PSEUDO-RIGID p-TORSION FINITE FLAT COMMUTATIVE GROUP SCHEMES

YUICHIRO HOSHI

MARCH 2021

ABSTRACT. — Let p be a prime number and k a perfect field of characteristic p. In the present paper, we study deformations of finite flat commutative group schemes over k to the ring W of Witt vectors with coefficients in k. We prove that, for a given principally quasi-polarizable p-torsion finite flat commutative group scheme over k, it holds that the group scheme is pseudo-rigid — i.e., roughly speaking, has a unique, up to isomorphism over W, deformation to W — if and only if the group scheme is superspecial.

CONTENTS

INTRODUCTION

Let p be a prime number and k a perfect field of characteristic p. In the present paper, we study deformations of finite flat commutative group schemes over k to the ring $W \stackrel{\text{def}}{=} W(k)$ of Witt vectors with coefficients in k. More specifically, we study *pseudo-rigid* p-torsion finite flat commutative group schemes over k.

A finite flat commutative group scheme over W is one fundamental object in the study of arithmetic geometry from the point of view of Galois representations. Now let us observe that, for two finite flat commutative group schemes H_1, H_2 over W, if H_1 is isomorphic to H_2 over W, then it is immediate that $H_1 \times_W k$ is isomorphic to $H_2 \times_W k$ over k. However, in this situation, the existence of an isomorphism $H_1 \times_W k \xrightarrow{\sim} H_2 \times_W k$ over k does in general *not imply* the existence of an isomorphism $H_1 \xrightarrow{\sim} H_2$ over W. Put another way, the isomorphism class of a finite flat commutative group scheme over W is

2010 MATHEMATICS SUBJECT CLASSIFICATION. — 14L15.
KEY WORDS AND PHRASES. — finite flat commutative group scheme, pseudo-rigid.

in general *not determined* by the isomorphism class of the special fiber over k. A central problem discussed in the present paper is as follows:

> Give a sufficient and necessary condition for a finite flat commutative group scheme that *ensures* this converse implication.

Let G be a p-torsion finite flat commutative group scheme over k. Then we shall say that G is *principally quasi-polarizable* [cf. Definition 1.4] if G is isomorphic to the Cartier dual of G over k. Moreover, we shall say that G is *pseudo-rigid* [cf. Definition 1.8] if the following two conditions are satisfied:

- There exists a p-torsion finite flat commutative group scheme H over W such that $H \times_W k$ is isomorphic to G over k.

- If H_1, H_2 are p-torsion finite flat commutative group schemes over W such that $H_i \times_W k$ is isomorphic to G over k for each $i \in \{1, 2\}$, then H_1 is isomorphic to H_2 over W.

Thus, roughly speaking, we say that G is pseudo-rigid if G has a deformation to W, and, moreover, arbitrary two deformations of G to W are isomorphic over W.

A typical example of a pseudo-rigid finite flat commutative group scheme is an *étale* commutative group scheme over k. Moreover, one verifies immediately, by considering the Cartier dual, that a *multiplicative* [cf. Definition 4.8, (i)] finite flat commutative group scheme over k is pseudo-rigid. The main result of the present paper gives a sufficient and necessary condition for a principally quasi-polarizable p-torsion finite flat commutative group scheme over k to be pseudo-rigid. The main result of the present paper is as follows [cf. Theorem 4.10, (i), (iii)]:

THEOREM. — *Let G be a p-torsion finite flat commutative group scheme over k. Suppose that either G or the Cartier dual of G is* **connected** *whenever $p = 2$. Then the following assertions hold:*

(i) *If G is either* **étale** *over k,* **multiplicative***, or* **superspecial** [*cf. Definition* 4.8, (ii)]*, then G is* **pseudo-rigid**.

(ii) *Suppose that G is* **principally quasi-polarizable**. *Then G is* **pseudo-rigid** *if and only if G is* **superspecial**.

The present paper is organized as follows: In §1, we introduce the notion of pseudo-rigidity, that is one central notion of the present paper. In §2, we give a review of a certain linear algebra theory for p-torsion finite flat commutative group schemes over k. In §3, we give a review of a certain linear algebra theory for p-torsion finite flat commutative group schemes over W. In §4, we prove the main result of the present paper.

ACKNOWLEDGMENTS

The author would like to thank the referee for some helpful comments. In particular, the author would especially like to express his gratitude the referee for a comment concerning removing a connectedness hypothesis from Lemma 3.12 in an earlier version of this manuscript. This research was supported by JSPS KAKENHI Grant Number 18K03239 and by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

1. p-Torsion Finite Flat Commutative Group Schemes

In the present §1, we introduce the notion of *pseudo-rigidity* [cf. Definition 1.8 below], that is one central notion of the present paper.

In the present §1, let p be a prime number and k a perfect field of characteristic p. Write $W \stackrel{\text{def}}{=} W(k)$ for the ring of Witt vectors with coefficients in k. Let R be a W-algebra.

Definition 1.1. — We shall write

$$\mathfrak{ffg}_R^{[p]}$$

for the category defined as follows:

- An object of the category $\mathfrak{ffg}_R^{[p]}$ is defined to be a p-torsion finite flat commutative group scheme over R.

- A morphism in the category $\mathfrak{ffg}_R^{[p]}$ is defined to be a homomorphism between finite flat commutative group schemes over R.

Definition 1.2. — We shall write

$$\mathfrak{cffg}_R^{[p]} \subseteq \mathfrak{ffg}_R^{[p]}$$

for the full subcategory of $\mathfrak{ffg}_R^{[p]}$ consisting of *connected* p-torsion finite flat commutative group schemes over R.

Definition 1.3. — Let G be an object of the category $\mathfrak{ffg}_R^{[p]}$. Then we shall write

$$G^D$$

for the object of the category $\mathfrak{ffg}_R^{[p]}$ obtained by forming the *Cartier dual* of G.

