Is a finite group scheme annihilated by its rank?

Frans Oort

Utrecht University

Workshop on Hopf Algebras,
Hanoi, October-November 2023

Introduction.

In the previous talk we considered finite group group schemes

(1) defined over over an *algebraically closed ground field*, and
(2) we considered *commutative* group schemes and
(3) moreover we considered group schemes *annihilated by p*.

In this talk we drop all three conditions, and we wonder

Is a finite group scheme annihilated by its rank?

In the previous talk I discussed a proved theorem, and I hope you enjoyed the beauty of that proof.
In this talk I discuss an *open problem* on which I am working since 1966.
Below I will discuss some cases where the answer is known to be positive. Furthermore I discuss some (im)possible approaches. Up to now these all failed. I give no guarantee that material developed and discussed is useful.

Some notation. Although the title says "group schemes" all of them will be *finite* and equivalently I will discuss Hopf algebras.

We write p for a fixed prime number. We write k for an algebraically closed field of characteristic p. Saying G/S is a *finite* group scheme we assume $G \to S$ is locally free and of finite presentation.
Most of the time we take a local artin ring R; over R for a finitely generated module the concepts

$$\text{"flat"} \leftrightarrow \text{"projective"} \leftrightarrow \text{"free"}$$

are equivalent. In this case a finite group scheme G over R corresponds with a R Hopf algebra E, where $E \cong R^m$ for some $m \in \mathbb{Z}_{>0}$; here m is called the *rank* of G/S: we distinguish the notion of *order* of a finite group, versus *rank* of a finite group scheme. In case we use the term "rank" we assume the group scheme is of constant rank over the base scheme.

For a finite group scheme G/S and an integer d we write $[d] : G \to G$ for the *morphism* "exponentiation" by d. For a group this is the map $g \to g^d$. For a group scheme G/S and a scheme theoretic point $x \in G(T)$ this is $x \to x^d$. On the level of a Hopf algebra this ring homomorphism is

$$[d] : \left(E \xrightarrow{s_d} E^{\otimes d} \xrightarrow{\text{mult}} E \right).$$

For a finite group scheme of constant rank m over the base we study the question:

$$[m] : \left(E \xrightarrow{s_m} E^{\otimes m} \xrightarrow{\text{mult}} E \right) \quad \stackrel{?}{=} \quad \left(E \xrightarrow{\varphi} E/I_E = R \to E \right).$$

In group theory, and in the theory of group scheme *in general* $[d]$ *is not a homomorphism*.
The set $G[d]$ of elements x with $x^d = e$ is in general not a subgroup. For a group scheme G/S the subscheme $G[d]$ in general is not a subgroup scheme and in general it is not flat over S.

A little warning

We consider finite group schemes $G \to S$ flat over S. However there are many examples of non-flat finite maps, and of *non-flat finite group schemes* $H \to S$.

Artificial example. Take $H \to \mathbb{A}^1$ with finite, non-trivial H_0 above $0 \in \mathbb{A}^1$ and $H_s = \{1\}$, the trivial group scheme above all $0 \neq s \in \mathbb{A}^1$. Clearly $H \to \mathbb{A}^1$ is a finite morphism and we have a non-flat group scheme.

Natural example. Let $G \to \mathbb{A}^1_k = S$ be a flat group scheme of rank p in characteristic p with $G_0 \cong \alpha_p$, and etale $(G \setminus G_0) \to (\mathbb{A}^1 \setminus \{0\})$. Define $H = \mathrm{Ker}(F : G \to G)$. We see $H \to S$ is a finite morphism and we have a non-flat group scheme.

Natural example. Let $G \to \mathbb{A}^1_k = S$ be a flat group scheme of rank p^2 with $G_0 \cong (\alpha_p)^2$ and geometric generic fiber $G_{\overline{\eta}} \cong \mu_{p^2}$. We see $H := \mathrm{Ker}([p] : G \to G)$ is a finite morphism and we have a non-flat group scheme.

In this talk we consider:

1 Known cases

2 Reduction of the problem

3 Some examples and questions

We will have short *break* after the discussion of examples and questions.

4 Moduli, lifting problems, deformation theory

5 Group schemes of rank p^2

6 Some answers

As you will see, in this talk almost all results are negative. The problem we discuss seems not solved. We discuss some possible, but failed attempts.

1 Known cases.

Etale group schemes.

