Doc. Math. (Online first)
DOI 10.4171/DM/1055

Lagrange's theorem for a class of finite flat group schemes over local Artin rings

Emiliano Torti

Abstract. Let R be a local Artin ring with residue field k of positive characteristic. We prove that every finite flat group scheme over R whose special fiber belongs to a certain explicit class of non-commutative k-group schemes is killed by its order. This is achieved via a classification result which relies on the study of the infinitesimal deformation theory for such non-commutative k-group schemes. The main result answers positively in a new case a question of Grothendieck in SGA 3 on whether all finite flat group schemes are killed by their order, and improves the currently best known result due to Schoof.

1. Introduction

Let S be a locally Noetherian base scheme and let G be an S-scheme. Denote by $\mathcal{O}_S$ and $\mathcal{O}_G$ their respective structure sheaves. The S-scheme G is finite and flat if and only if $\mathcal{O}_G$ is a locally free $\mathcal{O}_S$-module of finite rank. In order to study the relation between this rank (as a locally constant function) and the order of the elements in G we can focus, by a standard EGA reduction argument (see Sec. 8.9, Sec. 8.10 and especially Sec. 9.2 in EGA IV Tome 3 in [5]), to the case where $S = \mathrm{Spec}(R)$ for some local Noetherian ring R and $G = \mathrm{Spec}(A)$ where A is a finite and free R-module of finite rank, say the positive integer n_R. By functoriality, the positive integer n_R is the restriction to $\mathrm{Spec}(R)$ of a locally constant function say n defined on S with positive integer values. Such a function is called the order of the finite flat S-scheme G.

Assume now that $G = \mathrm{Spec}(A)$ over $\mathrm{Spec}(R)$ has the extra structure of an R-group scheme. Note that in notation and terminology in this article we will say R-group scheme instead of $\mathrm{Spec}(R)$-group scheme. The category of affine R-group schemes is anti-equivalent to the category of commutative Hopf R-algebras. This implies that A has a natural structure of Hopf algebra over R. Denote by n be the order of $G = \mathrm{Spec}(A)$ over R. We say that G is killed by its order if the multiplication-by-n morphism $[n] : G \to G$ is the zero morphism of R-group schemes. This is equivalent to saying that for the induced morphism of Hopf R-algebras $[n] : A \to A^{\otimes n} \to A$ (obtained via a composition of the diagonal map and the multiplication map on G) the kernel $\mathrm{Ker}([n])$ contains the augmentation ideal $I = \mathrm{Ker}(\varepsilon : A \to R)$ where ε denotes the unit section of G.

Mathematics Subject Classification 2020: 14L30 (primary); 14L15 (secondary).
Keywords: group schemes, deformation theory.

Around the 1960s, Grothendieck asked if every finite flat group scheme over any base scheme is killed by its order (see [1, SGA 3, Exp. VIII, Rem. 7.3.1], see also [15, p. 145] and the survey article [12]). This is the generalization in the context of finite flat group schemes of what is well known in abstract group theory, i.e., if G is a finite group of order n then for all $g \in G$ we have $g^n = e_G$. Note that strictly speaking this fact is an immediate consequence of Lagrange's theorem, which has indeed been generalized in the context of finite flat group schemes (see, for example, [13]). We clarify this in the hope that the title of the article will be interpreted properly.

Grothendieck's question has been positively answered in many important cases. When the group scheme G is commutative, this has been proven by Deligne around 1970. The proof has not been published by Deligne himself but it has been reproduced many times in the literature (see, for example, [16, Sec. 1], [15, Sec. 3.8] and Sec. 3.3 in J. Stix's lecture notes [14]). When the base scheme is the spectrum of a field, or more generally is a reduced scheme, this has been proven by Grothendieck in [3, SGA 3, Exp. VII, Sec. 8] (see also [11, Cor. 2.2]).

When studying Grothendieck's question for finite flat group schemes over a local Noetherian ring R, it is very useful to notice that it is possible to make a further reduction. First, by Krull's intersection theorem, we deduce that the answer is positive if and only if it holds for all local Artin quotients of R, i.e., we can assume without loss of generality that R is a local Artin ring (see also [11]). This simplification is known to be very useful as it opens up the possibility of proceeding by induction on the length of R, as it will be done in this article. Moreover, it is clear that the problem of understanding when a finite flat group scheme G over R is killed by its order can be studied up to faithfully flat extensions of R. Thanks to [4, EGA 3, Tome 1, Prop. 10.3.1], we know that there exists a faithfully flat local extension of R such that its residue field k is algebraically closed. This allows one to do a final reduction and assume that the residue field k of characteristic p is algebraically closed and that R is a strictly Henselian ring.

Coming back to the state of art on Grothendieck's question, the best known result in the general case is due to Schoof (see [11]).

Theorem 1.1 (Schoof, 2001). *Let p be a prime and let R be a local Artin ring with maximal ideal $\mathfrak{m}_R$ and with residue field k of positive characteristic p. Assume that $\mathfrak{m}_R^p = p\mathfrak{m}_R = 0$, then any finite flat group scheme G over R is killed by its order.*

The aim of this article is to extend the above result to a certain class of finite flat group schemes without any restriction on the length of R (i.e., without the hypothesis $\mathfrak{m}_R^p = p\mathfrak{m}_R = 0$). This is achieved by proving a complete classification result (of independent interest from Grothendieck's question) for all the finite flat deformations of the considered family.

Now, we briefly recall Schoof's strategy for the proof of Theorem 1.1. After reducing the problem to assuming that R is strictly Henselian and k is an algebraically closed field of characteristic p, Theorem 1.1 is proven by discussing separately two cases depending on whether the base change $G \otimes_R k$ of G from R to its residue field k (which we assume is a k-group scheme of order p^{m+1}) is killed or not by p^m.

Schoof proceeds by showing first that under the strong hypothesis on the length of R, the groups G whose base change $G \otimes_R k$ is already killed by p^m are killed by their order. The proof continues by showing that $G \otimes_R k$ is not killed by p^m if and only if $G \otimes_R k$ is isomorphic to μ_{p^m}/k or to the matrix k-group scheme

$$G_1 = \begin{pmatrix} 1 & \alpha_p \\ 0 & \mu_{p^m} \end{pmatrix} = \left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} : x^p = 0,\ y^{p^m} = 0 \right\},$$

endowed with the usual matrix multiplication. Finally, Schoof concludes by showing that all deformations of G_1 and μ_{p^m} for some positive integer m are killed by their order. It is interesting to remark that groups such as G_1 are historically very important in the study of finite flat group schemes. Indeed, for example when $m = 1$, the existence of the non-commutative k-group scheme G_1 of order p^2 reflects the existence of a non-trivial action of μ_p on α_p (which are both commutative groups of order p). This phenomenon does not have any analogue in the classical theory of finite abstract groups, where every group of order p^2 is commutative.

Note that the group G_1 is denoted G_0 in [11] but it will be clear soon enough why we adopt this new notation and why it is not an explicit attempt to confuse the reader.

Now, since finite flat deformations of μ_{p^m} over local Artin rings R are well known to be trivial (as we will see later on), Schoof's strategy is essentially reduced to the following result for which no restrictions are needed on the length of the local Artin ring R.

Theorem 1.2 (Schoof, 2001). *Let p be a prime and let R be a local Artin ring of residue field k of positive characteristic p. Any finite flat R-group scheme G such that $G \otimes_R k \cong G_1$ is killed by its order.*

We define now a certain family of finite flat group schemes G_λ over k where $\lambda \in \{1, \dots, p^m - 1\}$ and which interpolates $G_1 = \left(\begin{smallmatrix} 1 & \alpha_p \\ 0 & \mu_{p^m} \end{smallmatrix}\right)$ exactly when $\lambda = 1$.

Let G be any finite flat multiplicative group scheme over k acting on α_p, i.e., equipped with a non-trivial morphism $\varphi : G \to \mathrm{Aut}_k(\alpha_p) \cong \mathbb{G}_m$. Then there exists a unique extension of G by α_p, i.e., $\mathrm{Ext}^1_\varphi(G, \alpha_p) \cong 0$ (see [2, Chap. 3, Cor. 6.4]). This is a consequence of the fact that group extensions can be embedded in the group of extensions of fpqc sheaves (see [2, Rem. 2.5]) and such a group is trivial under the assumption that k is perfect. More generally, this holds when the base scheme is the spectrum of a small k-ring R (in the sense of Demazure and Gabriel, see [2]) such that $R/R^p = 0$. For more details on the relation between affine group schemes and fpqc sheaves we refer the reader to the nice summary in [14], and to SGA 1, Exp. VI for a more in depth treatment (see, for example, [6, Sec. 6]).

Taking $G = \mu_{p^m}$ we know that φ is the restriction to μ_{p^m} of the standard action of $\mathbb{G}_m$ on $\mathbb{G}_a$ which corresponds uniquely to an element $\lambda \in \{1, \dots, p^m - 1\}$. In more precise terms, for every $\lambda \in \{1, \dots, p^m - 1\}$ there is a unique finite flat k-group scheme G_λ corresponding to the unique split exact sequence $0 \to \alpha_p \to G_\lambda \to \mu_{p^m} \to 0$. In other words, the k-group scheme G_λ is the semi-direct product $\alpha_p \rtimes_\lambda \mu_{p^m}$ where the subscript

λ indicates exactly the action of μ_{p^m} which we are using to build the semi-direct product. To be completely explicit, we have the following.