Remark 1.3.1. — One verifies immediately that the assignment "$G \rightsquigarrow G^D$" defines a [contravariant] functor $\mathfrak{ffg}_R^{[p]} \to \mathfrak{ffg}_R^{[p]}$, that gives an *anti-equivalence* of categories.

Definition 1.4. — Let G be an object of the category $\mathfrak{ffg}_R^{[p]}$. Then we shall say that G is *principally quasi-polarizable* if G is isomorphic to G^D in $\mathfrak{ffg}_R^{[p]}$.

DEFINITION 1.5. — Let G be an object of the category $\mathfrak{ffg}_W^{[p]}$. Then one verifies immediately that $G \times_W R$ may be regarded as an object of the category $\mathfrak{ffg}_R^{[p]}$. Moreover, one also verifies immediately that the assignment "$G \rightsquigarrow G \times_W R$" defines a functor $\mathfrak{ffg}_W^{[p]} \to \mathfrak{ffg}_R^{[p]}$. We shall write

$$\mathrm{rdct}\colon \mathfrak{ffg}_W^{[p]} \longrightarrow \mathfrak{ffg}_k^{[p]}$$

for this functor in the case where we take the W-algebra "R" to be $k = W/pW$.

In the remainder of the present §1, let G be an object of the category $\mathfrak{ffg}_k^{[p]}$.

DEFINITION 1.6. — Let H be an object of the category $\mathfrak{ffg}_W^{[p]}$. Then we shall say that H is a *deformation* of G to W if G is isomorphic to $\mathrm{rdct}(H)$ in $\mathfrak{ffg}_k^{[p]}$.

DEFINITION 1.7. — We shall say that G is *deformable* if there exists a deformation of G to W.

The following notion is one central notion of the present paper.

DEFINITION 1.8. — We shall say that G is *pseudo-rigid* if the following two conditions are satisfied:

(1) The object G is deformable.

(2) If H_1, H_2 are deformations of G to W, then H_1 is isomorphic to H_2 in $\mathfrak{ffg}_W^{[p]}$.

REMARK 1.8.1.

(i) Let us observe that an arbitrary deformation [cf. condition (1) of Definition 1.8] of a *pseudo-rigid* object of the category $\mathfrak{ffg}_k^{[p]}$ may be regarded as an object H of the category $\mathfrak{ffg}_W^{[p]}$ that satisfies the following condition [cf. condition (2) of Definition 1.8]: For an object H' of the category $\mathfrak{ffg}_W^{[p]}$, it holds that H is *isomorphic* to H' in $\mathfrak{ffg}_W^{[p]}$ if and only if $H \times_W (W/pW)$ is *isomorphic* to $H' \times_W (W/pW)$ in $\mathfrak{ffg}_{W/pW}^{[p]}$.

(ii) Suppose that $p \neq 2$. Then it follows from [6, §3] that the functor $\mathfrak{ffg}_W^{[p]} \to \mathfrak{ffg}_{W[1/p]}^{[p]}$ of Definition 1.5 in the case where we take the W-algebra "R" to be $W[1/p]$ is *fully faithful*. In particular, one may conclude from [4, Corollary 8] that, for two objects H_1, H_2 of the category $\mathfrak{ffg}_W^{[p]}$, it holds that H_1 is *isomorphic* to H_2 in $\mathfrak{ffg}_W^{[p]}$ if and only if $H_1 \times_W (W/p^2W)$ is *isomorphic* to $H_2 \times_W (W/p^2W)$ in $\mathfrak{ffg}_{W/p^2W}^{[p]}$.

2. REVIEW OF A LINEAR ALGEBRA THEORY FOR GROUP SCHEMES OVER k

In the present §2, we maintain the notational conventions introduced at the beginning of the preceding §1. Write, moreover, Fr for the p-th power Frobenius automorphism of k.

In the present §2, we give a review of a certain linear algebra theory for p-torsion finite flat commutative group schemes *over* k [cf. Definition 2.1 and Proposition 2.5 below].

DEFINITION 2.1. — We shall write

$$\mathfrak{Dm}^{[p]}$$

for the category defined as follows:

- An object of the category $\mathfrak{Dm}^{[p]}$ is defined to be a collection $\mathbb{D} = (M_{\mathbb{D}} = M, F_{\mathbb{D}} = F, V_{\mathbb{D}} = V)$ of data consisting of a finitely generated k-module M and endomorphisms F, V of the module M such that the following three conditions are satisfied:
  - The endomorphism F is Fr-semilinear.
  - The endomorphism V is Fr^{-1}-semilinear.
  - The sequence of modules

$$M \xrightarrow{F} M \xrightarrow{V} M \xrightarrow{F} M$$

forms a complex.

- Let (M_1, F_1, V_1), (M_2, F_2, V_2) be objects of the category $\mathfrak{Dm}^{[p]}$. Then a morphism $(M_1, F_1, V_1) \to (M_2, F_2, V_2)$ in the category $\mathfrak{Dm}^{[p]}$ is defined to be a homomorphism $f \colon M_1 \to M_2$ of k-modules such that the equalities $f \circ F_1 = F_2 \circ f$, $f \circ V_1 = V_2 \circ f$ hold.

In the remainder of the present §2, let $\mathbb{D} = (M, F, V)$ be an object of the category $\mathfrak{Dm}^{[p]}$.

DEFINITION 2.2. — We shall say that $\mathbb{D}$ is *connected* if the endomorphism F of M is nilpotent.

DEFINITION 2.3. — We shall write

$$M^D \stackrel{\text{def}}{=} \mathrm{Hom}_k(M, k)$$

for the [necessarily finitely generated] k-module obtained by forming the k-dual of M,

$$F^D \colon M^D \longrightarrow M^D$$

for the [necessarily Fr-semilinear] endomorphism of M^D given by mapping $\phi \in M^D$ to the element of M^D obtained by forming the composite

$$M \xrightarrow{V} M \xrightarrow{\phi} k \xrightarrow[\sim]{\mathrm{Fr}} k,$$

and

$$V^D \colon M^D \longrightarrow M^D$$

for the [necessarily Fr^{-1}-semilinear] endomorphism of M^D given by mapping $\phi \in M^D$ to the element of M^D obtained by forming the composite

$$M \xrightarrow{F} M \xrightarrow{\phi} k \xrightarrow[\sim]{\mathrm{Fr}^{-1}} k.$$

DEFINITION 2.4. — One verifies immediately that the collection (M^D, F^D, V^D) of data may be regarded as an object of the category $\mathfrak{Dm}^{[p]}$. We shall write

$$\mathbb{D}^D$$

for this object.

