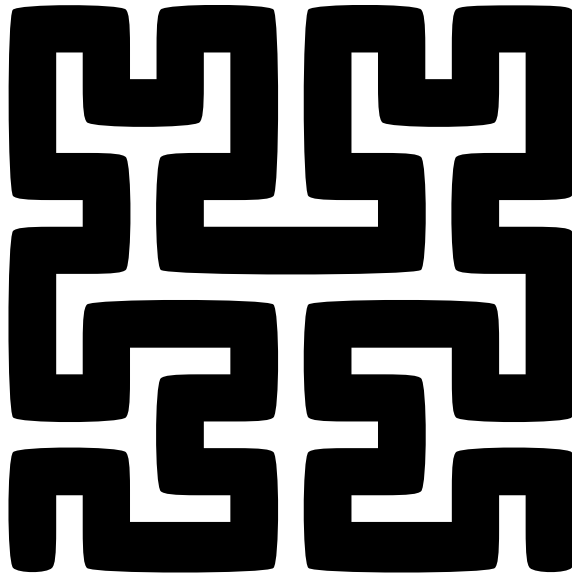




Polynesian Journal of Mathematics

Volume 4, Issue 6

Special volume AĴAX in honor of René Schoof

Order vs exponent for finite flat group schemes

Emiliano Torti

Received 28 Jan 2026

Revised 5 Jul 2026

Accepted 7 Jul 2026

Published 28 Sep 2026

Communicated by Samuele Anni

DOI: 10.69763/polyjmath.4.6

Order vs exponent for finite flat group schemes

Emiliano Torti

Laboratoire de mathématiques GAATI, Université de la Polynésie française, French Polynesia

Abstract

In this article, we study the notions of order and exponent for finite flat group schemes and explore the relationship between them. A question raised by Grothendieck in SGA3 around the 1970s asks whether, as in the classical theory of finite groups, the exponent necessarily divides the order. Despite its deceptively simple formulation, this question remains mysterious and is still open in full generality. It has an illustrious history: over the past sixty years, it has attracted contributions from many mathematicians, including Grothendieck, Deligne, and Schoof, whose work yields the most general affirmative result currently known. We present the known cases, outline the main ideas on which these results are based and we present some small recent improvements.

1 Introduction

The study of solutions to polynomial equations has a long and distinguished history. In the 1770s, Lagrange introduced the idea of using resolvents to obtain generic formulas for the solutions of polynomial equations in one variable. His key insight was the following: given a rational polynomial function $f(x_1, \dots, x_n)$ of n variables, consider the action of all $n!$ permutations of the variables. If the set of resulting permuted functions contains only r distinct elements, then r must divide $n!$. This observation enabled Lagrange to show that, when the degree of a polynomial equation is less than 5, there exist polynomial expressions in the roots that satisfy a polynomial equation of lower degree, making it possible to derive general solution formulas. For the interested reader, a nice historical survey on Lagrange's theorem is given by [5].

About fifty years later, with the advent of modern algebra and the introduction of the notion of group (thanks to Galois), Lagrange's result could be reformulated in contemporary terms. This reformulation, now known as Lagrange's theorem, states that the order of a subgroup H of a finite group G always divides the order of G . As a consequence of this result, we have the following (also called Lagrange's theorem):

Theorem 1.1 (Lagrange). *Every element in a finite group G of order n is killed by n , i.e. the order of g divides n for all $g \in G$.*

The author was supported by Agence Nationale de la Recherche under grant ANR-20-CE40-0013.

It is only with the development of modern algebraic geometry, particularly through the introduction of the language of schemes, that the full depth of this classical theorem became apparent. Indeed, the scheme theoretic viewpoint makes it possible to return, in some sense, to Lagrange's original perspective on polynomial equations and reinterpret it in a far more structural and conceptual way. Indeed, in his theory of resolvents, Lagrange treated all the roots of a polynomial as formal variables subject to algebraic relations, and he studied how polynomial expressions in these formal variables behaved under permutations.

In a similar spirit and in modern terms, one can start with a polynomial equation and consider the spectrum of the ring of polynomials over a fixed base ring modulo some starting equations. In special situations, this quotient ring admits a Hopf algebra structure. In other words, polynomial expressions in which the formal variable is a solution of the starting equations can be combined in a way that respects the standard axioms of a group operation. In modern language, one is then dealing with an affine group scheme, that is, a group object in the category of affine schemes over a fixed base ring.