Definition 1.1. For $\lambda \in \{1, \ldots, p^m - 1\}$, let G_λ be the k-group scheme given by:

$$G_\lambda = \operatorname{Spec}\left({}^{k[x,y]}\!\big/_{(x^p,\, y^{p^m})} \right)$$

with group law:

$$\begin{aligned} k[x,y]/(x^p, y^{p^m}) &\to k[x,y]/(x^p, y^{p^m}) \otimes_k k[x,y]/(x^p, y^{p^m}), \\ x &\mapsto (1+y)^\lambda \otimes x + x \otimes 1, \\ y &\mapsto y \otimes 1 + 1 \otimes y + y \otimes y. \end{aligned}$$

More concisely, we adopt the notation $(x, y) \circ (x', y') = ((1+y)^\lambda x' + x, y + y' + yy')$ for the group law in G between generic elements $h = (x, y)$ and $h' = (x', y')$. It is straightforward to verify that when $\lambda = 1$ one gets exactly the group G_1 described above which appears in [11].

We show that G_λ is a finite, flat, non-commutative group scheme of order p^{m+1} whose isomorphism class only depend on the p-adic valuation of λ, and that G_λ is not killed by p^m if and only if λ is a unit (see Lemma 2.1). Hence, taking a generic λ puts us outside of the range of Schoof's theorem (Theorem 1.2). The fact that λ is not in general a unit presents many subtle challenges which do not allow us to simply extend the proof of Schoof and force us to find a new and different strategy, especially when one wants to determine explicitly the R-scheme theoretical structure of a general deformation of G_λ. However, it is possible to find a way to extend Schoof's result without restriction on R and obtain the following.

Theorem 1.3. *Let R be a local Artin ring of positive residue characteristic p and let $\lambda \in \{1, \ldots, p^{m-1}\}$. Let G be a finite flat deformation over R of the k-group scheme G_λ, then G is killed by its order.*

This result constitutes a positive answer in a new case to Grothendieck's question on whether all finite flat group schemes over any base scheme are killed by their order. The above theorem is a direct consequence of the complete classification of all the deformations of the non-commutative k-group scheme G_λ. On a side note, we mention that one could also consider the case of $\lambda = 0$, which corresponds to the case of the k-group scheme $G_0 = \alpha_p \times \mu_{p^m}$. However, while it is possible to use the techniques in this article to show that the deformations of G_0 in characteristic p are also killed by their order, this still leaves the problem open. Indeed, contrary to the case when $\lambda \neq 0$ (see Theorem 4.1), the k-group scheme G_0 admits deformations in characteristic zero (because α_p does) which a priori do not have a clear R-schematic description. We hope to come back to this problem later on.

Going back to our original question, the study of the deformation problem for G_λ with $\lambda \in \{1, \ldots, p^m\}$ will allow us to prove the following complete and explicit classification.

Theorem 1.4. *Let p be a prime and let R be a local Artin ring of perfect residue field k of positive characteristic p. Let G be a deformation over R of the k-group scheme $G_\lambda \cong \alpha_p \rtimes_\lambda \mu_{p^m}$ with parameter $\lambda \in \{1, \ldots, p^m - 1\}$.*

Then the characteristic of R is p and we have the following classification:

(i) *if $v_p(\lambda) \neq m-1$, the deformations of G_λ over R are trivial, i.e.,*

$$G \cong (\alpha_p \rtimes_\lambda \mu_{p^m}) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R);$$

(ii) *if $v_p(\lambda) = m-1$, the deformations of $G_{p^{m-1}}$ over R form a 1-dimensional family (over k) of non-commutative finite flat R-group schemes of order p^{m+1}.*

Moreover, in (ii), there is a unique $a \in k$ such that we have an isomorphism:

$$G \cong \widetilde{H}_a \text{ as } R\text{-group schemes},$$

where $\widetilde{H}_a \cong \mathrm{Spec}(R[x, y]/(x^p, y^{p^m}))$ is endowed with the group law

$$x \mapsto (1+y)^{p^{m-1}} \otimes x + x \otimes 1 + a\pi W_p(x \otimes 1, 1 \otimes x),$$
$$y \mapsto y \otimes 1 + 1 \otimes y + y \otimes y$$

for the polynomial $W_p(x, x') = \frac{(x+x')^p - x^p - x'^p}{p}$.

Remark 1.1. Note that the above result extends to all $\lambda \in \{1, p^m - 1\}$ the main result in [11, Prop. 3.3] where the specific case $v_p(\lambda) = 0$ is treated. Moreover, for all λ, Theorem 4.1 ensures us that all deformations of G_λ are trivial over R rather than potentially trivial after base change to a faithful flat extension as shown in [11, Prop. 3.3] in the specific case $v_p(\lambda) = 0$.

Remark 1.2. Note that the groups $\widetilde{H}_a$ for $a \in k$ are isomorphic to the semi-direct product $H_a \rtimes \mu_{p^m}$ where H_a is the deformation of α_p as described by Proposition 4.1, where the action of μ_{p^m} on H_a is the one corresponding to $\lambda = p^{m-1}$.

In the first section after the introduction, we prove some useful properties concerning the groups G_λ, and in the second section we state and prove Theorem 4.1 via the study of the deformation problem for the k-group schemes G_λ. We conclude the second section by stating and proving Theorem 1.3.

Notation. For a prime number p, the letter k will denote a perfect field of characteristic p and by R we will denote a local Artin ring of residue field k. We denote by α_p the finite group scheme over k of order p given by $\mathrm{Spec}(k[x]/(x^p))$ with group law $x \mapsto x \otimes 1 + 1 \otimes x$. The base change of an R-group scheme via an R-algebra morphism $R \to S$ is usually denoted $G \times_{\mathrm{Spec}(R)} \mathrm{Spec}(S)$ but sometimes more concisely we adopt the notation $G \otimes_R S$, or simply $G \otimes S$. For a finite flat group G over R, according to [2], we denote by $\mathrm{Lie}(G)$ the Lie group scheme attached to G and by $\omega_{G\otimes k}$ the module of differentials of $G \otimes k$. By $\mathrm{Mod}_k(\cdot,\cdot)$, we denote the set of homomorphisms of k-modules and by $\mathrm{Gr}_R(\cdot,\cdot)$, the set of homomorphisms of group schemes over a base ring R. For all the rest we adopt standard notation, unless explicitly specified, which agrees with [11].

2. The family of finite flat group schemes G_λ over k

In this short section, we summarize the main properties of the family G_λ of finite flat group schemes over a perfect field k of characteristic p. First, note that the k-group scheme G_λ has order p^{m+1} and it is killed by its order. This can be checked either by a direct computation or by using the well-known fact that any finite flat group scheme over a field is killed by its order (see, for example, [3, SGA 3, Exp. VIIA, Prop. 8.5]). The family of k-group schemes G_λ also satisfies the following useful property.

Lemma 2.1. *The k-group scheme G_λ (of order p^{m+1}) is killed by p^m if and only if $v := v_p(\lambda) \geq 1$.*

Proof. We prove first the "if" part. We recall that the group operation on G_λ is as follows:

$$(x, y) \circ_{G_\lambda} (x', y') = \big(x'(1+y)^\lambda + x, y + y' + yy'\big).$$

By induction, it is straightforward to check that for all $h \in \mathbb{Z}_{\geq 0}$ we have that:

$$[p^h](x, y) = \left(x \sum_{i=0}^{p^h-1} (1+y)^{\lambda i}, (1+y)^{p^h} - 1\right)$$

Proving that p^m kills G_λ means to prove that $[p^m](x, y) = (0, 0)$ which boils down to prove that:

$$\sum_{i=0}^{p^m-1} (1+y)^{\lambda i} = 0$$

in the ring $k[y]/(y^{p^m})$, because it is clear that $(1+y)^{p^m} - 1 = 0$. Note first that the positive integer $m - v$ is the minimal positive integer h such that $(1+y)^{\lambda p^h} = 1$. For $r \leq s$ positive integers denote

$$a(r, s) = \sum_{i=r}^{s} (1+y)^{\lambda i}.$$

The claim is to prove that $a(0, p^m - 1) = 0$. Recall that $v := v_p(\lambda)$. We have:

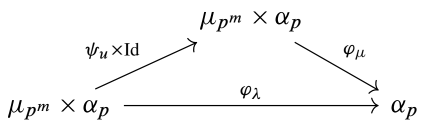
$$\begin{aligned} a(0, p^m - 1) &= a(0, p^{m-v} - 1) + a(p^{m-v}, 2p^{m-v} - 1) \\ &\quad + \cdots + a\big((p^v - 1)p^{m-v}, p^v p^{m-v} - 1\big) \\ &= a(0, p^{m-v} - 1) + (1+y)^{\lambda p^{m-v}} a(0, p^{m-v} - 1) \\ &\quad + \cdots + (1+y)^{\lambda (p^v-1)p^{m-v}} a(0, p^{m-v} - 1) \\ &= p^v a(0, p^{m-v} - 1) = 0 \end{aligned}$$

where the last equality holds because $v \geq 1$ and k is of characteristic p.