REMARK 2.4.1. — One verifies immediately that the assignment "$\mathbb{D} \rightsquigarrow \mathbb{D}^D$" defines a [contravariant] functor $\mathfrak{Dm}^{[p]} \to \mathfrak{Dm}^{[p]}$, that gives an *anti-equivalence* of categories.

PROPOSITION 2.5. — *There exists a contravariant functor*

$$\mathcal{M} \colon \mathfrak{ffg}_k^{[p]} \longrightarrow \mathfrak{Dm}^{[p]}$$

that gives an **anti-equivalence** *of categories and, for each object G of the category $\mathfrak{ffg}_k^{[p]}$, satisfies the following three conditions:*

(1) *It holds that G is* **connected** *if and only if $\mathcal{M}(G)$ is* **connected**.

(2) *The object $\mathcal{M}(G^D)$ is* **naturally isomorphic** [*cf. Remark* 1.3.1 *and Remark* 2.4.1] *to the object $\mathcal{M}(G)^D$ in $\mathfrak{Dm}^{[p]}$.*

(3) *It holds that G is* **étale** *over k if and only if $F_{\mathcal{M}(G)}$ is an* **isomorphism**.

PROOF. — This assertion follows from, for instance, [2, Chapitre III, §1]. □

3. REVIEW OF A LINEAR ALGEBRA THEORY FOR GROUP SCHEMES OVER W

In the present §3, we maintain the notational conventions introduced at the beginning of the preceding §2.

In the present §3, we give a review of a certain linear algebra theory for p-torsion finite flat commutative group schemes *over* W [cf. Definition 3.6 and Proposition 3.11 below].

DEFINITION 3.1. — Let $\mathbb{D} = (M, F, V)$ be an object of the category $\mathfrak{Dm}^{[p]}$. Then we shall write

$$C_{\mathbb{D}} = C \overset{\mathrm{def}}{=} \mathrm{Im}(F) \subseteq M, \qquad H_{\mathbb{D}} = H \overset{\mathrm{def}}{=} \mathrm{Im}(V) \subseteq M$$

for the k-submodules of M obtained by forming the images of the Fr-, Fr^{-1}-semilinear endomorphisms F, V, respectively.

LEMMA 3.2. — *Let $\mathbb{D}_1$, $\mathbb{D}_2$ be objects of the category $\mathfrak{Dm}^{[p]}$ and $f\colon \mathbb{D}_1 \to \mathbb{D}_2$ a morphism in the category $\mathfrak{Dm}^{[p]}$. Then the* **inclusions** $f(C_{\mathbb{D}_1}) \subseteq C_{\mathbb{D}_2}$*,* $f(H_{\mathbb{D}_1}) \subseteq H_{\mathbb{D}_2}$ *hold.*

PROOF. — This assertion follows from the definition of morphisms in the category $\mathfrak{Dm}^{[p]}$. ☐

LEMMA 3.3. — *Let $\mathbb{D}$ be an object of the category $\mathfrak{Dm}^{[p]}$. Then the following assertions hold:*

(i) *The* **equalities** $\dim_k(C_{\mathbb{D}}) = \dim_k(H_{\mathbb{D}^D})$, $\dim_k(H_{\mathbb{D}}) = \dim_k(C_{\mathbb{D}^D})$ *hold.*

(ii) *It holds that the* **inclusion** $H_{\mathbb{D}} \subseteq C_{\mathbb{D}}$ *holds if and only if the* **inclusion** $C_{\mathbb{D}^D} \subseteq H_{\mathbb{D}^D}$ *holds.*

PROOF. — These assertions follow immediately from the various definitions involved. ☐

DEFINITION 3.4. — Let $\mathbb{D} = (M, F, V)$ be an object of the category $\mathfrak{Dm}^{[p]}$. Then we shall say that $\mathbb{D}$ is *deformable* if the complex $M \xrightarrow{F} M \xrightarrow{V} M \xrightarrow{F} M$ [cf. Definition 2.1] forms an exact sequence.

DEFINITION 3.5. — Let $\mathbb{D}$ be an object of the category $\mathfrak{Dm}^{[p]}$. Suppose that $\mathbb{D}$ is deformable. Then we shall refer to a k-linear splitting of the natural surjective homomorphism $M_{\mathbb{D}} \twoheadrightarrow M_{\mathbb{D}}/C_{\mathbb{D}}$ as a *deformation structure* on $\mathbb{D}$.

REMARK 3.5.1. — Let $\mathbb{D}$ be an object of the category $\mathfrak{Dm}^{[p]}$.

(i) Suppose that $\mathbb{D}$ is *deformable*. Let $L \subseteq M_{\mathbb{D}}$ be a k-submodule of $M_{\mathbb{D}}$. Then one verifies immediately that L determines a *deformation structure* on $\mathbb{D}$ in the sense of Definition 3.5 if and only if the pair $(L, \mathbb{D})$ is a *finite Honda system* in the sense of [3, §9.4]. [Here, let us recall that a *finite Honda system* in the sense of [3, §9.4] is defined to be a collection $(J, (N, F_N, V_N))$ of data consisting of

- a W-module N of finite length,
- an endomorphism F_N of the module N semilinear with respect to the automorphism of W that lifts Fr,
- an endomorphism V_N of the module N semilinear with respect to the automorphism of W that lifts Fr^{-1}, and
- a W-submodule $J \subseteq N$ of N

such that

- both $F_N \circ V_N$ and $V_N \circ F_N$ coincide with the endomorphism of N given by multiplication by p,
- the restriction of V_N to the submodule $J \subseteq N$ is injective,
- the composite $J \hookrightarrow N \twoheadrightarrow N/\mathrm{Im}(F_N)$ factors through the natural surjective homomorphism $J \twoheadrightarrow J/pJ$, and, moreover,

- the resulting homomorphism $J/pJ \to N/\mathrm{Im}(F_N)$ is an isomorphism.]

