Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

GROUP SCHEMES WITH $\mathbb{F}_q$-ACTION

Thomas Poguntke

Tome 145
Fascicule 2

2017

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du Centre national de la recherche scientifique
pages 345-380

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 2, tome 145, juin 2017

Diffusion

Maison de la SMF - Case 916 - Luminy - 13288 Marseille Cedex 9 - France
`christian.smf@cirm-math.fr`

Hindustan Book Agency
O-131, The Shopping Mall
Arjun Marg, DLF Phase 1
Gurgaon 122002, Haryana
Inde

AMS
P.O. Box 6248
Providence RI 02940
USA
`www.ams.org`

Tarifs

Vente au numéro : 43 € ($ 64)
Abonnement électronique : 135 € ($ 202),
avec supplément papier : Europe 179 €, hors Europe 197 € ($ 296)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Nathalie Christiaën

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
`bullsmf@ihp.fr` • `smf.emath.fr`

ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Stéphane SEURET

Bull. Soc. Math. France
145 (2), 2017, p. 345-380

GROUP SCHEMES WITH $\mathbb{F}_q$-ACTION

BY THOMAS POGUNTKE

ABSTRACT. — Via a construction due to V. Drinfel′d, we prove an equivalence of categories, generalizing the equivalence between commutative flat group schemes in characteristic p with trivial Verschiebung and their Dieudonné modules to group schemes with $\mathbb{F}_q$-action.

RÉSUMÉ (*Schémas en groupes avec $\mathbb{F}_q$-action*). — Au moyen d'une construction par V. Drinfel′d, nous prouvons une équivalence de catégories, généralisant l'équivalence entre les schémas en groupes plats commutatifs en caractéristique p annulé par le décalage et leurs $\mathbb{F}_p$-modules de Dieudonné aux schémas en groupes avec action de $\mathbb{F}_q$.

Texte reccu le 20 mars 2015, modifié le 26 septembre 2016, accepté le 3 octobre 2016.

THOMAS POGUNTKE, Hausdorff Center for Mathematics, Villa Maria, Endenicher Allee 62, 53115 Bonn, Germany • *E-mail :* `thomas.poguntke@hcm.uni-bonn.de` • *Url :* `http://www.math.uni-bonn.de/people/poguntke`

Mathematical subject classification (2010). — 14L15, 14L17.

Key words and phrases. — Group schemes, shtukas, Verschiebung.

I would like to thank M. Rapoport for suggesting this topic, for his constant interest and his suggestions. I thank U. Hartl for granting us access to an early draft of the paper [10] with Singh. I am indebted to Lisa Sauermann for her contribution to the penultimate section. I would also like to thank M. Raynaud for interesting correspondences on group schemes with trivial Verschiebung. G. Faltings pointed out some mistakes in a preliminary version of the manuscript; for this I am grateful. Finally, I would like to thank the anonymous referee for very helpful suggestions and comments.

0037-9484/2017/345/$ 5.00
doi:10.24033/bsmf.2740

1. Introduction

Let p be a prime and let k be a field of characteristic p. Denote by Gr_k^+ the category of affine commutative group schemes over k which can be embedded into $\mathbb{G}_a^N$ for some set N. We assign to $G \in \mathrm{Gr}_k^+$ its Dieudonné $\mathbb{F}_p$-module $\mathcal{M}(G) = \mathrm{Hom}_{\mathrm{Gr}_k^+}(G, \mathbb{G}_a)$, with the obvious left module structure over $\mathrm{End}_{\mathrm{Gr}_k^+}(\mathbb{G}_a) \cong k[F]$, the non-commutative polynomial ring with

$$F\lambda = \lambda^p F \text{ for } \lambda \in k.$$

These Dieudonné modules completely classify group schemes of the above type, as shown by the following theorem.

THEOREM 1.1 ([2], IV, §3, 6.7). — *The contravariant functor $\mathcal{M}$ defines an exact anti-equivalence of categories*

$$\mathcal{M} : \mathrm{Gr}_k^+ \longrightarrow k[F]\text{-Mod}\,. \tag{1.1}$$

Under this duality, group schemes of finite presentation correspond to finitely generated $k[F]$-modules, and finite group schemes to finite-dimensional k-vector spaces.

The above result allows us to describe the structure of our category over a perfect field, and its simple objects if k is algebraically closed.

THEOREM 1.2 ([2], IV, §3, 6.9). — *Let k be a perfect field. Then $G \in \mathrm{Gr}_k^+$ is algebraic if and only if it can be written as a product*

$$G \cong \mathbb{G}_a^n \times \pi_0(G) \times H,$$

where $n \in \mathbb{N}$, H is a finite product of group schemes of the form α_{p^s}, and $\pi_0(G)$ is an étale sheaf of finite $\mathbb{F}_p$-vector spaces. If k is algebraically closed, then

$$\pi_0(G) \cong (\underline{\mathbb{F}_p})^m, m \in \mathbb{N}.$$

On the other hand, let S be a scheme of characteristic p. Consider the category $\mathrm{gr}_S^{+\vee}$ of flat group schemes locally of finite presentation over S of height ≤ 1 (i.e., killed by their Frobenius). Let $p\text{-}\mathrm{Lie}_S$ denote the category of finite locally free $\mathcal{O}_S$-p-Lie algebras. Then we have the following classification theorem.

THEOREM 1.3 ([7], Remark 7.5). — *The covariant functor*

$$\mathcal{L} : \mathrm{gr}_S^{+\vee} \longrightarrow p\text{-}\mathrm{Lie}_S, G \longmapsto \mathrm{Lie}(G),$$

defines an equivalence of categories.

Two of our main results generalize Theorem 1.1, and reduce (for "$q = p$") to Theorem 1.3 via Cartier duality, respectively. Moreover, we formulate two conjectures under which they unify.

Assume that S is an $\mathbb{F}_q$-scheme for some prime power $q = p^r$. Our group schemes G are affine, commutative, flat over S and carry an $\mathbb{F}_q$-action. We require that locally on S, there is an embedding $G \hookrightarrow \mathbb{G}_a^N$ for some set N, which respects the $\mathbb{F}_q$-actions.

The category of these group schemes will be denoted by $\mathbb{F}_q\text{-}\operatorname{Gr}_S^+$, and its full subcategory of finite group schemes of finite presentation is called $\mathbb{F}_q\text{-}\operatorname{gr}_S^+$.

On the other hand, we consider left $\mathcal{O}_S[F^r]$-modules, which are flat as $\mathcal{O}_S$-modules. They are called $\mathbb{F}_q$-shtukas over S, and their category is denoted by $\mathbb{F}_q\text{-}\operatorname{Sht}_S$. We write $\mathbb{F}_q\text{-}\operatorname{sht}_S$ for the full subcategory of $\mathbb{F}_q\text{-}\operatorname{Sht}_S$ of locally free modules of finite rank over $\mathcal{O}_S$.

We study the following generalization of the contravariant functor (1.1),

$$\mathcal{M}_q = \mathcal{M} : \mathbb{F}_q\text{-}\operatorname{gr}_S^+ \longrightarrow \mathbb{F}_q\text{-}\operatorname{sht}_S, G \longmapsto \operatorname{Hom}_{\mathbb{F}_q\text{-}\operatorname{Gr}_S^+}(G, \mathbb{G}_a).$$

We also explain the construction of a functor in the other direction,

$$\mathcal{G}_q = \mathcal{G} : \mathbb{F}_q\text{-}\operatorname{sht}_S \longrightarrow \mathbb{F}_q\text{-}\operatorname{gr}_S^+,$$

which is fully faithful and left-adjoint to $\mathcal{M}$. However, $\mathcal{G}_q$ does not define an equivalence of categories for $q \neq p$. Rather, we describe a full subcategory $\mathbb{F}_q\text{-}\operatorname{gr}_S^{+,\mathrm{b}}$ of *balanced* group schemes in $\mathbb{F}_q\text{-}\operatorname{gr}_S^+$, and prove that it is the essential image of $\mathcal{G}$.

Namely, let $G = \operatorname{Spec}(B_G) \in \mathbb{F}_q\text{-}\operatorname{gr}_S^+$. We show that the space of primitive elements in B_G decomposes into eigenspaces for the $\mathbb{F}_q^\times$-action as

$$\operatorname{Prim}(B_G) = \bigoplus_{s=0}^{r-1} \operatorname{Prim}_{p^s}(B_G). \tag{1.2}$$

We call G balanced, if the p-Frobenii $\operatorname{Prim}_{p^t}(B_G) \to \operatorname{Prim}_{p^{t+1}}(B_G), x \mapsto x^p$, are bijective for all $0 \leq t < r-1$. Note that when $q = p$, we recover $\mathbb{F}_p\text{-}\operatorname{gr}_S^{+,\mathrm{b}} = \operatorname{gr}_S^+$.

THEOREM 1.4. — *The functor $\mathcal{G} : \mathbb{F}_q\text{-}\operatorname{sht}_S \to \mathbb{F}_q\text{-}\operatorname{gr}_S^{+,\mathrm{b}}$ defines an exact anti-equivalence of categories with quasi-inverse $\mathcal{M}$.*

Our definition of the balanced subcategory of $\mathbb{F}_q\text{-}\operatorname{gr}_S^+$ is inspired by Raynaud's paper [15]. He considers finite commutative group schemes G with an action of $\mathbb{F}_q$, and the decomposition of the augmentation ideal into eigenspaces for the $\mathbb{F}_q^\times$-action,

$$I_G = \bigoplus_{j=1}^{q-1} I_j,$$

similarly to (1.2). Note that all summands I_j are finite locally free $\mathcal{O}_S$-modules. Raynaud imposes the condition that $\operatorname{rk}(I_j) = 1$, for all j.

We define a group scheme $G \in \mathbb{F}_q\text{-}\operatorname{gr}_S^+$ to be *quasi-balanced* if $\operatorname{rk}(I_j)$ is the same for all j. This turns out to be almost the same as being balanced; in

particular, Raynaud's condition implies the balance property. The following theorem is our second main result.

THEOREM 1.5. — *Let $G \in \mathbb{F}_q\text{-}\mathrm{gr}_S^+$. If G is balanced, then it is quasi-balanced. For $q \neq 4$, the converse holds.*

Finally, we consider the question whether $\mathcal{M} : \mathbb{F}_q\text{-}\mathrm{Gr}_S^{+,\mathrm{b}} \to \mathbb{F}_q\text{-}\mathrm{Sht}_S$ defines an equivalence of categories in general. In order to make sense of this, we have to assume the following.

CONJECTURE 1.6. — *For any $G \in \mathbb{F}_q\text{-}\mathrm{Gr}_S^+$, the $\mathcal{O}_S$-module $\mathcal{M}(G)$ is flat.*

Recall from above that it holds for finite G. Moreover assume the following key statement.

CONJECTURE 1.7. — *For $G \in \mathbb{F}_q\text{-}\mathrm{Gr}_S^+$ locally of finite presentation, there is an embedding $G \hookrightarrow \mathbb{G}_a^N$, for some $N \in \mathbb{N}$, locally on S, such that the induced morphism $\mathcal{M}(\mathbb{G}_a^N) \to \mathcal{M}(G)$ is surjective.*

This follows from Theorem 1.1 if $S = \mathrm{Spec}(k)$ is a point. Moreover, it is true in the finite case. We obtain the conditional result that $\mathcal{M}$ is an equivalence if we restrict ourselves to finitely presented group schemes and finitely generated $\mathcal{O}_S[F^r]$-modules, respectively.

In particular, we obtain the following generalization of Theorem 1.2.

THEOREM 1.8. — *Let k be a perfect field. Then a group scheme $G \in \mathbb{F}_q\text{-}\mathrm{Gr}_k^{+,\mathrm{b}}$ is algebraic if and only if it is isomorphic to a product*

$$G \cong \mathbb{G}_a^n \times \pi_0(G) \times H,$$

with $n \in \mathbb{N}$ and H a product of group schemes of the form α_{q^s}, and where $\pi_0(G)$ is an étale sheaf of finite $\mathbb{F}_q$-vector spaces. If k is algebraically closed, then $\pi_0(G) \cong (\underline{\mathbb{F}_q})^m$, for some $m \in \mathbb{N}$.

Theorem 1.4 has an interesting history. In his article [3], §2, Drinfel′d defines the functor $\mathcal{G} : \mathbb{F}_q\text{-}\mathrm{sht}_S \to \mathbb{F}_q\text{-}\mathrm{gr}_S^+$ and shows that it is fully faithful and exact. Furthermore, he proves that the étale group schemes in $\mathbb{F}_q\text{-}\mathrm{gr}_S^+$ lie in the essential image of $\mathcal{G}$.

In Laumon's book [11], App. B, he claims that $\mathbb{F}_q\text{-}\mathrm{sht}_k$ is anti-equivalent to $\mathbb{F}_q\text{-}\mathrm{gr}_k^+$, where k is a perfect field of characteristic p. However, $\mathbb{F}_q\text{-}\mathrm{gr}_k^+$ is not an abelian category for $q \neq p$, and α_p is of $\mathbb{F}_q$-additive type but not balanced. This error was pointed out to us by Hartl. Laumon's argument is sufficiently detailed to locate the mistake in his reasoning.

In [17], Proposition 1.7, Taguchi gives a (rather brief) proof of Theorem 1.4. He describes $\mathbb{F}_q\text{-}\mathrm{gr}_S^{+,\mathrm{b}}$ by a condition on the order of the group schemes however, which precludes a generalization to the category $\mathbb{F}_q\text{-}\mathrm{Gr}_S^+$ as above.

On the other hand, Abrashkin [1] considers a category $\mathrm{DGr}^*(\mathbb{F}_q)_S$, based on a definition of Faltings [4]. Roughly, the $\mathbb{F}_q$-action on $G \in \mathbb{F}_q\text{-}\,\mathrm{gr}_S^+$ is called *strict*, if G has a deformation $G^\flat$ (which is then universal with respect to its $\mathbb{F}_q$-action) such that $\mathbb{F}_q$ acts via scalar multiplication on the associated representative of the cotangent complex.

In *loc.cit.*, §2.3, Abrashkin gives the construction of an equivalence of categories $D_q : \mathbb{F}_q\text{-}\,\mathrm{sht}_S \xrightarrow{\sim} \mathrm{DGr}^*(\mathbb{F}_q)_S$. Moreover, he shows in *loc.cit.*, §2.3.2., that a group scheme carrying a strict $\mathbb{F}_q$-action is balanced. Hence, the obvious functor $\mathrm{DGr}^*(\mathbb{F}_q)_S \to \mathbb{F}_q\text{-}\,\mathrm{gr}_S^{+,\mathrm{b}}$ is well-defined, and it is clear from the constructions that the following diagram commutes.

$$\begin{array}{ccc} \mathbb{F}_q\text{-}\,\mathrm{sht}_S & \xrightarrow{D_q} & \mathrm{DGr}^*(\mathbb{F}_q)_S \\ & \searrow^{\mathcal{G}_q} & \downarrow \\ & & \mathbb{F}_q\text{-}\,\mathrm{gr}_S^{+,\mathrm{b}}\,. \end{array}$$

The above equivalence of categories appears in Hartl-Singh [10], Theorem 5.2, at the torsion level of the function field analog of the crystalline Dieudonné theory of p-divisible groups they establish over a general base. This was one of the main motivations for our study. For further applications in this direction, see for example Hartl-Kim [9], as well as the paper [8] by Genestier and V. Lafforgue, where Theorem 1.4 appears as Proposition 0.3.

