally, in section 4, we outline the proof of the result in [4].

2. Finite group schemes over fields.

In this section we show that finite group schemes over a field are killed by their orders. See [6] for basic facts concerning group schemes. The first proposition was explained to me by Bas Edixhoven several years ago.

Proposition 2.1. *Let $G = \mathrm{Spec}(A)$ be a finite flat group scheme over a ring R. Let $I \subset A$ denote the augmentation ideal of A. Let p be a prime and let $[p] : A \longrightarrow A$ denote the R-algebra morphism corresponding to the morphism $[p] : G \longrightarrow G$. Then*

$$[p](I) \subset pI + I^p.$$

Proof. Since A is a flat R-algebra, we have that $pI = pA \cap I$. Therefore we may replace R by the characteristic p ring R/pR and show that $[p](I) \subset I^p$. Let n denote the rank of G. Consider the closed immersion of G into the linear group GL_n that is induced by the action of G on its Hopf algebra A via left translations [6, 3.4]. Let φ denote the corresponding surjective morphism from the Hopf algebra $B = R[Y_{11}, \ldots, Y_{1n}, \ldots, Y_{n1}, \ldots, Y_{nn}, 1/\det(Y_{ij})]$ of GL_n to the Hopf algebra A of G. The entries of the matrix $\sigma - \mathrm{id}$, where σ is given by

$$\sigma = \begin{pmatrix} Y_{11} & \cdots & Y_{1n} \\ \vdots & & \vdots \\ Y_{n1} & \cdots & Y_{nn} \end{pmatrix},$$

generate the augmentation ideal J of B. So the entries of $\sigma^p - \mathrm{id}$ generate $[p](J)$. Since $=\sigma^p - \mathrm{id} = (\sigma - \mathrm{id})^p$, the usual matrix multiplication formulas show that $[p](J) \subset J^p$. Applying φ, we find that $[p](I) \subset I^p$ as required.

Corollary 2.2. *Finite group schemes over fields are annihilated by their orders.*

Proof. It suffices to show this for an algebraically closed field. By the remarks made in the introduction concerning the connected-étale exact sequence, we may assume that k has characteristic $p > 0$ and that G is local. By [6, 14.4], the order of G is equal to p^m for some $m \geq 0$ and the Hopf algebra A of G is a local Artin k-algebra of dimension p^m. Therefore the augmentation ideal I of A satisfies $I^{p^m} = 0$. Prop.2.1 then implies that $[p^m](I) = 0$. This means that the morphism $[p^m] : A \longrightarrow A$ factors through $A/I = k$, so that G is killed by its order p^m, as required.

3. Commutative group schemes.

Let G be a finite locally free *commutative* group scheme of order m over a base X. In 1969 Deligne showed the following [3, p.4].

Theorem 3.1. *The group scheme G is annihilated by m.*

Any element x of an ordinary finite group of order m, has the property that x^m is equal to the neutral element. For *commutative* groups this can be proved by the following well-known argument: let $P = \prod_x x$ be the product of all elements of the group and let y be an arbitrary element. Then $P = \prod_x x = \prod_x xy = y^m \prod_x x = y^m P$ and hence y^m is equal to the neutral element. Deligne's proof can be said to carry this argument over to *group schemes*.

It suffices to prove Theorem 3.1 for $X = \mathrm{Spec}(R)$ for a ring R and $G = \mathrm{Spec}(A)$ a finite free commutative group scheme over R. For any finite free R-algebra S we have

$$G(S) = \mathrm{Hom}_{\mathrm{alg}}(A, S) \subset \mathrm{Hom}_R(A, S) \cong A' \otimes_R S.$$

Here $\mathrm{Hom}_{\mathrm{alg}}(A, S)$ denotes the set of R-algebra homomorphisms $A \longrightarrow S$ and $\mathrm{Hom}_R(A, S)$ is the R-module of R-module homomorphisms $A \longrightarrow S$. We write A' for $\mathrm{Hom}_R(A, R)$. Since G is commutative, A' carries the structure of an R-algebra, the multiplication $A' \otimes_R A' \longrightarrow A'$ being given by the dual of the comultiplication map $c : A \longrightarrow A \otimes_R A$. Moreover A' is the Hopf algebra of the Cartier dual of G, with comultiplication map $c' : A' \otimes_R A' \longrightarrow A'$ equal to the dual of the multiplication map $m : A \otimes_R A \longrightarrow A$. This easily implies that for any R-algebra S we have

$$G(S) = \{f \in (A' \otimes_R S)^* : c'(f) = f \otimes f\}.$$

One easily checks that the group operation of $G(S)$ coincides with the algebra multiplication in the multiplicative group $(A' \otimes_R S)^*$ of the algebra $A' \otimes_R S$. See [6, 2.4].