For a group scheme G/S of rank m, where m is invertible in all local rings of S, we know $G \to S$ is *etale*, hence locally constant, and by group theory (the original Lagrange theorem) we conclude G/S is annihilated by its rank.

In case we work over a field of positive characteristic p, or, more generally over a local ring R with residue characteristic p,

we are reduced to the case that $\mathrm{rank}(G/S) = m = p^n$.

Commutative finite group schemes.

Theorem (Deligne, 1970). *Any* finite commutative *group scheme is annihilated by its rank.*

Comment. In general we can try to *transplant a proof in the theory of groups to the theory of group schemes.*

Suppose H is a finite *commutative* abstract group; in this case we can prove Lagrange's theorem as follows: for any $y \in H$ with $\#(H) = m$ we have

$$(\prod_{z \in H} z) = \prod_{x \in H} (yx) \stackrel{*}{=} y^m \times (\prod_{x \in H} x); \quad \text{hence} \quad y^m = e;$$

The equality $\stackrel{*}{=}$ uses the fact that H is commutative. Deligne had the insight how to formulate this proof "without using elements". For details see the TO paper, Theorem on page 4.

1 Known cases: over a field

Theorem. *Suppose E is a Hopf-algebra finite over a field $R = K$. In this case E is annihilated by its rank.*

There are many proofs for this. We will follow:

Proposition (Edixhoven). *Let A be a finite flat R-Hopf-algebra, with augmentation ideal $I \subset A$. Let p be a prime number. In this case*

$$[p](I) = pI + I^p.$$

Sketch of a proof of the proposition. We may replace R by R/pR.
The regular representation of the Hopf algebra E gives a $p^2 \times p^2$ matrix $S \in \mathrm{GL}_{p^2} = \mathrm{Spec}(B)$, $\quad \varphi : B \to E$.
The entries of $S - \mathbb{1}_{p^2}$ generate the augmentation ideal $I' = I_B \subset B$. As $0 = p \cdot 1 \in R$ we have $S^p - \mathbb{1}_{p^2} = (S - \mathbb{1}_{p^2})^p$.
Hence $[p](I') \subset (I')^p$.
Applying $\varphi : B \to E$ we obtain $[p](I) \subset I^p$ as required.

A finite group scheme over a field is annihilated by its rank

Theorem. *Suppose E is a Hopf-algebra finite over a field $R = K$. In this case E is annihilated by its rank.*

Sketch of a proof of the theorem.
By the exact sequence $G/G^0 = G^{et}$ we only need to show the case of local group schemes. It suffices to show the case $K - k$ is algebraically closed. We see the local Hopf algebra is of rank p^n for some n and p the characteristic of k. By the proposition we have $[p](I) = I^p$ hence $[p^n](I) = I^{p^n} = 0$, which proves the theorem.

2 Reduction of the problem

In order to show that any finite group scheme G/S is annihilated by its rank, or to give a counter example, it suffices to consider the following

Question. *Let p be a prime number, $n \in \mathbb{Z}_{>0}$ and $m = p^n$. Let R be a local artin ring with residue field $k = R/\mathfrak{m}_R$ algebraically closed of characteristic p. Is every finite local group scheme G/R of rank m annihilated by its rank?*

We sketch the reduction steps. (1) Start with a finite $G \to S$; covering S by affines it suffices to consider $S = Spec(\Gamma)$.
(2) It suffices to assume $S = \mathrm{Spec}(R)$, where R is a *local artin ring.*
(3) By the exact sequence $G/G^0 = G^{et}$ if suffices to consider G a *local group scheme.* In that case the residue characteristic of R is positive, call it p, and $\mathrm{rank}(G/R) = p^n$ for some integer n.
(4) Extending R we can assume $R/\mathfrak{m}_R = k$ is *algebraically closed.*

I do not have a definite, final approach to the question whether a finite group scheme is annihilated by its rank.

I present some examples, and some questions one can ask in order to try to achieve progress. This is just a very small list of the various approaches I tried.

3 Some examples and questions

3.1 TO group schemes

Group schemes of rank p are classified over a base with mild conditions. In particular if R is a complete local ring with residue characteristic p:

Theorem (John Tate - FO).

(1) *For a noetherian complete local ring R with residue class field $R/\mathfrak{m}_R = \kappa$, a field of characteristic p, and*

$a, c \in R$ with $ac = p$ and comultiplication $s(-)$ and coinverse $\iota(-)$

given above the result is a R-Hopf-algebra free of rank p.