(ii) One also verifies immediately from the discussion of (i) that $\mathbb{D}$ is *deformable* if and only if there exists a k-submodule $L \subseteq M_{\mathbb{D}}$ of $M_{\mathbb{D}}$ such that the pair $(L, \mathbb{D})$ is a *finite Honda system* in the sense of [3, §9.4].

DEFINITION 3.6. — We shall write $\mathfrak{fHs}^{[p]}$ for the category defined as follows:

- An object of the category $\mathfrak{fHs}^{[p]}$ is defined to be a collection $\mathbb{H} = (\mathbb{D}, s)$ of data consisting of a deformable object $\mathbb{D}$ of the category $\mathfrak{Dm}^{[p]}$ and a deformation structure s on $\mathbb{D}$.

- Let $(\mathbb{D}_1, s_1)$, $(\mathbb{D}_2, s_2)$ be objects of the category $\mathfrak{fHs}^{[p]}$. Then a morphism $(\mathbb{D}_1, s_1) \to (\mathbb{D}_2, s_2)$ in the category $\mathfrak{fHs}^{[p]}$ is defined to be a morphism $f \colon \mathbb{D}_1 \to \mathbb{D}_2$ in the category $\mathfrak{Dm}^{[p]}$ such that the inclusion $f(\mathrm{Im}(s_1)) \subseteq \mathrm{Im}(s_2)$ holds.

DEFINITION 3.7. — We shall write

$$\mathcal{R} \colon \mathfrak{fHs}^{[p]} \longrightarrow \mathfrak{Dm}^{[p]}$$

for the functor defined by the assignment "$(\mathbb{D}, s) \rightsquigarrow \mathbb{D}$".

DEFINITION 3.8. — Let $\mathbb{H}$ be an object of the category $\mathfrak{fHs}^{[p]}$. Then we shall say that $\mathbb{H}$ is *connected* if the object $\mathcal{R}(\mathbb{H})$ of the category $\mathfrak{Dm}^{[p]}$ is connected.

DEFINITION 3.9. — We shall write

$$\mathfrak{cfHs}^{[p]} \subseteq \mathfrak{fHs}^{[p]}$$

for the full subcategory of $\mathfrak{fHs}^{[p]}$ consisting of *connected* objects of $\mathfrak{fHs}^{[p]}$.

DEFINITION 3.10. — Let $\mathbb{H} = (\mathbb{D}, s)$ be an object of the category $\mathfrak{fHs}^{[p]}$. Then one verifies immediately that the k-submodule of $M_{\mathbb{D}}^D$ obtained by forming the kernel of the surjective homomorphism $M_{\mathbb{D}}^D \twoheadrightarrow \mathrm{Hom}_k(M_{\mathbb{D}}/C_{\mathbb{D}}, k)$ of k-modules induced by the injective homomorphism $s \colon M_{\mathbb{D}}/C_{\mathbb{D}} \hookrightarrow M_{\mathbb{D}}$ determines a deformation structure s^D on $\mathbb{D}^D$. We shall write

$$\mathbb{H}^D \stackrel{\mathrm{def}}{=} (\mathbb{D}^D, s^D)$$

for the resulting object of $\mathfrak{fHs}^{[p]}$.

REMARK 3.10.1. — One verifies immediately that the assignment "$\mathbb{H} \rightsquigarrow \mathbb{H}^D$" defines a [contravariant] functor $\mathfrak{fHs}^{[p]} \to \mathfrak{fHs}^{[p]}$, that gives an *anti-equivalence* of categories.

PROPOSITION 3.11. — *There exist contravariant functors*

$$\mathcal{M}\colon \mathfrak{ffg}_k^{[p]} \longrightarrow \mathfrak{Dm}^{[p]}, \qquad \mathcal{LM}\colon \mathfrak{ffg}_W^{[p]} \longrightarrow \mathfrak{f}\mathfrak{H}\mathfrak{s}^{[p]}$$

that satisfy the following five conditions:

(1) *The functor $\mathcal{M}$ gives an* **anti-equivalence** *of categories and satisfies the three conditions in the statement of Proposition* 2.5.

(2) *The functor $\mathcal{LM}$ restricts to an* **anti-equivalence** *of categories*

$$\mathfrak{cffg}_W^{[p]} \xrightarrow{\sim} \mathfrak{cf}\mathfrak{H}\mathfrak{s}^{[p]}.$$

Moreover, the functor $\mathcal{LM}\colon \mathfrak{ffg}_W^{[p]} \to \mathfrak{f}\mathfrak{H}\mathfrak{s}^{[p]}$ gives an **anti-equivalence** *of categories whenever $p \neq 2$.*

(3) *Let G be an object of the category $\mathfrak{ffg}_W^{[p]}$. Then it holds that G is* **connected** *if and only if $\mathcal{LM}(G)$ is* **connected**.

(4) *Let G be an object of the category $\mathfrak{ffg}_W^{[p]}$. Then $\mathcal{LM}(G^D)$ is* **naturally isomorphic** [*cf. Remark* 1.3.1 *and Remark* 3.10.1] *to $\mathcal{LM}(G)^D$ in $\mathfrak{f}\mathfrak{H}\mathfrak{s}^{[p]}$.*

(5) *Let G be an object of the category $\mathfrak{ffg}_W^{[p]}$. Then $\mathcal{M}(\mathrm{rdct}(G))$ is* **naturally isomorphic** *to $\mathcal{R}(\mathcal{LM}(G))$ in $\mathfrak{Dm}^{[p]}$.*

PROOF. — This assertion follows from, for instance, [3, §9] and [1, §1] [cf. also Remark 3.5.1, (i), (ii), of the present paper]. □

LEMMA 3.12. — *Let G be an object of the category $\mathfrak{ffg}_k^{[p]}$. Then it holds that G is* **deformable** *if and only if $\mathcal{M}(G)$ is* **deformable**.