Let us briefly outline the structure of the paper. In §2, we provide some basic theory of group schemes we need. Section §3 specializes to group schemes of additive type, and culminates in the proof of Theorem 1.4 in the crucial case $q = p$. Some details are postponed to avoid repetition and streamline the argument.

In §4 and §5, we define the categories $\mathbb{F}_q\text{-}\,\mathrm{sht}_A$ and $\mathbb{F}_q\text{-}\,\mathrm{gr}_A^+$, respectively, and study their internal structure. Section §6 is concerned with the construction of the functors $\mathcal{M}$ and $\mathcal{G}$, a more detailed analysis of their properties, and the proof of Theorem 1.4.

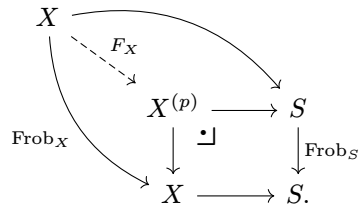
In §7, we introduce quasi-balanced group schemes, and compare the two balance conditions. Finally, §8 concerns the question what we can still say in the case of infinite group schemes.

2. Preliminaries on group schemes

Let p be a prime number, and S a scheme of characteristic p.

Definition 2.1. — For an S-scheme X, denote by $\mathrm{Frob}_X : X \to X$ its Frobenius endomorphism. Let $X^{(p)} = X \times_{S,\mathrm{Frob}_S} S$. The relative Frobenius

$F_X : X \to X^{(p)}$ of X is defined by the following diagram with cartesian square.



In particular, F_X is a morphism of S-schemes.

Definition 2.2. — We denote by Gr_S the category of affine commutative flat group schemes over S, and its full subcategory of finite group schemes locally of finite presentation by gr_S.

Convention: All of our considerations take place locally on S. To emphasize when we assume $S = \operatorname{Spec} A$, we will write $\mathrm{Gr}_A = \mathrm{Gr}_S$.

We also fix $G = \operatorname{Spec} B_G$ as a notation for the affine algebra of G.

Definition 2.3. — We write Hopf_A, resp. hopf_A, for the opposite category of Gr_A, resp. gr_A.

Definition 2.4. — Let $G = \operatorname{Spec} B_G \in \mathrm{Gr}_A$. Consider the symmetrization morphism

$$s : B_G^{\otimes p} \longrightarrow \mathrm{TS}^p(B_G), x_1 \otimes \cdots \otimes x_p \longmapsto \sum_{\pi \in S_p} x_{\pi(1)} \otimes \cdots \otimes x_{\pi(p)}, \tag{2.1}$$

where $\mathrm{TS}^p(B_G) := (B_G^{\otimes p})^{S_p}$. Since G is flat, $x \mapsto x^{\otimes p}$ induces an isomorphism

$$\sigma_p^* B_G := B_G \otimes_{A,\sigma_p} A \xrightarrow{\sim} \mathrm{TS}^p(B_G)/s(B_G^{\otimes p}),$$

see [2], IV, §3, 4.1. Here, σ_p denotes the Frobenius of A, and so we have $G^{(p)} = \operatorname{Spec}(\sigma_p^* B_G)$, which is a closed subscheme of $\mathrm{S}^p G := \operatorname{Spec}(\mathrm{TS}^p(B_G))$ by the above. The Verschiebung of G is then defined as the composition

$$V_G : G^{(p)} \hookrightarrow \mathrm{S}^p G \xrightarrow{\mathrm{mult}} G,$$

where mult is the p-fold multiplication on G, which factors over $\mathrm{S}^p G$, since G is commutative.

Remark 2.5. — We have that $F_G \circ V_G = p \cdot \mathrm{id}_G$, and $V_G \circ F_G = p \cdot \mathrm{id}_{G^{(p)}}$, by [2], IV, §3, 4.6. On affine algebras, V_G^* acts by taking p-th "copowers". In this sense, it is dual to the (relative) Frobenius, which we make precise below. The name (German for "shift") comes from the Verschiebung on Witt (co-)vectors, where it acts as an index shift (cf. [6], III, §3.1).

DEFINITION 2.6. — For $G \in \mathrm{Gr}_A$, let $\eta : B_G \to A$ be the augmentation—or counit—of B_G, given by the unit section of G. The augmentation ideal of G is defined by $I_G = \ker(\eta)$.

REMARK 2.7. — The short exact sequence

$$0 \longrightarrow I_G \longrightarrow B_G \xrightarrow{\eta} A \longrightarrow 0$$

is split on the right by the unit $\varepsilon : A \to B_G$ of B_G, so that in fact $B_G = A \oplus I_G$. In particular, the A-module I_G is flat.

DEFINITION 2.8. — Let $G \in \mathrm{Gr}_A$. The space of primitive elements in B_G is defined by

$$\mathrm{Prim}(B_G) := \{x \in I_G \mid \Delta(x) = x \otimes 1 + 1 \otimes x\},$$

where Δ is the comultiplication on B_G, i.e., the map induced by the multiplication of G. The subgroup of group-like elements of B_G is defined by

$$\mathrm{Grp}(B_G) := \{x \in B_G \mid \Delta(x) = x \otimes x, \eta(x) = 1\},$$

where $\eta : B_G \to A$ is the counit of B_G.

EXAMPLE 2.9. — The group structure on $\mathbb{G}_a = \mathrm{Spec}\, A[x]$ is defined by the condition $x \in \mathrm{Prim}(B_{\mathbb{G}_a})$. This also yields for $G \in \mathrm{Gr}_A$ that

$$\mathrm{Prim}(B_G) \cong \mathrm{Hom}(G, \mathbb{G}_a),$$

by the universal property of the polynomial algebra.

REMARK 2.10. — Let $G \in \mathrm{Gr}_A$ and $x \in I_G$. Then

$$\Delta(x) \equiv x \otimes 1 + 1 \otimes x \bmod I_G \otimes I_G,$$

cf. [18], §2.3. This explains the name "primitive element".

EXAMPLE 2.11. — Let $x \in B_G$. If $x \in \mathrm{Prim}(B_G)$, we have

$$V_G^*(x) = x \otimes 1 \otimes \cdots \otimes 1 + \cdots + 1 \otimes \cdots \otimes 1 \otimes x = \frac{1}{(p-1)!} s(x \otimes 1 \otimes \cdots \otimes 1) \equiv 0,$$

where s is the morphism (2.1). On the other hand, if $x \in \mathrm{Grp}(B_G)$, then

$$V_G^*(x) = x^{\otimes p} \cong x \otimes_{\sigma_p} 1$$

acts identically.

PROPOSITION 2.12. — *Let $B, C \in \mathrm{Hopf}_A$ be Hopf algebras over A. Then*

$$\mathrm{Prim}(B \otimes C) = \mathrm{Prim}(B) \otimes 1 + 1 \otimes \mathrm{Prim}(C)$$

is compatible with tensor products.

Proof. — Let $G = \operatorname{Spec} B$ and $H = \operatorname{Spec} C$ be the corresponding group schemes. Then $\operatorname{Hom}(G, \mathbb{G}_a) \times \operatorname{Hom}(H, \mathbb{G}_a) \cong \operatorname{Hom}(G \times H, \mathbb{G}_a)$. We have to show that the corresponding isomorphism

$$\operatorname{Prim}(B) \times \operatorname{Prim}(C) \xrightarrow{\sim} \operatorname{Prim}(B \otimes C)$$

is given by $(y, z) \mapsto y \otimes 1 + 1 \otimes z \in \operatorname{Prim}(B \otimes C)$. By definition, the image of an element (y, z) of the left-hand side in $\operatorname{Hom}(G \times H, \mathbb{G}_a)$ is induced by the unique Hopf algebra morphism $f : A[x] \to B \otimes C$ such that

$$\begin{array}{ccccccc} & & x & \in & A[x] & \ni & x \\ & \swarrow & & \swarrow & \exists! \downarrow f & \searrow & & \searrow \\ y \in B & \xleftarrow[\pi_B]{} & & B \otimes C & & \xrightarrow[\pi_C]{} & & C \ni z \end{array}$$

commutes. Here, the projection $\pi_B : B \otimes C \to B$ (and similarly π_C) is given by the injection $G \to G \times H, g \mapsto (g, 0)$. Explicitly, $\pi_B(b \otimes c) = b\varepsilon(\eta(c))$, where $\eta : C \to A$ is the counit and $\varepsilon : A \to C$ the unit of C. But now indeed,

$$\pi_B(f(x)) = \pi_B(y \otimes 1 + 1 \otimes z) = y\varepsilon(\eta(1)) + \varepsilon(\eta(z)) = y,$$

because $z \in I_H = \ker(\eta)$. We have $\pi_C(f(x)) = z$ by the same argument. □

Definition 2.13. — Let $G \in \mathrm{Gr}_S$. The Cartier dual $G^\vee = \underline{\mathrm{Hom}}(G, \mathbb{G}_m)$ of the group scheme G is defined by

$$G^\vee : R \longmapsto \operatorname{Hom}_{\mathrm{Gr}_R}(G \otimes R, \mathbb{G}_m \otimes R)$$

as a functor of points.

Example 2.14 (cf. [14], §5, p.11). — The group scheme $\alpha_p = \operatorname{Spec} A[x]/(x^p)$, with x primitive, is self-dual,

$$\alpha_p^\vee = \alpha_p.$$

On the other hand, consider the constant group scheme

$$\underline{\mathbb{F}_p} \cong \operatorname{Spec} A[x]/(x^p - x),$$

where $x \in \operatorname{Prim}(B_{\underline{\mathbb{F}_p}})$. Its dual is given by the roots of unity

$$\mu_p = \operatorname{Spec} A[T]/(T^p - 1),$$

where T is group-like.

Lemma 2.15 (cf. [2], II, §1, 2.10; [16], §3.2.2). — *Let $G = \operatorname{Spec} B_G \in \mathrm{gr}_A$. Then $G^\vee = \operatorname{Spec} B_G^\vee$, where the dual Hopf algebra $B_G^\vee = \operatorname{Hom}_A(B_G, A)$ carries as (co-)multiplication the transpose of the (co-)multiplication on B_G. That is,*

$$\nabla_{G^\vee} : B_G^\vee \otimes B_G^\vee \cong \operatorname{Hom}(B_G \otimes B_G, A) \xrightarrow{\Delta_G^*} \operatorname{Hom}(B_G, A),$$

$$\Delta_{G^\vee} : B_G^\vee \xrightarrow{\nabla_G^*} \operatorname{Hom}(B_G \otimes B_G, A) \cong B_G^\vee \otimes B_G^\vee,$$

and similarly for the unit and counit,

$$\varepsilon_{G^\vee} : A \cong \mathrm{Hom}_A(A,A) \xrightarrow{\eta_G^*} B_G^\vee,$$

$$\eta_{G^\vee} : B_G^\vee \xrightarrow{\varepsilon_G^*} \mathrm{Hom}_A(A,A) \cong A.$$

REMARK 2.16. — In the case of Lemma 2.15, it is easy to see that Frobenius and Verschiebung are dual to one another, seeing as Cartier duality exchanges multiplication and comultiplication. The same is indeed true for any $G \in \mathrm{Gr}_A$ by [2], IV, §3, 4.9. Namely,

$$F_{G^\vee} = (V_G)^\vee, \tag{2.2}$$

and assuming $G^\vee$ is represented by a flat group scheme over A, also

$$V_{G^\vee} = (F_G)^\vee.$$

The following result is crucial for our main theorem in the finite case.

PROPOSITION 2.17. — *For $G = \mathrm{Spec}\, B_G \in \mathrm{gr}_A$, there are natural isomorphisms of A-modules*

$$\mathrm{Lie}\, G^\vee \cong \mathrm{Hom}_A(I/I^2, A) \cong \mathrm{Der}_A(B^\vee, A) \cong \mathrm{Prim}\, B_G,$$

where $B^\vee = B_G^\vee$ and $I = \ker(\eta^\vee : B^\vee \to A)$ is the augmentation ideal of $G^\vee$.

Proof (cf. [6]*, I, §8.3 ff.)* Let $A(\varepsilon) = A[t]/(t^2)$ be the algebra of dual numbers and denote by $\pi : A(\varepsilon) \twoheadrightarrow A$ the projection. For $u \in G^\vee(A(\varepsilon))$, we have by definition

$$u \in \mathrm{Lie}\, G^\vee = \ker G^\vee(\pi) \iff (B^\vee \xrightarrow{u} A(\varepsilon) \xrightarrow{\pi} A) = \eta^\vee \iff u(I) \subseteq \varepsilon A(\varepsilon).$$

In that case, we get $u(I^2) \subseteq \varepsilon^2 A(\varepsilon) = 0$, hence an element in the tangent space of $G^\vee$, given by

$$\overline{u} : I/I^2 \longrightarrow A, \alpha \longmapsto \frac{u(\alpha)}{\varepsilon}.$$

The second isomorphism is just the universal property (cf. [18], §2.11)

$$\mathrm{Der}_A(B^\vee, A) \cong \mathrm{Hom}_{B^\vee}(\Omega^1_{B^\vee|A}, A) \cong \mathrm{Hom}_{B^\vee}(I/I^2 \otimes_A B^\vee, A) \cong \mathrm{Hom}_A(I/I^2, A)$$

where the $B^\vee$-module structure on A is induced by $\eta^\vee$. Finally, consider the natural pairing

$$\langle \text{-}, \text{-} \rangle : B^\vee \times B_G \longrightarrow A, (\alpha, x) \longmapsto \alpha(x).$$

For $x \in B_G$, recalling Lemma 2.15, we have $x \in \mathrm{Prim}(B_G)$ if and only if

$$\langle \alpha\beta, x \rangle = (\alpha \otimes \beta)(\Delta(x)) = (\alpha \otimes \beta)(x \otimes 1 + 1 \otimes x) = \langle \alpha, x \rangle \eta^\vee(\beta) + \eta^\vee(\alpha)\langle \beta, x \rangle,$$

that is to say $\langle \text{-}, x \rangle \in \mathrm{Der}_A(B^\vee, A)$. □

REMARK 2.18. — Proposition 2.17 will also allow us to dualize our theory, in the sense that

$$\operatorname{Lie}\underline{\operatorname{Hom}}(G,\mathbb{G}_m)=\operatorname{Hom}(G,\mathbb{G}_a),$$

for $G\in \operatorname{gr}_A$. Therefore, Cartier duality reduces Theorem 3.13 to Theorem 1.3.

3. Group schemes of additive type

DEFINITION 3.1. — A group scheme $G\in \operatorname{Gr}_S$ is of additive type if there exists a closed embedding of G into $\mathbb{G}_a^N$ for some set N, locally on S. We define Gr_A^+, resp. gr_A^+, to be the full subcategory of Gr_A, resp. gr_A, of group schemes of additive type.

THEOREM 3.2. — *Let $G\in \operatorname{Gr}_S$ be locally finitely presented. Then the following conditions are equivalent.*

(i) $G\in \operatorname{Gr}_S^+$.