(2) *Conversely if G is a flat R-group scheme of rank p there exist a, c, s, ι as above such that $G \cong \mathrm{Spec}(R[x])$.*

Notation.

This group scheme will be denoted by $G_a^c = G_{a,R}^c$.
(3) *The group schemes*

$$G_{a_1}^{c_1} \text{ and } G_{a_2}^{c_2} \text{ are isomorphic } R\text{-group schemes}$$

if and only if there exists a unit $u \in R^*$ *such that*

$$u^{p-1}a_1 = a_2 \quad \text{and} \quad u^{1-p}c_1 = c_2.$$

The group schemes $G_{a,b}$. *Using (over a base ring* R*, omitted in the notation here) the group scheme* G_a^c*, with* $ac = p$*, writing* $b = w_{p-1}c$*, we define* $G_{a,b}$ *by*

$$G_{a,b} = G_a^c = G_a^{b/w_{p-1}} = G_{a,w_{p-1}c}, \quad aw_{p-1}c = ab = w_{p-1}p.$$

In particular, if $p{\cdot}1 = 0 \in R$*:* $G_{0,0} = \alpha_p$.

$$\underline{\mathbb{Z}/p}_R = G_{1,0} = G_1^0, \quad \text{and} \quad \mu_{p,R} = G_0^{-1} = G_{0,1}.$$

3.2 Semidirect products

Let N and H be (abstract) groups, written multiplicatively. Let $\varphi : H \to \mathrm{Aut}(N)$ be a homomorphism of groups. We define the *semidirect product*

$$G = N \rtimes_{\varphi} H$$

as follows: as *sets* we have a bijection $G = N \times H$, and the group law on this product is given by:

$$(x_1, y_1) \cdot (x_2, y_2) := (x_1 \cdot \varphi(y_1)(x_2), y_1 \cdot y_2).$$

We see that conjugation on the normal subgroup $N \subset G$ is given by

$$(1, y) \cdot (x, 1) \cdot (1, y^{-1}) = (\varphi(y)(x), 1).$$

Note that $N = \{(x, 1)\} \subset G$ and $H = \{(1, y)\} \subset G$ are subgroups.

Easy considerations in theory of finite groups. The *exponent* of G is the minimum for $\mathrm{order}(x)$ for all $x \in G$.
Suppose the exponent of G is a prime number p. Does this imply G is commutative?
For $p = 2$: any G of exponent 2 is commutative.
Proof: $e = (xy)^2 = xyxy$ hence $xy = y^{-1}x^{-1} = yx$.

For $p \geq 2$: Heisenberg groups, **Construction of** UT(3,p).
Let G be the group generated by x and y with

$$z := x^{-1}y^{-1}xy, \quad xz = zx, \quad yz = zy, \quad x^p = y^p = z^p = e.$$

We see $xy = yxz$, the subgroups $< x, z >$ and $< y, z >$ are normal in G, every element can be written in a unique way as $x^u y^v z^w$, with $0 \leq u, v, w < p$, we have

$$G \quad \cong \quad < x, z > \rtimes < y > \quad \cong \quad < y, z > \rtimes < x >,$$

the order of G equals p^3 and G is *not commutative*.

The exponent of a Heisenberg group

$p = 2$ The Heisenberg group UT(3,2) $\cong D_8$ is the dihedral group of order 8, it is non-commutative, and its exponent is 4.

$p > 2$ *The Heisenberg group* UT(3,p) *is non-commutative and its exponent is p.*

Proof. Show that

$$(yxz)^k = y^k x^k z^{1+2+\cdots+k};$$

note that $1 + 2$ is not divisible by 2, and that for $p > 2$ the integer $1 + 2 + \cdots + p = p(p+1)/2$ is divisible by p.

Conclusion: for $p > 2$ there exists a non-commutative group of exponent p.

This Heisenberg group can be defined with the help of 3×3 matrices. I leave that interesting topic to the audience.

3.3 Question A: existence of flat subgroup schemes?

Note:

any finite p-group has a non-trivial centre
(not true for group schemes),

a group of order p^2 is commutative (not true for group schemes).