PROOF. — Necessity follows from condition (5) of Proposition 3.11, together with Remark 3.5.1, (ii). Next, we verify sufficiency. Suppose that $\mathcal{M}(G)$ is *deformable*. Let us first observe that since [we have assumed that] k is *perfect*, there exist objects G_1 and G_2 of $\mathfrak{ffg}_k^{[p]}$ and an isomorphism $G \xrightarrow{\sim} G_1 \times_k G_2$ in $\mathfrak{ffg}_k^{[p]}$ [which thus induces an isomorphism $\mathcal{M}(G) \xrightarrow{\sim} \mathcal{M}(G_1) \oplus \mathcal{M}(G_2)$ in $\mathfrak{Dm}^{[p]}$] such that G_1 is *connected*, and, moreover, G_2 is *étale* over k. Thus, since [it is immediate that] an arbitrary object of $\mathfrak{ffg}_k^{[p]}$ *étale* over k is *deformable*, to verify sufficiency, we may assume without loss of generality, by replacing G by G_1, that G is *connected*. In particular, it follows immediately, in light of condition (1) of Proposition 2.5, from conditions (1), (2), (5) of Proposition 3.11, together with Remark 3.5.1, (ii), that G is *deformable*, as desired. This completes the proof of sufficiency, hence also of Lemma 3.12. □

4. PSEUDO-RIGID p-TORSION FINITE FLAT COMMUTATIVE GROUP SCHEMES

In the present §4, we prove the main result of the present paper [cf. Theorem 4.10 below].

In the present §4, we maintain the notational conventions introduced at the beginning of §2. Moreover, let $\mathbb{D} = (M, F, V)$ be a *deformable* object of the category $\mathfrak{Dm}^{[p]}$. Thus, we have a commutative diagram of k-modules

$$\begin{tikzcd} 0 \arrow[r] & C \cap H \arrow[r] \arrow[d, hook] & H \arrow[r] \arrow[d, hook] & H/(C \cap H) \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & C \arrow[r] & M \arrow[r] & M/C \arrow[r] & 0 \end{tikzcd}$$

— where the horizontal sequences are *exact*, and the vertical arrows are *injective*. Now let us observe that it is immediate that the natural homomorphism $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D}) \to \mathrm{Aut}_k(M)$ of groups is *injective*. Let us regard $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ as a subgroup of $\mathrm{Aut}_k(M)$ by means of this injective homomorphism:

$$\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D}) \subseteq \mathrm{Aut}_k(M).$$

LEMMA 4.1. — *An arbitrary automorphism of M contained in the subgroup $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D}) \subseteq \mathrm{Aut}_k(M)$* **preserves** *the k-submodules C, $H \subseteq M$ of M. In particular, we have a natural action of the group $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ on the set of* **deformation structures** *on $\mathbb{D}$.*

PROOF. — This assertion follows from Lemma 3.2. □

LEMMA 4.2. — *Let G be an object of $\mathfrak{ffg}_k^{[p]}$ such that $\mathcal{M}(G)$ [cf. Proposition 3.11] is* **isomorphic** *to $\mathbb{D}$ in $\mathfrak{Dm}^{[p]}$. Suppose that either G or G^D is* **connected** *whenever $p = 2$. Then it holds that G is* **pseudo-rigid** *if and only if the action of the group $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ on the set of deformation structures on $\mathbb{D}$ [cf. Lemma 4.1] is* **transitive**.

PROOF. — This assertion follows immediately from Proposition 3.11. □

DEFINITION 4.3. — We shall write

$$U(\mathbb{D}) \subseteq \mathrm{Aut}_k(M)$$

for the subgroup of $\mathrm{Aut}_k(M)$ consisting of [necessarily unipotent] automorphisms of the k-module M that preserve the k-submodules C and H of M and, moreover, induce the identity automorphisms of the four subquotients C, H, M/C, and M/H of M.

LEMMA 4.4. — *The following assertions hold:*

(i) *The* **inclusion** *$U(\mathbb{D}) \subseteq \mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ holds.*

(ii) *Suppose that the* **equality** *$C = H$ holds. Then the action of $U(\mathbb{D})$ on the set of deformation structures on M [cf. (i) and Lemma 4.1] is* **transitive**.

PROOF. — Assertion (i) follows immediately from the definition of the category $\mathfrak{Dm}^{[p]}$ and the definition of the notion of *deformability*. Next, we verify assertion (ii). Let us first observe that it follows immediately from the various definitions involved that the set of deformation structures on $\mathbb{D}$ [i.e., the set of k-linear splittings of the natural surjective homomorphism $M \twoheadrightarrow M/C$] has a *natural structure of* $\mathrm{Hom}_k(M/C, C)$*-torsor*. Moreover, one also verifies immediately that the equality $C = H$, together with the definition of the subgroup $U(\mathbb{D})$, implies that there exists an isomorphism $U(\mathbb{D}) \xrightarrow{\sim} \mathrm{Hom}_k(M/C, C)$ of groups, that is *compatible* with the respective actions on the set of deformation structures on $\mathbb{D}$. Thus, we conclude that the action of $U(\mathbb{D})$ on the set of deformation structures on M is *transitive*, as desired. This completes the proof of assertion (ii), hence also of Lemma 4.4. □

DEFINITION 4.5. — Let s be a deformation structure on $\mathbb{D}$. Then we shall say that s is *H-full* if the image of the k-submodule $H/(C \cap H) \subseteq M/C$ by $s\colon M/C \hookrightarrow M$ is contained in the k-submodule $H \subseteq M$ [cf. the diagram in the discussion at the beginning of the present §4].