For an R-algebra S, the structure morphism $R \longrightarrow S$ gives rise to a group homomorphism $G(R) \longrightarrow G(S)$. When S is finite and free over R, Deligne constructs a *Trace* map $G(S) \longrightarrow G(R)$ in the other direction. To do this he uses the *Norm* map $N : S \longrightarrow R$, which for $s \in S$ is defined as the determinant of any representative matrix of the R-linear multiplication-by-s-map $S \longrightarrow S$.

The norm is multiplicative. It induces for all R-algebras B, norm maps $N_B = \mathrm{id}_B \otimes N$ from $B \otimes_R S$ to B. These are functorial in the sense that for every morphism $f : B \longrightarrow C$ of R-algebras the diagram

$$\begin{array}{ccc} B \otimes_R S & \xrightarrow{f \otimes \mathrm{id}_S} & C \otimes_R S \\ \downarrow N_B & & \downarrow N_C \\ B & \xrightarrow{f} & C \end{array} \qquad (*)$$

commutes.

Lemma 3.2. *Let S be a finite free R-algebra and let $G = \mathrm{Spec}(A)$ as above. Then the norm map $N_{A'} : A' \otimes_R S \longrightarrow A'$ maps $G(S)$ to $G(R)$ and is a group homomorphism.*

$$\begin{array}{ccc} G(S) & \subset & A' \otimes_R S \\ & & \big\downarrow N_{A'} \\ G(R) & \subset & A' \end{array}$$

Proof. Suppose that $a \in G(S) \subset A' \otimes_R S$. So, it is invertible and satisfies $c'(a) = a \otimes a$. Then we have

$$c'(N_{A'}(a)) = N_{A'}(a) \otimes N_{A'}(a).$$

This follows easily from the commutativity of the diagrams $(*)$ applied to the morphisms $A' \longrightarrow A' \otimes_R A'$ given by the maps $a \mapsto a \otimes 1'$, $a \mapsto 1' \otimes a$ and $c'(a)$ respectively. Here $1'$ denotes the unit element of the algebra A'. It is the counit map $e_A : A \longrightarrow R$.

The formula shows that $N_{A'}(a) \in G(R)$. Since the group laws in $G(R)$ and $G(S)$ agree with algebra multiplication in A' and $A' \otimes_R S$ respectively, and since the norm is multiplicative, we see that $N : G(S) \longrightarrow G(R)$ is a group homomomorphism. This proves the lemma.

Proof of Theorem 3.1 Let m denote the order of G. In other words, m is the R-rank of A. We must show that for every R-algebra S and any $u \in G(S)$ the m-th power of u is equal to the neutral element in $G(S)$. Replacing R by S, we see that it suffices to show this for all $u \in G(R)$.

Translation by u is an invertible morphism $G \longrightarrow G$ and therefore induces an R-automorphism σ of the R-algebra A and hence an A'-automorphism, $\mathrm{id} \otimes \sigma$ of $A' \otimes A$. On the other hand, translation by $u \in G(R) \subset G(A)$ agrees with multiplication by u in the algebra $A' \otimes A$. Applying this to the algebra homomorphism id_A in $G(A)$, we find that

$$(\mathrm{id} \otimes \sigma)(\mathrm{id}_A) = u \cdot \mathrm{id}_A.$$

Since applying σ to elements of A does not affect their norm to R, applying $\mathrm{id} \otimes \sigma$ does not affect $N_{A'}$. Therefore we have

$$N_{A'}(\mathrm{id}_A) = N_{A'}((\mathrm{id} \otimes \sigma)(\mathrm{id}_A)) = N_{A'}(u \cdot \mathrm{id}_A) = N_{A'}(u)\, N_{A'}(\mathrm{id}_A) = u^m N_{A'}(\mathrm{id}_A).$$

Since $N_{A'}(\mathrm{id}_A)$ is invertible in A', it follows that u^m is equal to the unit element $1'$ of A', as required.

Remark. In this proof, the element $N_{A'}(\mathrm{id}_A)$ of A' plays the role of the product P of all elements of a finite group. It is well known that P is not always equal to the neutral element, but its square is. Similarly, in Deligne's proof the norm $N_{A'}(\mathrm{id}_A)$ is in general not equal to the unit element $1' \in A'$, but its square is.

