Compositio Math. 142 (2006) 867–888
doi:10.1112/S0010437X06002041

Galois modules arising from Faltings's strict modules

V. Abrashkin

Abstract

Suppose that $O = \mathbb{F}_q[\pi]$ is a polynomial ring and R is a commutative unitary O-algebra. The category of finite flat group schemes over R with a strict action of O was recently introduced by Faltings and appears as an equal characteristic analogue of the classical category of finite flat group schemes in the equal characteristic case. In this paper we obtain a classification of these modules and apply it to prove analogues of properties that were known earlier for classical group schemes.

0. Introduction

Throughout all of this paper p is a fixed prime number. Suppose that R is a commutative unitary ring and Gr_R is the category of finite flat commutative group schemes over R. By definition its objects are $G = \mathrm{Spec}\, A(G)$, where $A(G)$ is a commutative flat R-algebra, which is a locally free R-module of finite rank, with the comultiplication $\Delta : A(G) \longrightarrow A(G) \otimes A(G)$, the counit $e : A(G) \longrightarrow R$ and the coinversion $i : A(G) \longrightarrow A(G)$ satisfying well-known axioms. Denote by Gr'_R the full subcategory of Gr_R consisting of p-group schemes G, i.e. such that G is killed by some power of $p\,\mathrm{id}_G$.

If $R = k$ is a perfect field of characteristic p, then the objects G of Gr'_k can be described in terms of Dieudonne theory, i.e. in terms of finitely generated $W(k)$-modules $M(G)$ with a σ-linear operator F and a σ^{-1}-linear operator V such that $FV = VF = p\,\mathrm{id}_{M(G)}$. ($W(k)$ is the ring of Witt vectors with coefficients in k and σ is its Frobenius automorphism induced by the pth power map in k.)

Suppose that R is the valuation ring of a complete discrete valuation field K of characteristic 0 with a perfect residue field k of characteristic p and $e = e(K/\mathbb{Q}_p)$ is the absolute ramification index of K. Then the classification of objects of the category Gr'_R was made in [Fon75] under the restriction $e = 1$ in terms of finite Honda systems (this classification was not complete for $p = 2$, for an improved version cf. [Abr87a]). Further progress was made in [Abr90] for $e \leqslant p - 1$ (group schemes killed by p), in [Con99] for $e < p - 1$ and, finally, in [Bre00] for an arbitrary e. Most interesting arithmetic applications of finite group schemes $G \in \mathrm{Gr}'_R$ are related to the properties of $\Gamma_K = \mathrm{Gal}(\bar{K}/K)$-modules $H = G(\bar{K})$ of their geometric points. We mention the following three results.

(a) *Serre's conjecture* (proved in [Ray74]). This result describes the action of the inertia subgroup $I_K \subset \Gamma_K$ on the semi-simple envelope of H. It is given by characters $\chi : I_K \longrightarrow \bar{k}^*$ such that for some $N \in \mathbb{N}$, $\chi = \chi_N^a$, where $\chi_N(\tau) = \tau(\eta_N)/\eta_N$, $\eta_N^{p^N-1} = \eta$ is a uniformiser of K, and $a = a_0 + a_1 p + \cdots + a_{N-1}p^{N-1}$ with p-digits $a_0, a_1, \ldots, a_{N-1} \in [0, e]$.

(b) *Ramification estimates.* If $p^M\,\mathrm{id}_G = 0$, then the ramification subgroups $\Gamma_K^{(v)}$ of Γ_K act trivially on H if $v > e(M - 1 + 1/(p - 1))$, cf. [Fon85].

Received 21 December 2004, accepted in final form 21 October 2005.
2000 Mathematics Subject Classification 14L15, 11G09, 11S15.
Keywords: group schemes, Galois modules.
This paper was written as a part of project supported by EPSRC, GR/S72252/01.

(c) *Complete description of the* Γ_K*-module* H (under some additional assumptions). If $e = 1$, $p > 3$ and the $\mathbb{F}_p[\Gamma_K]$-module H satisfies the above Serre's Conjecture and ramification estimates (i.e. the ramification subgroups $\Gamma_K^{(v)}$ act trivially on H if $v > 1/(p-1)$), then there is an $G \in \mathrm{Gr}'_R$ such that $H = G(K_{\mathrm{sep}})$, cf. [Abr90].

Suppose now that R is an $\mathbb{F}_p$-algebra. In this case the category Gr'_R is not interesting because it is 'too big'. For example, if R is an integral domain with the fraction field K then any finite continuous $\mathbb{Z}_p[\Gamma_K]$-module appears in the form $G(K_{\mathrm{sep}})$ for a suitable $G \in \mathrm{Gr}'_R$. Even if we assume that R is an O-algebra, where O is a complete discrete valuation ring (which plays a role of $\mathbb{Z}_p$ in the equal characteristic case), then the category $\mathrm{Gr}'(O)_R$ of all finite flat commutative group schemes with O-action is too big for studying special properties of finite subquotients of formal Drinfeld O-modules over R. This unpleasant situation became completely different when Faltings introduced a new concept of finite flat group schemes with strict O-action, cf. [Fal02]. The main idea of Faltings's definition can be explained as follows.

Suppose that $G = \mathrm{Spec}\, A(G)$ is a finite flat O-module over R. Present $A(G)$ as a complete intersection, i.e. as a quotient $R[X_1, \dots, X_n]/I$ of a ring of polynomials by an ideal I generated by elements of a regular sequence of length n, and define the deformation $A(G)^\flat$ of $A(G)$ as $R[X_1, \dots, X_n]/(I \cdot I_0)$, where $I_0 = (X_1, \dots, X_n)$. Faltings requires that the O-module structure on G, which is given by the endomorphisms $[o] : A(G) \longrightarrow A(G)$, $o \in O$, should have an extension to an O-module structure of the deformation $(A(G), A(G)^\flat)$ of the algebra $A(G)$ and this extension must satisfy the condition of strictness. This means that if $o \in O$ and $[o]^\flat : A(G)^\flat \longrightarrow A(G)^\flat$ is an extension of $[o]$, then $[o]^\flat$ must induce the 'scalar' multiplication by o on I_0/I_0^2 and $I/(I \cdot I_0)$. This definition gives (in our notation) the category $\mathrm{DGr}(O)_R$ of finite strict O-modules $(G, G^\flat)$, where $G^\flat = \mathrm{Spec}\, A(G)^\flat$, and its objects have many interesting properties discussed in [Fal02]. Note that the condition of strictness can be viewed as the absence of the first obstacle in the problem of embedding given finite flat local O-module scheme into a Drinfeld (= formal) O-module.

This paper deals with the classification of finite flat commutative group schemes over R with strict O-action, where $O = \mathbb{F}_q[\pi]$ with fixed variable π. Note that this approach can be easily 'sheafified' to obtain the classification over arbitrary $\mathbb{F}_p$-schemes S. Remarkably (for any O-algebra R!), this classification is an almost complete analogue of the classical Dieudonne theory of conventional group schemes over a perfect field of characteristic p. Main applications are obtained for the full subcategory $\mathrm{DGr}'(O)_R$ of π-torsion group subschemes. In particular, we prove an analogue of Raynaud's theorem, i.e. that locally on R any $(G, G^\flat) \in \mathrm{DGr}'(O)_R$ can be embedded into a π-divisible group consisting of objects of the category $\mathrm{DGr}(O)_R$. If G is a local scheme then this gives locally an embedding of G into a formal Drinfeld O-module over R. In other words, the condition of strictness, when treated as vanishing of the first obstacle for embedding of a local G into a formal O-module, appears as a necessary and sufficient condition for the existence of such an embedding. We also study number-theoretic properties of Galois modules $G(K_{\mathrm{sep}})$ if R is the valuation ring in a complete discrete valuation field K and $(G, G^\flat) \in \mathrm{DGr}(O)_R$. These properties are precise analogues of the above mentioned properties (a)–(c) of conventional group schemes over complete discrete valuation rings of mixed characteristic.

The paper is structured as follows. In § 1 we recall the concept of a strict O-module following the basic idea of Faltings's original definition. In § 2 we describe the category of strict $\mathbb{F}_q$-modules over R and apply this in § 3 to classify the objects of the category $\mathrm{DGr}(O)_R$ if $O = \mathbb{F}_q[\pi]$. This classification is based on the study of primitive elements (i.e. the elements $a \in A(G)$ such that $\Delta a = a \otimes 1 + 1 \otimes a$, where Δ is the comultiplication on G) of the R-algebra $A(G)$, where $(G, G^\flat) \in \mathrm{DGr}(O)_R$. In § 4 we apply this classification to prove that any object of $\mathrm{DGr}'(O)_R$ can be embedded into a π-divisible group over R. This section also contains a comparison of our anti-equivalence with the parallel results in the theory of conventional finite flat group schemes and p-adic

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

representations in the mixed characteristic case from the papers [Abr87a, Abr90, Bre00, Fon90]. In § 5 we establish analogues of the above properties (a), (b) and (c) in the category $\mathrm{DGr}'(O)_R$, where R is the valuation ring of a complete discrete valuation field K containing the ring O.

The author expresses a very deep gratitude to the referee. The original version of this paper dealt only with group schemes over a complete discrete valuation rings of characteristic p with etale generic fibre. The referee proposed to generalize the approach by the use of the classical description of finite flat group schemes having zero Verschiebung from SGA3, cf. [Gab70]. This allowed the author to develop methods from the thesis [Gib04] and to obtain the classification of strict modules over arbitrary ring R of characteristic p. The referee report also contains other interesting observations (the author is very sorry to not be able to mention all of them). In particular, in § 4.2 we follow the referee's ideas to prove the following statement conjectured in [Fal02]: if $O = \mathbb{F}_q[\pi]$, $(G, G^\flat) \in \mathrm{DGr}'(O)_R$ and $\mathrm{rk}_R\, A(G) = q^h$, then G is killed by $[\pi]^h$.

Notation and conventions

Everywhere in the paper p is a fixed prime number, O is a unitary commutative $\mathbb{F}_p$-algebra (in most cases O is the polynomial ring $\mathbb{F}_q[\pi]$) and R is a commutative unitary O-algebra. If $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are maps of sets, then we denote their decomposition as $f \circ g$, i.e. for any $a \in A$, $(f \circ g)(a) = g(f(a))$.

1. Definition and simplest properties

An R-algebra A will be called finite if it is a locally free R-module of finite rank.

1.1 Deformations of augmented R-algebras

For an augmented O-algebra A, we agree to use the following notation: $\varepsilon_A : A \longrightarrow O$, the morphism of augmentation, and $\mathrm{Ker}\, \varepsilon_A = I_A$, the augmentation ideal. If $R[\bar{X}] = R[X_1, \ldots, X_n]$, $n \geqslant 0$, is a polynomial ring we always assume that its augmentation ideal $I_{R[\bar{X}]} = (X_1, \ldots, X_n)$.

The objects of the category DAug_R are the triples $\mathcal{A} = (A, A^\flat, i_{\mathcal{A}})$, where A is a finite augmented R-algebra, $A^\flat$ is an augmented R-algebra and $i_{\mathcal{A}} : A^\flat \longrightarrow A$ is an epimorphic map of augmented R-algebras such that there is a polynomial ring $R[\bar{X}] = R[X_1, \ldots, X_n]$, $n \geqslant 0$, and an epimorphism of augmented R-algebras $j : R[\bar{X}] \longrightarrow A^\flat$ satisfying the following properties:

- the ideal $I := \mathrm{Ker}(j \circ i_{\mathcal{A}})$ is generated by elements of a regular sequence of length n in $R[\bar{X}]$;
- $\mathrm{Ker}\, j = I \cdot I_{R[\bar{X}]}$.

A morphism $\bar{f} = (f, f^\flat) : \mathcal{A} \longrightarrow \mathcal{B} = (B, B^\flat, i_{\mathcal{B}})$ in DAug_R is given by morphisms of augmented R-algebras $f : A \to B$ and $f^\flat : A^\flat \longrightarrow B^\flat$ such that $i_{\mathcal{A}} \circ f = f^\flat \circ i_{\mathcal{B}}$.

Note that if $(A, A^\flat, i_{\mathcal{A}}) \in \mathrm{DAug}_R$, then $A^\flat$ is a finite R-algebra.

Below, we use the simpler notation $(A, A^\flat)$ instead of $(A, A^\flat, i_{\mathcal{A}})$ if it does not lead to a misunderstanding.

In the category DAug_R, $\mathcal{R} = (R, R, \mathrm{id}_R)$ is an initial object and any $\mathcal{A} = (A, A^\flat, i_{\mathcal{A}})$ has a natural augmentation to $\mathcal{R}$, $\varepsilon_{\mathcal{A}} = (\varepsilon_A, \varepsilon_{A^\flat}) : \mathcal{A} \longrightarrow \mathcal{R}$, where $\mathrm{Ker}\, \varepsilon_{A^\flat} = \mathrm{Ann}(\mathrm{Ker}\, i_{\mathcal{A}}) := I_{A^\flat}$.

Introduce the R-modules $t^*_{\mathcal{A}} = I_{R[\bar{X}]}/I^2_{R[\bar{X}]}$ and $N_{\mathcal{A}} = I/(I \cdot I_{R[\bar{X}]})$. They do not depend on the choice of the above covering $j : R[\bar{X}] \longrightarrow A^\flat$. Indeed, the first coincides with $I_{A^\flat}/I^2_{A^\flat}$ and the second with $\mathrm{Ker}\, i_{\mathcal{A}}$. Note also that both R-modules are free. (This is obvious for the first module and follows from the fact that A is a complete intersection for the second.)

If $\mathcal{A} = (A, A^\flat)$ and $\mathcal{B} = (B, B^\flat)$ are objects in DAug_R and $f : A \longrightarrow B$ is a morphism of augmented R-algebras, then the set of all $f^\flat$ such that $(f, f^\flat) \in \mathrm{Hom}_{\mathrm{DAug}_R}(\mathcal{A}, \mathcal{B})$ is not empty and has a natural structure of a principal homogeneous space over the group $\mathrm{Hom}_{R\text{-mod}}(t^*_{\mathcal{A}}, N_{\mathcal{B}})$.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

Let DAug_R^* be a quotient category for DAug_R: it has the same objects but its morphisms are equivalence classes of morphisms from $\mathrm{Hom}_{\mathrm{DAug}_R}(\mathcal{A},\mathcal{B})$ arising from the same R-algebra morphisms $f : A \longrightarrow B$. Then the above description of morphisms in the category DAug_R implies that the forgetful functor $(A, A^\flat) \mapsto A$ is an equivalence of DAug_R^* and the category of augmented finite R-algebras.