LEMMA 4.6. — *The following assertions hold:*

(i) *A deformation structure on* $\mathbb{D}$ *obtained as an element of the* $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$*-orbit of an* ***$H$*-full** *deformation structure on* $\mathbb{D}$ *is* ***H*-full**.

(ii) *There exists an* ***H*-full** *deformation structure on* $\mathbb{D}$.

(iii) *The following two conditions are equivalent:*

(1) *Either the* **inclusion** $C \subseteq H$ *or the* **inclusion** $H \subseteq C$ *holds.*

(2) *An arbitrary deformation structure on* $\mathbb{D}$ *is* ***H*-full**.

(iv) *Suppose that condition* (2) *in* (iii) *is* **not satisfied**. *Then the action of the group* $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ *on the set of deformation structures on* $\mathbb{D}$ *is* **not transitive**.

PROOF. — Assertion (i) follows from Lemma 4.1. Assertion (ii) follows from the elementary theory of linear algebra. Next, we verify assertion (iii). If the inclusion $C \subseteq H$ holds, then it follows immediately from assertion (ii) that condition (2) is satisfied. Moreover, if the inclusion $H \subseteq C$ holds, then the k-module $H/(C \cap H)$ is *zero*, which thus implies that condition (2) is satisfied. This completes the proof of the implication (1) ⇒ (2).

Next, to verify the implication (2) ⇒ (1), suppose that condition (1) is *not satisfied.* Let s be an *H-full* deformation structure on $\mathbb{D}$ [cf. assertion (ii)] and $e_1, \ldots, e_d$ elements of M/C that form a *basis* of the finitely generated k-module M/C such that $e_1, \ldots, e_h$ form a *basis* of the k-submodule $H/(C \cap H)$ for some $h \in \{0, \ldots, d\}$. Now let us observe that since [we have assumed that] $H \not\subseteq C$, the inequality $h \neq 0$ holds. Moreover, let us also observe that since [we have assumed that] $C \not\subseteq H$, there exists an element m of $C \setminus (C \cap H)$. Then, by considering the assignment "$(e_1, e_2, \ldots, e_d) \mapsto (s(e_1) + m, s(e_2), \ldots, s(e_d))$", one may obtain a deformation structure on $\mathbb{D}$ that is *not H-full*, as desired. This completes the proof of the implication (2) ⇒ (1), hence also of assertion (iii).

Finally, we verify assertion (iv). It follows from assertion (ii) that there exists a deformation structure on $\mathbb{D}$ that is *H-full.* Moreover, it follows from our assumption that there exists a deformation structure on $\mathbb{D}$ that is *not H-full.* Thus, it follows from assertion (i) that the action of the group $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ on the set of deformation structures on $\mathbb{D}$ is *not transitive*, as desired. This completes the proof of assertion (iv), hence also of Lemma 4.6. □

One main technical observation of the present paper is as follows:

LEMMA 4.7. — *The following assertions hold:*

(i) *Suppose that one of the following three conditions is satisfied:*

(1) *The* **equality** $C = \{0\}$ *holds.*

(2) *The* **equality** $H = \{0\}$ *holds.*

(3) *The* **equality** $C = H$ *holds.*

Then the action of the group $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ *on the set of deformation structures on* $\mathbb{D}$ *is* **transitive**.

(ii) *If the action of the group* $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ *on the set of deformation structures on* $\mathbb{D}$ *is* **transitive**, *then either the* **inclusion** $C \subseteq H$ *or the* **inclusion** $C_{\mathbb{D}^D} \subseteq H_{\mathbb{D}^D}$ *holds.*

PROOF. — First, we verify assertion (i). If condition (1) is satisfied, then it is immediate that the set of deformation structures on $\mathbb{D}$ is *of cardinality one*. If condition (2) is satisfied, then since $\mathbb{D}$ is *deformable*, the equality $C = M$ holds, which thus implies that the set of deformation structures on $\mathbb{D}$ is *of cardinality one*. Thus, we conclude that assertion (i) holds if either condition (1) or condition (2) is satisfied. Assertion (i) in the case where condition (3) is satisfied follows from Lemma 4.4, (i), (ii). This completes the proof of assertion (i). Assertion (ii) follows from Lemma 3.3, (ii), and Lemma 4.6, (iii), (iv). This completes the proof of Lemma 4.7. ☐

DEFINITION 4.8. — Let G be an object of the category $\mathfrak{ffg}_k^{[p]}$.

(i) We shall say that G is *multiplicative* if either G is zero or the following condition is satisfied: Let $\overline{k}$ be an algebraic closure of k. Then the finite flat commutative group scheme $G \times_k \overline{k}$ over $\overline{k}$ is isomorphic to the fiber product of finitely many copies of the finite flat commutative group scheme "$\boldsymbol{\mu}_p$", i.e., of p-th roots of unity, over $\overline{k}$.

(ii) We shall say that G is *superspecial* if either G is zero or the following condition is satisfied: Let $\overline{k}$ be an algebraic closure of k. Then there exist a positive integer r and, for each $i \in \{1, \ldots, r\}$, a supersingular elliptic curve E_i over $\overline{k}$ such that if, for each $i \in \{1, \ldots, r\}$, one writes $E_i[p]$ for the finite flat commutative group scheme over k obtained by forming the kernel of the endomorphism of E_i given by multiplication by p, then the finite flat commutative group scheme $G \times_k \overline{k}$ over $\overline{k}$ is isomorphic to the fiber product $E_1[p] \times_{\overline{k}} \cdots \times_{\overline{k}} E_r[p]$ over $\overline{k}$.

(iii) Let n be a positive integer. Then we shall say that G is *of Frobenius height* $\leq n$ if the image of the n-th iterate of the Frobenius endomorphism of G is zero.

REMARK 4.8.1. — Let us recall that every elliptic curve over a field admits a *principal polarization*. In particular, one verifies immediately from the various definitions involved that if k is *algebraically closed*, then every *superspecial* object of the category $\mathfrak{ffg}_k^{[p]}$ is *principally quasi-polarizable*.