(ii) $I_G=(\operatorname{Prim} B_G)$, *i.e.,* $\operatorname{Prim} B_G$ *generates* I_G *as an ideal, locally on* S.

Moreover, the above conditions imply the following.

(iii) $V_G=0$.

For finite $G\in \operatorname{gr}_S$, all three conditions are equivalent.

Proof (Raynaud). — The equivalence of (i) and (ii) is clear. Indeed, an embedding $G\hookrightarrow \mathbb{G}_a^N$ is the same as a Hopf algebra epimorphism $A[x_1,\dots,x_N]\twoheadrightarrow B_G$, and the x_n are primitive by definition. The implication "(ii) $\Rightarrow$ (iii)" is settled by Example 2.11.

Now it remains to show that if $G\in \operatorname{gr}_A$ and A is a local ring, then $V_G=0$ implies that there exists a closed embedding $G\hookrightarrow \mathbb{G}_a^N$ for some $N\in\mathbb{N}$.

Consider the Cartier dual $G^\vee$ of G, with affine algebra $B^\vee=B_{G^\vee}$ (cf. Lemma 2.15) and augmentation ideal $I=I_{G^\vee}$. Since B_G is finite and locally free, it is reflexive. Thus on R-valued points, we have

$$G(R)\cong \operatorname{Hom}_{\operatorname{Gr}_R}(G^\vee\otimes R,\mathbb{G}_m\otimes R)\cong \operatorname{Grp}(B^\vee\otimes R)\subseteq (B^\vee\otimes R)^\times. \tag{3.1}$$

The functor $\operatorname{Res}_{B^\vee/A}(\mathbb{G}_m\otimes B^\vee)$ on the right-hand side is represented by a group scheme, because $B^\vee$ is finite flat, and (3.1) defines a closed embedding $G\hookrightarrow \operatorname{Res}_{B^\vee/A}(\mathbb{G}_m\otimes B^\vee)$. Now, the counit of $B^\vee$ induces a natural splitting

$$\eta\colon \operatorname{Res}_{B^\vee/A}(\mathbb{G}_m\otimes B^\vee)\longrightarrow\!\!\!\!\!\rightarrow \mathbb{G}_m$$

of the natural inclusion $\mathbb{G}_m\hookrightarrow \operatorname{Res}_{B^\vee/A}(\mathbb{G}_m\otimes B^\vee)$. This yields a split short exact sequence

$$\begin{aligned} 1\longrightarrow \mathbb{G}_m\longrightarrow \operatorname{Res}_{B^\vee/A}(\mathbb{G}_m\otimes B^\vee)&\longrightarrow 1+\mathcal{I}\longrightarrow 1,\\ \alpha&\longmapsto \tfrac{\alpha}{\eta_R(\alpha)}\quad \text{(on } R\text{-points)}, \end{aligned}$$

where $(1+\mathcal{I})(R) := 1 + \ker(\eta_R)$. Consider the kernel H of the composition

$$G \hookrightarrow \mathrm{Res}_{B^\vee/A}(\mathbb{G}_m \otimes B^\vee) \cong \mathbb{G}_m \times (1+\mathcal{I}) \twoheadrightarrow 1+\mathcal{I}.$$

Then H embeds into $\mathbb{G}_m$, so its fibres are of multiplicative type. But they are also killed by the Verschiebung, hence vanish ([2], IV, §3, 4.11). By Nakayama, we obtain $H = 0$.

Finally, since $F_{G^\vee} = (V_G)^\vee = 0$ by (2.2), we have $\mathcal{I}^p = 0$. Thus $1+\mathcal{I}$ is isomorphic via truncated exp and log to the additive group $\mathcal{I} \cong \mathbb{G}_a^{\mathrm{ord}(G)-1}$. □

REMARK 3.3. — Over a field $A = k$, all three conditions in Theorem 3.2 are equivalent, as shown in [2], IV, §3, 6.6. We conjecture that this holds over an arbitrary base scheme S.

REMARK 3.4. — If condition (ii) in Theorem 3.2 holds, the Hopf algebra B_G is also called primitively generated, i.e., it is generated as an algebra by its primitive elements.

EXAMPLE 3.5. — The constant group scheme $\underline{\mathbb{F}_p}$ over the $\mathbb{F}_p$-algebra A embeds into $\mathbb{G}_a$ via the projection

$$A[x] \twoheadrightarrow A[x]/(x^p - x).$$

The same holds for the group schemes $\alpha_{p^s} = \mathrm{Spec}\, A[x]/(x^{p^s})$, for $s \in \mathbb{N}$, since x is primitive by definition. That is, they are all of additive type.

We now compute the order of a finite group scheme G of additive type. This is the essential step towards our main theorem.

PROPOSITION 3.6. — *Let $G \in \mathrm{gr}_A^+$, and consider its dual $B^\vee = B_G^\vee$. Locally on* Spec A*, there exists an algebra isomorphism*

$$B^\vee \cong A[t_1, \ldots, t_n]/(t_1^p, \ldots, t_n^p).$$

Moreover, the A-module Prim(B_G) *is locally free, and the order of G is*

$$\mathrm{ord}(G) = p^{\mathrm{rk}(\mathrm{Prim}\, B_G)}.$$

Proof (cf. [7]*, §7.4.3 and* [11]*, Lemma B.3.14).* — Let A be a local ring with residue field k. Let I be the augmentation ideal of $B^\vee$, which is then free of finite rank d. Write $I_k := I \otimes k$, and choose a basis $e_1, \ldots, e_d$ such that $e_{n+1}, \ldots, e_d$ is a basis of I_k^2. Let $t_i \in I$ be a lift of e_i for $1 \le i \le d$, so that $t_1, \ldots, t_d$ is an A-basis of I by Nakayama.

Now consider the free A-submodule $M := \mathrm{span}_A(t_1, \ldots, t_n) \subseteq I$, and define

$$B' := \mathrm{Sym}(M)/(t^{\otimes p} \mid t \in M) \cong A[t_1, \ldots, t_n]/(t_1^p, \ldots, t_n^p).$$

Since $F_{G^\vee} = (V_G)^\vee = 0$, we have $I^p = 0$, and the canonical morphism

$$\psi : B' \longrightarrow B^\vee, t_i \longmapsto t_i,$$

is well-defined. Surjectivity of ψ is easy to check along the filtration

$$0 = I^p \subseteq I^{p-1} \subseteq \cdots \subseteq I \subseteq B^\vee.$$

We claim that in fact $\dim_k(B' \otimes k) = \dim_k(B^\vee \otimes k)$, so that $\psi \otimes k$ is an isomorphism. To show this, we can assume k to be perfect. Using $I_k^p = 0$, we then know by [2], III, §3, 6.3, that there is an algebra isomorphism

$$B^\vee \otimes k \cong k[T_1, \ldots, T_N]/(T_1^p, \ldots, T_N^p).$$

But then in particular $N = \dim(I_k/I_k^2) = n$. Since both $B^\vee$ and B' are finite flat A-modules of finite presentation, ψ is an isomorphism.

For the second part, it suffices by Proposition 2.17 to show that I/I^2 is free. But ψ^{-1} induces an isomorphism of A-modules

$$I/I^2 \xrightarrow{\sim} J/J^2 \cong M,$$

where J denotes the augmentation ideal of B'. Finally, Proposition 2.17 then tells us that $\mathrm{rk}(\mathrm{Prim}\, B_G) = \mathrm{rk}(I/I^2) = n$, and therefore indeed

$$\mathrm{ord}\, G = \mathrm{rk}(B^\vee) = p^n = p^{\mathrm{rk}(\mathrm{Prim}\, B_G)},$$

as desired. □

REMARK 3.7. — It is easy to see that for any A-algebra R, and any $G \in \mathrm{Gr}_A$, we have a canonical map

$$\mathrm{Prim}(B_G) \otimes_A R \longrightarrow \mathrm{Prim}(B_G \otimes_A R). \tag{3.2}$$

Now let $G \in \mathrm{gr}_A^+$, and assume that R is the residue field at some point of $\mathrm{Spec}\, A$. To show that (3.2) is an isomorphism, we may assume A to be local. But then (3.2) is clearly injective, and both sides of (3.2) are finite R-modules of the same rank by Proposition 3.6.

DEFINITION 3.8. — Let $A[F]$ be the non-commutative polynomial ring over A with $F\lambda = \lambda^p F$ for any $\lambda \in A$. Note that $A[F] \cong \mathrm{span}_A(x^{p^e} \mid e \in \mathbb{N}) \subseteq A[x]$ as $A[F]$-modules via $Fx = x^p$. The category of $A[F]$-modules, which are finite and locally free over A, is denoted by sht_A.

PROPOSITION 3.9. — *Let N be a set. The primitive elements in the affine algebra of $\mathbb{G}_a^N$ are given by*

$$\mathrm{Prim}(A[x_n \mid n \in N]) = \mathrm{span}_A(x_n^{p^e} \mid n \in N, e \in \mathbb{N}),$$

the space of additive polynomials in $A[x_n \mid n \in N]$. In other words,

$$\mathrm{Hom}(\mathbb{G}_a^N, \mathbb{G}_a) \cong A[F]^{\oplus N}$$

as $A[F]$-modules. In particular, $\mathrm{End}(\mathbb{G}_a) = A[F]$.

Proof. — Of course, "$\supseteq$" holds by definition. Now it suffices to see that

$$\mathrm{Prim}(A[x]) \subseteq \mathrm{span}_A(x^{p^e} \mid e \in \mathbb{N}),$$

since we may assume N to be finite, and then use induction over $\#N$, applying Proposition 2.12. Let thus $z = \sum_{n\in\mathbb{N}} \lambda_n x^n \in \mathrm{Prim}(A[x])$. Then

$$\Delta(z) = \sum_{n\in\mathbb{N}} \lambda_n (x^n \otimes 1) + \sum_{n\in\mathbb{N}} \lambda_n (1 \otimes x^n).$$

On the other hand, since Δ is an algebra morphism and x is primitive,

$$\Delta(z) = \sum_{n\in\mathbb{N}} \lambda_n (x \otimes 1 + 1 \otimes x)^n = \sum_{n\in\mathbb{N}} \lambda_n \sum_{k\leq n} \binom{n}{k} (x^k \otimes x^{n-k}).$$

Comparing coefficients, we see that if $\lambda_n \neq 0$, then $\binom{n}{k} \equiv 0 \bmod p$ for all $0 < k < n$. But this implies $n = p^e$ for some $e \in \mathbb{N}$, cf. [5], Theorem 3. □

Definition 3.10. — We denote the Dieudonné $\mathbb{F}_p$-module functor on gr_A^+ by

$$\mathcal{M} : \mathrm{gr}_A^+ \longrightarrow \mathrm{sht}_A, G \longmapsto \mathrm{Hom}(G, \mathbb{G}_a).$$

Here, the $A[F]$-module structure on $\mathcal{M}(G)$ is given as in Definition 3.8 by

$$Fx = x^p \in \mathrm{Prim}(B_G).$$

Equivalently, this is the obvious left module structure on $\mathrm{Hom}(G, \mathbb{G}_a)$ over $\mathrm{End}(\mathbb{G}_a) = A[F]$, cf. Proposition 3.9. Conversely, let us define for $M \in \mathrm{sht}_A$ the corresponding group scheme

$$\mathcal{G}(M) = \mathrm{Spec}(\mathrm{Sym}(M)/\mathfrak{f}),$$

where $\mathfrak{f}$ is the ideal $\mathfrak{f} = (x^{\otimes p} - Fx \mid x \in M)$ in the symmetric algebra over A. The group structure on $\mathcal{G}(M)$ is defined by $\mathrm{Prim}(B_{\mathcal{G}(M)}) \supseteq M$, by extension to the whole algebra.

Remark 3.11. — The easy verification that the functors $\mathcal{M}$ and $\mathcal{G}$ are well-defined is a special case of Remark 6.2 and Remark 6.4, respectively.

Example 3.12. — Proposition 3.9 implies for the standard subgroup schemes of $\mathbb{G}_a$ that

$$\mathcal{M}(\alpha_{p^s}) \cong A[F]/(F^s), \text{ and } \mathcal{M}(\underline{\mathbb{F}_p}) \cong A[F]/(F-1).$$

Theorem 3.13. — *The functor $\mathcal{M}$ defines an exact anti-equivalence of categories.*

Proof. — Locally on $\mathrm{Spec}\, A$, choose a basis $x_1, \ldots, x_N$ of $M \in \mathrm{sht}_A$. This yields the basis

$$\left\{ \prod_{i=1}^N x_i^{e_i} \mid 0 \leq e_i < p \right\}$$

of $B_{\mathcal{G}(M)} = \mathrm{Sym}(M)/\mathfrak{f}$, locally over $\mathrm{Spec}\, A$. Therefore, we obtain

$$\mathrm{ord}\, \mathcal{G}(M) = p^{\mathrm{rk}\, M}. \tag{3.3}$$

Now, it is not hard to see that the functor $\mathcal{G} : \mathrm{sht}_A \to \mathrm{gr}_A^+$ is left-adjoint to $\mathcal{M}$. We will give the details in Lemma 8.4. For $G \in \mathrm{gr}_A^+$ and $M \in \mathrm{sht}_A$, consider the adjunction morphisms

$$u_G : G \longrightarrow \mathcal{G}(\mathcal{M}(G)), \text{ and } v_M : M \longrightarrow \mathcal{M}(\mathcal{G}(M)).$$

By construction, v_M is the inclusion $M \hookrightarrow \mathrm{Prim}(B_{\mathcal{G}(M)})$. From (3.3) and Proposition 3.6, as well as base change (Remark 3.7), we see that v_M is an isomorphism. Now consider the map

$$u_G^* : \mathrm{Sym}(\mathrm{Prim}(B_G))/(x^{\otimes p} - x^p \mid x \in \mathrm{Prim}(B_G)) \longrightarrow B_G,$$

which is the identity on $\mathrm{Prim}(B_G)$. Since B_G is primitively generated, we see that u_G^* is surjective. By Proposition 3.6 and (3.3), we have

$$\mathrm{ord}\, \mathcal{G}(\mathcal{M}(G)) = p^{\mathrm{rk}(\mathrm{Prim}\, B_G)} = \mathrm{ord}\, G.$$

Thus u_G^* is an epimorphism between finite locally free modules of the same rank, and hence bijective. Finally, we see that $\mathcal{M}$ is exact by (Lemma 8.4 and) additivity of the rank. □

4. The category of $\mathbb{F}_q$-shtukas

Let $q = p^r$ be a power of the prime p, and assume that S an $\mathbb{F}_q$-scheme.

Definition 4.1. — A finite $\mathbb{F}_q$-shtuka over S is a pair (M, f), where M is a finite locally free $\mathcal{O}_S$-module, and f is a q-linear endomorphism of M. Equivalently, f is a linearized map

$$f^{(q)} : \sigma_q^* M = M \otimes_{\mathcal{O}_S, \sigma_q} \mathcal{O}_S \longrightarrow M,$$

where $\sigma_q = \sigma_p^r$ is the Frobenius of $\mathcal{O}_S$. A morphism $\Phi : (M, f) \to (M', f')$ in the category $\mathbb{F}_q\text{-}\mathrm{sht}_S$ of finite $\mathbb{F}_q$-shtukas over S is an $\mathcal{O}_S$-module morphism such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{\Phi} & M' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ M & \xrightarrow{\Phi} & M' \end{array}$$

commutes. We shall write $\mathbb{F}_q\text{-}\mathrm{sht}_A = \mathbb{F}_q\text{-}\mathrm{sht}_S$, when $S = \mathrm{Spec}\, A$.