When an affine group scheme $G = \text{Spec}(A)$ over any local base ring R (sufficiently nice, see Notation and Terminology) is finite and flat, there is a well-defined notion of order of G , which is a positive integer and we denote it n_G . As we will clarify better later on, such integer is simply the rank of the finite and free R -Hopf algebra A . Now, since for every positive integer n , we have a natural R -morphism $[n]: G \rightarrow G$ which is the multiplication-by- n morphism, it makes sense to consider the property for a finite flat group scheme G to be killed by its order. Indeed, this means that the morphism n_G is the zero morphism. For a comprehensive introduction to the theory of finite affine group schemes, we refer the reader to [11] and [8].

It is very interesting, rephrasing the words of Grothendieck [2, Exposé VIII, Remarque 7.3.1] around the 1970s, to try to understand when Lagrange's theorem (i.e. Theorem 1.1) can be extended in the context of group schemes, i.e. is it true that every finite flat group scheme G over any base scheme is killed by its order?

Denote by $\exp(G)$ the minimal positive integer m such that the multiplication-by- m morphism $[m]: G \rightarrow G$ factors through the unit section $e_G: S \rightarrow G$. In Hopf algebra terms, this is equivalent to ask that the Kernel of the induced ring morphism $[m]: G \rightarrow G$ contains the augmentation ideal I_G . Grothendieck's question can then be rephrased by asking whether the positive integer $\exp(G)$ divides the order $\text{ord}(G)$ of the group scheme G .

More than 55 years after Grothendieck's question was first posed, it still remains unanswered in its full generality. In this short note, we investigate the question, its history, and the main ideas behind the most general results in the literature.

Structure of the paper. Section 2, immediately following the introduction, is devoted to the introduction of the main objects of study and the central question, together with some historical remarks and relevant examples. Section 3 discusses the cases in which the main question has already been settled. Finally, Section 4 presents the most general results and outlines the methods used in their proofs.

Acknowledgements. This short article is based on a talk given in August 2025 at the conference RENE25, held in Tahiti, French Polynesia, on the occasion of the retirement of Prof. René Schoof and in celebration of his research interests. I would like to thank the organizers of the conference, Gaetan Bisson and Roger Oyono, for inviting me to participate and for their support. I am also grateful to René Schoof for the numerous exchanges on this subject and for sharing his insights. I would like to thank both reviewers for their careful reading of the manuscript and for their detailed and insightful feedback, which significantly improved the clarity and exposition of the article. I would also like to thank Alexander Rahm for his constant support.

Notation and Terminology. If X is a scheme, we denote by $\mathcal{O}_X$ its structure sheaf. When the base scheme T of the scheme G is affine, i.e. $T = \operatorname{Spec}(R)$, we may refer to G as defined over R , rather than T . We also write $G \otimes_R S$ for the base change of G from $\operatorname{Spec}(R)$ to $\operatorname{Spec}(S)$.

2 The general setting and the main question

Let S be any base scheme and let G be an S -scheme. We say that 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. Note that in order to study the properties of the $\mathcal{O}_S$ -rank of $\mathcal{O}_G$ we can assume by restriction and without loss of generality, that the base scheme S is the spectrum of a local ring. In this case, since any finite scheme over an affine base is affine, we have that G is an affine, finite flat group scheme over S , i.e. if $S = \operatorname{Spec}(R)$ where R is a local ring then we have that $G = \operatorname{Spec}(A)$ where A is an Hopf algebra over R which is finite and free as an R -module. Without loss of generality, we can also assume that R is a local Noetherian ring. It is indeed sufficient to note that the Hopf algebra structure of A is determined by a finite number of matrix entries once a basis as an R -module is fixed. These reduction arguments are well known in algebraic geometry (see for example [6, Section 1] and [7]) and they go back to the 1960s when they have been precisely described by Grothendieck [3, Sections 8.9, 8.10, and especially 9.2]).

The order of the finite flat group scheme G over $\operatorname{Spec}(R)$ is defined as the rank of the finite free R -module A . Denote by $m: A \rightarrow A \otimes A$ the associated comultiplication morphism of algebras, by $\varepsilon: A \rightarrow R$ the unit section of G and by I the augmentation ideal, i.e. $I = \operatorname{Ker}(\varepsilon)$. For every positive integer n , we have the multiplication-by- n morphism, denoted $[n]: G \rightarrow G$, obtained via a composition of the comultiplication m with the diagonal map).