1.2 Deformations of affine group schemes

Let DSch_R be the dual category for DAug_R. Its objects appear in the form $\mathcal{H} = \mathrm{Spec}\,\mathcal{A} = (H, H^\flat, i_\mathcal{H})$, where $H = \mathrm{Spec}\,A$ and $H^\flat = \mathrm{Spec}\,A^\flat$ are finite flat pointed R-schemes, $\mathcal{A} = (A, A^\flat, i_\mathcal{A})$ $\in \mathrm{DAug}_R$, and $i_\mathcal{H} : H \to H^\flat$ is a closed embedding of pointed R-schemes induced by $i_\mathcal{A}$. We agree to use the simpler notation $(H, H^\flat)$ if there is no danger of misunderstanding. The category DSch_R has direct products: if for $i = 1, 2$, $\mathcal{A}_i = (A_i, A_i^\flat, i_{\mathcal{A}_i})$ with $A_i = R[\bar{X}_i]/I_i$, $A_i^\flat = R[\bar{X}_i]/(I_i \cdot I_{0i})$ (where $I_{0i} = I_{R[\bar{X}_i]}$), then the product $\mathrm{Spec}\,\mathcal{A}_1 \times \mathrm{Spec}\,\mathcal{A}_2$ is given by $\mathrm{Spec}(\mathcal{A}_1 \otimes \mathcal{A}_2)$, where $\mathcal{A}_1 \otimes \mathcal{A}_2 := (A_1 \otimes_R A_2, (A_1 \otimes_R A_2)^\flat, \kappa)$, $(A_1 \otimes_R A_2)^\flat$ is the quotient of $R[\bar{X}_1 \otimes 1, 1 \otimes \bar{X}_2]$ by the product of ideals $I_1 \otimes 1 + 1 \otimes I_2$ and $I_{01} \otimes 1 + 1 \otimes I_{02}$ and κ is the natural projection. Note that for $i = 1, 2$, the projections $\mathrm{pr}_i : \mathrm{Spec}(\mathcal{A}_1 \otimes \mathcal{A}_2) \longrightarrow \mathrm{Spec}\,\mathcal{A}_i$ come from the natural embeddings of $R[\bar{X}_i]$ into $R[\bar{X}_1 \otimes 1, 1 \otimes \bar{X}_2]$.

Let DGr_R be the category of group objects in DSch_R. If $\mathcal{G} = \mathrm{Spec}\,\mathcal{A} \in \mathrm{DGr}_R$, then its group structure is given via the comultiplication $\bar{\Delta} = (\Delta, \Delta^\flat) : \mathcal{A} \longrightarrow \mathcal{A} \otimes \mathcal{A}$, the counit $\bar{\varepsilon} = (\varepsilon, \varepsilon^\flat) : \mathcal{A} \longrightarrow \mathcal{R}$ and the coinversion $\bar{\imath} = (i, i^\flat) : \mathcal{A} \longrightarrow \mathcal{A}$ morphisms, which satisfy the usual axioms. The morphisms in DGr_R are morphisms of group objects. Clearly, DGr_R is an additive category.

Note that:

(a) $G = \mathrm{Spec}\,A$ is a finite flat group scheme over R with the comultiplication Δ, the counit ε and the coinversion i;

(b) $\bar{\varepsilon} = \varepsilon_\mathcal{A}$, where $\varepsilon_\mathcal{A}$ is the natural augmentation from § 1.1;

(c) the counit axiom gives for $i = 1, 2$, that $\Delta_i^\flat \circ \mathrm{pr}_i = \mathrm{id}_{A^\flat}$ and implies the uniqueness of $\Delta^\flat$ as a lifting of Δ;

(d) if $\mathcal{A} = (A, A^\flat, i_\mathcal{A}) \in \mathrm{DAug}_R$ and $G = \mathrm{Spec}\,A$ is a finite flat group scheme over R, then there is a unique structure of a group object on $\mathrm{Spec}\,\mathcal{A}$, which is compatible with that of G;

(e) if $f : G \longrightarrow H$ is a morphism of group schemes and $(f, f^\flat) \in \mathrm{Hom}_{\mathrm{DSch}_R}(\mathcal{G}, \mathcal{H})$, then $(f, f^\flat) \in \mathrm{Hom}_{\mathrm{DGr}_R}(\mathcal{G}, \mathcal{H})$.

The above properties have the following interpretation. Define the quotient category DGr_R^* as the category consisting of the objects of the category DGr_R but where $\mathrm{Hom}_{\mathrm{DGr}_R^*}(\mathcal{G}, \mathcal{H})$ consists of equivalence classes of morphisms from the category DGr_R which induce the same morphisms of group schemes $G \to H$. Then the forgetful functor $\mathcal{G} \mapsto G$ is an equivalence of categories.

1.3 The categories of strict O-modules

Suppose that $\mathcal{G}$ is an O-module object in the category DSch_R. Then $\mathcal{G}$ is an object of DGr_R and there is a map $O \longrightarrow \mathrm{End}_{\mathrm{DGr}_R}(\mathcal{G})$ satisfying the usual axioms from the definition of O-modules. For $o \in O$ and $\mathcal{G} = \mathrm{Spec}\,\mathcal{A}$, denote by $[\bar{o}] = ([o], [o]^\flat)$ the morphism of action of o on $\mathcal{A} = (A, A^\flat, i_\mathcal{A})$. Clearly, $G = \mathrm{Spec}\,A$ is an O-module in the category of finite flat schemes over R. For any such G, the O-module structure on the deformation $(G, G^\flat) \in \mathrm{DGr}_R$ is given by liftings $[o]^\flat : A^\flat \longrightarrow A^\flat$ of morphisms $[o] : A \longrightarrow A$, $o \in O$. Note that $[o]^\flat$ are morphisms of augmented algebras. All such liftings are automatically compatible with the group structure on this deformation, i.e. for any $o \in O$, one has $[o]^\flat \circ \Delta^\flat = \Delta^\flat \circ ([o]^\flat \otimes [o]^\flat)$. So, the above system of liftings $[o]^\flat$, $o \in O$, gives an O-module

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

structure if and only if for any $o_1, o_2 \in O$,

$$[o_1 + o_2]^\flat = \Delta^\flat \circ ([o_1] \otimes [o_2])^\flat, \quad [o_1 o_2]^\flat = [o_1]^\flat \circ [o_2]^\flat \tag{1}$$

where $([o_1] \otimes [o_2])^\flat$ is induced by $[o_1]^\flat \otimes [o_2]^\flat$.

Denote by $\mathrm{DGr}(O)_R$ the category of the above O-module objects where the corresponding O-module structure satisfies the following condition of strictness. If $\mathcal{G} = \operatorname{Spec} \mathcal{A}$ then any $o \in O$ acts on $t^*_{\mathcal{A}}$ and $N_{\mathcal{A}}$ via the scalar multiplication by o. This is the basic definition from the paper [Fal02].

Suppose that $\mathcal{G}_1 = (G, G_1^\flat) = \operatorname{Spec} \mathcal{A}_1 \in \mathrm{DGr}_R$ and $\mathcal{G}_2 = (G, G_2^\flat) = \operatorname{Spec} \mathcal{A}_2 \in \mathrm{DGr}_R$ are two deformations of a finite flat group scheme G over R. By § 1.2, $\mathcal{G}_1$ and $\mathcal{G}_2$ are isomorphic in the category DGr^*_R. Suppose that $\mathcal{G}_1$ is equipped with a strict O-action. Then there is a unique (strict) O-action on $\mathcal{G}_2$ such that any $(\mathrm{id}_G, \phi) \in \mathrm{Hom}_{\mathrm{DGr}_R}(\mathcal{G}_1, \mathcal{G}_2)$ and any $(\mathrm{id}_G, \psi) \in \mathrm{Hom}_{\mathrm{DGr}_R}(\mathcal{G}_2, \mathcal{G}_1)$ are, actually, morphisms in the category $\mathrm{DGr}(O)_R$. This is implied by the following observation. If ϕ is given by the morphism of R-algebras $\phi^* : A(G_2)^\flat \longrightarrow A(G_1)^\flat$, then it induces the identifications $A(G_2)^\flat = \operatorname{Im} \phi^* \oplus J_2$ and $A(G_1)^\flat = \operatorname{Im} \phi^* \oplus J_1$, where J_1, J_2 are ideals such that $J_1 \subset N_{\mathcal{A}_1}$ and $J_2 \subset N_{\mathcal{A}_2}$.

Denote by $\mathrm{DGr}^*(O)_R$ the quotient category of $\mathrm{DGr}(O)_R$ where the morphisms are the equivalence classes of morphisms $(G, G^\flat) \longrightarrow (H, H^\flat)$ in the category $\mathrm{DGr}(O)_R$, which induce the same morphism $G \longrightarrow H$. By the above property, all isomorphism classes of objects in $\mathrm{DGr}(O)_R$ appear as O-module finite flat schemes G together with a lifting of its O-action to some chosen deformation $G^\flat$, which satisfies the above conditions (1).

For example, if $q = p^n$ with $n \in \mathbb{N}$, the objects of the category $\mathrm{DGr}(\mathbb{F}_q)_R$ appear as $\operatorname{Spec} \mathcal{A}$, where $\mathcal{A} = (A, A^\flat)$, $A = R[\bar{X}]/I$ and $A^\flat = R[\bar{X}]/(I \cdot I_{R[\bar{X}]})$, the $\mathbb{F}_q$-action is induced by the scalar action of $\mathbb{F}_q$ on $\bar{X}$ (i.e. $[\alpha](\bar{X}) = \alpha \bar{X}$, $\alpha \in \mathbb{F}_q$) and there are generators $j_1, \dots, j_n$ of the ideal I such that $[\alpha] j_i = \alpha j_i$ for all $i = 1, \dots, n$ and $\alpha \in \mathbb{F}_q$.

If O is the ring of polynomials $\mathbb{F}_q[\pi]$ and $\mathcal{G} \in \mathrm{DGr}(O)_R$ then $\mathcal{G} \in \mathrm{DGr}(\mathbb{F}_q)_R$ and (in addition to the above assumptions) the $\mathbb{F}_q[\pi]$-action will be determined completely by the action of π given by the correspondence

$$\bar{X} \mapsto \psi_\pi(\bar{X}) = \pi \bar{X} + \bar{F}(\bar{X})$$

where $\bar{F}$ is any vector power series from $I^2_{R[\bar{X}]}$ such that $\bar{F}(\alpha \bar{X}) = \alpha \bar{F}(\bar{X})$ for all $\alpha \in \mathbb{F}_q$. This action is strict if and only if $\psi_\pi(j_i) \equiv \pi j_i \bmod (I \cdot I_{R[\bar{X}]})$ for the above generators $j_1, \dots, j_n$ of I.

Finally, note that when classifying below the objects $(G, G^\flat)$ of the categories $\mathrm{DGr}(\mathbb{F}_q)_R$ and $\mathrm{DGr}(\mathbb{F}_q[\pi])_R$ we use a choice of the deformation $G^\flat$ that depends functorially on G.

2. Group schemes with strict $\mathbb{F}_q$-action

In this section we assume that R is an $\mathbb{F}_p$-algebra and study the category $\mathrm{DGr}(\mathbb{F}_p)_R$ of strict finite $\mathbb{F}_p$-modules G over R. Clearly, $\mathrm{DGr}(\mathbb{Z})_R = \mathrm{DGr}_R$, i.e. the natural action of $\mathbb{Z}$ on elements of DGr_R is always strict. Therefore, $(G, G^\flat) \in \mathrm{DGr}(\mathbb{F}_p)_R$ if and only if $(G, G^\flat) \in \mathrm{DGr}_R$ and $[p]^\flat$ is a zero map on $G^\flat$. In §§ 2.1 and 2.2 we give a complete description of the category $\mathrm{DGr}(\mathbb{F}_p)_R$ and in § 2.3 apply it to describe the category $\mathrm{DGr}(\mathbb{F}_q)_R$, where $q = p^N$ with $N \in \mathbb{N}$.

2.1 An interpretation of strict $\mathbb{F}_p$-action

Suppose that G is a finite flat commutative group scheme over R. Consider $G^{(p)} = G \times_{(R, \sigma_p)} R$, where R is considered as an R-module via the map $\sigma_p : R \longrightarrow R$ such that for any $r \in R$, $\sigma_p(r) = r^p$. Then $G^{(p)}$ has a natural structure of a finite flat commutative group scheme over R.

Let $F_G : G \longrightarrow G^{(p)}$ be the relative Frobenius morphism of G over $\operatorname{Spec} R$. It is given by the morphism of R-algebras $F^*_G : A(G^{(p)}) = A(G) \otimes_{(R, \sigma_p)} R \longrightarrow A(G)$ such that for all $a \in A(G)$ and $r \in R$, $F^*_G(a \otimes r) = a^p r$.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

Let $V_G : G^{(p)} \longrightarrow G$ be the Verschiebung morphism of group schemes. Recall that it is given by the morphism of R-algebras $V_G^* : A(G) \longrightarrow A(G^{(p)})$, which can be described as follows. We can proceed locally on $\operatorname{Spec} R$ and, therefore, can assume that $A(G)$ is a free R-module with a basis $a_1, \dots, a_n$. Let

$$\Delta^{(p)} = \Delta \circ (\Delta \otimes \mathrm{id}) \circ \dots \circ (\Delta \otimes \mathrm{id}^{\otimes p-2}) : A(G) \longrightarrow A(G)^{\otimes p}.$$

For $1 \leqslant i \leqslant n$, we have a unique decomposition

$$\Delta^{(p)}(a_i) = \sum_{1 \leqslant i_1, \dots, i_p \leqslant n} \alpha_{i,i_1,\dots,i_p} a_{i_1} \otimes \dots \otimes a_{i_p}$$

with all α-coefficients from R. Then the Verschiebung is defined by the relation

$$V_G^*(a_i) = \sum_{1 \leqslant j \leqslant n} \alpha_{i,j,\dots,j} \otimes a_j.$$

The above definitions imply easily that $F_G \circ V_G = p\,\mathrm{id}_G$ and $V_G \circ F_G = p\,\mathrm{id}_{G^{(p)}}$, cf. our agreement about composition of maps from § 0.