Now we prove the "only if" part. Assume by contradiction that $[p^m](x, y) = (0, 0)$, i.e., that p^m kills G_λ (where $v_p(\lambda) = 0$, i.e., λ is a unit). Since $\psi_\lambda : \mu_{p^m} \to \mu_{p^m}$ such that $\psi_\lambda(y) = (1+y)^\lambda - 1$ is an isomorphism, we have that $\sum_{i=0}^{p^m-1}(1+y)^{\lambda i} = 0$ if and only if $\sum_{i=0}^{p^m-1}(1+y)^i = 0$. Denote by $f(y) := \sum_{i=0}^{p^m-1}(1+y)^i$. We have that $f(0) = 0$ and that the degree $\deg(f) = p^{m-1}$. However, as k-vector space we have that $\dim_k(k[y]/(y^{p^m})) = p^m$ so there cannot be any non-trivial zero linear combination of the standard basis and this gives the desired contradiction. ∎

Lemma 2.2. *We have that $G_\lambda \cong G_\mu$ if and only if $v_p(\lambda) = v_p(\mu)$.*

Proof. Let u be a positive integer (strictly smaller than p^m) such that $v_p(u) = 0$. We have an isomorphism of finite flat R-group schemes $\psi_u : \mu_{p^m} \to \mu_{p^m}$ such that $\psi_u(y) = (1+y)^u - 1$, where y is a chosen variable parametrizing μ_{p^m} (which is endowed with the group law $y \to y \otimes 1 + 1 \otimes y + y \otimes y$). Pick λ and $\mu := u\lambda$, so we have $v_p(\lambda) = v_p(\mu)$. Let φ_λ and φ_μ denote the two actions of μ_{p^m} corresponding respectively to the integers λ and μ. Then a direct computation shows that we have the following commutative diagram:



where $\psi_u \times \mathrm{Id}$ is an isomorphism. Via the isomorphism $\psi_u \times \mathrm{Id}$, we have that

$$\mathrm{Ext}_\lambda(\mu_{p^m}, \alpha_p) \cong \mathrm{Ext}_\mu(\mu_{p^m}, \alpha_p) \cong 0$$

(see, for example, [2, Cor. 6.4]). In particular, there is a unique extension which implies that $G_\lambda \cong G_\mu$. On the other hand, if we have such an isomorphism it is straightforward to conclude after comparing the group laws of G_λ and G_μ. ∎

3. Adjoint representation and infinitesimal deformations

In this section, we recall the notion of adjoint representation for a finite flat group scheme and we recall some useful results concerning the description of its infinitesimal deformations.

We start by introducing the cohomology of a linear representation of finite flat group schemes (in terms of Hochschild cohomology) which will play a central role later on. Consider the following general situation. Let R be a sufficiently nice ring, e.g., it is enough to take the class of "models" in the sense of Demazure and Gabriel (see the beginning of [2]). These rings form a full subcategory of the category of rings which is the subcategory of U-small rings where U is a certain Grothendieck universe.

Let H be a finite, flat group scheme over R and let V be a projective R-module of finite type. Denote by $\mathrm{GL}(V)$ the R-group functor sending each R-algebra S to $\mathrm{GL}(V \otimes_R S)$ (where GL is the usual general linear group). A linear representation of G in V is a natural transformation $\rho : G \to \mathrm{GL}(V)$. Equivalently, writing $G = \mathrm{Spec}(A)$ for the R-Hopf algebra A, the morphism ρ corresponds to a R-linear map $\Delta_\rho : V \to V \otimes_R A$ such that for all

$v \in V$ we have that $\Delta_\rho(v) = \rho(g_0)v_A \in V \otimes_R A$ (here $v_A = v \otimes_R 1_A$) where $g_0 \in G(A)$ is the element corresponding to the identity map on A. Of course, the map Δ_ρ also reflects other functorial relations corresponding to the fact that A is a R-Hopf algebra. The point of view of considering Δ_ρ instead of ρ is useful as it allows explicit computations as we will see later on. Now, starting from an R-module V, we denote by V_a the commutative R-group functor on the category of R-algebras sending $S \mapsto V_a(S) = V \otimes_R S$.

For all positive integers n, we define the n-th cohomology group

$$H^n(G, V) := H^n_{\text{Hoc}}(G, V_a)$$

where $H^*_{\text{Hoc}}(G, V_a)$ denotes the Hochschild cohomology of the G-module V_a. An important point is that the groups $H^n(G, V)$ depend only on the action of G on V. To be precise, there exists a complex $C^*(G, V)$ where $C^n(G, V) = V \otimes_R A \cdots \otimes_R A$ (n-times $\otimes_R A$) whose boundary maps depend only on Δ_ρ and such that $H^n(G, V) \cong H^n(C^n(G, V))$. For more information on this, we refer the reader to the book of Demazure and Gabriel (see [2, Chap. 2, Sec. 3]).

One important tool that we need for studying deformations of a finite flat group scheme is the adjoint representation. As we will see later on, such special representation plays a central role in the description of the group structures which can be attached to a certain deformation. Let $R(\varepsilon)$ be the R-algebra of dual R-numbers, i.e., $R[T]/(T^2)$. Denote by $p : R(\varepsilon) \to R$ the projection which sends $p(1) = 1$ and $p(\varepsilon) = 0$. The Lie group of a finite flat group scheme G over R is defined as $\text{Lie}(G)(R) = \text{Ker}(p : G(R(\varepsilon)) \to G(R))$. The group G acts functorially on $\text{Lie}(G)$ in the following way, called adjoint representation of G:

$$\begin{aligned} \text{Ad}_G : G(R) &\to \text{GL}\left(\text{Lie}(G)(R)\right) \\ g &\mapsto \left(x \mapsto i(g)xi(g)^{-1}\right) \end{aligned}$$

where $i : G(R) \to G(R(\varepsilon))$ is induced by the injection $i : R \hookrightarrow R(\varepsilon)$ such that $i(1) = 1$.

We recall that there are two compatible operations on $\text{Lie}(G)(R)$ by R and $G(R)$. Now, we have a canonical isomorphism as R-modules (see, for example, [2, Chap. II, Sec. 4, Cor. 3.6]) $\text{Lie}(G)(R) \cong D_a(\omega_{G\otimes k})(R) \cong \text{Mod}_k(\omega_{G\otimes k}, R)$. Moreover, since G is finite flat we have that such an R-module is also canonically isomorphic to $\text{Mod}_k(I_G/I_G^2, R)$ where I_G is the augmentation ideal of G. Using the additive notation for the elements of the Lie group of G (namely $x = e^{\varepsilon x}$), we have that the explicit adjoint representation as R-module:

$$\text{Ad}_G : G(R) \to \text{GL}\left(\text{Mod}_k(I_G/I_G^2, R)\right)$$

is determined by the formula

$$ge^{\varepsilon f}g^{-1} = e^{\varepsilon \text{Ad}_G(g) f}$$

for all $g \in G(R)$ and all $f \in \text{Mod}_k(I_G/I_G^2, R)$. We denote with $V_{\text{ad}} = \text{Mod}_k(I_G/I_G^2, R)$ the adjoint representation of G.

Now, we introduce the connection between the adjoint representation introduced above and the deformation theory of the group scheme G. The first result deals with deformations of group laws (this is a specialization of [3, SGA 3, Exp. III, Thm. 3.5]).

Theorem 3.1. *Let S be a scheme and let I and J be two quasi-coherent ideals such that $J \subset I$ and $I \cdot J = 0$ defining respectively closed sub-schemes S_0 and S_J.*

Let X be a finite flat S-scheme and denote by X_J and X_0 the S-subschemes of X obtained by base change via natural projections modulo the ideals I and J. Assume that X_J has the structure of S-group scheme and denote by L_0 the commutative S_0-group functor given by the derivations of X_0/S_0, i.e.,

$$\mathrm{Hom}_{S_0}(*, L_0) := \mathrm{Hom}_{\mathcal{O}_*}(\omega^1_{X_0/S_0} \otimes_{\mathcal{O}_{S_0}} \mathcal{O}_*, J \otimes_{\mathcal{O}_{S_0}} \mathcal{O}_*).$$

The S_0-group functor L_0 acts on X_0 via its adjoint representation. Moreover, the existence of a structure of S-group scheme on X is equivalent to the following two conditions:

(i) *there exists a S-scheme morphism $P : X \times X \to X$ which induces modulo J the group law P_J of X_J,*

(ii) *a certain obstruction class $c(P_J) \in H^3(X_0, L_0)$ (corresponding to the associativity property which P has to satisfy) is zero.*

In addition, if the conditions $(i), (ii)$ are both satisfied, the set E of group laws of X (modulo S-automorphisms of X) inducing the group law P_J on X_J is a principal homogeneous space for the abelian group $H^2(X_0, L_0)$.