Method (?!): try to "transplant an idea that works for abstract groups into the theory of group schemes". We saw the wonderful theorem of Deligne for commutative groups. Here is another attempt:

Question A. *Let $G \to \mathrm{Spec}(R)$ be a finite local group scheme over a local artin ring (say, of rank p^n with $n \geq 2$). Does G contain a subgroup scheme $\{e\} \subsetneqq N \subsetneqq G$ flat over S?*

Comment. A positive answer to this question would solve our problem (apply induction on the rank of G).
For any non-trivial G and $R \neq R/\mathfrak{m}_R$ the answer is "yes" for the question where you drop the condition N is flat over R.

3.4 A non-commutative group scheme of rank p^2

An easy way to remember the construction over a field of characteristic p is:

$$\mathcal{T} = \begin{pmatrix} \mu_p & \alpha_p \\ 0 & 1 \end{pmatrix}.$$

This group scheme $\mathcal{T}$ has the following properties:

- $\mathrm{rank}(\mathcal{T}) = p^2$ and $\mathcal{T}$ is non-commutative;
- $\mathcal{T} = \mathrm{Spec}(R[\rho, \sigma]/(\rho^p - 1, \sigma^p))$, the comultiplication is given by

  $$s(\rho) = \rho \otimes \rho, \quad s(\sigma) = \rho \otimes \sigma + \sigma \otimes 1,$$

  the augmentation is given by $\rho \mapsto 1$, $\sigma \mapsto 0$,
  and the coinverse is given by $\rho \mapsto 1/\rho$, $\sigma \mapsto -\sigma/\rho$;

- there is an exact sequence

$$e \to \alpha_p \to \mathcal{T} \to \mu_p \to e,$$

$$R[\sigma'] \twoheadleftarrow R[\rho, \sigma] \hookleftarrow R[\rho], \quad \sigma' \leftarrow\!\shortmid \sigma,$$

where the normal subgroup $\alpha_p \subset \mathcal{T}$ is given by $\rho \mapsto 1$ and there is a subgroup $\mu_p \subset \mathcal{T}$ given by $\sigma = 0$;

- in fact

$$\mathcal{T} = \alpha_p \rtimes \mu_p, \text{ given by the natural map } \mu_p \hookrightarrow \underline{\mathrm{Aut}}(\alpha_p) \cong \mathbb{G}_m,$$

and *the center of this semi-direct product is the trivial subgroup* $e : S \to \mathcal{T}$.

- Note that $\varphi_1 : \mu_p \hookrightarrow \mathbb{G}_m$ and $\varphi_2 : \mu_p \hookrightarrow \mathbb{G}_m$ give

$$\alpha_p \rtimes_{\varphi_1} \mu_p \cong \alpha_p \rtimes_{\varphi_2} \mu_p.$$

- $\mathcal{T}$ is not annihilated by p, and $\mathcal{T}$ is annihilated by p^2.

3.5 Group schemes of rank p^2

Theorem (Schoof, 2001). *Let $k = \overline{k} \supset \mathbb{F}_p$. Suppose G is a* non-commutative *group scheme of rank p^2 over k. Then $G \cong \mathcal{T} \otimes k$.*

As a corollary we have a classification of all isomorphism classes of group schemes of rank p^2 over k. There are 9 isomorphism classes.

- If G is non-commutative $G \cong \mathcal{T} \otimes k$.
  For commutative group schemes:
- If G is etale with local dual, either $G \cong \underline{\mathbb{Z}/(p^2)}$ or $G \cong (\underline{\mathbb{Z}/p})^2$.
- If G is local with etale dual, either $G \cong \mu_{p^2}$ or $G \cong (\mu_p)^2$.
- If G is local with local dual, as we have seen, there are 4 cases for the Dieudonné modules: $(M'_\emptyset)^2$, $M'_\mathcal{F}$, $M'_\mathcal{V}$, $M_{[\mathcal{FV}]}$.

3.6 Question B: lifting to an integral domain

Note that a finite group scheme over a field is annihilated by its rank. Hence a finite group scheme over an integral domain is annihilated by its rank. Hence we could be interested in:

Question B. *Suppose R is a local artin ring and G_0 a finite group scheme over R. Does there exist an integral domain Γ, a finite group scheme over Γ, and a homomorphism $\Gamma \to R$ such that $G \otimes_\Gamma R \cong R$?*

3.7 Question C: non-commutative group schemes of rank p^2

It is know that for a field $K \supset \mathbb{F}_p$ and the non-commutative group scheme $H_0 = \mathcal{T}$ of rank p^2 constructed in 3.4, and a lifting of H_0 to a local artin ring $R \to K$, with G finite over R and $H \otimes_R K \cong \mathcal{T} = H_0$

$$\text{then } 0 = p{\cdot}1 \in R.$$

Hence, naturally the following question comes up:

Question C. *Suppose R is a local artin ring, residue characteristic p and G is a finite, non-commutative group scheme over R of rank p^2. Does this imply $0 = p{\cdot}1 \in R$?*

We have a short break now.