Theorem 1. *We have $\mathcal{G} = (G, G^\flat) \in \mathrm{DGr}(\mathbb{F}_p)_R$ if and only if $V_G = 0$.*

Proof. Both properties can be verified locally on $\operatorname{Spec} R$. Therefore, we can assume that R is a local ring. As we have already noticed, $\mathcal{G} \in \mathrm{DGr}(\mathbb{F}_p)_R$ if and only if $[p]^\flat$ is a zero morphism.

2.1.1 Suppose first that $V_G = 0$. Use the antiequivalence L_p of the category of finite flat commutative group schemes G over R with zero Verschiebung and the category $\mathrm{Mod}(\mathbb{F}_p)_R$ of locally free finite R-modules L equipped with an R-linear map $F_p : L^{(p)} := L \otimes_{R,\sigma_p} R \longrightarrow L$, cf. [Gab70, VII$_\mathrm{A}$, 7.4]. Here $\mathrm{L}_p(G) = (L, F_p)$, where

$$L = \mathrm{Hom}(G, \mathbb{G}_a) = \{a \in A(G) \mid \Delta(a) = a \otimes 1 + 1 \otimes a\}$$

is a free R-module of finite R-rank and F_p is induced by the Frobenius F_G^*.

The inverse functor D_p can be described as follows. If $\mathcal{L} = (L, F_p) \in \mathrm{Mod}(\mathbb{F}_p)_R$ and $m_1, \dots, m_n$ is an R-basis for L then for $1 \leqslant i \leqslant n$,

$$F_p(m_i \otimes 1) = \sum_{1 \leqslant j \leqslant n} r_{ij} m_j.$$

Then $\mathrm{D}_p(\mathcal{L}) = \operatorname{Spec} A(G)$, where $A(G) = R[X_1, \dots, X_n]/I$ with the ideal I generated by the polynomials

$$X_i^p - \sum_{1 \leqslant j \leqslant n} r_{ij} X_j, \quad 1 \leqslant i \leqslant n, \tag{2}$$

with the group structure given via the comultiplication Δ such that $\Delta(X_i) = X_i \otimes 1 + 1 \otimes X_i$ and the counit e such that $e(X_i) = 0$ for $1 \leqslant i \leqslant n$. Note that $A(G)$ is a finite flat R-algebra, given by n equations (2) in $R[X_1, \dots, X_n]$ and, therefore, it is a relative complete intersection.

With the above notation take $G^\flat = \operatorname{Spec} A(G)^\flat$, where $A(G)^\flat = R[X_1, \dots, X_n]/(I \cdot I_0)$ with $I_0 = (X_1, \dots, X_n)$. Note that the R-module $A(G)^\flat$ is free with the basis

$$\{X_1^{i_1} \dots X_n^{i_n} \mid 0 \leqslant i_1, \dots, i_n < p\} \cup \{X_i^p \mid 1 \leqslant i \leqslant n\}.$$

Similarly, $A(G \times G)^\flat$ is a free R-module with the basis

$$\{X_1^{i_1} \dots X_n^{i_n} \otimes X_1^{j_1} \dots X_n^{j_n} \mid 0 \leqslant i_1, \dots, i_n, j_1, \dots, j_n < p\} \cup \{X_i^p \otimes 1, 1 \otimes X_i^p \mid 1 \leqslant i \leqslant n\}.$$

With this notation we have $e^\flat(X_i) = 0$ and

$$\Delta^\flat(X_i) = X_i \otimes 1 + 1 \otimes X_i + \sum_{1 \leqslant j \leqslant n} (r'_{ij} X_j^p \otimes 1 + r''_{ij} 1 \otimes X_j^p)$$

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

with r-coefficients from R. Then the identities

$$\Delta^\flat \circ (\mathrm{id}_{A(G)} \otimes e)^\flat = \Delta^\flat \circ (e \otimes \mathrm{id}_{A(G)})^\flat = \mathrm{id}_{A(G)^\flat}$$

imply that all r-coefficients are equal to 0. This easily implies that

$$[p]^\flat = \Delta^{(p)\flat} \circ \mathrm{mult}_p^\flat = 0,$$

where $\mathrm{mult}_p^\flat : A(G)^{\otimes p\flat} \longrightarrow A(G)^\flat$ is induced by the multiplication in $A(G)^\flat$.

2.1.2 Suppose now that $\mathcal{G} = (G, G^\flat) \in \mathrm{DGr}(\mathbb{F}_p)_R$. When proving that this implies $V_G = 0$ we can use any flat base changes. Therefore, we can assume that R is a finitely generated complete local ring with an algebraically closed residue field k of characteristic p. Then R is an inverse limit of artinian rings and by transfinite induction it will be sufficient to consider the following two cases:

(a) $R = k$;

(b) R contains an ideal J such that $J \cdot I_R = 0$ (where I_R is the augmentation ideal in R) and if $\bar{R} = R/J$ and $\bar{G} = G \otimes_R \bar{R}$, then $V_{\bar{G}} = 0$.

2.1.3 *Case* (a). Apply induction on the order $|G| = p^N$, $N \in \mathbb{N}$. If $N = 1$, then there are the following three possibilities:

- $G \simeq (\mathbb{Z}/p\mathbb{Z})_{/k}$, i.e. it is the constant etale group scheme of order p;
- $G \simeq \alpha_p$, i.e. $A(G) = k[x]$, $x^p = 0$, $\Delta(x) = x \otimes 1 + 1 \otimes x$;
- $G \simeq \mu_p$, i.e. it is the constant multiplicative group scheme of order p.

In the first two cases $V_G = 0$. In the third case $V_G = \mathrm{id}_G$, but $[p]^\flat \neq 0$. Indeed, $A(\mu_p)^\flat = k[x]/(x^{p+1})$, $e^\flat(x) = 0$, $\Delta^\flat(1+x) = (1+x)\otimes(1+x)$ and $[p]^\flat(1+x) = (1+x)^p = 1+x^p \neq 1 = e^\flat(1+x)$ in $A(\mu_p)^\flat$.

Now assume that $N > 1$ and $V_{G_1} = 0$ for any proper subquotient of G. Consider the Dieudonne module $M(G) = \mathrm{Hom}(G, CW_k)$ of G, where CW_k is the k-valued Witt covectors functor, cf. [Fon75]. Then $M(G)$ is a k-vector space of dimension N with a σ_p-linear operator F and a σ_p^{-1}-linear operator V, which are induced by F_G and V_G, respectively. The inductive assumption implies the existence of a k-basis $m_1, \ldots, m_N$ in $M(G)$ such that for $1 \leqslant i \leqslant N$, $Fm_i = \sum_{1 \leqslant i \leqslant N} c_{ij} m_j$, $Vm_1 = \cdots = Vm_{N-1} = 0$ and $Vm_N = c_0 m_1$ where all c-coefficients belong to k. By the Dieudonne theory,

$$A(G) = k[X_1, \ldots, X_N]/I,$$

where the ideal I is generated by the polynomials $X_i^p - \sum c_{ij} X_j$, $1 \leqslant i \leqslant N$, with the counit $e : A(G) \longrightarrow k$ such that $e(X_i) = 0$, $1 \leqslant i \leqslant N$, and the comultiplication $\Delta : A(G) \longrightarrow A(G) \otimes A(G)$ such that for $1 \leqslant i < N$, $\Delta(X_i) = X_i \otimes 1 + 1 \otimes X_i$ and

$$\Delta(X_N) = X_N \otimes 1 + 1 \otimes X_N + c_0 \varphi(X_1 \otimes 1, 1 \otimes X_1).$$

Here $\varphi(T, U) \in k[T, U]$ is the polynomial $\frac{1}{p}(T^p + U^p - (T+U)^p) \in \mathbb{Z}[T, U]$ taken modulo p.

As earlier, take $A(G)^\flat = k[X_1, \ldots, X_N]/(I \cdot I_0)$ with $I_0 = (X_1, \ldots, X_N)$. Consider the k-basis

$$\{X_1^{i_1} \ldots X_N^{i_N} \mid 0 \leqslant i_1, \ldots, i_N < p\} \cup \{X_i^p \mid 1 \leqslant i \leqslant N\}$$

in $A(G)^\flat$ and the k-basis

$$\{X_1^{i_1} \ldots X_N^{i_N} \otimes X_1^{j_1} \ldots X_N^{j_N} \mid 0 \leqslant i_s, j_s < p, 1 \leqslant s \leqslant N\} \cup \{X_i^p \otimes 1, 1 \otimes X_i^p \mid 1 \leqslant i \leqslant N\}$$

in $A(G \times G)^\flat$. Similarly to § 2.1.1 one sees that

$$\Delta^\flat(X_N) = X_N \otimes 1 + 1 \otimes X_N + c_0 \varphi(X_1 \otimes 1, 1 \otimes X_1)$$

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

and $\Delta^\flat(X_1) = X_1 \otimes 1 + 1 \otimes X_1$. This implies easily that

$$\Delta^{(p)\flat}(X_N) = X_N \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes X_N \otimes 1 \otimes \cdots \otimes 1 + \cdots + 1 \otimes \cdots \otimes 1 \otimes X_N + c_0\varphi^{(p)}(X_1 \otimes 1 \otimes \cdots \otimes 1, 1 \otimes X_1 \otimes 1 \otimes \cdots \otimes 1, \ldots, 1 \otimes \cdots \otimes 1 \otimes X_1),$$

where $\varphi^{(p)}(U_1, \ldots, U_p) \in k[U_1, \ldots, U_p]$ is the reduction of the polynomial

$$\frac{1}{p}(U_1^p + \cdots + U_p^p - (U_1 + \cdots + U_p)^p) \in \mathbb{Z}[U_1, \ldots, U_p]$$

modulo p. Therefore, $0 = [p]^\flat(X_N) = (\Delta^{(p)} \circ \mathrm{mult}_p)^\flat(X_N) = c_0 X_1^p$, hence $c_0 = 0$ and $V_G = 0$. Case (a) is completely considered.

Remark. Case (a) was also considered in [Gib04].

2.1.4 *Case* (b). Since $V_{\bar{G}} = 0$, we can again apply the antiequivalence from [Gab70], to describe explicitly the structure of $\bar{G}$. It can be given by the algebra $A(\bar{G}) = \bar{R}[\bar{X}_1, \ldots, \bar{X}_N]/\bar{I}$, where $\bar{I}$ is generated by the polynomials

$$\bar{X}_i^p - \sum_{1 \leqslant j \leqslant N} \bar{c}_{ij}\bar{X}_j \in \bar{R}[\bar{X}_1, \ldots, \bar{X}_N]$$

with the comultiplication $\Delta(\bar{X}_i) = \bar{X}_i \otimes 1 + 1 \otimes \bar{X}_i$, $1 \leqslant i \leqslant N$.

Let $l_1, \ldots, l_s$ be a k-basis of the ideal J with respect to its natural structure as a k $(= R/I_R)$-module. As $A(G)$ is a flat R-module we can take liftings $X_i \in A(G)$ of $\bar{X}_i$ and $c_{ij} \in R$ of $\bar{c}_{ij} \in \bar{R}$ such that $A(G) = R[X_1, \ldots, X_N]/I$, where I is generated by the polynomials of the form

$$X_i^p - \sum_{1 \leqslant j \leqslant N} c_{ij}X_j - \sum_{1 \leqslant t \leqslant s} f_{it}l_t, \quad 1 \leqslant i \leqslant N,$$

with $f_{it} \in A(G) \otimes J \simeq A(G_k)$ and $G_k = G \otimes k$.

Similarly,

$$\Delta(X_i) = X_i \otimes 1 + 1 \otimes X_i + \sum_{1 \leqslant t \leqslant s} g_{it}l_t, \quad 1 \leqslant i \leqslant N, \tag{3}$$

where all $g_{it} \in A(G_k \times G_k)$.

Consider the second Hochschild cohomology group $H^2(G, k)$. Recall that it appears as the quotient $Z^2(G, k)/B^2(G, k)$, where

$$Z^2(G, k) = \{f \in A(G_k \times G_k) \mid (\Delta \otimes \mathrm{id})(f) + f \otimes 1 = 1 \otimes f + (\mathrm{id} \otimes \Delta)(f)\},$$

$$B^2(G, k) = \{\Delta(h) - h \otimes 1 - 1 \otimes h \mid h \in A(G_k)\}.$$

As $V_{G_k} = 0$, $H^2(G, k)$ is an N-dimensional k-vector space with the basis given by the classes of 2-cocycles $\varphi(X_i \otimes 1, 1 \otimes X_i)$, $1 \leqslant i \leqslant N$, cf. [DG70]. This implies that the liftings $X_i \in A(G)$ of $\bar{X}_i \in A(\bar{G})$ can be chosen such that in the equalities (3) for $1 \leqslant i \leqslant N$ and $1 \leqslant t \leqslant s$,

$$g_{it} = \sum_{1 \leqslant j \leqslant N} \alpha_{ijt}\varphi(X_j \otimes 1, 1 \otimes X_j),$$

where all α-coefficients belong to k.

As earlier, this implies that

$$\Delta^{(p)}(X_i) = X_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes X_i \otimes 1 \otimes \cdots \otimes 1 + \cdots + 1 \otimes \cdots \otimes 1 \otimes X_i + \sum_{j,t} \alpha_{ijt}l_t\varphi^{(p)}(X_j \otimes 1 \otimes \cdots \otimes 1, 1 \otimes X_j \otimes 1 \otimes \cdots \otimes 1, \ldots, 1 \otimes \cdots \otimes 1 \otimes X_j)$$

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

and, therefore, for all $1 \leqslant i \leqslant N$,

$$V_G(X_i) = \sum_{j,t} \alpha_{ijt} l_t X_j.$$

On the other hand, we have (as earlier)

$$\Delta^\flat(X_i) = X_i \otimes 1 + 1 \otimes X_i + \sum_{j,t} \alpha_{ijt} l_t \varphi(X_j \otimes 1, 1 \otimes X_j)$$

in $A(G)^\flat = R[X_1, \ldots, X_N]/(I \cdot I_0)$ and this implies that

$$0 = [p]^\flat(X_i) = \sum_{j,t} \alpha_{ijt} l_t X_j^p.$$

Therefore, all α-coefficients are equal to 0 and $V_G = 0$.

The theorem is completely proved. □

The above Theorem 1 together with the antiequivalence L_p from the beginning of § 2.1.1 means that the forgetful functor $\mathcal{G} = (G, G^\flat) \mapsto G$ is an equivalence of the category of group schemes over R with strict $\mathbb{F}_p$-action $\mathrm{DGr}(\mathbb{F}_p)_R$ and the full subcategory of the category of finite flat group schemes G over R such that $V_G = 0$. The resulting antiequivalence of the categories $\mathrm{DGr}(\mathbb{F}_p)_R$ and $\mathrm{Mod}(\mathbb{F}_p)_R$ will be denoted by the same symbol L_p.