Indeed, since the coinverse morphism $i_A : A \longrightarrow A$ is the inverse of id_A in the group $G(A)$, the same is true in the multiplicative group $(A' \otimes_R A)*$. It follows that

$$N_{A'}(i_A \cdot \mathrm{id}_A) = 1'.$$

On the other hand, i_A is an R-automorphism of A so that $\mathrm{id}_{A'} \otimes i_A$ is an A'-automorphism of $A' \otimes_R A = \mathrm{Hom}_R(A, A)$. It carries id_A to i_A. Since A'-automorphisms do not change $N_{A'}$, we get

$$N_{A'}(\mathrm{id}_A) = N_{A'}(i_A).$$

It follows that $N_{A'}(\mathrm{id}_A)^2 = 1'$ as required.

4. Finite group schemes over Artin rings.

In this section we outline the proof given in [4] of the following result.

Theorem 4.1. *Let R be an Artin ring with maximal ideal $\mathfrak{m}$ and residue field of characteristic $p > 0$, with the property that*

$$\mathfrak{m}^p = p\mathfrak{m} = 0.$$

Then every finite free local group scheme G over R is annihilated by its order.

We first reduce to the special case that k is separably closed. Indeed, by [2, 18.8.8], the strict Henselization of R is a local faithfully flat R-algebra whose maximal ideal is generated by the maximal ideal of R. Therefore it is Artinian and its maximal ideal $\mathfrak{m}$ satisfies $\mathfrak{m}^p = p\mathfrak{m} = 0$. It follows that we may replace R by its strict Henselization and hence assume that its residue field k is separably closed.

Recall that $G = \mathrm{Spec}(A)$, where A is a local free R-Hopf algebra of rank p^n for some $n \geq 1$. Theorem 4.1 says that the augmentation ideal $I \subset A$ has the property that $[p^n](I) = 0$. If $n = 1$, it follows from [3, Thm. 1] that G is commutative, so that Deligne's theorem implies that G is killed by its order. Therefore we may assume that $n \geq 2$. By the result in SGA 3, the group scheme G considered over the residue field k, is killed by p^n. If it happens to already be killed by p^{n-1}, then the augmentation ideal $I \subset A$ has the property that $[p^{n-1}](I) \subset \mathfrak{m}I$. Then Proposition 2.1 easily implies $[p^n](I) \subset \mathfrak{m}^p + p\mathfrak{m} = 0$ and the theorem follows.

We are left with the local group schemes G over R of order p^n whose reductions over k are killed by p^n, but *not* by p^{n-1}. In [4] the group schemes with this property are determined. There are only two possibilities: over k they are either isomorphic to the multiplicative group μ_{p^n} or to the non-commutative matrix group scheme M_n given by

$$M_n(S) = \{\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} : x, y \in A \text{ satisfying } x^p = 0 \text{ and } y^{p^{n-1}} = 1\}.$$

for every k-algebra S.

If G is isomorphic to μ_{p^n} over k, then it is a deformation of μ_{p^n}. However, since k is separably closed, [1, Exp. X, Corollaires 2.3 and 2.4] imply that G must then be diagonalizable. Therefore we have $G \cong \mu_{p^n}$ over R. In particular, G is killed by p^n.

If G is over k isomorphic to M_n for some $n \geq 2$, then R must have characteristic p and is therefore a k-algebra. Moreover, there exists a faithfully flat R-algebra R' such that the base change of G to R' is isomorphic to a base change from k to R' of the group scheme M_n. See [4] for more details. It follows that G is killed by p^n.

This completes the outline of the proof of the theorem.

Acknowledgements.
The author was supported by Tor Vergata funds n. E82F16000470005.

Bibliography

[1] Demazure, M. et Grothendieck, A.: *Schémas en Groupes*, dans Sém. de Géometrie Algébrique du Bois Marie (1962/64) SGA 3, vols. I, II and III, Lecture Notes in Math. **151**, **152** and **153**, Springer-Verlag, Berlin Heidelberg New York 1970.

[2] Grothendieck, A. and Dieudonné, J.: *Étude local des schémas et des morphismes de schémas*, dans Éléments de Géometrie Algébrique IV, *Publ. Math. IHES* **32** (1966).

[3] Tate, J. and Oort, F.: Group schemes of prime order, *Ann. Scient. Éc. Norm. Sup.* **3** (1970), 1–21.

[4] Schoof, R.: Finite Flat Group Schemes over Local Artin Rings, *Compositio Mathematica* **128** (2001), 1–15

[5] Tate, J.: Finite flat group schemes, in: Cornell, G. Silverman, J. and Stevens, G.: *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, New York 1997.

[6] Waterhouse, W.: *Introduction to affine group schemes*, Graduate Texts in Math. **66**, Springer-Verlag, Berlin Heidelberg New York 1979.