LEMMA 4.9. — *Let G be an object of $\mathfrak{ffg}_k^{[p]}$ such that $\mathcal{M}(G)$ [cf. Proposition 3.11] is* **isomorphic** *to $\mathbb{D}$ in $\mathfrak{Dm}^{[p]}$. Then the following two conditions are equivalent:*

(1) *The finite flat commutative group scheme G is* **superspecial**.

(2) *The* **equality** *$C = H$ holds.*

PROOF. — Let us first observe that one verifies immediately from, for instance, [2, Chapitre III, §2] that, to verify Lemma 4.9, we may assume without loss of generality, by replacing G by the base-change of G to an algebraic closure of k, that k is *algebraically closed*.

Now we verify the implication (1) ⇒ (2). Let us first observe that it is immediate that, to verify the implication (1) ⇒ (2), we may assume without loss of generality that G is *isomorphic* to "$E_i[p]$" as in Definition 4.8, (ii). Then it is well-known [cf., e.g., [5, §5.6]] that condition (2) is satisfied, as desired. This completes the proof of the implication (1) ⇒ (2).

Finally, we verify the implication (2) ⇒ (1). Suppose that condition (2) is satisfied. Let us first observe that since the sequence $M \xrightarrow{F} M \xrightarrow{V} M \xrightarrow{F} M$ is *exact*, the Fr-, Fr^{-1}-semilinear endomorphisms F, V determine Fr-, Fr^{-1}-semilinear isomorphisms $M/H \xrightarrow{\sim} C$, $M/C \xrightarrow{\sim} H$, respectively. Write $\overline{F}$, $\overline{V}$ for these Fr-, Fr^{-1}-semilinear isomorphisms $M/C = M/H \xrightarrow{\sim} C = H$ [cf. condition (2)], respectively. Then since k is *algebraically closed*, and the composite

$$M/C \xrightarrow[\sim]{\overline{F}} C \xrightarrow[\sim]{\overline{V}^{-1}} M/C$$

is an Fr^2-*semilinear isomorphism*, it follows from [7, Exposé XXII, Proposition 1.1] that there exist elements $e_1, \dots, e_d$ of M/C such that these elements form a *basis* of the finitely generated k-module M/C, and, moreover, the equality $(\overline{V}^{-1} \circ \overline{F})(e_i) = e_i$, i.e., the equality $\overline{F}(e_i) = \overline{V}(e_i)$, holds for each $i \in \{1, \dots, d\}$. For each $i \in \{1, \dots, d\}$, let us fix a lifting $\widetilde{e}_i \in M$ of $e_i \in M/C$ and write $M_i \subseteq M$ for the k-submodule of M generated by $\overline{F}(e_i) = \overline{V}(e_i) \in C \subseteq M$ and the fixed lifting $\widetilde{e}_i \in M$. Then one verifies immediately from condition (2), together with the various definitions involved, that

- the collection $\mathbb{D}_i \stackrel{\mathrm{def}}{=} (M_i, F|_{M_i}, V|_{M_i})$ of data *forms* a deformable object of the category $\mathfrak{Dm}^{[p]}$ such that $C_{\mathbb{D}_i} = H_{\mathbb{D}_i}$ for each $i \in \{1, \dots, d\}$, and, moreover,
- the natural inclusions $M_i \hookrightarrow M$ — where i ranges over the elements of $\{1, \dots, d\}$ — determine an *isomorphism* $\mathbb{D}_1 \oplus \cdots \oplus \mathbb{D}_d \xrightarrow{\sim} \mathbb{D}$ in $\mathfrak{Dm}^{[p]}$.

In particular, we conclude immediately from Proposition 3.11 that, to verify the implication (2) ⇒ (1), we may assume without loss of generality, by replacing $\mathbb{D}$ by $\mathbb{D}_i$ for each $i \in \{1, \dots, d\}$, that $\dim_k(M) = 2$. On the other hand, if $\dim_k(M) = 2$, then the implication (2) ⇒ (1) is well-known [cf., e.g., [5, §5.6]]. This completes the proof of the implication (2) ⇒ (1), hence also of Lemma 4.9. □

The main result of the present paper is as follows:

THEOREM 4.10. — *Let p be a prime number, k a perfect field of characteristic p, and G a p-torsion finite flat commutative group scheme over k. Suppose that either G or the Cartier dual of G is* **connected** *whenever $p = 2$. Then the following assertions hold:*

(i) *If G is either* **étale** *over k,* **multiplicative** [*cf. Definition* 4.8, (i)], *or* **superspecial** [*cf. Definition* 4.8, (ii)], *then G is* **pseudo-rigid** [*cf. Definition* 1.8].

(ii) *If G is* **pseudo-rigid**, *then either G or the Cartier dual of G is* **of Frobenius height ≤ 2** [*cf. Definition* 4.8, (iii)].

(iii) *Suppose that G is* **principally quasi-polarizable** [*cf. Definition* 1.4]. *Then G is* **pseudo-rigid** *if and only if G is* **superspecial**.

PROOF. — First, we verify assertion (i). Let us observe that it follows — in light of Lemma 3.12 — from Lemma 4.2 and Lemma 4.7, (i), that G is *pseudo-rigid* if $\mathcal{M}(G)$ [cf. Proposition 3.11] is *deformable*, and, moreover, one of the three conditions of Lemma 4.7, (i) — i.e., in the case where we take the "$\mathbb{D}$" of Lemma 4.7, (i), to be $\mathcal{M}(G)$ — is satisfied. On the other hand,

- by conditions (2), (3) of Proposition 2.5, Lemma 3.3, (i), and condition (1) of Proposition 3.11, one concludes that, under the assumption that $\mathcal{M}(G)$ is *deformable*, condition (1) of Lemma 4.7, (i), is *equivalent* to the condition that G is *multiplicative*,
- by condition (3) of Proposition 2.5 and condition (1) of Proposition 3.11, one concludes that, under the assumption that $\mathcal{M}(G)$ is *deformable*, condition (2) of Lemma 4.7, (i), is *equivalent* to the condition that G is *étale* over k, and
- by Lemma 4.9, one concludes that, under the assumption that $\mathcal{M}(G)$ is *deformable*, condition (3) of Lemma 4.7, (i), is *equivalent* to the condition that G is *superspecial.*

This completes the proof of assertion (i).