Finally, we are ready to describe in precise terms what it means for G to be killed by its order. Indeed, we say that the positive integer n kills G if $I \subseteq \operatorname{Ker}([n]: A \rightarrow A)$, i.e. the morphism $[n]$ factors via the unit section ε .

We now state Grothendieck question, as it was originally formulated [2, Exposé VIII, Section 7]:

Question (Grothendieck, 1970s). *Is it true that every finite flat group scheme G over any locally Noetherian base scheme S is killed by its order?*

We can do a further reduction and assume that R is a local Artin ring. Indeed, denote by $\mathfrak{m}$ the maximal ideal of the local Noetherian ring R and assume that the question has a positive answer for every finite flat group scheme G defined over a local Artin ring. For every positive integer k , let h be the R -linear morphism $A \rightarrow A$ defined as $h := [n_G] - p \circ e_S$ where p is the structure morphism $G = \text{Spec}(A) \rightarrow \text{Spec}(R)$ and, as usual, e_S is the unit section. By our assumption, the R -linear morphism is 0 modulo $\mathfrak{m}^k$ for all positive integers k . By Krull's intersection theorem, we deduce that h must be the zero morphism, i.e. the multiplication-by- n_G morphism factors through the unit section.

Moreover, we have the connected-étale fundamental exact sequence

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

where G° is the connected component and $G^{\text{ét}}$ is the largest étale quotient (see for example [8, Section 3.7]). Classical group theory implies that $G^{\text{ét}}$ is killed by its order. Hence, we can assume that G is connected (i.e. it is a local group scheme, meaning that its attached R -Hopf algebra is local). Indeed, thanks to a result of Grothendieck (see, for example, [8, Sections 3.4 and 3.5]), we have $\text{ord}(G) = \text{ord}(G^\circ) \cdot \text{ord}(G^{\text{ét}})$. Now, since every étale group scheme is killed by its order, we find that G is killed by its order if and only if its connected component G° is killed by its order.

Since finite flat group schemes over the local Artin ring R of residue field of characteristic 0 are étale, we can also assume that the residue field of R has characteristic p for a rational prime p .

In view of all the reductions explained above, a positive answer to Grothendieck's original question would follow from a positive answer to the following:

Question (Grothendieck, 1960s, reduced version). *Is it true that every finite flat connected group scheme $G = \text{Spec}(A)$ over a local Artin ring R of positive residue characteristic is killed by its order?*

This is the final version of Grothendieck's question that still has not found an answer. Much progress have been made since the 1960s and most of them concerns special cases where strong assumptions are made on G or on R . We will discuss the known cases in the next section. Let's now take a look at some important examples that will be useful later on.

Example 2.1 (the group of roots of unity). Consider the multiplicative group G_m over a ring R as an affine group scheme and fix a positive integer n . We define $\mu_{n,R}$ (or simply μ_n when the base ring is clear) as the kernel of the multiplication-by- n morphism $[n]: G_m \rightarrow G_m$. The group scheme μ_n is finite and flat of order n . Indeed, it is determined by the R -Hopf algebra $A := R[x]/(x^n - 1)$ with comultiplication $m: A \rightarrow A \otimes_R A$ sending $x \mapsto x \otimes x$ and unit section generated by $x - 1$.

Example 2.2 (the group α_p). Let R be a ring of characteristic p and define the finite flat group scheme α_p as the subgroup of the additive group scheme G_a defined by the R -Hopf algebra $A := R[x]/(x^p)$ with comultiplication $m: A \rightarrow A \otimes_R A$ sending $x \mapsto x \otimes 1 + 1 \otimes x$ (as expected from a subgroup scheme of G_a) and unit section generated

by x . As R -schemes, we have that α_p and μ_p are isomorphic but as group schemes they are not. For example, the group scheme α_p is self-dual and it is defined only over base ring of characteristic p .

Example 2.3 (semi-direct product). One way to construct interesting group schemes is (as for the classical groups case) to consider actions and the associated semi-direct products. Let R be a ring of characteristic p . As we will see later on, there is an action of G_m over G_a which induces several possible actions of the group scheme μ_{p^m} on α_p , where m is any fixed positive integer. Note that here an action is a R -scheme morphism $\mu_{p^m} \times \alpha_p \rightarrow \alpha_p$. Let k be a perfect field of characteristic p and define the k -group scheme $G_1 = \text{Spec}(k[x, y]/(x^p, y^{p^m} - 1))$ where the comultiplication m sends $x \mapsto y \otimes x + x \otimes 1$ and $y \mapsto y \otimes y$ and the unit section is given by x and y . There are several ways to describe the finite flat k -group scheme G_1 . For example, it can be described as a semi-direct product of μ_{p^m} by α_p , i.e. $G_1 = \alpha_p \rtimes \mu_{p^m}$. Another description, maybe more intuitive, consists in writing G_1 as a k -subgroup scheme of GL_2 , i.e.