The proof of this result is particularly useful as it allows explicit computations. Indeed, we now briefly recall how the second cohomology group of the adjoint representation acts on the set of group laws. As it will be clear later on, this will allow us to classify certain group structures. We translate the above theorem with the terminology adopted in this article. Let E be the set of R-automorphisms orbits of group laws P on a finite flat group scheme G defined over R, such that after reducing modulo the ideal J we have that P coincides exactly with the group law of $G \otimes R/JR$ over R/JR. Let $I = \mathfrak{m}$ be the maximal ideal of the local Artin ring R of residue field k. By the above result, we know that E is a principal homogeneous space for the abelian group $H^2(G_k, V_{\mathrm{Ad}})$ where V_{Ad} is the k-adjoint representation of G_k. Note that for this fact we are using that the groups involved are finite and flat. Denote the action of an element $\delta \in H^2(G_k, V_{\mathrm{Ad}})$ on an element $\mu \in E$ by $\delta \cdot \mu$. Now, in order to make computations explicit we consider the action of $H^2(G/k, V_{\mathrm{Ad}})$ on E on points. Set a coefficient ring, say the R-algebra S. We have that for all $g, g' \in G(S)$ and for all $\mu, \mu' \in E(S)$ we have that:

$$\begin{aligned}\mu'(g, g') = \delta(\mu, \mu')(g_0, g'_0) \cdot \mu(g, g') = \mu(g, g') + D_{\delta(\mu,\mu')(g_0,g'_0)} \in G(S)\\ = \mathrm{Hom}_{R\text{-Alg}}(A, S)\end{aligned}$$

where the derivation $D_{\delta(\mu,\mu')(g_0,g'_0)}$ is the derivation associated to the image of (g_0, g'_0) via the 2-cocycle $\delta(\mu, \mu') \in H^2(G_k, V_{\mathrm{Ad}})$ which is the one corresponding to the couple

(μ, μ'). Note that we are using that E is a principal homogeneous space, i.e., the action of the abelian group $H^2(G_k, V_{\mathrm{Ad}})$ is free and transitive which grant the existence and unicity of δ as a function of μ and μ'. Moreover, as a k-module homomorphism, the image of $D_{\delta(\mu,\mu')(g_0,g_0')}$ is contained in the ideal (π) in R. This is a fundamental point which ensures that the R-algebra homomorphism determined by $\mu(g, g')$ plus the R-module homomorphism $D_{\delta(\mu,\mu')(g_0,g_0')}$ is still an R-algebra homomorphism.

The second and final result that we need concerns lifts of group morphisms and allows us to transport group structures via infinitesimal deformations. To be precise, we have the following (this is specialization of [3, SGA 3, Exp. III, Thm. 2.1]).

Theorem 3.2. *Let S be a scheme and let I and J be two quasi-coherent ideals such that $J \subset I$ and $I \cdot J = 0$ defining respectively closed sub-schemes S_0 and S_J.*

Consider the following:

(i) *X an S-group scheme,*

(ii) *L_0 the commutative S_0-group scheme given by the derivations of X_0/S_0, i.e.,*

$$\mathrm{Hom}_{S_0}(*, L_0) := \mathrm{Hom}_{\mathcal{O}_*}(\omega^1_{X_0/S_0} \otimes_{\mathcal{O}_{S_0}} \mathcal{O}_*, J \otimes_{\mathcal{O}_{S_0}} \mathcal{O}_*),$$

(iii) *Y a flat S-group scheme and $f_J : Y_J \to X_J$ a morphism of S_J-group schemes.*

Then we have that f_J lifts to a S-group scheme morphism $f : Y \to X$ if and only if the following two statements hold:

(i) *f_J lifts to a S-scheme morphism $f : Y \to X$,*

(ii) *a certain obstruction class $c(f_J) \in H^2(Y_0, L_0)$ is zero.*

4. Classification of the deformations of G_λ

In this section, we study the problem of classifying as explicitly as possible all the deformations of the groups G_λ. Deformation theory for general finite flat group schemes is a relatively complicated problem in the sense that the deformation functor is not always representable. In the case of deformations of commutative groups, the problem has been solved by Oort and Mumford in a positive way (see [9]). For example, we mention now a useful result which will be used later on and it concerns the classification of finite flat R-group schemes of order a prime p. To be precise, Oort and Tate have proven the following (see [16] or [8]).

Proposition 4.1. *Let p be a prime. There exists a polynomial $W_p \in \mathbb{Z}_p[x, y]$ such that for every R complete local Noetherian ring of residue characteristic p and for any finite flat group scheme G over R of order p, we have that $G = \mathrm{Spec}(A)$ where $A = R[\tau]/(\tau^p - a\tau)$ with group operation given by:*

$$\tau \mapsto \tau_1 + \tau_2 + bW_p(\tau_1, \tau_2)$$

for some $a, b \in R$ such that $ab = p \in R$.

This result is a fundamental step in deformation theory of finite flat group schemes in order to understand how complicated deformations might be in relation to possible necessary ramification of the base ring (here represented by the relation $ab = p$ in R). In particular, the above result describes all the possible deformations of the finite flat group scheme α_p. As the k-group schemes in the family G_λ are non-commutative extra care is needed. We are ready now to present the first main result of the section.

Theorem 4.1. *Let p be a prime and let R be a local Artin ring of perfect residue field k of positive characteristic p. Let G be a deformation over R of the k-group scheme $G_\lambda \cong \alpha_p \rtimes_\lambda \mu_{p^m}$ with parameter $\lambda \in \{1, \dots, p^m - 1\}$.*

Then the characteristic of R is p and we have the following classification:

(i) *if $v_p(\lambda) \neq m - 1$, the deformations of G_λ over R are trivial, i.e.,*

$$G \cong (\alpha_p \rtimes_\lambda \mu_{p^m}) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R);$$

(ii) *if $v_p(\lambda) = m - 1$, the deformations of $G_{p^{m-1}}$ over R form a 1-dimensional family (over k) of non-commutative finite flat R-group schemes of order p^{m+1}.*

Moreover, in (ii)*, there is a unique $a \in k$ such that we have an isomorphism:*

$$G \cong \widetilde{H}_a \text{ as } R\text{-group schemes},$$

where $\widetilde{H}_a \cong \mathrm{Spec}(R[x, y]/(x^p, y^{p^m}))$ is endowed with the group law

$$\begin{aligned} x &\mapsto (1 + y)^{p^{m-1}} \otimes x + x \otimes 1 + a\pi W_p(x \otimes 1, 1 \otimes x), \\ y &\mapsto y \otimes 1 + 1 \otimes y + y \otimes y. \end{aligned}$$

for the polynomial $W_p(x, x') = \frac{(x+x')^p - x^p - x'^p}{p}$.

We now proceed in proving the above result in several different steps. The strategy is to proceed by induction on the length of R. When the length of R is 1, everything follows by observing that one can take $R = k$. Now, assume that we are under the induction hypothesis and let $\pi \in \mathrm{Ann}(\mathfrak{m}_R)$. We have that the length of $R/\pi R$ is strictly smaller than the one of R, so we can apply the inductive hypothesis. First, this implies that the characteristic of $R/\pi R$ is p, hence there exists an element $\gamma \in R$ such that $p = \gamma\pi$. Now, the deformation G over R of G_λ can be described explicitly (scheme-theoretically) by polynomials f and g inside $R[x, y]$ such that, writing $G = \mathrm{Spec}(A)$,

$$A \cong {R[x, y]}\big/{\left(x^p - \pi f(x, y), y^{p^m} - \pi g(x, y)\right)}.$$

Now, the Hopf R-algebra structure on A is given by the group law:

$$(x, y) \circ_G (x', y') = \left(x'(1 + y)^\lambda + x + \pi h_1(x, x', y, y'), y + y' + yy' + \pi h_2(x, x', y, y')\right),$$

for certain polynomials h_1 and h_2 in $R[x, x', y, y']/(x^p, x'^p, y^{p^m}, y'^{p^m})$.

We first prove that the characteristic of R is p, i.e., every deformation of G_λ lives in positive characteristic p. Consider two points $h=(x,y)$ and $h'=(x',y')$ in G and impose that $h\circ_G h'$ is still an element in G to deduce relations concerning the polynomials f, g, h_1 and h_2.