2.2 Standard deformations of strict $\mathbb{F}_p$-modules

By Theorem 1 the objects $\mathcal{G} \in \mathrm{DGr}(\mathbb{F}_p)_R$ are constructed from locally free R-modules L of finite R-rank with a given R-linear map $F_p : L^{(p)} \longrightarrow L$. This construction gives $\mathcal{G} = \operatorname{Spec} \mathcal{A}$ with $\mathcal{A} = (A(L), A(L)^\flat, i_{\mathcal{A}})$, where $A(L) = \mathrm{Sym}_R(L)/I$, $A(L)^\flat = \mathrm{Sym}_R(L)/(I \cdot I_0)$, the ideal I is generated by $\{l^p - F_p(l \otimes 1) \mid l \in L\}$, I_0 is the augmentation ideal generated by $\{l \mid l \in L\}$ and the comultiplications Δ and $\Delta^\flat$ are induced by the correspondences $l \mapsto l \otimes 1 + 1 \otimes l$. This deformation $\mathcal{G}$ depends functorially on the group scheme $G = \operatorname{Spec} A(L)$. Note that $L = \{a \in A(L) \mid \Delta(a) = a \otimes 1 + 1 \otimes a\}$.

Definition. With the above notation, set $L^\flat = \{l \in A(L)^\flat \mid \Delta^\flat(l) = l \otimes 1 + 1 \otimes l\}$.

Such $L^\flat$ is a locally free R-module of rank $2 \operatorname{rk}_R L$. In the notation of § 2.1.1 it is generated as an R-module by the elements $X_1, \ldots, X_n, X_1^p, \ldots, X_n^p$ in the algebra $A(L)^\flat$. Clearly, we have a natural projection $i_{\mathcal{A}} : L^\flat \longrightarrow L$. There is also a natural inclusion

$$N_{\mathcal{A}} = \{l^p - F_p(l \otimes 1) \mid l \in L\} \bmod (I \cdot I_0) \subset L^\flat,$$

the natural projection $\mathrm{pr} : L^\flat \longrightarrow t_{\mathcal{A}}^*$ given by the correspondence $l \mapsto l \bmod I_0^2$, where $l \in L$, and the R-linear map $j_{\mathcal{A}} : L^{(p)} \longrightarrow L^\flat$ induced by the correspondence $l \mapsto \hat{l}^p$, where $\hat{l} \in L^\flat$ is such that $i_{\mathcal{A}}(\hat{l}) = l$.

The following lemma is an easy consequence of the above definitions.

Lemma. *There are exact sequences of locally free R-modules*

$$0 \longrightarrow N_{\mathcal{A}} \longrightarrow L^\flat \xrightarrow{i_{\mathcal{A}}} L \longrightarrow 0 \tag{4}$$

and

$$0 \longrightarrow L^{(p)} \xrightarrow{j_{\mathcal{A}}} L^\flat \longrightarrow t_{\mathcal{A}}^* \longrightarrow 0. \tag{5}$$

2.3 Group schemes with strict $\mathbb{F}_q$-action

Assume now that R is an $\mathbb{F}_q$-algebra, where $q = p^N$ and $N \in \mathbb{N}$, and study the category $\mathrm{DGr}(\mathbb{F}_q)_R$ of strict finite $\mathbb{F}_q$-modules G over R as a full subcategory of $\mathrm{DGr}(\mathbb{F}_p)_R$.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

For any R-module M set $M^{(q)} = M \otimes_{(R,\sigma_q)} R$, where the R-module structure on the second component of this tensor product is given via the qth power map $\sigma_q : R \longrightarrow R$. If $f : M \longrightarrow N$ is a morphism of R-modules, then we use the notation $f^{(q)} = f \otimes_{(R,\sigma_q)} R : M^{(q)} \longrightarrow N^{(q)}$.

Consider the category $\mathrm{Mod}(\mathbb{F}_q)_R$ consisting of locally free finite rank R-modules M with an R-linear morphism $F_q : M^{(q)} \longrightarrow M$. If N is another object, then $\mathrm{Hom}_{\mathrm{Mod}(\mathbb{F}_q)_R}(M, N)$ consists of R-linear morphisms $f : M \longrightarrow N$ such that $F_q \circ f = f^{(q)} \circ F_q$.

Define the functor $\mathrm{L}_q : \mathrm{DGr}(\mathbb{F}_q)_R \longrightarrow \mathrm{Mod}(\mathbb{F}_q)_R$ by setting for any $\mathcal{G} = (G, G^\flat) \in \mathrm{DGr}(\mathbb{F}_q)_R$, $\mathrm{L}_q(\mathcal{G}) = (L(\mathcal{G}), F_q)$ with

$$L(\mathcal{G}) = \{a \in A(G) \mid \Delta(a) = a \otimes 1 + 1 \otimes a,\ [\alpha](a) = \alpha a,\ \forall \alpha \in \mathbb{F}_q\},$$

where $F_q : L(\mathcal{G})^{(q)} \longrightarrow L(\mathcal{G})$ is induced by the qth power map on $A(G)$. If $\mathcal{H} \in \mathrm{DGr}(\mathbb{F}_q)_R$, $\mathrm{L}_q(\mathcal{H}) = (L(\mathcal{H}), F_q)$ and $(f, f^\flat) : \mathcal{G} \longrightarrow \mathcal{H}$ is a morphism in the category $\mathrm{DGr}(\mathbb{F}_q)_R$, then $f(L(\mathcal{H})) \subset L(\mathcal{G})$ and $\mathrm{L}_q(f) = f|_{L(\mathcal{H})}$.

Theorem 2. *The above defined functor* $\mathrm{L}_q : \mathrm{DGr}(\mathbb{F}_q)_R \longrightarrow \mathrm{Mod}(\mathbb{F}_q)_R$ *induces an antiequivalence of the categories* $\mathrm{DGr}^*(\mathbb{F}_q)_R$ *and* $\mathrm{Mod}(\mathbb{F}_q)_R$.

Proof. The proof below is standard: cf., for example, [Ray74] (in the context of finite flat group schemes with $\mathbb{F}_q$-action) or [Gen96] (in the context of formal modules).

2.3.1 We first construct the functor $\mathrm{D}_q : \mathrm{Mod}(\mathbb{F}_q)_R \longrightarrow \mathrm{DGr}^*(\mathbb{F}_q)_R$ in a similar manner to the construction from § 2.1.1.

If $(L, F_q) \in \mathrm{Mod}(\mathbb{F}_q)_R$, then $\mathrm{D}_q(L, F_q) = \mathrm{Spec}\,\mathcal{A}$ with $\mathcal{A} = (A(G), A(G)^\flat, i_\mathcal{A})$, defined by:

- $A(G) = \mathrm{Sym}_R(L)/I$ where the ideal I is generated by $\{l^q - F_q(l \otimes 1) \mid l \in L\}$, the comultiplication Δ is such that $\Delta(l) = l \otimes 1 + 1 \otimes l$ and the $\mathbb{F}_q$-action is such that $[\alpha](l) = \alpha l$ for all $l \in L$ and $\alpha \in \mathbb{F}_q$;
- $A(G)^\flat = \mathrm{Sym}_R(L)/(I \cdot I_0)$ where the augmentation ideal I_0 is generated by all $l \in L$, the comultiplication $\Delta^\flat$ is such that $\Delta^\flat(l) = l \otimes 1 + 1 \otimes l$ and the $\mathbb{F}_q$-action $[\alpha]^\flat$ is given by the correspondences $l \mapsto l \otimes 1 + 1 \otimes l$ and $l \mapsto \alpha l$ for all $l \in L$ and $\alpha \in \mathbb{F}_q$;
- $i_\mathcal{A}$ is the natural projection from $A(G)^\flat$ to $A(G)$.

Clearly, $\mathcal{G} = \mathrm{Spec}\,\mathcal{A} \in \mathrm{DGr}(\mathbb{F}_q)_R$ and the correspondence $\mathrm{D}_q : (L, F_q) \mapsto \mathcal{G}$ can be naturally extended to the functor $\mathrm{D}_q : \mathrm{Mod}(\mathbb{F}_q)_R \longrightarrow \mathrm{DGr}(\mathbb{F}_q)_R$. This functor is additive and faithful.

2.3.2 We now prove that any $\mathcal{G} \in \mathrm{DGr}(\mathbb{F}_q)_R$ can be identified in the category $\mathrm{DGr}^*(\mathbb{F}_q)_R$ with some $\mathrm{D}_q(L_0, F_q)$, where $(L_0, F_q) \in \mathrm{Mod}(\mathbb{F}_q)_R$. Since $\mathcal{G} \in \mathrm{DGr}(\mathbb{F}_p)_R$ we can assume that it is presented by the deformation $\mathrm{Spec}(A, A^\flat)$ where the R-algebras A and $A^\flat$ are described in terms of the R-module L such that $(L, F_p) = \mathrm{L}_p(\mathcal{G})$, cf. § 2.2.

For all $\alpha \in \mathbb{F}_q$, there are the R-linear actions $[\alpha] : L \longrightarrow L$ and $[\alpha]^\flat : L^\flat \longrightarrow L^\flat$. Therefore, we have the direct sum decompositions of locally free modules $L = \bigoplus_{n \in \mathbb{Z}/N\mathbb{Z}} L_n$ and $L^\flat = \bigoplus_{n \in \mathbb{Z}/N\mathbb{Z}} L_n^\flat$, where for all $n \in \mathbb{Z} \bmod N$,

$$L_n = \{l \in L \mid [\alpha](l) = \sigma_p^n(\alpha) l, \forall \alpha \in \mathbb{F}_q\}, \quad L_n^\flat = \{l \in L^\flat \mid [\alpha](l) = \sigma_p^n(\alpha) l, \forall \alpha \in \mathbb{F}_q\}.$$

The exact sequence (4) from the lemma in § 2.2 implies that $i_\mathcal{A}$ induces isomorphisms of R-modules $i_n : L_n^\flat \longrightarrow L_n$ for all $n \in \mathbb{Z}/N\mathbb{Z}$, $n \neq 0$. Similarly, exact sequence (5) from the same lemma implies that $j_\mathcal{A}$ induces isomorphisms of R-modules $j_n : L_{n-1} \longrightarrow L_n^\flat$ for all $n \in \mathbb{Z}/N\mathbb{Z}$, $n \neq 0$. Then from the relation $j_\mathcal{A} \circ i_\mathcal{A} = F_p$ it follows that for all $n = 0, \ldots, N-2$, F_p induces isomorphisms $L_n \simeq L_{n+1}$ and, therefore, $L = \bigoplus_{n \in \mathbb{Z} \bmod N} F_p^n(L_0)$.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

Let $\kappa : \mathrm{Sym}_R(L) \longrightarrow \mathrm{Sym}_R(L_0)$ be an R-algebra morphism uniquely determined by the correspondences $\kappa : F_p^n(l_0) \mapsto l_0^{p^n}$ for all $0 \leqslant n < N$ and $l_0 \in L_0$. Then a straightforward calculation shows that κ induces an isomorphism of $\mathcal{G}$ and $\mathrm{D}_q(L_0, F_q)$ in the category $\mathrm{DGr}^*(\mathbb{F}_q)_R$. The theorem is proved. □

3. Group schemes with strict $\mathbb{F}_q[\pi]$-action

Suppose that $O = \mathbb{F}_q[\pi]$ with a fixed indeterminate π and $\mathcal{G} = \operatorname{Spec} \mathcal{A}(\mathcal{G}) \in \mathrm{DGr}(O)_R$.

3.1 The R-module $L(\mathcal{G})^\flat$

Consider $\mathcal{G}$ as an object of the category $\mathrm{DGr}(\mathbb{F}_q)_R$. Then there is a $(L, F_q) \in \mathrm{Mod}(\mathbb{F}_q)_R$ such that $\mathcal{G}$ is isomorphic to $\operatorname{Spec} \mathcal{A}$, where $\mathcal{A} = (A(G), A(G)^\flat, i_{\mathcal{A}})$ is given in the notation of § 2.3.1.

Note that $L = L(\mathcal{G}) = \{a \in A(G) \mid \Delta(a) = a \otimes 1 + 1 \otimes a,\ [\alpha](a) = \alpha a,\ \forall \alpha \in \mathbb{F}_q\}$. Similarly to § 2.2 introduce

$$L^\flat = L(\mathcal{G})^\flat = \{a \in A(G)^\flat \mid \Delta^\flat(a) = a \otimes 1 + 1 \otimes a,\ [\alpha](a) = \alpha a,\ \forall \alpha \in \mathbb{F}_q\}.$$

Then $L^\flat$ is a locally free R-module, $\mathrm{rk}_R L^\flat = 2 \mathrm{rk}_R L$, it is generated by the images of elements $\{l, l^q \mid l \in L\}$ in $A(G)^\flat$ and therefore can be identified with $L \oplus L^{(q)}$.

The action $[\pi]_{\mathcal{G}} = ([\pi], [\pi]^\flat)$ of $\pi \in O$ on $\mathcal{G}$ is uniquely determined by R-linear endomorphisms $[\pi] : L \longrightarrow L$ and $[\pi]^\flat : L^\flat \longrightarrow L^\flat$ such that $[\pi]^\flat \circ i_L = i_L \circ [\pi]$, where $i_L = i_{\mathcal{A}}|_{L^\flat} : L^\flat \longrightarrow L$ is an epimorphism of R-modules.

Note that $N_{\mathcal{A}} = I \bmod (I \cdot I_0) \subset L^\flat$. With respect to the above-mentioned identification $L^\flat = L \oplus L^{(q)}$, we have $i_L(l_1, l_2) = l_1 + F_q(l_2)$, $N_{\mathcal{A}} = \{(F_q(l), -l) \mid l \in L^{(q)}\}$ and the natural sequence

$$0 \longrightarrow N_{\mathcal{A}} \longrightarrow L^\flat \xrightarrow{i_L} L \longrightarrow 0 \tag{6}$$

is an exact sequence of O-R-modules.