4 Moduli, lifting problems, deformation theory

Please see te notes for explanation, examples and much more.
We use one construction.

For a given $m \in \mathbb{Z}_{>0}$ we study triples (R, N, β), were R is a commutative ring with $1 \in R$, and $N = \mathrm{Spec}(E) \to \mathrm{Spec}(R)$ is a (finite) group scheme, with augmentation ideal $I = I_E = \mathrm{Ker}(E \to R)$, and

$$\beta : R^{m-1} \xrightarrow{\sim} I$$

is an isomorphism of R-modules. This implies that E is R-free hence R-flat. Note that the interesting case that R is a local ring and E is finitely generated and flat implies that E is R-projective, hence E is R-free, and I is R-free of rank equal to $\mathrm{rank}(E/R) - 1$.

We show that $R \mapsto (R, N, \beta)$ defines a representable functor.
Theorem. *There exists such a triple $(\mathcal{R}^{(m)}, \mathcal{N}^{(m)}, \beta^{(m)})$, we write $\mathcal{R} = \mathcal{R}^{(m)}$, $\mathcal{N}^{(m)} = \mathrm{Spec}(\mathcal{R}^{(m)})$, such that for any triple (R, N, β) there exists a unique ring homomorphism $\psi : \mathcal{R}^{(m)} \to R$ such that*

$$(R, N, \beta) \quad \cong \quad (\mathcal{R}^{(m)}, \mathcal{N}^{(m)}, \beta^{(m)}) \otimes_{\mathcal{R}^{(m)}} R.$$

Proof. The equations for comultiplication, coinverse, and augmentation are given by a finite number of coefficients. Use these as variables T_i; the Hopf-algebra conditions give an ideal $J = J^{(m)} \subset \mathbb{Z}[T_i]$, write $\mathcal{R}^{(m)} = \mathbb{Z}[T_i]/J$, and define the $\mathcal{R}^{(m)}$-Hopf-algebra $\mathcal{R}^{(m)}$ by these relations. For any (R, N, β) the coefficients in its comultiplication, coinverse, and augmentation define $\psi : \mathcal{R}^{(m)} \to R$ and the result follows.

Remark. For any algebraically closed field k the set of k-isomorphism classes of finite group schemes of rank p equals $\mathrm{GL}(k,p)\backslash\mathrm{RingHom}(\mathcal{R}^{(\mathrm{m})},\mathrm{k})$. Even in case the quotient $\mathrm{GL}_p\backslash(\mathrm{Spec}(\mathcal{R}^{(m)})$ would exist, in general $\mathcal{N}^{(m)}$ does not descend to this quotient.

Example. In case $n = p = 2$ we know $R = \mathrm{Spec}(\mathbb{Z}[A, C]/(AC - p))$, and the structure of $R^{(2)} \subset \mathbb{A}^{(2)}_{\mathbb{Z}}$ is known as is proved in the Tate-FO paper.

If $n = p > 2$ the structure of $R^{(p)}$ is more complicated. For Λ_p as in Tate-FO paper, the quotient of $\mathrm{Spec}(\mathcal{R}^{(p)}) \otimes \Lambda_p$ by GL_p and by $\mathbb{Z}/(p-1)$ is isomorphic with $\mathrm{Spec}(\Lambda_p[A, B]/(AB + p))$, which is an integral domain.

It seems not easy to describe $\mathcal{R}^{(m)}$ explicitly for every m.

Expectation. We expect that in case $m = p^n$ any irreducible component $S \subset \mathrm{Spec}(\mathcal{R}^{(p^n)})$ has a geometric point $P_0 \in S(k)$ such that $(\mathcal{N}^{(n)} \mid_S) \times_S P_0 \cong (\alpha_p)^n$.