The following conditions have to hold:

$$\begin{cases}\big(x'(1+y)^\lambda + x + \pi h_1\big)^p - \pi f\big(x'(1+y)^\lambda + x + \pi h_1, y + y' + yy' + \pi h_2\big) = 0,\\ (y+y'+yy'+\pi h_2)^{p^m} - \pi g\big(x'(1+y)^\lambda + x + \pi h_1, y + y' + yy' + \pi h_2\big) = 0.\end{cases}$$

Since $\pi^2=0$ and since $R/\pi R$ has characteristic p we have that:

$$\begin{cases}(x'(1+y)^\lambda + x)^p - \pi f(x'(1+y)^\lambda + x, y + y' + yy') = 0,\\ (y+y'+yy')^{p^m} - \pi g(x'(1+y)^\lambda + x, y + y' + yy') = 0\end{cases}$$

because $\pi f(z+\pi h_1, z'+\pi h_2) = \pi f(z,z')$. Now, since h and h' belong to G we have that $x^p - \pi f(x,y) = x'^p - \pi f(x',y') = 0$ and focusing on the first equation in the above system we have:

$$x'^p(1+y)^{\lambda p} + \sum_{k=1}^{p-1}\binom{p}{k}\big(x'(1+y)^\lambda\big)^k x^{p-k} + x^p - \pi f\big(x'(1+y)^\lambda + x, y+y'+yy'\big) = 0$$

so we deduce that:

$$\pi f(x',y')(1+y)^{\lambda p} + \big(x'(1+y)^\lambda + x\big)^p - x'^p(1+y)^{\lambda p} - x^p + \pi f(x,y) - \pi f\big(x'(1+y)^\lambda + x, y+y'+yy'\big) = 0.$$

Denoting by $W_p(x,x') = \frac{(x+x')^p - x^p - x'^p}{p}$, the expression becomes:

$$\pi\big(\gamma W_p\big(x, x'(1+y)^\lambda\big) - f\big(x'(1+y)^\lambda + x, y+y+yy'\big) + f(x,y) + f(x',y')(1+y)^{\lambda p}\big) = 0$$

imposing $y=y'=0$, we get:

$$\pi\big(\gamma W_p(x,x') - f(x+x',0) + f(x,0) + f(x',0)\big) = 0.$$

Note that inside the square parenthesis, there is the monomial $\gamma x' x^{p-1}$ (coming from the polynomial W_p) and it is the only monomial of that degree because $\deg_x(f(x,y)) \le p-1$. We deduce that $\gamma\in\mathfrak{m}_R$ and as a consequence, since $\pi\gamma = p$ and since $\pi\in\mathrm{Ann}(\mathfrak{m}_R)$ we deduce that $p=0$ in R, i.e., $\mathrm{char}(R) = p > 0$. This completes the first part of the proof.

Remark 4.1. It is interesting to notice that the above computation still holds when $\lambda = 0$, i.e., if we were in a situation where G is a deformation of the k-group scheme $G_0 \cong \alpha_p \times \mu_{p^m}$. However, it is clear that deformations of $\alpha_p\times\mu_{p^m}$ exist also over some ring of characteristic 0, e.g. $H \times \mu_{p^m}$ where H is a deformation of α_p (described by Oort and Tate in [16]) and all groups are taken over a ring R over which p ramifies. Indeed, the issue is in the assumption that a generic deformation G are only of the form considered in this article. In other words, a similar conclusion of Theorem 4.1 is false for the case $\lambda = 0$.

Taking up again the system of equations of before, and implementing the new information that the characteristic of R is p, we have that:

$$\begin{cases} f\big(x'(1+y)^\lambda + x, y + y' + yy'\big) = f(x,y) + f(x',y')(1+y)^{\lambda p}, \\ g\big(x'(1+y)^\lambda + x, y + y' + yy'\big) = g(x,y) + g(x',y') \end{cases}$$

for the second equation we have used that:

$$(y + y' + yy')^{p^m} - \pi g\big(x'(1+y)^\lambda + x, y + y' + yy'\big) = 0$$

and so

$$y^{p^m} + y'^{p^m} + y^{p^m} y'^{p^m} - \pi g\big(x'(1+y)^\lambda + x, y + y' + yy'\big) = 0$$

and substituting inside

$$y^{p^m} - \pi g(x,y) = y'^{p^m} - \pi g(x',y') = 0.$$

In order to understand the underlying R-scheme structure of G, we have to classify all the possible polynomials $f, g \in R[x,y]$, knowing that the characteristic of R is p. It might be possible that a direct computational approach allows one to classify f and g by imposing that the couple f, g has to satisfy that if h and h' are two generic points in G then the coordinates of $h \circ_G h'$ have also to satisfy the equations $x^p - \pi f(x,y) = y^{p^m} - \pi g(x,y) = 0$. We prefer here to proceed in a more conceptual way.

We know that:

$$G = \operatorname{Spec}\left(R[x,y] \big/ \big(x^p - \pi f(x,y)\big), y^{p^m} - \pi g(x,y) \right)$$

with group law depending on the parameter $\lambda \in \{1, \dots, p^m - 1\}$ and certain polynomials h_1 and h_2 in $R[x,x',y,y']$. Define the vector $F(x,y) = (f(x,y), g(x,y))^T$ and $\overline{F}(x,y) := F(x,y) \bmod \mathfrak{m}_R$. Consider now as usual two generic elements $h = (x,y)$ and $h' = (x',y')$ in G_λ, we have:

$$\begin{aligned} \overline{F}(h \circ_G h') &= \overline{F}\big((x,y) \circ_{G_\lambda} (x',y')\big) \\ &= \begin{pmatrix} f\big((x,y) \circ_{G_\lambda} (x',y')\big) \\ g\big((x,y) \circ_{G_\lambda} (x',y')\big) \end{pmatrix} \mod \mathfrak{m}_R \\ &= \begin{pmatrix} f(x,y) + f(x',y')(1+y)^{\lambda p} \\ g(x,y) + g(x',y') \end{pmatrix} \mod \mathfrak{m}_R \\ &= \begin{pmatrix} f(x,y) \\ g(x,y) \end{pmatrix} + \begin{pmatrix} (1+y)^{\lambda p} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} f(x',y') \\ g(x',y') \end{pmatrix} \mod \mathfrak{m}_R \end{aligned}$$

hence we deduce the relation:

$$\bar{F}(h \circ_{G_\lambda} h') = \bar{F}(h) + \begin{pmatrix} (1+y)^{\lambda p} & 0 \\ 0 & 1 \end{pmatrix} \bar{F}(h').$$

Define now the k-vector space $\bar{V} = ke_1 \oplus ke_2$ over which G_λ acts via:

$$\Delta : \bar{V} \to \bar{V} \otimes_k {}^{k[x,y]}\!\big/_{(x^p, y^{p^m})}$$

where $\Delta(e_1) = e_1 \otimes (1+y)^{\lambda p}$ and $\Delta(e_2) = e_2$.

The relation proven above for $\bar{F}(x, y)$ is equivalent to say that $\bar{F}$ is a crossed homomorphism from G_λ to $\bar{V}$ and as such, we can identify it with a 1-cocycle for the representation $\bar{V}$, i.e., $\bar{F} \in H^1(G_\lambda, \bar{V})$.

We recall now that $G_\lambda \cong \alpha_p \rtimes_\lambda \mu_{p^m}$, i.e., it fits into a split exact sequence $0 \to \alpha_p \to G_\lambda \to \mu_{p^m} \to 0$. The action of G_λ on V factors via the quotient μ_{p^m}. Now, diagonalizable group schemes, such as μ_{p^m}, satisfy the following useful property (on which we rely also later on, so we state it properly).

Proposition 4.2. *Let H be a diagonalizable k-group scheme and $\rho : H \to \mathrm{GL}(V)$ a linear representation of H, then for all $n > 0$ we have that $H^n(H, V) = 0$.*

Proof. See, for example, [2, Chap. II, Sec. 3, Prop. 4.2]. This result holds for any base R which is a "model" in the sense of [2]. ■

Moreover, we can combine the above result with the following.

Proposition 4.3. *Let G be a finite flat k-group scheme and let N be a finite flat normal subgroup scheme inside G. Let W be any G-module and assume that G/N (which is as well a finite flat k-group scheme) is diagonalizable. Then for all $i \geq 0$ we have isomorphisms:*

$$H^i(G, W) \xrightarrow{\cong} H^i(N, W)^{G/N}.$$

Proof. This is a consequence of Proposition 4.2 applied to Grothendieck's generalization of the Lyndon–Hochschild–Serre spectral sequence. See, for example, [7, Cor. 6.9]. ■

For $n \in \mathbb{N}$, we recall that the action of G on the cohomology groups $H^n(N, W)$ is deduced by the action of G on the cocycles $C^n(N, W) = W \otimes \mathcal{O}(N)^{\otimes n}$ which comes from the action of G on N via conjugation and on W via its G-module structure (see, for example, [7, Sec. 6.7]). Finally, we have that Proposition 4.3 allows us to compute explicitly.