Consider the R-linear morphism $j_L : L^{(q)} \longrightarrow L^\flat$ given by the correspondence $l \otimes 1 \mapsto \hat{l}^q$, where $l \in L$ and $\hat{l} \in L^\flat$ is such that $i_L(\hat{l}) = l$. Clearly, $j_L \circ i_L = F_q$ and the sequence

$$0 \longrightarrow L^{(q)} \xrightarrow{j_L} L^\flat \xrightarrow{\mathrm{pr}_1} t^*_{\mathcal{A}} \longrightarrow 0 \tag{7}$$

is an exact sequence of O-R-modules. (Here pr_1 is induced by the natural projection $I_{A(G)^\flat} \longrightarrow t^*_{\mathcal{A}}$.) Note that with respect to the identification $L^\flat = L \oplus L^{(q)}$, $j_L : l_2 \mapsto (0, l_2)$ and $\mathrm{pr}_1 : (l_1, l_2) \mapsto l_1$ for any $l_1 \in L$ and $l_2 \in L^{(q)}$.

3.2 The morphism $V_\pi(\mathcal{G})$

With the notation from § 3.1 consider the map $\psi_\pi := [\pi]^\flat - \pi \,\mathrm{id}_{L^\flat} : L^\flat \longrightarrow L^\flat$. As the action of π on $\mathcal{G}$ is strict, ψ_π induces the zero morphisms on $N_{\mathcal{A}}$ and $t^*_{\mathcal{A}}$. From the exact sequences (6) and (7) it follows then that there is a unique R-linear morphism $V_\pi = V_\pi(\mathcal{G}) : L \longrightarrow L^{(q)}$ such that $\psi_\pi = i_L \circ V_\pi \circ j_L$.

LEMMA. *We have the following:*

(a) $V_\pi \circ F_q = [\pi] - \pi \,\mathrm{id}_L$;

(b) $F_q \circ V_\pi = [\pi]^{(q)} - \pi \,\mathrm{id}_{L^{(q)}}$.

Proof. (a) The relation $j_L \circ i_L = F_q$ implies that

$$i_L \circ ([\pi] - \pi \,\mathrm{id}_L) = ([\pi]^\flat - \pi \,\mathrm{id}_{L^\flat}) \circ i_L = i_L \circ V_\pi \circ j_L \circ i_L = i_L \circ (V_\pi \circ F_q).$$

Since i_L is an epimorphism, we can cancel it from this equality to give the result.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

(b) Take $l \in L$, $\hat{l} \in L^\flat$ such that $i_L(\hat{l}) = l$ and compute in $A(G)^\flat$:

$$j_L(V_\pi(l^q)) = ([\pi]^\flat - \pi \mathrm{id}_{L^\flat})(\hat{l}^q) = ([\pi]^\flat(\hat{l}))^q - \pi \hat{l}^q = j_L([\pi](l) \otimes 1 - l \otimes \pi).$$

Since j_L is a monomorphism we can cancel both sides by j_L and obtain for any $l \in L$, that

$$(F_q \circ V_\pi)(l \otimes 1) = [\pi]^{(q)}(l \otimes 1) - \pi \mathrm{id}_{L^{(q)}}(l \otimes 1).$$

The lemma is proved. □

Remark. (a) For any $\mathcal{G} \in \mathrm{DGr}(O)_R$, F_q induces the morphism $F_{\mathcal{G}} \in \mathrm{Hom}_{\mathrm{DGr}(O)_R}(\mathcal{G}, \mathcal{G}^{(q)})$; this follows from the identity $F_q \circ [\pi] = [\pi]^{(q)} \circ F_q$.

(b) If $\pi \cdot 1_R = 0$, then V_π induces the morphism $V_{\mathcal{G}} \in \mathrm{Hom}_{\mathrm{DGr}(O)_R}(\mathcal{G}^{(q)}, \mathcal{G})$ and we have $F_{\mathcal{G}} \circ V_{\mathcal{G}} = \pi \,\mathrm{id}_{\mathcal{G}}$ and $V_{\mathcal{G}} \circ F_{\mathcal{G}} = \pi \,\mathrm{id}_{\mathcal{G}^{(q)}}$.

3.3 The functor $\mathrm{L}_{q,\pi} : \mathrm{DGr}(O)_R \longrightarrow \mathrm{Mod}(O)_R$

The category $\mathrm{Mod}(O)_R$ consists of triples (L, F_q, V_π), where:

- $(L, F_q) \in \mathrm{Mod}(\mathbb{F}_q)_R$, i.e. L is a locally free R-module of finite R-rank with an R-linear morphism $F_q : L^{(q)} \longrightarrow L$;
- $V_\pi : L \longrightarrow L^{(q)}$ is an R-linear morphism such that $(V_\pi \circ F_q + \pi \,\mathrm{id}_L)^{(q)} = F_q \circ V_\pi + \pi \,\mathrm{id}_{L^{(q)}}$;
- morphisms $f : (L, F_q, V_\pi) \longrightarrow (L_1, F_q, V_\pi)$ in $\mathrm{Mod}(O)_R$ are given by R-linear morphisms $f : L \longrightarrow L_1$ such that $F_q \circ f = f^{(q)} \circ F_q$ and $V_\pi \circ f^{(q)} = f \circ V_\pi$.

Define the contravariant functor $\mathrm{L}_{q,\pi}$ from $\mathrm{DGr}(O)_R$ to $\mathrm{Mod}(O)_R$ by setting (where L_q is the functor from § 2.3):

- $\mathrm{L}_{q,\pi}(\mathcal{G}) = (L(\mathcal{G}), F_q, V_\pi(\mathcal{G}))$, where $(L(\mathcal{G}), F_q) = \mathrm{L}_q(\mathcal{G})$;
- if $\mathcal{H} = (H, H^\flat, i_{\mathcal{H}}) \in \mathrm{DGr}(O)_R$ and $f \in \mathrm{Hom}_{\mathrm{DGr}(O)_R}(\mathcal{G}, \mathcal{H})$, then $\mathrm{L}_{q,\pi}(f) = \mathrm{L}_q(f) : L(\mathcal{H}) \longrightarrow L(\mathcal{G})$ is an R-linear map induced by the corresponding map of R-algebras $A(H) \longrightarrow A(G)$.

Theorem 3. *The functor* $\mathrm{L}_{q,\pi}$ *induces an antiequivalence of categories* $\mathrm{L}^*_{q,\pi} : \mathrm{DGr}^*(O)_R \longrightarrow \mathrm{Mod}(O)_R$.

Remark. The case of a perfect field R of characteristic p was considered in [Gib04].

Proof. Clearly, $\mathrm{L}_{q,\pi}$ is additive and faithful. We construct the inverse functor $\mathrm{D}_{q,\pi} : \mathrm{Mod}(O)_R \longrightarrow \mathrm{DGr}^*(O)_R$ in the following way.

Let $\mathcal{L} = (L, F_q, V_\pi) \in \mathrm{Mod}(O)_R$. Take $\mathcal{G} = \mathrm{D}_q(\mathcal{L}) = \mathrm{Spec}(A(G), A(G)^\flat, i_{\mathcal{A}}) \in \mathrm{DGr}(\mathbb{F}_q)_R$, where D_q is the functor from § 2.3.1, and provide it with a functorial strict action of π as follows.

Define

$$L^q := \left\{ \sum_i r_i l_i^q \,\middle|\, l_i \in L, r_i \in R \right\} \subset \mathrm{Sym}_R(L).$$

Then the R-module L^q can be identified with $L^{(q)}$ by the map

$$\sum_i l_i \otimes r_i \mapsto \left(\sum_i l_i \otimes r_i \right)^{(q)} := \sum_i r_i l_i^q.$$

Consider the map of R-algebras $\phi_\pi : \mathrm{Sym}_R(L) \longrightarrow \mathrm{Sym}_R(L)$ such that $\phi_\pi : l \mapsto \pi l + V_\pi(l)^{(q)}$ for any $l \in L$. Then

$$\begin{aligned} \phi_\pi(l^q - F_q(l \otimes 1)) &= \phi_\pi(l)^q - \pi F_q(l \otimes 1) - ((F_q \circ V_\pi)(l \otimes 1))^{(q)} \\ &= \pi^q l^q + (V_\pi(l)^{(q)})^q - \pi F_q(l \otimes 1) - ((F_q \circ V_\pi)(l \otimes 1))^{(q)}. \end{aligned} \tag{8}$$

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

From the definition of objects of $\mathrm{Mod}(O)_R$ we obtain

$$(F_q \circ V_\pi)(l \otimes 1)^{(q)} = -\pi l^q + \pi^q l^q + ((V_\pi \circ F_q)(l))^q.$$

Substituting this in (8) we obtain for any $l \in L$,

$$\phi_\pi(l^q - F_q(l \otimes 1)) = \pi(l^q - F_q(l \otimes 1)) + (V_\pi(l)^{(q)} - F_q(V_\pi(l)))^q.$$

Therefore, ϕ_π induces morphisms of R-algebras $[\pi] : A(G) \longrightarrow A(G)$ and $[\pi]^\flat : A(G)^\flat \longrightarrow A(G)^\flat$, which determine an action of π. This action is strict because $(V_\pi(l)^{(q)} - F_q(V_\pi(l)))^q \in I \cdot I_0$.

So, we obtain an object of the category $\mathrm{DGr}(O)_R$ which will be denoted by $\mathrm{D}_{q,\pi}(\mathcal{L})$. Clearly, $\mathrm{L}_{q,\pi}(\mathrm{D}_{q,\pi}(\mathcal{L})) = \mathcal{L}$.

Suppose that $\mathcal{L}_1 = (L_1, F_q, V_\pi) \in \mathrm{Mod}(O)_R$ and $f \in \mathrm{Hom}_{\mathrm{Mod}(O)_R}(\mathcal{L}, \mathcal{L}_1)$. Then we have the R-linear morphism $f : L \longrightarrow L_1$ such that $f \circ V_\pi = V_\pi \circ f^{(q)}$ and $f^{(q)} \circ F_q = F_q \circ f$. Therefore, f induces the morphism of R-algebras

$$\psi_f : \mathrm{Sym}_R(L) \longrightarrow \mathrm{Sym}_R(L_1),$$

which determines the morphism $\bar{\psi}_f$ in the category $\mathrm{Mod}(\mathbb{F}_q)_R$. It remains to prove that $\bar{\psi}_f$ commutes with the action of π on $\mathrm{D}_{q,\pi}(\mathcal{L})$ and $\mathrm{D}_{q,\pi}(\mathcal{L}_1)$.

For any $l \in L$, let $V_\pi(l) = \sum l_i \otimes r_i \in L^{(q)}$. Then $V_\pi(\psi_f(l)) = V_\pi(f(l)) = f^{(q)}(V_\pi(l)) = \sum f(l_i) \otimes r_i = \sum \psi_f(l_i) \otimes r_i$. Therefore,

$$\begin{aligned}\psi_f(\phi_\pi(l)) &= \psi_f(\pi l + V_\pi(l)^{(q)}) = \psi_f\left(\pi l + \sum_i r_i l_i^q\right) \\ &= \pi\psi_f(l) + \sum r_i \psi_f(l)^q = \pi\psi_f(l) + V_\pi(\psi_f(l))^{(q)} = \phi_\pi(\psi_f(l)).\end{aligned}$$

So, $\bar{\psi}_f \in \mathrm{Hom}_{\mathrm{DGr}(O)_R}(\mathrm{D}_{q,\pi}(\mathcal{L}_1), \mathrm{D}_{q,\pi}(\mathcal{L}))$. It is easy to see that $\mathrm{L}_{q,\pi}(\bar{\psi}_f) = f$.

The theorem is proved. □

Remark. The above theorem shows that the category of strict O-modules $\mathrm{DGr}^*(O)_R$ is equivalent to the category of finite v-modules introduced by Taguchi in [Tag95].

4. The category of π-torsion strict modules

Denote by $\mathrm{DGr}'(O)_R$, respectively by $\mathrm{DGr}'^*(O)_R$, the full subcategory in $\mathrm{DGr}(O)_R$, respectively in $\mathrm{DGr}^*(O)_R$, consisting of 'π-torsion objects', i.e. of $(G, G^\flat) \in \mathrm{DGr}(O)_R$ such that $[\pi]_G : A(G) \longrightarrow A(G)$ is nilpotent.

Clearly, the functor $\mathrm{L}_{q,\pi}$ induces an antiequivalence of $\mathrm{DGr}'^*(O)_R$ and the full subcategory $\mathrm{Mod}'(O)_R$ in $\mathrm{Mod}(O)_R$, which consists of (L, F_q, V_π) such that $[\pi]_L = \pi\,\mathrm{id}_L + V_\pi \circ F_q$ is a nilpotent endomorphism of L.

4.1 Let R^* be the multiplicative group of invertible elements of R.

PROPOSITION. *Suppose that $\pi \cdot 1_R \in R^*$ and $\mathcal{G} = (G, G^\flat) \in \mathrm{DGr}(O)_R$. Then G is etale over R.*

Proof. Let $\mathrm{L}_{q,\pi}(\mathcal{G}) = (L, F_q, V_\pi)$. Then $[\pi]_L$ acts on $L/\mathrm{Im}\, F_q$ via the scalar multiplication by $\pi \cdot 1_R \in R^*$. On the other hand, this action should be nilpotent. Therefore, $L = \mathrm{Im}\, F_q$ and G is etale over R. □

COROLLARY. *Suppose that R is an integral domain, $K = \mathrm{Frac}\, R$ and $\Gamma_K = \mathrm{Gal}(K_{\mathrm{sep}}/K)$. If $(G, G^\flat) \in \mathrm{DGr}'(O)_R$, then $G \otimes K$ is etale and $G(K_{\mathrm{sep}})$ is a finite $O[\Gamma_K]$-module of order $\mathrm{rk}_R\, A(G)$.*

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

4.2 The following statement was conjectured in [Fal02] and is proved here following the referee's idea.

Theorem 4. *Suppose that* $(G, G^\flat) \in \mathrm{DGr}'(O)_R$ *and* $\mathrm{rk}_R\, A(G) = q^h$, *then* $[\pi]_G^h = 0$.

Note that for any $\mathcal{G} = (G, G^\flat) \in \mathrm{DGr}(\mathbb{F}_q)_R$ with $\mathrm{L}_q(\mathcal{G}) = (L, F_q)$, we have $\mathrm{rk}_R\, A(G) = q^h$, where $h = \mathrm{rk}_R\, L$.

Via the antiequivalence $\mathrm{L}_{q,\pi}$, Theorem 4 can be obtained from the following proposition.

Proposition. *Suppose that* R *is a local ring,* $\mathcal{L} = (L, F_q, V_\pi) \in \mathrm{Mod}'(O)_R$ *and* $h = \mathrm{rk}_R\, L$. *Then* $[\pi]_L^h = 0$.