Remark 4.2. — Note that $(M, f) \in \mathbb{F}_p\text{-}\mathrm{sht}_A$ is the same as the left $A[F]$-module M, defined by $Fx = f(x)$ for $x \in M$. Thus we recover $\mathrm{sht}_A = \mathbb{F}_p\text{-}\mathrm{sht}_A$.

The definition comes from the following geometric example.

EXAMPLE 4.3. — Let X be a smooth projective geometrically irreducible curve over $\mathbb{F}_q$. A (right) shtuka (or F-sheaf) of rank $d \in \mathbb{N}$ over S is a diagram

$$\begin{array}{ccccc} \mathcal{L} & & \xrightarrow{\ i\ } & & \\ & \searrow & & \mathcal{E} & \\ & & \xrightarrow{\ \tau\ } & & \\ (\mathrm{id}_X \times F_S)^*\mathcal{L} & & & & \end{array} \tag{4.1}$$

with $\mathcal{L}$ and $\mathcal{E}$ locally free sheaves of $\mathcal{O}_{X\times S}$-modules of rank d, injective homomorphisms τ and i, and such that $\mathrm{coker}(\tau)$, resp. $\mathrm{coker}(i)$, is supported on the graph Γ_α, resp. Γ_β, of some sections $\alpha, \beta : S \to X$ (called the zero, resp. the pole, of the shtuka).

Let $D \subseteq X$ be a finite subscheme away from the pole, i.e., $\beta(S) \subseteq X \smallsetminus D$. Then $i|_{D\times S}$ is an isomorphism. Setting $\mathcal{L}_D := \mathcal{L}|_{D\times S}$, we therefore obtain a morphism completing the restriction to $D \times S$ of diagram (4.1),

$$f' = (i|_{D\times S})^{-1} \circ \tau|_{D\times S} : (\mathrm{id}_D \times F_S)^*\mathcal{L}_D \longrightarrow \mathcal{L}_D.$$

Denote by $\pi : D \times S \to S$ the projection, then $(\pi_*\mathcal{L}_D, f)$ is a finite $\mathbb{F}_q$-shtuka over $\mathcal{O}_S$, where

$$f^{(q)} : F_S^*\pi_*\mathcal{L}_D \cong \pi_*(\mathrm{id}_D \times F_S)^*\mathcal{L}_D \xrightarrow{\pi_* f'} \pi_*\mathcal{L}_D.$$

Drinfel′d [3] introduced F-sheaves in the proof of the Langlands conjecture for GL_2 over a global field of characteristic p.

Let us remark here a simple dichotomy in the category $\mathbb{F}_q\text{-}\mathrm{sht}_k$, where k is a perfect field. We will later use it to generalize Theorem 1.2.

LEMMA 4.4. — *Let k be a perfect field. For $(M, f) \in \mathbb{F}_q\text{-}\mathrm{sht}_k$, there is a unique decomposition*

$$(M, f) = (M_{\mathrm{ss}}, f_{\mathrm{ss}}) \oplus (M_{\mathrm{nil}}, f_{\mathrm{nil}})$$

such that $f_{\mathrm{ss}} = f|_{M_{\mathrm{ss}}}$ is bijective and $f_{\mathrm{nil}} = f|_{M_{\mathrm{nil}}}$ is nilpotent.

Proof ([11]*, Lemma B.3.10).* — Since k is perfect, let us identify $f^{(q)} = f$. Let

$$M_{\mathrm{ss}} = \bigcap_{n\in\mathbb{N}} \mathrm{im}(f^n), \text{ and } M_{\mathrm{nil}} = \bigcup_{n\in\mathbb{N}} \ker(f^n).$$

Then there is some $N \in \mathbb{N}$ with $M_{\mathrm{ss}} = \mathrm{im}(f^N)$ and $M_{\mathrm{nil}} = \ker(f^N)$, so that in particular

$$\dim(M) = \dim(M_{\mathrm{ss}}) + \dim(M_{\mathrm{nil}}).$$

Now suppose that $m \in M_{\mathrm{ss}} \cap M_{\mathrm{nil}}$. Then $m = f^N(m')$ for some $m' \in M$, and we obtain $f^{2N}(m') = f^N(m) = 0$. But since we have $\ker(f^{2N}) = \ker(f^N)$, in fact $m = f^N(m') = 0$. □

5. $\mathbb{F}_q$-actions on group schemes

DEFINITION 5.1. — Let S be an $\mathbb{F}_q$-scheme, and let $G \in \mathrm{Gr}_S$. An $\mathbb{F}_q$-action on G is a ring morphism

$$[-]_G : \mathbb{F}_q \longrightarrow \mathrm{End}_{\mathrm{Gr}_S}(G), \alpha \longmapsto [\alpha]_G.$$

A morphism of group schemes with $\mathbb{F}_q$-action $\varphi : (G, [-]_G) \to (H, [-]_H)$ is a morphism of group schemes over S such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ {\scriptstyle [\alpha]_G}\downarrow & & \downarrow{\scriptstyle [\alpha]_H} \\ G & \xrightarrow{\varphi} & H \end{array} \tag{5.1}$$

commutes for all $\alpha \in \mathbb{F}_q$. When there is no ambiguity, we will just write $[\alpha]$ for the action.

We denote by $\mathbb{F}_q\text{-}\mathrm{Gr}_S$ the category of group schemes in Gr_S, together with an $\mathbb{F}_q$-action. For its objects, we will write G instead of $(G, [-]_G)$. The full subcategory of $\mathbb{F}_q\text{-}\mathrm{Gr}_S$ of finite group schemes is $\mathbb{F}_q\text{-}\mathrm{gr}_S$.

We replace S by A in the notation, when $S = \mathrm{Spec}\, A$. As before, we consider the dual categories $\mathbb{F}_q\text{-}\mathrm{Hopf}_A$, resp. $\mathbb{F}_q\text{-}\mathrm{hopf}_A$.

EXAMPLE 5.2. — When we consider $\mathbb{G}_a = \mathrm{Spec}\, A[x]$ as an object of $\mathbb{F}_q\text{-}\mathrm{Gr}_A$, we mean that

$$[\alpha]^* x = \alpha x \text{ for all } \alpha \in \mathbb{F}_q,$$

unless explicitly stated otherwise. The same extends to the subgroup schemes $\alpha_{p^s} \subseteq \mathbb{G}_a$ and the constant group $\underline{\mathbb{F}_q} \subseteq \mathbb{G}_a$, as well as any product of these groups.

REMARK 5.3. — Let $G, H \in \mathbb{F}_q\text{-}\mathrm{Gr}_A$. Then the product $G \times H$ is endowed with the $\mathbb{F}_q$-action

$$[\alpha]_{G\times H} = [\alpha]_G \times [\alpha]_H.$$

Let $\varphi, \psi : G \to H$ be morphisms in $\mathbb{F}_q\text{-}\mathrm{Gr}_A$. Then the diagram

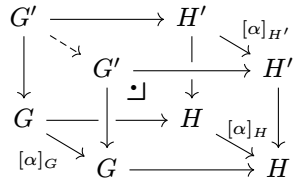
$$\begin{array}{ccccccc} G & \xrightarrow{\mathrm{diag}} & G\times G & \xrightarrow{\varphi\times\psi} & H\times H & \xrightarrow{\mathrm{mult}} & H \\ {\scriptstyle [\alpha]_G}\downarrow & & {\scriptstyle [\alpha]_{G\times G}}\downarrow & & \downarrow{\scriptstyle [\alpha]_{H\times H}} & & \downarrow{\scriptstyle [\alpha]_H} \\ G & \xrightarrow{\mathrm{diag}} & G\times G & \xrightarrow{\varphi\times\psi} & H\times H & \xrightarrow{\mathrm{mult}} & H \end{array}$$

commutes for all $\alpha \in \mathbb{F}_q$, so that $\varphi + \psi \in \mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(G, H)$ again.

Moreover, $\mathbb{F}_q\text{-}\mathrm{Gr}_A$ is an $\mathbb{F}_q$-linear category. Namely, $\mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(G, H)$ is given a vector space structure by the obvious actions (which agree by definition) of $\alpha \in \mathbb{F}_q$ via

$$[\alpha]_G \in \mathrm{End}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(G), \text{ resp. } [\alpha]_H \in \mathrm{End}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(H).$$

Now consider an arbitrary fibre product diagram in $\mathbb{F}_q\text{-}\operatorname{Gr}_A$ as in (5.2). Then

(5.2)


defines a canonical $\mathbb{F}_q$-action on G', since all squares in (5.2) commute, for all $\alpha \in \mathbb{F}_q$. The dual construction yields an $\mathbb{F}_q$-action for pushouts.

Explicitly, if A is a field, we see directly from (5.1) that the $\mathbb{F}_q$-action of B_G descends to $\ker(\varphi) = \operatorname{Spec}(B_G/\varphi^*(I_H)B_G)$ (cf. [13], VII, Proposition 4.1).

Similarly, the $\mathbb{F}_q$-action on H restricts to $\operatorname{coker}(\varphi) = \operatorname{Spec} C$, where

$$C = \{x \in B_H \mid \Delta(x) - 1 \otimes x \in \ker(\varphi^*) \otimes B_H\},$$

see [6], I, §6.3. Indeed, by (5.1) again, for all $x \in C$, we have

$$\Delta([\alpha]^* x) - 1 \otimes [\alpha]^* x = ([\alpha]^* \otimes [\alpha]^*)(\Delta(x) - 1 \otimes x) \in \ker(\varphi^*) \otimes B_H.$$

Definition 5.4. — Let $G = \operatorname{Spec} B_G \in \mathbb{F}_q\text{-}\operatorname{Gr}_A$. The eigenspaces of the $\mathbb{F}_q^\times$-action on the augmentation ideal $I = I_G$ are given by

$$I_j := I_j(G) := \{x \in I_G \mid [\alpha]^* x = \alpha^j x \text{ for all } \alpha \in \mathbb{F}_q\},$$

for $0 < j < q$, identifying $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)$. We also set

$$\operatorname{Prim}_j(B_G) := \operatorname{Prim}(B_G) \cap I_j.$$

Remark 5.5. — Since $\operatorname{ord}(\mathbb{F}_q^\times)$ is prime to p, the ideal I_G decomposes into its eigenspaces as

$$I_G = \bigoplus_{j=1}^{q-1} I_j. \tag{5.3}$$

Indeed, we can write $\mathbb{F}_q[\mathbb{F}_q^\times] = \mathbb{F}_q[X]/(X^{q-1} - 1) = \bigoplus_{j=1}^{q-1} \mathbb{F}_q \chi_j$, with $\chi_j(\alpha) = \alpha^j$ for $\alpha \in \mathbb{F}_q^\times$. This yields a system of orthogonal idempotents of $\operatorname{End}_A(I_G)$,

$$e_j = \frac{1}{q-1} \sum_{\alpha \in \mathbb{F}_q^\times} \chi_j^{-1}(\alpha)[\alpha]^*, 0 < j < q,$$

cf. [19], Lemma 2. Hence we obtain (5.3), since $I_j = e_j I_G$. In particular, it follows that the I_j are flat over A, as direct summands of the flat A-module I. The analogous statements hold for the $\operatorname{Prim}_j(B_G)$, if $\operatorname{Prim}(B_G)$ is flat, noting that $\operatorname{Prim}(B_G)$ is stable under $[\alpha]^* \in \operatorname{End}_{\operatorname{Hopf}_A}(B_G)$, $\alpha \in \mathbb{F}_q$.

DEFINITION 5.6. — Let $G \in \mathbb{F}_q\text{-}\mathrm{Gr}_S$. We say that G is of $\mathbb{F}_q$-additive type, if locally on S, there exists an $\mathbb{F}_q$-equivariant closed embedding

$$G \hookrightarrow \mathbb{G}_a^N \text{ for some set } N.$$

The full subcategory of $\mathbb{F}_q\text{-}\mathrm{Gr}_A$, resp. $\mathbb{F}_q\text{-}\mathrm{gr}_A$, of group schemes G of $\mathbb{F}_q$-additive type is denoted by $\mathbb{F}_q\text{-}\mathrm{Gr}_A^+$, resp. $\mathbb{F}_q\text{-}\mathrm{gr}_A^+$. For $q = p$, we drop $\mathbb{F}_q$ from the notation, as before.

REMARK 5.7. — Let $G \in \mathbb{F}_q\text{-}\mathrm{Gr}_S$ be locally of finite presentation. Then

$$G \text{ is of } \mathbb{F}_q\text{-additive type} \iff I_G = (\mathrm{Prim}_1(B_G)), \text{ locally on } S,$$

in analogy to Theorem 3.2.

REMARK 5.8. — Let $G, H \in \mathbb{F}_q\text{-}\mathrm{Gr}_A^+$. If we have embeddings $G \hookrightarrow \mathbb{G}_a^N$ as well as $H \hookrightarrow \mathbb{G}_a^L$ in $\mathbb{F}_q\text{-}\mathrm{Gr}_A$, then also

$$G \times H \hookrightarrow \mathbb{G}_a^{N \cup L}.$$

Therefore, $G \times H \in \mathbb{F}_q\text{-}\mathrm{Gr}_A^+$. Conversely, the embeddings $G, H \hookrightarrow G \times H$ respect the $\mathbb{F}_q$-actions. Hence if $G \times H$ is of $\mathbb{F}_q$-additive type, then so are G and H. This does not generalize to arbitrary extensions, as the following example illustrates. That is, $\mathbb{F}_q\text{-}\mathrm{Gr}_A^+$ is not a Serre subcategory of $\mathbb{F}_q\text{-}\mathrm{Gr}_A$ (indeed, nor is $\mathbb{F}_q\text{-}\mathrm{gr}_A^+ \subseteq \mathbb{F}_q\text{-}\mathrm{gr}_A$).

EXAMPLE 5.9. — Let $q \neq p$, and consider the following short exact sequence

$$0 \longrightarrow \alpha_p \longrightarrow \alpha_q \longrightarrow H \longrightarrow 0$$

in $\mathbb{F}_q\text{-}\mathrm{gr}_A$. Note that $\alpha_p, \alpha_q \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$. Applying $\mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(-, \mathbb{G}_a)$, we get

$$0 \longrightarrow \mathrm{Prim}_1(B_H) \longrightarrow \mathrm{Prim}_1(B_{\alpha_q}) \xrightarrow{\sim} \mathrm{Prim}_1(B_{\alpha_p}),$$

so $I_H \neq (\mathrm{Prim}_1(B_H)) = 0$, and H is not of $\mathbb{F}_q$-additive type, by Remark 5.7.