$$G_1 = \begin{pmatrix} 1 & \alpha_p \\ 0 & \mu_{p^m} \end{pmatrix}$$

The interested reader can explicitly check that the comultiplication described above for G_1 coincides exactly with the 2×2 matrix multiplication in GL_2 over k . As a side note, we remark that, when $m = 1$ the finite flat k -group scheme G_1 has order p^2 but it is not commutative, contrary to the classical finite groups setting where every finite group of order p^2 is indeed commutative.

Example 2.4 (torsion points of elliptic curves). Finally, in the last example we show how the commutative group schemes that we introduced above actually appear in nature. Indeed, one of the main sources of finite group schemes is given by torsion points on abelian varieties. Consider for example an elliptic curve E over a Noetherian scheme S and fix as usual a positive integer n . Then the S -morphism $[n]: E \rightarrow E$ is finite and flat among Noetherian schemes and so the n -torsion points are represented by $E[n] := \text{Ker}([n])$ which is a commutative finite flat S -group scheme of order n^2 . In some cases, we can describe explicitly the structure of $E[n]$ as a group scheme. Assume that $S = \text{Spec}(R)$ where R is a complete Noetherian local ring with perfect residue field of positive characteristic p , and assume that the elliptic curve E has good reduction. If n is invertible, the finite flat group scheme $E[n]$ is étale and so it is isomorphic to the constant group scheme $(\mathbb{Z}/n\mathbb{Z})^2$ over an algebraic closure of k . By the Chinese remainder theorem, we can focus on the case where n is a power of p , say $n = p^r$ for some positive integer r . First, we consider the connected-étale exact sequence:

$$0 \longrightarrow E[p^r]^\circ \longrightarrow E[p^r] \longrightarrow E[p^r]^{\text{ét}} \longrightarrow 0.$$

Over the perfect field k of characteristic p , the sequence splits and by a result of Grothendieck (see [1, Exposé VII_A, Section 4 “Frobeniusseries”]) the kernel of the Frobenius morphism is not an isomorphism, and so the connected component in the above exact sequence is non-zero. In other words, the finite flat group scheme $E[p^r]$ is not étale. Now, we have (over k) that $E[p^r] = E[p^r]^\circ \times E[p^r]^{\text{ét}}$ and the finite flat k -group scheme

$E[p^r]^\circ$ has order p^r or p^{2r} . When E has ordinary reduction, the étale part $E[p^r]^{\text{ét}}$ has order exactly p^r and over a separable closure of k we have that $E[p^r]^{\text{ét}}$ is the constant group scheme $\mathbb{Z}/p^r\mathbb{Z}$. Since elliptic curves are principally polarized abelian varieties, the k -group scheme $E[p^r]$ is self-dual and since the dual of the constant group scheme of order p^r is the group scheme μ_{p^r} , we conclude that over a separable closure of k we have that $E[p^r] \cong \mu_{p^r} \times \mathbb{Z}/p^r\mathbb{Z}$. If E has supersingular reduction, the étale component is trivial and the k -group scheme $E[p^r]$ is connected (i.e. local) of order p^{2r} . Moreover, the group scheme $E[p^r]$ admits a complete filtration of successive quotients (induced by the kernel of the powers of the Frobenius morphism) isomorphic to α_p , which is the only local (with local Cartier dual) simple group. This connected group might be particularly difficult to describe and one has to rely on the theory of Dieudonné modules. For example, one can prove that, for $r = 1$, the group scheme $E[p]$ is a non-split extension of α_p by α_p .

3 The known cases

3.1 The commutative case

In this section, we describe the special case where the finite flat group scheme $G = \text{Spec}(A)$ over the ring R is commutative. In intuitive terms, this means that if we look at the formulas describing the comultiplication morphism $m: A \rightarrow A \otimes A$, then we have that these are symmetric in the variables chosen to generate the R -Hopf algebra A (see the examples in Section 2).