Proof. Let $e_1, \dots, e_h$ be an R-basis of L. Let $C = (c_{ij}) \in M_h(R)$ and $D = (d_{ij}) \in M_h(R)$ be such that for all $1 \leqslant j \leqslant h$,

$$V_\pi(e_j) = \sum_i e_i \otimes c_{ij}, \quad F_q(e_j \otimes 1) = \sum_i e_i d_{ij}.$$

Here and below we use the matrix notation $\bar{e} = (e_1, \dots, e_h)$, $V_\pi(\bar{e}) = \bar{e} \otimes C$ and $F_q(\bar{e}) = \bar{e}D$.

Then the R-linear morphism $V_\pi \circ F_q$ is given by the matrix DC in the basis $e_1, \dots, e_n$ and $F_q \circ V_\pi$, and by the matrix CD in the basis $e_1 \otimes 1, \dots, e_h \otimes 1$. From the definition of objects of the category $\mathrm{Mod}(O)_R$ it follows that

$$D^{(q)}C^{(q)} + \pi^q E = CD + \pi E,$$

where E is the unit matrix of order h and $C^{(q)} = (c_{ij}^q)$, $D^{(q)} = (d_{ij}^q)$. Note also that if $\Pi \in M_h(R)$ is such that $[\pi]_L(\bar{e}) = \bar{e}\Pi$, then $DC + \pi E = \Pi$ and $CD + \pi E = \Pi^{(q)}$.

Let λ be an indeterminate.

Lemma. *We have* $\det(CD - \lambda E) = \det(DC - \lambda E)$.

Proof. We can assume that all coefficients in C and D are independent variables over $\mathbb{Q}$. Then our lemma holds over a Zariski closed subset $\mathcal{V}$ in $\mathbb{A}_{\mathbb{Q}}^{2h^2}$, which must contain the Zariski open subset $\det C \neq 0$ (where CD and DC become conjugate). Therefore, $\mathcal{V} = \mathbb{A}_{\mathbb{Q}}^{2h^2}$. The lemma is proved. □

Corollary. *Let* $\Phi(\lambda)$ *be the characteristic polynomial for* $[\pi]_L$. *Then* $\Phi(\lambda) \in \mathbb{F}_q[\lambda] \subset R[\lambda]$.

Proof. It will be sufficient to prove that $\Phi(\lambda) = \Phi^{(q)}(\lambda)$, where all coefficients of $\Phi^{(q)}$ are qth powers of the corresponding coefficients of Φ

$$\begin{aligned}\Phi(\lambda) &= \det(\Pi - \lambda E) = \det(DC + (\pi - \lambda)E) \\ &= \det(CD + (\pi - \lambda)E) = \det(\Pi^{(q)} - \lambda E) = \Phi(\lambda)^{(q)}.\end{aligned}$$ □

We now complete the proof of our proposition. Let k be the residue field of R. Then $[\pi]_L \otimes k$ is a nilpotent endomorphism of $L \otimes k$ with the same characteristic polynomial $\Phi(\lambda) \in \mathbb{F}_q[\lambda] \subset k[\lambda]$. Therefore, $\Phi(\lambda) = \lambda^h$ and by the Cayley–Hamilton theorem $[\pi]_L^h = 0$.

The proposition is proved. □

The above method also gives the following property.

Corollary. *Suppose that* $\mathrm{Spec}\, R$ *is connected,* $x \in \mathrm{Spec}\, R$ *with the residue field* $k(x)$ *and* $\mathcal{G} \in \mathrm{DGr}(O)_R$. *Then* $\mathcal{G} \in \mathrm{DGr}'(O)_R$ *if (and only if)* $\mathcal{G} \otimes k(x) \in \mathrm{DGr}'(O)_{k(x)}$.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

4.3 Embedding into a π-divisible group

By § 1 the objects $\mathcal{G}$ of the category $\mathrm{DGr}(O)_R$ can be treated as conventional group schemes with an endomorphism $[\pi]_{\mathcal{G}}$, which satisfies an extra condition of strictness. Therefore, we can consider short exact sequences in $\mathrm{DGr}(O)_R$ and define the concept of a π-divisible group following the original definition of Tate, cf. [Tat67]. Then a π-divisible group appears as an inductive system $\{\mathcal{G}_n \mid n \in \mathbb{N}\}$ of objects $\mathcal{G}_n = (G_n, G_n^\flat) \in \mathrm{DGr}(O)_R$ such that the corresponding inductive system $\{G_n \mid n \in \mathbb{N}\}$ is a π-divisible group in the category of finite flat O-module schemes over R. Note that for any $n \in \mathbb{N}$, $[\pi]^n_{\mathcal{G}_n} = 0$ in $\mathrm{DGr}^*(O)_R$ and, therefore, $\mathcal{G}_n \in \mathrm{DGr}'(O)_R$ for all $n \in \mathbb{N}$.

THEOREM 5. *Any $\mathcal{G} \in \mathrm{DGr}'(O)_R$ admits locally on R an embedding into a π-divisible group in the category $\mathrm{DGr}(O)_R$.*

Proof. Suppose that $\mathrm{L}_{q,\pi}(\mathcal{G}) = (L, F_q, V_\pi)$. Then we can assume that L has an R-basis $\bar{e} = (e_1, \dots, e_h)$. Therefore, V_π and F_q can be given via the matrices $C, D \in M_h(R)$ such that with notation as in § 3.4, $V_\pi(\bar{e}) = \bar{e} \otimes C$ and $F_q(\bar{e} \otimes 1) = \bar{e}D$. Recall that $DC + \pi E = \Pi$ and $CD + \pi E = \Pi^{(q)}$, where $[\pi]_L(\bar{e}) = \bar{e}\Pi$ and $\Pi^{(q)} = \sigma_q \Pi$.

For $N \in \mathbb{N}$, consider the inductive system of R-modules $\widetilde{L}_N = \bigoplus_{1 \leqslant n \leqslant 2N} L_n$, where each L_n is just a copy of the R-module L. Use the notation $\bar{e}_n$ for the basis $\bar{e}$ of L_n. Define the structural morphisms $\widetilde{V}_\pi : \widetilde{L}_N \longrightarrow \widetilde{L}_N^{(q)}$ and $\widetilde{F}_q : \widetilde{L}_N^{(q)} \longrightarrow \widetilde{L}_N$ by setting for $1 \leqslant n \leqslant N$,

$$\widetilde{V}_\pi(\bar{e}_{2n}) = \bar{e}_{2n} \otimes C + \bar{e}_{2n-1} \otimes 1, \quad \widetilde{V}_\pi(\bar{e}_{2n-1}) = -\bar{e}_{2n-1} \otimes D - \bar{e}_{2n} \otimes \Pi^{(q)} + \delta^*_{n1} \bar{e}_{2n-2} \otimes 1$$
$$\widetilde{F}_q(\bar{e}_{2n} \otimes 1) = \bar{e}_{2n} D + \bar{e}_{2n-1}, \quad \widetilde{F}_q(\bar{e}_{2n-1} \otimes 1) = -\bar{e}_{2n-1} C - \bar{e}_{2n} \Pi + \delta^*_{n1} \bar{e}_{2n-2},$$

where δ^* is the opposite Kronecker symbol, i.e. $\delta^*_{n1} = 0$ if $n = 1$ and $\delta^*_{n1} = 1$, otherwise. Then a straightforward computation shows that for $1 \leqslant n \leqslant 2N$,

$$(\widetilde{V}_\pi \circ \widetilde{F}_q + \pi \,\mathrm{id}_{\widetilde{L}_N})(\bar{e}_n) = \delta^*_{n1} \delta^*_{n2} e_{n-2}$$
$$(\widetilde{F}_q \circ \widetilde{V}_\pi + \pi \,\mathrm{id}_{\widetilde{L}_N^{(q)}})(\bar{e}_n \otimes 1) = \delta^*_{n1} \delta^*_{n2} e_{n-2} \otimes 1.$$

Therefore, each $\widetilde{L}_N$ is an object of the category $\mathrm{Mod}(O)_R$ and for all $1 \leqslant n \leqslant 2N$, one has $[\pi]_{\widetilde{L}_N}(\bar{e}_n) = \delta^*_{n1} \delta^*_{n2} \bar{e}_{n-2}$. This means that $\{\widetilde{L}_N \mid N \geqslant 1\}$ is a π-divisible group in the category $\mathrm{Mod}(O)_R$. We have also an epimorphic map from $(\widetilde{L}_h, \widetilde{F}_q, \widetilde{V}_\pi)$ to (L, F_q, V_π) given by the correspondences $\bar{e}_{2n} \mapsto [\pi]^{h-n}_L(\bar{e})$ and $\bar{e}_{2n-1} \mapsto \bar{0}$ if $1 \leqslant n \leqslant h$.

Finally, applying the antiequivalence $\mathrm{L}_{q,\pi}$ we obtain the statement of our theorem. □

4.4 For any $\mathbb{F}_q$-algebra R define the category $\mathrm{Mod}^1(O)_R$ as follows. Its objects are the triples (L, F_q, Π) such that:

- $(L, F_q) \in \mathrm{Mod}(\mathbb{F}_q)_R$ and F_q is injective;
- $\Pi \in \mathrm{End}_R(L)$ is nilpotent, $\Pi^{(q)} \circ F_q = F_q \circ \Pi$ and for any $l \in L$, $\Pi(l) \equiv \pi l \bmod (\mathrm{Im}\, F_q)$.

The morphisms $f : (L, \mathbb{F}_q) \longrightarrow (L_1, F_q)$ in $\mathrm{Mod}^1(O)_R$ arise from the morphisms of the category $\mathrm{Mod}(\mathbb{F}_q)_R$ that commute with Π.

Consider the functor $M^1_\pi : \mathrm{Mod}'(O)_R \longrightarrow \mathrm{Mod}^1(O)_R$ given by the correspondence $(L, F_q, V_\pi) \mapsto (L, F_q, [\pi]_L)$. The following theorem easily follows from the proposition of § 4.1.

THEOREM 6. *If R is an integral domain then the functor $\mathrm{L}^1_q = \mathrm{L}_{q,\pi} \circ M^1_\pi$ gives an antiequivalence of the categories $\mathrm{DGr}^{*\prime}(O)_R$ and $\mathrm{Mod}^1(O)_R$.*

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

4.5 Relation to the mixed characteristic case

In this section R is the valuation ring in a complete discrete valuation field K of characteristic p. We denote by k the residue field in K and by η one of its uniformisers. We assume also that the O-algebra structure on R is given via the embedding $O \subset R$ such that $\pi \notin R^*$. Then $\hat{O} = \mathbb{F}_q[[\pi]]$ is the valuation ring of a complete discrete valuation subfield E in K. We denote below by $e(K/E)$ the ramification index of K over E.

With the above notation introduce the full subcategory $\mathrm{DGr}_1(O)_R$ in $\mathrm{DGr}^*(O)_R$ consisting of objects killed by $[\pi]$. Via the functor L_q^1 this category is antiequivalent to the full subcategory $\mathrm{Mod}_1^1(O)_R$ in $\mathrm{Mod}^1(O)_R$ consisting of the objects $(L, F_q, 0)$.

4.5.1 Suppose that $e(K/E) = 1$. Introduce the category $\mathrm{SH}_1(\mathbb{F}_q)_R$ with objects $(M_0, M_1, \varphi_0, \varphi_1)$, where M_0 is an R-module of finite length such that $\pi M_0 = 0$, $\varphi_0 : M_0^{(q)} \longrightarrow M_0$ is an R-linear morphism, $M_1 = \mathrm{Ker}\,\varphi_0$, $\varphi_1 : M_1^{(q)} \longrightarrow M_0$ is an R-linear morphism and $\mathrm{Im}\,\varphi_0 + \mathrm{Im}\,\varphi_1 = M$. This is an analogue of Fontaine's category of 'filtered modules of length 1 killed by p'.

Consider the functor $\mathrm{SH} : \mathrm{Mod}_1^1(O)_R \longrightarrow \mathrm{SH}_1(\mathbb{F}_q)_R$ defined by the correspondence $(L, F_q, 0) \mapsto (M_0, M_1, \varphi_0, \varphi_1)$, where $M_0 = L \bmod \pi L$, $\varphi_0 = F_q \bmod \pi L$ and φ_1 is induced by $\frac{1}{\pi}F_q$. The functor SH is an equivalence of categories if $q > 2$ and is 'very close' to such an equivalence if $q = 2$. This shows that strict O-modules have a similar description as conventional group schemes in the case $e(K/E) = 1$.

4.5.2 Suppose that $e(K/E) \leqslant q - 1$. Define the category $\mathrm{SH}_1(O)_R$ of the collections $(M, M_0, M_1, \varphi_0, \varphi_1)$, where M is an R-module of finite length killed by π, $M_0 = \{m \in M \mid \eta m = 0\}$, $\varphi_0 : M_0^{(q)} \longrightarrow M$ is an R-linear map, $M_1 = \mathrm{Ker}\,\varphi_0$, $\varphi_1 : M_1^{(q)} \longrightarrow M$ is an R-linear map, and $\mathrm{Im}\,\varphi_0 + \mathrm{Im}\,\varphi_1 = M$. This category is an analogue of the category SH_O from[Abr90].

Consider the functor $\mathrm{SH} : \mathrm{Mod}_1^1(O)_R \longrightarrow \mathrm{SH}_1(O)_R$ defined by the correspondence $(L, F_q, 0) \mapsto (M, M_0, M_1, \varphi_0, \varphi_1)$, where:

- M is the image of $\frac{\eta}{\pi}F_q(L^{(q)}) + \frac{1}{\pi}F_q(L_1^{(q)})$ in $\frac{\eta}{\pi}L \bmod(\eta L)$ with $L_1^{(q)} = \{l \in L^{(q)} \mid F_q(l) \in \eta L\}$;
- $M_0 = L \bmod \eta L$ and $\varphi_0 : M_0^{(q)} \longrightarrow M$ is induced by $\frac{\eta}{\pi}F_q$;
- $M_1 = L_1^{(q)} \bmod \eta L$ and $\varphi_1 : M_1^{(q)} \longrightarrow M$ is induced by $\frac{1}{\pi}F_q$.

If $e < q - 1$ then SH is an equivalence of categories and, if $e = q - 1$, then SH is 'very close' to such an equivalence.