Proposition 4.4. *For $\lambda \in \{1, \ldots, p^m - 1\}$, we have $H^1(G_\lambda, \bar{V}) = 0$.*

Proof. First, we recall that the G_λ-representation $\bar{V}$ decomposes as a direct sum $L \oplus \mathbb{G}_a$ (with $L \cong \mathbb{G}_a$ as k-group schemes) where the action of a generic element $g = (x, y) \in G_\lambda$ on L is given by the multiplication by $(1+y)^{\lambda p}$ and it is the trivial one on the second factor $\mathbb{G}_a$. By Proposition 4.3, we have that:

$$H^1(G_\lambda, \bar{V}) \cong H^1(G_\lambda, L) \oplus H^1(G_\lambda, \mathbb{G}_a) \cong H^1(\alpha_p, L)^{\mu_{p^m}} \oplus H^1(\alpha_p, \mathbb{G}_a)^{\mu_{p^m}}.$$

We have that $H^1(\mathbb{G}_a, \mathbb{G}_a) \cong \mathrm{Gr}_k(\mathbb{G}_a, \mathbb{G}_a)$ is the k-group scheme of endomorphisms of $\mathbb{G}_a$ which is isomorphic to the group $\{p(x) = \sum_{k\geq 0} a_i x^{p^i}$ with $a_i \in k\}$ with the usual addition of polynomials (see, for example, [2, Chap. 2, Sec. 3.4]). Hence, we have that any 1-cocycle $z : \alpha_p \to \mathbb{G}_a$ corresponds to a polynomial $p_z(x) = a_z x$ for some $a_z \in k$ (since $x^p = 0$). A direct computation shows that both actions of μ_{p^m} on L and the trivial one on $\mathbb{G}_a$ are incompatible with the conjugation on α_p (which corresponds to sending a generic element x of α_p to $(1+y)^\lambda x$). As a consequence, we have that $H^1(\alpha_p, L)^{\mu_{p^m}} = H^1(\alpha_p, \mathbb{G}_a)^{\mu_{p^m}} = 0$. ■

We deduce then that $\bar{F}$ is a 1-coboundary, or equivalently, there exists $(c, d) \in k^2$ such that for every $h = (x, y) \in G_\lambda$ we have that $\bar{F}(h) = \rho(h) \cdot (c, d)^T - (c, d)^T$. After making the representation ρ explicit, we have that there exists some polynomials z_1 and z_2 in $R[x, y]$ with coefficients in $\mathfrak{m}_R$ such that

$$F(x, y) = \begin{pmatrix} f(x, y) \\ g(x, y) \end{pmatrix} = \begin{pmatrix} c\big[(1+y)^{\lambda p} - 1\big] + z_1 \\ z_2 \end{pmatrix}.$$

Since $\pi \in \mathrm{Ann}(\mathfrak{m}_R)$, we deduce that $\pi f(x, y) = c\pi[(1+y)^{\lambda p} - 1]$ and $\pi g(x, y) = 0$. Finally, we conclude that the underlying R-scheme structure of the generic deformation G over R of G_λ has to have the form:

$$G = \mathrm{Spec}\left(R[x, y] \big/ \left(x^p - c\pi\big[(1+y)^{\lambda p} - 1\big], y^{p^m}\right)\right).$$

Note also that (since $\mathrm{char}(R) = p$) $(1+y)^{\lambda p} = 1 + y^{\lambda p}$ if and only if λ is a power of p. Hence, we first simplify a bit the expression $c\pi[(1+y)^{\lambda p} - 1]$ by using the results in Section 2. By Lemma 2.2, we have indeed that without loss of generality we can assume that $\lambda = p^v$ for a certain integer $v \geq 0$ and so $c\pi[(1+y)^{\lambda p} - 1] = c\pi y^{p^{v+1}}$. Summarizing what we have proven until now, we have that for every deformation G of G_λ we have the following isomorphisms of R-schemes:

$$G \cong \mathrm{Spec}\left(R[x, y] \big/ \left(x^p - c\pi y^{p^{v+1}}, y^{p^m}\right)\right) \quad \text{for some } c \in k.$$

Our goal is to prove the following stronger description.

Proposition 4.5. *For all $\lambda \in \{1, \ldots, p^m - 1\}$, we have that every finite flat deformation G over R of G_λ is isomorphic as R-scheme to* $\mathrm{Spec}(R[x, y]/(x^p, y^{p^m}))$*, i.e., to the base change $G_\lambda \otimes_k R$.*

Our aim is now to prove that as R-schemes, we have an isomorphism between G and $\mathrm{Spec}(R[x, y]/(x^p, y^{p^m}))$, i.e., $c = 0$. This point of the proof is the most delicate as the situation is substantially different from the one treated in [11] where $v_p(\lambda) = 0$ and a new approach is necessary. Indeed, if $v_p(\lambda) = 0$, it is possible to directly conclude by a linear isomorphic substitution after observing that $x^p - c\pi[(1+y)^{\lambda p} - 1] = (x - \omega y)^p$ after suitably extending R finitely flatly by adding an element ω such that $\omega^p = c\pi$. However, when $v_p(\lambda) > 1$, the situation is much more subtle because such a substitution is not available. Our first goal is to determine the possible values of the constant $c \in k$. Since G is an R-group scheme with neutral element $(0, 0)$ we have that in order for the group axioms to be satisfied we have that $h_i(x, y, 0, 0) = h_i(0, 0, x', y') = 0$ for $i = 1, 2$. The strategy is to use the inductive hypothesis on $R/\pi R$ and k to transport certain group structures from the infinitesimal deformations (i.e., deformations over $R/\pi R$ where $\pi^2 = 0$) to G over R. We recall that, using the additive notation for the elements of the Lie group of G (namely $x = e^{\varepsilon x}$), the explicit adjoint representation as R-module:

$$\mathrm{Ad}_G : G(R) \to \mathrm{GL}\left(\mathrm{Mod}_k(I_G/I_G^2, R)\right)$$

is determined by the formula

$$g e^{\varepsilon f} g^{-1} = e^{\varepsilon \mathrm{Ad}_G(g) f}$$

for all $g \in G(R)$ and all $f \in \mathrm{Mod}_k(I_G/I_G^2, R)$. Let now consider the case where $G = G_\lambda$ defined over a finite perfect field k of positive characteristic p. We know that:

$$G_\lambda = \mathrm{Spec}\left(k[x, y] \big/ (x^p, y^{p^m}) \right)$$

with group law given by $(x, y) \circ_{G_\lambda} (x', y') = (x'(1+y)^\lambda + x, y + y' + yy')$.

Let $g = (x', y')$ and denote by $g^{-1} = (x'', y'')$. The following relations hold:

$$\begin{cases} (1+y')^\lambda x'' + x' = 0, \\ y' + y'' + y'y'' = 0. \end{cases}$$

Let $f(x, y) = a_f x + b_f y \in \mathrm{Mod}_k(I_{G_\lambda}/I_{G_\lambda}^2, R)$ where $I_{G_\lambda} = (x, y)$ as an ideal inside $\mathcal{O}(G_\lambda)$. Now, we impose that $g e^{\varepsilon f} g^{-1} = e^{\varepsilon \mathrm{Ad}_G(g) f}$. In other words, we have to compute $g e^{\varepsilon f} g^{-1} = f(g \circ (x, y) \circ g^{-1})$ as an element in $\mathrm{Mod}_k(I_{G_\lambda}/I_{G_\lambda}^2, R)$. We have that:

$$\begin{aligned} &f\left((x', y') \circ (x, y) \circ (x'', y'')\right) \\ &= f\left((1+y')^\lambda\left[(1+y)^\lambda x'' + x\right] + x', y' + y + y'' + yy'' + y'(y + y'' + yy'')\right) \end{aligned}$$

Now, using the relations between g and g^{-1} and that we are doing computations modulo the ideal $(x, y)^2$ inside $\mathcal{O}(G_\lambda) = k[x, y](x^p, y^{p^m})$, we conclude that the above expression is equal to:

$$f\left((1+y')^\lambda x - \lambda x' y, y\right) = f\left(\begin{pmatrix} (1+y')^\lambda & -\lambda x' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \right)$$

where we used that $(1+y)^\lambda = 1 + \lambda y \bmod (x, y)^2$. We deduce finally that the a adjoint representation of G_λ is the representation:

$$\mathrm{Ad}_{G_\lambda} : G_\lambda(R) \to \mathrm{GL}\left(\mathrm{Mod}_k(I_{G_\lambda}/I^2_{G_\lambda}, R)\right)$$
$$g = (x, y) \mapsto \begin{pmatrix} (1+y)^\lambda & -\lambda x \\ 0 & 1 \end{pmatrix}.$$

We have now enough information for computing the cohomology of V_{ad} as a G_λ-module. To be precise, we have the following.

Proposition 4.6. *Let $\lambda \in \{1, \dots, p^m - 1\}$ and let V_{ad} be the adjoint representation of G_λ over k.*

We have that:

$$H^2(G_\lambda, V_{\mathrm{ad}}) = \begin{cases} \langle W_p \rangle & \text{if } v_p(\lambda) = m-1, \\ 0 & \text{otherwise}; \end{cases}$$

where the class W_p represents the polynomial $W_p(x, x') = \frac{1}{p}[(x + x')^p - x^p - x'^p]$.