The assumption of G being commutative has several consequences in regard to our question. Indeed, starting by looking at the classical finite groups case, the fact that one deals with a commutative group implies that multiplication-by- n is a group homomorphism. This allows us to conclude directly that if G is a finite commutative group and if n is its order then for every $g \in G$ we have:

$$\prod_{h \in G} h = \prod_{h \in G} gh = g^n \prod_{h \in G} h,$$

or in other words, the finite group G is killed by its order. Despite the many differences between the general case of finite flat group schemes and the classical finite groups, here is when the theories somehow get closer again. Indeed, Pierre Deligne proved around 1970s, that the above proof can essentially be adapted to the finite commutative group schemes case, once the proper language is introduced.

In order to be precise, Deligne proved the following:

Theorem 3.1 (Deligne, 1969). *Let R be a Noetherian ring and let G be a finite flat commutative group scheme. Then G is killed by its order, i.e. the morphism $[n_G]: G \rightarrow G$ is the zero morphism.*

Proof. Although Deligne didn't publish the result himself, there are several references available with Deligne's original proof. See for example [7, Section 3] or [9, Section 1].

□

The idea behind the proof is to mimic the proof for the classical finite groups case mentioned above, once the proper terminology is introduced. Consider the finite flat group scheme $G = \text{Spec}(A)$ over R , without loss of generality we can assume that A is finite and free as an R -algebra. For any R -algebra S , Deligne introduces a norm map $N: S \rightarrow R$ defined as the determinant of the multiplication-by- s morphism for all elements $s \in S$. Since G is commutative, there exists a notion of dual of G , say $G^\vee$, which is also a finite flat group scheme over R . In particular, the Hopf algebra $A^\vee$ of $G^\vee$ is the R -linear dual of the R -Hopf algebra of G . The key point is that using these notions, one can write the equivalent for finite flat group schemes of what it was the product of all elements for finite groups, i.e. the norm map of the dual group scheme evaluated in the identity, or in other words $N_{A^\vee}(\text{Id}_A)$ where Id_A is the identity morphism of A . The proof then proceeds in the same way as the classical case. Note that extending this proof to the case of non-commutative group schemes is not possible since we do not have anymore a notion of dual group scheme, i.e. the R -linear dual of the R -Hopf algebra A does not have anymore a natural structure of Hopf algebra.

For more details, the interested reader can take a look at [7, Section 3].

3.2 The base scheme is reduced

In this section, we treat one of the first special cases considered by Grothendieck himself which already appears in [2, Exposé VIII]. This is the case where we consider finite flat group schemes over a field k , or as we will see later, over a reduced base ring.

Hence, let $G = \text{Spec}(A)$ be a finite flat group scheme over a field k . Since finite flat group schemes over a field of characteristic zero are étale, in order to answer's Grothendieck's question, we can assume without loss of generality that the field k has characteristic p , where p is a prime number.

The main result of this section is the following:

Proposition 3.2. *Let G be a connected group scheme over a field k of characteristic p . Let n_G be the order of G , then the morphism $n_G: G \rightarrow G$ is the zero morphism, i.e. G is killed by n_G .*

Proof. The original proof of this result by Gabriel and Grothendieck can be found in [1, Exposé VII_A, Proposition 8.5]; for a version using a result of Edixhoven which we describe below, see [6, Section 2]. $\square$

We describe briefly below the main ideas and key steps. There are several possible approaches in order to prove this result, but they all revolve around the following argument. Let $G = \text{Spec}(A)$ where A is a k -Hopf algebra and denote by I_A its augmentation ideal, i.e. the kernel of the unit section $\varepsilon: A \rightarrow k$. Since G is connected and k is of characteristic p , we have that $n_G = p^r$ for some positive integer r . Since we are in characteristic p , we can consider the Frobenius morphism $F: G \rightarrow G^{(p)}$ and its Kernel which is a proper finite flat group scheme over k . The sequence $G[F^i]$ defines a composition series of subgroups of G whose consecutive quotients have height less or equal 1. This opens up the possibility of reducing the problem to show that the above proposition holds for those group schemes of height 1 and then proceed by induction

on the unipotent length. If the height is 1, the situation can be described explicitly in simple terms. Indeed, since k is perfect, it means that the k -Hopf algebra A is of the form $k[x_1, \dots, x_r]/(x_1^p, \dots, x_r^p)$ where $x_1, \dots, x_r$ are the so called primitive elements (see for example [1, Exposé VII_A, Section 7.4]). In particular, in this special situation, it is clear that the maximal length of a monomial in A (where variables are counted with multiplicities) is $r(p-1)$. In other words, this observations is equivalent to say that the augmentation ideal I_A satisfies $I_A^{r(p-1)+1} = 0$. This fact is very important (and it doesn't have a known analogue in the general height case) because it implies that if one can prove that the multiplication-by- p morphism $p: G \rightarrow G$ satisfies $p(I_A) \subset I_A^p$, then the claim follows since

$$n_G(I_A) = p^r(I_A) \subseteq I_A^{p^r} \subseteq I_A^{r(p-1)+1} = 0,$$

and so G is killed by n_G . This is exactly the original approach of Gabriel and Grothendieck in [1, Exposé VII_A] (see for example prop. 8.5), where the key point $p(I_A) \subset I_A^p$ is proven using the p -Lie algebra associated to G .