Note that when working in the equal characteristic case, the category $\mathrm{SH}_1(O)_R$ can be replaced by a simpler category $\mathrm{SH}'_1(O)_R$ consisting of triples (M, M_0, φ), where M is an R-module of finite length killed by π, $M_0 = \{m \in M \mid \eta m = 0\}$ and $\varphi : M_0^{(q)} \longrightarrow M$ is an R-linear morphism such that $\mathrm{Im}\,\varphi = M$. The functor $\mathrm{SH}' : \mathrm{Mod}_1^1(O)_R \longrightarrow \mathrm{SH}'_1(O)_R$ is defined by the correspondence $(L, F_q, 0) \mapsto (M, M_0, \varphi)$, where $M = \frac{1}{\pi}L^{(q)} \bmod \eta L$, $M_0 = L \bmod \eta L$ and φ is induced by $\frac{1}{\pi}F_q$ (this map is additive because of the equal characteristic assumption).

4.5.3 Suppose that $e(K/E)$ is arbitrary. Introduce the category $\mathrm{BR}_1(O)_R$. Its objects are the triples (M, M_1, φ), where M is an R-module of finite length such that $\pi M = 0$, M_1 is an R_1-submodule in $M \otimes_R R_1$, where $R_1 = R[\eta_1]$ with $\eta_1^q = \eta$, and $\varphi : M_1^{(q)} \longrightarrow M$ is an R-linear map such that $\varphi(M_1) = M \otimes_R R_1$. This category is an equicharacteristic version of Breuil's category $\mathrm{Mod}_{/S_1}$ that appeared in his classification of period p group schemes in the mixed characteristic case, cf. [Bre00].

Again there is a natural functor from $\mathrm{Mod}_1^1(O)_R$ to $\mathrm{BR}_1(O)_R$ defined by the correspondence $(L, F_q, 0) \mapsto (M, M_1, \varphi)$, where $M = L \bmod \pi L$ and φ is induced by $\frac{1}{\pi}F_q$.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

4.5.4 Again $e(K/K_0)$ is arbitrary. Introduce an equal characteristic analogue of the concept of 'p-etale φ-module of q-height r over S' from [Fon90].

Let $r \in \mathbb{N}$. Introduce the category $\mathrm{Mod}^r(O)_R$ by generalizing the definition of $\mathrm{Mod}^1(O)_R$ from § 4.4. Its objects are (L, F_q, Π), where:

- $(L, F_q) \in \mathrm{Mod}(\mathbb{F}_q)_R$ and F_q is injective;
- $\Pi \in \mathrm{End}_R L$ is nilpotent and satisfies the relation $F_q \circ \Pi = \Pi^{(q)} \circ F_q$;
- for any $l \in L$, $(\Pi - \pi\,\mathrm{id}_L)^r(l) \in \mathrm{Im}\, F_q$.

The morphisms in this category are morphisms of the category $\mathrm{Mod}(O)_R$, which commute with Π.

Let $\mathrm{MG(O)_K}$ be the category of finite continuous $O[\Gamma_K]$-modules. Consider the functor $\mathrm{MG} : \mathrm{Mod^r(O)_R} \longrightarrow \mathrm{MG(O)_K}$ defined by the correspondence $(L, F_q, \Pi) \mapsto G(K_{\mathrm{sep}})$, where $\mathrm{D}_q(L, F_q) = (G, G^\flat) \in \mathrm{DGr}(\mathbb{F}_q)_R$, cf. § 2.3.1, and the action of $O = \mathbb{F}_q[\pi]$ on $G(K_{\mathrm{sep}})$ comes from the $\mathbb{F}_q$-action on G and the action of π via the morphism $\mathrm{D}_q(\Pi)$.

For any $r \in \mathbb{N}$, let $\mathrm{MG^r(O)_K}$ be the full subcategory in $\mathrm{MG(O)_K}$ consisting of the $O[\Gamma_K]$-modules $\mathrm{MG}(\mathcal{L})$, where $\mathcal{L} \in \mathrm{Mod}^r(O)_R$. The study of properties of its objects appears as equicharacteristic analogue of the problem of study of finite subquotients of crystalline representations with Hodge–Tate weights from $[0, r]$. If $r = 1$, then objects of $\mathrm{MG}^1(\mathrm{O})_\mathrm{K}$ come from the Galois modules of generic fibres of strict O-modules over R.

4.6 Several remarks about duality in $\mathrm{DGr}^*(O)_R$

Suppose that $\mathcal{L} = (L, F_q, V_\pi) \in \mathrm{Mod}(O)_R$. Let $L^D = \mathrm{Hom}_{R\text{-mod}}(L, R)$. Then L^D is a locally free R-module and $L^{D(q)} = \mathrm{Hom}_{R\text{-mod}}(L^{(q)}, R)$. Therefore, we have R-linear maps $F_q : L^{D(q)} \longrightarrow L^D$ and $V_\pi : L^D \longrightarrow L^{D(q)}$ such that for any $\tilde{l} \in L^D$ and $l \in L$, $F_q(\tilde{l} \otimes 1)(l) = (\tilde{l} \otimes 1)(V_\pi l)$ and $V_\pi(\tilde{l})(l \otimes 1) = \tilde{l}(F_q(l \otimes 1))$.

It can be easily verified that $\mathcal{L}^D := (L^D, F_q, V_\pi) \in \mathrm{Mod}(O)_R$. The correspondence $\mathcal{L} \mapsto \mathcal{L}^D$ gives a perfect duality in $\mathrm{Mod}(O)_R$ that has all nice functorial properties. This duality was introduced and studied in [Tag95].

Consider the formal Lubin–Tate group $G_{LT} = \mathrm{Spf} R[[X]]$ such that $\mathrm{End}_R(G_{LT}) = \hat{O}$ and the endomorphism $[\pi]_{LT}$ of multiplication by $\pi \in O$ is given by $[\pi]_{LT}(X) = X^q + \pi X$. Then for $h \in \mathbb{N}$, $G_{LT,h} := \mathrm{Ker}[\pi]^h_{LT}$ has a natural structure of an object $\mathcal{G}_{LT,h}$ of the category $\mathrm{DGr}(O)_R$. Let $\mathrm{L}_{q,\pi}(\mathcal{G}_{LT,h}) = \mathcal{L}_{LT,h} = (L_h, F_q, V_\pi)$. Then $\mathcal{L}_{LT,h} \in \mathrm{Mod}'(O)_R$ and $L_h = \bigoplus_{1 \leqslant i \leqslant h} R m_i$, where for $1 \leqslant i \leqslant h$, $F_q(m_i \otimes 1) = m_{i-1} - \pi m_i$ and $V_\pi(m_i) = m_i \otimes 1$ with the agreement $m_0 = 0$.

Suppose that $\mathcal{L} = (L, F_q, V_\pi) \in \mathrm{Mod}'(O)_R$ and $[\pi]^h_L = 0$. Then $\mathcal{L}^D = (L^D, F_q, V_\pi) \in \mathrm{Mod}'(O)_R$ and $[\pi]^h_{L^D} = 0$. Consider the R-linear map

$$c : L_h \longrightarrow L \otimes L^D = \mathrm{Hom}_R(L, L),$$

which is uniquely determined by the requirements $c(m) = \mathrm{id}_L$ and $c \circ F_q = F_q \circ c^{(q)}$. Consider the natural embeddings $L_h \subset A(G_{LT,h})$, $L \subset A(G)$ and $L^D \subset A(G^D)$, where $\mathcal{G} = (G, G^\flat)$ and $\mathcal{G}^D = (G^D, G^{D\flat})$ are such that $\mathrm{L}_{q,\pi}(\mathcal{G}) = \mathcal{L}$ and $\mathrm{L}_{q,\pi}(\mathcal{G}^D) = \mathcal{L}^D$. Together with the above map c these embeddings determine a morphism of R-schemes $G \times G^D \longrightarrow G_{LT,h}$, which induces a non-degenerate bilinear pairing of strict O-modules

$$C : \mathcal{G} \times \mathcal{G}^D \longrightarrow \mathcal{G}_{LT,h}.$$

This is an analogue of the Cartier duality. Its direct construction is given in [Fal02]. In the context of finite v-modules, cf. the remark at the end of § 3.3, the pairing C appears in [Tag95].

Remark. The referee pointed out that the existence of the pairing C implies a short proof of the difficult part of our Theorem 1 from § 2.1.

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

5. Properties of Galois modules from $\mathbf{MG}^1(O)_K$

As in § 4.5, $E \subset K$ are complete discrete valuation fields of characteristic p with uniformisers π and, respectively, η. The valuation ring of E is $\hat{O} = \mathbb{F}_q[[\pi]]$ and the residue field k of K is perfect and the valuation ring of K is R.

Suppose that $\mathcal{G} = (G, G^\flat) \in \mathrm{DGr}'(O)_R$, $H = G(K_{\mathrm{sep}})$ is the $O[\Gamma_K]$-module of geometric points of G and $e = e(K/E)$ – is the ramification index of K over E. We also set $\Gamma_K = \mathrm{Gal}(K_{\mathrm{sep}}/K)$ and denote by I_K the inertia subgroup of Γ_K.

5.1 Characters of the semisimple envelope of H

Suppose that $\bar{k}$ is an algebraic closure of k and the character $\chi : I_K \longrightarrow \bar{k}^*$ appears with a nonzero multiplicity in the semisimple envelope of the $O[\Gamma_K]$-module H. An analogue of the Serre conjecture for H can be stated as follows.

Theorem 7. *For the above character χ, there are $a, N \in \mathbb{N} \setminus p\mathbb{N}$ such that $\chi = \chi_N^a$, where $a = a_0 + a_1 q + \cdots + a_{N-1} q^{N-1}$ with $0 \leqslant a_i \leqslant e$ and $\chi_N : I_K \longrightarrow \bar{k}^*$ is such that for any $\tau \in I_K$, $\chi_N(\tau) = \tau(\eta_N)/\eta_N$, where $\eta_N \in K_{\mathrm{sep}}$ and $\eta_N^{q^N-1} = \eta$.*

Proof. This can be deduced in the same way as it has been obtained in the case of usual group schemes in [Ray74]. First, we can assume that $k = \bar{k}$ and $e < q - 1$. Then any simple object of the category $\mathrm{Mod}^1(O)_R$ appears in the form $(L, F_q, 0)$, where $L = \bigoplus_{0 \leqslant i < n} Rm_i$, $F_q m_0 = \eta^{a_0} m_1, \ldots, F_q m_{N-1} = \eta^{a_{N-1}} m_0$ with $0 \leqslant a_i \leqslant e$, $0 \leqslant i < N$.

Then the corresponding Galois module consists of K_{sep}-points of the R-algebra $R[T_0, \ldots, T_{N-1}]$, where $T_0^q = \eta^{a_0} T_1, \ldots, T_{N-1}^q = \eta^{a_{N-1}} T_0$. It can be naturally identified with the $\mathbb{F}_q[\Gamma_K]$-module $\{\alpha \eta_N^a \mid \alpha \in \mathbb{F}_{q^N}\}$, where $a = a_0 + a_1 q + \cdots + a_{N-1} q^{N-1}$. Clearly, I_K acts on it via the conjugacy class of characters $\{\sigma^i \chi_N^a \mid 0 \leqslant i < N\}$. □

Following Raynaud's method, cf. [Ray74], one can deduce from the above description of simple objects in $\mathrm{Mod}^1(O)_R$ that if $e < q-1$, then the functor $(G, G^\flat) \mapsto G(K_{\mathrm{sep}})$ is a fully faithful functor from $\mathrm{DGr}'(O)_R$ to the category $\mathrm{MG(O)_K}$ of finite $O[\Gamma_K]$-modules. The proof uses induction on the length of the Jordan–Hoelder series for $G(K_{\mathrm{sep}})$ and the description of simple objects in $\mathrm{Mod}^1(O)_R$ from the proof of the above Theorem 7.

5.2 Ramification estimates

These estimates are given in Theorem 8 below and are very similar to the known estimates in the case of conventional group schemes, cf. [Fon85]. The proof is based on the knowledge of 'equations' of the strict module G and is done below by the methods of [Abr98]. Note that the methods from [Fon93] can also be adjusted to obtain similar estimates, cf. also [Tag92]. Our method is simpler, but it works only in positive characteristic.

Theorem 8. *If H is killed by $[\pi^N]$, then the ramification subgroups $\Gamma_K^{(v)}$ act trivially on H for $v > e(N + 1/(q-1)) - 1$.*

Proof. By Theorem 5 we can assume that there is a π-divisible group $\{\mathcal{G}_n\}_{n \geqslant 1}$ of a height h in $\mathrm{DGr}(O)_R$ such that $\mathcal{G}_N = \mathcal{G}$.

5.2.1 Let $\mathrm{L}_q^1(\mathcal{G}) = (L, F_q, \Pi)$, cf. § 4.4. Then L is a free R-module of rank hN and we can choose its R-basis in the form

$$m_1, \ldots, m_h, \Pi m_1, \ldots, \Pi m_h, \ldots, \Pi^{N-1} m_1, \ldots, \Pi^{N-1} m_h.$$

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

For $1 \leqslant i \leqslant N$, introduce the vector-columns $\bar{m}^{(i)} = (\Pi^{N-i}m_1, \dots, \Pi^{N-i}m_h)^{\mathrm{t}}$ and set $F_q\bar{m}^{(i)} = (F_q(\Pi^{N-i}m_1^{\mathrm{t}}), \dots, F_q(\Pi^{N-i}m_h^{\mathrm{t}}))^{\mathrm{t}}$. Then, the condition $\mathrm{Im}(\Pi - \pi\,\mathrm{id}_L) \subset \mathrm{Im}\,F_q$ implies the existence of unique matrices $C_1, \dots, C_N \in M_h(R)$ such that

$$C_1F_q\bar{m}^{(N)} + C_2F_q\bar{m}^{(N-1)} + \dots + C_NF_q\bar{m}^{(1)} = \pi\bar{m}^{(N)} - \bar{m}^{(N-1)}$$
$$C_1F_q\bar{m}^{(N-1)} + \dots + C_{N-1}F_q\bar{m}^{(1)} = \pi\bar{m}^{(N-1)} - \bar{m}^{(N-2)}$$
$$\vdots$$
$$C_1F_q\bar{m}^{(1)} = \pi\bar{m}^{(1)}.$$

Note that C_1 divides πE_h, where E_h is the unit matrix of order h.

Consider the vector columns $\bar{X}_i = (X_{i1}, \dots, X_{ih})^{\mathrm{t}}$ of independent variables X_{ij}, $1 \leqslant i \leqslant N$, $1 \leqslant j \leqslant h$. Then the algebra $A(G) \otimes_R K$ appears as the quotient of $K[\bar{X}_1, \dots, \bar{X}_N]$ by the ideal generated by the equations

$$\sum_{1 \leqslant i \leqslant s} C_i\bar{X}_{s+1-i}^q = \pi\bar{X}_s - \bar{X}_{s-1} \tag{9}$$

where $1 \leqslant s \leqslant N$ and by definition $\bar{X}_0 = \bar{0}$.