THEOREM 5.10. — *Let $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A$. Then G is of $\mathbb{F}_q$-additive type if and only if it is of additive type and the p-Frobenii*

$$f_t : \mathrm{Prim}_{p^t}(B_G) \longrightarrow \mathrm{Prim}_{p^{t+1}}(B_G), x \longmapsto x^p,$$

are surjective, $0 \leq t < r - 1$. Moreover, if $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$, the primitive elements decompose as

$$\mathrm{Prim}(B_G) = \bigoplus_{s=0}^{r-1} \mathrm{Prim}_{p^s}(B_G)$$

into eigenspaces. Equivalently, $\mathrm{Prim}_j(B_G) = 0$ for all $j \neq p^s$, $s \in \mathbb{N}$.

Proof. — Assume A to be local. Let $\iota : G \hookrightarrow \mathbb{G}_a^N$ in $\mathbb{F}_q\text{-}\mathrm{Gr}_A$ be an embedding. Proposition 3.9 implies that the additive polynomials decompose as desired,

$$\mathcal{P} := \mathrm{Prim}(A[x_1, \ldots, x_N]) = \bigoplus_{s=0}^{r-1} \mathcal{P}_s,$$

with $\mathcal{P}_s = \mathrm{Prim}_{p^s}(A[x_1, \dots, x_N])$. Let k be the residue field of A. We have the epimorphism

$$\iota^*|_{\mathcal{P}} \otimes_A k : \mathcal{P} \otimes_A k = \mathrm{Prim}(k[x_1, \dots, x_N]) \twoheadrightarrow \mathrm{Prim}(B_G \otimes_A k)$$

by Theorem 1.1. Thus $\mathcal{P} \otimes_A k \twoheadrightarrow \mathrm{Prim}(B_G) \otimes_A k$ is surjective, as well, by Remark 3.7. Now consider the filtration

$$\mathrm{Prim}(B_G) =: M \supseteq M^p \supseteq M^{p^2} \supseteq \cdots,$$

where $M^{p^t} := \mathrm{im}((\sigma_p^t)^* M \to M, x \mapsto x^{p^t})$. Then we may conclude that

$$\iota^* : \mathcal{P}^{p^t}/\mathcal{P}^{p^{t+1}} \twoheadrightarrow M^{p^t}/M^{p^{t+1}}$$

is surjective, for all $t \geq 0$, by Nakayama's lemma. Therefore,

$$\iota^*(\mathrm{Prim}\, A[x_1, \dots, x_N]) = \mathrm{Prim}(B_G). \tag{5.4}$$

But ι^* respects the $\mathbb{F}_q$-action, so in fact $\iota^*(\mathcal{P}_s) = \mathrm{Prim}_{p^s}(B_G)$ for all $0 \leq s < r$. This settles the second part, and moreover implies that the epimorphism ι^* induces surjections

$$0 = \mathcal{P}_{t+1}/(\mathcal{P}_t)^p \twoheadrightarrow \mathrm{Prim}_{p^{t+1}}(B_G)/f_t(\mathrm{Prim}_{p^t}(B_G)).$$

Conversely, if all the f_t are surjective, we have

$$I_G = (\mathrm{Prim}(B_G)) = (\mathrm{Prim}_1(B_G)),$$

and G is of $\mathbb{F}_q$-additive type by Remark 5.7. □

REMARK 5.11. — In the previous proof, we need not invoke Theorem 1.1. With the above notation, we may assume k algebraically closed. Then

$$\mathrm{Ext}^1_{\mathrm{Gr}_k}(\mathrm{coker}\, \iota \otimes k, \mathbb{G}_{a,k}) = 0,$$

cf. [11], Lemma B.3.15. This implies as before the surjectivity of

$$\iota^*|_{\mathcal{P}} : \mathrm{Hom}(\mathbb{G}_a^N, \mathbb{G}_a) \longrightarrow \mathrm{Hom}(G, \mathbb{G}_a).$$

LEMMA 5.12. — *Let $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$, and f_t the p-Frobenii from Theorem 5.10. The following conditions are equivalent.*

(i) *The maps f_t are bijective, for all $0 \leq t < r-1$.*
(ii) *The map $f' : \mathrm{Prim}_1(B_G) \to \mathrm{Prim}_{p^{r-1}}(B_G), x \mapsto x^{p^{r-1}}$, is injective.*
(iii) *The rank of $\mathrm{Prim}_{p^s}(B_G)$ is the same for all $0 \leq s \leq r-1$.*
(iv) $\mathrm{ord}(G) = q^{\mathrm{rk}\,\mathrm{Prim}_1(B_G)}$.

Proof. — The first two conditions are equivalent by Theorem 5.10. Furthermore, by Nakayama, they are equivalent to (iii). Now, Proposition 3.6 tells us that $\mathrm{rk}\,\mathrm{Prim}_{p^s}(B_G) = \mathrm{rk}\,\mathrm{Prim}_1(B_G)$ for all $0 \leq s \leq r-1$ if and only if

$$\mathrm{ord}(G) = p^{\mathrm{rk}(\mathrm{Prim}\, B_G)} = q^{\mathrm{rk}(\mathrm{Prim}_1\, B_G)}.$$

Hence (iii) is equivalent to (iv). □

DEFINITION 5.13. — If the conditions in Lemma 5.12 hold for $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$, we say that G is balanced. The full subcategory of $\mathbb{F}_q\text{-}\mathrm{gr}_A^+$ of balanced group schemes will be called $\mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}}$.

REMARK 5.14. — In [17], Taguchi defines $\mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}}$ using condition (iv) from Lemma 5.12. The first two conditions will be useful to generalize the definition to infinite group schemes.

REMARK 5.15. — We have $\mathbb{F}_p\text{-}\mathrm{gr}_A^{+,\mathrm{b}} = \mathrm{gr}_A^+$, since the condition on the p-Frobenii is empty.

EXAMPLE 5.16. — Consider $G = \alpha_{p^s} = \operatorname{Spec} A[x]/(x^{p^s})$ with the usual $\mathbb{F}_q$-action $[\alpha]^* x = \alpha x$ for $\alpha \in \mathbb{F}_q$. Then

$$\alpha_{p^s} \text{ is balanced} \iff r \mid s.$$

Indeed, $\mathrm{Prim}(B_{\alpha_{p^s}}) = \mathrm{span}_A(x, x^p, \dots, x^{p^{s-1}})$ by Proposition 3.9, and hence

$$\mathrm{Prim}_1(B_{\alpha_{p^s}}) = \mathrm{span}_A(x^{q^a} \mid 0 \le a < s/r),$$

since $p^s \equiv 1 \bmod q-1 \iff \frac{p^s-1}{q-1} \in \mathbb{Z} \iff r \mid s$.

REMARK 5.17. — Let $G \in \mathbb{F}_q\text{-}\mathrm{gr}_S^+$. If S is connected, then

$$G \text{ is balanced} \iff G_s \text{ is balanced for some point } s \in S,$$

because $\mathrm{Prim}(B_G)$ is locally free and stable under base change (Remark 3.7). Therefore, the balanced locus of $G \in \mathbb{F}_q\text{-}\mathrm{gr}_S^+$ in S is a union of connected components. If S is noetherian, it is thus closed and open.

REMARK 5.18. — If $G \in \mathbb{F}_q\text{-}\mathrm{gr}_S^+$ is étale, its Frobenius is an isomorphism. Therefore, G is balanced by Lemma 5.12, (i).

LEMMA 5.19. — *Let $G, H \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$. If two of G, H and $G \times H$ are balanced, then so is the third.*

Proof. — Proposition 2.12 implies that

$$\mathrm{Prim}_{p^s}(B_G \otimes B_H) = \mathrm{Prim}_{p^s}(B_G) \otimes 1 + 1 \otimes \mathrm{Prim}_{p^s}(B_H)$$

for all $0 \le s \le r-1$. Then it is clear that if two of G, H and $G \times H$ satisfy condition (i) from Lemma 5.12, the third does as well. □

REMARK 5.20. — A posteriori, Lemma 5.19 in fact holds true for general extensions $0 \to G \to E \to H \to 0$. Namely, by Theorem 6.5, we obtain a short exact sequence

$$0 \longrightarrow \mathrm{Prim}_1(B_H) \longrightarrow \mathrm{Prim}_1(B_E) \longrightarrow \mathrm{Prim}_1(B_G) \longrightarrow 0.$$

Then the equivalence follows using Lemma 5.12, (iv).

6. The functors $\mathcal{G}$ and $\mathcal{M}$

We continue to denote by A an $\mathbb{F}_q$-algebra, for $q = p^r$.

DEFINITION 6.1. — The Dieudonné $\mathbb{F}_q$-functor is the contravariant functor

$$\mathcal{M}_q = \mathcal{M} : \mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}} \longrightarrow \mathbb{F}_q\text{-}\mathrm{sht}_A, G \longmapsto (\mathrm{Prim}_1(B_G), x \mapsto x^q).$$

Recall that $\mathrm{Prim}_1(B_G) \cong \mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{gr}_A}(G, \mathbb{G}_a)$, and that it is locally free over A, cf. Remark 5.5.

REMARK 6.2. — The functor $\mathcal{M}$ is well-defined, since on the one hand, we have $\Delta(x^q) = (x \otimes 1 + 1 \otimes x)^q = x^q \otimes 1 + 1 \otimes x^q$, and on the other,

$$[\alpha]^* x^q = \alpha^q x^q = \alpha x^q \text{ for } x \in \mathcal{M}(G), \alpha \in \mathbb{F}_q.$$

DEFINITION 6.3. — The Drinfel′d $\mathbb{F}_q$-functor is defined to be the contravariant functor

$$\mathcal{G}_q = \mathcal{G} : \mathbb{F}_q\text{-}\mathrm{sht}_A \longrightarrow \mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}}, (M, f) \longmapsto \mathrm{Spec}(\mathrm{Sym}(M)/\mathfrak{f}),$$

where $\mathfrak{f}$ is the ideal $\mathfrak{f} = (x^{\otimes q} - f(x) \mid x \in M)$. Comultiplication and $\mathbb{F}_q$-action are given by

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \text{ and } [\alpha]^* x = \alpha x \text{ for } x \in M, \alpha \in \mathbb{F}_q,$$

extended to the whole algebra.

REMARK 6.4. — Let $(M, f) \in \mathbb{F}_q\text{-}\mathrm{sht}_A$. The $\mathbb{F}_q$-action on $\mathcal{G}(M, f)$ is well-defined, since

$$[\alpha]^* x^{\otimes q} = \alpha^q x^{\otimes q} = \alpha f(x) = [\alpha]^* f(x) \text{ for } \alpha \in \mathbb{F}_q, x \in M.$$

Furthermore, locally on $\mathrm{Spec}\, A$, we can take a basis $x_1, \ldots, x_N$ of M and the projection

$$\mathrm{Sym}(M) \twoheadrightarrow \mathrm{Sym}(M)/\mathfrak{f}$$

will define an $\mathbb{F}_q$-equivariant embedding $\mathcal{G}(M, f) \hookrightarrow \mathbb{G}_a^N$. Moreover, note that the products $\{\prod_{i=1}^N x_i^{e_i} \mid 0 \leq e_i < q\}$ form a basis of $B_{\mathcal{G}(M,f)} = \mathrm{Sym}(M)/\mathfrak{f}$. Therefore

$$\mathrm{ord}(\mathcal{G}(M, f)) = q^{\mathrm{rk}\, M}, \tag{6.1}$$

and indeed $\mathcal{G}(M, f) \in \mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}}$ by Lemma 5.12, (iv).

We are now prepared to state the main result of this section.

THEOREM 6.5. — *The Drinfel'd $\mathbb{F}_q$-functor $\mathcal{G} : \mathbb{F}_q\text{-}\mathrm{sht}_A \to \mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}}$ defines an exact anti-equivalence of categories with quasi-inverse $\mathcal{M}$.*

Proof. — The proof is the same as for Theorem 3.13, where we use (6.1) in place of (3.3). This yields that the adjunction morphisms $v_{(M,f)}$ are bijective. On the other hand,

$$u_G^* : \mathrm{Sym}(\mathrm{Prim}_1(B_G))/(x^{\otimes q} - x^q \mid x \in \mathrm{Prim}_1(B_G)) \longrightarrow B_G$$

is surjective, since B_G is generated as an algebra by $\mathrm{Prim}_1(B_G)$, as noted in Remark 5.7. Finally,

$$\mathrm{ord}\,\mathcal{G}(\mathcal{M}(G)) = q^{\mathrm{rk}(\mathrm{Prim}_1 B_G)} = p^{\mathrm{rk}(\mathrm{Prim}\, B_G)} = \mathrm{ord}\, G,$$

by Proposition 3.6, and because G is balanced. □

Let us note some properties of the functor $\mathcal{G}$ (cf. [3], Proposition 2.1).

PROPOSITION 6.6. — *Let $(M, f) \in \mathbb{F}_q\text{-}\mathrm{sht}_A$, and denote by $I = I_{\mathcal{G}(M,f)}$ the augmentation ideal of $\mathcal{G}(M, f)$. The cotangent space of $\mathcal{G}(M, f)$ is described by*

$$I/I^2 \cong \mathrm{coker}(f^{(q)})$$

as an A-module, where $f^{(q)} : \sigma_q^* M \to M$, as before. Moreover,

(a) *The group scheme $\mathcal{G}(M, f)$ is étale $\iff$ f is bijective.*

(b) *$\mathcal{G}(M, f)$ has connected fibres $\iff$ f is nilpotent, locally on* $\mathrm{Spec}\, A$.

Proof. — For the first part, we note that the composition $\tau : M \hookrightarrow I \twoheadrightarrow I/I^2$ is surjective, since every element of I/I^2 is represented by a linear polynomial in M. But

$$\ker(\tau) = M \cap I^2 = f(M).$$

Indeed, an element of M lies in I^2 if and only if it is of the form

$$f(x) \equiv x^{\otimes q} \in I^2 \text{ for some } x \in M.$$

The statements (a),(b) follow from the fact that f is a power of the Frobenius on $\mathrm{Sym}(M)/\mathfrak{f}$. Hence f is bijective if and only if $\mathrm{Frob}_{\mathcal{G}(M,f)}$ is an isomorphism, which is equivalent to $\mathcal{G}(M, f)$ being étale ([2], IV, §3, 5.3), because $\mathcal{G}(M, f)$ is finite flat and finitely presented.

Analogously, f is locally nilpotent if and only if $\mathrm{Frob}_{\mathcal{G}(M,f)}$ is. But each fibre of $\mathcal{G}(M, f)$ is connected if and only if its Frobenius is nilpotent (*loc.cit.*). □

REMARK 6.7. — If A is a field, Theorem 6.5 in particular says that $\mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}}$ is an abelian category. On the other hand, it follows from Example 5.9 that for $q \neq p$, the category $\mathbb{F}_q\text{-}\mathrm{gr}_A^{+}$ is not abelian. The problem is of course that α_p is not balanced, by Example 5.16.

EXAMPLE 6.8. — Let $q \neq p$. Take $B_G = A[x_1, \dots, x_r]/(x_1^p, \dots, x_r^p)$ such that all $x_i \in \mathrm{Prim}_{p^{i-1}}(B_G)$. Clearly, $\mathrm{rk}\,\mathrm{Prim}_{p^s}(B_G)$ is the same for all $0 \leq s < r$, and $\mathrm{Prim}_j B_G = 0$ for all $j \neq p^s$. Then the Hopf algebra morphism

$$u^* : A[x]/(x^q) \longrightarrow B_G, x \longmapsto x_1$$

is compatible with the $\mathbb{F}_q$-actions, i.e., it induces $u : G \to \alpha_q$ in $\mathbb{F}_q\text{-}\mathrm{gr}_A$. Setting the augmentation ideal of α_q to be $I = (x)$, we see that

$$\ker(u) = \mathrm{Spec}\, A[x_2, \dots, x_r]/(x_2^p, \dots, x_r^p) = \mathrm{Spec}(B_G/u^*(I)B_G)$$

is not balanced. Of course, G is not of $\mathbb{F}_q$-additive type.