Structure of moduli spaces of finite group schemes, expectations:

The following could very well be true: consider all irreducible components of $\mathrm{Spec}(\mathcal{R}^{(p^n)})$ and of $\mathrm{Spec}(\mathcal{R}^{(p^n)} \otimes \mathbb{F}_p)$. I would guess:

the number of irreducible components of $\mathrm{Spec}(\mathcal{R}^{(p^2)})$ equals 3 (?)

the number of irreducible components of $\mathrm{Spec}(\mathcal{R}^{(p^2)} \otimes \mathbb{F}_p)$ equals 5, and every of these irreducible components is a reduced scheme (??).

It might be that a precise description of $\mathrm{Spec}(\mathcal{R}^{(p^2)})$ gives an answer to the question whether every group of rank p^2 is annihilated by p^2.

Comments. Compare different situations, e.g. the (coarse) moduli scheme $\mathcal{M}_g$ of algebraic curves of genus $g > 1$ on the one hand and the "moduli space" $\mathrm{Spec}(\mathcal{R}^{(m)})$ for finite group schemes of rank $m = p^n$ constructed here. Note that the automorphism group of a curve of genus $g > 1$ is finite, however the automorphism group of may finite group schemes is infinite. This makes the difference in constructions and in properties

For curves, the geometric points in $\mathcal{M}_g$: there are the infinitely many isomorphism classes of algebraic curves of genus g.

For example for $m = p$ or $m = p^2$ the number of geometric isomorphism classes of group schemes of rank m is finite, but $\mathrm{Spec}(\mathcal{R}^{(m)})$ has infinitely many geometric points because of the rigidification $\beta : R^{m-1} \xrightarrow{\sim} I$. The "moduli space" of isomorphism classes of finite group schemes is not interesting; for geometric and arithmetic applications we have to consider the situation as described here.

5 Group schemes of rank p^2; a negative answer for Question C

We will see that answer to all questions A-B-C are negative, hence no progress in the annihilation-by-rank-problem along these ideas.

Question C. *Suppose R is a local artin ring, residue characteristic p and G is a finite,* non-commutative *group scheme over R of rank p^2. Does this imply $0 = p{\cdot}1 \in R$?*

In fact what is true:

Answer C. *For any prime number p, for any integer $r \in \mathbb{Z}_{>0}$ there exists an R with $p^r{\cdot}1 \neq 0 \in R$, and $a, c, C \in \mathfrak{m}_R$ and $A \in R$ and a non-commutative $G_a^c \rtimes G_A^C$ over R.*
A proof can be found in the notes: study $\underline{\mathrm{Aut}}(G_a^c)$ and find appropriate R and non-trivial $G_A^C \to \underline{\mathrm{Aut}}(G_a^c)$.
For later use we mention: there is a non-commutative $G_a^c \rtimes G_A^C$ over R with $\varepsilon \in \mathfrak{m}_R$, and $\varepsilon^2 = p$ and $\varepsilon^3 = 0$.

An afterthought. We see the curious situation that:

(non-lift) *the non-commutative* $\mathcal{T} = \alpha_p \rtimes_\varphi \mu_p$ *over* $K \supset \mathbb{F}_p$ *cannot be lifted to a ring* R *in which* $0 \neq p{\cdot}1 \in R$

however, for any $r \in \mathbb{Z}_{>0}$

(lift) $\alpha_p \times \alpha_p$ *over* $K \supset \mathbb{F}_p$ *can be lifted to a non-commutative group scheme over a ring* R *in which* $0 \neq p^r{\cdot}1 \in R$.

I have no good description of the moduli space of group schemes of rank p^2.
We see there is a least one irreducible component not over $\mathbb{F}_p$ that carries non-commutative group schemes, but this component does not have a point over an integral domain of characteristic zero.

Problem. *Describe all components of the moduli space* $\mathrm{Spec}(\mathcal{R}^{(p^2)} \otimes \mathbb{F}_p)$. *Is every component of this a reduced scheme?*

6 Some answers: questions B and C

Question B. *Suppose R is a local artin ring and G_0 a finite group scheme over R. Does there exist an integral domain Γ, a finite group scheme over Γ, and a homomorphism $\Gamma \to R$ such that $G \otimes_\Gamma R \cong R$?*

There are many counter examples possible.