Consider the points of $G(K_{\mathrm{sep}})$ as solutions $\bar{a} = (\bar{a}_1, \dots, \bar{a}_N)$ of the system (9).

LEMMA. *We have the following.*

(a) *If $\bar{a} = (\bar{a}_1, \dots, \bar{a}_N) \in G(K_{\mathrm{sep}})$, then $\bar{a}_1, \dots, \bar{a}_N$ have coordinates in $O_{K_{\mathrm{sep}}}$.*

(b) *If $\bar{a}' = (\bar{a}'_1, \dots, \bar{a}'_N) \in G(K_{\mathrm{sep}})$ and $\bar{a} \equiv \bar{a}' \bmod \pi^{1/(q-1)}m_{\mathrm{sep}}$, where m_{sep} is the maximal ideal of the valuation ring of K_{sep}, then $\bar{a} = \bar{a}'$.*

Proof. Both statements follow easily by induction on N from the above equations for points of G. Statement (b) requires only that $C_1, \dots, C_h \in M_h(R)$, in statement (a) we need also that C_1 divides πE_h. □

5.2.2 Suppose that $\alpha \in \mathbb{Q}_{>0}$ has the zero p-adic valuation. Then $\alpha = m/(q^M - 1)$ with suitable $m, M \in \mathbb{N}$, $(m, p) = 1$. Note that the presentation of α in the form of fraction $m/(q^M - 1)$ is not unique and can always be chosen with an arbitrary large value of M. For any such α there is an extension K_α of K of degree q^M with the Herbrand function

$$\varphi_{K_\alpha/K}(x) = \begin{cases} x, & \text{for } 0 \leqslant x \leqslant \alpha \\ \alpha + \dfrac{x - \alpha}{q^M}, & \text{for } x \geqslant \alpha. \end{cases}$$

Note that $\varphi_{K_\alpha/K}$ has only one edge point $x = \alpha$.

Explicit construction of K_α can be found in [Abr98] and can be briefly described as follows. Let $\eta_M \in K_{\mathrm{sep}}$ be such that $\eta_M^{q^M-1} = \eta$ and let $L_\alpha = K(\eta_M)(T)$, where

$$T^{q^M} - T = \eta_M^{-m}.$$

Then $K_\alpha = K(\eta_\alpha)$, where η_α is a uniformising element in K_α such that $\eta_\alpha^{-m} = T^{q^M-1}$. From the above construction of K_α, it follows that

$$\eta_\alpha^{q^M}(1 - \eta_\alpha^m)^{-1/\alpha} = \eta,$$

where $(-1/\alpha)$th power is taken via the binomial series. In particular,

$$\eta \equiv \eta_\alpha^{q^M} \bmod (\eta\eta_\alpha^m). \tag{10}$$

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

Note that K_α is totally ramified over K and, therefore, there is a field isomorphism $h_\alpha : K \longrightarrow K_\alpha$ such that $h_\alpha(\eta) = \eta_\alpha$ and $h_\alpha|_k = \mathrm{id}$. (Here k is the residue field of K and K_α.)

Relation (10) now implies that for any $a \in \eta R$, $a = h_\alpha(a)^{q^M} + \tilde{a}$, with $\tilde{a} \in K_\alpha$ such that $v_K(\tilde{a}) \geqslant v_K(a) + \alpha(1 - q^{-M})$ (v_K is the valuation in K such that $v_K(\eta) = 1$). Below we use the following consequence of this fact: *if $a \in R$, then $v_K(a - h_\alpha(a)^{q^M}) \geqslant 1 + \alpha(1 - q^{-M})$.*

5.2.3 Denote by the same symbol an extension of h_α to an isomorphism of K_{sep} onto $K_{\alpha,\mathrm{sep}} = K_{\mathrm{sep}}$. Clearly, $\bar{X} = (\bar{X}_1, \dots, \bar{X}_s) \mapsto h_\alpha(\bar{X}) = (h_\alpha(\bar{X}_1), \dots, h_\alpha(\bar{X}_s))$ is a one-to-one correspondence between solutions of the system (9) and solutions $\bar{Y} = (\bar{Y}_1, \dots, \bar{Y}_N)$ of the similar system

$$\sum_{1 \leqslant i \leqslant s} h_\alpha(C_i) \bar{Y}_{s+1-i}^q = h_\alpha(\pi) \bar{Y}_s - \bar{Y}_{s-1} \tag{11}$$

where $1 \leqslant s \leqslant N$ and by definition $\bar{Y}_0 = \bar{0}$.

Lemma. *If $\alpha(1 - 1/q^M) > e(N + 1/(q-1)) - 1$, then for any solution $\bar{X}^{(0)}$ of (9) there is a unique solution $\bar{Y}^{(0)}$ of (11) such that $\bar{X}^{(0)} \equiv \bar{Y}^{(0)q^M} \bmod \pi^{1/(q-1)} m_{\mathrm{sep}}$.*

Proof. The correspondence $\bar{Y} \mapsto \bar{Z} = \bar{Y}^{q^M} - \bar{X}^{(0)}$ establishes a one-to-one correspondence between solutions $\bar{Y}$ of (11) and solutions $\bar{Z} = (\bar{Z}_1, \dots, \bar{Z}_N)$ of the system of equations

$$\sum_{1 \leqslant i \leqslant s} C_i \bar{Z}_{s+1-i}^q = \pi \bar{Z}_s - \bar{Z}_{s-1} - \bar{F}_s \tag{12}$$

where $1 \leqslant s \leqslant N$, $\bar{Z}_0 = 0$ and

$$\bar{F}_s = \tilde{\pi} \bar{Y}_s^{q^M} - \sum_{1 \leqslant i \leqslant s} \tilde{C}_i \bar{Y}_{s+1-i}^{q^{M+1}} \in \pi^{N+1/(q-1)} m_{\mathrm{sep}}$$

because the v_K-valuations of $\tilde{\pi} = \pi - h_\alpha(\pi)^{q^M}$ and of $\tilde{C}_i = C_i - h_\alpha(C_i)^{(q^M)}$ are strictly bigger than $e(N + 1/(q-1))$.

Now induction on s shows that the system (12) has a unique solution $\bar{Z} = (Z_1, \dots, Z_N)$ with coordinates in $\pi^{1/(q-1)} m_{\mathrm{sep}}$. (Note that these coordinates $Z_1, \dots, Z_N$ are such that for $1 \leqslant s \leqslant N$, $\bar{Z}_s \equiv \bar{0} \bmod \pi^{N-s+1/(q-1)} m_{\mathrm{sep}}$.)

The lemma is proved. □

With the above notation and assumptions we have the following corollary.

Corollary. *Suppose that L, respectively L_α, is obtained by joining to K, respectively K_α, all coordinates of all solutions of the system of equations (9), respectively (11), in K_{sep}. Then $LK_\alpha = L_\alpha$.*

Proof. Suppose that $\tau \in \mathrm{Gal}(K_{\mathrm{sep}}/K_\alpha)$. Then $\tau \in \mathrm{Gal}(K_{\mathrm{sep}}/LK_\alpha)$ if and only if for any solution $\bar{X}^{(0)}$ of the system (9), we have (cf. the lemma in § 5.2.1)

$$\tau \bar{X}^{(0)} \equiv \bar{X}^{(0)} \bmod \pi^{1/(q-1)} m_{\mathrm{sep}}.$$

By the above lemma this is equivalent to the congruences

$$\tau \bar{Y}^{(0)} \equiv \bar{Y}^{(0)} \bmod \pi_\alpha^{1/(q-1)} m_{\mathrm{sep}}$$

for all solutions $\bar{Y}^{(0)}$ of the system (11), and this means that $\tau \in \mathrm{Gal}(K_{\mathrm{sep}}/L_\alpha)$.

The corollary is proved. □

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

5.2.4 For any finite extension $F \subset F_1$ in K_{sep}, let $v(F_1/F)$ be the minimal rational number such that the ramification groups $\Gamma_F^{(v)}$ act trivially on F_1 if $v > v(F_1/F)$.

Proposition. *With the notation from § 5.2.3 there is the following inequality*

$$v(L/K) \leqslant e\left(N + \frac{1}{q-1}\right) - 1$$

Proof. Suppose that this inequality does not hold. Then there is a rational number $\alpha = m/(q^M - 1)$ satisfying the assumptions from the beginning of n.5.2.2 and the inequalities

$$v(L/K) > \alpha > \alpha\left(1 - \frac{1}{q^M}\right) > e\left(N + \frac{1}{q-1}\right) - 1.$$

(We can always choose a sufficiently large M.)

Then by the lemma of § 5.2.3 one has $L_\alpha = LK_\alpha$ and this implies that

$$v(L_\alpha/K) = \max\{v(L/K), v(K_\alpha/K)\} = v(L/K). \tag{13}$$

On the other hand, looking at the maximal edge points of Herbrand functions we obtain from the composition property $\varphi_{L_\alpha/K} = \varphi_{L_\alpha/K_\alpha} \circ \varphi_{K_\alpha/K}$ that

$$\begin{aligned} v(L_\alpha/K) &= \max\left\{v(K_\alpha/K), \varphi_{K_\alpha/K}(v(L_\alpha/K_\alpha))\right\} \\ &= \max\left\{\alpha, \frac{v(L_\alpha/K_\alpha) - \alpha}{q} + \alpha\right\} < v(L_\alpha/K_\alpha), \end{aligned}$$

because $\alpha < v(L/K) = v(L_\alpha/K_\alpha)$. However, this contradicts (13).

Theorem 8 is proved. □

5.3 As was noticed in § 3.5.1, if $e = 1$ then strict O-modules that are killed by $[\pi]$ behave very similarly to group schemes of period p over Witt vectors. For this reason, one can apply directly methods from [Abr87b] to prove the following result.

Theorem 9. *Suppose that $q \geqslant 4$ and H is an $\mathbb{F}_q[\Gamma_K]$-module such that:*

(a) *the action of the inertia subgroup of Γ_K on the semisimple envelope of H is given by characters, which satisfy Serre's conjecture, cf. Theorem 7;*

(b) *the ramification subgroups $\Gamma_K^{(v)}$ act trivially on H if $v > 1/(q-1)$ (i.e. the ramification estimate from Theorem 8 holds for H).*

Then there is a $\mathcal{G} = (G, G^\flat) \in \mathrm{DGr}'(O)_R$ such that $H \simeq G(K_{\mathrm{sep}})$. □

Acknowledgement

The author expresses his gratitude for hospitality to the Max-Planck-Institute in Mathematics where a part of this paper was written.

References

Abr87a V. Abrashkin, *Honda systems of group schemes of period p*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), 451–484. (Engl. transl. Math. USSR Izv. **30** (1988), 419–453.)

Abr87b V. Abrashkin, *Galois modules of period p group schemes over the ring of Witt vectors*, Izv. Akad. Sci. SSSR Ser. Mat. **51** (1987), 691–736. (Engl. transl. Math. USSR Izv. **31** (1988), 1–46.)

Abr90 V. Abrashkin, *Group schemes over a discrete valuation ring with small ramification*, Algebra i Analiz **1** (1989), 60–95. (Engl. transl. Leningrad Math. J. **1** (1990), 57–97.)

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press

Abr98 V. Abrashkin, *The ramification filtration of the Galois group of a local field. III*, Izv. Ross. Akad. Nauk Ser. Mat. **62** (1998), 3–48. (Engl. transl. Izv. Math. **62** (1998), 857–900.)

Bre00 C. Breuil, *Groupes p-divisibles, groupes finis et modules filtres*, Ann. of Math. (2) **152** (2000), 489–549.

Con99 B. Conrad, *Finite group schemes over bases with low ramification*, Compositio Math. **119** (1999), 239–320.

DG70 M. Demazure and P. Gabriel, *Groupes algébriques. Tome 1: géométrie algébrique, généralités, groupes commutatifs* (North-Holland, Amsterdam, 1970).

Fal02 G. Faltings, *Group schemes with strict $\mathcal{O}$-action*, Moscow Math. J. **2** (2002), 249–279.

Fon75 J. M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C. R. Acad. Sci. Paris Sér. A-B **280** (1975), A1423–A1425.

Fon85 J.-M. Fontaine, *Il n'y a pas de variété abélienne sur $\mathbb{Z}$*, Invent. Math. **81** (1985), 515–538.

Fon90 J.-M. Fontaine, *Représentations p-adiques des corps locaux. I*, in *The Grothendieck Festschrift, vol. II*, Progress in Mathematics, vol. 87 (Birkhäuser, Boston, MA, 1990), 249–309.

Fon93 J.-M. Fontaine, *Schémas propres et lisses sur $\mathbb{Z}$*, in *Proceedings of the Indo–French Conference on Geometry (Bombay, 1989)* (Hindustan Book Agency, Delhi, 1993), 43–56.

Gab70 P. Gabriel, *Étude infinitésimale des schémas en groupes*, in *Schémas en Groupes I*, Lecture Notes in Mathematics, vol. 151 (Springer, Berlin, 1970), 474–560.

Gen96 A. Genestier, *Espaces symmetriques de Drinfeld*, Astérisque **234** (1996).

Gib04 W. Gibbons, *Dieudonné theory for Faltings's strict modules*, PhD thesis, University of Durham, September (2004).

Ray74 M. Raynaud, *Schémas en groupes de type $(p, \ldots, p)$*, Bull. Soc. Math. France **102** (1974), 241–280.

Tag92 Yu. Taguchi, *Ramification arising from Drinfeld modules*, in *The Arithmetic of Function Fields. Proceedings of the Workshop (Ohio State University, 1991)* (de Gruyter, Berlin, 1992), 171–188.

Tag95 Yu. Taguchi, *A duality for finite t-modules*, J. Math. Sci. Univ. Tokyo **2** (1995), 563–588.

Tat67 J. Tate, *p-divisible groups*, in *Proc. conf. local fields (Driebergen, 1966)* (Springer, Berlin, 1967), 158–183.

V. Abrashkin victor.abrashkin@durham.ac.uk
Steklov Mathematics Institute, Gubkina 8, 117966 Moscow, Russia
Current address: Department of Mathematics, University of Durham, Science Laboratories, Durham DH1 3LE, UK

https://doi.org/10.1112/S0010437X06002041 Published online by Cambridge University Press