In Theorem 8.14, we will be able to describe the structure of our category over a perfect field k. This allows the following fibrewise characterization.

COROLLARY 6.9. — *Let $G \in \mathbb{F}_q\text{-}\mathrm{gr}_S^+$ be fibrewise connected. Then G is balanced if and only if it is of the form $\prod \alpha_{q^{s_i}}$ on all geometric fibres over S.*

Proof. — We can check G to be balanced on the fibres, by Remark 5.17 and since the condition is stable under base change (cf. Remark 3.7). By Theorem 8.14, a geometric fibre of G is balanced if and only if it is of the form $\prod \alpha_{q^{s_i}}$. □

The following result gives another perspective on the balance property (see Remark 6.11).

PROPOSITION 6.10. — *Assume that A is an $\mathbb{F}_{q^n}$-algebra, $n \geq 1$. Consider the forgetful functor $\mathcal{F} : \mathbb{F}_{q^n}\text{-}\mathrm{gr}_A^+ \to \mathbb{F}_q\text{-}\mathrm{gr}_A^+$. The following diagram commutes,*

$$\begin{array}{ccc} (M, f) \in \mathbb{F}_{q^n}\text{-}\mathrm{sht}_A & \xrightarrow{\mathcal{G}_{q^n}} & \mathbb{F}_{q^n}\text{-}\mathrm{gr}_A^+ \\ \downarrow \quad \downarrow & & \downarrow \mathcal{F} \\ \Big(\bigoplus_{i=0}^{n-1} (\sigma_q^i)^* M, F\Big) \in \mathbb{F}_q\text{-}\mathrm{sht}_A & \xrightarrow{\mathcal{G}_q} & \mathbb{F}_q\text{-}\mathrm{gr}_A^+, \end{array} \tag{6.2}$$

where $F : (x_0, \dots, x_{n-1}) \mapsto (x_1, \dots, x_{n-1}, f(x_0))$ is the matrix $\begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ f & & & 0 \end{pmatrix}$.

Proof. — We denote the scalar multiplication on $(\sigma_q^i)^* M$ by $\lambda.x = \lambda^{q^i} x$ (the usual action without the dot), for $\lambda \in A, x \in M$. Since f is q^n-linear, we get

$$F(\lambda.(x_0, \dots, x_{n-1})) = (\lambda^q x_1, \dots, \lambda^{q^{n-1}} x_{n-1}, \lambda^{q^n} f(x_0)) = \lambda^q.F(x_0, \dots, x_{n-1}),$$

for all $(x_0, \dots, x_{n-1}) \in M' := \bigoplus_{i=0}^{n-1} (\sigma_q^i)^* M$. We have to show that

$$\mathrm{Sym}(M)/\mathfrak{f}_M \cong \mathrm{Sym}(M')/\mathfrak{f}_{M'} \text{ in } \mathbb{F}_q\text{-}\mathrm{hopf}_A,$$

where $\mathfrak{f}_M = (x^{\otimes q^n} - f(x) \mid x \in M)$ and $\mathfrak{f}_{M'} = (\underline{x}^{\otimes q} - F(\underline{x}) \mid \underline{x} \in M')$.

We define

$$\varphi : \mathrm{Sym}(M) \longrightarrow \mathrm{Sym}(M')/\mathfrak{f}_{M'} \text{ via } M \ni x \longmapsto (x, 0, \dots, 0) \in M',$$

extended to an algebra morphism. Note that for $x \in M$, we have

$$\varphi(x^{q^i}) = (x, 0, \dots, 0)^{q^i} = F^i(x, 0, \dots, 0) = (\dots, 0, x, 0, \dots) \in (\sigma_q^i)^* M \subseteq M'.$$

Now, φ factors through the quotient, because

$$\varphi(x^{q^n} - f(x)) = F^n(x, 0, \dots, 0) - (f(x), 0, \dots, 0) = 0.$$

Finally, $\overline{\varphi} : \mathrm{Sym}(M)/\mathfrak{f}_M \to \mathrm{Sym}(M')/\mathfrak{f}_{M'}$ is an isomorphism in $\mathbb{F}_q\text{-}\mathrm{Hopf}_A$, since by definition,

$$\overline{\varphi}(\mathrm{Prim}_1(\mathrm{Sym}(M)/\mathfrak{f}_M)) = \mathrm{Prim}_1(\mathrm{Sym}(M')/\mathfrak{f}_{M'}),$$

and locally on $\mathrm{Spec}(A)$, it maps bases to bases. □

REMARK 6.11. — Consider the following diagram,

$$\begin{array}{ccc} \mathbb{F}_q\text{-}\mathrm{gr}_A^+ & \xrightarrow{\mathcal{M}_q} & \mathbb{F}_q\text{-}\mathrm{sht}_A \ni (M, f) \\ \mathcal{F}\downarrow & & \downarrow \qquad \downarrow \\ \mathbb{F}_p\text{-}\mathrm{gr}_A^+ & \xrightarrow{\mathcal{M}_p} & \mathbb{F}_p\text{-}\mathrm{sht}_A \ni \Big(\bigoplus_{t=0}^{r-1} (\sigma_p^t)^* M, F\Big) \end{array} \tag{6.3}$$

corresponding to the commutative diagram (6.2). Requiring (6.3) to commute recovers the balance condition. Namely, for $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$, we have

$$\mathrm{Prim}(B_G) \cong \bigoplus_{t=0}^{r-1} (\sigma_p^t)^* \mathrm{Prim}_1(B_G)$$

if and only if all the (linearized) maps

$$(\sigma_p^t)^* \mathrm{Prim}_1(B_G) \longrightarrow \mathrm{Prim}_{p^t}(B_G), x \longmapsto x^{p^t}, (0 \le t < r)$$

are isomorphisms. This is equivalent to condition (ii) in Lemma 5.12.

7. Quasi-balanced group schemes

Let A be an $\mathbb{F}_q$-algebra, $q = p^r$. For $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$, consider the eigenspace decomposition

$$I_G = \bigoplus_{j=1}^{q-1} I_j$$

for the $\mathbb{F}_q^\times$-action on the augmentation ideal of G, cf. (5.3).

DEFINITION 7.1. — A group scheme $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$ is called quasi-balanced if $\mathrm{rk}(I_j)$ is the same for all $1 \leq j \leq q-1$.

REMARK 7.2. — Let $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$ be quasi-balanced. By Proposition 3.6, we have $\mathrm{rk}(I_G) = p^N - 1$, where $N = \mathrm{rk}(\mathrm{Prim}(B_G))$. Then we have $\frac{p^N-1}{q-1} \in \mathbb{Z}$, and thus $r|N$, say $rn = N$. This yields

$$\mathrm{rk}(I_j) = q^{n-1} + \cdots + q + 1 \text{ for all } 1 \leq j \leq q-1,$$

and of course $\operatorname{ord} G = q^n$. Note that the analog of Remark 5.17 holds, i.e., for $G \in \mathbb{F}_q\text{-}\mathrm{gr}_S^+$, the quasi-balanced locus of G in S is closed and open (if the base is noetherian).

LEMMA 7.3. — *Every $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^{+,\mathrm{b}}$ is quasi-balanced.*

Proof. — We may assume that A is a local ring. If $x_1, \ldots, x_n$ is a basis of $\mathrm{Prim}_1(B_G)$, then, since G is balanced,

$$\{\prod_{i=1}^n x_i^{e_i} \mid 0 \leq e_i < q, (e_1, \ldots, e_n) \neq 0\}$$

is a basis of I_G (cf. Remark 6.4). On this basis, $\alpha \in \mathbb{F}_q$ acts via

$$[\alpha]^* \prod_{i=1}^n x_i^{e_i} = \alpha^{\sum e_i} \prod_{i=1}^n x_i^{e_i}.$$

Therefore, it decomposes into eigenbases for I_j,

$$\{\prod_{i=1}^n x_i^{e_i} \mid 0 \leq e_i < q, (e_1, \ldots, e_n) \neq 0, \sum_{i=1}^n e_i \equiv j \bmod q-1\}.$$

In order to count the ranks, we identify the bases with

$$E_j^{(n)} := \{0 \neq \underline{e} = (e_1, \ldots, e_n) \mid 0 \leq e_i < q, \sum_{i=1}^n e_i \equiv j \bmod q-1\}.$$

We claim that

$$\#E_j^{(n)} = q^{n-1} + \cdots + q + 1 \text{ for all } 1 \leq j \leq q-1.$$

Let us prove this by induction on n. For $n = 1$, there is nothing to show. For $n > 1$, we have

$$E_j^{(n)} = \coprod_{e=0}^{q-1} \{\underline{e} \in E_j^{(n)} \mid e_n = e\} = \coprod_{e=0}^{q-1} \{(\underline{e}, e) \mid \underline{e} \in E_{j-e}^{(n-1)}\} \amalg \{(0, \ldots, 0, j)\}.$$

Therefore indeed: $\#E_j^{(n)} = q(q^{n-2} + \cdots + q + 1) + 1 = q^{n-1} + \cdots + q + 1$. □

REMARK 7.4. — For $G \in \mathrm{gr}_A^+$, i.e., $q = p$, the condition of being quasi-balanced is therefore automatic. We can also see this concretely via p-adic expansion. Namely, let

$$\rho : \mathbb{Z}/(p^n - 1) \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}/(p-1)$$

be the projection, where $\operatorname{ord} G = p^n$, as above. Then we have the bijection

$$E_j = E_j^{(n)} \xrightarrow{\sim} \rho^{-1}(j), (e_1, \dots, e_n) \longmapsto \sum_{i=1}^{n} e_i p^i,$$

and thus again $\#E_j = \frac{p^n-1}{p-1} = p^{n-1} + \cdots + p + 1$.

LEMMA 7.5. — *Let $G, H \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$. For $1 \leq j \leq q-1$, the eigenspaces in the product satisfy*

$$\operatorname{rk} I_j(G \times H) = \sum_{\substack{k+l \equiv j \bmod q-1 \\ 0 \leq k,l \leq q-1}} \operatorname{rk} I_k(G) \cdot \operatorname{rk} I_l(H), \tag{7.1}$$

with the convention $I_0(-) := A$.

Proof. — The product decomposes as follows,

$$B_G \otimes_A B_H = \Big(\bigoplus_{k=0}^{q-1} I_k(G)\Big) \otimes_A \Big(\bigoplus_{l=0}^{q-1} I_l(H)\Big) = \bigoplus_{k,l} \Big(I_k(G) \otimes_A I_l(H)\Big),$$

and, of course, whenever $k + l \equiv j \bmod q-1$, we have

$$I_k(G) \otimes_A I_l(H) \subseteq I_j(G \times H),$$

by definition of the product $\mathbb{F}_q$-action. □

COROLLARY 7.6. — *Let $G, H \in \mathbb{F}_q\text{-}\mathrm{gr}_A$. If two of G, H and $G \times H$ are quasi-balanced, then so is the third.*

Proof. — Let G, H be quasi-balanced. By Remark 7.2, we have $\operatorname{ord} G = q^n$ and $\operatorname{ord} H = q^m$ for some $n, m \in \mathbb{N}$. Then for any $1 \leq j \leq q-1$, the product formula (7.1) becomes

$$\begin{aligned}
&\operatorname{rk} I_j(G \times H) \\
&= \sum_{\substack{k+l \equiv j \bmod q-1 \\ 1 \leq k,l \leq q-1}} \operatorname{rk} I_k(G) \cdot \operatorname{rk} I_l(H) + \operatorname{rk} I_j(G) + \operatorname{rk} I_j(H) \\
&= (q-1)(q^{n-1} + \cdots + q + 1)(q^{m-1} + \cdots + q + 1) + \operatorname{rk} I_j(G) + \operatorname{rk} I_j(H) \\
&= (q^n - 1)(q^{m-1} + \cdots + q + 1) + (q^{n-1} + \cdots + q + 1) + (q^{m-1} + \cdots + q + 1) \\
&= q^n(q^{m-1} + \cdots + q + 1) + q^{n-1} + \cdots + q + 1 \\
&= q^{n+m-1} + \cdots + q^n + q^{n-1} + \cdots + q + 1.
\end{aligned}$$

We conclude that $G \times H$ is quasi-balanced.

Conversely, assume that H and $G \times H$ are quasi-balanced. By Remark 7.2,

$$\operatorname{ord} H = q^m, \text{ and } \operatorname{ord}(G \times H) = q^{n+m},$$

for some $m, n \in \mathbb{N}$, and hence $\operatorname{ord} G = q^n$. Applying (7.1) again, we get that

$$\begin{aligned} & q^{n+m-1} + \cdots + q + 1 \\ = & \sum_{1 \leq k \leq q-1} \operatorname{rk} I_k(G)(q^{m-1} + \cdots + q + 1) + \operatorname{rk} I_j(G) + \operatorname{rk} I_j(H) \\ = & (q^n - 1)(q^{m-1} + \cdots + q + 1) + \operatorname{rk} I_j(G) + (q^{m-1} + \cdots + q + 1) \\ = & q^{n+m-1} + \cdots + q^n + \operatorname{rk} I_j(G), \end{aligned}$$

for $1 \leq j \leq q-1$, and hence the claim. □

REMARK 7.7. — Let us consider group schemes of the form

$$G = \operatorname{Spec}(A[x_1, \ldots, x_h]/(x_1^{p^{s_1}}, \ldots, x_h^{p^{s_h}})) = \prod_{i=1}^{h} \alpha_{p^{s_i}},$$

so that all $x_i \in \operatorname{Prim}_1(B_G)$. Consider the standard basis of I_G,

$$\{\prod_{i=1}^{h} x_i^{e_i} \mid 0 \leq e_i < p^{s_i}, (e_1, \ldots, e_h) \neq 0\}.$$

As always, it decomposes into eigenbases for the I_j. This yields

$$\operatorname{rk} I_j = \sum_{\substack{a \equiv j \bmod q-1 \\ a \neq 0}} n_a,$$

where

$$n_a := \#\{0 \neq (e_1, \ldots, e_h) \mid 0 \leq e_i < p^{s_i}, \sum_{i=1}^{h} e_i = a\}.$$

Note that n_a is precisely given by the coefficient of X^a in the polynomial

$$S(X) = (X^{p^{s_1}-1} + \cdots + X + 1) \cdot \ldots \cdot (X^{p^{s_h}-1} + \cdots + X + 1) \in \mathbb{Z}[X]. \tag{7.2}$$

EXAMPLE 7.8. — Let $q = 4$, and consider the special case

$$G = \operatorname{Spec}(A[x_1, \ldots, x_6]/(x_1^p, \ldots, x_6^p)).$$

Then $G \in \mathbb{F}_q\text{-}\operatorname{gr}_A$ is quasi-balanced, since

$$S(X) = (X+1)^6 = X^6 + 6X^5 + 15X^4 + 20X^3 + 15X^2 + 6X + 1.$$

Hence $\operatorname{rk} I_j = 21$ for all $1 \leq j \leq 3$. But obviously $G \notin \mathbb{F}_q\text{-}\operatorname{gr}_A^{+,\mathrm{b}}$, because $\operatorname{Prim}_p(B_G) = 0$. Thus the converse to Lemma 7.3 is false in general.