Another very elegant and general way to prove the key point above has been proposed by Edixhoven (see for example [6]) who proved the following:

Proposition 3.3 (Edixhoven, 2001). *Let $G = \text{Spec}(A)$ be a finite flat group scheme over any ring R . Let p be a prime and let $[p]: A \rightarrow A$ be the algebra morphism associate to the multiplication-by- p morphism $G \rightarrow G$. Then we have $[p](I_A) \subseteq pI_A + I_A^p$, where I_A denotes the augmentation ideal.*

Proof. The result has not been published by Edixhoven himself but its original statement and proof can be found in [6, Proposition 2.1]. $\square$

From this proposition, it is immediate that, when G is a connected finite flat group scheme defined over a field of characteristic p , then our Question has a positive answer.

Moreover, assume that G is now defined over a reduced local scheme $S = \text{Spec}(R)$. Then the morphism $n_G: G \rightarrow G$ is zero if it is zero on its fibers on closed points. In particular, for any closed point $s \in S$, the fiber $G_s := G \times_S \text{Spec}(k(s))$ is killed by its order or, in other words, the multiplication-by- n_G morphism is the zero morphism.

4 Some results on the general case

In this section, we present the few results known about the general case and the main ideas behind those results. As a notation remark, in order to be consistent with the references [6] and [10], we will use the additive description for the finite flat k -group scheme μ_{p^n} when k is a perfect field of characteristic p , i.e. $\mu_{p^n} = \text{Spec}(k[y]/(y^{p^n}))$ with group law $y \mapsto 1 \otimes y + y \otimes 1 + y \otimes y$ and unit section generated by y .

According to the reductions made in section 1, we deal here with finite flat group schemes defined over a local Artin ring R whose residue field has characteristic p . We denote by $\mathfrak{m}$ the maximal ideal of R .

We start by the following:

Theorem 4.1 (Schoof, 2001). *Assume that $\mathfrak{m}^p = p\mathfrak{m} = 0$. Every finite flat group scheme over R is killed by its order, i.e. $[n_G]: G \rightarrow G$ is the zero morphism.*

Proof. This is [6, Theorem 1.1]. □

In order to obtain this general result, several strategies are put in place. We now describe these strategies and how they lead to a proof of the above result. First, we observe that studying the reduced version of the Question has the great advantage that local Artin rings can be ordered by their length. Hence, this opens up the possibility of proceeding by induction. Now, since the strict Henselization of the local Artin ring R is flat over R , without loss of generality we can assume that the residue field k of characteristic p is separably closed. Now, we consider two separate cases. Indeed, if G is our finite flat group scheme over R we can consider the base change $\overline{G} := G \otimes_R k$ (i.e. the special fiber of G). Assume that $\overline{G}$ (and G) has order p^{m+1} (for psychological reasons that will be clear later on) for a certain non-negative integer m . We have that $\overline{G}$ is either killed or not killed by p^m . We will treat the two cases separately. Note that we can also assume that m is a positive integer. Indeed, if $m = 0$ then our finite flat group scheme G has order p , and a theorem of Tate (see [9, Theorem 1]) ensures that every such group is commutative, and so by Deligne's theorem (see [9, Section 1]) is killed by its order.

Now, the case when $\overline{G}$ (of order p^{m+1}) is killed by p^m , is the most difficult to treat and it is the reason why Schoof introduces the hypothesis $\mathfrak{m}^p = p\mathfrak{m} = 0$ on the ring R . Under this hypothesis we can conclude in one line. Indeed, the fact that $\overline{G}$ is killed by p^m implies that $[p^m](I) \subset \mathfrak{m}A \cap I = \mathfrak{m}I$, where as usual I denotes the augmentation ideal of G over R . Now, it is enough to apply Edixhoven's result (i.e. Prop. 3.3), and deduce that $[p^{m+1}](I) \subset p\mathfrak{m}I + (\mathfrak{m}I)^p = 0$ under the strong hypothesis $\mathfrak{m}^p = p\mathfrak{m} = 0$.