Proof. When $v_p(\lambda) = 0$, the claim has been proven by Schoof (see [11, Lem. 3.2]). Assume now that $v_p(\lambda) \geq 1$. It is well known that $H^2(\alpha_p, \mathbb{G}_a) \cong \langle W_p \rangle$ (see, for example, [2, Chap. II, Sec. 3, Cor. 4.8]). By Proposition 4.3, we have that:

$$H^2(G_\lambda, V_{\mathrm{ad}}) \cong H^2(\alpha_p, V_{\mathrm{ad}})^{\mu_{p^m}} \cong H^2(\alpha_p, L')^{\mu_{p^m}} \oplus H^2(\alpha_p, \mathbb{G}_a)^{\mu_{p^m}},$$

where $L' \cong \mathbb{G}_a$ (as k-group schemes) has a μ_{p^m}-module structure given by the action of μ_{p^m} sending x to $(1 + y)^\lambda x$ and where the action of μ_{p^m} on $\mathbb{G}_a$ is the trivial one. It is straightforward to check how μ_{p^m} acts on every 2-cocycle $\alpha_p^2 \to \mathbb{G}_a$ by directly checking how it acts on the 2-cocycle given by W_p. In order to find the μ_{p^m}-invariants, we have to impose that the 2-cocycle W_p is invariant under the simultaneous action of μ_{p^m} via conjugation on α_p and the adjoint representation action on either the first factor L' or the second factor $\mathbb{G}_a$. A direct computation shows that only one case is non-trivial. Indeed, let $\gamma \in \mu_{p^m}$ be represented by the variable y. Then considering the trivial action of μ_{p^m} on $\mathbb{G}_a$ we have:

$$W_p\left(\gamma(x, x')\right) = W_p\left((1 + y)^\lambda x, (1 + y)^\lambda x'\right) = (1 + y)^{\lambda p} W_p(x, x').$$

Hence, we have that $H^2(\alpha_p, \mathbb{G}_a)^{\mu_{p^m}}$ is different from zero if and only if

$$W_p\left(\gamma(x, x')\right) = W_p(x, x')$$

which happens, by the above computation, if and only if $v_p(\lambda) = m - 1$ (note that we are assuming $\lambda \geq 1$). We deduce that $H^2(\alpha_p, L')^{\mu_{p^m}} = 0$ and $H^2(\alpha_p, \mathbb{G}_a)^{\mu_{p^m}} \cong \langle W_p \rangle$ (if $v_p(\lambda) = m - 1$ and 0 otherwise). ∎

As a consequence of Proposition 4.6 and thanks to Theorem 3.1 (see also the discussion following the theorem), we can completely classify all group structures of the generic deformation of G_λ by describing explicitly the polynomials h_1 and h_2. To be precise, we have the following.

Lemma 4.1. *The polynomials h_1 and h_2 in $R[x, y, x', y']$ satisfy the following properties:*

$$\text{if } v_p(\lambda) \neq m-1, \quad \text{then } h_1 = h_2 = 0,$$
$$\text{if } v_p(\lambda) = m-1, \quad \text{then } h_1 \in \langle W_p(x, x') \rangle \text{ and } h_2 = 0.$$

Proof. We have that the action of $H^2(G_\lambda, V_{\mathrm{Ad}})$ on the principal homogeneous space E of group laws on G depends only on the derivations evaluated in α_p by Proposition 4.6. A direct computation shows that for $g = (x, y)$ and $g' = (x', y')$ the morphism $\mu_0(g, g') := (x + x', y + y' + yy')$ defines a group law on G, i.e., $\mu_0 \in E$, and because of Theorem 3.1 any other group law μ is uniquely obtained by translations via derivations, i.e., $\mu(g, g') = \mu_0(g, g') + D_{\mu_0,\mu}(g_0, g_0')$ where g_0 and g_0' are the reductions mod k of g and g' and are generic elements of G_λ. Finally, since the derivation $D_{\mu_0,\mu}(g_0, g_0')$ has image living in the ideal (π) and depends only on x and x', in the only non-zero case (i.e., when $v_p(\lambda) = m - 1$) we have that the image of $D_{\mu_0,\mu}(g_0, g_0')$ is exactly $a\pi W_p(x, x')$ for some $a \in k$. ■

Note that in all cases we have $h_i(x, 0) = h_i(0, x') = 0$ for $i = 1, 2$ because of the axiom for the neutral element. If $v_p(\lambda) = v = m - 1$, one obtains immediately Proposition 4.5. Hence, we restrict our attention to the case $v_p(\lambda) \neq m - 1$. Consider the R-scheme morphism:

$$\varphi : N := \operatorname{Spec}\left(R[x]/(x^p)\right) \hookrightarrow G = \operatorname{Spec}\left(R[x, y]/\left(x^p - c\pi y^{p^{v+1}}, y^{p^m}\right)\right)$$

where φ corresponds to the natural projection for $y = 0$.

Lemma 4.2. *For all $\lambda \in \{1, \ldots, p^m - 1\}$, the R-scheme N has a group law for which it is a normal R-subgroup scheme of G with the closed immersion given by the R-group morphism φ and $N \cong \alpha_p$ as R-group schemes.*

Proof. By inductive hypothesis, we know that after taking a base change to $R/\pi R$, we have that $H \otimes R/\pi R$ has the structure of an $R/\pi R$-group scheme isomorphic to $\mu_{p^m}/R/\pi R$ and $\varphi \otimes R/\pi R$ is a $R/\pi R$-group scheme homomorphism. The idea now is to use the results from SGA mentioned above to transport these group structures from the infinitesimal deformations over $R/\pi R$ to R. Note the fundamental fact that N is a flat R-scheme of finite type over R.

According to Theorem 3.1, in order to prove that N has the structure of group scheme we have to verify two statements. First that there exists a R-scheme morphism $P_N : N \times N \to N$ which specialize to the group law of α_p after base change to $R/\pi R$ and second, that a certain class $c(P_N) \in H^3(\alpha_p/k, V_{\mathrm{Ad}})$ (corresponding to the associativity property of P_N) is zero. For the first part, note that G as a R-group scheme has its group law which can be seen as a R-scheme morphism $P : G \times G \to G$ which induces the usual group law on G_λ after base changing to $R/\pi R$ (by inductive hypothesis). Because of Lemma 4.1, taking the restriction of P to generic elements of N we get that $P((x, 0), (x', 0)) = (x + x' + \pi h_1, 0)$. Hence, defining P_N as the restriction of P to N

we get a well-defined R-schemes morphism $P_N : N \times N \to N$ satisfying the required properties. Now, the class $c(P_N) \in H^3(\alpha_p, V_{\mathrm{Ad}})$ which corresponds to the associativity property of P_N is nothing else than the image of the respective class $c(P) \in H^3(G_\lambda, V_{\mathrm{Ad}})$ under the group homomorphism $H^3(G_\lambda, V_{\mathrm{Ad}}) \to H^3(\alpha_p, V_{\mathrm{Ad}})$ induced by the inclusion $\alpha_p \hookrightarrow G_\lambda$ (because P_N is defined as the restriction of P to $N \times N$). Since P is a group law, we have that $c(P) = 0$ which implies that $c(P_N) = 0$. We conclude that N has the structure of a finite flat group R-scheme. Now, applying Theorem 3.2 to the R-scheme morphism φ together with the (necessary) induction hypothesis that $\varphi \otimes R/\pi R$ is the closed immersion corresponding to the projection $y = 0$, we can conclude that φ is also a closed immersion R-group scheme morphism.

Alternatively, it can be checked by formulas that the R-scheme morphism φ preserves the group law via a direct computation as everything is explicit. Finally, because the group law of N is explicit, another direct computation shows that N is a normal R-subgroup scheme inside G. This concludes the lemma. ■

Now that we endowed N with a finite flat R-subgroup scheme structure which makes it normal inside G, which allows us to take the quotient. As this procedure is usually delicate because the category of finite flat affine group schemes over an arbitrary R is not an abelian category, we state precisely a result of Grothendieck which grants us the existence of the quotient of G by N as a finite flat group scheme over R (see, for example, [15, Sec. 3] or [14, Sec. 6.3] or [10]):

Theorem 4.2. *Let N be a finite flat closed normal subgroup of an affine finite group scheme G over R. Then the quotient group fpqc sheaf G/N is representable by an affine finite group scheme H, which coincides with the categorical cokernel for the inclusion $N \subset G$ with the natural projection $G \to G/N$ being finite and faithfully flat.*

Moreover, if $G = \mathrm{Spec}(A)$ and $N = \mathrm{Spec}(A/J)$ is commutative then $G/N = \mathrm{Spec}(B)$ where the R-algebra B is described explicitly by $B = \{a \in A : c(a) \equiv 1 \otimes a \mod (J \otimes A)\}$, where c denotes the co-multiplication on A.