However, this is essentially the "only" counter-example, as shown below.

PROPOSITION 7.9. — *Let $G = \alpha_{p^{s_1}} \times \ldots \times \alpha_{p^{s_h}}$ as in Remark 7.7.*

1. *If $q \neq 4$, then G is quasi-balanced if and only if $r \mid s_i$ for all $1 \leq i \leq h$.*
2. *If $q = 4$, then G is quasi-balanced if and only if $6 \mid \#\{i \mid s_i \not\equiv 0 \bmod r\}$.*

Proof (joint with Sauermann). — By Corollary 7.6, G is quasi-balanced if and only if $G \times \alpha_{q^m}$ is quasi-balanced, for $m \in \mathbb{N}$. Eliminating the factors of the form α_{q^m} from G, we can therefore assume that $s_i \not\equiv 0 \bmod r$ for all i. Then we have to show that

$$G \text{ is quasi-balanced if and only if } h = 0 \text{ in case (1), and } 6 \mid h \text{ in case (2).}$$

Note that for $r = 1$, the claims are vacuous.

First, let us assume that G is quasi-balanced. We keep the notation from Remark 7.7. Evaluating (7.2) at the primitive root of unity $\zeta = e^{\frac{2\pi i}{q-1}} \in \mu_{q-1}(\mathbb{C})$ yields

$$S(\zeta) = \sum_{a \geq 0} n_a \zeta^a = \sum_{j=0}^{q-1} \mathrm{rk}(I_j)\zeta^j = 1 + \mathrm{rk}(I_1) \sum_{j=1}^{q-1} \zeta^j = 1 + \mathrm{rk}(I_1) \frac{\zeta^{q-1} - 1}{\zeta - 1} = 1.$$

Let $0 < t_i < r$ with $s_i \equiv t_i \bmod r$. Then

$$1 = S(\zeta) = \prod_{i=1}^{h} (\zeta^{p^{s_i}-1} + \cdots + \zeta + 1) = \prod_{i=1}^{h} \frac{\zeta^{p^{s_i}} - 1}{\zeta - 1} = \prod_{i=1}^{h} \frac{\zeta^{p^{t_i}} - 1}{\zeta - 1}. \tag{7.3}$$

On the other hand, $|\zeta^j - 1| \geq |\zeta - 1|$ for all $1 \leq j < q - 1$. Hence by (7.3) we must have

$$|\zeta^{p^{t_i}} - 1| = |\zeta - 1| \text{ for all } 1 \leq i \leq h.$$

Since $0 < t_i < r$, this implies that $p^{t_i} \equiv -1 \bmod q - 1$, and therefore

$$q = p^{t_i} + 2, \text{ for } 1 \leq i \leq h.$$

Thus $q = 4$ (unless $h = 0$), and $t_i = 1$ for all i. In that case then, (7.3) reads

$$(\zeta + 1)^h = 1.$$

But $\zeta + 1 = e^{\frac{2\pi i}{3}} + 1 = e^{\frac{2\pi i}{6}}$, and therefore $6 \mid h$.

Conversely, the "if"-direction in (1) is trivial ($h = 0$). In case (2), keeping in mind (7.3),

$$\mathrm{rk}(I_1) + \mathrm{rk}(I_2)\zeta + \mathrm{rk}(I_3)\overline{\zeta} = S(\zeta) - 1 = (\zeta + 1)^h - 1 = 0.$$

Conjugating this equation, we see that indeed $\mathrm{rk}(I_1) = \mathrm{rk}(I_2) = \mathrm{rk}(I_3)$. □

THEOREM 7.10. — *Let $q \neq 4$. Then $G \in \mathbb{F}_q\text{-}\mathrm{gr}_A^+$ is quasi-balanced if and only if it is balanced.*

Proof. — We have already seen "$\Leftarrow$" in Lemma 7.3. Now let G be quasi-balanced. Since the condition is stable under base change, we can assume A to be a perfect field. As in (the proof of) Theorem 8.14, we have an $\mathbb{F}_q$-equivariant decomposition

$$G = \pi_0(G) \times H.$$

By Remark 5.18, $\pi_0(G)$ is balanced, hence quasi-balanced, and so H is quasi-balanced as well by Corollary 7.6. Again as in Theorem 8.14,

$$B_H \cong k[x_1, \dots, x_h]/(x_1^{p^{s_1}}, \dots, x_h^{p^{s_h}}) \text{ in } \mathbb{F}_q\text{-}\operatorname{hopf}_A .$$

Therefore, by Proposition 7.9, since H is quasi-balanced, $r \mid s_i$ for all $1 \leq i \leq h$, and thus H is balanced, which means so is G. □

8. The infinite case

In this section, we detail some of the difficulties one encounters when trying to transfer the theory from the finite to the infinite case.

DEFINITION 8.1. — The category $\mathbb{F}_q\text{-}\operatorname{Sht}_A$ consists of pairs (M, f) of a flat A-module M and a q-linear endomorphism f of M. Morphisms in $\mathbb{F}_q\text{-}\operatorname{Sht}_A$ are defined as in $\mathbb{F}_q\text{-}\operatorname{sht}_A$. Note that again $\mathbb{F}_p\text{-}\operatorname{Sht}_A = \operatorname{Sht}_A$.

The shtuka (M, f) is called locally finitely generated if locally over $\operatorname{Spec} A$, there exist some $x_1, \dots, x_N \in M$ such that

$$M = \{\sum_{i=1}^{N} \sum_{a=0}^{d} \lambda_a f^a(x_i) \mid \lambda_a \in A,\ d \in \mathbb{N}\}.$$

We denote by $\mathbb{F}_q\text{-}\operatorname{Sht}_{A,\mathrm{f.g.}}$ the full subcategory of $\mathbb{F}_q\text{-}\operatorname{Sht}_A$ of locally finitely generated shtukas.

Trying to define the functor $\mathcal{M}$ in general, the first problem to arise is the following.

CONJECTURE 8.2. — *Let $G \in \operatorname{Gr}_A^+$. Then the A-module $\operatorname{Prim}(B_G)$ is flat.*

Let us provisionally include the condition in the definition, and denote the corresponding full subcategories by $\operatorname{Gr}_A^{\boxplus}$, $\mathbb{F}_q\text{-}\operatorname{Gr}_A^{\boxplus}$, and so forth. Then we may define

$$\mathcal{M}_q = \mathcal{M} : \mathbb{F}_q\text{-}\operatorname{Gr}_A^{\boxplus} \longrightarrow \mathbb{F}_q\text{-}\operatorname{Sht}_A, \text{ and } \mathcal{G}_q = \mathcal{G} : \mathbb{F}_q\text{-}\operatorname{Sht}_A \longrightarrow \mathbb{F}_q\text{-}\operatorname{Gr}_A^{\boxplus},$$

as before. Recall that $\mathcal{M}_q(G)$ is flat if $\operatorname{Prim}(B_G)$ is, cf. Remark 5.5.

REMARK 8.3. — The routine verifications in §6, together with the following, show that the two functors are well-defined. Let $(M, f) \in \mathbb{F}_q\text{-}\operatorname{Sht}_A$. Then we can write $M = \varinjlim M_i$, where the M_i are finitely generated free A-modules, by

[12], Théorème 1.2. For each i, choose a basis N_i of M_i, and set $N := \coprod N_i$. Denote by $\gamma_i : M_i \hookrightarrow \mathrm{Sym}(M_i) \to \varinjlim \mathrm{Sym}(M_i)$. Then

$$\begin{aligned} A[x_n \mid n \in N] &\twoheadrightarrow \varinjlim \mathrm{Sym}(M_i) \cong \mathrm{Sym}(M) \twoheadrightarrow \mathrm{Sym}(M)/\mathfrak{f}, \\ x_n &\longmapsto \gamma_i(n), \text{ when } n \in N_i. \end{aligned}$$

This yields $\mathcal{G}(M,f) \hookrightarrow \mathbb{G}_a^N$, by universality $\mathbb{F}_q$-equivariantly. Thus $\mathcal{G}(M,f)$ is of $\mathbb{F}_q$-additive type.

The adjunction (cf. [11], Lemma B.3.9) holds in this generality.

LEMMA 8.4. — *The functors $\mathcal{G}$ and $\mathcal{M}$ form an adjoint pair $(\mathcal{G},\mathcal{M})$ of $\mathbb{F}_q$-linear functors, that is, there exist bifunctorial isomorphisms of $\mathbb{F}_q$-vector spaces*

$$\mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(G, \mathcal{G}(M,f)) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Sht}_A}((M,f), \mathcal{M}(G)).$$

In particular, $\mathcal{G}$ is right-exact and $\mathcal{M}$ is left-exact.

Proof. — We use $\mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(G, \mathcal{G}(M,f)) \cong \mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Hopf}_A}(\mathrm{Sym}(M)/\mathfrak{f}, B_G)$. Now $\varphi \longmapsto \varphi|_M$ yields a well-defined and bijective map

$$\mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Hopf}_A}(\mathrm{Sym}(M)/\mathfrak{f}, B_G) \longrightarrow \mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Sht}_A}((M,f), \mathcal{M}(G)). \tag{8.1}$$

Indeed, by definition, $M \subseteq \mathrm{Prim}_1(\mathrm{Sym}(M)/\mathfrak{f})$, and hence $\varphi(M) \subseteq \mathrm{Prim}_1(B_G)$. Furthermore, $\varphi|_M$ is a morphism of shtukas. Namely, the diagram

$$\begin{array}{ccc} M & \xrightarrow{\varphi|_M} & \mathrm{Prim}_1(B_G) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle z\mapsto z^q} \\ M & \xrightarrow{\varphi|_M} & \mathrm{Prim}_1(B_G) \end{array}$$

commutes, because $\varphi(x^{\otimes q} - f(x)) = 0$ for all $x \in M$, by definition. The inverse map of (8.1) is given by

$$\mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Sht}_A}((M,f), \mathcal{M}(G)) \longrightarrow \mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Hopf}_A}(\mathrm{Sym}(M)/\mathfrak{f}, B_G), \Phi \longmapsto \widehat{\Phi},$$

where $\widehat{\Phi}$ is the extension of Φ to all of $\mathrm{Sym}(M)$, which descends to $\mathrm{Sym}(M)/\mathfrak{f}$. Namely, the diagram

$$\begin{array}{ccc} M & \xrightarrow{\Phi} & \mathrm{Prim}_1(B_G) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle z\mapsto z^q} \\ M & \xrightarrow{\Phi} & \mathrm{Prim}_1(B_G) \end{array}$$

commutes, and thus $\widehat{\Phi}(x^{\otimes q} - f(x)) = \Phi(x)^q - \Phi(f(x)) = 0$ for $x \in M$. Finally, $\widehat{\Phi}$ clearly respects the coalgebra structure and $\mathbb{F}_q$-action, since it is universal.

Now, $\mathrm{Hom}_{\mathbb{F}_q\text{-}\mathrm{Gr}_A}(-, \mathbb{G}_a)$ is additive, and it follows from Proposition 2.12 that

$$\mathrm{Prim}_1(B_G \otimes B_H) = \mathrm{Prim}_1(B_G) \otimes 1 + 1 \otimes \mathrm{Prim}_1(B_H).$$

Hence $z \mapsto z^q$ in $\mathcal{M}(G \times H)$ is given by $(x, y) \mapsto (x^q, y^q)$ in $\mathcal{M}(G) \oplus \mathcal{M}(H)$, and so $\mathcal{M}$ is additive. By adjunction, so is $\mathcal{G}$. Note that it is evident that $\mathcal{G}$ sends surjective morphisms to closed embeddings in $\mathbb{F}_q\text{-}\operatorname{Gr}_A$.

The $\mathbb{F}_q$-linearity is trivial, as it reduces to the statement that $\alpha \in \mathbb{F}_q$ acts on the eigenspace $\operatorname{Prim}_1(-)$ by scalar multiplication. □

In order to show the analog of Theorem 6.5, we would like to restrict ourselves to group schemes which are locally of finite presentation over the base. However, the following question remains open.

CONJECTURE 8.5. — *Let $G \in \operatorname{Gr}_A^{\boxplus}$ be locally finitely presented. There exists a closed embedding $\iota : G \hookrightarrow \mathbb{G}_a^N$, $N \in \mathbb{N}$, locally on* $\operatorname{Spec} A$*, such that the induced morphism*

$$\iota^* : \mathcal{M}_p(\mathbb{G}_a^N) = A[F]^N \longrightarrow \mathcal{M}_p(G)$$

is surjective.

REMARK 8.6. — It seems reasonable to presume that if G satisfies Conjecture 8.5, then indeed any embedding $G \hookrightarrow \mathbb{G}_a^N$, $N \in \mathbb{N}$, induces a surjection on the primitive elements. Certainly, if $A = k$ is a field, this is true by Theorem 1.1, specifically the exactness of $\mathcal{M}$.

Moreover, recall that it holds for finite G over any base A, cf. (5.4).

REMARK 8.7. — The restricted functor $\mathcal{M} : \mathbb{F}_q\text{-}\operatorname{Gr}_{A,\mathrm{f.p.}}^{\boxplus} \to \mathbb{F}_q\text{-}\operatorname{Sht}_{A,\mathrm{f.g.}}$ is well-defined, assuming Conjecture 8.5 holds. For this, we have to see that for a surjective morphism

$$\iota^* : A[x_1, \ldots, x_N] \twoheadrightarrow B_G \text{ in } \mathbb{F}_q\text{-}\operatorname{Hopf}_A,$$

the elements $\iota^*(x_1), \ldots, \iota^*(x_N) \in \operatorname{Prim}_1(B_G)$ form a system of generators under $x \mapsto x^q$. But indeed, recall from Proposition 3.9 that

$$\operatorname{Prim}_1(A[x_1, \ldots, x_N]) = \operatorname{span}_A(x_i^{q^a} \mid 1 \leq i \leq N, a \in \mathbb{N}).$$

On the other hand, Conjecture 8.5 implies that $\mathcal{M}(\iota) = \iota^*|_{\mathcal{P}_1}$ surjects onto $\operatorname{Prim}_1(B_G)$, as in the proof of Theorem 5.10.