Now, if $\overline{G}$ is not killed by p^m , then Schoof introduces the new strategy of using deformation theory in order to classify all such finite flat group schemes. Indeed, Schoof first proves that (recall that here k is separably closed of characteristic p) every finite flat group scheme $\overline{G}$ of order p^{m+1} over k is not killed by p^m if and only if it is isomorphic to either $\mu_{p^{m+1}}$ or the k -group scheme $G_1 = \begin{pmatrix} 1 & \alpha_p \\ \alpha_p & \mu_{p^m} \end{pmatrix}$ which we encountered in the first section. By earlier work of Grothendieck et al. [2, Exposé X, Corollaires 2.3 and 2.4] on group schemes of multiplicative type, it follows that the finite flat group scheme μ_{p^m} has no non-trivial deformations, meaning that if $\overline{G} \cong \mu_{p^{m+1}}$ over k forces $G \cong \mu_{p^{m+1}}$ over R .

Finally, the remaining case to be treated is when G is a deformation over R of $\overline{G} \cong G_1$ as finite flat k -group schemes. Schoof is able to completely classify such deformations and Theorem 4.1 follows at once from the following final statement:

Theorem 4.2. *Let p be a prime and let R be a local Artin ring of residue field k of positive characteristic p . Let G be a finite flat group scheme over R such that $\overline{G} \cong G_1$, then:*

- (1) R has characteristic p ,
- (2) G is potentially the trivial deformation, i.e. there is a finite flat R -algebra S such that $G \otimes_R S \cong G_1 \otimes_R S$.

Proof. This is [6, Proposition 3.3]. $\square$

From this classification result on the deformations of G_1 , it follows that any such deformation is killed by its order, since G_1 is killed by its order over any base ring. This concludes the proof of Theorem 4.1.

We can continue on this line of attack a bit more. Indeed, over the perfect residue field k , there are other finite flat group schemes G , apart from G_1 , which sits in the exact sequence:

$$1 \longrightarrow \alpha_p \longrightarrow G \longrightarrow \mu_{p^m} \longrightarrow 1.$$

Indeed, for any $\lambda \in \{1, \dots, p^m - 1\}$, there is a unique (up to isomorphism) finite flat k -group scheme G_λ which sits in the above sequence (see for example [10]). Namely, we have that G_λ coincides with the semi-direct product $\alpha_p \rtimes_\lambda \mu_{p^m}$, where the subscript λ denotes that the action of μ_{p^m} on α_p is given by the R -morphism $\varphi_\lambda: \mu_{p^m} \times \alpha_p \rightarrow \alpha_p$ where $\varphi_\lambda(y, x) = (1 + y)^\lambda \otimes x + x \otimes 1$ (here x and y are the chosen variables respectively for the R -Hopf algebra of α_p and μ_{p^m}).

We recall here its explicit description (for more details on this construction see [10]): for $\lambda \in \{1, \dots, p^m - 1\}$, the k -group scheme G_λ is given by:

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

with group law:

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

Imposing the condition $\lambda = 1$, we recover the finite flat k -group scheme G_1 (introduced before with multiplicative notation) which can be described as the k -group scheme

$\begin{pmatrix} 1 & \alpha_p \\ 0 & \mu_{p^m} \end{pmatrix}$. One can indeed check that the group law described above coincide with the matrix multiplication law when $\lambda = 1$. It is interesting to note 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). No analogous phenomenon occurs in the classical theory of finite abstract groups, where every group of order p^2 is commutative.

One important properties of the k -group schemes G_λ is that they only depend on the p -adic valuation of λ , i.e. if λ and λ' have the same p -adic valuation then the groups G_λ and $G_{\lambda'}$ are isomorphic (see [10, Section 2]).

Moreover, the k -group scheme G_1 is the only one (up to isomorphism) among the k -group schemes G_λ which is not killed by p^m , even though they are all of order p^{m+1} (see [10, Section 2]). This means that Grothendieck's question for R -deformations of the k -group schemes G_λ (for a generic λ) cannot be answered via Schoof's strategy, unless imposing the conditions $\mathfrak{m}^p = p\mathfrak{m} = 0$ on R . In what follows, we describe the author's result that aims at covering these missing cases. Indeed, we have the following:

Theorem 4.3 (T., 2025). *Let p be a prime and let R be a local Artin ring of residue characteristic p . Let G be a finite flat group scheme over R such that there is a $\lambda \in \{1, \dots, p^m - 1\}$ such that $\overline{G} \cong G_\lambda$, i.e. G is a deformation of one of the G_λ 's.*

Then G is killed by its order, i.e. Grothendieck's question has a positive answer for G .