Next, we verify assertion (ii). Let us observe that it follows — in light of Lemma 3.12 — from Lemma 4.2 and Lemma 4.7, (ii), that if G is *pseudo-rigid*, then either the inclusion $C_{\mathcal{M}(G)} \subseteq H_{\mathcal{M}(G)}$ or the inclusion $C_{\mathcal{M}(G)^D} \subseteq H_{\mathcal{M}(G)^D}$ holds. Thus, it follows immediately from the *exactness* of the sequence $M \xrightarrow{F} M \xrightarrow{V} M \xrightarrow{F} M$, together with condition (2) of Proposition 2.5 and condition (1) of Proposition 3.11, that either G or G^D is *of Frobenius height* ≤ 2, as desired. This completes the proof of assertion (ii).

Finally, we verify assertion (iii). Sufficiency follows from assertion (i). To verify necessity, suppose that G is *principally quasi-polarizable* and *pseudo-rigid*, which thus implies [cf. Lemma 4.2 and Lemma 4.7, (ii)] that either the inclusion $C_{\mathcal{M}(G)} \subseteq H_{\mathcal{M}(G)}$ or the inclusion $C_{\mathcal{M}(G)^D} \subseteq H_{\mathcal{M}(G)^D}$ holds. If the inclusion $C_{\mathcal{M}(G)} \subseteq H_{\mathcal{M}(G)}$ (respectively, $C_{\mathcal{M}(G)^D} \subseteq H_{\mathcal{M}(G)^D}$) holds, then since G [hence also G^D] is *principally quasi-polarizable*, it follows from Lemma 3.3, (ii), together with condition (2) of Proposition 2.5 and condition (1) of Proposition 3.11, that the equality $C_{\mathcal{M}(G)} = H_{\mathcal{M}(G)}$ (respectively, $C_{\mathcal{M}(G)^D} = H_{\mathcal{M}(G)^D}$) holds. In particular, it follows from Lemma 4.9 that G (respectively, G^D, hence also G) is *superspecial*, as desired. This completes the proof of assertion (iii), hence also of Theorem 4.10. □

REMARK 4.10.1. — Let p be a prime number and k a perfect field of characteristic p. Then there exists a *pseudo-rigid* p-torsion finite flat commutative group scheme over k

which is *neither étale* over k, *multiplicative*, *nor superspecial*. Such an example may be obtained by considering the following object "$\mathbb{D}$" of the category $\mathfrak{Dm}^{[p]}$ [cf. also the proof of Theorem 4.10]: Write

- $M \stackrel{\text{def}}{=} k \cdot e_1 \oplus k \cdot e_2 \oplus k \cdot e_3$ for the finitely generated k-module that admits a basis $\{e_1, e_2, e_3\} \subseteq M$,
- F for the Fr-semilinear endomorphism of M given by mapping

$$(e_1, e_2, e_3) \mapsto (0, e_1, e_2),$$

and

- V for the Fr^{-1}-semilinear endomorphism of M given by mapping

$$(e_1, e_2, e_3) \mapsto (0, 0, e_1).$$

Then one verifies easily that $\mathbb{D} \stackrel{\text{def}}{=} (M, F, V)$ is an object of the category $\mathfrak{Dm}^{[p]}$. Moreover, one also verifies easily that

- this object $\mathbb{D}$ is *connected* and *deformable*, and
- *neither* $C_{\mathbb{D}} = \{0\}$, $H_{\mathbb{D}} = \{0\}$, *nor* $C_{\mathbb{D}} = H_{\mathbb{D}}$ holds.

On the other hand, it follows from the various definitions involved that, for every a, $b \in k$, the automorphism of the k-module M given by mapping

$$(e_1, e_2, e_3) \mapsto (e_1,\ b^p e_1 + e_2,\ a e_1 + b e_2 + e_3)$$

determines an automorphism of $\mathbb{D}$ in $\mathfrak{Dm}^{[p]}$. In particular, one verifies immediately that

- the action of the group $\mathrm{Aut}_{\mathfrak{Dm}^{[p]}}(\mathbb{D})$ on the set of deformation structures on $\mathbb{D}$ is *transitive*.

REFERENCES

[1] B. Conrad: Finite group schemes over bases with low ramification. *Compositio Math.* **119** (1999), no. **3**, 239–320.

[2] J.-M. Fontaine: Groupes p-divisibles sur les corps locaux. Astérisque, No. **47-48**. *Société Mathématique de France, Paris*, 1977.

[3] J.-M. Fontaine and G. Laffaille: Construction de représentations p-adiques. *Ann. Sci. École Norm. Sup.* (**4**) **15** (1982), no. **4**, 547–608 (1983).

[4] S. Hattori: Ramification of a finite flat group scheme over a local field. *J. Number Theory* **118** (2006), no. **2**, 145–154.

[5] K.-Z. Li and F. Oort: Moduli of supersingular abelian varieties. Lecture Notes in Mathematics, **1680**. *Springer-Verlag, Berlin*, 1998.

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

[7] Groupes de monodromie en géométrie algébrique. II. Séminaire de Géométrie Algébrique du Bois-Marie 1967-1969 (SGA 7 II). Dirigé par P. Deligne et N. Katz. Lecture Notes in Mathematics, Vol. **340**. *Springer-Verlag, Berlin-New York*, 1973.

(Yuichiro Hoshi) RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO UNIVERSITY, KYOTO 606-8502, JAPAN

Email address: yuichiro@kurims.kyoto-u.ac.jp