LEMMA 8.8. — *Assume Conjecture 8.5. For $G \in \mathbb{F}_q\text{-}\operatorname{Gr}_{A,\mathrm{f.p.}}^{\boxplus}$, the following are equivalent.*

(i) *All $f_t : \operatorname{Prim}_{p^t}(B_G) \to \operatorname{Prim}_{p^{t+1}}(B_G), x \mapsto x^p$, are bijective.*

(ii) *The map $f' : \operatorname{Prim}_1(B_G) \to \operatorname{Prim}_{p^{r-1}}(B_G), x \mapsto x^{p^{r-1}}$, is injective.*

Proof. — The claim tautologically follows from the analog of Theorem 5.10, the key ingredient in the proof of which is precisely Conjecture 8.5. □

DEFINITION 8.9. — We say $G \in \mathbb{F}_q\text{-}\mathrm{Gr}^{\boxplus}_{A,\mathrm{f.p.}}$ is balanced if the conditions in Lemma 8.8 hold. We denote by $\mathbb{F}_q\text{-}\mathrm{Gr}^{\boxplus,\mathrm{b}}_{A,\mathrm{f.p.}}$ the full subcategory of $\mathbb{F}_q\text{-}\mathrm{Gr}^{\boxplus}_{A,\mathrm{f.p.}}$ of balanced group schemes.

REMARK 8.10. — The functor $\mathcal{G} : \mathbb{F}_q\text{-}\mathrm{Sht}_{A,\mathrm{f.g.}} \to \mathbb{F}_q\text{-}\mathrm{Gr}^{\boxplus,\mathrm{b}}_{A,\mathrm{f.p.}}$ is well-defined. To see this, let $(M, f) \in \mathbb{F}_q\text{-}\mathrm{Sht}_{A,\mathrm{f.g.}}$ and locally over $\operatorname{Spec} A$, choose a system of generators $x_1, \dots, x_N$ of (M, f). Then this yields an epimorphism

$$A[x_1, \dots, x_N] \twoheadrightarrow \mathrm{Sym}(M)/\mathfrak{f},$$

locally on $\operatorname{Spec} A$. Indeed, all elements of $\mathrm{Sym}(M)/\mathfrak{f}$ are polynomial in the x_i, as we can write any $x \in M$ as

$$x = \sum_{i=1}^{N}\sum_{a=0}^{d} \lambda_a f^a(x_i) = \sum_{i=1}^{N}\sum_{a=0}^{d} \lambda_a x_i^{\otimes q^a} \text{ in } \mathrm{Sym}(M)/\mathfrak{f}.$$

Keeping in mind Theorem 5.10, it then moreover follows that for all $0 \leq s < r$, the maps

$$M = \mathrm{Prim}_1(\mathrm{Sym}(M)/\mathfrak{f}) \twoheadrightarrow \mathrm{Prim}_{p^s}(\mathrm{Sym}(M)/\mathfrak{f}), x \longmapsto x^{p^s},$$

are bijective. We conclude that $\mathcal{G}(M, f)$ is balanced, by Lemma 8.8, (ii).

REMARK 8.11. — Let $G \in \mathbb{F}_q\text{-}\mathrm{Gr}^{\boxplus}_{A,\mathrm{f.p.}}$ and $\iota : G \hookrightarrow \mathbb{G}_a^N$. Let further R be the residue field at a point $s \in \operatorname{Spec} A$. Then $\iota_s : G_s \hookrightarrow \mathbb{G}_{a,s}^N$ is a closed embedding as well. Therefore,

$$\begin{array}{ccc} \mathrm{Prim}(A[x_1, \dots, x_N]) \otimes_A R & \twoheadrightarrow & \mathrm{Prim}(B_G) \otimes_A R \\ \downarrow (*) & & \downarrow \\ \mathrm{Prim}(R[x_1, \dots, x_N]) & \twoheadrightarrow & \mathrm{Prim}(B_G \otimes_A R) \end{array}$$

by Conjecture 8.5 (and recalling Remark 3.7). We can see for example from Proposition 3.9 that $(*)$ is an isomorphism. Thus, the primitive elements are stable under taking fibres.

Note that if we assume Conjecture 8.5, then we only need Conjecture 8.2 to hold for locally finitely presented G. Indeed, we can then prove the adjunction of $\mathcal{G}$ and $\mathcal{M}$ as functors between $\mathbb{F}_q\text{-}\mathrm{Gr}^{+,\mathrm{b}}_{A,\mathrm{f.p.}}$ and $\mathbb{F}_q\text{-}\mathrm{Sht}_{A,\mathrm{f.g.}}$ by the identical argument.

THEOREM 8.12. — *Assume that Conjectures 8.2 and 8.5 are true. The functor*

$$\mathcal{G} : \mathbb{F}_q\text{-}\mathrm{Sht}_{A,\mathrm{f.g.}} \longrightarrow \mathbb{F}_q\text{-}\mathrm{Gr}^{+,\mathrm{b}}_{A,\mathrm{f.p.}}$$

defines an anti-equivalence of categories with quasi-inverse $\mathcal{M}$.

Proof. — We follow [2], IV, §3, 6.5. First of all, we may assume that A is a local ring, and in fact even an Artin local ring, by Remark 8.11. We consider the short exact sequence

$$0 \longrightarrow G \xrightarrow{u_G} \mathcal{G}(\mathcal{M}(G)) \longrightarrow Q \longrightarrow 0, \tag{8.2}$$

defined by the adjunction morphism. On the other hand, we once again have the isomorphism

$$v^{-1}_{\mathcal{M}(G)} = \mathcal{M}(u_G) : \mathcal{M}(\mathcal{G}(\mathcal{M}(G))) \xrightarrow{\sim} \mathcal{M}(G).$$

Since G is balanced, $\mathcal{M}(u_G)$ extends to all primitive elements, i.e.,

$$\mathrm{Hom}_{\mathrm{Gr}_A}(u_G, \mathbb{G}_a) : \mathrm{Hom}_{\mathrm{Gr}_A}(\mathcal{G}(\mathcal{M}(G)), \mathbb{G}_a) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Gr}_A}(G, \mathbb{G}_a).$$

Then applying $\mathcal{M}_p = \mathrm{Hom}_{\mathrm{Gr}_A}(-, \mathbb{G}_a)$ to (8.2) yields the exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathrm{Gr}_A}(Q, \mathbb{G}_a) \longrightarrow \mathrm{Hom}_{\mathrm{Gr}_A}(\mathcal{G}(\mathcal{M}(G)), \mathbb{G}_a) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Gr}_A}(G, \mathbb{G}_a). \tag{8.3}$$

The fibre of Q over the closed point of $\operatorname{Spec} A$ is unipotent by [2], IV, §2, 2.3, i.e., there is a non-trivial morphism to the additive group.

Since A is an Artin ring, this lifts to $Q \to \mathbb{G}_a$, up to a Frobenius twist on $\mathbb{G}_a$. But (8.3) tells us that $\mathrm{Hom}_{\mathrm{Gr}_A}(Q, \mathbb{G}_a) = 0$, hence Q must be trivial. □

REMARK 8.13. — In particular, if $A = k$ is a field, then $\mathbb{F}_q\text{-}\mathrm{Gr}^{+,\mathrm{b}}_{k,\mathrm{f.p.}}$ is an abelian category, in which $\mathbb{G}_a$ is an injective object.

Moreover, in this case, we can drop the conditions that our group schemes G are finitely presented and that our $k[F^r]$-modules are finitely generated, respectively. Indeed, we may argue as above, applying Theorem 1.1 on the way.

In fact, we can use [2], III, §3, 7.5, in order to write $G = \varprojlim G_i$ with $G_i \in \mathbb{F}_q\text{-}\mathrm{Gr}^+_k$ finitely presented, compatibly with $\mathcal{M}$ and $\mathcal{G}$. Namely, $G \to G_i$ is an epimorphism (cf. *loc.cit.*, 7.4), hence G_i inherits an $\mathbb{F}_q$-action from G, by Remark 5.3. These agree in the limit,

$$\begin{array}{ccccc} G & \twoheadrightarrow & G_j & \twoheadrightarrow & G_i \\ \downarrow{\scriptstyle [\alpha]} & & \downarrow{\scriptstyle [\alpha]_j} & & \downarrow{\scriptstyle [\alpha]_i} \\ G & \twoheadrightarrow & G_j & \twoheadrightarrow & G_i \end{array} \tag{8.4}$$

since the left square and the outer rectangle in (8.4) commute, and so the two compositions in the right square agree up to $G \twoheadrightarrow G_j$, hence must be equal.

Now choose an $\mathbb{F}_q$-equivariant embedding $G \hookrightarrow \mathbb{G}_a^N$. Then we can take the pushout

$$\begin{array}{ccc} G & \hookrightarrow & \mathbb{G}_a^N \\ \downarrow & \ulcorner & \downarrow \\ G_i & \hookrightarrow & H. \end{array} \tag{8.5}$$

But then $H \cong \mathbb{G}_a^n$, by [2], IV, §3, 6.8. To wit, $\mathcal{M}_p(H) \hookrightarrow \mathcal{M}_p(\mathbb{G}_a^N) = k[F]^{\oplus N}$ is injective by left-exactness, hence $\mathcal{M}_p(H) \cong k[F]^{\oplus n}$ for some n, since $k[F]$ is left-Euclidean. Therefore,

$$H = \mathcal{G}_p(\mathcal{M}_p(H)) \cong \mathbb{G}_a^n.$$

From Remark 5.3, we know that the diagram (8.5) in fact lies in $\mathbb{F}_q\text{-}\operatorname{Gr}_k^+$.

Finally, we prove the following structure theorem, generalizing Theorem 1.2.

THEOREM 8.14. — *If k is a perfect field, then $G \in \mathbb{F}_q\text{-}\operatorname{Gr}_k^{+,\mathrm{b}}$ lies in $\mathbb{F}_q\text{-}\operatorname{Gr}_{k,\mathrm{f.p.}}^{+,\mathrm{b}}$ if and only if*

$$G \cong \mathbb{G}_a^n \times \pi_0(G) \times H,$$

with H a product of group schemes of the form α_{q^s} and where $\pi_0(G)$ is an étale sheaf of finite-dimensional $\mathbb{F}_q$-vector spaces. If k is algebraically closed, then

$$\pi_0(G) \cong (\underline{\mathbb{F}_q})^m$$

for some $m \in \mathbb{N}$.

Proof. — As in [2], IV, §3, 6.9, we use the fact that $k[F^r]$ is left-Euclidean to decompose $\mathcal{M}(G)$ into its $k[F^r]$-torsion submodule $M = \mathcal{M}(G)_{\mathrm{tors}}$ and its torsionfree part. Furthermore, applying Lemma 4.4 to M altogether yields the decomposition

$$G = \mathcal{G}(\mathcal{M}(G)) = \mathcal{G}(\mathcal{M}(G)/(M,f)) \times \mathcal{G}(M_{\mathrm{ss}}, f_{\mathrm{ss}}) \times \mathcal{G}(M_{\mathrm{nil}}, f_{\mathrm{nil}}).$$

Then $\mathcal{M}(G)/(M,f)$ is free of finite rank $n \in \mathbb{N}$, and $\mathcal{G}(\mathcal{M}(G)/(M,f)) \cong \mathbb{G}_a^n$. The finite part of G consists of the étale part $\pi_0(G) = \mathcal{G}(M_{\mathrm{ss}}, f_{\mathrm{ss}})$, maximal by Lemma 4.4, and the connected part $H = \mathcal{G}(M_{\mathrm{nil}}, f_{\mathrm{nil}})$, cf. Proposition 6.6. By Theorem 1.2, as a group scheme,

$$H \cong \alpha_{p^{s_1}} \times \ldots \times \alpha_{p^{s_h}} = \operatorname{Spec}(k[x_1, \ldots, x_h]/(x_1^{p^{s_1}}, \ldots, x_h^{p^{s_h}})).$$

By Theorem 5.10, the maps $\operatorname{Prim}_1(B_H) \to \operatorname{Prim}_{p^s}(B_H), x \mapsto x^{p^s}$, are surjective. Thus H can be written as above even in $\mathbb{F}_q\text{-}\operatorname{gr}_k^{+,\mathrm{b}}$. But then $r | s_i$ for all i, cf. Example 5.16.

If k is algebraically closed, then $\pi_0(G)$ is constant. Furthermore, it is killed by $p = F \circ V$ (cf. Remark 2.5) and of q-power order. Hence it is indeed a power of $\underline{\mathbb{F}_q} = \mathrm{Spec}(k[x]/(x^q - x))$. Again as above, the $\mathbb{F}_q$-action must be the canonical one. □

REMARK 8.15. — Note that $\underline{\mathbb{F}_{p^t}}$ is of $\mathbb{F}_q$-additive type if and only if $r|t$.

BIBLIOGRAPHY

[1] V. ABRASHKIN – "Galois modules arising from Faltings's strict modules", *Compos. Math.* **142** (2006), p. 867–888.

[2] M. DEMAZURE & P. GABRIEL – *Groupes algébriques*, North-Holland Publishing Company, 1970.

[3] V. G. DRINFEL′D – "Varieties of modules of F-sheaves", *Funktsional. Anal. i Prilozhen.* **21** (1987), p. 23–41.

[4] G. FALTINGS – "Group schemes with strict $\mathcal{O}$-action", *Mosc. Math. J.* **2** (2002), p. 249–279.

[5] N. J. FINE – "Binomial coefficients modulo a prime", *Amer. Math. Monthly* **54** (1947), p. 589–592.

[6] J.-M. FONTAINE – *Groupes p-divisibles sur les corps locaux*, Astérisque, vol. 47–48, Soc. Math. France, Paris, 1977.

[7] P. GABRIEL – "Étude infinitésimale des schémas en groupes", in *SGA 3, Schémas en Groupes I, exposé VII$_A$ (new edition)*, 2011, available at `https://www.imj-prg.fr/~patrick.polo/SGA3/`, p. 411–499.

[8] A. GENESTIER & V. LAFFORGUE – "Théorie de Fontaine en égales caractéristiques", *Ann. Sci. Éc. Norm. Supér.* **44** (2011), p. 263–360.

[9] U. HARTL & W. KIM – "Local shtukas, Hodge-Pink structures and Galois representations", preprint arXiv:1512.05893, 3000effacer.

[10] U. HARTL & R. K. SINGH – "Local shtukas and divisible local Anderson modules", preprint arXiv:1511.03697, 3000effacer.

[11] G. LAUMON – *Cohomology of Drinfeld modular varieties. Part I*, Cambridge Studies in Advanced Math., vol. 41, Cambridge Univ. Press, Cambridge, 1996.

[12] D. LAZARD – "Autour de la platitude", *Bull. Soc. Math. France* **97** (1969), p. 81–128.

[13] J. S. MILNE – "Basic theory of affine group schemes", course notes, `http://www.jmilne.org/math/CourseNotes/AGS.pdf`, 2012.

[14] R. PINK – "Finite group schemes", course notes, ETH Zürich, `https://people.math.ethz.ch/~pink/ftp/FGS/CompleteNotes.pdf`, 2004/05.

[15] M. RAYNAUD – "Schémas en groupes de type $(p, \ldots, p)$", *Bull. Soc. Math. France* **102** (1974), p. 241–280.

[16] J. Stix – "A course on finite flat group schemes and p-divisible groups", course notes, `http://www.uni-frankfurt.de/52288632/Stix_finflat_Grpschemes.pdf`, 2009.
[17] Y. Taguchi – "A duality for finite t-modules", *J. Math. Sci. Univ. Tokyo* **2** (1995), p. 563–588.
[18] J. Tate – "Finite flat group schemes", in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, Springer, New York, 1997, p. 121–154.
[19] J. Tate & F. Oort – "Group schemes of prime order", *Ann. Sci. École Norm. Sup.* **3** (1970), p. 1–21.