The fact that the natural projection $G \to G/N$ is finite and faithfully flat implies in particular that G is finite flat if and only if G/N is finite and flat (note that we are assuming as hypothesis that N is already finite and flat). Coming back to our case, since G is a finite flat deformation of G_λ we have that G/N is a finite flat R-group scheme. Moreover, we have that $N = \mathrm{Spec}(R[x]/(x^p))$ with the group law mentioned above is commutative because it is a finite flat group scheme of prime order (this is a result of Oort and Tate, see, for example, [16]). Hence, G/N is isomorphic to $\mathrm{Spec}(B)$ where B is the R-subalgebra of $R[x, y]/(x^p - c\pi y^{p^{v+1}}, y^{p^m})$ such that

$$B = \left\{ a \in {}^{R[x,y]}\big/_{\left(x^p - c\pi y^{p^{v+1}},\, y^{p^m}\right)} : c(a) \equiv 1 \otimes a \mod \big((y) \otimes A\big) \right\}$$

where as usual, the group law of G is determined by $c(x) = (1 + y)^\lambda \otimes x + x \otimes 1$ and $c(y) = 1 \otimes y + y \otimes 1 + y \otimes y$ (after Lemma 4.1). It is straightforward to check that B is the R-subalgebra of $R[x, y]/(x^p - c\pi y^{p^{v+1}}, y^{p^m})$ generated by the elements x^p and y

with relation $x^p - c\pi y^{p^{v+1}} = 0$. Indeed we have that because the formulas for c holds as above, the element x does not belong to B but the elements x^p and y do (and no smaller power of x belongs to B). Note also that $(x^p)^2 = 0$ because $\pi^2 = 0$. If $c \neq 0$, the relation $x^p - c\pi y^{p^{v+1}} = 0$ prevents the R-algebra B to be free (note that R is local) which would contradict the fact that $\mathrm{Spec}(B)$ is a finite and flat R-group scheme. This allows us to conclude directly that c must be zero. Another equivalent way to prove that $c = 0$ comes from the deformation theory of μ_{p^m}. Indeed, the finite flat R-group scheme G/N is a deformation of μ_{p^m}, i.e., $G/N \otimes_R k \cong \mu_{p^m}/k$ (because base change of algebraic groups preserves exactness under flatness hypothesis). However, the k-group scheme μ_{p^m} does not admit non-trivial deformations over a local Artin ring R, i.e., we have the following.

Proposition 4.7. *Let R be a local Artin ring. Let H be a finite flat R-group scheme such that $H \otimes_R k \cong \mu_{p^m}$, then we have that $H \cong \mu_{p^m}/R$. In other words, all deformations of μ_{p^m} are trivial for all positive integers m.*

Proof. This is a direct consequence of the fact that the category of R-group schemes which are of multiplicative type and finite over R is equivalent to the same category over $R/\mathfrak{m}_R R \cong k$, and we know that $H \otimes_R k \cong \mu_{p^m}$ is of multiplicative type. This implies that H and μ_{p^m} over R have to be isomorphic. See, for example, [1, SGA 3, Exp. X, Cors. 2.3 and 2.4, Rem. 4.0.1 and Lem. 4.1]. ∎

We conclude that we have an isomorphism $G/N \cong \mu_{p^m}$ as R-group schemes, which implies that $B \cong R[y]/(y^{p^m})$ which holds if and only if $c = 0$. Finally, for all λ we have that:

$$G \cong \mathrm{Spec}\left(R[x,y] \big/ (x^p, y^{p^m}) \right)$$

with group law given for a certain $a \in k$ by:

$$(x, y) \circ_G (x'y') = \left((1+y)^{\lambda} x' + x + a\pi W_p(x, x'), y + y' + yy' \right).$$

This concludes the proof of Proposition 4.5. By Lemma 4.1, we conclude that if $v_p(\lambda) \neq m-1$ there are no non-trivial deformations of G_λ over R, i.e., $G \cong G_\lambda \otimes_k R \cong \alpha_p \rtimes_\lambda \mu_{p^m}$ which explicitly is the R-scheme $R[x,y]/(x^p, y^{p^m})$ with group structure given by $(x, y) \circ_{G_\lambda} (x', y') = ((1+y)^\lambda x' + x, y + y' + yy')$.

If $v_p(\lambda) = m - 1$, we have that the deformations of G_λ form a 1-dimensional family $\widetilde{H}_a$ (with parameter $a \in k$) of non-commutative R-group schemes of order p^{m+1}. We have that the family of finite flat R-group schemes $\widetilde{H}_a$ can be explicitly described as:

$$\widetilde{H}_a \cong \mathrm{Spec}\left(R[x,y] \big/ (x^p, y^{p^m}) \right)$$

with group law given by:

$$(x, y) \circ_G (x', y') = \left((1+y)^{p^m} x' + x + a\pi W_p(x, x'), y + y' + yy' \right).$$

This concludes the proof of Theorem 4.1. Finally, we can apply Theorem 4.1 to the problem of understanding if any finite flat deformation G over R of G_λ is killed by its order. In particular, we conclude with the following.

Theorem 4.3. *Let R be a local Artin ring of positive residue characteristic p. Let G be a deformation over R of the k-group scheme G_λ for any $\lambda \in \{1, \dots, p^{m-1}\}$. Then G is killed by its order.*

Proof. By Theorem 4.1, if $v_p(\lambda) \neq m-1$, we have that $G \cong (\alpha_p \rtimes_\lambda \mu_{p^m}) \times_{\mathrm{Spec}(k)} \mathrm{Spec}(R)$ over R and we conclude that also G is killed by its order.

Now, assume that $v_p(\lambda) = m-1$. By Theorem 4.1, for any deformation G over R of $G_{p^{m-1}}$ there exist $a \in k$ such that we have that $G \cong \widetilde{H}_a$. We can perform now computations as the group law is also explicit in this case. Indeed, given a generic element $h = (x, y) \in \widetilde{H}_a$, we have that

$$[p^m](x, y) = \left(x \sum_{k=0}^{p^m-1} (1+y)^{kp^{m-1}}, y^{p^m} \right)$$

because $W_p(x, x) = 0$ since $x^p = 0$. Since $y^{p^m} = 0$ the second component is zero. Finally, the same exact computation performed in Section 2 can be repeated here which grants us that also the first component is indeed zero because $\sum_{k=0}^{p^m-1}(1+y)^{kp^{m-1}} = p^{m-1}\sum_{k=0}^{p-1}(1+y)^{kp^{m-1}} = 0$ because R is of characteristic p. This proves that $[p^m]$ kills $\widetilde{H}_a$ and in particular we deduce that G is killed by its order. This concludes the proof of the theorem. ∎

Acknowledgments. I would like to thank René Schoof for sharing his insights on the topic. I would also like to thank Arnaud Vanhaecke and Andrea Conti for many interesting conversations. I would also like to thank Gaetan Bisson and Alexander Rahm in the GAATI group at University of French Polynesia who supported my research as part of the MELODIA project. Ultimately, I would like to thank the anonymous reviewer for their precise suggestions which greatly improved the exposition of the paper.

Funding. This work was partially supported by the ANR under grant number ANR-20-CE40-0013 (MELODIA project).

References

[1] M. Artin et al., *Schémas en groupes. Fasc. 3: Exposés 8 à 11*. Institut des Hautes Études Scientifiques, Paris, 1964 MR 207705

[2] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeurs, Paris; North-Holland Publishing, Amsterdam, 1970 Zbl 0203.23401 MR 0302656

[3] M. Demazure and A. Grothendieck (eds.), *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*. Doc. Math. (Paris) 7, Société Mathématique de France, Paris, 2011 Zbl 1241.14002 MR 2867621

[4] A. Grothendieck, Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I. *Publ. Math. Inst. Hautes Études Sci.* **11** (1961), 5–159 Zbl 0118.36206 MR 0217085

[5] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. *Publ. Math. Inst. Hautes Études Sci.* **28** (1966), 5–248 Zbl 0144.19904 MR 217086
[6] A. Grothendieck and M. Raynaud (eds.), *Revêtements étales et groupe fondamental*. Lecture Notes in Math. 224, Springer, Berlin, 1971 Zbl 0234.14002 MR 0354651
[7] J. C. Jantzen, *Representations of algebraic groups*. Pure Appl. Math. 131, Academic Press, Boston, MA, 1987 Zbl 0654.20039 MR 0899071
[8] F. Oort, Finite group schemes, local moduli for abelian varieties, and lifting problems. *Compos. Math.* **23** (1971), 265–296 Zbl 0223.14024 MR 0301026
[9] F. Oort and D. Mumford, Deformations and liftings of finite, commutative group schemes. *Invent. Math.* **5** (1968), 317–334 Zbl 0179.49901 MR 0228505
[10] R. Schoof, Introduction to finite group schemes. 2000, lecture notes
[11] R. Schoof, Finite flat group schemes over local Artin rings. *Compos. Math.* **128** (2001), no. 1, 1–15 Zbl 1042.14021 MR 1847662
[12] R. Schoof, Is a finite locally free group scheme killed by its order? In *Open problems in arithmetic algebraic geometry*, pp. 1–7, Adv. Lect. Math. (ALM) 46, Int. Press, Somerville, MA, 2019 Zbl 1427.14095 MR 3971179
[13] S. S. Shatz, Group schemes, formal groups, and p-divisible groups. In *Arithmetic geometry (Storrs, Conn., 1984)*, pp. 29–78, Springer, New York, 1986 Zbl 0603.14033 MR 0861972
[14] J. Stix, A course on finite flat group schemes and p-divisible groups. 2009, lecture notes
[15] J. Tate, Finite flat group schemes. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pp. 121–154, Springer, New York, 1997 Zbl 0924.14024 MR 1638478
[16] J. Tate and F. Oort, Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)* **3** (1970), 1–21 Zbl 0195.50801 MR 0265368

Communicated by Nikita A. Karpenko

Received 10 January 2025; revised 2 September 2025.

Emiliano Torti
Laboratoire de Géométrie Algébrique et Applications à la Théorie de l'Information (GAATI), Université de la Polynésie française, B.P. 6570, Punaauia 98702 Tahiti, French Polynesia; emiliano.torti@upf.pf, torti.emiliano@gmail.com