Proof. See [10, Theorem 1.3]. □

The key strategy is again to take a look at all the possible deformations of the group schemes G_λ . An analysis of the possible deformations shows that all the R -deformations of the k -group schemes G_λ are trivial, apart from the unexpected case where $\lambda = p^m - 1$. As a consequence, the above theorem follows easily for all λ apart from the case $\lambda = p^m - 1$ where the deformations can be in any case described explicitly and it is straightforward to check that they are killed by their order. The Hopf algebra computations necessary to classify explicitly the infinitesimal deformations of the groups G_λ allow us to bypass Schoof's original restriction on the maximal ideal $\mathfrak{m}$, i.e. $\mathfrak{m}^p = p\mathfrak{m} = 0$. Indeed, the use of the techniques developed in SGA and EGA concerning the infinitesimal deformations (see [10, Section 3]) allow us to classify explicitly the polynomials $a(x, y)$ and $b(x, y)$ for any generic deformation $R[x, y]/(x^p - a(x, y), y^{p^m} - b(x, y))$ by imposing flatness conditions and compatibility as deformations of the k -group scheme G_λ . This strategy allows us also to describe all deformations of the group schemes G_λ without having to consider base changes (as is done in part (2) in Theorem 4.2).

Theorem 4.3 is the final piece that ensures that Grothendieck's Question has an affirmative answer for all finite flat R -group schemes G whose special fiber is an extension of μ_{p^m} by α_p . In general, the strategy of classifying all deformations of a given finite flat group scheme seems hard to carry on apart from specific cases, however the techniques from SGA and EGA considered in order to prove Theorem 4.3 are very powerful and they contributed to answering unconditionally on R Grothendieck's Question for certain types of groups, so maybe they will play an important role in the future concerning this question.

References

- [1] Michel Demazure and Alexandre Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie: Schémas en groupes (SGA 3), tome 1*. Volume 151 of *Lecture Notes in Mathematics*, Springer, 1970. DOI: 10.1007/BFb0058993.
- [2] Michel Demazure and Alexandre Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie: Schémas en groupes (SGA 3), tome 2*. Volume 152 of *Lecture Notes in Mathematics*, Springer, 1970. DOI: 10.1007/BFb0059005.
- [3] Alexander Grothendieck. *Éléments de Géométrie Algébrique, chapitre IV: Étude locale des schémas et des morphismes de schémas, troisième partie*. Volume 28 of *Publications Mathématiques*, Institut des Hautes Études Scientifiques, 1966. DOI: 10.1007/BF02684343.

- [4] Ariane Mézard, Matthieu Romagny, and Dajano Tossici. Models of group schemes of roots of unity. *Annales de l'Institut Fourier*, 63(3):1055–1135, 2013. doi: 10.5802/aif.2784.
- [5] Richard L. Roth. A history of Lagrange's theorem on groups. *Mathematics Magazine*, 74(2):99–108, 2001. doi: 10.1080/0025570X.2001.11953045.
- [6] René Schoof. Finite flat group schemes over local Artin rings. *Compositio Mathematica*, 128:1–15, 2001. doi: 10.1023/A:1017560215203.
- [7] René Schoof. Is a finite locally free group scheme killed by its order? In *Open Problems in Algebraic Geometry*, volume 46 of *Advanced Lectures in Mathematics*, pages 1–7. International Press, 2018. ISBN: 9781571463739.
- [8] John Tate. Finite flat group schemes. In *Modular Forms and Fermat's Last Theorem*, pages 121–154. Springer, 1997. doi: 10.1007/978-1-4612-1974-3_5.
- [9] John Tate and Frans Oort. Group schemes of prime order. *Annales scientifiques de l'École normale supérieure*, 3(1):1–21, 1970. doi: 10.24033/asens.1186.
- [10] Emiliano Torti. Lagrange's theorem for a class of finite flat group schemes over local Artin rings. *Documenta Mathematica*, forthcoming. doi: 10.4171/DM/1055.
- [11] William C. Waterhouse. *Introduction to Affine Group Schemes*. Volume 66 of *Graduate Texts in Mathematics*. Springer, 1979. doi: 10.1007/978-1-4612-6217-6.