Here is an easy example. Take $a = \varepsilon = b$ with $\varepsilon^2 = 0$. The finite group scheme $G = G_{a,b}$ in characteristic p does not admit a lift to an integral domain $\Gamma \supset \mathbb{F}_p$ (do you see a proof?). However this group scheme G does admit a lift to a mixed characteristic domain where p is ramified.

We will see "better" examples.

Questions A and B have a negative answer.

Question A. *Let $G \to \mathrm{Spec}(R)$ be a finite local group scheme over a local artin ring. Does G contain a subgroup scheme $\{e\} \subsetneqq N \subsetneqq G$ flat over S?*

Question B. *Suppose R is a local artin ring and G_0 a finite group scheme over R. Does there exist an integral domain Γ, a finite group scheme over Γ, and a homomorphism $\Gamma \to R$ such that $G \otimes_\Gamma R \cong R$?*

Construction. Choose any p and $m = p^2$. Take the moduli space given by $M = \mathrm{Spec}(\mathcal{R}^{(p^2)})$. Choose $0 \in M$ such that $\mathcal{N}_0^{(p^2)} \cong (\alpha_p)^2$. Let $\mathcal{O}$ be the local ring $\mathcal{O} = \mathcal{O}_{M,0}$. Define $R = \mathcal{O}/((\mathfrak{m}_\mathcal{O})^3)$ and $G = \mathcal{N}^{(p^2)} \otimes_{\mathcal{R}^{(p^2)}} R$.

Comment / explanation. We see that G/R is "the universal deformation" of $G_0 = (\alpha_p)^2$ over artin rings with $\mathfrak{m}^3 = 0$.

Claim. *The situation G/R constructed here gives a negative answer to Question A* (existence of a flat subgroup scheme) *and a negative answer to Question B* (lifting to a domain). We fix the G/R as constructed above.

(1) Observe that G/R is not commutative, as we have seen in **(lift)** above.
(2) Observe that α_p can be deformed over $R' = k[\varepsilon]/(\varepsilon^2)$ to $G_{\varepsilon,0}$ and to $G_{0,\varepsilon}$. Hence G/R admits $\rho : R \to R'$ with $G \otimes R' \cong G_{\varepsilon,0} \times G_{0,\varepsilon}$.

Question A. *Let* $G \to \mathrm{Spec}(R)$ *be a finite local group scheme over a local artin ring. Does* G *contain a subgroup scheme* $\{e\} \subsetneqq N \subsetneqq G$ *flat over* S?

(A) Note that $\mathrm{End}((\alpha_{p,\mathbb{F}_p})^2) = \mathrm{GL}(2, \mathbb{F}_p)$. By "transport of structure" this ring operates faithfully on G/R. Suppose there would exist $\{e\} \subsetneqq N \subsetneqq G$ flat over R. Using the the action of $\mathrm{End}((\alpha_{p,\mathbb{F}_p})^2)$ on $N \subset G$ shows that any

$$N_{0,\psi} = \alpha_{p,\mathbb{F}_p} \stackrel{\psi}{\hookrightarrow} (\alpha_{p,\mathbb{F}_p})^2$$

can be lifted to a flat $N_\psi \subset G$ over R. This would imply that any $\psi = \{(1,1)\}$ would give a flat $N_\psi \otimes R' \subset G_{\varepsilon,0} \times G_{0,\varepsilon}$, giving an isomorphism between $G_{\varepsilon,0}$ and $G_{0,\varepsilon}$. This contradiction shows $N \subset G$ as indicated does not exist: a negative answer to Question A, a proof of the claim part A.

Question B. *Suppose R is a local artin ring and G_0 a finite group scheme over R. Does there exist an integral domain Γ, a finite group scheme over Γ, and a homomorphism $\Gamma \to R$ such that $G \otimes_\Gamma R \cong R$?*

(B) Note that $0 \neq p{\cdot}1 \in R$ and G/R is not-commutative of rank p^2. Suppose G/R could be lifted to a domain $\Gamma \twoheadrightarrow R$. Then the characteristic of Γ is not positive, hence equal to zero. We would obtain a finite group scheme of rank p^2 over the fraction field of Γ, hence an etale group scheme, over the algebraic closure a constant group scheme of rank p^2. That is commutative by group theory, a contradiction. This shows the lift as assumed to an integral domain does not exist: a negative answer to Question B a proof of the claim part B.

I thank the organizers for giving me the opportunity to talk to you.

Thank you for your attention.

Wish you many happy mathematics years.